ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ
ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ
ΚΑΤΕΥΘΥΝΣΗ: ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ ΚΑΙ ΔΙΚΤΥΩΝ

Διπλωματική Εργασία

« *Σχεδίαση Μηχανισμών Υποστήριξης Συνεργασίας σε Ad-Hoc Networks*»

ΡΟΥΣΣΙΝΟΣ ΠΑΡΙΣ – ΑΛΕΞΑΝΔΡΟΣ
Α.Μ. 92

Επιβλέπων: Δρ. ΛΟΥΤΑ ΜΑΛΑΜΑΤΗ

Κοζάνη, Οκτώβριος 2011

ΕΥΧΑΡΙΣΤΙΕΣ

Κατ' αρχάς θα ήθελα να ευχαριστήσω τους γονείς μου για τη στήριξη που μου έδωσαν καθ' όλη τη διάρκεια των σπουδών μου, και την καθηγήτρια μου κ. Λούτα για τη βοήθεια που μου προσέφερε κατά την υλοποίηση της παρούσας διπλωματικής, και για την άριστη συνεργασία μας. Τέλος, ευχαριστώ τους φίλους μου και τους συντρόφους μου που ήταν στο πλευρό μου όλο αυτό το διάστημα.

Αφιερώνω την διπλωματική εργασία στο Λαό μας, στην υπηρεσία του οποίου πρέπει να τίθεται η εκπαίδευση, η επιστήμη και η έρευνα.

«…τα βιβλία μου, στέρεα κι απλά
θα βρίσκουν πάντοτε μια θέση πάνω στα ξύλινα τραπέζια
ανάμεσα στο ψωμί
και τα εργαλεία του λαού».

Τ. Λειβαδίτης

ΠΕΡΙΕΧΟΜΕΝΑ

Κεφάλαιο 1

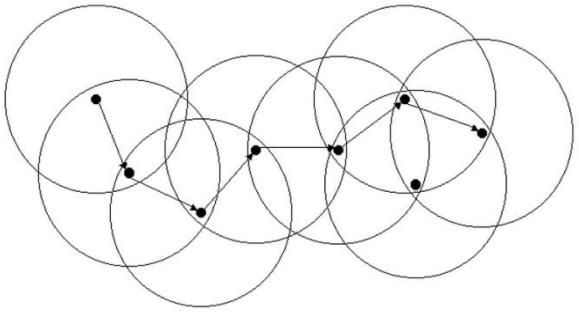
ΕΙΣΑΓΩΓΗ

1.1 ΕΙΣΑΓΩΓΗ ΣΤΑ AD-HOC ΔΙΚΤΥΑ

Οι σύγχρονες ανάγκες ασύρματης επικοινωνίας, καθώς και το γεγονός ότι ο βιώσιμος εξοπλισμός επικοινωνίας και οι φορητοί υπολογιστές γίνονται συμπαγέστεροι και διαθέσιμοι, έχουν δώσει το έναυσμα για ευρεία έρευνα και χρήση των **Δικτύων Ειδικού Σκοπού**, γνωστών και ως **Ad-Hoc Δίκτυα** [23].
Η έρευνα για τα ασύρματα ad-hoc δίκτυα βρίσκεται σε εξέλιξη εδώ και δεκαετίες. Η ιστορία των ad-hoc δικτύων, μπορεί να αναζητηθεί πίσω στα ραδιοφωνικά δίκτυα πακέτων της Υπηρεσίας Προηγμένων Ερευνητικών Έργων Άμυνας (DARPA)(PRnet), τα οποία εξελίχθηκαν στο προσαρμοστικό πρόγραμμα ραδιοφωνικών δικτύων (SURAD). Τα ad-hoc δίκτυα παίζουν σημαντικό ρόλο στις στρατιωτικές εφαρμογές και τις σχετικές ερευνητικές προσπάθειες, όπως το Σφαιρικό Κινητό Πρόγραμμα Συστημάτων Πληροφοριών (GloMo) και ο Βραχυπρόθεσμος Ψηφιακός Ραδιοφωνικός Σταθμός (NTDR). Τα τελευταία χρόνια αναπτύσσεται ραγδαία πλήθος βιομηχανικών και εμπορικών εφαρμογών για τα ασύρματα ad-hoc δίκτυα.

1.1.1 ΑΡΧΙΚΤΕΚΤΟΝΙΚΗ ΤΩΝ AD-HOC ΔΙΚΤΥΩΝ

Από τη δεκαετία του 1970, τα ασύρματα δίκτυα έχουν γίνει πολύ δημοφιλή στη βιομηχανία των επικοινωνιών, καθώς παρέχουν στους κινητούς χρήστες μεγάλες υπολογιστικές δυνατότητες και πρόσβαση σε πληροφορίες ανεξάρτητα από την θέση των χρηστών. Τα ασύρματα δίκτυα χωρίζονται σε δύο κατηγορίες, τα δίκτυα που βασίζονται σε κάποια εσωτερική υποδομή, και σε αυτά τα οποία δεν απαιτούν τη δομή αυτή. Τα ad-hoc δίκτυα αποτελούν την δεύτερη κατηγορία. Στα δίκτυα αυτά, δεν υπάρχουν καθορισμένοι δρομολογητές, ή κεντρικοί severs και σημεία πρόσβασης, καθώς κάθε κόμβος έχει ευθύνη για την οργάνωση και τον έλεγχο του δικτύου. Το σύνολο του ad-hoc δικτύου είναι κινητό και οι κόμβοι που το απαρτίζουν, μπορούν να κινούνται ελεύθερα, έχοντας τη δυνατότητα να συνδέονται και να επικοινωνούν μεταξύ τους. Βέβαια, απομακρυσμένοι κόμβοι, δεν έχουν τη δυνατότητα να επικοινωνούν άμεσα μεταξύ τους, και για το λόγο αυτό χρειάζεται να συμβάλουν στην προώθηση των μηνυμάτων τους, οι ενδιάμεσοι κόμβοι. Οι κόμβοι αναλαμβάνουν επίσης την αναζήτηση και εγκαθίδρυση διαδρομών δρομολόγησης, και μπορούν να βρίσκονται πάνω σε κάθε κινητό μέσο, όπως σε αυτοκίνητα, πλοία, φορτηγά, αεροπλάνα, ακόμα και να κατέχονται από ανθρώπους που κινούνται με τη μορφή πολύ μικρών συσκευών. Λόγω της συνεχούς κίνησης των κόμβων, οι ασύρματες ζεύξεις που τους συνδέουν, πρέπει να αλλάζουν διαρκώς. Παρακάτω φαίνεται ένα ad-hoc δίκτυο με κινητούς κόμβους ,όπου οι κύκλοι αναπαριστούν την εμβέλεια μετάδοσης τους.



Σχήμα 1.1.1 [24]

1.1.2 ΔΡΟΜΟΛΟΓΗΣΗ ΣΤΑ AD-HOC ΔΙΚΤΥΑ

Όπως αναφέρθηκε, τα ad-hoc δίκτυα λειτουργούν χωρίς κάποια εσωτερική υποδομή. Η μεγάλη κινητικότητα, το μεγάλο μέγεθος των δικτύων συνδυασμένο με την ετερογένεια και το εύρος ζώνης των συσκευών, καθώς και οι περιορισμοί στην διάθεση ενέργειας μπαταρίας, αποτελούν παράγοντες που λαμβάνονται υπόψη στη διαδικασία της δρομολόγησης. Τα δύο κύρια είδη πρωτοκόλλων δρομολόγησης που υπάρχουν σήμερα είναι τα εξής:

- Τα πρωτόκολλα δρομολόγησης οδηγούμενα από πίνακες που περιέχουν διανύσματα απόστασης και την κατάσταση των ζεύξεων.
- Τα πρωτόκολλα δρομολόγησης on-demand

Στην πρώτη κατηγορία, οι συνεπείς και ανανεωμένες πληροφορίες δρομολόγησης κρατούνται στους κόμβους, ενώ στη δεύτερη οι διαδρομές δρομολόγησης δημιουργούνται μόνο όταν αυτό απαιτείται από την πηγή, και διατηρούνται για όσο αυτή χρειάζεται. Μερικά από τα γνωστότερα πρωτόκολλα δρομολόγησης είναι τα LAR, DSDV, AODV και DSR. Παρόλα αυτά, όλα τα υπάρχοντα πρωτόκολλα δρομολόγησης, ενέχουν μειονεκτήματα όσον αφορά την εφαρμογή τους σε ad-hoc δίκτυα. Μερικοί λόγοι για τους οποίους συμβαίνει αυτό είναι οι παρακάτω:

- Η συνεχής αλλαγή τοπολογίας στο δίκτυο, οδηγεί σε μεγάλη απώλεια πακέτων.
- Η τροποποίηση των πινάκων δρομολόγησης κάθε κόμβου που βρίσκεται στην εμβέλεια επικοινωνίας, οδηγεί σε αύξηση της κατανάλωσης εύρους ζώνης και της επιβάρυνσης στο δίκτυο. Το ίδιο συμβαίνει και με την αποστολή των πινάκων δρομολόγησης και άλλων μηνυμάτων και αιτήσεων δρομολόγησης. Λαμβανομένου υπόψη, και του περιορισμένου εύρους ζώνης των ad-hoc δικτύων.
- Εισάγεται καθυστέρηση των δεδομένων που αποστέλλονται στους κινητούς κόμβους.
- Οι μεταδόσεις μεταξύ δύο κόμβων σε ένα ασύρματο δίκτυο, μπορεί να μην λειτουργούν ορθά και προς τις δύο κατευθύνσεις, με αποτέλεσμα κάποιες διαδρομές δρομολόγησης που εισάγονται από το εκάστοτε πρωτόκολλο να μην δουλεύουν σε κάθε περιβάλλον.
- Η δημιουργία πλεονάζουσων διαδρομών από τα πρωτόκολλα εισάγουν επιβάρυνση στο δίκτυο.
- Η περιοδική αποστολή πινάκων δρομολόγησης εισάγει σπατάλη της πολύτιμης για τους κινητούς κόμβους ενέργειας μπαταρίας.

Οι παραπάνω δυσκολίες στη δρομολόγηση αποτελούν παράγοντες που συνέβαλαν και λήφθηκαν υπόψη κατά ένα μερίδιο στη δημιουργία των μηχανισμών υποστήριξης συνεργασίας που διαπραγματεύεται η παρούσα εργασία.

1.1.3 ΚΑΤΑΝΑΛΩΣΗ ΕΝΕΡΓΕΙΑΣ ΣΤΑ AD-HOC ΔΙΚΤΥΑ

Η κατανάλωση ενέργειας αποτελεί έναν από τους σημαντικότερους παράγοντες στην απόδοση των ad-hoc δικτύων, και σχετίζεται με τη διάρκεια ζωής τους. Η κύρια πρόκληση για τα δίκτυα αυτά, αποτελεί το γεγονός ότι αν και η τεχνολογία των μπαταριών βελτιώνεται συνεχώς, οι ανάγκες για ενέργεια δεν θα ελαττωθούν ποτέ,

αφού αυξάνεται η ζήτηση σε εύρος ζώνης και ποιότητα υπηρεσιών, την ώρα που οι κινητοί κόμβοι έχουν περιορισμένα αποθέματα ενέργειας.
Στα ασύρματα ad-hoc δίκτυα χρειάζεται συνεχώς να εξοικονομείται ενέργεια, αφού η αντικατάσταση της μπαταρίας των κόμβων μπορεί να μην είναι εφικτή ανά πάσα στιγμή. Έτσι, το μέγεθος της συνδεσιμότητας των κόμβων εξαρτάται σε μεγάλο βαθμό από τα αποθέματα ενέργειας.
Η διαθέσιμη ενέργεια και η κατανάλωση της αποτελεί κρίσιμο σημείο των ad-hoc δικτύων και λόγω του γεγονότος ότι η ανάγκη για κατανάλωση όσο το δυνατόν λιγότερης ενέργειας, οδηγεί πολλές φορές τους κόμβους σε εγωιστικές συμπεριφορές. Κάτι τέτοιο σημαίνει ότι ένας κόμβος ad-hoc δικτύου μπορεί να επιλέξει να μην παρέχει απαιτούμενες υπηρεσίες, ώστε να εξυπηρετήσει με την εξοικονομούμενη από αυτές ενέργεια, τα δικά του συμφέροντα και τις δικές του μεταδόσεις.

1.1.4 ΑΣΦΑΛΕΙΑ ΣΤΑ AD-HOC ΔΙΚΤΥΑ

Εκτός των άλλων, η συνεχής αλλαγή της τοπολογίας, τα μικρά αποθέματα ενέργειας, μνήμης και εύρους ζώνης στα ad-hoc δίκτυα, καθιστούν την εγκαθίδρυση ασφάλειας, πιο δύσκολη στα ad-hoc από ότι στα υπόλοιπα ασύρματα δίκτυα. Η έλλειψη κεντρικής εσωτερικής δομής, καθιστά δύσκολη και την πιστοποίηση των δεδομένων.
Ένα ζήτημα που απαιτεί ασφάλεια στα δίκτυα είναι οι επιθέσεις σε αυτά. Τα θέματα ασφάλειας που λαμβάνονται υπόψη είναι τα εξής:

- Η *Διαθεσιμότητα* που εξασφαλίζει την παροχή των υπηρεσιών παρά τις επιθέσεις άρνησης παροχής.
- Η *Εμπιστευτικότητα* που εξασφαλίζει ότι οι πληροφορίες δεν αποκαλύπτονται σε μη εξουσιοδοτημένες οντότητες.
- Η *Ακεραιότητα* που εξασφαλίζει ότι τα μεταδιδόμενα μηνύματα δεν διαφθείρονται.
- Η *Πιστοποίηση* που ταυτοποιεί την οντότητα με την οποία επικοινωνεί ένας κόμβος.

Αν και έχουν δοθεί πολλές λύσεις ενάντια σε επιθέσεις όπως η διαγραφή ή τροποποίηση μηνυμάτων, η υπόδηση κάποιου κόμβου, φαίνεται ότι λόγω της ελαττωματικής αρχιτεκτονικής των ad-hoc δικτύων, αυτά καθίστανται ευάλωτα σε επιθέσεις ασφαλείας.
Ακόμα, στα δίκτυα υπάρχουν αλγόριθμοι που χρησιμοποιούνται για την ανίχνευση και απομόνωση από το δίκτυο ελαττωματικών κόμβων. Οι αλγόριθμοι αυτοί δεν βρίσκουν εύκολα εφαρμογή στα ad-hoc δίκτυα λόγω της συνεχούς αλλαγής της τοπολογίας, αφού απαιτούν επαναλαμβανόμενες μεταδόσεις μηνυμάτων σε όλους τους κινητούς κόμβους.

1.2 ΣΥΝΕΡΓΑΣΙΑ ΚΑΙ ΜΗΧΑΝΙΣΜΟΙ ΥΠΟΣΤΗΡΙΞΗΣ

Από τις προηγούμενες ενότητες, φαίνεται ότι τα δίκτυα ad-hoc στηρίζονται στη συνεργασία των κόμβων τους ώστε να υποστηρίξουν βασικές λειτουργίες τους, όπως προώθηση πακέτων, δρομολόγηση και διαχείριση, γεγονός το οποίο αυξάνει την ευαισθησία του δικτύου στη μη σωστή συμπεριφορά των κόμβων. Γενικά, η μη σωστή συμπεριφορά μπορεί να οριστεί ως απόκλιση από τη συνηθισμένη λειτουργικότητα, η οποία μπορεί να είναι μη ηθελημένη λόγω π.χ. σφαλμάτων, λαθών μετάδοσης και κινητικότητας κόμβων ή ηθελημένη, ώστε οι κόμβοι, λειτουργώντας με εγωιστικά κίνητρα να επωφεληθούν από συγκεκριμένες καταστάσεις. Η ηθελημένη μη σωστή συμπεριφορά των κόμβων μπορεί να αποδοθεί α) στο γεγονός ότι οι κόμβοι θέλουν να κάνουν οικονομία σε δικούς τους πόρους (π.χ. CPU, μνήμη, μπαταρία) μη προωθώντας πακέτα τα οποία δεν τους αφορούν (αν και περιμένουν οι υπόλοιποι κόμβοι να μεταφέρουν τη δική
τους κίνηση) και β) στην επιθυμία κάποιων κόμβων να επιφέρουν βλάβη και να διακόψουν την ορθή λειτουργία του δικτύου.
Η έλλειψη κεντρικής υποδομής λοιπόν, δίνει ευκαιρίες σε κακόβουλους επιτιθέμενους κόμβους, βλάπτοντας την ομαλή λειτουργία του δικτύου και επιτρέποντας τους να αποκτούν πλεονεκτήματα έναντι των υπόλοιπων κόμβων του ad-hoc δικτύου όπως:

- Καλύτερες υπηρεσίες έναντι των συνεργαζόμενων κόμβων
- Χρηματικά οφέλη, με την αξιοποίηση των μέτρων παροχής κινήτρων ή με την διακίνηση εμπιστευτικών πληροφοριών
- Εξοικονόμηση ενέργειας δρώντας εγωιστικά
- Αποτροπή κάποιου κόμβου από την ομαλή εξυπηρέτηση του
- Εξόρυξη δεδομένων για την εύρεση εμπιστευτικών πληροφοριών

Η ανάγκη για αποτροπή τέτοιων συμπεριφορών, για τη διατήρηση της απόδοσης και της ομαλής λειτουργίας των ad-hoc δικτύων, οδήγησε πολλούς επιστήμονες στον σχεδιασμό μηχανισμών υποστήριξης συνεργασίας, πρωτοκόλλων δηλαδή που εφαρμόζονται ως επέκταση στους εκάστοτε αλγόριθμους δρομολόγησης. Οι μηχανισμοί αυτοί, έχουν ως βασικό στόχο από τη μία την ενίσχυση της συνεργασίας μεταξύ των κόμβων με απόδοση κινήτρων ή επιβραβεύσεων, κι από την άλλη τον εντοπισμό και την παραδειγματική τιμωρία των κόμβων που δρουν εγωιστικά, δεν προσφέρουν τις απαιτούμενες υπηρεσίες, ή με κακές προθέσεις αποκτούν συμπεριφορά που βλάπτει τους υπόλοιπους κόμβους και γενικά το δίκτυο.

Οι Μηχανισμοί Υποστήριξης Συνεργασίας για Ad-Hoc δίκτυα, που αποτελούν και το αντικείμενο μελέτης της παρούσας διπλωματικής εργασίας, χωρίζονται ανάλογα με τον τρόπο λειτουργίας τους στις εξής τρεις βασικές κατηγορίες:

1. Οι ***Μηχανισμοί Υποστήριξης Συνεργασίας που βασίζονται στη φήμη (Reputaion – based)***. Η βασική λογική με την οποία λειτουργούν τα συγκεκριμένα πρωτόκολλα, είναι η δημιουργία και ανταλλαγή φήμης για κάθε κόμβο. Η φήμη των κόμβων χτίζεται βάσει του βαθμού συνεργασίας τους στο δίκτυο, βάσει της συμβολής τους στην προωθητική διαδικασία και την διαδικασία της δρομολόγησης. Ανάλογα με τη φήμη τους οι κόμβοι απολαμβάνουν τις υπηρεσίες του δικτύου (κόμβοι με καλή φήμη), ή αντίθετα στερούνται των υπηρεσιών, τιμωρούνται ή αποβάλλονται από την κοινότητα

του δικτύου (κόμβοι με κακή φήμη). Η μοντελοποίηση αυτή, ωθεί τους κόμβους στη συνεργασία με χρήση κινήτρων ή και φόβητρων, πράγμα που βελτιώνει την απόδοση των ad-hoc δικτύου και επιτρέπει την ομαλή λειτουργία τους.

2. Οι ***Μηχανισμοί Υποστήριξης Συνεργασίας που βασίζονται στις πιστώσεις (Credit – based)***. Τα πρωτόκολλα αυτά αντιμετωπίζουν την προώθηση πακέτων ως μια υπηρεσία που μπορεί να εκτιμηθεί και να χρεωθεί ανάλογα. Στην λειτουργία τους, εισάγεται η έννοια του εικονικού νομίσματος για την πραγματοποίηση συναλλαγών μεταξύ των κόμβων. Με άλλα λόγια, στα συγκεκριμένα σχήματα, ένας κόμβος χρεώνεται ή επιβραβεύεται για την χρήση ή την παροχή αντίστοιχα της υπηρεσία προώθησης πακέτων. Οι κόμβοι που διατηρούν υψηλό αριθμό πιστώσεων, έχουν τη δυνατότητα να εξυπηρετούν τα δικά τους συμφέροντα, αποκτώντας άνεση για τη μετάδοση των δικών τους πακέτων. Με τον τρόπο αυτό, εξασφαλίζεται ότι οι κόμβοι συμμετέχουν στην προωθητική διαδικασία, τους δίνονται δηλαδή οικονομικά κίνητρα για να συνεργαστούν. Από την άλλη, κόμβοι που δεν κατέχουν πιστώσεις, αδυνατούν να μεταδώσουν τα δικά τους μηνύματα στο δίκτυο, καθώς κάτι τέτοιο απαιτεί χρέωση.
3. Οι ***Υβριδικοί Μηχανισμοί Υποστήριξης Συνεργασίας (Hybrid)***. Οι μηχανισμοί αυτοί που αποτελούν αντικείμενο έρευνας τα τελευταία χρόνια, προσπαθούν να απαλείψουν τα μειονεκτήματα των δύο παραπάνω κατηγοριών, χρησιμοποιώντας στοιχεία από τις βασικές λειτουργίες τους. Βασική λογική που χρησιμοποιούν, είναι η χρήση του συστήματος χρέωσης της υπηρεσίας προώθησης, με βάση αυτή τη φορά, της φήμης των κόμβων. Περιληπτικά, κόμβοι με υψηλή φήμη, χρεώνονται λιγότερο από κόμβους με χαμηλή φήμη. Η τρίτη αυτή κατηγορία πρωτοκόλλων συνεργασίας, είναι η πιο νέα, και για το λόγο αυτό περιέχει μικρό αριθμό πρωτοκόλλων. Παρόλα αυτά, θεωρείται το μέλλον στην υποστήριξη συνεργασίας των κόμβων στα ad-hoc.

Όπως αναφέρθηκε, τα δίκτυα ad-hoc αποτελούν καινοτόμα λύση για πληθώρα σύγχρονων εφαρμογών και το λόγο αυτό, έχει μεγάλη σημασία η βέλτιστη λειτουργία τους και η αποσόβηση επιθέσεων, ή εγωιστικών και μη ομαλών συμπεριφορών των κόμβων, που μπορούν να βλάψουν την απόδοσή τους. Η παρούσα διπλωματική εργασία, επεξεργάζεται τη λειτουργία και την αποτελεσματικότητα των μηχανισμών υποστήριξης συνεργασίας που έχουν τη δυνατότητα να πετύχουν την καλύτερη λειτουργία των ad-hoc και την απαλλαγή τους από εγγενείς δυσλειτουργίες.

1.3 ΔΙΑΡΘΡΩΣΗ

Μέσα από την διπλωματική εργασία, επιδιώκεται η παρουσίαση δημοφιλών μηχανισμών υποστήριξης συνεργασίας από όλες τις βασικές κατηγορίες, η ανάλυση της λειτουργίας τους και η εκτίμηση της αποτελεσματικότητας τους όσον αφορά την ενίσχυση της συνεργασίας και την πρόληψη και τιμωρία ενάντια στους εγωιστικούς και κακόβουλους κόμβους στα ad-hoc δίκτυα. Πρωτότυπο μέρος της εργασίας, αποτελεί η προσπάθεια που πραγματοποιήθηκε για διάκριση και παρουσίαση όλων των βασικών ζητημάτων που λαμβάνονται υπόψη κατά τον σχεδιασμό των σχημάτων, η ύπαρξη τους ή όχι στα αναφερθέντα πρωτόκολλα με σκοπό την σύγκριση τους, και σε τελική ανάλυση η εξαγωγή συμπερασμάτων πάνω στην αποτελεσματικότητα τους συνολικά.
Η διπλωματική εργασία διαρθρώνεται ως εξής:
Στο Κεφάλαιο 2 παρουσιάζονται οι βασικότεροι και πιο γνωστοί μηχανισμοί υποστήριξης συνεργασία για ad-hoc δίκτυα που βασίζονται στη φήμη και αναλύεται διεξοδικά ο τρόπος με τον οποίο λειτουργούν και οι υποθέσεις που έχουν γίνει για το σχεδιασμό τους. Ακολουθεί, στο Κεφάλαιο 3 η σύγκριση των μηχανισμών αυτών πάνω σε βασικά θέματα που λαμβάνονται υπόψη για το σχεδιασμό τους, και η ανάλυση των θεμάτων αυτών. Αντίστοιχα, στο Κεφάλαιο 4 παρατίθενται βασικοί μηχανισμοί υποστήριξης συνεργασίας που βασίζονται στις πιστώσεις και ο τρόπος με τον οποίο βοηθούν στην τόνωση της συνεργασίας διεξοδικά. Ως συνέχεια στο Κεφάλαιο 5 αναλύονται αντιστοίχως τα κρίσιμα ζητήματα για το σχεδιασμό αυτών των πρωτοκόλλων και η διάκριση και σύγκριση τους πάνω στα ζητήματα αυτά. Τέλος, στο Κεφάλαιο 6 παρουσιάζονται πρότυποι υβριδικοί μηχανισμοί υποστήριξης συνεργασίας που έχουν προταθεί καθώς και η λογική που ακολουθούν και οι διαδικασίες λειτουργίας τους, με το Κεφάλαιο 7 να εξηγεί τις διαφορές και τα πλεονεκτήματα των υβριδικών σχημάτων έναντι στα μη υβριδικά. Η διπλωματική εργασία ολοκληρώνεται με την εξαγωγή συμπερασμάτων για το σύνολο των μηχανισμών υποστήριξης συνεργασίας, τις δυσκολίες που παρουσιάζονται κατά το σχεδιασμό τους, τη σύγκριση τους πάνω στα κρίσιμα ζητήματα και την εκτίμηση της αποτελεσματικότητας τους στο σκοπό για τον οποίο δημιουργήθηκαν. Η εξαγωγή των τελικών συμπερασμάτων γίνεται στο Κεφάλαιο 8, ενώ στο τέλος αναφέρεται και η χρησιμοποιηθείσα βιβλιογραφία και πηγές.

Κεφάλαιο 2

ΜΗΧΑΝΙΣΜΟΙ ΥΠΟΣΤΗΡΙΞΗΣ ΣΥΝΕΡΓΑΣΙΑΣ ΒΑΣΙΖΟΜΕΝΟΙ ΣΤΗ ΦΗΜΗ

Όπως αναφέρθηκε, οι μηχανισμοί υποστήριξης που βασίζονται στη φήμη, λειτουργούν βάσει της αρχής κατά την οποία διατηρούνται βαθμολογίες φήμης σε κάθε κόμβο, για μια μερίδα των υπόλοιπων κόμβων, που δημιουργείται και ανανεώνεται ανάλογα με τη συμπεριφορά τους, όσον αφορά την προώθηση, τη δρομολόγηση ή και άλλες λειτουργίες. Σε κάποιους μάλιστα μηχανισμούς, πραγματοποιείται και ανταλλαγή πληροφοριών φήμης που προκύπτουν από τις παρατηρήσεις και τις εμπειρίες των κόμβων, αναμεταξύ τους, για την προειδοποίηση των υπολοίπων κατά την εμφάνιση μη ομαλής συμπεριφοράς, και την ανάλογη τιμωρία των κακόβουλων ή εγωιστικών κόμβων. Παρακάτω, αναλύεται η λειτουργία των πιο γνωστών μηχανισμών του είδους και παρουσιάζονται τα εξαχθέντα αποτελέσματα και τα συμπεράσματα σχετικά με την ικανότητα τους στην ενίσχυση της συνεργασίας μεταξύ των κόμβων, και την τιμωρία των μη ομαλά συμπεριφερόμενων.

2.1 CONFIDANT

Το πρωτόκολλο CONFIDANT [1] λειτουργεί ως επέκταση σε πρωτόκολλα δρομολόγησης από την πηγή των δεδομένων. Παράδειγμα τέτοιου πρωτοκόλλου αποτελεί το DSR.

Το DSR αναπτύχθηκε ως πρωτόκολλο δρομολόγησης σε ασύρματα ad-hoc δίκτυα. Ως κλασικό πρωτόκολλο δρομολόγησης στα MANET, είναι θεμιτό να εξεταστεί σε γενικές γραμμές η λειτουργία του, καθώς τέτοιου είδους πρωτόκολλα αποτελούν τη βάση για επέκταση με πρωτόκολλα που υποστηρίζουν τη συνεργασία των κόμβων των ad-hoc δικτύων με σκοπό την εξάλειψη της μη επιθυμητής-εγωιστικής συμπεριφοράς κάποιων κόμβων του δικτύου.

Περιληπτικά το DSR λειτουργεί ως εξής: Όλοι οι κόμβοι αποστέλλουν ένα μήνυμα Αίτησης Διαδρομής(ROUTE REQUEST). Οι κόμβοι που λαμβάνουν το μήνυμα εισάγονται στην διαδρομή δρομολόγησης της πηγής των δεδομένων και προωθούν το μήνυμα στους γειτονικούς τους κόμβους, με εξαίρεση την περίπτωση που έχουν ξαναλάβει το μήνυμα στο παρελθόν. Εάν ο κόμβος που λαμβάνει το μήνυμα αποτελεί τον προορισμό των δεδομένων, η έχει στον πίνακα δρομολόγησης του διαδρομή προς τον προορισμό, αποστέλλει πίσω ένα μήνυμα Απάντησης(ROUTE REPLY), όπου περιέχει την συνολική διαδρομή δρομολόγησης της πηγής. Το μήνυμα ROUTE REPLY, μπορεί να αποσταλεί μέσω της αντίστροφης διαδρομής από όπου ήρθε το αρχικό μήνυμα. Εάν αυτό δεν είναι εφικτό λόγω ασύμμετρων ζεύξεων, ο κόμβος στέλνει ένα πακέτο ROUTE REQUEST που περιέχει την διαδρομή για να φτάσει στην πηγή. Η πηγή, αφού λάβει μια ή περισσότερες διαδρομές δρομολόγησης, επιλέγει την καλύτερη, την αποθηκεύει, και αποστέλλει μηνύματα μέσω αυτής. Κριτήρια όπως ο αριθμός των αλμάτων, η καθυστέρηση, το εύρος ζώνης, αλλά και ο χρόνος της άφιξης του μηνύματος REPLY, παίζουν κρίσιμο ρόλο στην επιλογή της διαδρομής δρομολόγησης και στον χρόνο παραμονής της στη μνήμη της πηγής. Ενδεικτικό σημάδι σύντομης διαδρομής είναι η ταχύτατη άφιξη του μηνύματος REPLY μετά την αποστολή ενός μηνύματος ROUTE REQUEST. Σε περίπτωση βλάβης σε κάποια ζεύξη ο κόμβος που αδυνατεί να προωθήσει το πακέτο στον επόμενο, αποστέλει πίσω στην πηγή ένα μήνυμα σφάλματος. Σε περίπτωση

διαδρομών που περιέχουν κάποια λανθασμένη ζεύξη(ζεύξη δύο κόμβων που βρίσκονται πλέον εκτός εμβέλειας ο ένας από τον άλλο), μπορεί να επιλεχθεί μια εναλλακτική διαδρομή που δεν θα περιέχει την ζεύξη αυτή.

Το πρωτόκολλο CONFIDANT δημιουργήθηκε ως μηχανισμός υποστήριξης συνεργασίας στα ad-hoc, σκοπεύοντας να προσφέρει προστασία ενάντια σε μη επιθυμητές συμπεριφορές όπως οι παρακάτω:

- Μη προώθηση δεδομένων ή μηνυμάτων ελέγχου από κάποιους κόμβους
- Απόκλιση κίνησης – ασυνήθιστη προσέλκυση κίνησης από κάποιους κόμβους που αποστέλλουν στην πηγή πολλές εξαιρετικές διαδρομές παταγωδώς, ή το αντίθετο, αποστέλλοντας μόνο μη συμφέρουσες διαδρομές
- Μη αποστολή μηνυμάτων σφάλματος ενώ έχει συμβεί σφάλμα, ή το αντίθετο
- Ασυνήθιστα συχνή ανανέωση διαδρομών δρομολόγησης
- Σιωπηλή αλλαγή διαδρομής, με την αλλοίωση της επικεφαλίδας των μηνυμάτων ελέγχου ή δεδομένων

Το CONFIDANT στοχεύει στην παρεμπόδιση των επιθέσεων από κακόβουλους κόμβους βασιζόμενο στην πρόληψη τους, τον εντοπισμό τους και την άμεση αντίδραση του συστήματος, καθώς οι περισσότερες από αυτές βασίζονται στην παράκαμψη μηχανισμών πρόληψης. Η λογική του CONFIDANT είναι σε γενικές γραμμές η εξής:
Επιδιώκεται η μη προώθηση των πακέτων κακόβουλων κόμβων ή κόμβων με μη ομαλή συμπεριφορά, από τους ομαλά συμπεριφερόμενους κόμβους του δικτύου, από τη στιγμή της ανίχνευσης της κακόβουλης συμπεριφοράς των πρώτων. Παρόλα αυτά, το CONFIDANT προσφέρει και έναν μηχανισμό που επιτρέπει σε κόμβους που έχουν κατηγορηθεί λανθασμένα για κακόβουλη συμπεριφορά ή σε κακόβουλους κόμβους που έχουν συμπεριφερθεί ομαλά για ένα συγκεκριμένο χρονικό διάστημα, να επανέλθουν ενεργά στις επικοινωνίες του δικτύου.
Η βασική ιδέα είναι ότι είναι ασύμφορο για τους κόμβους να συμπεριφέρονται κακόβουλα και ότι μόνο η ομαλή συμπεριφορά τους θα τους επιφέρει εξυπηρέτηση στις υπηρεσίες και λογική κατανάλωση ενέργειας.

2.1.1 ΛΕΙΤΟΥΡΓΙΑ

Το πρωτόκολλο CONFIDANT αναπτύχθηκε πάνω σε τέσσερις βασικές λειτουργίες:

1. Την **ανίχνευση των κακόβουλων – μη ομαλά συμπεριφερόμενων κόμβων** εντός του δικτύου, από τους γειτονικούς κόμβους
2. Την **προειδοποίηση των κόμβων** για την ύπαρξη κακόβουλων κόμβων
3. Την **δημιουργία καλής ή κακής φήμης** των κόμβων, ανάλογα με τη δραστηριότητά τους
4. Την **θέσπιση ή διαγραφή μονοπατιών** μέσω των οποίων θα δρομολογηθούν τα πακέτα

Βάσει τον λειτουργιών αυτών, το CONFIDANT διαθέτει τέσσερις μηχανισμούς – εργαλεία που αντιστοιχούν στην υλοποίηση κάθε μιας από τις παραπάνω λειτουργίες, με τη σειρά που αναφέρονται. Οι μηχανισμοί αυτοί είναι:

1. Το ***Monitor***
2. Το ***Trust Manager***

3. Το ***Reputation System***
4. Το ***Path Manager***

2.1.1.1 ΑΝΙΧΝΕΥΣΗ

Το εργαλείο Monitor, είναι υπεύθυνο για την ανίχνευση μη ομαλών ή κακόβουλων συμπεριφορών από τους κόμβους. Στα ασύρματα δίκτυα, το πιο πιθανό είναι η ανίχνευση μη ομαλής συμπεριφοράς από τους κόμβους που βρίσκονται στην εμβέλεια του κόμβου - «παραβάτη», από την πηγή και τον προορισμό. Σε γενικές γραμμές το πρωτόκολλο συμβάλει στην ανίχνευση καταστροφικής συμπεριφοράς όπως η άρνηση παροχής υπηρεσιών από κάποιον κόμβο ή η κακομεταχείριση των κινήτρων για την συνεργασία των κόμβων, με τον εξής τρόπο: κάθε κόμβος ανιχνεύει τους γειτονικούς του κόμβους για αποκλίνουσα από το ομαλό, συμπεριφορά.
Πιο συγκεκριμένα, οι κόμβοι εντοπίζουν αποκλίσεις του επόμενου κόμβου στην διαδρομή δρομολόγησης της πηγής με δύο τρόπους:

1. Ακούγοντας την μετάδοση του επόμενου κόμβου
2. Παρατηρώντας την συμπεριφορά του πρωτοκόλλου δρομολόγησης

Οι κόμβοι κρατώντας στη μνήμη τους ένα αντίγραφο του πακέτου που αποστέλλουν στον επόμενο κόμβο, ακούγοντας τη μετάδοση του επόμενου κόμβου, μπορούν να ανιχνεύσουν αλλαγές στο περιεχόμενο του πακέτου. Μπορούν επίσης να ανιχνευτούν όλες οι δυσλειτουργίες και οι μη επιθυμητές συμπεριφορές που αναφέρθηκαν παραπάνω, και για την αντιμετώπιση των οποίων δημιουργήθηκε το CONFIDANT.
Το Monitor, που αποτελεί συστατικό στοιχείο κάθε κόμβου, καταγράφει τις αποκλίσεις από την ομαλή συμπεριφορά, και στην περίπτωση που ανιχνεύει κακή συμπεριφορά από κάποιον κόμβο, καλείται το Reputation System για την διαχείριση της φήμης του κόμβου αυτού.

2.1.1.2 ΠΡΟΕΙΔΟΠΟΙΗΣΗ

Το στοιχείο Trust Manager, είναι υπεύθυνο για την προειδοποίηση των κόμβων για την ύπαρξη κακόβουλων κόμβων, καθώς και για τον έλεγχο της εμπιστοσύνης απέναντι στον κόμβο που προειδοποιεί. Η λειτουργία αυτή, έγκειται στην αποστολή και λήψη μηνυμάτων προειδοποίησης(ALARM) από τον Trust Manager κάθε κόμβου για την προειδοποίηση των υπόλοιπων κόμβων όσον αφορά την ύπαρξη και την ταυτότητα κακόβουλων κόμβων. Το εργαλείο λειτουργεί ως εξής:
Κάθε κόμβος που έχει παρατηρήσει ή έχει λάβει κάποια προειδοποίηση αναφερόμενη σε κάποια κακόβουλη συμπεριφορά, αποστέλλει μηνύματα ALARM, σε μια λίστα «φίλων» κόμβων που κρατά.
Καθώς ένα μήνυμα ALARM μπορεί να αποσταλεί είτε από τους κόμβους «φίλους» είτε από άγνωστους κόμβους του δικτύου, ο παραλήπτης πρέπει να εξακριβώσει την αξιοπιστία του, και για τον λόγο αυτό χρησιμοποιείται ένας μηχανισμός φιλτραρίσματος(επικύρωση κλειδιών, πιστοποίηση) των εισερχόμενων μηνυμάτων. Με χρήση διαφορετικών επιπέδων εμπιστοσύνης για κάθε υπογραφή πιστοποίησης, το Trust Manager προσδιορίζει εάν υπάρχει επαρκής και έμπιστη απόδειξη για την μη ομαλή λειτουργία κάποιου κόμβου.
Πιο συγκεκριμένα, ο Trust Manager αποτελείται από τα εξής συστατικά στοιχεία:

- Έναν πίνακα προειδοποιήσεων που περιέχει πληροφορίες για τα ληφθέντα μηνύματα ALARM στον κόμβο

- Έναν πίνακα εμπιστοσύνης που διαχειρίζεται τα επίπεδα εμπιστοσύνης των κόμβων για να προσδιοριστεί η αξιοπιστία των προειδοποιήσεων
- Μια λίστα φίλων, στην οποία περιέχονται οι φιλικοί κόμβοι στους οποίους ο κόμβος θα στέλνει δυνητικά, μηνύματα ALARM

Η εμπιστοσύνη μεταξύ των κόμβων είναι σημαντική στη δρομολόγηση και προώθηση πακέτων δεδομένων, κατά την λήψη απόφασης για:

1. την παροχή ή αποδοχή πληροφοριών δρομολόγησης
2. την αποδοχή ενός κόμβου ως μέρος της διαδρομής δρομολόγησης
3. την συμμετοχή σε μια διαδρομή δρομολόγησης που έχει προσδιοριστεί από άλλους κόμβους.

2.1.1.3 ΦΗΜΗ

Τα συστήματα φήμης χρησιμοποιούνται σε συστήματα online δημοπρασιών μεταξύ των κόμβων, για να αποφασιστεί ποιος κόμβος θα συμμετέχει στη διαδρομή δρομολόγησης, και παρέχουν μια βαθμονόμηση των συμμετεχόντων στην επικοινωνία. Οι συμμετέχοντες παρέχουν ανάδραση μεταξύ τους πάνω στις δραστηριότητες τους, ώστε να γίνουν αντιληπτές και να αξιολογηθούν.
Για να αποφευχθεί η κεντρικοποιημένη βαθμολόγηση των κόμβων στα ad-hoc δίκτυα, χρησιμοποιούνται τοπικές λίστες ή «μαύρες» λίστες για τους κακόβουλους κόμβους, σε κάθε κόμβο, που ανταλλάσσονται μεταξύ των κόμβων - «φίλων». Επιτρέπεται έτσι κατά την αναζήτηση διαδρομής δρομολόγησης, η αποφυγή της συμμετοχής σε αυτήν ανεπιθύμητων κόμβων. Για την αποφυγή λανθασμένων κατηγοριών για κάποιον κόμβο, χρησιμοποιούνται timeouts, και λίστες όπου μπορούν να καταχωρηθούν τέτοιοι κόμβοι και να επανέλθουν στην επικοινωνία μετά από κάποιο χρονικό διάστημα φυσιολογικής συμπεριφοράς.

Το στοιχείο Reputation System, είναι υπεύθυνο για τη βαθμολόγηση των κόμβων και την δημιουργία καλής ή κακής φήμης αυτών, όσον αφορά τη συμμετοχή τους στην δρομολόγηση και στην προώθηση πακέτων. Στο CONFIDANT, το Reputation System, διαχειρίζεται έναν πίνακα που περιέχει εγγραφές για τους κόμβους και την βαθμολόγηση τους. Η βαθμολογία κάθε κόμβου αλλάζει μόνο όταν υπάρχει επαρκής απόδειξη κακόβουλης συμπεριφοράς που έχει εκδηλωθεί κατά έναν αριθμό φορών, που ξεπερνά ένα ορισμένο κατώφλι για να αποφευχθούν οι συμπτώσεις. Η αλλαγή στη βαθμολογία γίνεται βάσει μιας συνάρτησης που δίνει διαφορετική βαρύτητα στις αναφορές, με γνώμονα την προέλευση τους. Πιο συγκεκριμένα, δίνει τη μεγαλύτερη βαρύτητα στις αναφορές που βασίζονται στην εμπειρία του ίδιου του κόμβου, μια μικρότερη βαρύτητα στις παρατηρήσεις του κόμβου για τους γειτονικούς κόμβους, και μια ακόμη μικρότερη βαρύτητα στην εμπειρία άλλων κόμβων που έχει αναφερθεί στον κόμβο.
Αφού προσδιοριστεί η βαρύτητα, αλλάζει αναλόγως η εγγραφή για τον κόμβο που έχει την μη ομαλή συμπεριφορά. Εάν η βαθμολογία του κόμβου έχει περιοριστεί τόσο πολύ ώστε να πέσει κάτω από ένα ορισμένο επιτρεπτό επίπεδο, καλείται το στοιχείο Path Manager. Το Reputation System βασίζεται στην αρνητική εμπειρία, καθώς

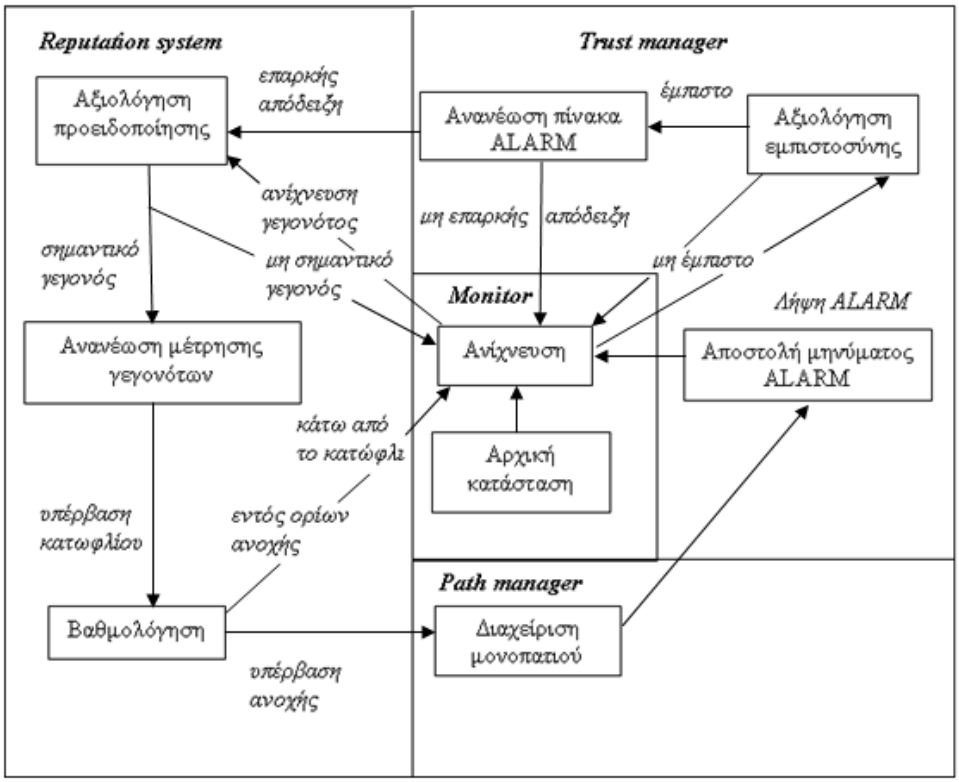
θεωρείται ότι η κακόβουλη συμπεριφορά κάποιων κόμβων, είναι εξαίρεση και όχι κανόνας, αποτελούν δηλαδή μειοψηφία στην διαδικασία της επικοινωνίας.

2.1.1.4 ΘΕΣΠΙΣΗ ΜΟΝΟΠΑΤΙΩΝ

Το στοιχείο Path Manager είναι υπεύθυνο για τη δρομολόγηση και τις αλλαγές στην διαδρομή δρομολόγησης κάθε κόμβου. Όπως αναφέρθηκε, καλείται όταν η βαθμολογία ενός κόμβου, που υπολογίζεται μέσω του μηχανισμού Reputation System, πέφτει κάτω από ένα συγκεκριμένο κατώφλι. Πιο συγκεκριμένα το Path Manager εκτελεί τις παρακάτω λειτουργίες:

- Ανακατατάσσει τα μονοπάτια δρομολόγησης, ανάλογα με συγκεκριμένες μετρήσεις ασφαλείας, όπως για παράδειγμα η φήμη των κόμβων σε ένα μονοπάτι
- Διαγραφή μονοπατιών που περιέχουν κακόβουλους κόμβους
- Αναλαμβάνει δράση όταν λαμβάνει αίτηση για μια διαδρομή δρομολόγησης, από κάποιον κακόβουλο κόμβο, όπως για παράδειγμα να αγνοήσει ή να μην απαντήσει σε αυτήν την αίτηση.
- Αναλαμβάνει δράση όταν λαμβάνει αίτηση για μια διαδρομή δρομολόγησης που περιέχει κάποιον κακόβουλο κόμβο στην διαδρομή δρομολόγησης της πηγής. Μπορεί να την αγνοήσει και να ειδοποιήσει την πηγή.

Παρακάτω φαίνεται σχηματικά η αρχιτεκτονική του CONFIDANT στον κόμβο:



Σχήμα 2.1.1

2.1.2 ΠΕΡΙΓΡΑΦΗ ΤΟΥ CONFIDANT

Μετά την ανάλυση των βασικών λειτουργιών και στοιχείων του CONFIDANT, μπορεί να γίνει μια περιγραφική ανάλυση της λειτουργίας του πρωτοκόλλου, όπως παρακάτω:
Κάθε κόμβος παρακολουθεί τη συμπεριφορά των γειτονικών κόμβων που βρίσκονται ένα βήμα(hop) μακριά του. Στην περίπτωση που μέσω της παρακολούθησης ανιχνευθεί κάποιο ύποπτο γεγονός, δίνεται η πληροφορία στο Reputation System του κόμβου. Εάν το γεγονός αυτό είναι σημαντικό για τον κόμβο, ελέγχεται αν η συχνότητα της εμφάνισης του ξεπερνά ένα προκαθορισμένο κατώφλι, το οποίο ορίζεται για κάθε κόμβο ανάλογα με τις απαιτήσεις που έχει για ασφάλεια. Με τον τρόπο αυτό, διαχωρίζεται η περίπτωση ύπαρξης κακόβουλης συμπεριφοράς στο δίκτυο, από την σύμπτωση όπως η σύγκρουση πακέτων. Σε περίπτωση λοιπόν που ξεπεραστεί αυτό το κατώφλι, το Reputation System του κόμβου ανανεώνει τη βαθμολογία που έχει ο κόμβος που δημιούργησε το ύποπτο γεγονός. Εάν η βαθμολογία αυτή ξεφύγει από το επιτρεπτό όριο, αποστέλλεται η πληροφορία στον Path Manager, που διαγράφει από τη μνήμη δρομολόγησης του κόμβου, όλες τις διαδρομές δρομολόγησης που περιέχουν τον ύποπτο κόμβο. Στην συνέχεια ο κόμβος συνεχίζει την ανίχνευση των γειτονικών κόμβων μέσω του Monitor.
Για να ειδοποιήσει το υπόλοιπο δίκτυο για το γεγονός, αποστέλλει ένα μήνυμα ALARM με τον εξής τρόπο:
Το μήνυμα αποστέλλεται από τον Trust Manager του κόμβου που ανίχνευσε το ύποπτο γεγονός. Το μήνυμα ALARM περιέχει τον τύπο της παραβίασης του πρωτοκόλλου, τον αριθμό των περιστατικών που έχει παρατηρήσει ο κόμβος, εάν το μήνυμα έχει προέλθει από τον αποστολέα, την διεύθυνση του κόμβου που στέλνει την προειδοποίηση, την διεύθυνση του κόμβου που παρατηρήθηκε για κακόβουλη συμπεριφορά και την διεύθυνση του παραλήπτη.
Όταν το Monitor ενός κόμβου παραλάβει ένα μήνυμα προειδοποίησης ALARM, το παραδίδει στο στοιχείο Trust Manager όπου αξιολογείται η πηγή του μηνύματος. Εάν η πηγή είναι τουλάχιστον μερικώς έμπιστη, ανανεώνεται ο πίνακας στον οποίο κρατούνται τα μηνύματα ALARM. Όταν υπάρχουν επαρκείς αποδείξεις ότι ο κατηγορούμενος για κακόβουλη συμπεριφορά κόμβος που αναφέρθηκε, όντως είναι κακόβουλος, η πληροφορία αυτή αποστέλλεται στο στοιχείο Reputation System, όπου αξιολογείται και πάλι για την σημαντικότητα της, για τον αριθμό των περιστατικών, και την ήδη συσσωρευμένη φήμη του κόμβου.
Επαρκείς αποδείξεις υπάρχουν όταν είτε η πηγή του μηνύματος ALARM είναι πλήρως έμπιστη, είτε όταν αρκετοί μερικώς έμπιστοι κόμβοι έχουν αναφέρει το ίδιο γεγονός και το άθροισμα της εμπιστευτικότητας τους είναι ίσο με την εμπιστευτικότητα ενός πλήρως έμπιστου κόμβου.

2.1.3 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ CONFIDANT

Η αποτελεσματικότητα του CONFIDANT, ως προς την ικανότητα του στην αντιμετώπιση των κακόβουλων κόμβων, ακόμα και σε δικτυακά περιβάλλοντα που περιλαμβάνουν κίνηση των κόμβων, και η επιβάρυνση του στο δίκτυο, αποδεικνύονται με τον υπολογισμό συγκεκριμένων δεικτών και μετρήσεων.
Τέτοιοι αντιπροσωπευτικοί δείκτες είναι οι παρακάτω:

- Η ***ρυθμαπόδοση του δικτύου(Throughput)***, που ορίζεται ως το σύνολο των δεδομένων που έχουν σταλεί προς τον χρόνο που απαιτήθηκε για την ολοκλήρωση της μετάδοσης
- Το σύνολο των ***απορριφθέντων πακέτων***
- Το συνολικό ***Goodput*** του δικτύου, που αντιπροσωπεύει τα δεδομένα που προωθήθηκαν προς την σωστή κατεύθυνση για κάθε κόμβο i ενός δικτύου με n κόμβους. Το Goodput, σε αντίθεση με το throughput επηρεάζεται από τις αναμεταδόσεις και την απώλεια πακέτων. Απώλεια πακέτων μπορεί να υπάρξει λόγω της γενικής κατάστασης του δικτύου που προκαλεί σφάλματα στις ζεύξεις και απροσιτότητα των κόμβων, αλλά και όταν κάποιος κακόβουλος κόμβος απορρίπτει πακέτα. Το τελευταίο αποτελεί και άμεση ένδειξη για την ύπαρξη μη ομαλής συμπεριφοράς από κάποιον κόμβο, γι αυτό και ο αριθμός των απορριφθέντων πακέτων μετράται ως απόλυτος αριθμός, αλλά και ως προς τον αριθμό των πακέτων που προέρχονται από κάποιον κόμβο και είναι προς λήψη.
  Το Goodput εκφράζεται με τον εξής μαθηματικό τύπο:

$$G = \frac{\sum_{i=1}^{n} Packets_{\mathrm{Re}ceived}}{\sum_{i=1}^{n} Packets_{Originated}}$$

Όπου Packets $_{\text{Received}}$ τα πακέτα που έχουν παραληφθεί από τον κόμβο, και Packets $_{\text{Originated}}$ τα πακέτα που έχουν προέλθει από κάθε κόμβο και είναι προς λήψη.

- Η ***επιβάρυνση(Overhead)*** του δικτύου, που προκαλείται από τα έξτρα μηνύματα(ALARM) που αποστέλλονται βάσει του CONFIDANT για να επαναπροσδιοριστούν οι διαδρομές δρομολόγησης στην περίπτωση ύπαρξης κακόβουλων κόμβων, επιδρώντας και στην κατανάλωση ενέργειας. Η μέτρηση του Overhead αφορά την επιπλέον επιβάρυνση που προκαλείται από το CONFIDANT σε σχέση με τη φυσιολογική επιβάρυνση δρομολόγησης στο δίκτυο, και που προκαλείται από τα μηνύματα ROUTE REQUEST, ROUTE REPLY και ERROR για παράδειγμα, του τυπικού πρωτοκόλλου DSR που περιγράφηκε. Σε ένα δίκτυο n κόμβων, όπου θεωρείται ως tx κάθε μετάδοση μηνύματος ελέγχου, το Overhead μπορεί να οριστεί μαθηματικά ως εξής:

$$O = \frac{\sum_{i=1}^{n} ALARM_{tx}}{\sum_{i=1}^{n} RREQ_{tx} + RREP_{tx} + ERROR_{tx}}$$

Όπου ALARM τα μηνύματα προειδοποίησης του CONFIDANT και RREQ, RREP, ERROR τα μηνύματα ROUTE REQUEST, ROUTE REPLY και ERROR του πρωτοκόλλου δρομολόγησης DSR, όπως έχουν περιγραφεί, για κάθε μετάδοση.

- Η ***ωφέλεια(Utility)*** στο δίκτυο για κάθε κόμβο, το κατά πόσο δηλαδή η συνεργασία που προωθεί το CONFIDANT επωφελεί τους κόμβους. Πιο

συγκεκριμένα μπορεί να εκφραστεί ως ο αριθμός των πακέτων που παράγονται η λαμβάνονται από τον κόμβο έναντι του αριθμού των πακέτων που προωθεί ο κόμβος για λογαριασμό άλλων κόμβων. Για τον λόγο αυτό υπολογίζεται η αναλογία των πακέτων που παράγονται από τους κόμβους με τα πακέτα που μεταδίδονται. Ορίζοντας ένα κόστος c_f για την προώθηση ενός πακέτου(βάσει της ισχύος που χρειάζεται, της χρήσης CPU και της χρήσης μνήμης) και ένα όφελος b_r για την λήψη ενός πακέτου ως προορισμός ή ένα όφελος b_s για την λήψη ενός πακέτου του κόμβου από τον προορισμό στον οποίο έχει αποσταλλεί, μπορεί μαθηματικά να οριστεί η ωφέλεια κάθε κόμβου i σε ένα δίκτυο ως εξής:

$$u_i = b_r \sum Packets_{received} + b_s \sum Packets_{sent\_successfully} - c_f \sum Packets_{transmitted}$$

Όπου $Packets_{received}$ τα πακέτα που έχει λάβει ο κόμβος, $Packets_{sent\text{-}successfully}$ τα πακέτα που έχουν αποσταλεί επιτυχώς από αυτόν και $Packets_{transmitted}$ τα πακέτα που έχει μεταδώσει συνολικά.

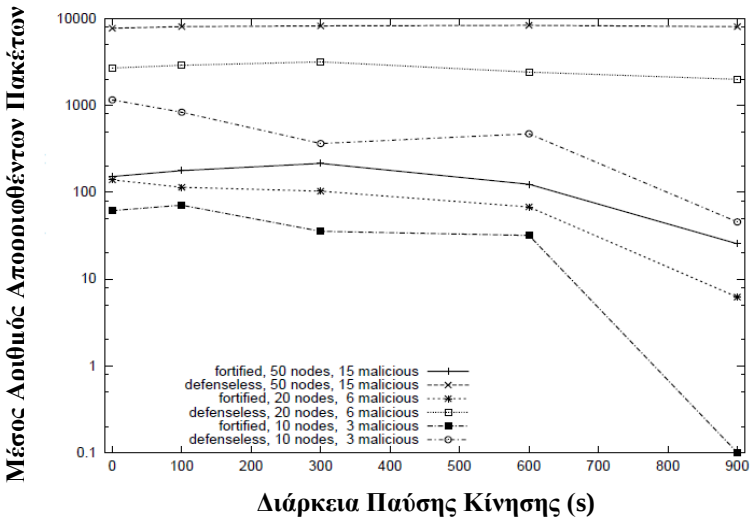
Σε ένα δίκτυο n κόμβων, η συνολική ωφέλεια μπορεί να εκφραστεί μαθηματικά ως:

$$U = \sum_{i=1}^{n} u_i$$

Οι προσομοιώσεις που πραγματοποίησαν οι δημιουργοί του CONFIDANT, έγιναν μέσω του προσομοιωτή κινητών ad-hoc δικτύων GloMoSim. Οι προσομοιώσεις έλαβαν μέρος σε εικονικό περιβάλλον με τα εξής χαρακτηριστικά:

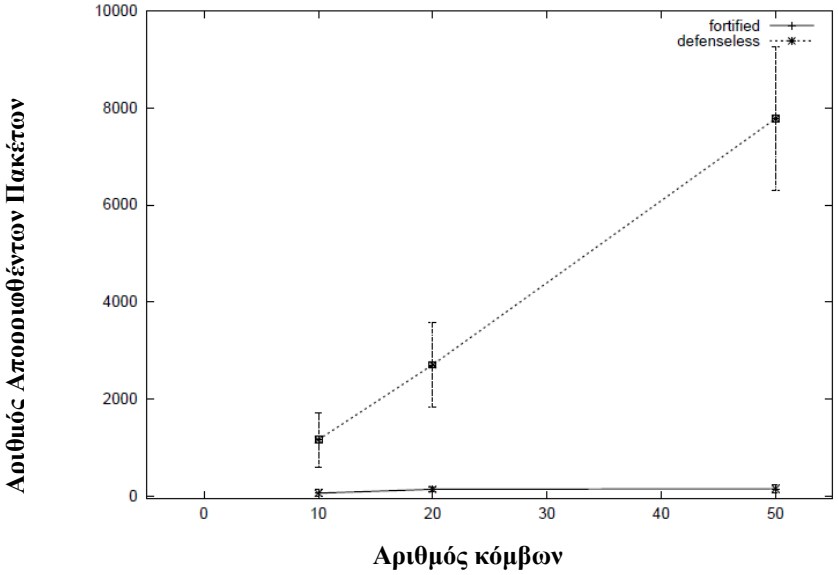
- Περιοχή 1000m x 1000m
- Ταχύτητα κόμβων μεταξύ 0 και 20m/s
- Εμβέλεια μετάδοσης 250m
- Ομοιόμορφη τοποθέτηση
- Τυχαία κίνηση
- Πρωτόκολλο MAC 802.11
- Χωρητικότητα αποστολής 2Mbps
- Εφαρμογή CBR
- Μέγεθος πακέτου 64B
- Χρόνος προσομοίωσης 900s

Βάσει μετρήσεων που αναφέρθηκαν αλλά και μελετώντας διαφορετικά σενάρια ως προς τον αριθμό των κόμβων, την κινητικότητα και το ποσοστό των κακόβουλων κόμβων, οι δημιουργοί του CONFIDANT έχουν καταλήξει στα εξής συμπεράσματα (που φαίνονται και στα εξαγόμενα διαγράμματα) σχετικά με την αποδοτικότητα του στην αντιμετώπιση μη ομαλής συμπεριφοράς στο δίκτυο, αλλά και την επιβάρυνση που αποφέρει:



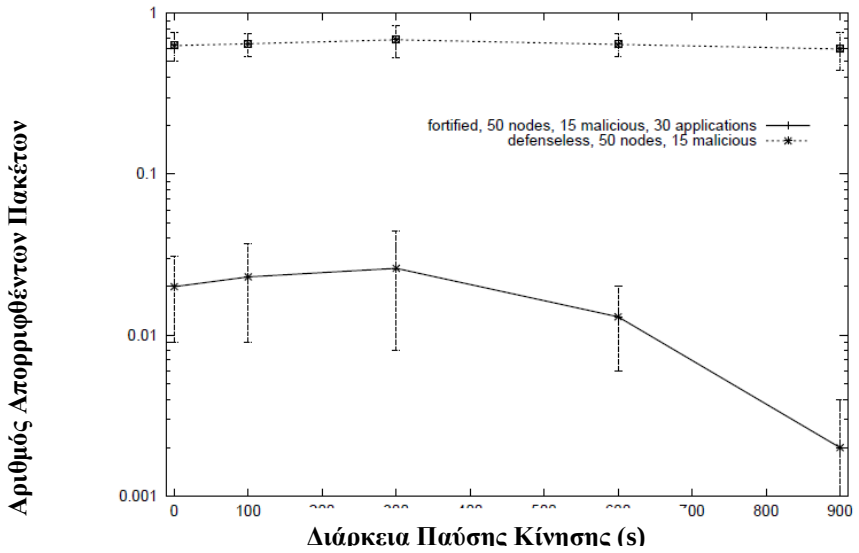
Διάγραμμα 2.1.1 (Πηγή [1])

Στο διάγραμμα αυτό που στον κάθετο άξονα έχει τον ***μέσο αριθμό απορριφθέντων πακέτων***, και στον οριζόντιο άξονα ***τη διάρκεια της παύσης της κίνησης σε δευτερόλεπτα***, γίνεται σύγκριση για δίκτυα στα οποία εφαρμόζεται το CONFIDANT και για δίκτυα στα οποία δεν εφαρμόζεται κάποιος μηχανισμός υποστήριξης συνεργασίας, για ποικίλο αριθμό συνολικών και κακόβουλων κόμβων. Συμπεραίνεται ότι αριθμός των απορριφθέντων πακέτων είναι σημαντικά χαμηλότερος σε ένα δίκτυο που εφαρμόζεται το CONFIDANT από όταν δεν εφαρμόζεται, και μειώνεται σταδιακά όσο μειώνεται και η κινητικότητα των κόμβων.



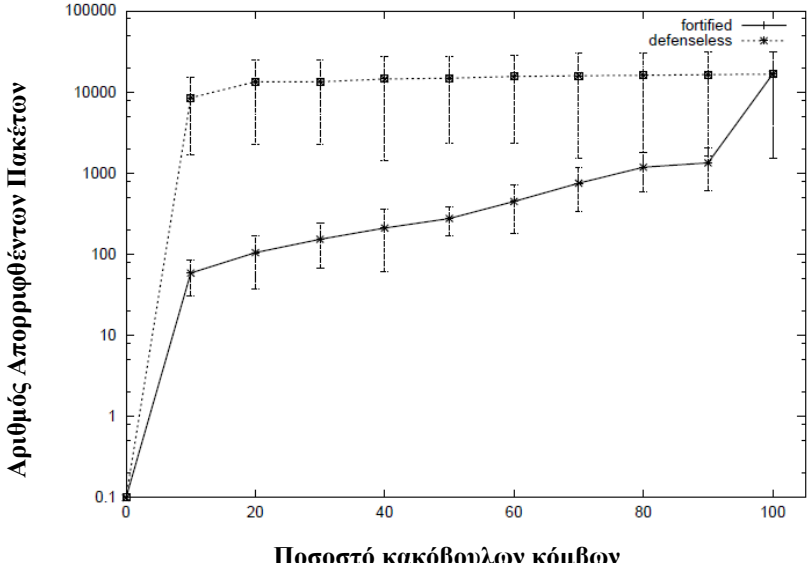
Διάγραμμα 2.1.2 (Πηγή [1])

Στο παραπάνω διάγραμμα, που στον κάθετο άξονα έχει τον ***αριθμό απορριφθέντων πακέτων***, και στον οριζόντιο άξονα ***τον αριθμό των κόμβων του δικτύου***, φαίνεται ότι ο αριθμός των απορριφθέντων πακέτων σε ένα δίκτυο με εφαρμοζόμενο το CONFIDANT μένει σταθερός άσχετα με το πλήθος των κόμβων του δικτύου, σε αντίθεση με ένα απλό ad-hoc δίκτυο.



Διάγραμμα 2.1.3 (Πηγή [1])

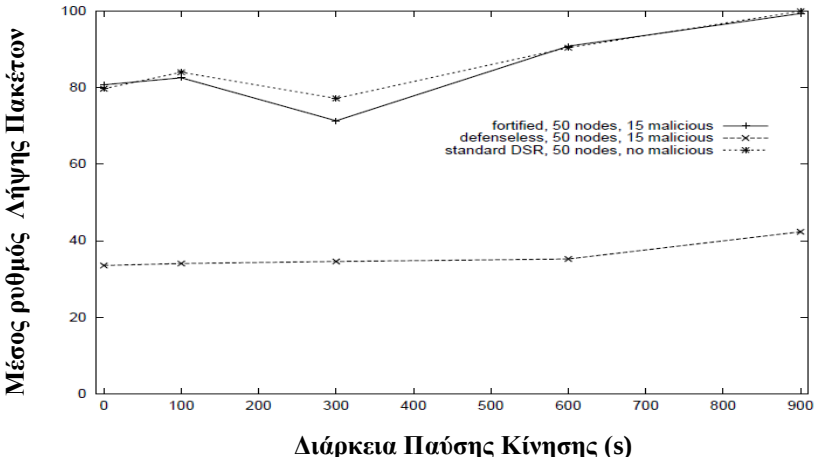
Στο παραπάνω διάγραμμα, που στον κάθετο άξονα έχει τον ***αριθμό απορριφθέντων πακέτων σε σχέση με τον συνολικό αριθμό πακέτων που παράγονται***, και στον οριζόντιο άξονα ***τη διάρκεια της παύσης της κίνησης σε δευτερόλεπτα***, γίνεται σύγκριση για δίκτυα στα οποία εφαρμόζεται το CONFIDANT και για δίκτυα στα οποία δεν εφαρμόζεται κάποιος μηχανισμός υποστήριξης συνεργασίας, για συγκεκριμένο αριθμό συνολικών και κακόβουλων κόμβων. Εξάγεται το συμπέρασμα ότι, ο αριθμός των απορριφθέντων πακέτων σε σχέση με τον συνολικό αριθμό των πακέτων που αποστέλλονται είναι σημαντικά χαμηλότερος (δεν ξεπερνούν το 3%) σε σχέση με ένα δίκτυο που δεν χρησιμοποιεί το CONFIDANT, και μειώνεται σταδιακά όσο μειώνεται η κινητικότητα των κόμβων.



Διάγραμμα 2.1.4 (Πηγή [1])

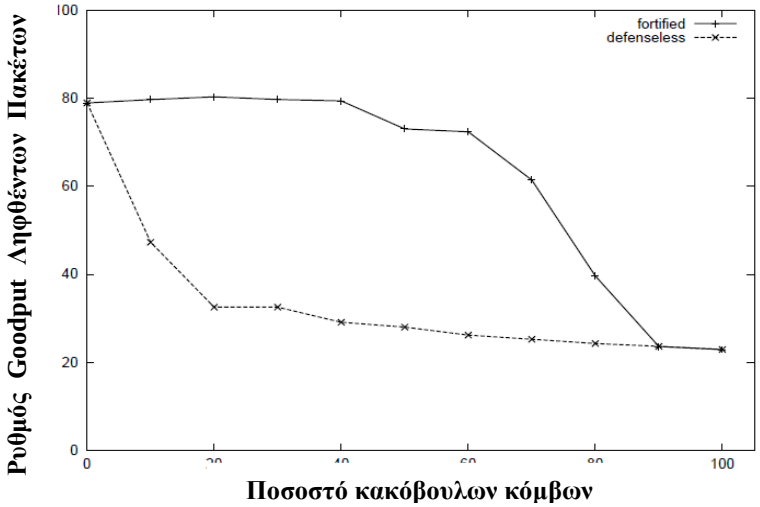
Στο παραπάνω διάγραμμα, που στον κάθετο άξονα έχει τον ***αριθμό απορριφθέντων πακέτων σε σχέση με τον συνολικό αριθμό πακέτων που παράγονται***, και στον οριζόντιο άξονα ***το ποσοστό των κακόβουλων κόμβων στο δίκτυο***, γίνεται σύγκριση

για δίκτυα στα οποία εφαρμόζεται το CONFIDANT και για δίκτυα στα οποία δεν εφαρμόζεται κάποιος μηχανισμός υποστήριξης συνεργασίας. Συμπεραίνεται ότι, ο αριθμός των απορριφθέντων πακέτων σε ένα δίκτυο συνεχούς κίνησης που χρησιμοποιεί το CONFIDANT, αυξάνεται μεν σταδιακά όσο αυξάνεται ο αριθμός των κακόβουλων κόμβων στο δίκτυο, αλλά παραμένει αισθητά χαμηλότερος σε σχέση με τον αντίστοιχο σε ένα δίκτυο χωρίς άμυνα, ακόμα και όταν το ποσοστό των κακόβουλων κόμβων φτάσει το 90%.



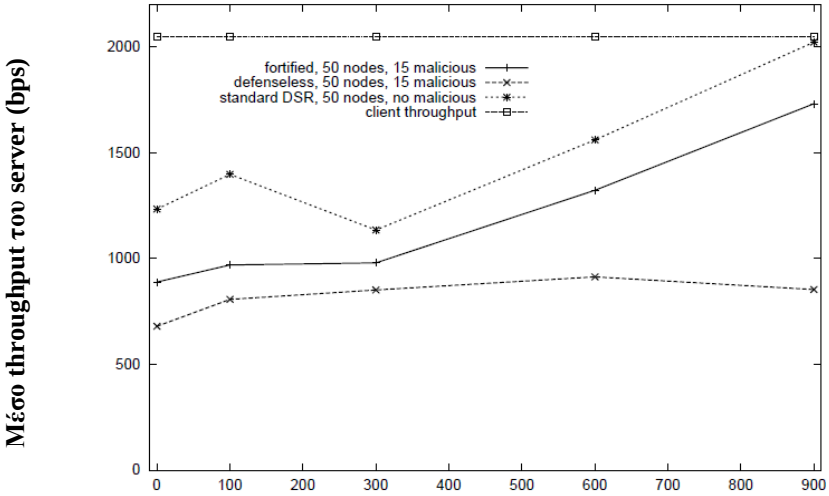
Διάγραμμα 2.1.5 (Πηγή [1])

Στο παραπάνω διάγραμμα, που στον κάθετο άξονα έχει τον ***μέσο ρυθμό λήψης πακέτων***, και στον οριζόντιο άξονα ***τη διάρκεια της παύσης της κίνησης σε δευτερόλεπτα***, γίνεται σύγκριση για δίκτυα στα οποία εφαρμόζεται το CONFIDANT και για δίκτυα στα οποία δεν εφαρμόζεται κάποιος μηχανισμός υποστήριξης συνεργασίας, με καθορισμένο αριθμό συνολικών και κακόβουλων κόμβων. Παρατηρείται ότι, το μέσο Goodput σε ένα δίκτυο που χρησιμοποιεί το CONFIDANT είναι υπερδιπλάσιο από το αντίστοιχο σε ένα δίκτυο χωρίς άμυνα, αυξάνεται όσο μειώνεται η κινητικότητα των κόμβων και προσεγγίζει το Goodput σε ένα δίκτυο με κάποιο τυπικό πρωτόκολλο δρομολόγησης στο οποίο όμως δεν υπάρχουν καθόλου κακόβουλοι κόμβοι.



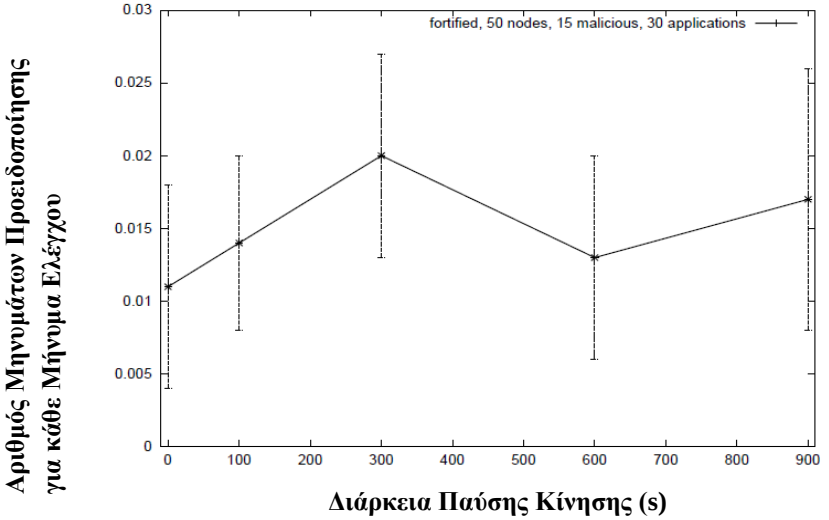
Διάγραμμα 2.1.6 (Πηγή [1])

Στο παραπάνω διάγραμμα, που στον κάθετο άξονα έχει τον ***ρυθμό του Goodput των λγφθέντων πακέτων σε σχέση με τον συνολικό αριθμό πακέτων που παράγονται***, και στον οριζόντιο άξονα ***το ποσοστό των κακόβουλων κόμβων στο δίκτυο***, γίνεται σύγκριση για δίκτυα στα οποία εφαρμόζεται το CONFIDANT και για δίκτυα στα οποία δεν εφαρμόζεται κάποιος μηχανισμός υποστήριξης συνεργασίας. Συμπεραίνεται ότι, το μέσο Goodput σε ένα φορτωμένο δίκτυο που χρησιμοποιεί το CONFIDANT είναι σταθερά μεγαλύτερο από το αντίστοιχο σε ένα δίκτυο χωρίς άμυνα, ακόμα και όταν το ποσοστό των κακόβουλων κόμβων φτάνει στο 80%.



Διάγραμμα 2.1.7 (Πηγή [1])

Στο διάγραμμα αυτό, που στον κάθετο άξονα έχει το ***μέσο throughput του server σε bps,*** και στον οριζόντιο ***τη διάρκεια της παύσης της κίνησης σε δευτερόλεπτα***, γίνεται σύγκριση για δίκτυα στα οποία εφαρμόζεται το CONFIDANT και για δίκτυα στα οποία δεν εφαρμόζεται κάποιος μηχανισμός υποστήριξης συνεργασίας, για συγκεκριμένο αριθμό συνολικών και κακόβουλων κόμβων. Φαίνεται ότι, το Throughput του server σε ένα δίκτυο που χρησιμοποιεί το CONFIDANT είναι μεγαλύτερο από το αντίστοιχο σε ένα δίκτυο χωρίς άμυνα και αυξάνεται όσο μειώνεται η κινητικότητα των κόμβων.



Διάγραμμα 2.1.8 (Πηγή [1])

Τέλος, στο διάγραμμα αυτό, που στον κάθετο άξονα έχει ***τον αριθμό των μηνυμάτων προειδοποίησης που μεταδίδονται για κάθε μήνυμα ελέγχου,*** και στον οριζόντιο ***τη διάρκεια της παύσης της κίνησης σε δευτερόλεπτα***, παρατηρείται ότι το μέσο Overhead που προκαλείται από τα μηνύματα προειδοποίησης του CONFIDANT είναι πολύ χαμηλό, το πολύ 3% των υπόλοιπων μηνυμάτων ελέγχου του δικτύου.

Συμπερασματικά, φαίνεται ότι το CONFIDANT είναι ένα πρωτόκολλο που μπορεί να αντιμετωπίσει επιθέσεις που αφορούν την προώθηση και την δρομολόγηση στα ασύρματα ad-hoc δίκτυα, επιβαρύνει ελάχιστα το δίκτυο, βελτιώνει τους δείκτες αξιολόγησης της λειτουργίας του δικτύου και λειτουργεί θετικά ακόμα και σε δίκτυα με υψηλό ποσοστό κακόβουλων κόμβων.

2.2 CONFIDANT IMPROVED

Το CONFIDANT αποτελεί έναν από τους πιο γνωστούς μηχανισμούς υποστήριξης συνεργασίας στα ad-hoc δίκτυα. Βασίζεται σε μεγάλο βαθμό στον σύστημα φήμης που διαθέτει(Reputation System) για την αξιολόγηση της συμπεριφοράς των κόμβων και τη βαθμολογία τους στην επικοινωνία, το οποίο όμως παίρνει υπόψη του κυρίως την αρνητική εμπειρία. Γενικότερα, τα συστήματα φήμης μπορεί να αποκτήσουν πρόβλημα στη σωστή λειτουργία τους λόγω λάθος κατηγοριών ή λάθος επαίνων για κάποιον κόμβο. Τα προβλήματα αυτά μπορούν να λυθούν εάν οι κόμβοι αξιοποιούν μόνο την δική τους εμπειρία, πράγμα που όμως ενέχει το βασικό μειονέκτημα της μη χρησιμοποίησης όλης της προσφερόμενης πληροφορίας από το δίκτυο. Για το λόγο αυτό, έχει δημιουργηθεί ένα Reputation System που μπορεί να εφαρμοστεί στο πρωτόκολλο CONFIDANT [2] και έχει τη δυνατότητα να αντιμετωπίσει την λανθασμένη μεταδιδόμενη πληροφορία.
Το σύστημα αυτό λειτουργεί σε γενικές γραμμές ως εξής:
Κάθε κόμβος του δικτύου κρατά μια βαθμολογία φήμης και μια βαθμολογία εμπιστοσύνης για κάθε άλλο κόμβο του δικτύου που τον αφορά. Σε τακτά χρονικά διαστήματα η πληροφορία από πρώτο χέρι(first-hand), που αντιπροσωπεύει την εξ ιδίων εμπειρία του κάθε κόμβου, ανταλλάσσεται με τους υπόλοιπους. Το σύστημα βασίζεται σε μια τροποποιημένη Βαϋσιανή προσέγγιση κατά την οποία, η πληροφορία από δεύτερο χέρι(second-hand) που αναφέρεται στην εμπειρία που αποκτάται χάρη στις αναφορές άλλων κόμβων, είναι αποδεκτή αν και μόνο αν δε είναι ασυμβίβαστη με την τρέχουσα βαθμολογία φήμης για κάθε κόμβο. Με τον τρόπο αυτό, οι βαθμολογίες φήμης ανανεώνονται ελαφρώς από την second-hand πληροφορία. Οι βαθμολογίες εμπιστοσύνης πάλι, ανανεώνονται βάσει της της συμβατότητας της second-hand πληροφορίας για την φήμη ενός κόμβου, με την εξ ιδίων βαθμολογία φήμης για αυτόν. Έτσι η βαθμολογία φήμης και εμπιστοσύνης κάθε κόμβου, είναι το αποτέλεσμα μιας συλλογής βαθμολογιών που διατηρούν οι υπόλοιποι κόμβοι. Με το παρόν σύστημα επίσης, επιτυγχάνεται η «λύτρωση» ενός κόμβου από τις κατηγορίες, αλλά και η αποτροπή της απότομης εκμετάλλευσης της καλής φήμης, με την χρήση επαναξιολόγησης και μηχανισμών ξεθωριάσματος - αλλαγής της τρέχουσας φήμης ενός κόμβου.
Η ουσία του συγκεκριμένου συστήματος φήμης είναι η δημιουργία συστημάτων που θα είναι ταυτόχρονα εύρωστα στο να αντιμετωπίζουν λανθασμένες βαθμολογίες φήμης και εμπιστοσύνης, και ικανά στο να ανιχνεύουν την κακόβουλη συμπεριφορά των κόμβων.

2.2.1 ΒΑΣΙΚΗ ΛΕΙΤΟΥΡΓΙΑ

Τα βασικά στοιχεία των συστημάτων φήμης είναι:

- Η αναπαράσταση της φήμης
- Ο τρόπος με τον οποίον υπολογίζεται και ανανεώνεται
- Ο τρόπος με τον οποίο λαμβάνονται υπόψη οι βαθμολογίες των υπολοίπων κόμβων.

Στο παρόν σύστημα φήμης, κάθε κόμβος i διατηρεί δύο βαθμολογίες για κάθε κόμβο j για τον οποίο ενδιαφέρεται:

1. Την ***βαθμολογία φήμης***, που αντιπροσωπεύει την γνώμη που έχει ο κόμβος i για τον κόμβο j, σχετικά με τη συμπεριφορά του στο

ad-hoc δίκτυο, κατά πόσο δηλαδή ο j συμμετέχει σωστά στη διαδικασία δρομολόγησης.

2. Την ***βαθμολογία εμπιστοσύνης***, που αντιπροσωπεύει την γνώμη που έχει ο κόμβος i για τον κόμβο j, σχετικά με την συμπεριφορά του στο σύστημα φήμης, κατά πόσο δηλαδή οι εξ ιδίων πληροφορίες που μεταδίδει ο j είναι αληθείς.

Στο συγκεκριμένο σύστημα φήμης, κάθε κόμβος i κρατά τις παραπάνω βαθμολογίες για κάθε κόμβο j, στις εξής δομές δεδομένων:

1. Την $\mathbf{R_{i,j}}$ για τη βαθμολογία φήμης
2. Την $\mathbf{T_{i,j}}$ για τη βαθμολογία εμπιστοσύνης
3. Την $\mathbf{F_{i,j}}$ για την first-hand πληροφορία που έχει ο κόμβος i σχετικά με τον κόμβο j

Το πλεονέκτημα που δίνει το συγκεκριμένο σύστημα φήμης, είναι η αξιοποίηση της διαδιδόμενης πληροφορίας φήμης από τους υπόλοιπους κόμβους του δικτύου, που έχει αποκτηθεί μέσω των παρατηρήσεων τους. Αυτό υλοποιείται με την εξής διαδικασία:
Κάθε φορά που ο κόμβος i κάνει μια εξ ιδίων παρατήρηση για την συμπεριφορά του κόμβου j, η first-hand πληροφορία $F_{i,j}$, και η βαθμολογία φήμης $R_{i,j}$, ανανεώνονται. Στη συνέχεια, ανά τακτά χρονικά διαστήματα οι κόμβοι αποστέλλουν την first-hand πληροφορία που έχουν αποκτήσει σε ένα μέρος των υπόλοιπων κόμβων. Το παρακάτω παράδειγμα βοηθάει στην κατανόηση της διαδικασίας:

- Όταν ο κόμβος i, λάβει από τον κόμβο k, first-hand πληροφορία $F_{k,j}$, για τον κόμβο j, εάν ο k είναι καταταγμένος ως έμπιστος ή εάν το $F_{k,j}$ είναι κοντά στο $R_{i,j}$, το $F_{k,j}$ γίνεται αποδεκτό από τον i, και χρησιμοποιείται για να μετατρέψει ελαφρώς το $R_{i,j}$. Αλλιώς, η βαθμολογία φήμης δεν ανανεώνεται.
  Η βαθμολογία εμπιστοσύνης $T_{i,k}$, ανανεώνεται σε κάθε περίπτωση, και βελτιώνεται ελαφρώς αν το $F_{k,j}$ είναι κοντά στο $R_{i,j}$, ενώ χειροτερεύει στην αντίθετη περίπτωση.

Κρίσιμη παρατήρηση για το παρόν σύστημα φήμης, είναι το γεγονός ότι από τις βαθμολογίες που αναφέρθηκαν και χρησιμοποιούνται από το σύστημα, μόνο η first-hand πληροφορία $F_{i,j}$ μεταδίδεται, ενώ η βαθμολογία φήμης και εμπιστοσύνης δεν δημοσιοποιούνται ποτέ.

2.2.2 ΥΠΟΛΟΓΙΣΜΟΣ ΚΑΙ ΑΝΑΝΕΩΣΗ ΒΑΘΜΟΛΟΓΙΩΝ

Μετά την περιγραφή του τρόπου λειτουργίας του συστήματος φήμης, είναι σημαντική η ανάλυση του τρόπου υπολογισμού και ανανέωσης των βαθμολογιών φήμης και εμπιστοσύνης καθώς και της first-hand πληροφορίας. Ο υπολογισμός βασίζεται στην στατιστική του Bayes, και ιδιαίτερα στις κατανομές πιθανοτήτων Beta που ορίζονται στο διάστημα (0,1), και χρησιμοποιούνται ευρέως σε αυτήν.

2.2.2.1 ΒΑΫΣΙΑΝΗ ΔΙΑΔΙΑΚΑΣΙΑ

Η βασική σκέψη είναι η εξής:
Ο κόμβος i θεωρεί ότι ο κόμβος j εμφανίζει μη ομαλή συμπεριφορά με μια πιθανότητα θ, και ότι το αποτέλεσμα αυτής εξάγεται ανεξάρτητα, από παρατήρηση σε

παρατήρηση. Πιο συγκεκριμένα, ο κόμβος i θεωρεί ότι κάθε κόμβος j παρουσιάζει διαφορετική πιθανότητα θ, αλλά και κάθε κόμβος i μπορεί να θεωρεί διαφορετικές πιθανότητες για κάθε κόμβο j. Οι παράμετροι θ, είναι άγνωστες, και υπολογίζονται βάση μιας «ηγούμενης» κατανομής πιθανοτήτων που ανανεώνεται μετά από κάθε παρατήρηση. Στο παρόν σύστημα φήμης, ως ηγούμενη κατανομή χρησιμοποιείται η Beta(α,β).

Στην διαδικασία αυτήν λοιπόν, η ηγούμενη κατανομή είναι η Beta(1,1), όπου αναπαριστά την έλλειψη πληροφορίας για το ποιο θ θα επέλθει. Στη συνέχεια, όταν πραγματοποιείται μια νέα παρατήρηση, υποθέτοντας ότι ως s ορίζονται οι μη ομαλές συμπεριφορές που παρατηρούνται και ως f οι σωστές συμπεριφορές που παρατηρούνται, η κατανομή ανανεώνεται ως εξής:

$\alpha := \alpha + s$
$\beta := \beta + f$

Μετά από έναν μεγάλο αριθμό παρατηρήσεων n, και βασιζόμενοι στις πιθανότητες, θα είναι: $\alpha \sim n\theta$ και $\beta \sim n(1-\theta)$, επομένως η Beta(α,β), μετατρέπεται σχεδόν σε μια Dirac του θ.
Η χρήση της συνάρτησης αυτής δίνει το πλεονέκτημα ότι απαιτούνται μόνο δύο παράμετροι, οι α και β, που ανανεώνονται συνέχεια βάσει των νέων παρατηρήσεων.

Αυτό είναι το βασικό μαθηματικό πλαίσιο πάνω στο οποίο βασίζονται οι μέθοδοι υπολογισμού της βαθμολογίας φήμης και εμπιστοσύνης καθώς και της first-hand πληροφορίας.

2.2.2.2 ΥΠΟΛΟΓΙΣΜΟΣ FIRST-HAND ΠΛΗΡΟΦΟΡΙΑΣ

Βάσει του μαθηματικού μοντέλου που περιγράφηκε, η εγγραφή $F_{i,j}$, είναι μια συνάρτηση Beta, που αναπαριστά την εξ ιδίων πληροφορία του κόμβου i για τον κόμβο j, και ορίζεται στην αρχή της επικοινωνίας ως Beta(1,1).
Η κλασική Βαϋσιανή μέθοδος που αναφέρθηκε, δίνει το ίδιο βάρος σε κάθε παρατήρηση ανεξάρτητα από τη στιγμή που πραγματοποιήθηκε. Για να επιτευχθεί όμως το «ξεθώριασμα» της φήμης με σκοπό την αντιμετώπιση λανθασμένων κατηγοριών ή επαίνων ώστε να καταφερθεί η επανακοινωνικοποίηση του κόμβου στο δίκτυο, πρέπει να δοθεί λιγότερο βάρος στις παρατηρήσεις που έγιναν στο παρελθόν από αυτές που έγιναν πιο πρόσφατα. Για τον λόγο αυτό ακολουθείται η παρακάτω διαδικασία:

Ορίζεται ως s=1 η παρατήρηση μιας μη ομαλής συμπεριφοράς και ως s=0 η παρατήρηση σωστής συμπεριφοράς, από έναν κόμβο i για έναν κόμβο j. Η ανανέωση των παραμέτρων της Beta για την first-hand πληροφορία ανανεώνεται σε:

$\alpha := u\alpha + s$
$\beta := u\beta + (1-s)$

Όπου u, το βάρος που λειτουργεί σαν παράγοντας που βοηθά στο «ξεθώριασμα» μνήμης. Για τον υπολογισμό του u ακολουθείται το εξής σκεπτικό:

Εάν υποθέσουμε ότι $s_1,\ldots..,s_n$, οι παρατηρήσεις, προκύπτει ότι:

$$a_n = s_n + us_{n-1} + ... + u^{n-1}s_1 + u^n$$

Υποθέτοντας ότι η θ, είναι σταθερή, για μεγάλο n, οι συναρτήσεις πιθανότητας είναι:

$$E(\alpha_n) \approx \frac{\theta}{1-u} \qquad E(\beta_n) \approx \frac{1-\theta}{1-u}$$

Υποθέτοντας ακόμα ότι $\frac{1}{1-u} = m$ είναι ακέραιος, που αναπαριστά το μέγεθος του αριθμού των παρατηρήσεων που είναι απαραίτητες για να θεωρηθεί σταθερή η συμπεριφορά ενός κόμβου, καταλήγουμε στο εξής u:

$$u = 1 - \frac{1}{m}$$

Για να γίνει εφικτό το ξεθώριασμα φήμης, ακόμα και όταν δεν υπάρχουν παρατηρήσεις, ή επικοινωνία μεταξύ των κόμβων, σε περιόδους αδράνειας, μειώνονται σταδιακά τα α και β. Μόλις η περίοδος αδράνειας τελειώσει, τα α και β τίθενται:

α := uα και β := uβ

2.2.2.3 ΥΠΟΛΟΓΙΣΜΟΣ ΒΑΘΜΟΛΟΓΙΑΣ ΦΗΜΗΣ

Όπως και η first-hand πληροφορία, έτσι και η βαθμολογία φήμης $R_{i,j}$, είναι μια συνάρτηση Beta(α΄, β΄), και ορίζεται στην αρχή της επικοινωνίας ως Beta(1,1). Η βαθμολογία φήμης ανανεώνεται βάσει δύο γεγονότων:

1. **Όταν ανανεώνεται η first-hand παρατήρηση.**
   Στην περίπτωση αυτή, η ανανέωση γίνεται ακριβώς με τον ίδιο τρόπο που πραγματοποιείται για την first-hand πληροφορία. Επιγραμματικά:

   α΄ := uα΄ + s και β΄ := uβ΄ + (1 – s)

   Σε περίπτωση περιόδου αδράνειας προκύπτει πάλι:

   α΄ := uα΄ και β΄ := uβ΄

2. **Όταν η βαθμολογία φήμης που δημοσιοποιεί ένας άλλος κόμβος ,γίνεται αποδεκτή και αντιγράφεται.**
   Στην περίπτωση αυτή, ακολουθείται η παρακάτω διαδικασία, που λαμβάνει υπόψη την εμπιστοσύνη και την συμβατότητα:
   Έστω ότι ο κόμβος i λαμβάνει την first-hand πληροφορία $F_{k,j}$, από τον κόμβο k για τον κόμβο j. Εάν το $T_{i,k}$, είναι τέτοιο ώστε ο i να θεωρεί τον k έμπιστο, ο κόμβος i ανανεώνει το $R_{i,j}$, παίρνοντας υπόψη την πληροφορία $F_{k,j}$, ως εξής:

   $$R_{i,j} := R_{i,j} + w\, F_{k,j}$$

Όπου w μια μικρή σταθερά.

Εάν το $T_{i,k}$, είναι τέτοιο ώστε ο i να μην θεωρεί τον k έμπιστο, ο i χρησιμοποιεί τα αποτελέσματα του *τεστ απόκλισης* ως εξής:
Υποτίθενται $F_{k,j} = (\alpha_F, \beta_F)$, $R_{i,j} = (\alpha,\beta)$ και d μία θετική σταθερά. Το τεστ απόκλισης πηγάζει από την εξίσωση:

$$|E(Beta(\alpha_F, \beta_F)) - E(Beta(\alpha, \beta))| >= d$$

Εάν το τεστ είναι θετικό, η first-hand πληροφορία $F_{k,j}$, θεωρείται ασυμβίβαστη και δεν χρησιμοποιείται, αλλιώς χρησιμοποιείται στην ανανέωση της βαθμολογίας φήμης, με τον τρόπο που αναφέρθηκε προηγουμένως.

2.2.2.4 ΥΠΟΛΟΓΙΣΜΟΣ ΒΑΘΜΟΛΟΓΙΑΣ ΕΜΠΙΣΤΟΣΥΝΗΣ

Με παρόμοιο τρόπο υπολογίζονται και οι βαθμολογίες εμπιστοσύνης. Θεωρείται από τον κόμβο i, ότι ο κόμβος j δίνει λανθασμένες αναφορές με πιθανότητα φ. Η βαθμολογία εμπιστοσύνης $T_{i,j}$, αναπαρίσταται ως μια συνάρτηση Beta(γ,δ), όπου αρχικοποιείται ως Beta(1,1). Η ανανέωση γίνεται όταν ο κόμβος λαμβάνει μια first-hand πληροφορία από τον κόμβο k για τον κόμβο j. Έτσι, αν υποτεθεί ότι s=1 εάν το τεστ απόκλισης πετύχει, και s=0 αλλιώς, η βαθμολογία εμπιστοσύνης ανανεώνεται ως εξής:

$$\gamma := v\gamma + s \qquad \text{και} \qquad \delta := v\delta + (1 - s)$$

Όπου v είναι ο παράγοντας που βοηθά στο ξεθώριασμα της εμπιστοσύνης. Για περιόδους αδράνειας, η ανανέωση είναι ανάλογη με αυτή για τις βαθμολογίες φήμης.
Το τεστ απόκλισης πραγματοποιείται πάντα, άσχετα με το αν ο κόμβος k θεωρείται έμπιστος από τον i ή όχι. Στην πρώτη περίπτωση όμως, ανανεώνεται μόνο το $T_{i,k}$, ενώ στην δεύτερη επιπρόσθετα αποφασίζεται κατά πόσο πρέπει να ανανεωθεί το $R_{i,j}$, ή όχι.

Βάσει όλων των παραπάνω, παρουσιάζεται στο σημείο αυτό η μέθοδος με την οποία κατατάσσονται οι κόμβοι όσον αφορά την συμπεριφορά τους αλλά και την αξιοπιστία τους. Συγκεκριμένα ο κόμβος i κατατάσσει την συμπεριφορά του κόμβου j ως εξής:

- ***Φυσιολογική*** εάν $E(Beta(\alpha', \beta')) < r$
- ***Μη ομαλή*** εάν $E(Beta(\alpha', \beta')) >= r$

Όπου r το κατώφλι που αναπαριστά την ανεκτικότητα στην μη επιθυμητή συμπεριφορά(π.χ. αν ο κόμβος i θεωρεί ότι ο κόμβος j παρουσιάζει μη ομαλή συμπεριφορά για όχι περισσότερο από τον μισό χρόνο, θέτει r = 0.5.

Αντίστοιχα για την αξιοπιστία του κόμβου j:

- ***Αξιόπιστος****(έμπιστος)* εάν $E(Beta(\gamma, \delta)) < t$
- ***Αναξιόπιστος*** εάν $E(Beta(\gamma, \delta)) >= t$

Όπου t το κατώφλι που αναπαριστά την ανεκτικότητα στις λανθασμένες αναφορές.

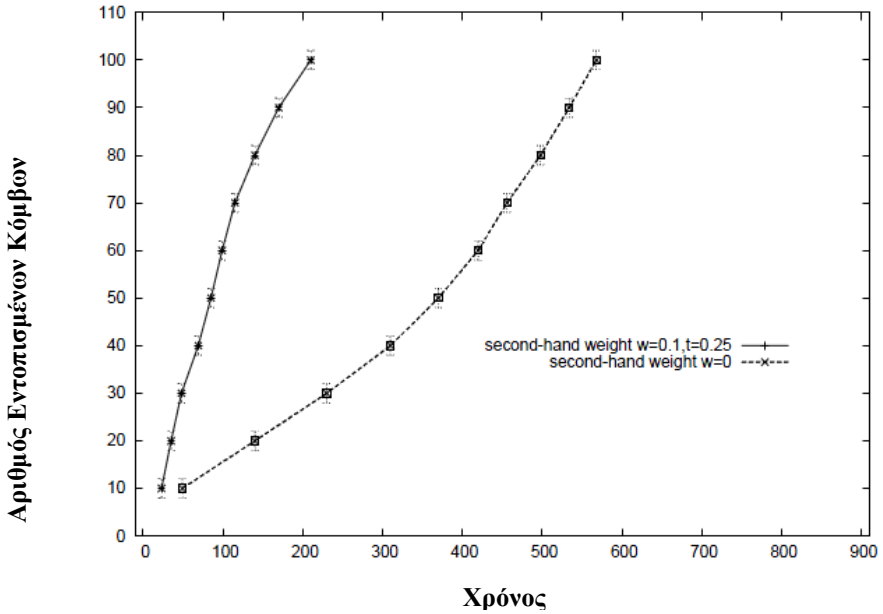
2.2.3 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ IMPROVED CONFIDANT

Σύμφωνα με τους κατασκευαστές του συστήματος φήμης που παρουσιάστηκε, το τελευταίο, εφαρμοζόμενο στο πρωτόκολλο υποστήριξης συνεργασίας CONFIDANT, μπορεί να προσφέρει αισθητές βελτιώσεις. Οι προσομοιώσεις έχουν πραγματοποιηθεί με χρήση του προσομοιωτή GloMoSim. Η απόδοση του IMPROVED CONFIDANT έχει εξεταστεί βάσει:

- Του χρόνου ανίχνευσης των μη ομαλά συμπεριφερόμενων κόμβων. Για να για γίνει σύγκριση μεταξύ της χρήσης και second-hand πληροφορίας με τη χρήση μόνο first-hand παρατηρήσεων, δόθηκε συντελεστής βαρύτητας w, 0.1 για τις second-hand πληροφορίες, και 0 όταν αυτές δεν υπολογίζονται. Πραγματοποιήθηκαν μετρήσεις σε προσομοίωση δικτύου 50 κόμβων.
- Της ευρωστίας απέναντι σε λάθος κατηγορίες ή επαίνους.
- Της επιβάρυνσης στο δίκτυο λόγω των μηνυμάτων ελέγχου, των υπολογισμών και της χωρητικότητας, η οποία προκύπτει λόγω των first-hand δημοσιοποιήσεων κάθε κόμβου με TTL = 1. Ο χρόνος μεταξύ διαδοχικών δημοσιοποιήσεων τέθηκε στις προσομοιώσεις, 10s.

Συγκεκριμένα:

- Λαμβάνοντας υπόψη την second-hand πληροφορία, μειώνεται αισθητά ο χρόνος ανίχνευσης των κόμβων με μη ομαλή συμπεριφορά, κάτι που φαίνεται και από το παρακάτω διάγραμμα που έχει εξαχθεί, και που στον κάθετο άξονα έχει ***το ποσοστό των κόμβων με μη ομαλή συμπεριφορά που έχουν εντοπιστεί,*** και στον οριζόντιο ***τον χρόνο.***



Διάγραμμα 2.2.1 (Πηγή [2])

- Το σύστημα εμπιστοσύνης μειώνει αισθητά τις λάθος κατηγορίες και τους λάθος επαίνους.
- Η επιβάρυνση στο δίκτυο, μπορεί να ελεγχθεί διαμορφώνοντας το διάστημα του χρόνου κατά το οποίο γίνονται οι δημοσιοποιήσεις της πληροφορίας, ενώ

η επιβάρυνση στην αποθηκευτική ικανότητα των κόμβων έγκειται μόνο στις τρεις βαθμολογίες που αποθηκεύουν οι κόμβοι.

- Με το τεστ απόκλισης αντιμετωπίζονται οι προσπάθειες των κακόβουλων κόμβων να επηρεάσουν τη φήμη κάποιου κόμβου, θετικά ή αρνητικά (π.χ. αλλάζοντας τις παραμέτρους α και β).
- Με το ξεθώριασμα φήμης ενισχύεται το άνωθεν αποτέλεσμα, καθώς και την προσπάθεια κακόβουλων κόμβων να δρουν για ένα διάστημα σωστά ώστε να αποκτήσουν φήμη, και στη συνέχεια να αποστέλλουν εσφαλμένες πληροφορίες.

Το πρωτόκολλο CONFIDANT ενισχυμένο με το σύστημα φήμης που παρουσιάστηκε, είναι αρκετά ισχυρό στην ανίχνευση μη ομαλά συμπεριφερόμενων κόμβων. Δεν βασίζεται στην τιμωρία των κόμβων αυτών, αλλά στον περιορισμό της επιρροής λανθασμένων πληροφοριών στη φήμη και την αξιοπιστία των κόμβων, ώστε να μην αποθαρρύνεται η αναφορά στοιχείων που μπορεί να αποδεικνύουν την μη ομαλή συμπεριφορά ενός κόμβου. Με το ξεθώριασμα μνήμης και την περιοδική επαναξιολόγηση των κόμβων, καθώς και με τη δυνατότητα που δίνεται στους κόμβους να διατηρούν τη δική τους γνώμη για τους υπολοίπους, επιτρέπεται η επαναφορά των λανθασμένα κατηγορημένων κόμβων στην επικοινωνία και η προοπτική να δείξουν σωστή συμπεριφορά.

2.3 SORI

Το πρωτόκολλο SORI [3], είναι ακόμα ένας μηχανισμός υποστήριξης συνεργασίας στα ad-hoc δίκτυα, βασισμένος στη φήμη. Έχει σχεδιαστεί για να ενθαρρύνει την προώθηση των πακέτων από τους ενδιάμεσους κόμβους και να τιμωρεί τους κόμβους που εμφανίζουν εγωιστική συμπεριφορά μέσα στο δίκτυο. Στο SORI, η φήμη των κόμβων διαμορφώνεται από αντικειμενικούς παράγοντες, ενώ η διάδοση της φήμης προστατεύεται από ένα μηχανισμό πιστοποίησης(one-way-hash-chain), ώστε να μην μπορεί να τροποποιηθεί από κακόβουλους κόμβους. Διαθέτει επίσης έναν μηχανισμό για την τιμωρία των εγωιστικών κόμβων. Δεδομένου ότι στο SORI η φήμη διαδίδεται μόνο στους γειτονικούς κόμβους, καθώς χρησιμοποιείται μόνο από αυτούς, η επιβάρυνση που επιφέρει στο δίκτυο είναι αρκετά μικρή.
Το SORI, έχει προσομοιωθεί σε ad-hoc δίκτυα που έχουν τα παρακάτω χαρακτηριστικά:

- Υποστηρίζουν broadcast μετάδοση, όπου κάθε πακέτο που αποστέλλεται από έναν κόμβο μπορεί να ληφθεί από όλους τους γειτονικούς.
- Όλοι οι κόμβοι επιθυμούν να επικοινωνήσουν στο δίκτυο
- Όλοι οι κόμβοι διατηρούν την ταυτότητα τους.
- Κανένας κόμβος δεν πρόκειται να ξοδέψει περισσότερους ενεργειακούς υπολογιστικούς πόρους για να προβεί σε μια κακόβουλη ενέργεια, από αυτούς που είναι απαραίτητοι για να προωθήσει απλά τα πακέτα.
- Όλοι οι κόμβοι μπορούν αν ακούσουν την μετάδοση των γειτόνων τους ακόμα κι αν τα μεταδιδόμενα πακέτα δεν προορίζονται για αυτούς.
- Οι κόμβοι δεν συνωμοτούν μεταξύ τους.

2.3.1 ΛΕΙΤΟΥΡΓΙΑ

Η λειτουργία του SORI βασίζεται σε τρεις βασικές διαδικασίες:

1. Την ανίχνευση της συμπεριφοράς των γειτονικών κόμβων(***Neighbor Monitoring***)
2. Την διάδοση της φήμης(***Reputation Propagation***)
3. Την τιμωρία των εγωιστικών κόμβων(***Punishment***)

Διαθέτει επίσης έναν μηχανισμό ασφαλείας για την αντιμετώπιση αδυναμιών του βασικού σχήματος:

- ***Security Enhancement***

2.3.1.1 ΑΝΙΧΝΕΥΣΗ

Στο σύστημα SORI κάθε κόμβος πραγματοποιεί ανίχνευση των γειτονικών κόμβων για να συλλέξει πληροφορίες σχετικά με την συμπεριφορά τους όσον αφορά την προώθηση πακέτων, «ακούγοντας» τη μετάδοσή τους. Έτσι, κάθε κινητός κόμβος N διατηρεί μια λίστα που περιέχει τους γειτονικούς κόμβους που έχει ανιχνεύσει, την $\mathbf{NNL_N}$ (neighbor node list). Για κάθε κόμβο της λίστας του, ο κόμβος N, διατηρεί τους εξής δύο αριθμούς:

- Τον $\mathbf{RF_N(X)}$ (Request-for-forwarding), που αναπαριστά τον συνολικό αριθμό των πακέτων που ο κόμβος N έχει μεταδώσει στον κόμβο X, με σκοπό αυτός αν τα προωθήσει.

- Τον **$HF_N(X)$** (Has-Forwarded), που αναπαριστά τον συνολικό αριθμό των πακέτων που έχουν προωθηθεί από τον X, και έχουν παρατηρηθεί από τον N. Ο αριθμός αυτός δεν μπορεί να συμπεριλάβει τα πακέτα που υφίστανται σύγκρουση, αλλά αυτό δεν επηρεάζει σε μεγάλο βαθμό την ανίχνευση, και περαιτέρω την τιμωρία των εγωιστικών κόμβων, σε δίκτυα με μέτριο φόρτο.

Οι δύο αυτοί αριθμοί ανανεώνονται με την εξής διαδικασία:
Όταν ο κόμβος N αποστέλλει ένα πακέτο στον κόμβο X με σκοπό ο δεύτερος να το προωθήσει, ο αριθμός $RF_N(X)$ αυξάνεται κατά ένα. Στη συνέχεια ο κόμβος N ακούει το ασύρματο κανάλι και ελέγχει αν ο κόμβος X προώθησε το πακέτο αυτό, όπως ήταν αναμενόμενο. Εάν ο κόμβος X, έχει προωθήσει το πακέτο μέσα σε ένα προκαθορισμένο χρονικό διάστημα, ο αριθμός $HF_N(X)$ αυξάνεται κατά ένα.
Διατηρώντας τους δύο αυτούς αριθμούς, ο κόμβος N, δημιουργεί μια εγγραφή αξιολόγησης, την **$LER_N(X)$(**local evaluation record) για τον γειτονικό κόμβο X. Η εγγραφή αυτή, απαρτίζεται από δύο καταχωρήσεις:

- Την **$G_N(X)$**, όπου $G_N(X) = \frac{RF_N(X)}{HF_N(X)}$
- Την **$C_N(X)$**(confidence), που αναπαριστά την σιγουριά του κόμβου N σχετικά με την άποψη του για την φήμη του κόμβου X. Για την καταχώρηση αυτή ισχύει: $C_N(X) = RF_N(X)$, καθώς όσο περισσότερα πακέτα έχουν αποσταλλεί στον X προς προώθηση, τόσο καλύτερη εκτίμηση μπορεί να έχει ο κόμβος N για την δραστηριότητα του X όσον αφορά την προώθηση πακέτων.

2.3.1.2 ΔΙΑΔΟΣΗ ΦΗΜΗΣ

Με την διαδικασία της ανίχνευσης, κάθε κόμβος μπορεί να δημιουργήσει μια εγγραφή για την φήμη κάθε κόμβου που βρίσκεται στη γειτονιά του. Η φήμη κάθε κόμβου, επηρεάζει άμεσα την υπηρεσία που μπορεί να λάβει από τους υπολοίπους. Η εξ ιδίων παρατήρηση όμως κάθε κόμβου, δεν είναι αρκετή για να καταφερθεί η αποτελεσματική τιμωρία των κόμβων που δρουν εγωιστικά. Για τον λόγο αυτό, χρησιμοποιείται η διαδικασία διάδοσης φήμης, ώστε να ανταλλάσσονται μεταξύ των κόμβων οι πληροφορίες για την φήμη των υπόλοιπων, με σκοπό οι εγωιστικοί κόμβοι να μην τιμωρούνται μόνο από τους κόμβους που πλήττονται από την μη ομαλή συμπεριφορά τους, αλλά από όλους τους γειτονικούς κόμβους των εγωιστικών. Η διαδικασία διάδοσης φήμης λειτουργεί ως εξής:

1. Κάθε κόμβος N, ανανεώνει περιοδικά την εγγραφή $LER_N(X)$ του για κάθε γειτονικό κόμβο X, βασιζόμενος στις αλλαγές των $RF_N(X)$ και $HF_N(X)$, και μεταδίδει την ανανεωμένη εγγραφή στους γείτονες του, στην περίπτωση που η καταχώρηση $G_N(X)$ έχει αλλάξει σημαντικά.
2. Ο κόμβος N χρησιμοποιεί την εγγραφή $LER_N(X)$ του καθώς και τις εγγραφές $LER_i(X)$(όπου i οι κόμβοι που βρίσκονται στην λίστα NNL_N του, για να δημιουργήσει μια συνολική εγγραφή αξιολόγησης για τον κόμβο X, την **$OER_N(X)$**(overall evaluation record). Για την εγγραφή αυτή λοιπόν ισχύει:

$$OER_N(X) = \frac{\sum_{i \in NNL_N \cup \{N\}, i \neq X} \lambda_N(i) \cdot C_i(X) \cdot G_i(X)}{\sum_{k \in NNL_N \cup \{N\}, k \neq X} \lambda_N(k) \cdot C_k(X)}$$

Όπου $\lambda_N(i)$, η αξιοπιστία που έχει λάβει ο κόμβος i από την άποψη του κόμβου N. Μπορεί να οριστεί $\lambda_N(i) = G_N(i)$, $\lambda_N(N) = 1$ καθώς και $\lambda_N(i) = 0$ αν $RF_N(i) = 0$, ώστε κάποιος κόμβος να μην λαμβάνει αξιοπιστία από τον N αν δεν του έχει ζητηθεί από τον N να προωθήσει πακέτα. Η αξιοπιστία κάθε κόμβου, συμμετέχει στον υπολογισμό της φήμης. Το γεγονός αυτό, δυσκολεύει τους κόμβους που θέλουν να χρησιμοποιήσουν πολλαπλές ταυτότητες, χρησιμοποιώντας την μια ταυτότητα για να μεταδώσουν ψεύτικες πληροφορίες ώστε να βελτιώσουν την φήμη τους κάτω από άλλη ταυτότητα. Με την χρήση της αξιοπιστίας, περιορίζεται η συνεισφορά που μπορεί να έχει η μια ταυτότητα του εγωιστικού κόμβου στην βελτίωση της φήμης της άλλης, αφού, όντας εγωιστικός κόμβος θα έχει τουλάχιστον σε μια ταυτότητα μειωμένη αξιοπιστία.

2.3.1.3 ΤΙΜΩΡΙΑ

Έχοντας στην κατοχή του την εγγραφή $OER_N(X)$, ο κόμβος N μπορεί να προχωρήσει στην διαδικασία τιμωρίας του κόμβου X, απορρίπτοντας πακέτα βασισμένος στις πιθανότητες. Πιο συγκεκριμένα η διαδικασία τιμωρίας έχει ως εξής:
Εάν το $OER_N(X)$, είναι χαμηλότερο από ένα προκαθορισμένο κατώφλι, ο κόμβος N απορρίπτει πακέτα που προέρχονται από τον X, με σκοπό να τον τιμωρήσει, πιθανοτικά. Η πιθανότητα με την οποία απορρίπτει πακέτα είναι p:

$$p = q - \delta \quad ,\text{αν } q < \delta \qquad \text{και} \qquad p = 0 \quad ,\text{αλλιώς}$$

Όπου $q = 1 - OER_N(X)$ και $0 < \delta < 1$. Το περιθώριο δ, έχει σκοπό την αποφυγή αντιποίνων μεταξύ δύο ομαλά συμπεριφερόμενων κόμβων, που αυξάνουν συνεχώς την πιθανότητα απόρριψης πακέτων λόγω κάποιων συμπτώσεων όπως π.χ. κάποια σύγκρουση πακέτων.

2.3.1.4 ΑΣΦΑΛΕΙΑ

Στα ad-hoc δίκτυα όπου εφαρμόζεται το SORI, οι εγωιστικοί κόμβοι, μπορεί να προσπαθήσουν να χρησιμοποιήσουν τεχνάσματα για να επωφεληθούν οι ίδιοι, χωρίς να εντοπιστούν από το δίκτυο. Πιο συγκεκριμένα ένας εγωιστικός κόμβος μπορεί:

1. Να υποδυθεί έναν κόμβο με καλή φήμη που βρίσκεται κοντά του, ώστε να αποστέλλει τα δικά του πακέτα.
2. Να υποδυθεί έναν κόμβο με καλή φήμη, ώστε να μεταδώσει ψεύτικες πληροφορίες παρατήρησης, ώστε να βελτιώσει την φήμη του που υπολογίζεται από τους άλλους κόμβους.

Για την αντιμετώπιση των προβλημάτων αυτών, υπάρχει ένας μηχανισμός πιστοποίησης βασισμένος σε μια one-way-hash αλυσίδα, χωρίς να χρειάζεται η παρουσία μιας κεντρικής δομής πιστοποίησης. Ο μηχανισμός αυτός λειτουργεί ως εξής:
Ο κόμβος N παίρνει μια ταυτότητα $\mathbf{ID_N}$, επιλέγοντας έναν τυχαίο αριθμό r_N, και εφαρμόζοντας αναδρομικά μια ψευδοτυχαία συνάρτηση h στο r_N, k φορές, ώστε $ID_N = H_k(r_N)$ που υπολογίζεται αναδρομικά όπως φαίνεται παρακάτω:

$$H_i(r_N) = \begin{cases} h(H_{i-1}(r_N)) \quad \alpha\nu \quad i \in \{1,2,.....,k\} \\ h(r_N) \quad \alpha\nu \quad i = 0 \end{cases}$$

Όταν ένας κόμβος εισέρχεται στο ad-hoc δίκτυο, μεταδίδει ευρέως την ταυτότητα του, και όλοι οι γειτονικοί του κόμβοι την λαμβάνουν και την τοποθετούν στην NNL λίστα τους, ώστε να μπορούν να πιστοποιήσουν τα μηνύματα που προωθούνται από τον κόμβο αυτό στο εξής. Η διαδικασία αυτή της πιστοποίησης περιγράφεται παρακάτω:
Ο κόμβος N χωρίζει τον χρόνο σε ίσα διαστήματα και αναθέτει στο i-οστό διάστημα το κλειδί $\mathbf{K_i}$, στην one-way-hash αλυσίδα, όπου $K_i = H_{k-i}(r_N)$. Τα μηνύματα που αποστέλλονται σε ένα από τα διαστήματα, ακολουθούνται από έναν κωδικό πιστοποίησης μηνύματος(MAC), τον **MAC(K,M)**, ο οποίος υπολογίζεται με το αντίστοιχο κλειδί K και το μήνυμα M σαν είσοδο. Για παράδειγμα, το περιεχόμενο του πακέτου P_i, που αποστέλλεται στο i-οστό διάστημα είναι:

$$\{M_i \,||\, MAC(K_i', M_i) \,||\, K_{i-d}\}$$

Όπου M_i, το μήνυμα που θα σταλεί στο i-οστό διάστημα, και K_i' το κλειδί που προκύπτει από την εξίσωση $K_i' = f(K_i)$, όπου f μια δεύτερη ψευδοτυχαία συνάρτηση. Το d αναπαριστά την καθυστέρηση γνωστοποίησης του κλειδιού.

Όταν οι παραλήπτες λαμβάνουν ένα πακέτο, ελέγχουν αν το κλειδί που χρησιμοποιήθηκε για την εξαγωγή του MAC, έχει ήδη γνωστοποιηθεί. Εάν το κλειδί δεν έχει γνωστοποιηθεί ακόμη, αποθηκεύουν το μήνυμα και ελέγχουν την αυθεντικότητά του όταν το κλειδί K_i έχει γνωστοποιηθεί. Σε αντίθετη περίπτωση, οι παραλήπτες απορρίπτουν το πακέτο καθώς αν το κλειδί έχει γνωστοποιηθεί πριν την παραλαβή του, υπάρχει περίπτωση να έχει παραβιαστεί ο MAC. Πακέτα με μη έγκυρο MAC, απορρίπτονται επίσης.

Ο μηχανισμός ασφαλείας που περιγράφηκε, δυσκολεύουν τους εγωιστικούς κόμβους με κακή φήμη να προσποιηθούν κόμβους με καλή φήμη, με σκοπό να στείλουν τα πακέτα τους ή να μεταδώσουν ψεύτικες πληροφορίες για τις παρατηρήσεις τους ώστε να βελτιώσουν τη φήμη τους. Βασικό ρόλο σε αυτό, παίζει ο κωδικός MAC, που παραβιάζεται πολύ δύσκολα, απουσία κλειδιού. Ο μηχανισμός ασφαλείας, καταλήγοντας, αποτελεί μια φθηνή υπολογιστικά λύση, που εξαλείφει την ανάγκη για κάποια κεντρική δομή πιστοποίησης.

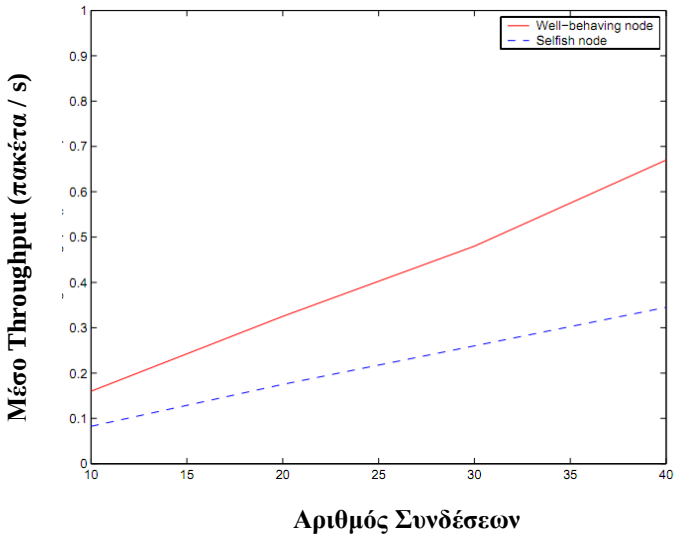
2.3.2 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ SORI

Οι δημιουργοί του SORI πραγματοποίησαν προσομοιώσεις για να ελέγξουν την αποτελεσματικότητα του, μέσω του προσομοιωτή δικτύων ns-2. Το περιβάλλον της προσομοίωσης διαμορφώθηκε για τις μετρήσεις ως εξής:

- Περιοχή 670m x 670m
- Δίκτυο 50 κόμβων
- Πρωτόκολλο MAC 802.11
- Εμβέλεια μετάδοσης 250m
- Ρυθμός δεδομένων 2Mbps

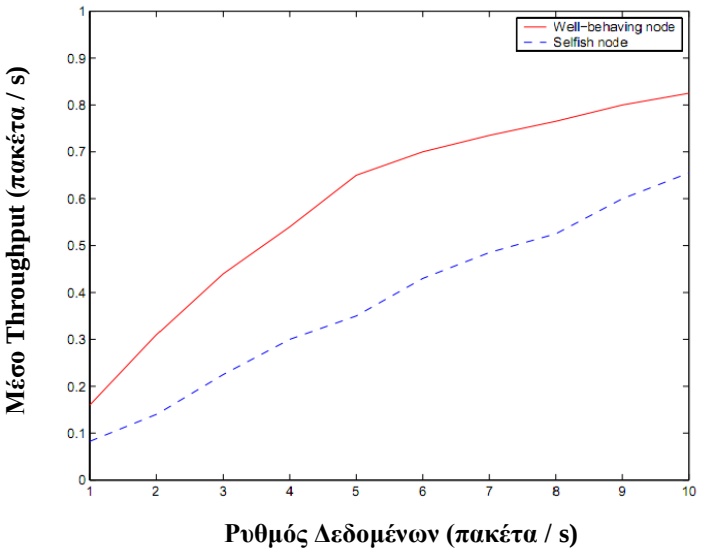
- Ύψος κεραιών εκπομπής-λήψης 1.5m
- Τυχαία κίνηση
- Ταχύτητα μεταξύ 0 και 20m/s
- Διάρκεια παύσης κίνησης 600s
- 5 τυχαία επιλεγμένοι εγωιστικοί κόμβοι
- Διάρκεια προσομοίωσης 1000s
- Συνολικός αριθμός συνδέσεων 10
- Τυχαία επιλεγμένος αριθμός ζευγών σύνδεσης πηγής-προορισμού
- Εφαρμογή CBR

Εξετάζοντας την λειτουργία του SORI, κάτω από διαφορετικά σενάρια επικοινωνίας όσον αφορά τον αριθμό των συμμετεχόντων κόμβων και εγωιστικών κόμβων, την πιθανότητα απόρριψης πακέτων, τον ρυθμό μετάδοσης δεδομένων και την ταχύτητα κίνησης των κόμβων και τον αριθμό των συνδέσεων, οι δημιουργοί του SORI, έχουν βγάλει τα εξής συμπεράσματα και τα αντίστοιχα διαγράμματα για την αποδοτικότητα του δικτύου στο οποίο έχει εφαρμοστεί το SORI, και την τιμωρία των εγωιστικών κόμβων:



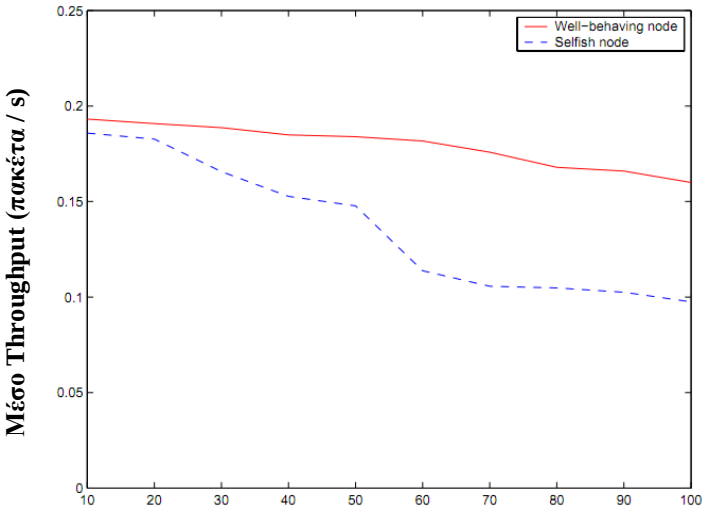
Διάγραμμα 2.3.1 (Πηγή [3])

Από το παραπάνω διάγραμμα που στον κάθετο άξονα του έχει το ***μέσο throughput σε πακέτα/sec,*** και στον οριζόντιο άξονα ***τον αριθμό των συνδέσεων,*** συμπεραίνεται ότι οι κόμβοι με ομαλή συμπεριφορά έχουν εμφανώς μεγαλύτερο throughput, περίπου 50%, σε σχέση με τους εγωιστικούς κόμβους καθώς αυτοί ανιχνεύονται και τιμωρούνται.



Διάγραμμα 2.3.2 (Πηγή [3])

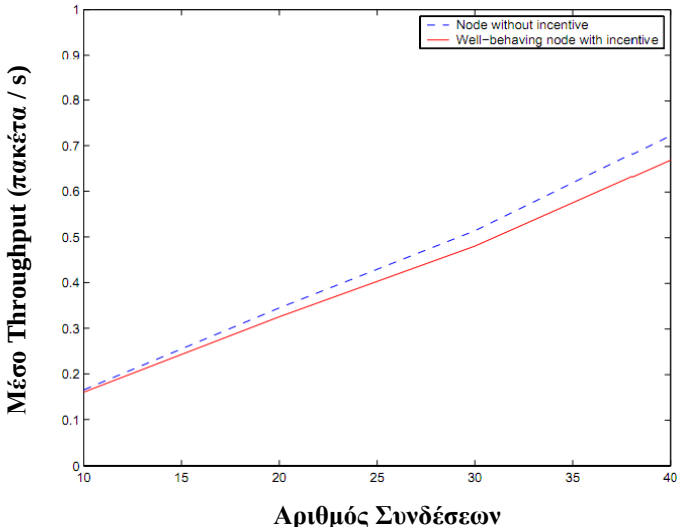
Από το παραπάνω διάγραμμα που στον κάθετο άξονα του έχει το ***μέσο throughput σε πακέτα/sec,*** και στον οριζόντιο άξονα ***τον ρυθμό δεδομένων σε πακέτα/sec,*** γίνεται σύγκριση μεταξύ ομαλά συμπεριφερόμενων και εγωιστικών κόμβων, και παρατηρείται ότι οι κόμβοι με ομαλή συμπεριφορά έχουν εμφανώς μεγαλύτερο throughput, σε σχέση με τους εγωιστικούς κόμβους. Η διαφορά όμως μεταξύ του throughput των εγωιστικών και των ομαλά συμπεριφερόμενων κόμβων, μειώνεται όσο αυξάνεται ο ρυθμός δεδομένων, καθώς ταυτόχρονα αυξάνονται και οι συγκρούσεις πακέτων με αποτέλεσμα να αυξάνεται η πιθανότητα λανθασμένου υπολογισμού της φήμης των κόμβων.



Διάγραμμα 2.3.3 (Πηγή [3])

Από το παραπάνω διάγραμμα που στον κάθετο άξονα του έχει το ***μέσο throughput σε πακέτα/sec,*** και στον οριζόντιο άξονα ***την πιθανότητα απόρριψης πακέτων από τους εγωιστικούς κόμβους επί τοις εκατό***, γίνεται σύγκριση μεταξύ ομαλά

συμπεριφερόμενων και εγωιστικών κόμβων, και συμπεραίνεται ότι οι κόμβοι με ομαλή συμπεριφορά έχουν εμφανώς μεγαλύτερο throughput, σε σχέση με τους εγωιστικούς κόμβους, με την διαφορά μεταξύ των δύο αυτών να αυξάνεται όσο αυξάνεται η πιθανότητα απόρριψης πακέτων από τους κόμβους. Αυτό, συμβαίνει λόγω της δυνατότητας του SORI, να αναγνωρίζει τους εγωιστικούς κόμβους και να επιβάλλει τιμωρία στην συμπεριφορά τους. Όσο αυξάνεται η πιθανότητα απόρριψης πακέτων βέβαια, μειώνεται και το throughput των σωστά συμπεριφερόμενων κόμβων, αφού ενισχύεται η απώλεια πακέτων.



Διάγραμμα 2.3.4 (Πηγή [3])

Τέλος, από το τελευταίο εξαχθέν διάγραμμα που στον κάθετο άξονα του έχει το ***μέσο throughput σε πακέτα/sec,*** και στον οριζόντιο άξονα ***τον αριθμό των συνδέσεων,*** γίνεται σύγκριση μεταξύ κόμβων σε δίκτυα που χρησιμοποιούν – ή όχι, το SORI, και παρατηρείται ότι το throughput ενός κόμβου σε ένα ad-hoc δίκτυο που δεν χρησιμοποιεί το SORI, είναι ελαφρώς μεγαλύτερο από το αντίστοιχο, ενός ομαλά συμπεριφερόμενου κόμβου σε δίκτυο που εφαρμόζεται το SORI, καθώς το πρωτόκολλο εισάγει μια επιβάρυνση λόγω της μετάδοσης της φήμης αλλά και του λάθους υπολογισμού φήμης λόγω συγκρούσεων, που μπορεί να οδηγήσει σε λανθασμένη τιμωρία κόμβων. Παρόλα αυτά, η επιβάρυνση είναι πολύ μικρή σε σχέση με τις δυνατότητες ανίχνευσης και τιμωρίας εγωιστικών κόμβων που προσφέρει το SORI. Φυσικά, όσο αυξάνονται οι συγκρούσεις, με την αύξηση των συνδέσεων, θα αυξάνεται και η επιβάρυνση του δικτύου λόγω του λάθος υπολογισμού φήμης που αναφέρθηκε.

Συμπερασματικά, το SORI, αποτελεί έναν μηχανισμό υποστήριξης συνεργασίας σε ad-hoc δίκτυα, που βασίζεται στην αποτελεσματική αναγνώριση και τιμωρία των εγωιστικών κόμβων. Κρίσιμα σημεία του πρωτοκόλλου, είναι ο υπολογισμός της φήμης βασιζόμενο σε αντικειμενικούς παράγοντες, η ασφαλής μετάδοση της φήμης, και η διάδοση της φήμης μόνο στους γειτονικούς κόμβους ώστε να μην αυξάνεται η επιβάρυνση στο δίκτυο.

2.4 CORE

Το CORE [4] αποτελεί άλλο ένα πρωτόκολλο υποστήριξης συνεργασίας των κόμβων στα ad-ho δίκτυα, βασισμένο στην φήμη. Στοχεύει όχι μόνο στην σωστή εκτέλεση των κρίσιμων λειτουργιών του δικτύου από τους κόμβους, αλλά και στην δίκαιη χρήση τους από τους κόμβους. Βασικό στοιχείο του CORE, είναι ο διαχωρισμός των εγωιστικών κόμβων από τους κακόβουλους, καθώς οι εγωιστικοί κόμβοι δεν έχουν ως σκοπό να βλάψουν το δίκτυο, αν και δεν συνεργάζονται στη σωστή λειτουργία του δικτύου για λόγους εξοικονόμησης ενέργειας. Από την άλλη μεριά, οι κακόβουλοι κόμβοι έχουν ως κύριο στόχο να βλάψουν το δίκτυο χωρίς να έχουν σαν προτεραιότητα την εξοικονόμηση μπαταρίας. Το πρωτόκολλο, χρησιμοποιεί έναν μηχανισμό αξιολόγησης της φήμης των κόμβων, ώστε οι εγωιστικοί κόμβοι να μην αποκλείονται τελείως από το δίκτυο, λόγω κάποιας σποραδικής μη ομαλής συμπεριφοράς. Το CORE, είναι βασισμένο στην δημιουργία φήμης στους κόμβους, είτε από την εξ ιδίων παρατήρηση, είτε από πληροφορίες που λαμβάνονται από τους άλλους κόμβους. Καταφέρνει επίσης την αποτροπή της άρνησης παροχής υπηρεσιών από κάποιους κόμβους, που είναι βασισμένη στην κακόβουλη μετάδοση αρνητικών βαθμολογιών φήμης για ομαλά συμπεριφερόμενους κόμβους, από κακόβουλους κόμβους. Η φήμη στο CORE, έχει σημασία στο κατά πόσο οι κόμβοι έχουν πρόσβαση στους πόρους του δικτύου. Κόμβοι με καλή φήμη, που συνεισφέρουν στην λειτουργία του δικτύου έχουν πρόσβαση στους πόρους, ενώ κόμβοι που δεν συνεισφέρουν, αποκλείονται σταδιακά από την κοινότητα των κόμβων.

2.4.1 ΦΗΜΗ

Η φήμη στο CORE, διαμορφώνεται και ανανεώνεται, με τον συνδυασμό των εξ ιδίων άμεσων παρατηρήσεων του κόμβου, και των πληροφοριών που μεταδίδουν οι υπόλοιποι κόμβοι του δικτύου. Η συνολική άποψη που δημιουργείται δηλαδή για έναν κόμβο, διαμορφώνεται από τον συνδυασμό διαφορετικών τύπων αξιολόγησης μέσα στο δίκτυο. Το CORE, χρησιμοποιεί τρία είδη φήμης:

- Την ***υποκειμενική φήμη****(subjective reputation)*
- Την ***έμμεση φήμη****(indirect reputation)*
- Την ***λειτουργική φήμη****(functional reputation)*

2.4.1.1 ΥΠΟΚΕΙΜΕΝΙΚΗ ΦΗΜΗ

Η υποκειμενική φήμη, είναι η φήμη που υπολογίζεται από την εξ ιδίων άμεση παρατήρηση ενός κόμβου. Η υποκειμενική φήμη ενός κόμβου s_i, στον χρόνο t, υπολογίζεται με την απόδοση βαρύτητας στους παράγοντες βαθμολόγησης της παρατήρησης. Για τον υπολογισμό της υποκειμενικής φήμης, δίδεται περισσότερο βάρος στις παρελθοντικές παρατηρήσεις, ώστε η σποραδική μη ομαλή συμπεριφορά που μπορεί να υπάρξει σε πρόσφατες παρατηρήσεις να έχει την μικρότερη δυνατή επίδραση στη φήμη. Επιτυγχάνεται έτσι, η αποφυγή λανθασμένων ανιχνεύσεων λόγω προβληματικών ζεύξεων και η λήψη υπόψη της πιθανότητας ύπαρξης κάποιας εντοπισμένης μη ομαλής συμπεριφοράς από μειονεκτικούς κόμβους. Η υποκειμενική φήμη των κόμβων υπολογίζεται από την ακόλουθη εξίσωση:

$$r_{s_i}^{t}(s_j \mid f) = \sum \rho(t, t_k) \cdot \sigma_k$$

Όπου:

- $r_{s_i}^t(s_j \mid f)$ η υποκειμενική φήμη που υπολογίζεται στον χρόνο t, από τον κόμβο s_i για τον κόμβο s_j, όσον αφορά τη λειτουργία f. Παίρνει τιμές από -1 έως 1.
- $\rho(t, t_k)$ μια συνάρτηση εξαρτώμενη από τον χρόνο, που δίνει μεγαλύτερη σημασία στις παρελθοντικές τιμές του σ_k.
- σ_k ο παράγοντας βαθμολόγησης που δίδεται στην k-οστή παρατήρηση, που παίρνει τιμές από -1(για αρνητική γνώμη) όπου το αποτέλεσμα της παρατήρησης δεν συμπίπτει με το αναμενόμενο, έως 1(για θετική γνώμη) όπου το αποτέλεσμα της παρατήρησης συμπίπτει με το αναμενόμενο. Στην περίπτωση που ο αριθμός ή η ποιότητα των παρατηρήσεων δεν είναι αρκετά για την εξαγωγή γνώμης για έναν κόμβο, ο παράγοντας παίρνει την τιμή 0(για ουδέτερη γνώμη).
- s_j οι γειτονικοί κόμβοι του s_i, που βρίσκονται δηλαδή στην εμβέλεια ασύρματης διάδοσης του.

2.4.1.2 ΕΜΜΕΣΗ ΦΗΜΗ

Σε αντίθεση με την υποκειμενική φήμη, που υπολογίζεται αποκλειστικά βασιζόμενη στην άμεση αλληλεπίδραση μεταξύ ενός κόμβου και των γειτονικών του κόμβων, η έμμεση φήμη δίνει τη δυνατότητα συνυπολογισμού στην τελική φήμη, πληροφοριών που δίδονται από τους υπόλοιπους κόμβους του δικτύου. Η έμμεση φήμη ενός κόμβου s_j, που έχει συλλεχθεί από έναν κόμβο s_i, στον χρόνο t για την λειτουργία f, ορίζεται ως $ir_{s_i}^t(s_j \mid f)$. Η πληροφορία που συλλέγεται μέσω της έμμεσης φήμης, μπορεί να πάρει μόνο θετικές τιμές. Έτσι επιτυγχάνεται η αποτροπή της άρνησης παροχής υπηρεσιών από κάποιους κόμβους, που είναι βασισμένη στην κακόβουλη μετάδοση αρνητικών βαθμολογιών φήμης για ομαλά συμπεριφερόμενους κόμβους, από κακόβουλους κόμβους.

2.4.1.3 ΛΕΙΤΟΥΡΓΙΚΗ ΦΗΜΗ

Η λειτουργική φήμη στο CORE, αναπαριστά την υποκειμενική και έμμεση φήμη που υπολογίζεται όσον αφορά διαφορετικές λειτουργίες f. Με αυτόν τον τύπο φήμης, δίνεται η δυνατότητα υπολογισμού μιας συνολικής φήμης ενός κόμβου, που λαμβάνει υπόψη διαφορετικές παρατηρήσεις και κριτήρια. Το παρακάτω παράδειγμα βοηθάει στην κατανόηση της λειτουργίας της λειτουργικής φήμης:

- Ένας κόμβος s_i, μπορεί να υπολογίσει την υποκειμενική φήμη $r_{s_i}^t(s_j \mid f(προώθηση\ \ πακέτων))$ ενός κόμβου s_j, όσον αφορά τη λειτουργία προώθησης πακέτων και την υποκειμενική φήμη $r_{s_i}^t(s_j \mid f(δρομολόγηση))$, όσον αφορά τη λειτουργία δρομολόγησης, και να τις συνδυάσει δίνοντας τους διαφορετική βαρύτητα ώστε να διαμορφώσει μια συνολική τιμή φήμης για τον κόμβο s_j.

2.4.1.4 ΣΥΔΥΑΣΜΟΣ ΠΛΗΡΟΦΟΡΙΩΝ ΦΗΜΗΣ – ΕΠΙΚΥΡΩΣΗ ΦΗΜΗΣ

Οι πληροφορίες φήμης συνδυάζονται βάσει της παρακάτω εξίσωσης:

$$r_{s_i}^t(s_j) = \sum w_k \cdot \{r_{s_i}^t(s_j \mid f_k) + ir_{s_i}^t(s_j \mid f_k)\}$$

Όπου $r_{s_i}^t(s_j)$ η συνολική φήμη που υπολογίζεται για κάθε κόμβο. Η βαρύτητα w_k, τίθεται με τέτοιον τρόπο ώστε να δίνεται έμφαση στην λειτουργία της προώθησης πακέτων, καθώς αυτή παίζει τον μεγαλύτεροι ρόλο στην απόδοση του δικτύου.

Για την επικύρωση της φήμης, το CORE διαθέτει ένα μηχανισμό ο οποίος συγκρίνει τα αποτελέσματα των παρατηρήσεων με τα αναμενόμενα αποτελέσματα. Εάν αυτά συμπίπτουν ο παράγοντας σ_k, για την k-οστή παρατήρηση θα είναι θετικός, ενώ αν δεν συμπίπτουν θα είναι αρνητικός.

2.4.2 ΛΕΙΤΟΥΡΓΙΑ

Το CORE αποτελείται από τα εξής συστατικά στοιχεία, που συμμετέχουν στον συνεργατικό μηχανισμό φήμης:

- Την ***οντότητα δικτύου****(network entity)*
- Τον ***πίνακα φήμης****(reputation table)*
- Τον ***μηχανισμό-φύλακα****(Watchdog mechanism)*

2.4.2.1 ΟΝΤΟΤΗΤΑ ΔΙΚΤΥΟΥ

Η οντότητα δικτύου αποτελεί ουσιαστικά, έναν κινητό κόμβο του ad-hoc δικτύου. Κάθε τέτοια οντότητα s_i, κατέχει ένα σετ πινάκων φήμης(RT) και έναν μηχανισμό φύλακα(WD). Τα δύο αυτά στοιχεία επιτρέπουν στην οντότητα να παρατηρήσει και να κατατάξει κάθε άλλη οντότητα που συμμετέχει στην διαδικασία ερώτησης-απάντησης. Η κατάταξη των οντοτήτων βάσει της συμπεριφοράς τους, αναδεικνύει τον τρόπο με τον οποίο συνδέεται η συμπεριφορά των κόμβων όσον αφορά την συνεργασία τους με τους υπόλοιπους, με την με την πρόσβαση στους πόρους του δικτύου που είναι διαθέσιμες στους υπόλοιπους κόμβους.
Μια οντότητα χαρακτηρίζεται ως **αιτούσα** όταν αιτείται την εκτέλεση μιας λειτουργίας f. Αντίστοιχα μια οντότητα χαρακτηρίζεται ως **πάροχος** όταν εκτελεί ορθά την λειτουργία f.

2.4.2.2 ΠΙΝΑΚΑΣ ΦΗΜΗΣ

Ο πίνακας φήμης(RT), όπως αναφέρθηκε, αποτελεί μια δομή δεδομένων αποθηκευμένη σε κάθε οντότητα. Σε κάθε γραμμή του πίνακα περιέχονται τα δεδομένα φήμης που αφορούν έναν κόμβο. Κάθε γραμμή αποτελείται από τέσσερις εγγραφές:

- Το μοναδικό αναγνωριστικό(ταυτότητα) της οντότητας.
- Μια συλλογή πρόσφατων υποκειμενικών παρατηρήσεων που αφορούν την συμπεριφορά της συγκεκριμένης οντότητας.
- Μια λίστα πρόσφατων τιμών έμμεσης φήμης που έχουν δοθεί από άλλες οντότητες.
- Την τιμή της φήμης που έχει υπολογιστεί, για μια προκαθορισμένη λειτουργία.

Κάθε οντότητα δικτύου, κατέχει έναν πίνακα φήμης για κάθε λειτουργία που παρακολουθείται.

2.4.2.3 ΜΗΧΑΝΙΣΜΟΣ-ΦΥΛΑΚΑΣ

Ο μηχανισμός-φύλακας(WD) πραγματοποιεί την επικύρωση φήμης, που αναφέρθηκε παραπάνω, και χρησιμοποιείται στην ανίχνευση των μη ομαλά συμπεριφερόμενων κόμβων. Κάθε φορά που μια οντότητα δικτύου($s_{i,m}$ οντότητα που παρακολουθεί) χρειάζεται να παρακολουθήσει την σωστή εκτέλεση μιας λειτουργίας υλοποιούμενης από κάποια γειτονική οντότητα($s_{j,o}$ οντότητα που παρακολουθείται), πυροδοτείται ο WD συγκεκριμένα για την λειτουργία αυτήν(f). Ο WD αποθηκεύει το αναμενόμενο αποτέλεσμα $e_r(f)$ σε μια προσωρινή μνήμη στην $s_{i,m}$, και επαληθεύει αν το αποτέλεσμα της παρατήρησης $o_r(f)$ ταιριάζει με το πρώτο. Εάν η παρακολουθούμενη λειτουργία εκτελείται ομαλά, ο WD διαγράφει από την προσωρινή μνήμη την εγγραφή που αφορά υο ζευγάρι $s_{j,o}$ - $e_r(f)$, και μπαίνει σε κατάσταση χαλαρότητας, περιμένοντας την επόμενη λειτουργία προς παρατήρηση. Εάν η λειτουργία f όμως, δεν εκτελείται σωστά, ή αν το ζευγάρι $s_{j,o}$ - $e_r(f)$, παραμένει στην προσωρινή μνήμη για περισσότερο από ένα συγκεκριμένο χρονικό διάστημα, τίθεται στην εγγραφή που αφορά την $s_{j,o}$ στον πίνακα φήμης RT, μια αρνητική τιμή στον παράγοντα παρατήρησης σ_k, και υπολογίζεται μια νέα τιμή φήμης για την οντότητα αυτή.

2.4.3 ΠΕΡΙΓΡΑΦΗ ΤΟΥ CORE

Για την καλύτερη κατανόηση της λειτουργίας του CORE, περιγράφονται μερικά σενάρια επικοινωνίας, μεταξύ μιας αιτούσας οντότητας και μιας οντότητας παρόχου σε ένα ad-hoc δίκτυο που εφαρμόζεται το CORE, καθώς και ο τρόπος με τον οποίο ανανεώνονται οι πίνακες RT και ενισχύται η συνεργασία των κόμβων. Γενικότερα, το CORE λειτουργεί με την λογική, ότι αν μια οντότητα πάροχος αρνηθεί να συνεργαστεί, μειώνεται η φήμη της, πράγμα που σταδιακά μπορεί να οδηγήσει στον αποκλεισμό της από το δίκτυο. Ακολουθούν τα σενάρια:

1. **Λειτουργία του CORE όταν δεν ανιχνεύεται μη ομαλή συμπεριφορά**

   Αρχικά η αιτούσα οντότητα ζητά την εκτέλεση μιας λειτουργίας f από τον πάροχο. Στη συνέχεια ενεργοποιεί τον WD που σχετίζεται με τον πάροχο για την λειτουργία αυτή, και περιμένει τα αποτελέσματα του WD μέσα σε ένα προκαθορισμένο χρονικό διάστημα. Εάν και οι δύο οντότητες συμπεριφέρονται ομαλά, το αποτέλεσμα του WD επιβεβαιώνει ότι η λειτουργία εκτελέστηκε σωστά, και η αιτούσα οντότητα απενεργοποιεί τον WD. Το μήνυμα που αναπαριστά την επιβεβαίωση αυτή, περιέχει μια λίστα όλων των οντοτήτων που συμμετείχαν σωστά στην λειτουργία του πρωτοκόλλου. Τέλος, η αιτούσα οντότητα χρησιμοποιεί την έμμεση αυτή πληροφορία, για να ανανεώσει τον πίνακα RT της, και μπαίνει σε κατάσταση χαλαρότητας.

2. **Λειτουργία του CORE όταν ανιχνεύεται μη ομαλή συμπεριφορά**

   Αρχικά η αιτούσα οντότητα ζητά την εκτέλεση μιας λειτουργίας f από τον πάροχο. Στη συνέχεια ενεργοποιεί τον WD που σχετίζεται με τον πάροχο για την λειτουργία αυτή, και περιμένει τα αποτελέσματα του WD μέσα σε ένα

προκαθορισμένο χρονικό διάστημα. Εάν η οντότητα πάροχος δεν συνεργαστεί, το αποτέλεσμα του WD θα είναι αρνητικό. Τότε, η αιτούσα οντότητα ανανεώνει την εγγραφή που αφορά την μη ομαλά συμπεριφερόμενη οντότητα στον πίνακα RT της, με έναν αρνητικό παράγοντα και μπαίνει σε κατάσταση χαλαρότητας.

3. Λειτουργία του CORE όταν αιτείται μια μη ομαλά συμπεριφερόμενη οντότητα

Η οντότητα που λαμβάνει την αίτηση για την εκτέλεση μιας λειτουργίας f, ελέγχει την τιμή της φήμης της αιτούσας οντότητας, στον πίνακα RT της. Εάν η φήμη έχει αρνητική τιμή, η οντότητα δεν εκτελεί την αιτούμενη λειτουργία. Στην συνέχεια επιλέγει αν θα αναφέρει ή όχι την άρνηση της παροχής υπηρεσίας.

Ο μηχανισμός με τον οποίο ανανεώνονται οι πίνακες RT, έχει ως εξής:
Οι πίνακες RT ανανεώνονται σε δύο περιπτώσεις:

1. Κατά τη φάση της αίτησης για εκτέλεση κάποιας λειτουργίας. Στην περίπτωση αυτή ανανεώνεται μόνο η τιμή της υποκειμενικής φήμης. Εάν το αποτέλεσμα του WD δείχνει ότι η οντότητα δεν συνεργάστηκε, ένας αρνητικός παράγοντας βαθμολογίας δίδεται στην παρατήρηση και σταδιακά μειώνεται η φήμη του κόμβου που παρουσιάζει μη ομαλή λειτουργία. Εάν δεν ανιχνευθεί μη ομαλή συμπεριφορά, οι πίνακες RT δεν ανανεώνονται.
2. Κατά τη φάση απάντησης που αφορά την εκτέλεση της λειτουργίας f. Στην περίπτωση αυτή ανανεώνεται μόνο η έμμεση φήμη. Υποθέτοντας ότι το μήνυμα απάντησης περιέχει μια λίστα με όλες τις οντότητες που συμπεριφέρθηκαν σωστά, στην περίπτωση αυτή, η έμμεση φήμη είναι θετική και σταδιακά η φήμη που αφορά στις οντότητες που συνεργάζονται στη διαδικασία, θα αυξάνεται.

Οι παράγοντες βαθμολογίας που ανταλλάσσονται και διαδίδονται μεταξύ των κόμβων είναι μόνο θετικές. Έτσι αποφεύγεται η άρνηση υπηρεσιών, λόγω επιτηδευμένης μετάδοσης λανθασμένων πληροφοριών από κάποια μη ομαλά συμπεριφερόμενη οντότητα.
Οι τιμές φήμης για κάθε εγγραφή των RT, δεν είναι σταθερές. Υπάρχει η τάση οι θετικές τιμές φήμης να μειώνονται με το πέρασμα του χρόνου ώστε οι οντότητες να μην μένουν για μεγάλο χρονικό διάστημα σε κατάσταση χαλαρότητας, ακόμα και αν αυτές συνεργάζονται όταν βρίσκονται σε κατάσταση επικοινωνίας.
Η φήμη συνδέεται στο CORE, άμεσα, με την συνεργατική συμπεριφορά κάθε οντότητας. Έτσι, μια οντότητα με αρνητική τιμή φήμης κατατάσσεται σαν μια μη ομαλά συμπεριφερόμενη οντότητα, ενώ μια οντότητα με θετική τιμή φήμης κατατάσσεται σαν μια αξιόπιστη οντότητα. Η εκτέλεση μια λειτουργίας από τον πάροχο, εξαρτάται από την συνολική φήμη που έχει ο πάροχος στον πίνακα RT του για την αιτούσα οντότητα, καθώς αν η τιμή της φήμης αυτής είναι αρνητική, η λειτουργία δεν θα εκτελεστεί. Στο CORE, οι οντότητες δεν αποκτούν κάποιο πλεονέκτημα με το να εφαρμόσουν κάποια μη ομαλή συμπεριφορά, καθώς έτσι αποκλείονται από τους διαθέσιμους πόρους. Η αρνητική τιμή που μπορεί να αποδώσει για αυτές ο WD κάποιας οντότητας, μπορεί να τις οδηγήσει σε αποκλεισμό.

Το πρωτόκολλο CORE, μπορεί να εφαρμοστεί ως επέκταση στο πρωτόκολλο δρομολόγησης DSR. Πιο συγκεκριμένα η λειτουργία f που πρέπει κάθε φορά να εκτελεστεί, αναφέρεται στην λειτουργία Ανεύρεσης Διαδρομής Δρομολόγησης του DSR, ενώ με τον μηχανισμό WD ανιχνεύεται η μη ομαλή συμπεριφορά κάποιου κόμβου κατά την φάση αίτησης της λειτουργίας Ανεύρεσης Διαδρομής Δρομολόγησης. Ανάλογα με τη φήμη τους, οι κόμβοι συμμετέχουν ή όχι στην λειτουργία αυτή. Με την ίδια λογική ο μηχανισμός WD μπορεί να ανιχνεύσει κόμβους που δεν συνεργάζονται στην λειτουργία Προώθησης Πακέτων του DSR.

2.4.4 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ CORE

Η προσομοίωση του CORE με σκοπό τον έλεγχο της απόδοσης του, είναι σε εξέλιξη, και πραγματοποιούνται μέσω του προσομοιωτή δικτύων QualNet. Σκοπεύεται να προσομοιωθούν ποικίλες επιθέσεις όπως επιθέσεις παθητικής άρνησης παροχής υπηρεσιών στην λειτουργία της προώθησης και της δρομολόγησης, επιθέσεις ενεργητικής άρνησης παροχής υπηρεσιών, υπονόμευση κίνησης. Οι προσομοιώσεις σκοπεύεται να πραγματοποιηθούν βάσει διαφορετικών σεναρίων όσον αφορά την κινητικότητα και την πυκνότητα των κόμβων, καθώς και το ποσοστό των μη ομαλά συμπεριφερόμενων κόμβων.

Σε γενικές γραμμές, το CORE αποτελεί πρωτόκολλο που σκοπεύει στην υποστήριξη συνεργασία μεταξύ των κόμβων, είναι βασισμένο στη φήμη και δίνει προτεραιότητα στην αποφυγή της άρνησης παροχής υπηρεσιών από τους κόμβους. Για το λόγο αυτό, μεταδίδεται μόνο η θετική φήμη των κόμβων. Βοηθάει στον εντοπισμό των εγωιστικών κόμβων, στον αποκλεισμό τους από τους πόρους, ενώ είναι σχεδιασμένο για λειτουργίες τόσο του επιπέδου δικτύου όσο και του επιπέδου εφαρμογής. Θεωρείται από τους δημιουργούς του, ότι η επιβάρυνση του CORE κατα την εφαρμογή του στα ήδη υπάρχοντα πρωτόκολλα, είναι πού μικρή.

2.5 OCEAN

Το πρωτόκολλο OCEAN [5] αποτελεί μηχανισμό υποστήριξης συνεργασίας σε ad-hoc δίκτυα, βασιζόμενο στη φήμη. Χρησιμοποιεί μόνο τις first-hand πληροφορίες για την συμπεριφορά των κόμβων, ενώ αποφεύγει τις πληροφορίες φήμης που μεταδίδονται από άλλους κόμβους, ώστε να αποφύγει τις λανθασμένες κατηγορίες που μπορεί να προκύψουν από αυτές. Λόγω αυτής του της λειτουργίας, δεν χρειάζεται η εγκαθίδρυση μηχανισμού εμπιστοσύνης μεταξύ των κόμβων. Το OCEAN επικεντρώνει στο επίπεδο της δρομολόγησης ενώ δεν δίνει βάρος σε μηχανισμούς πιστοποίησης ή κωδικοποίησης των μηνυμάτων. Επίσης δίνει βάση στην αυτοτελή μη ομαλή συμπεριφορά των κόμβων, και αγνοεί την περίπτωση συνεργασίας μεταξύ των κόμβων.

2.5.1 ΛΕΙΤΟΥΡΓΙΑ

Το OCEAN θεωρεί δύο τύπους μη ομαλής συμπεριφοράς των κόμβων όσον αφορά τη δρομολόγησης:

1. Την ***παραπλανητική***, όπου ένας κόμβος μπορεί να αποκριθεί θετικά σε αιτήσεις δρομολόγησης αλλά στη συνέχεια να μην προωθήσει τα πακέτα, παραπλανώντας τους κόμβους που επιθυμούν να προωθήσουν πακέτα μέσω αυτού. Παρόλα αυτά δεν χρησιμοποιεί μηχανισμούς για ενημέρωση των υπολοίπων κόμβων του δικτύου για την παραπλανητική αυτή συμπεριφορά ώστε να τιμωρηθεί ο κόμβος που την πραγματοποιεί, αποφεύγοντας έτσι την εγκαθίδρυση εμπιστοσύνης μεταξύ των κόμβων. Αποφεύγει επίσης τους μηχανισμούς πιστοποίησης για την αποφυγή λάθος κατηγοριών κόμβων, που προσθέτουν πολυπλοκότητα.
   Στην περίπτωση αυτή μη ομαλής συμπεριφοράς, το OCEAN δεν επιτρέπει καμία ανταλλαγή second-hand πληροφοριών φήμης. Αντιθέτως, κάθε κόμβος παίρνει αποφάσεις για τη δρομολόγηση βασιζόμενος στην άμεση παρατήρηση των γειτονικών του κόμβων, εξαλείφοντας την πολυπλοκότητα της διαχείρισης της εμπιστοσύνης μεταξύ των κόμβων. Σύμφωνα με τους κατασκευαστές του, η λιγότερη πληροφορία που μεταδίδεται δεν επηρεάζει και την απόδοσή του. Δεν καταφέρνει παρόλα αυτά την τιμωρία των μη ομαλά συμπεριφερόμενων κόμβων στον βαθμό που το καταφέρνουν μηχανισμοί με πιο αναπτυγμένα συστήματα φήμης.
2. Την ***εγωιστική***, όπου ένας κόμβος δεν ανταποκρίνεται καν στις αιτήσεις δρομολόγησης άλλων κόμβων, και παρόλα αυτά αποστέλλει την δική του κίνηση μέσα από το δίκτυο, διαχειριζόμενος άδικα σε σχέση με τους άλλους κόμβους τους πόρους του δικτύου. Η συμπεριφορά είναι δύσκολα ανιχνεύσιμη και για την ανίχνευση της χρειάζεται η παρατήρηση της προώθησης δεδομένων από τους γειτονικούς κόμβους. Το OCEAN χρησιμοποιεί για τον σκοπό αυτό, απλές, ελαφριές και οικονομικές μεθόδους για την άμεση παρατήρηση των γειτονικών κόμβων που μπορεί να μην επιτυγχάνουν τον μέγιστο βαθμό δικαιοσύνης αλλά δεν επηρεάζουν πολύ αρνητικά την απόδοση.

2.5.1.1 ΑΝΤΙΜΕΤΩΠΙΣΗ ΠΑΡΑΠΛΑΝΗΤΙΚΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ

Το OCEAN έχει σχεδιαστεί για να λειτουργεί ως επέκταση του κλασικού πρωτοκόλλου δρομολόγησης DSR. Απαρτίζεται από πέντε βασικά συστατικά

στοιχεία που βοηθούν στην ανίχνευση και μετρίαση της παραπλανητικής μη ομαλής συμπεριφοράς των κόμβων:

- ***Ανιχνευτής Γειτονιάς****(Neighbor Watch)*. Το εργαλείο αυτό παρατηρεί τη συμπεριφορά των γειτονικών κόμβων ενός κόμβου. Βασίζεται στην πανκατευθυντική φύση των κεραιών των κόμβων καθώς και υποθέτει ότι οι ζεύξεις μεταξύ των κόμβων είναι συμμετρικές και διπλής κατεύθυνσης. Το εργαλείο λειτουργεί ως εξής:
  Όταν ένας κόμβος προωθεί ένα πακέτο, το εργαλείο αποθηκεύει το άθροισμα ελέγχου(ckecksum) του πακέτου, και στη συνέχεια ανιχνεύει το ασύρματο κανάλι αφού έχει στείλει το πακέτο στον γειτονικό κόμβο. Εάν δεν ανιχνεύσει την προσπάθεια του γειτονικού κόμβου να προωθήσει το πακέτο μέσα σε ένα συγκεκριμένο χρονικό διάστημα, καταγράφει ένα αρνητικό γεγονός εναντίον του γειτονικού κόμβου, και διαγράφει από τη μνήμη του το άθροισμα ελέγχου του πακέτου. Στην περίπτωση πάλι, που ο Neighbor Watch, ανιχνεύσει μια απόπειρα προώθησης του πακέτου από τον γειτονικό κόμβο, συγκρίνει το πακέτο που προωθεί με το αποθηκευμένο άθροισμα ελέγχου, και αν ταιριάζουν καταγράφει ένα θετικό γεγονός για τον γειτονικό κόμβο, και διαγράφει από τη μνήμη του το άθροισμα ελέγχου του πακέτου. Εάν δεν ταιριάζουν, ο κόμβος θεωρεί ότι το πακέτο του δεν έχει προωθηθεί. Τα γεγονότα που καταγράφονται, παραδίδονται στον ***Βαθμολογητή Διαδρομής Δρομολόγησης****(RouteRanker),* που κρατά βαθμολογίες για τους γειτονικούς κόμβους.
  Ο Neighbor Watch, δεν είναι μια εγγυημένη υπηρεσία. Πάσχει από αδυναμίες όπως για παράδειγμα, το γεγονός ότι έστω και αν το πακέτο του κόμβου έχει προωθηθεί σωστά από τον γειτονικό, δεν είναι βέβαιο ότι έχει παραληφθεί σωστά από τον επόμενο κόμβο. Ο Neighbor Watch, θα μπορούσε να ανιχνεύσει και άλλα γεγονότα όπως, η επιτυχία ή η αποτυχία των υπόλοιπων κόμβων να προωθήσουν πακέτα μεταξύ τους, αλλά στα πλαίσια του OCEAN χρησιμεύει μόνο στην ανίχνευση της παραπλανητικής συμπεριφοράς μόνο των γειτονικών κόμβων, για λόγους χαμηλότερης πολυπλοκότητας και ανάλυσης.
- ***Βαθμολογητής Διαδρομής Δρομολόγησης****(RouteRanker).*Το εργαλείο αυτό λειτουργεί ως εξής:
  Κάθε κόμβος διατηρεί βαθμολογίες για κάθε γειτονικό του κόμβο. Η βαθμολογία κάθε κόμβου αρχικοποιείται ως ουδέτερη, και αυξάνεται ή μειώνεται κάθε φορά που λαμβάνονται θετικά ή αρνητικά γεγονότα από τον Neighbor Watch. Το CORE λειτουργεί πιο αποτελεσματικά όταν η απόλυτη τιμή της αρνητικής μείωσης των βαθμολογιών είναι μεγαλύτερη από την τιμή της θετικής αύξησης. Όταν η βαθμολογία ενός κόμβου πέφτει κάτω από ένα προκαθορισμένο κατώφλι, το Κατώφλι Λάθους, ο κόμβος εισάγεται σε μια λίστα, την *ελαττωματική* λίστα. Η λίστα αυτή περιέχει όλους τους ανιχνευμένους μη ομαλά συμπεριφερόμενους κόμβους. Μια διαδρομή δρομολόγησης χαρακτηρίζεται ως θετική η αρνητική, ανάλογα με το αν ο επόμενος κόμβος στην διαδρομή ανήκει ή όχι στην λίστα αυτή. Η βαθμολόγηση των διαδρομών δρομολόγησης είναι πολύ απλή, καθώς αυτές διαχωρίζονται μόνο σε θετικές και αρνητικές. Οι παράμετροι στο OCEAN έχουν τις παρακάτω προκαθορισμένες τιμές:

  Ουδέτερη Βαθμολογία: 0
  Θετικό Βήμα: 1

Αρνητικό Βήμα: -2
Κατώφλι Λάθους: -40

- ***Δρομολόγηση βασισμένη στην κατάταξη****(Rank-Based Routing)*. Το εργαλείο αυτό αξιοποιεί τις πληροφορίες που δίνει ο Neighbor Watch, για την επιλογή των διαδρομών δρομολόγησης. Για την αποφυγή διαδρομών που περιέχουν κόμβους οι οποίοι βρίσκονται στην ελαττωματική λίστα, το OCEAN προσθέτει στο πακέτο ROUTE REQUEST(RREQ) του DSR, ένα πεδίο μεταβλητού μήκους, που ονομάζεται λίστα *αποφυγής*. Η λίστα αυτή περιέχει τους κόμβους που ο αποστολέας των RREQ θέλει να αποφύγει σε μελλοντικές διαδρομές δρομολόγησης. Για το λόγο αυτό, ο αποστολέας των RREQ ενσωματώνει την ελαττωματική του λίστα, στην λίστα αποφυγής του πακέτου RREQ. Έτσι, κάθε κόμβος που λαμβάνει το πακέτο αυτό, ελέγχει τη λίστα αποφυγής του, με σκοπό να αποφασίσει αν θα καταστείλει το πακέτο ή θα το μεταδώσει παραπέρα ή αν θα στείλει πίσω ένα μήνυμα ROUTE REPLY, όπου περιέχει τη συνολική διαδρομή δρομολόγηση της πηγής. Εάν κάποιος κόμβος προς αποφυγή, βρίσκεται μέσα στη διαδρομή δρομολόγησης, το πακέτο RREQ καταστέλλεται ενώ αν η διαδρομή δρομολόγησης δεν περιέχει κάποιον τέτοιον κόμβο στο πακέτο ROUTE REPLY, αποστέλλεται το πακέτο αυτό. Σε άλλη περίπτωση το ROUTE REPLY απορρίπτεται.
  Με τον τρόπο αυτό, κάθε κόμβος αποφασίζει ο ίδιος τοπικά, ποιους κόμβους θα εμπιστευτεί, και έχει έλεγχο μόνο των διαδρομών που περνούν άμεσα από αυτόν. Υπάρχει περίπτωση βέβαια, να αποπειραθεί αλλοίωση των λιστών αποφυγής από κάποιον κακόβουλο κόμβο, πράγμα που αποτρέπεται από το ίδιο το OCEAN.
- ***Απόρριψη Κακόβουλης Κίνησης****(Malicious Traffic Reject).* Το εργαλείο αυτό απορρίπτει την κίνηση δεδομένων από κόμβους που θεωρεί ότι έχουν παραπλανητική μη ομαλή συμπεριφορά. Για να αποφευχθεί η περίπτωση όπου ένας τέτοιος κόμβος προωθεί τα πακέτα του υποτιθέμενος ότι προωθεί πακέτα για λογαριασμό κάποιου άλλου κόμβου, απορρίπτεται συνολικά όλη η εκπεμπόμενη κίνηση του κόμβου αυτού.
- ***Μηχανισμός Δεύτερης Ευκαιρίας****(Second Chance Mechanism).* Το εργαλείο αυτό, έχει ως σκοπό να επιτρέπει σε κόμβους που μέχρι στιγμής θεωρούνταν παραπλανητικοί, να ξαναεισέλθουν στην επικοινωνία. Χωρίς την ύπαρξη τέτοιου μηχανισμού, κάθε φορά που κάποιος κόμβος θα εισερχόταν στην ελαττωματική λίστα, θα αποφεύγονταν από τους υπολοίπους κάθε διαδρομή δρομολόγησης που τον περιείχε, με αποτέλεσμα να μην δίνεται η δυνατότητα στον κόμβο να αποδείξει ότι έχει βελτιώσει την συμπεριφορά του. Κάτι τέτοιο θα ήταν πολύ σκληρή τιμωρία για έναν κόμβο, ιδιαίτερα αν αναλογισθεί κανείς το γεγονός ότι ο Neighbor Watch δεν δίνει εγγυημένα σωστά αποτελέσματα. Χάρη στο εργαλείο αυτό, αποφεύγονται οι «αιώνιες» τιμωρίες σε κόμβους που μπορεί απλά να αντιμετώπιζαν πρόβλημα λόγω κάποιων προβληματικών ζεύξεων ή που αναγκάστηκαν να επανεκκινήσουν την διεπαφή τους. Το εργαλείο, φροντίζει ώστε ένας κόμβος με παραπλανητική συμπεριφορά να βγαίνει από την ελαττωματική λίστα, μετά από μια περίοδο απραγίας. Η περίοδος αυτή ονομάζεται **Ανάπαυλα Λάθους**. Παρόλα αυτά, ακόμα κι αν σβηστεί από την ελαττωματική λίστα, η βαθμολογία του παραμένει αρνητική ώστε αν συνεχίσει τα παραπτώματα, να ξαναεισαχθεί άμεσα στην λίστα αυτή.

2.5.1.2 ΑΝΤΙΜΕΤΩΠΙΣΗ ΕΓΩΙΣΤΙΚΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ

Το OCEAN σε γενικές γραμμές τιμωρεί κόμβους με εγωιστική συμπεριφορά, απορρίπτοντας την κίνηση δεδομένων τους, χρησιμοποιώντας αυτήν την τιμωρία σαν φόβητρο για τους υπόλοιπους κόμβους. Η ανίχνευση εγωιστικής συμπεριφοράς μέσω παρατηρήσεων στο πρωτόκολλο δρομολόγησης, είναι σχετικά δύσκολη υπόθεση, καθώς υπάρχουν αρκετές τεχνικές μέσα από τις οποίες ένας κόμβος μπορεί να αποφύγει να είναι ορατός σαν ένας πιθανός δρομολογητής πακέτων. Τέτοιες τεχνικές με τις οποίες οι κόμβοι στο DSR μπορούν να γίνουν μη ανιχνεύσιμοι είναι οι εξής:

1. Απόρριψη πακέτων RREQ. Μια τέτοια μη επιτρεπτή απόρριψη μπορεί να γίνει εύκολα μη ανιχνεύσιμη, καθώς τα RREQ εκπέμπονται πλατιά στους κόμβους και δεν ακολουθούνται από κάποια επιβεβαίωση, ενώ σε κάποιες περιπτώσεις η απόρριψη τους μπορεί να είναι και νόμιμη.
2. Εισαγωγή υπερβολικού αριθμού κόμβων στην διαδρομή δρομολόγησης στο πακέτο RREQ. Εάν ένας κόμβος προσθέσει πολλούς άλλους κόμβους σε ένα πακέτο RREQ, το μονοπάτι θα φαίνεται πολύ μακρύ σε σχέση με μονοπάτια που περνούν από κόμβους που δεν έχουν ανάμιξη με το RREQ. Αυτό έχει σαν αποτέλεσμα, κόμβοι που ακολουθούν την διαδικασία υπερβολικής εισαγωγής κόμβους στις διαδρομές στα πακέτα RREQ, να μην επιλέγονται.
3. Εισαγωγή μιας μη υπαρκτής διαδρομής στο RREQ. Εάν ένας κόμβος αλλοιώσει τη διαδρομή στο πακέτο RREQ, με τέτοιον τρόπο ώστε αυτή να μην είναι υπαρκτή, η κίνηση δεδομένων δεν θα φτάσει ποτέ στον κόμβο με την μη ομαλή αυτή συμπεριφορά.

Καθώς τέτοιες τεχνικές μπορούν να περάσουν απαρατήρητες, αν το πρωτόκολλο δεν προστατευτεί βαριά κρυπτογραφικά μέσα(κάτι που δεν γίνεται στο OCEAN), η καλύτερη απόδειξη ότι ένας κόμβος συνεργάζεται στην διαδικασία της επικοινωνίας μπορεί να είναι ο αριθμός των πακέτων που αυτός προωθεί. Στην περίπτωση αυτή, η απόφαση ενός κόμβου σχετικά με το αν πρέπει ή όχι να προωθήσει ένα πακέτο, βασίζεται στην προηγούμενη απόδοσή του σχετικά με την προώθηση πακέτων. Μια τέτοια τεχνική, επιφέρει μια χαλαρή οικονομία στην προώθηση πακέτων μεταξύ των κόμβων.
Σε αντίθεση με αυτά, το OCEAN βασίζεται αποκλειστικά στις άμεσες παρατηρήσεις της επικοινωνίας με τους γειτονικούς κόμβους για να αξιολογηθεί η απόδοσή τους. Κάθε κόμβος, διατηρεί μετρητές(chipcounts) για κάθε γείτονά του. Ένας κόμβος κερδίζει chips(που αυξάνουν τον αντίστοιχο μετρητή), από έναν κόμβο, όταν ο πρώτος προωθεί ένα πακέτο για χάρη του δεύτερου. Αντιστοίχως, ένας κόμβος χάνει chips, όταν του ζητηθεί από κάποιον κόμβο να προωθήσει ένα πακέτο και αυτός δεν το κάνει. Κάθε φορά που ένας κόμβος πρέπει να αποφασίσει αν θα προωθήσει ή όχι πακέτα κάποιου άλλου κόμβου, ελέγχει τον μετρητή του για τον κόμβο αυτό, και αν αυτός πέσει κάτω από ένα κατώφλι, αρνείται να προωθήσει.

Υπάρχουν και άλλες τεχνικές βασισμένες σε μεγάλο βαθμό στους μηχανισμούς υποστήριξης συνεργασίας που χρησιμοποιούν χρεώσεις. Υπάρχουν δύο βασικά σχήματα που υλοποιούν τη διαδικασία αυτή:

1. Το ***αισιόδοξο***. Στο σχήμα αυτό, ένας κόμβος Α αυξάνει τον μετρητή για ένα κόμβο Β, όταν ο Β δέχεται ένα πακέτο από τον Α, άσχετα από το αν ο Β τελικά προωθήσει το πακέτο.

2. Το ***απαισιόδοξο***. Στο σχήμα αυτό, ένας κόμβος Α αυξάνει μετρητή για τον κόμβο Β, μόνο όταν παρατηρήσει ότι ο Β έχει προωθήσει το πακέτο.

Και στις δύο περιπτώσεις, ο Α ζητά από τον Β να προωθήσει πακέτα, μόνο όταν ο Β συμμετείχε και στο παρελθόν στο πρωτόκολλο για αίτηση διαδρομής δρομολόγησης, και βρίσκεται έτσι σε κάποια διαδρομή δρομολόγησης που περνά από τον Α. Εάν ο Β αποτύχει να προωθήσει τα πακέτα του Α, ο Neighbor Watch ανιχνεύει την μη ομαλή συμπεριφορά του. Και τα δύο όμως σχήματα έχουν σοβαρά ελαττώματα, καθώς στο δεύτερο υπάρχει η περίπτωση δύο κόμβοι να σταματήσουν να προωθούν πακέτα ο ένας για τον άλλον για μεγάλο διάστημα, όταν ο ένα κόμβος αποτυγχάνει να ανιχνεύσει την προώθηση πακέτων από τον άλλον όταν ο πρώτος έχει κάνει μια τέτοια αίτηση. Στο πρώτο πάλι, υπάρχει μια χαλαρότητα στην αντιμετώπιση των μη ομαλά συμπεριφερόμενων κόμβων, αφού τα chips αυξάνονται για τους κόμβους ακόμα κι αν αυτοί δεν προωθήσουν τα πακέτα

Για το λόγο αυτό το OCEAN δεν χρησιμοποιεί αυτά τα σχήματα, αλλά το σχήμα που βασίζεται στους μετρητές και αναφέρθηκε παραπάνω, το οποίο ανιχνεύει την συμπεριφορά όταν ο κόμβος Β ζητά εγωιστικά από τον Α να προωθήσει πακέτα του, ακόμα και όταν ο Β δεν βρίσκεται σε καμία διαδρομή δρομολόγησης που περνά από τον Α. Το σχήμα αυτό βέβαια δεν είναι τόσο δίκαιο για τους κόμβους που βρίσκονται στην περιφέρεια του δικτύου, αφού δεν έχουν μεγάλη δυνατότητα να προωθήσουν πακέτα για άλλους κόμβους με αποτέλεσμα να τιμωρούνται. Το γεγονός αυτό μπορεί να μειώσει σημαντικά το throughput του δικτύου . Για την αντιμετώπιση του προβλήματος αυτού, το OCEAN εισάγει μια ρυθμιζόμενη παράμετρο, την **CAR**(Chip Accumulation Rate). Η παράμετρος αυτή, είναι ο βαθμός στον οποίο όλοι οι μετρητές στο δίκτυο αυξάνονται με το πέρασμα του χρόνου. Έτσι, ακόμα και όταν κάποιος γειτονικός κόμβος δεν προωθεί πακέτα για κάποιο κόμβο, ο μετρητής του δεν είναι μηδενικός με αποτέλεσμα να έχει τη δυνατότητα να προωθήσει πακέτα και αυτός σε έναν περιορισμένο βαθμό.
Μια πολύ μεγάλη τιμή στο CAR βέβαια, θα έδινε τη δυνατότητα στους εγωιστικούς κόμβους να αναμεταδίδουν συνέχεια τα πακέτα τους αφού δεν θα ξέμεναν ποτέ από chips για κανένα κόμβο. Μια μηδενική τιμή πάλι στο CAR, δημιουργεί πρόβλημα στους περιφερειακούς κόμβους και μειώνει το throughput όπως αναφέρθηκε. Για τους παραπάνω λόγους το OCEAN χρησιμοποιεί στο σχήμα αυτό, μια ενδιάμεση τιμή στο CAR που παραμένει όμως χαμηλή, καταφέρνοντας να τιμωρεί τους εγωιστικούς κόμβους πολύ περισσότερο από τους κόμβους που συνεργάζονται σωστά.

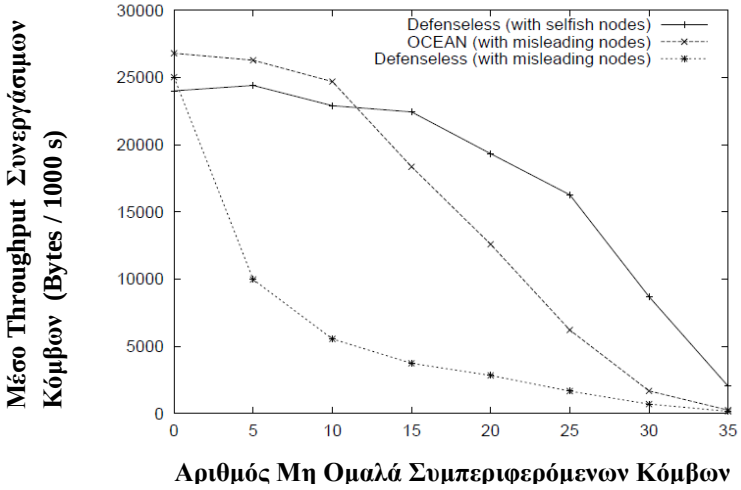
2.5.2 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ OCEAN

Οι απαραίτητες προσομοιώσεις για την εξέταση της απόδοσης του OCEAN πραγματοποιήθηκαν από τους δημιουργούς του, μέσω του προσομοιωτή ad-hoc δικτύων GloMoSim. Το περιβάλλον των προσομοιώσεων διαμορφώθηκε ως εξής:

- Περιοχή 1500m x 300m
- Αριθμός κόμβων 40
- Εμβέλεια μετάδοσης 250m
- Μέγιστη ταχύτητα 20m/s
- Διάρκεια ζωής σύνδεσης 8 πακέτα
- Ελάχιστο μήκος σύνδεσης 2 βήματα
- Εύρος ζώνης ζεύξεων 2Mbps
- Ρυθμός μετάδοσης δεδομένων πηγής 4 πακέτα/s

- Payload δεδομένων εφαρμογής 64 bytes/πακέτο

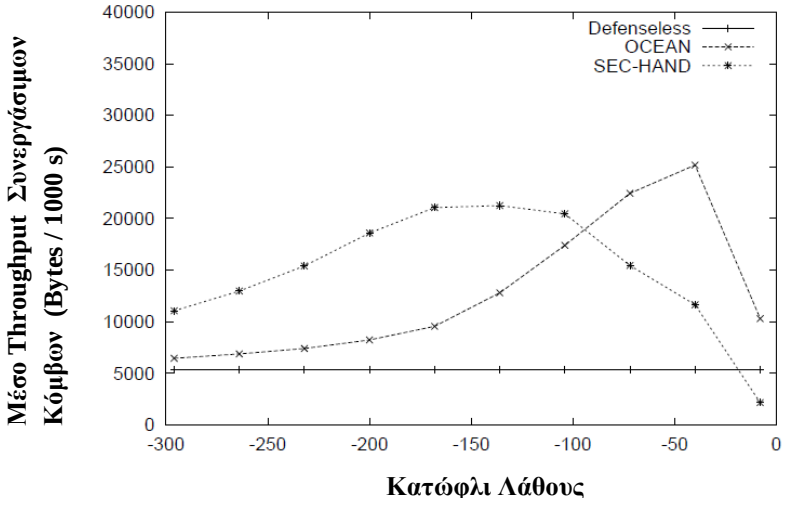
Όπως αναφέρθηκε, βασικό στοιχείο του OCEAN είναι ότι δεν χρησιμοποιεί καθόλου second-hand πληροφορίες. Έχοντας το γεγονός αυτό σαν γνώμονα, και βάσει των προσομοιώσεων, οι κατασκευαστές του, έχουν καταλήξει στα εξής συμπεράσματα και έχουν εξάγει τα παρακάτω διαγράμματα όσον αφορά την απόδοσή του:



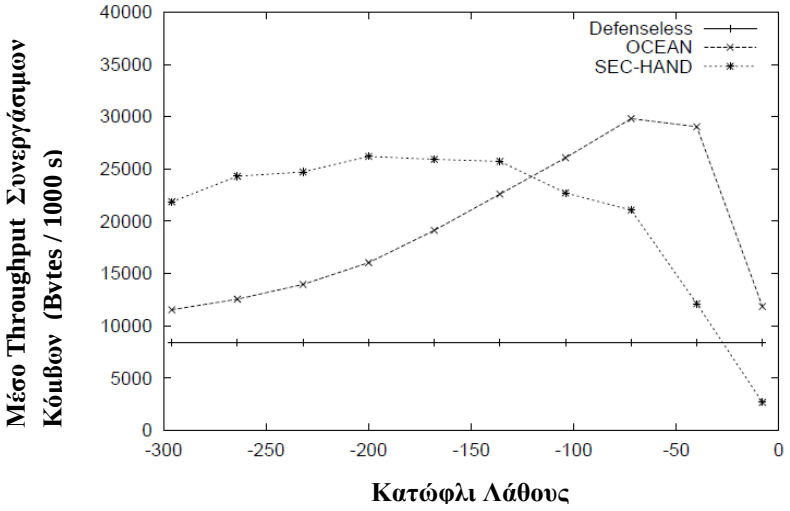
Διάγραμμα 2.5.1 (Πηγή [5])

Από το παραπάνω διάγραμμα που στον κάθετο άξονα έχει το ***μέσο throughput των συνεργάσιμων κόμβων σε Bytes/1000s,*** και στον οριζόντιο άξονα τον ***αριθμό των μη ομαλά συμπεριφερόμενων κόμβων***, συμπεραίνεται ότι ένα δίκτυο που χρησιμοποιεί το OCEAN πετυχαίνει πολύ υψηλότερο throughput από ότι ένα δίκτυο χωρίς αμυντικό μηχανισμό, που περιέχει κόμβους με παραπλανητική συμπεριφορά, ενώ πετυχαίνει throughput κοντά στο αντίστοιχο ενός δικτύου χωρίς αμυντικό μηχανισμό, που περιέχει όμως εγωιστικούς κόμβους, όταν ο αριθμός των κόμβων αυτών είναι σχετικά μικρός.

Τα παρακάτω διαγράμματα έχουν στον κάθετο άξονα έχει το ***μέσο throughput των συνεργάσιμων κόμβων σε Bytes/1000s,*** και στον οριζόντιο άξονα το ***κατώφλι λάθους***, για ***διάρκεια της παύσης της κίνησης*** 0, 100, 400, 1000 δευτερόλεπτα αντίστοιχα με τη σειρά που εμφανίζονται:

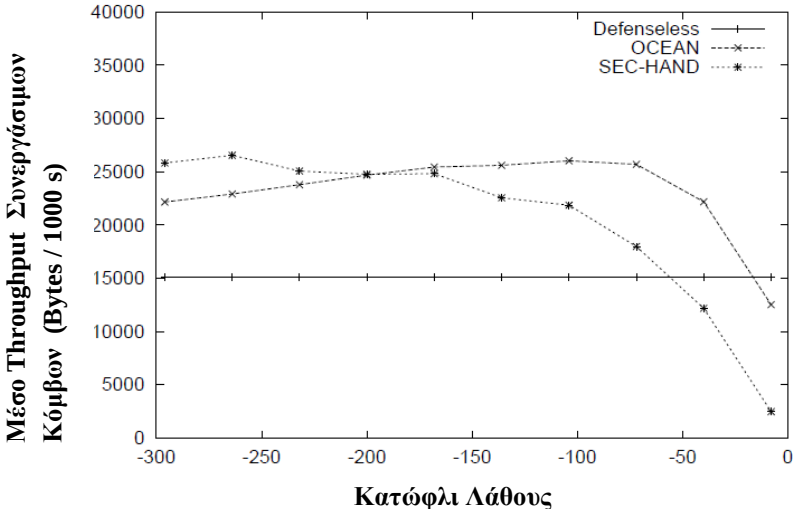


Διάγραμμα 2.5.2 (Πηγή [5])



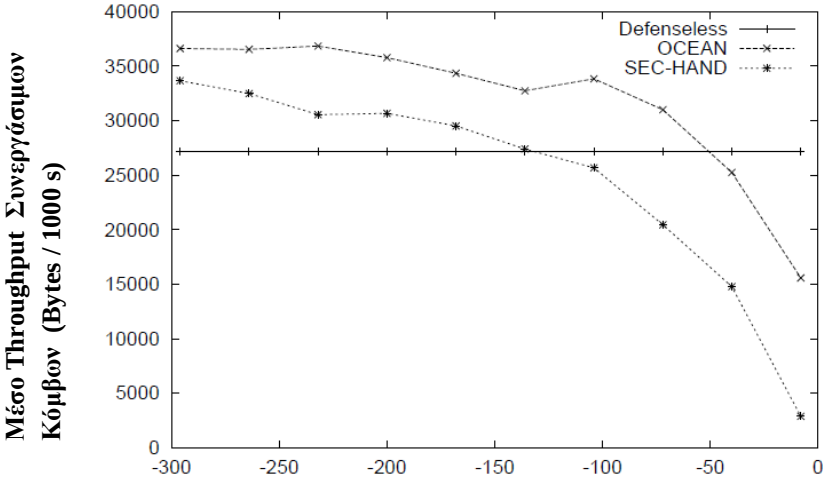
Διάρκεια Παύσης Κίνησης 100

Διάγραμμα 2.5.3 (Πηγή [5])



Διάρκεια Παύσης Κίνησης 400

Διάγραμμα 2.5.4 (Πηγή [5])

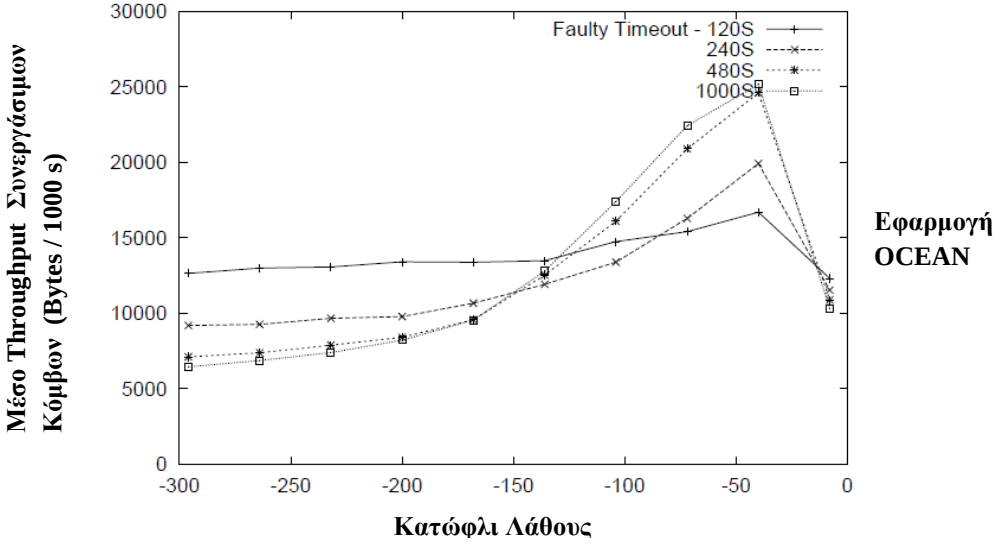


Διάρκεια Παύσης Κίνησης 1000

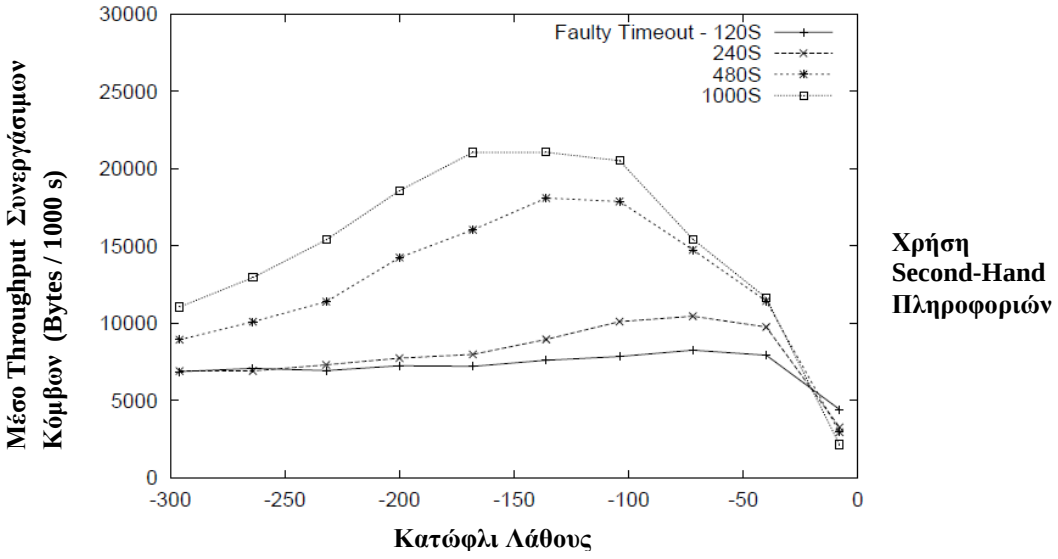
Διάγραμμα 2.5.5 (Πηγή [5])

Από τα παραπάνω συμπεραίνεται ότι ένα δίκτυο που χρησιμοποιεί το OCEAN πετυχαίνει μεγαλύτερο throughput από ένα δίκτυο που χρησιμοποιεί κάποιον μηχανισμό υποστήριξης συνεργασίας με χρήση second-hand πληροφοριών, μόνο όταν η τιμή του Κατωφλίου Λάθους είναι χαμηλή. Σε αντίθετη περίπτωση πετυχαίνει χαμηλότερο throughput. Οι τιμές του throughput είναι πάντα καλύτερες όταν είναι χαμηλή η κινητικότητα των κόμβων.

Αντίστοιχα, εξήχθησαν τα παρακάτω διαγράμματα που στον κάθετο άξονα έχουν το ***μέσο throughput των συνεργάσιμων κόμβων σε Bytes/1000s,*** και στον οριζόντιο άξονα το ***κατώφλι λάθους***, για σύγκριση των δικτύων για τιμές timeout 120, 240, 480 και 1000 δευτερόλεπτα. Το πρώτο κατά σειρά εξήχθη από προσομοίωση δικτύου με εφαρμογή OCEAN, ενώ το δεύτερο από δίκτυο που χρησιμοποιεί second-hand πληροφορίες.



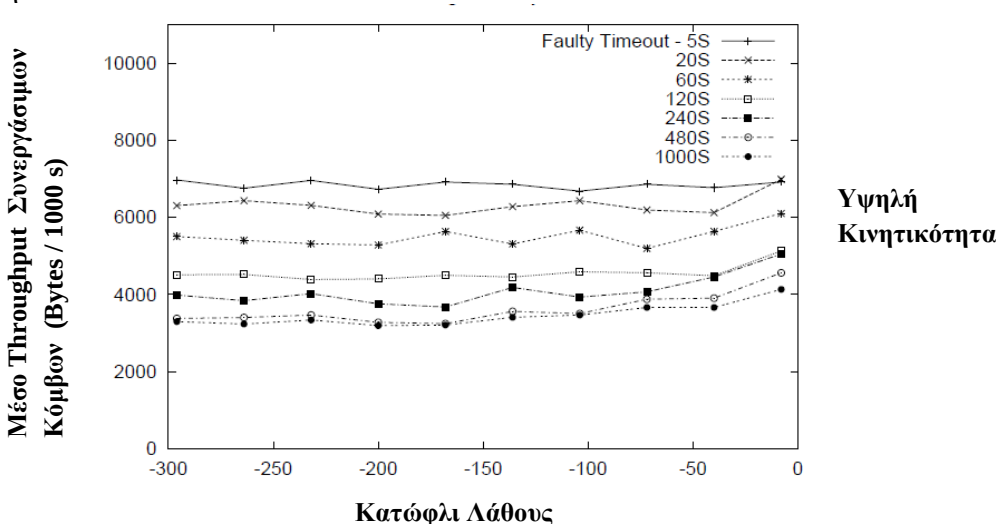
Διάγραμμα 2.5.6 (Πηγή [5])



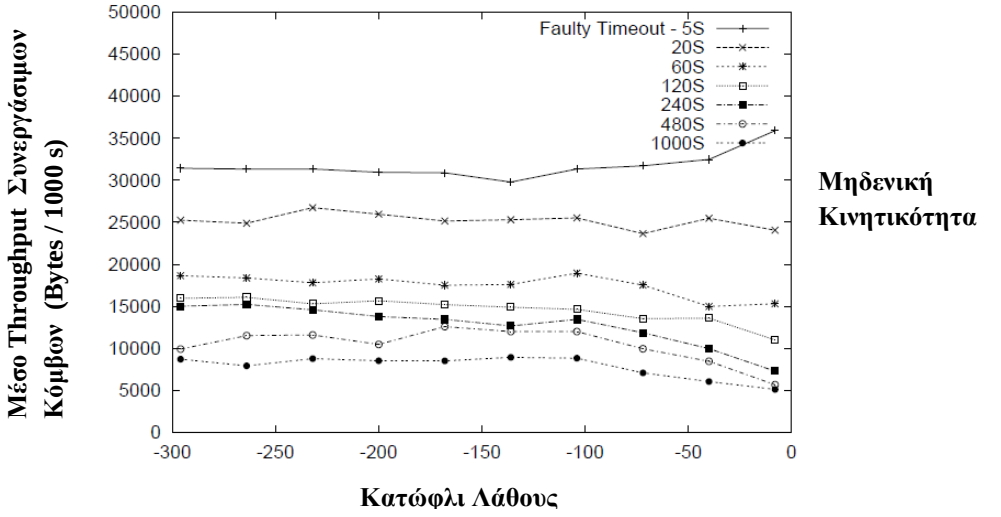
Διάγραμμα 2.5.7 (Πηγή [5])

Παρατηρείται από τα διαγράμματα αυτά, ότι το OCEAN είναι πιο ανθεκτικό απέναντι σε χαμένες πληροφορίες λόγω των timeouts, από ότι ένα δίκτυο που χρησιμοποιεί second-hand πληροφορίες.

Ακόμα φαίνονται τα παρακάτω διαγράμματα που στον κάθετο άξονα έχουν το ***μέσο throughput των παραπλανητικών κόμβων σε Bytes/1000s,*** και στον οριζόντιο άξονα το ***κατώφλι λάθους***, για τιμές timeout 5, 20, 60, 120, 240, 280 και 1000 δευτερόλεπτα, το πρώτο για υψηλή κινητικότητα κόμβων και το δεύτερο για μηδενική:



Διάγραμμα 2.5.8 (Πηγή [5])

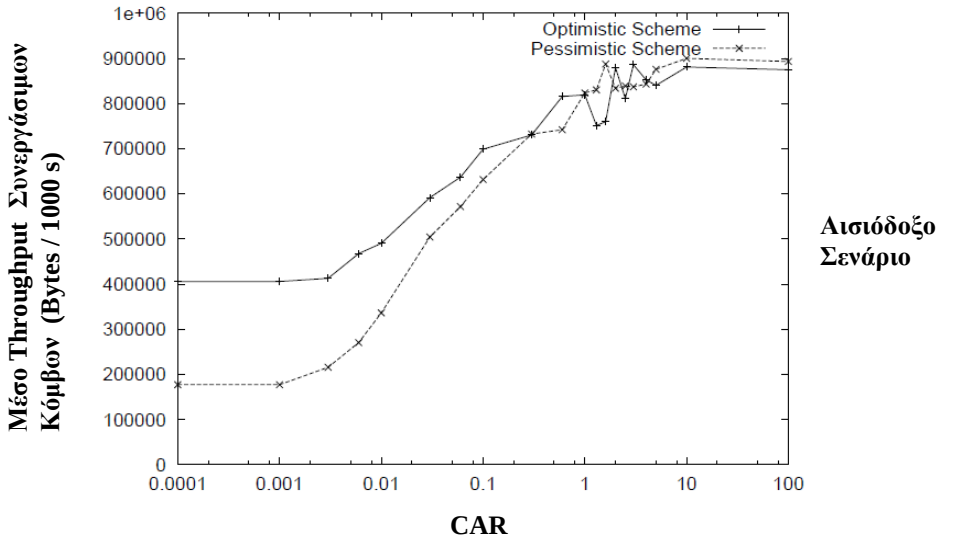


Διάγραμμα 2.5.9 (Πηγή [5])

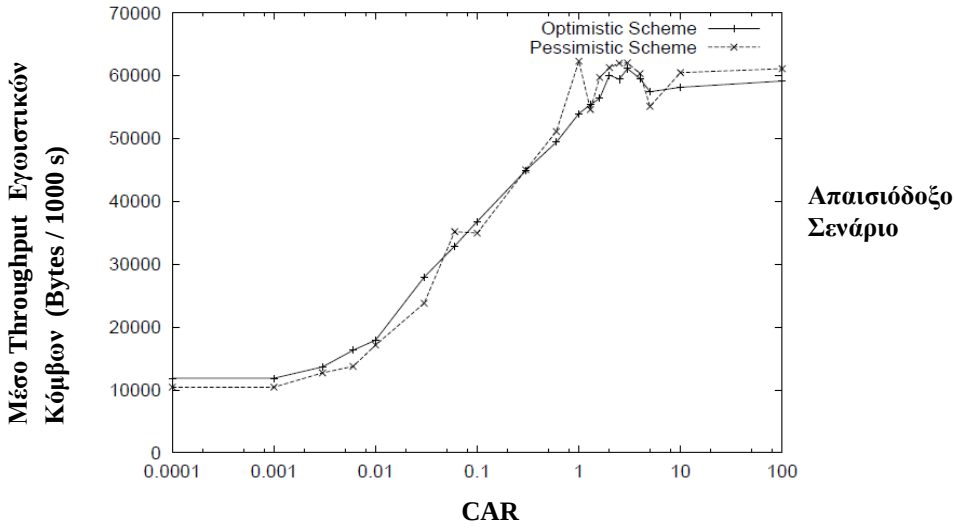
Συμπεραίνεται από αυτά ότι η μείωση της τιμής timeout δίνει περισσότερες ευκαιρίες στου παραπλανητικούς κόμβους, και για το λόγο αυτό αυξάνεται το throughput τους.

Τέλος, τα δύο διαγράμματα που ακολουθούν έχουν στον κάθετο άξονα το ***μέσο throughput των συνεργάσιμων κόμβων σε Bytes/1000s*** το πρώτο***, το μέσο throughput των εγωιστικών κόμβων σε Bytes/1000s*** το δεύτερο, και στον οριζόντιο

την ***τιμή του CAR,*** για προσομοιώσεις που έγιναν σε αισιόδοξο και απαισιόδοξο σενάριο.



Διάγραμμα 2.5.10 (Πηγή [5])



Διάγραμμα 2.5.11 (Πηγή [5])

Φαίνεται ότι το throughput των συνεργάσιμων κόμβων για ίδια τιμή CAR, είναι πολύ μεγαλύτερο από το throughput των εγωιστικών κόμβων.

Κάποια άλλα συμπεράσματα που βγήκαν από τις προσομοιώσεις είναι τα εξής:

- Ένα δίκτυο που χρησιμοποιεί το OCEAN, αποφασίζει γρηγορότερα εάν θα αποφασίσει να επανεισάγει έναν τιμωρημένο κόμβο στην επικοινωνία, από ότι ένα δίκτυο που χρησιμοποιεί κάποιον μηχανισμό υποστήριξης συνεργασίας με χρήση second-hand πληροφοριών.
- Η προσπάθεια αλλοίωσης των λιστών αποφυγής από κάποιον κακόβουλο κόμβο, έχουν πολύ μικρή επίδραση στο OCEAN.

- Σε ένα δίκτυο που χρησιμοποιεί το OCEAN, το throughput των κόμβων με παραπλανητική συμπεριφορά είναι αρκετά υψηλό, πράγμα που είναι αρνητικό.
- Το OCEAN δεν μπορεί να αποφύγει την κατά βούληση αλλαγή του CAR από εγωιστικούς κόμβους.
- Δεν υπάρχει κάποιος μηχανισμός πιστοποίησης που να είναι αρκετά απλός ώστε να ταιριάζει με το πνεύμα του OCEAN.

Συμπερασματικά, το OCEAN είναι ένας πολύ απλός όσον αφορά την πολυπλοκότητα του, μηχανισμός υποστήριξης συνεργασίας. Βασίζεται στην αποφυγή της ανταλλαγής second-hand πληροφοριών και της χρήσης μηχανισμών πιστοποίησης. Καταφέρνει σε μεγάλο βαθμό να ανιχνεύσει και να αντιμετωπίσει κόμβους με παραπλανητική συμπεριφορά ενώ δεν είναι τόσο αποτελεσματικό στην αντιμετώπιση και μείωση της εγωιστικής συμπεριφοράς. Τέλος, το OCEAN συμπεριφέρεται αρκετά καλά σε περιβάλλοντα με κινητικότητα ποικίλης κλίμακας.

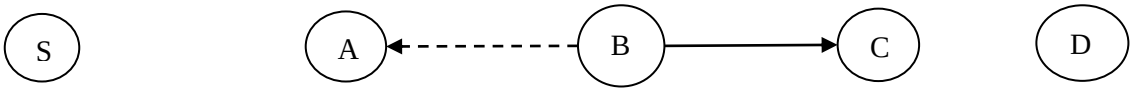
2.6 WATCHDOG - PATHRATER

Ο μηχανισμός υποστήριξης συνεργασίας αυτός βασίζεται από την μία στον εντοπισμό των μη ομαλά συμπεριφερόμενων κόμβων, και από την άλλη στην αποφυγή ένταξης των κόμβων αυτών στις διαδρομές δρομολόγησης από το πρωτόκολλο δρομολόγησης. Το Watchdog - Pathrater [6] λειτουργεί ορθά σε ad-hoc δίκτυα που χρησιμοποιούν αμφίδρομες ζεύξεις. Στο σχήμα αυτό, δεν χρησιμοποιούνται τεχνικές εγκαθίδρυσης εμπιστοσύνης μεταξύ των κόμβων, καθώς κάτι τέτοιο προϋποθέτει ανταλλαγή κλειδιών αλλά ενέχει και τον κίνδυνο δημιουργίας προβλημάτων στην προώθηση, στις περιπτώσεις που αξιόπιστοι κόμβοι είναι υπερφορτωμένοι ή εκτός λειτουργίας και στην περίπτωση που μη αξιόπιστοι κόμβοι ενώ συμπεριφέρονται σωστά, δεν αξιοποιούνται στην επικοινωνία. Δεν χρησιμοποιεί επίσης την τεχνική της απομόνωσης μη ομαλά συμπεριφερόμενων κόμβων από το ίδιο το πρωτόκολλο δρομολόγησης, καθώς κάτι τέτοιο προσθέτει μεγάλη πολυπλοκότητα. Το Watchdog - Pathrater λειτουργεί ως επέκταση στο DSR και προσθέτει σε αυτό κάποιες επιπλέον λειτουργίες με σκοπό τον εντοπισμό και την μετρίαση της μη ομαλής συμπεριφοράς., χωρίς να επηρεάζει σε μεγάλο βαθμό το DSR αυτό καθ' αυτό. Το Watchdog – Pathrater αξιοποιεί δύο βασικά εργαλεία, που απαρτίζουν και το όνομά του, το watchdog και το pathrater, που πραγματοποιούν τις λειτουργίες εντοπισμού των μη ομαλά συμπεριφερόμενων κόμβων και την εξαίρεση τους από τις διαδρομές δρομολόγησης αντίστοιχα. Σε γενικές γραμμές το watchdog, ακούγοντας το ασύρματο κανάλι(ακόμα και αν οι προωθήσεις δεν αφορούν τον κόμβο που πραγματοποιεί την ανίχνευση), επιβεβαιώνει ότι και ο επόμενος κόμβος στο μονοπάτι προωθεί το πακέτο. Εάν ο επόμενος κόμβος δεν προωθήσει το πακέτο, χαρακτηρίζεται ως μη ομαλά συμπεριφερόμενος. Το pathrater χρησιμοποιώντας την πληροφορία αυτή επιλέγει τα μονοπάτια που είναι πιο πιθανό να επιτύχουν την ορθή προώθηση των πακέτων. Στόχος του μηχανισμού είναι η αύξηση του throughput του δικτύου χωρίς να επιφέρεται υψηλή επιβάρυνση, πράγμα που επιτυγχάνεται με χρήση ειδικού μηχανισμού. Παρακάτω αναλύονται οι βασικές λειτουργίες του πρωτοκόλλου:

- ***Ανίχνευση***, που πραγματοποιείται από το εργαλείο **Watchdog.**
- ***Θέσπιση Μονοπατιών***, που πραγματοποιείται από το εργαλείο **Pathrater.**

2.6.1 ΑΝΙΧΝΕΥΣΗ

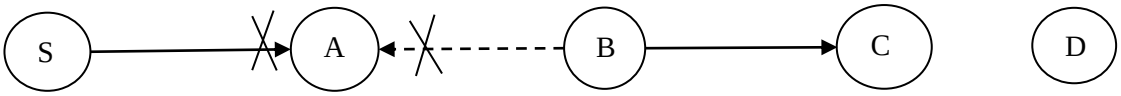
Η μέθοδος που χρησιμοποιεί το Watchdog για τον εντοπισμό των μη ομαλά συμπεριφερόμενων κόμβων λειτουργεί ως εξής:
Έστω ένα κόμβος S θέλει να αποστείλει πακέτα στον κόμβο D, μέσω ενός μονοπατιού που περιέχει τους ενδιάμεσους κόμβους A, B και C. Εάν ο κόμβος A δεν μπορεί να μεταδώσει πακέτα απευθείας στον κόμβο C, πρέπει να το κάνει μέσω του κόμβου B. Για το λόγο αυτό ο A προωθεί το πακέτο στον B και ελέγχει αν αυτός θα το προωθήσει με τη σειρά του στον C. Ο A μπορεί να ελέγξει επίσης, εάν ο κόμβος B έχει αλλοιώσει την επικεφαλίδα του πακέτου. Η διαδικασία αυτή φαίνεται σχηματικά παρακάτω, όπου η ενιαία γραμμή δείχνει την προώθηση του πακέτου, ενώ η διακεκομμένη δείχνει την δυνατότητα του A να ακούσει τη μετάδοση του B.



Σχήμα 2.6.1

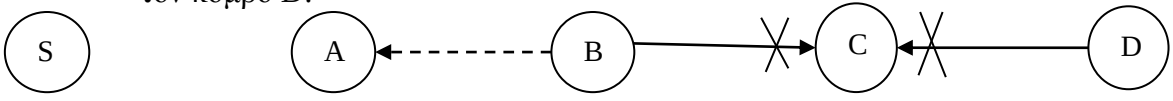
Ο κόμβος με τη χρήση του watchdog, διατηρεί μια μνήμη με τα πακέτα που έχει στείλει πρόσφατα. Ελέγχει αν τα πακέτα που προωθούνται από τον επόμενο κόμβο ταιριάζουν με αυτά που έχει αποθηκεύσει στη μνήμη του, και αν αυτό ισχύει διαγράφει τα πακέτα αυτά από τη μνήμη. Εάν ένα πακέτο μείνει στην μνήμη περισσότερο από ένα συγκεκριμένο χρονικό διάστημα, το watchdog δημιουργεί μια καταγραφή βλάβης για τον κόμβο που ήταν υπεύθυνος για την προώθηση του πακέτου. Στην περίπτωση που η καταγραφή ξεπεράσει ένα συγκεκριμένο εύρος ζώνης, το εργαλείο θεωρεί ότι ο κόμβος είναι μη ομαλά συμπεριφερόμενος και στέλνει ένα μήνυμα στην πηγή αποστολής του πακέτου ενημερώνοντας για την συμπεριφορά του κόμβου αυτού.
Το watchdog έχει πλεονεκτήματα, όπως το ότι ανιχνεύει την μη ομαλή συμπεριφορά στο επίπεδο της προώθησης, αλλά και μειονεκτήματα. Τέτοιες αδυναμίες που εμφανίζει όσον αφορά την ανίχνευση μη ομαλής συμπεριφοράς είναι:

- Η *ασαφής σύγκρουση*, κατά την οποία ο κόμβος Α αδυνατεί να ακούσει τις μεταδόσεις του κόμβου Β. Στην περίπτωση αυτή, συμβαίνει μια σύγκρουση στον Α, τη στιγμή που προσπαθεί να ακούσει αν ο Β προώθησε ένα πακέτο. Έτσι, ο Α δεν γνωρίζει αν η σύγκρουση συνέβη κατά την προσπάθεια του Β να προωθήσει το πακέτο, ή αν ο Β δεν προώθησε ποτέ το πακέτο και η σύγκρουση συνέβη από άλλους γειτονικούς κόμβους του Α. Λόγω της αβεβαιότητας αυτής, ο Α δεν μπορεί να κατηγορήσει άμεσα τον β σαν μη ομαλά συμπεριφερόμενο κόμβο, αλλά πρέπει να συνεχίσει να παρακολουθεί τον Β για ένα χρονικό διάστημα. Εάν ο Α δεν ανιχνεύει συνεχόμενα την προώθηση πακέτων από τον Β, τότε τον θεωρεί μη ομαλά συμπεριφερόμενο. Η αδυναμία αυτή φαίνεται σχηματικά παρακάτω, όπου ο Α δεν μπορεί να καταλάβει αν η σύγκρουση προήλθε από τον Β ή από τον S, με αποτέλεσμα να μην γνωρίζει αν τελικά ο Β προώθησε το πακέτο όπως αναμενόταν:



Σχήμα 2.6.2

- Η *σύγκρουση στον παραλήπτη*, κατά την οποία ο κόμβος Α γνωρίζει μόνο ότι ο Β προώθησε το πακέτο, αλλά δεν γνωρίζει εάν ο κόμβος C το παρέλαβε. Στην περίπτωση αυτή, που η σύγκρουση συμβαίνει στον C, ο Α ακούει μόνο ότι ο Β προώθησε το πακέτο, άσχετα με το αν ελήφθη από τον C, και υποθέτει ότι ο C έλαβε το πακέτο. Έτσι, δίνεται η δυνατότητα στον Β να μην ξαναπροωθήσει το πακέτο, αφήνοντας τον Α να νομίζει ότι η αποστολή και λήψη έγιναν όπως ήταν αναμενόμενο, όπως επίσης και η δυνατότητα να προκαλέσει επίτηδες σύγκρουση, προωθώντας το πακέτο την ίδια στιγμή που ο C μεταδίδει. Στην πρώτη περίπτωση ο Β πράττει αυτήν την ενέργεια για εγωιστικούς σκοπούς ενώ στην δεύτερη επειδή είναι κακόβουλος. Η δεύτερη περίπτωση βέβαια είναι αρκετά σπάνια καθώς ο κόμβος Β πρέπει να σπαταλήσει μεγάλο χρόνο υπολογισμού αλλά και εύρος ζώνης. Η αδυναμία αυτή φαίνεται σχηματικά παρακάτω, όπου ο Α λανθασμένα θεωρεί ότι το πακέτο του έφτασε στον C, κάτι που δεν έγινε ποτέ λόγω σύγκρουσής του με πακέτο που προέρχεται από τον κόμβο D:



Σχήμα 2.6.3

- Η *λανθασμένη κατηγορία κόμβων ως μη ομαλά συμπεριφερόμενων*, κατά την οποία ένας κακόβουλος κόμβος Α μπορεί να προσπαθήσει να διατμήσει το δίκτυο υποστηρίζοντας ότι κάποιοι κόμβοι που ακολουθούν αυτόν στο μονοπάτι δρομολόγησης, είναι μη ομαλά συμπεριφερόμενοι. Για παράδειγμα, ο κόμβος Α μπορεί αναφέρει ότι ο κόμβος Β δεν προωθεί πακέτα, ενώ στην πραγματικότητα προωθεί, κάνοντας τον κόμβο S λανθασμένα να θεωρήσει τον β σαν μη ομαλά συμπεριφερόμενο. Παρόλα αυτά μια τέτοια συμπεριφορά είναι ανιχνεύσιμη, καθώς ο κόμβος S κάποια στιγμή θα λάβει μηνύματα επιβεβαίωσης από τον D, πράγμα που εάν ίσχυαν οι κατηγορίες για τον Β δεν θα μπορούσε να συμβεί. Ανιχνεύσιμη από τον Β ο οποίος θα την αναφέρει στον D, θα είναι και η προσπάθεια του Α να απορρίψει τα μηνύματα επιβεβαίωσης ώστε να τα αποκρύψει από τον S.
- Ο *έλεγχος της ισχύος μετάδοσης από κάποιον μη ομαλά συμπεριφερόμενο κόμβο*, κατά την οποία ένας κόμβος μπορεί να περιορίσει την ισχύ μετάδοσης του έτσι ώστε το σήμα του να είναι αρκετά ισχυρό ώστε να φτάσει στον προηγούμενο κόμβο αλλά ανίσχυρο να φτάσει στον αληθινό παραλήπτη. Μια τέτοια ενέργεια μπορεί να γίνει μόνο από κάποιον κακόβουλο κόμβο που γνωρίζει πόση ισχύς απαιτείται για να φτάσει το σήμα του στους γειτονικούς κόμβους, καθώς κάποιος εγωιστικός κόμβος δεν θα σπαταλούσε ενέργεια για να προβεί στην ενέργεια αυτή.
- Η *δημιουργία συμπαιγνίας από μια ομάδα κόμβων*, κατά την οποία για παράδειγμα ο κόμβος Β και ο κόμβος C του προηγούμενου παραδείγματος, μπορούν να συνεννοηθούν ώστε να διαπράξουν ζημιά στο δίκτυο. Στην περίπτωση αυτή, ο Β προωθεί ένα πακέτο στον C αλλά δεν αναφέρει στον κόμβο Α ότι τελικά ο C απέρριψε το πακέτο. Σε μια τέτοια κατάσταση, είναι αναγκαία η εξαίρεση από τα μονοπάτια δρομολόγησης δύο σε σειρά κόμβους που δρουν κακόβουλα.
- Η *απόρριψη πακέτων από κάποιον κόμβο με χαμηλότερο ρυθμό από τον ελάχιστο ρυθμό που κατανοεί το watchdog*. Στην περίπτωση αυτή βέβαια, ο κόμβος που διαπράττει αυτήν την ενέργεια είναι αναγκασμένος να προωθεί με το ελάχιστο εύρος ζώνης που υποδεικνύει το δίκτυο, έστω και αν το watchdog δεν αντιληφθεί την μη ομαλή συμπεριφορά.

Το εργαλείο watchdog για να είναι αποτελεσματικό πρέπει να γνωρίζει που πρέπει να βρίσκεται το πακέτο σε δύο άλματα ζεύξεων(hops), πράγμα που πετυχαίνεται από το πρωτόκολλο DSR. Με τον τρόπο αυτό αποφεύγεται η ενδεχόμενη προσπάθεια ενός κακόβουλου κόμβου να προωθήσει πακέτα σε έναν μη υπαρκτό κόμβο, χωρίς να το καταλάβει το watchdog.

2.6.2 ΘΕΣΠΙΣΗ ΜΟΝΟΠΑΤΙΩΝ

Το εργαλείο pathrater, που εκτελείται από κάθε κόμβο στο δίκτυο, συνδυάζει πληροφορίες σχετικά με την μη ομαλή συμπεριφορά κάποιων κόμβων, και δεδομένα που αφορούν την αξιοπιστία των ζεύξεων, με σκοπό την επιλογή της πιο αξιόπιστης διαδρομής δρομολόγησης. Κάθε κόμβος διατηρεί μια βαθμολογία για κάθε κόμβο που γνωρίζει στο δίκτυο, και υπολογίζει μία μέτρηση για κάθε μονοπάτι βγάζοντας τον μέσο όρο των βαθμολογιών των κόμβων που παίρνουν μέρος στο μονοπάτι. Μια τέτοια μέθοδος επιλέγει στο pathrater να επιλέγει το πιο σύντομο μονοπάτι όταν δεν

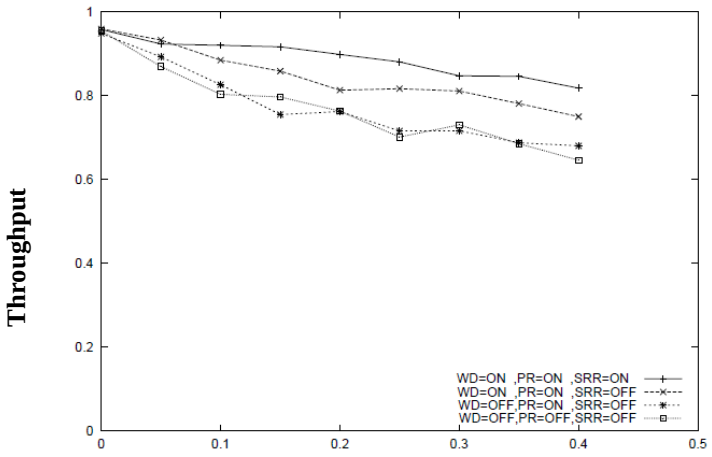
υπάρχουν άλλες διαθέσιμες πληροφορίες για την αξιοπιστία των ζεύξεων. Έτσι, το pathrater, στην περίπτωση που υπάρχουν πολλά διαφορετικά μονοπάτια για έναν προορισμό, επιλέγει αυτό με τον υψηλότερο μέσο όρο βαθμολογιών.
Η ανάθεση βαθμολογιών σε κάθε κόμβο από το pathrater πραγματοποιείται με τον παρακάτω αλγόριθμο:
Όταν ένας κόμβος γίνεται γνωστός στο pathrater, το εργαλείο του αναθέτει την ουδέτερη βαθμολογία 0,5. Όλοι οι κόμβοι βαθμολογούν τον εαυτό τους με την τιμή 1. Μια τέτοια μέθοδος επιβεβαιώνει ότι εάν όλοι οι υπόλοιποι κόμβοι έχουν ουδέτερη βαθμολογία, το pathrater θα επιλέξει την συντομότερη διαδρομή. Το εργαλείο, αυξάνει την βαθμολογία των κόμβων σε όλα τα μονοπάτια που έχουν χρησιμοποιηθεί ενεργά, κατά 0,01 ανά τακτά χρονικά διαστήματα των 200ms. Με τον όρο ενεργά χρησιμοποιημένο μονοπάτι, εννοείται το μονοπάτι από το οποίο ο κόμβος έχει αποστείλει κάποιο πακέτο μέσα στο προηγούμενο διάστημα των 200ms. Η μέγιστη τιμή που μπορεί να πάρει η βαθμολογία ενός ουδέτερου κόμβου είναι 0,8, ενώ η μικρότερη είναι 0. Επίσης, η βαθμολογία ενός κόμβου μειώνεται κατά 0,05 κάθε φορά που ανιχνεύεται βλάβη σε κάποια ζεύξη με αποτέλεσμα ο κόμβος να είναι αδύνατο να προσπελαστεί. Το pathrater δεν διαμορφώνει βαθμολογίες κόμβων που δεν είναι σε ενεργή χρήση.
Στην περίπτωση ύπαρξης μη ομαλά συμπεριφερόμενων κόμβων, τίθεται σε αυτούς μια πολύ υψηλή αρνητική βαθμολογία -100, ώστε όταν ο pathrater υπολογίζει την μέτρηση για τα μονοπάτια, να αντιλαμβάνεται μέσα από την αρνητική τιμή την ύπαρξη ενός ή περισσότερων μη ομαλά συμπεριφερόμενων κόμβων στο μονοπάτι. Βέβαια, για να μην μένουν έξω από την δρομολόγηση για πάντα, κόμβοι οι οποίοι έχουν κατηγορηθεί λανθασμένα ή λόγω κάποιας δυσλειτουργίας ως μη ομαλά συμπεριφερόμενοι, στους κόμβους με αρνητικές βαθμολογίες πρέπει οι βαθμολογίες τους σταδιακά να αυξάνονται ή να μετατρέπονται σε θετικές μετά από ένα μεγάλο χρονικό διάστημα.
Εάν τέλος, το pathrater, δεν μπορεί να βρει μονοπάτι δρομολόγησης που να μην περιέχει μη ομαλά συμπεριφερόμενους κόμβους, αποστέλλει ένα πακέτο ROUTE REQUEST, σύμφωνα με την επιπρόσθετη λειτουργία SRR(Send Route Request).

2.6.3 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ WATCHDOG-PATHRATER

Για την πραγματοποίηση των απαραίτητων προσομοιώσεων οι δημιουργοί του Watchdog-Pathrater χρησιμοποίησαν μια έκδοση του προσομοιωτή Berkeley's Network Simulator, που περιέχει επεκτάσεις όσον αφορά το ζήτημα της ασύρματης επικοινωνίας . Το περιβάλλον προσομοίωσης διαμορφώθηκε ως εξής:

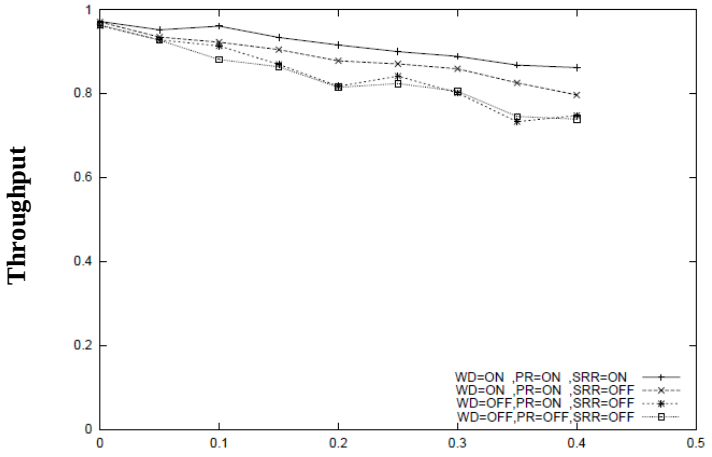
- Περιοχή 670m x 670m
- Αριθμός ασύρματων κόμβων 50
- Πρωτόκολλο MAC 802.11
- Εφαρμογή CBR
- 10 συνδέσεις από κόμβο σε κόμβο
- 4 κόμβοι πηγές με δύο συνδέσεις ο καθένας
- 2 κόμβοι πηγές με μία σύνδεση ο καθένας
- 9 προορισμοί λαμβάνουν μόνο μία ροή δεδομένων
- 1 προορισμός λαμβάνει δύο ροές δεδομένων
- Ταχύτητα από 0 έως 20m/s
- Διάρκεια προσομοίωσης 200s
- Διάρκεια παύσης μέχρι την επόμενη μετάδοση από 0 έως 60s

Οι δημιουργοί του Watchdog – Pathrater ελέγχοντας την λειτουργία του, κάτω από διαφορετικά σενάρια σχετικά με την κινητικότητα των κόμβων, τον συνολικό αριθμό τους αλλά και τον αριθμό των μη ομαλά συμπεριφερόμενων κόμβων, έχουν καταλήξει σε συμπεράσματα όσον αφορά την απόδοση του εξάγοντας και τα αντίστοιχα διαγράμματα, αξιοποιώντας κάποιες μετρήσεις όπως αυτές του throughput και της επιβάρυνσης στο δίκτυο. Ένα ακόμη στοιχείο που σχετίζεται με την απόδοση του πρωτοκόλλου είναι το κατά πόσο επιδρά στο δίκτυο, η περίπτωση στην οποία το Watchdog αναφέρει την μη ομαλή συμπεριφορά ενός κόμβου, την ώρα που αυτή δε συμβαίνει. Παρακάτω φαίνονται τα αποτελέσματα και τα αντίστοιχα συμπεράσματα.



Διάρκεια Παύσης Κίνησης 0

Διάγραμμα 2.6.1 (Πηγή [6])



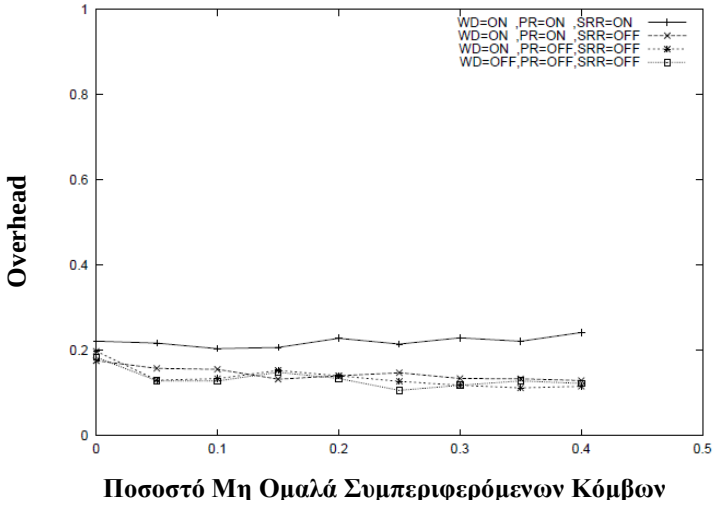
Διάρκεια Παύσης Κίνησης 60

Διάγραμμα 2.6.2 (Πηγή [6])

Τα παραπάνω διαγράμματα έχουν στον κάθετο άξονα τους ***το throughput,*** και στον οριζόντιο άξονα ***το ποσοστό των μη ομαλά συμπεριφερόμενων κόμβων***, για ***διάρκεια παύσης κίνησης των κόμβων 0 και 60 δευτερόλεπτα,*** αντίστοιχα με τη σειρά που εμφανίζονται. Γίνεται σύγκριση για δίκτυα στα οποία εφαρμόζονται ή όχι το Watchdog, το Pathrater και το SRR. Συμπεραίνεται ότι όταν το Watchdog, το

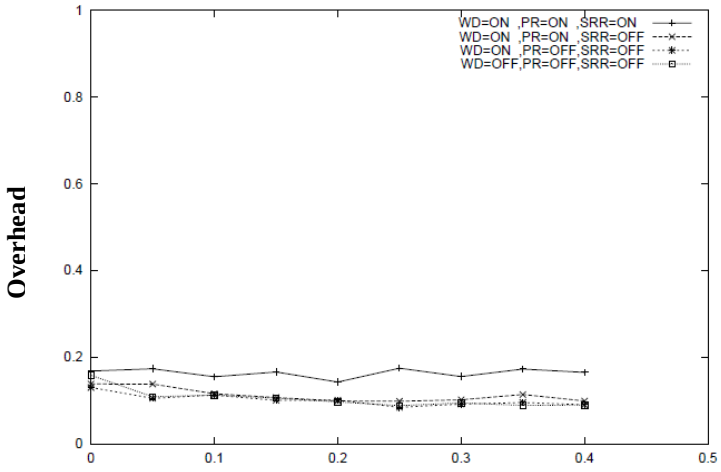
Pathrater και το SRR είναι ενεργά σε ένα ad-hoc δίκτυο, το throughput του δικτύου είναι αρκετά βελτιωμένο(27% πάνω) σε σχέση με το δίκτυο όταν χρησιμοποιεί μόνο το DSR. Το throughput γίνεται πολύ υψηλό όταν οι κόμβοι δεν κινούνται, ακόμα και αν οι μη ομαλά συμπεριφερόμενοι κόμβοι αγγίξουν το 40%. Ακόμα φαίνεται ότι το πρωτόκολλο αγγίζει τις επιθυμητές επιδόσεις σχετικά με την ανίχνευση των μη ομαλά συμπεριφερόμενων κόμβων και της δρομολόγησης, μόνο όταν τα Watchdog, Pathrater και SRR, είναι ταυτοχρόνως ενεργοποιημένα.

Σχετικά με το Overhead στο δίκτυο έχουν παραχθεί τα παρακάτω δύο διαγράμματα έχουν στον κάθετο άξονα τους ***την επιβάρυνση Overhead στο δίκτυο,*** καις τον οριζόντιο άξονα ***το ποσοστό των μη ομαλά συμπεριφερόμενων κόμβων***, για ***διάρκεια παύσης κίνησης των κόμβων 0 και 60 δευτερόλεπτα,*** αντίστοιχα με τη σειρά που εμφανίζονται. Γίνεται σύγκριση για δίκτυα στα οποία εφαρμόζονται ή όχι το Watchdog, το Pathrater και το SRR.



Διάρκεια Παύσης Κίνησης 0

Διάγραμμα 2.6.3 (Πηγή [6])

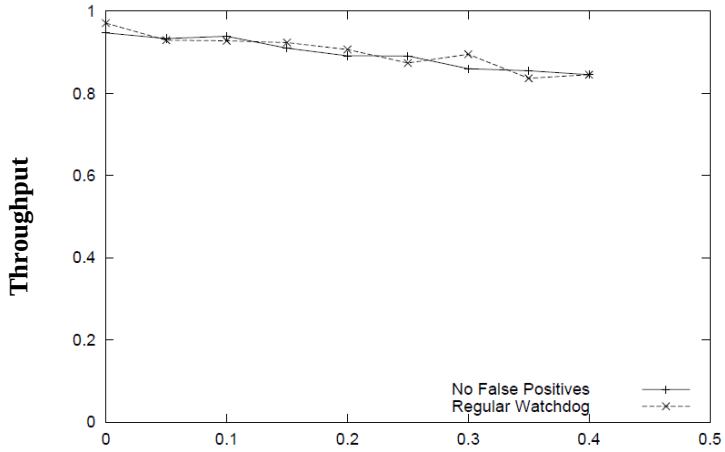


Διάρκεια Παύσης Κίνησης 60

Διάγραμμα 2.6.4 (Πηγή [6])

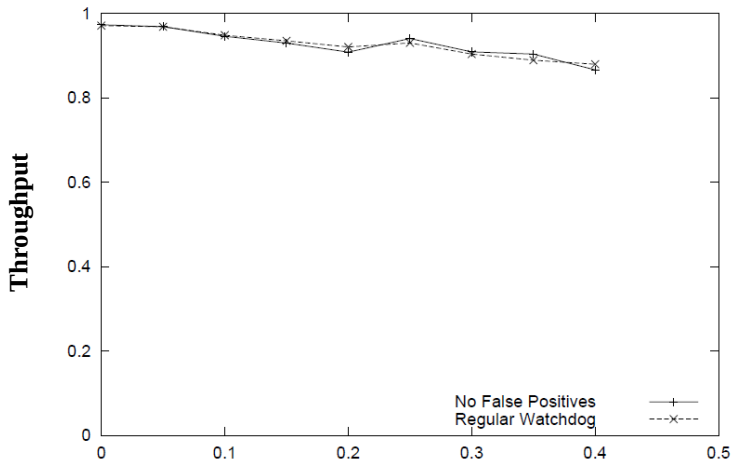
Προκύπτει το συμπέρασμα ότι το πρωτόκολλο επιφέρει μια σημαντική επιβάρυνση στο δίκτυο, ιδιαίτερα λόγω της λειτουργίας του Pathrater και SRR και όχι λόγω του Watchdog, κυρίως εξαιτίας των πακέτων ROUTE REQUEST και ROUTE REPLY που κατακλύζουν το δίκτυο. Η επιβάρυνση αυτή μπορεί να μειωθεί αν μετριαστεί η καθυστέρηση στην μετάδοση ROUTE REQUEST πακέτων από τον Pathrater, και ο αριθμός τους.

Τέλος ελέγχθηκε η λειτουργία του δικτύου σχετικά με την επιρροή στην απόδοση των λανθασμένων αναφορών, εξάγοντας διαγράμματα που συγκρίνουν το δίκτυο για εφαρμογή του Watchdog με δίκτυο χωρίς λανθασμένες αναφορές. Τα παρακάτω διαγράμματα που έχουν στον κάθετο άξονα τους ***το throughput,*** και στον οριζόντιο άξονα ***το ποσοστό των μη ομαλά συμπεριφερόμενων κόμβων***, για ***διάρκεια παύσης κίνησης των κόμβων 0 και 60 δευτερόλεπτα,*** αντίστοιχα με τη σειρά που εμφανίζονται.



Διάρκεια Παύσης Κίνησης 0

Διάγραμμα 2.6.5 (Πηγή [6])



Διάρκεια Παύσης Κίνησης 60

Διάγραμμα 2.6.6 (Πηγή [6])

Από την σύγκριση διαπιστώνεται ότι η απόδοση του δικτύου και το throughput του, δεν επηρεάζονται ιδιαίτερα από την πιθανή λανθασμένη αναφορά μη ομαλής συμπεριφοράς κάποιων κόμβων από το εργαλείο watchdog.

Συμπερασματικά, το πρωτόκολλο Watchdog – Pathrater, αποτελεί έναν μηχανισμό υποστήριξης συνεργασίας στα ad-hoc δίκτυα, που λειτουργεί ως επέκταση στο πρωτόκολλο δρομολόγησης DSR. Βασικές λειτουργίες του είναι ο εντοπισμός των μη ομαλά συμπεριφερόμενων κόμβων που πραγματοποιείται ακούγοντας τις μεταδόσεις των επόμενων κόμβων, και η εξαίρεσή τους από τις διαδρομές δρομολόγησης. Το Watchdog – Pathrater, προσφέρει μια αισθητή βελτίωση στο throughput του δικτύου αλλά και μια σημαντική επιβάρυνση overhead.

2.7 LARS

Το LARS [7] αποτελεί έναν απλό μηχανισμό υποστήριξης συνεργασίας στα ad-hoc δίκτυα, βασισμένο στη φήμη, που έχει ως σκοπό στην μετρίαση της μη ομαλής συμπεριφοράς από τους κόμβους. Το πρωτόκολλο αυτό χρησιμοποιεί μόνο τοπική φήμη, με την έννοια ότι κάθε κόμβος διατηρεί τιμές για την φήμη μόνο των γειτονικών του κόμβων. Το LARS για να μετριάσει τις επιζήμιες συνέπειες που επιφέρουν οι εγωιστικοί και οι κακόβουλοι κόμβοι, όταν αναγνωρίζεται ένας μη συνεργάσιμος κόμβος, οι γειτονικοί κόμβοι που βρίσκονται k βήματα από αυτόν, συνειδητοποιούν την μη ομαλή συμπεριφορά, όπου k μια παράμετρος που προσαρμόζεται ανάλογα με τις απαιτήσεις ασφαλείας του δικτύου. Για την αποφυγή λανθασμένων κατηγοριών, η τιμωρία ενός μη συνεργάσιμου κόμβου, συνυπογράφεται από m διαφορετικούς γειτονικούς κόμβους που βρίσκονται ένα βήμα μακριά, υποθέτοντας ότι m – 1 είναι ένα άνω όριο στον αριθμό των κακόβουλων κόμβων, στο σύνολο των κόμβων που βρίσκονται ένα βήμα μακριά.

2.7.1 ΦΗΜΗ - ΕΜΠΙΣΤΟΣΥΝΗ

Το LARS έχει σκοπό να ενισχύει την συνεργασία των κόμβων σε αυτοοργανούμενα ad-hoc δίκτυα, αντιμετωπίζοντας τους κακόβουλους κόμβους καθώς και τους κόμβους που δεν εκτελούν κάποιες λειτουργίες με σκοπό να κάνουν εξοικονόμηση ενέργειας. Το πρωτόκολλο, χρησιμοποιεί την εμπιστοσύνη μεταξύ των κόμβων. Στο LARS, η εμπιστοσύνη συνδέεται άμεσα με την τιμή της φήμης. Υπάρχουν τρία επίπεδα εμπιστοσύνης που ορίζονται με την **τιμή εμπιστοσύνης T**, για να αναπαραστήσουν την αξιοπιστίας ενός κόμβου. Πιο συγκεκριμένα, ένας κόμβος A θεωρεί έναν άλλο κόμβο B:

- **Αξιόπιστο**, με **T = 1**. Αξιόπιστος κόμβος θεωρείται ένας ομαλά συμπεριφερόμενος κόμβος που μπορεί κανείς να εμπιστευτεί.
- **Αναξιόπιστο**, με **T = -1**. Αναξιόπιστος κόμβος θεωρείται ένας κόμβος με μη ομαλή συμπεριφορά, ο οποίος πρέπει να αποφεύγεται και να στερείται υπηρεσιών.
- **Αβέβαιο όσον αφορά την αξιοπιστία**, με **T = 0**. Αβέβαιος όσον αφορά την αξιοπιστία, θεωρείται ένας κόμβος που συνήθως είναι νέος στο δίκτυο και δεν έχει διαμορφωθεί ακόμα γνώμη για αυτόν, επομένως μπορεί να είναι είτε ομαλά είτε μη ομαλά συμπεριφερόμενος. Η τιμή εμπιστοσύνης που θα ορίσει την αξιοπιστία του, διαμορφώνεται ανάλογα με τις επιδόσεις του στην επικοινωνία του δικτύου από τη στιγμή που θα εισαχθεί σε αυτό.

Κάθε κόμβος διατηρεί ένας πίνακα φήμης, ο οποίος συνδέει μια τιμή φήμης με κάθε γειτονικό του κόμβο. Βασικό στοιχείο στο LARS αποτελεί το γεγονός ότι οι πίνακες φήμης ανανεώνονται βάσει μόνο των άμεσων εξ ιδίων παρατηρήσεων. Δεν χρησιμοποιείται καθολική φήμη όπου κάθε κόμβος διατηρεί τιμή φήμης για κάθε άλλο κόμβο στο δίκτυο, αλλά ούτε και διαδίδονται μηνύματα έμμεσης φήμης από άλλους κόμβους του δικτύου.
Οι **τιμές φήμης R**, κινούνται μέσα σε ένα διάστημα $R_{min} < R < R_{max}$. Για τις τιμές αυτές υπάρχουν δύο κατώφλια έτσι ώστε $R_u > R_{min}$, για αναξιόπιστους κόμβους, και $R_t < R_{max}$, για τους αξιόπιστους. Έτσι, όπως αναφέρθηκε παραπάνω συνδέονται άμεσα οι τιμές εμπιστοσύνης με τις τιμές φήμης κάθε κόμβου N, και διαμορφώνονται με τον εξής τρόπο:

- T = 1(όπου ο N θεωρείται αξιόπιστος), αν $R_t < R < R_{max}$

- T = -1 (όπου ο N θεωρείται αναξιόπιστος), αν $R_{min} < R < R_u$
- T = 0 (όπου είναι αβέβαιη η αξιοπιστία του N), αν $R_u < R < R_t$

Νέοι κόμβοι που μόλις εισήχθησαν στο δίκτυο, παίρνουν τιμές φήμης μεταξύ R_u και R_t, καθώς δεν είναι ακόμα γνωστή η αξιοπιστία τους. Στο LARS, για να γίνεται εφικτό το ξεθώριασμα φήμης με σκοπό να μην μένουν αιώνια κατηγορίες πάνω στους κόμβους, χρησιμοποιείται ένας παράγοντας w ώστε να δίνεται λιγότερη βαρύτητα στις πληροφορίες που λήφθηκαν στο παρελθόν. Το LARS έχει δοκιμαστεί σε δίκτυα όπου τηρούνται υποθέσεις όπως η μοναδική ταυτότητα κάθε κόμβου, τα αμφίδρομα κανάλια, η χρήση πρωτοκόλλων δρομολόγησης όπως το DSR και το AODV.

2.7.2 ΛΕΙΤΟΥΡΓΙΑ

Παρακάτω αναλύεται η λειτουργία του πρωτοκόλλου LARS. Κάθε κόμβος X, διατηρεί μια τιμή φήμης για κάθε γειτονικό κόμβο που απέχει ένα βήμα από τον X κα υπάγεται στη γειτονιά του, η οποία ορίζεται ως N(X) και περιέχει όλους τους γειτονικούς κόμβους που βρίσκονται ένα βήμα μακριά. Οι τιμές φήμες ανανεώνονται βάσει των άμεσων παρατηρήσεων για τους γειτονικούς κόμβους. Εάν η τιμή φήμης ενός γειτονικού κόμβου M, πέσει χαμηλότερα από το κατώφλι R_u, τότε ο M θεωρείται από τον X ως μη ομαλά συμπεριφερόμενος. Ο κόμβος X στη συνέχεια, ειδοποιεί τους γειτονικούς του κόμβους για τη μη ομαλή συμπεριφορά του M, αποστέλλοντας ένα προειδοποιητικό μήνυμα WARNING.
Για να αποφευχθούν οι λανθασμένες κατηγορίες προς κάποιον κόμβο, τα μηνύματα WARNING, πρέπει να συνυπογράφονται από m κόμβους προτού να μεταδοθούν στους κόμβους που βρίσκονται k βήματα μακριά. Κάθε κόμβος που βρίσκεται ένα βήμα μακριά από τον X, μπορεί να υπογράψει με την προϋπόθεση ότι η φήμη του M έχει πέσει κάτω από το κατώφλι R_u, και στους δικούς τους πίνακες φήμης.
Το LARS λειτουργεί ως επέκταση σε πρωτόκολλα δρομολόγησης όπως το AODV και το DSR. Κατά τη διαδικασία της δρομολόγησης είναι πολύ πιθανή η εμφάνιση μη ομαλής συμπεριφοράς. Για την αντιμετώπιση του φαινομένου αυτού, μπορούν να μεταδοθούν πλατιά μηνύματα αίτησης διαδρομής δρομολόγησης στο δίκτυο, ώστε να εξασφαλιστεί η εγκαθίδρυση μονοπατιού μεταξύ ενός ομαλά συμπεριφερόμενου κόμβου πηγής S, και ενός ομαλά συμπεριφερόμενου κόμβου προορισμού D.
Η επικοινωνία διεξάγεται ως εξής:
Έστω ότι ο κόμβος S αποστέλλει ένα μήνυμα στον κόμβο D χρησιμοποιώντας ένα μονοπάτι πολλών βημάτων. Κάθε φορά που ένας ενδιάμεσος κόμβος I, προωθεί το μήνυμα, οι γειτονικοί κόμβοι που βρίσκονται στη γειτονιά N(I), μπορούν να ακούσουν την προώθηση, να κρατήσουν μια καταγραφή του πακέτου και να εκκινήσουν ένα χρονόμετρο. Λόγω συγκρούσεων και άλλων συμπτώσεων, δεν μπορούν όλοι οι κόμβοι που βρίσκονται στην N(I) να ακούσουν την προώθηση.
Εάν το πακέτο φτάσει στον προορισμό D, ο D επιστρέφει ένα μήνυμα επιβεβαίωσης ack, στον κόμβο πηγή S, ακλουθώντας το ανάποδο μονοπάτι. Στην περίπτωση που ο S λάβει την επιβεβαίωση μέσα σε ένα συγκεκριμένο χρονικό διάστημα, η επικοινωνία θεωρείται επιτυχής, ενώ σε αντίθετη περίπτωση, εκκινεί μια διαδικασία εύρεσης «ιχνών» ώστε να αναγνωρίσει κάποιον μη ομαλά συμπεριφερόμενο κόμβο. Ένα ειδικό πακέτο ίχνους αποστέλλεται από τον S, μέσω του ιδίου μονοπατιού. Οι γειτονικοί κόμβοι των κόμβων δια μήκους του μονοπατιού, οι οποίοι έχουν ήδη μια καταγραφή του μηνύματος, συμμετέχουν και αυτοί στη διαδικασία εύρεσης ιχνών. Για κάθε γειτονικό κόμβο, αν ένα πακέτο ίχνους ληφθεί πριν την λήξη του χρονομέτρου που έχει τεθεί, ο κόμβος μεταδίδει ευρέως την καταγραφή που διατηρεί,

και βοηθάει στην εύρεση του μη ομαλά συμπεριφερόμενου κόμβου. Σε αντίθετη περίπτωση η καταγραφή του μηνύματος απορρίπτεται.

2.7.2.1 ΥΠΟΛΟΓΙΣΜΟΣ ΦΗΜΗΣ

Όπως αναφέρθηκε, στο LARS κάθε κόμβος διατηρεί τιμές φήμης, μόνο για τους γειτονικούς του κόμβους που βρίσκονται ένα βήμα μακριά του, οι οποίες ανανεώνονται μόνο μέσω των εξ ιδίων παρατηρήσεων. Δεν χρησιμοποιείται επομένως ανταλλαγή second-hand πληροφορίας. Για το λόγο αυτό, το LARS έχει τα εξής πλεονεκτήματα:

- Οι πληροφορίες φήμης μπορούν να παραχθούν απευθείας από τις εξ ιδίων παρατηρήσεις των κόμβων, από τη στιγμή που οι γειτονικοί κόμβοι βρίσκονται εντός εμβέλειας επικοινωνίας μεταξύ τους. Η τιμή της φήμης είναι ακριβής και υπολογίζεται απλά και γρήγορα χωρίς να χρειάζονται πληροφορίες από άλλους κόμβους πέρα των γειτονικών για την ανανέωσή της.
- Δεν αυξάνεται η κίνηση στο δίκτυο, που θα μπορούσε να προκύψει λόγω μεταφοράς second-hand πληροφοριών.
- Εξοικονομείται αποθηκευτικός χώρος στους κόμβους από τη στιγμή που αυτοί δεν αναγκάζονται να διατηρούν τιμές φήμης για κόμβους πέρα των γειτονικών.

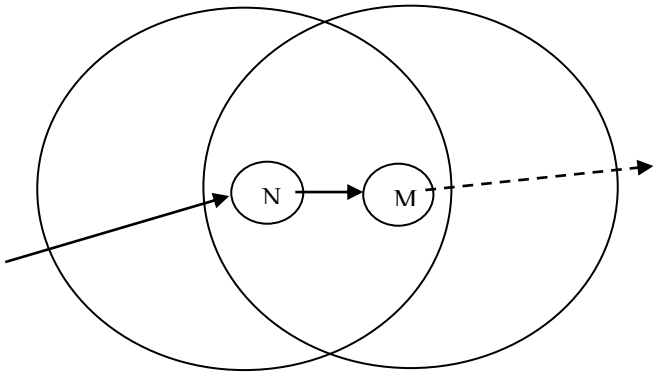
Κάθε φορά που ένας κόμβος συμμετέχει στο πρωτόκολλο του δικτύου, οι γειτονικοί του κόμβοι ανανεώνουν την τιμή φήμης του αναλόγως. Εάν η συμμετοχή του στη διαδικασία της επικοινωνίας κριθεί θετική, η τιμή φήμης του αυξάνεται, ενώ σε αντίθετη περίπτωση μειώνεται. Πιο αναλυτικά προκύπτουν οι εξής περιπτώσεις:

1. Έστω ένας ενδιάμεσος κόμβος I συμπεριφέρεται ομαλά. Κάθε φορά που αυτός προωθεί ένα μήνυμα, οι γειτονικοί του κόμβοι παρατηρούν την ομαλή συμπεριφορά του και αυξάνουν την τιμή φήμης του κατά μ. Μαθηματικά αυτό ορίζεται ως:

$$R_X(I) = R_X(I) + \mu, \mathrm{X} \in \mathrm{N(I)}$$

   Όπου $R_X(I)$, η τιμή φήμης που διατηρεί ο κόμβος X για τον κόμβο I στον πίνακα φήμης του.

2. Έστω ότι ο M είναι ένας κακόβουλος κόμβος και απορρίπτει το μήνυμα του προηγούμενου κόμβου N. Στην περίπτωση αυτή προκύπτουν οι εξής υποπεριπτώσεις:
   - Η περίπτωση, ο N να έχει στείλει το μήνυμα στον M, και ο δεύτερος να έχει αποτύχει να το προωθήσει. Σχηματικά:

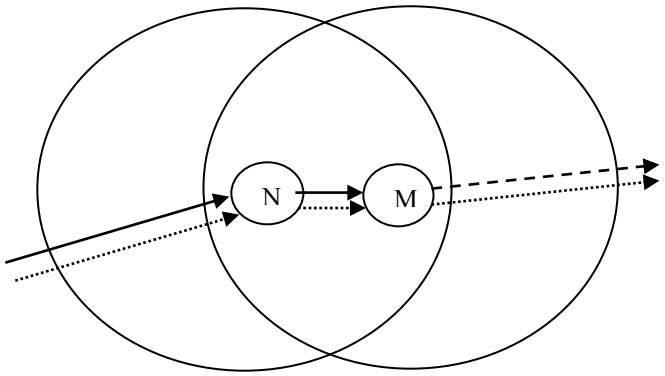


Σχήμα 2.7.1

Όπου οι δύο κύκλοι αναπαριστούν τις γειτονιές των N και M, που περιέχουν τους γειτονικούς τους κόμβους που απέχουν ένα βήμα από αυτούς αντίστοιχα, οι σκούρες γραμμές την προώθηση μηνυμάτων, και η διακεκομμένη γραμμή την μη προώθηση ενός πακέτου είτε αυτό είναι μήνυμα είτε πακέτο ίχνους.
Στην περίπτωση αυτή, για κάθε κόμβο X που βρίσκεται στην τομή των δύο γειτονιών και επομένως απέχει ένα βήμα και από τον N και από τον M, ο X ανιχνεύει την μη ομαλή συμπεριφορά του M και μειώνει την τιμή φήμης του κατά α, όπου α > μ. Μαθηματικά αυτό ορίζεται ως:

$$R_X(\mathrm{M}) = R_X(\mathrm{M}) - \alpha, \mathrm{X} \in \mathrm{N}(\mathrm{M}) \cap \mathrm{N}(\mathrm{N})$$

- Η περίπτωση, ο M να μην έχει προωθήσει το μήνυμα αλλά να έχει προωθήσει το πακέτο ίχνους. Σχηματικά:



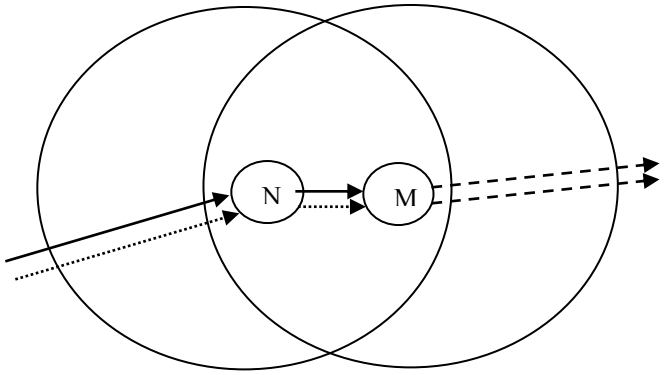
Σχήμα 2.7.2

Όπου η γραμμή με τις τελείες αναπαριστά την προώθηση ενός πακέτου ίχνους.
Στην περίπτωση αυτή, για κάθε κόμβο X που βρίσκεται στην τομή των δύο γειτονιών και επομένως απέχει ένα βήμα και από τον N και από τον M, ο X μειώνει την τιμή φήμης του κατά α. Για κάθε κόμβο X που απέχει ένα βήμα από τον M αλλά όχι και από τον N, ο X αντιλαμβάνεται ότι ο M δεν έχει προωθήσει το μήνυμα όταν λαμβάνει το πακέτο ίχνους, και μειώνει την τιμή φήμης του M κατά α, με

αποτέλεσμα όλοι οι γειτονικοί κόμβοι του Μ να μειώνουν την τιμή φήμης τους κατά α. Μαθηματικά αυτό ορίζεται ως:

$$R_X(\mathrm{M}) = R_X(\mathrm{M}) - \alpha, \mathrm{X} \in \mathrm{N(M)}$$

- Η περίπτωση, ο Μ να μην έχει προωθήσει το μήνυμα, και να έχει απορρίψει επίσης το μήνυμα ίχνους. Σχηματικά:

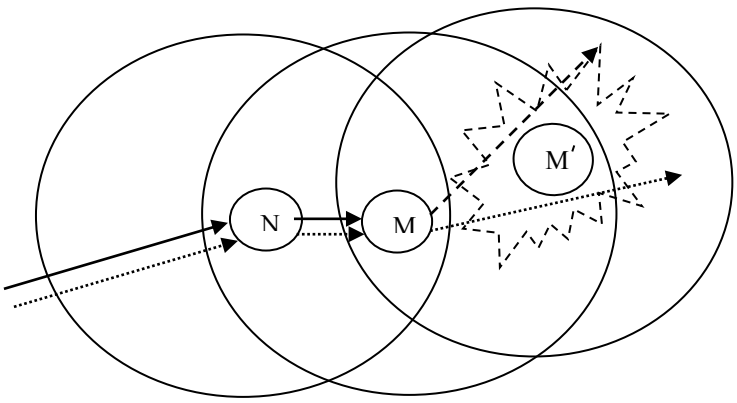


Σχήμα 2.7.3

Στην περίπτωση αυτή, για κάθε κόμβο Χ που βρίσκεται ένα βήμα μακριά από τον Μ, αλλά όχι από τον Ν, ο Χ δεν παρατηρεί την μη ομαλή συμπεριφορά του Μ και δεν ανανεώνει την τιμή φήμης του.
Για κάθε κόμβο Χ πάλι που βρίσκεται στην τομή των δύο γειτονιών και είναι επομένως ένα βήμα μακριά από τον Ν και τον Μ, ο Χ ανιχνεύει ότι το μήνυμα και το πακέτο ίχνους έχουν απορριφθεί, και επομένως μειώνει την τιμή φήμης του Μ κατά β, όπου β > α. Μαθηματικά αυτό ορίζεται ως:

$$R_X(M) = R_X(M) - \beta, X \in N(M) \cap N(N)$$

- Η περίπτωση, ο Μ να έχει προωθήσει το μήνυμα, και ένας γειτονικός του κόμβος, ο Μ΄, να έχει δημιουργήσει συμπαιγνία με τον Μ και να έχει αποστείλει μια πλαστή καταγραφή. Σχηματικά:



Σχήμα 2.7.4

Στην περίπτωση αυτή, για κάθε κόμβο Χ που βρίσκεται ένα βήμα μακριά από τον Μ και από τον Μ΄, ο Χ ανιχνεύει την συμπαιγνία τους και την εξαπάτησή τους, και μειώνει τις τιμές φήμης και των δύο κατά γ, όπου $\gamma < \beta < \alpha$.
Για όλους τους υπόλοιπους γειτονικούς κόμβους που απέχουν ένα βήμα από τον Μ, ισχύει η δεύτερη περίπτωση που αναφέρθηκε και η τιμή του Μ μειώνεται κατά α. Τα παραπάνω ορίζονται μαθηματικά ως:

$$R_X(M) = R_X(M) - \gamma, X \in N(M) \cap N(M')$$
$$R_X(M') = R_X(M') - \gamma, X \in N(M) \cap N(M')$$
$$R_X(M) = R_X(M) - \alpha, X \in N(M) \cap N(M')$$

Τίθεται α > μ, έτσι ώστε η τιμωρία να είναι μεγαλύτερη από την επιβράβευση, ώστε να ενθαρρύνεται η συνεργασία. Έτσι, είναι δύσκολο κάποιος κόμβος να δημιουργήσει μια καλή φήμη και στη συνέχεια να αλλάξει τη συμπεριφορά του σε μη ομαλή, αφού ακόμα κι αν ένας κόμβος αποκτήσει καλή φήμη, σε περίπτωση που συμπεριφερθεί μη ομαλά, η φήμη του θα μειωθεί γρήγορα.
Επίσης, ανάλογα με την περίπτωση, η κάθε μη ομαλή συμπεριφορά αντιμετωπίζεται με διαφορετικό τρόπο. Εάν απορριφθεί μόνο το μήνυμα δεδομένων, μπορεί αυτό να οφείλεται σε ατύχημα ή σύμπτωση. Στην περίπτωση πάλι, απόρριψης από κάποιον κόμβο και του μηνύματος και του πακέτου ίχνους, υποτίθεται ότι η μη ομαλή συμπεριφορά είναι επιτηδευμένη και ο κόμβος τιμωρείται αυστηρότερα. Η μεγαλύτερη τιμωρία από όλες τις περιπτώσεις εφαρμόζεται στην περίπτωση δημιουργίας συμπαιγνίας. Σε όλες τις περιπτώσεις, η τιμή φήμης $R_X(M)$ ανανεώνεται κατά w, όπου w ο παράγοντας ξεθωριάσματος φήμης, μετά από ένα συγκεκριμένο χρονικό διάστημα, ώστε να δίνεται λιγότερη βαρύτητα στις παρελθοντικές εμπειρίες των κόμβων. Μαθηματικά αυτό ορίζεται ως:

$$R_X^{t1+\Delta}(M) = wR_X^{t1}(M)$$

Όπου Δ το χρονικό διάστημα που αναφέρθηκε και $R_X^{t1}(M)$, η τιμή φήμης για τον Μ στον πίνακα φήμης του Χ την χρονική t1.

2.7.2.2 ΑΛΓΟΡΙΘΜΟΣ ΕΥΡΕΣΗΣ ΙΧΝΩΝ

Όπως αναφέρθηκε, αν η πηγή S δεν λάβει επιβεβαίωση από τον κόμβο προορισμό D μέσα σε ένα συγκεκριμένο χρονικό διάστημα, αποστέλλεται ένα πακέτο ίχνους δια μήκους του μονοπατιού και ξεκινά η διαδικασία εύρεσης ιχνών του σφάλματος που προέκυψε. Ο αλγόριθμος εύρεσης ιχνών ιχνηλατεί το λάθος ως τον κόμβο που δημιούργησε το πρόβλημα στην επικοινωνία. Πιο συγκεκριμένα ο αλγόριθμος λειτουργεί ως εξής:
Όταν ένας ενδιάμεσος κόμβος Ι, λάβει το πακέτο ίχνους, το προωθεί. Οι γειτονικοί του κόμβοι, απαντούν με τη καταγραφή που έχουν διατηρήσει, αν ο Ι είχε προωθήσει το μήνυμα. Η καταγραφή αυτή μεταδίδεται πλατιά ώστε όποιος κόμβος έχει λάβει το πακέτο ίχνους, να την λάβει, και να μπορέσει με τη σειρά του να την προωθήσει παραπέρα. Εάν κάποιος κόμβος δεν έχει λάβει το πακέτο ίχνους, αγνοεί την καταγραφή. Με τον τρόπο αυτό, η καταγραφή μεταδίδεται στον κόμβο πηγή, και

μέσω των απαντήσεων που έχει λάβει μπορεί πλέον να αναγνωρίσει τον μη ομαλά συμπεριφερόμενο κόμβο και να επιλέξει μια εναλλακτική διαδρομή δρομολόγησης για να τον αποφύγει. Το παρακάτω παράδειγμα καθιστά κατανοητή την διαδικασία:

- Όταν δεν υπάρχει μη ομαλή συμπεριφορά, ένα μήνυμα προωθείται βήμα-βήμα από τον S στον προορισμό D. Οι γειτονικοί κόμβοι ενός κόμβου κατά μήκους του μονοπατιού, κρατούν καταγραφές των προωθημένων πακέτων και περιμένουν για χρόνο T = 2nτ, όπου n ο αριθμός των βημάτων από τον S στον D, και τ, το άνω όριο του χρόνου που χρειάζεται ένα πακέτο για να κάνει ένα βήμα και να γυρίσει πίσω. Αν μέχρι την λήξη του χρονομέτρου αυτού, δεν έχει ληφθεί κάποιο πακέτο ίχνους, οι κόμβοι διαγράφουν την καταγραφή τους. Εάν ο κόμβος D, λάβει το μήνυμα και επιβεβαιώσει ότι είναι έγκυρο, αποστέλλεται ένα μήνυμα επιβεβαίωσης ack στον κόμβο πηγή S.
  Εάν ο κόμβος D δεν έχει λάβει το μήνυμα, τότε ο κόμβος S δεν λαμβάνει επιβεβαίωση στο χρονικό διάστημα T = 2nτ, και ξεκινά την διαδικασία εύρεσης ιχνών στέλνοντας ένα πακέτο ίχνους από το ίδιο μονοπάτι. Κάθε ενδιάμεσος κόμβος στο μονοπάτι, μόλις λάβει το πακέτο ίχνους, το προωθεί. Αν ένας κόμβος απορρίψει το πακέτο ίχνους, τότε οι γειτονικοί του κόμβοι δεν θα λάβουν το πακέτο ίχνους, με αποτέλεσμα να μην απαντήσουν. Πιο συγκεκριμένα, έστω δύο ενδιάμεσοι κόμβοι N και M, εκ των οποίων ο M είναι κακόβουλος ή εγωιστικός και έχει απορρίψει το μήνυμα. Ο κόμβος N τότε, προωθεί το πακέτο ίχνους στον κόμβο M. Οι γειτονικοί κόμβοι του N που ακούνε το πακέτο ίχνους, προωθούν την καταγραφή που έχουν κρατήσει, επιβεβαιώνοντας ότι ο N προώθησε το πακέτο. Από τη στιγμή που ο M δεν προώθησε το μήνυμα, δεν θα απαντήσουν οι κόμβοι που βρίσκονται στην εγγύτητά του. Έτσι, ο S αντιλαμβάνεται ότι ο τελευταίος κόμβος που προώθησε το πακέτο είναι ο N, και ο επόμενος του, ο M δηλαδή, είναι μη ομαλά συμπεριφερόμενος.

2.7.2.3 ΑΝΤΙΜΕΤΩΠΙΣΗ ΜΗ ΟΜΑΛΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ

Αν η τιμή φήμης ενός κόμβου πέσει κάτω από ένα κατώφλι, R_u, τότε ο κόμβος αυτός θεωρείται μη ομαλά συμπεριφερόμενος και δημιουργείται ένα μήνυμα προειδοποίησης WARNING για αυτόν.
Προτού το μήνυμα WARNING μεταδοθεί στους γειτονικούς κόμβους, όπως αναφέρθηκε, συνυπογράφεται από m κόμβους, όπου m -1 το άνω όριο του αριθμού των κακόβουλων κόμβων στη γειτονιά, εξασφαλίζοντας την αξιοπιστία του μηνύματος και αποφεύγοντας τις λανθασμένες κατηγορίες. Η προϋπόθεση αυτή πρέπει να τηρείται για δύο λόγους:

- Πρώτον, κάθε κόμβος μπορεί να έχει διαφορετική τιμή φήμης για τον ίδιο κόμβο, κάνοντας έτσι έναν κόμβο που θεωρείται από τον κόμβο A ως μη ομαλά συμπεριφερόμενος, να θεωρείται από έναν άλλο κόμβο B ως ομαλά συμπεριφερόμενος. Ο κόμβος καταδικάζεται λοιπόν, μόνο στην περίπτωση που m γειτονικοί του κόμβοι τον θεωρούν μη ομαλά συμπεριφερόμενο.
- Δεύτερον, προϋποθέτοντας ότι χρειάζεται η συνυπογραφή m κόμβων στο μήνυμα WARNING, αποφεύγονται οι λανθασμένες κατηγορίες. Λόγω του περιορισμού που τίθεται στον αριθμό των κακόβουλων κόμβων, εκμηδενίζεται η πιθανότητα δημιουργίας συμπαιγνίας από

κάποιους κόμβους για να πλαστογραφήσουν ένα μήνυμα WARNING με σκοπό να κατηγορήσουν έναν ομαλά συμπεριφερόμενο κόμβο.

Η διαδικασία για την υπογραφή του μηνύματος WARNING έχει ως εξής:
Αξιοποιείται ένα σχήμα κατωφλίου (k,n). Αρχικά ένας μυστικός αριθμός S, χωρίζεται σε n κομμάτια(S_1,…..S_N) έτσι ώστε η γνώση k η περισσότερων κομματιών να καθιστούν εφικτό τον υπολογισμό του S, ενώ η γνώση λιγότερων από k κομματιών να μην είναι επαρκής ώστε να προσδιοριστεί το S. Με βάση αυτά, το LARS χρησιμοποιεί ένα σχήμα κατωφλίου (n, m), όπου n ο αριθμός των γειτονικών κόμβων που απέχουν ένα μόνο βήμα, και m το άνω όριο του αριθμού των κακόβουλων κόμβων στη γειτονιά. Κάθε κόμβος X διατηρεί ένα προσωπικό RSA ζεύγος κλειδιών <SK_X, PK_X>, όπου SK_X είναι το ιδιωτικό μυστικό κλειδί του X και PK_X το δημόσιο κλειδί του X. Το ιδιωτικό κλειδί μοιράζεται σε όλους τους n γειτονικούς κόμβους του X, βάσει ενός τυχαίου πολυωνύμου της τάξης m -1 όπου m – 1, το άνω όριο του αριθμού των κακόβουλων κόμβων στη γειτονιά του X. Το ιδιωτικό αυτό κλειδί βέβαια, δεν είναι ορατό και δεν μπορεί να είναι γνωστό σε οποιονδήποτε κόμβο. Έτσι π.χ. κάθε γειτονικός κόμβος ενός κόμβου M που αντιλαμβάνεται τη μη ομαλή συμπεριφορά του, μπορεί να υπογράψει το μήνυμα WARNING με το SK_M, και να επιβεβαιωθεί με το δημόσιο κλειδί PK_M. Έτσι ένας κόμβος που λαμβάνει ένα μήνυμα WARNING για τον M, από m διαφορετικούς κόμβους, μπορεί να χρησιμοποιήσει τις ψηφιακές υπογραφές τους που έχουν συνάψει στο μήνυμα, ώστε να δημιουργήσει την συνολική υπογραφή.
Μόλις το μήνυμα WARNING επιβεβαιωθεί, μεταδίδεται στους γειτονικούς κόμβους του μη ομαλά συμπεριφερόμενου που απέχουν k βήματα από αυτόν, ώστε να ενημερωθούν για την μη ομαλή συμπεριφορά του, και να του αρνηθούν την παροχή υπηρεσιών.

Στόχος του LARS όμως, δεν είναι ο ισόβιος αποκλεισμός των μη ομαλά συμπεριφερόμενων κόμβων από το δίκτυο, αλλά το να μαθαίνουν από την τιμωρία τους ώστε να βελτιώσουν τη συμπεριφορά τους στο μέλλον. Έτσι, μετά από ένα χρονικό διάστημα, ο μη ομαλά συμπεριφερόμενος κόμβος γίνεται πάλι αποδεκτός από το δίκτυο αλλά με απαράλλαχτη την τιμή φήμης του, ώστε να αναγκάζεται να την βελτιώσει μέσω της συνεργασία του στην επικοινωνία.

2.7.3 ΒΕΛΤΙΣΤΟΠΟΙΗΣΗ

Οι δημιουργοί του LARS, έχουν βελτιστοποιήσει τον μηχανισμό με τους εξής τρόπους:

1. Για την εξοικονόμηση ενέργειας στους γειτονικούς κόμβους σε ένα πυκνό δίκτυο, μόνο k από τους n συνολικά γειτονικούς κόμβους ενός κόμβου, κρατούν καταγραφή του προωθημένου μηνύματος, όπου k ένας τυχαίος αριθμός από 1 μέχρι n. Έτσι, κάθε φορά που προωθείται ένα μήνυμα, επιλέγονται τυχαία k κόμβοι, που αποκαλούνται «ανιχνευτές», για να συμμετέχουν στην διαδικασία ανίχνευσης της προώθησης. Η διαδικασία αυτή προσφέρει δύο βασικά πλεονεκτήματα:
   Πρώτον λόγω της τυχαιότητας στην επιλογή των ανιχνευτών, επιτυγχάνεται η δικαιοσύνη όσον αφορά την συμμετοχή των κόμβων στην ανίχνευση και επομένως στην κατανάλωση χρόνου και ενέργειας. Δεύτερον, εφόσον διαφορετικοί κόμβοι επιλέγονται ως ανιχνευτές κάθε φορά, εκμηδενίζεται η πιθανότητα δημιουργίας συμπαιγνίας από μια μερίδα κόμβων.

Από εκεί και πέρα, οι ανιχνευτές πραγματοποιούν την διαδικασία που αναφέρθηκε παραπάνω – διατηρούν καταγραφή του προωθημένου πακέτου και εκκινούν ένα χρονόμετρο, και αν πριν τη λήξη του λάβουν πακέτο ίχνους, μεταδίδουν την καταγραφή βοηθώντας στην διαδικασία ανίχνευσης του μη ομαλά συμπεριφερόμενου κόμβου, ενώ σε αντίθετη περίπτωση την απορρίπτουν. Η τυχαιότητα της επιλογής των ανιχνευτών, πετυχαίνεται ως εξής: Κάθε φορά που κάποιος γειτονικός κόμβος ακούει την προώθηση ενός μηνύματος, χρησιμοποιεί μια συνάρτηση hash, που παίρνει ως είσοδο την ταυτότητα του κόμβου ID_x, την χρονοσφραγίδα t του μηνύματος, και τον αριθμό ακολουθίας seq του μηνύματος. Εάν η συνάρτηση βγάλει έξοδο 1, ο κόμβος επιλέγεται ως ανιχνευτής, ενώ αν βγάλει αποτέλεσμα 0 απορρίπτει το μήνυμα. Οι δύο αυτές περιπτώσεις ορίζονται αντίστοιχα, μαθηματικά ως:

$$h(seq,t,ID_X)=1 \quad \text{και} \quad h(seq,t,ID_X)=0$$

Όπου h, η συνάρτηση hash.

2. Μειώνεται η χρήση εύρους ζώνης με τον ακόλουθο τρόπο:
   Οι κόμβοι πριν προωθήσουν τις αναδράσεις των γειτονικών κόμβων ανιχνευτών, περιμένουν για ένα χρόνο T = mτ, όπου m ο αριθμός των βημάτων από τον κόμβο στον κόμβο προορισμό, και τ το άνω όριο του χρόνου που χρειάζεται ένα πακέτο για να κάνει ένα βήμα και να γυρίσει πίσω. Μόλις ο χρόνος αυτός λήξει, ο κόμβος προωθεί την τελευταία ανάδραση που μπορεί αν προέρχεται είτε από τον επόμενο κόμβο, είτε από κάποιον άλλο κόμβο στην συνέχεια του μονοπατιού.

2.7.4 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ LARS

Μέχρι στιγμής ο μηχανισμός υποστήριξης συνεργασίας LARS δεν έχει δοκιμαστεί και δεν έχει προσομοιωθεί από τους κατασκευαστές του. Παρόλα αυτά υπάρχει στόχευση, να εξεταστεί η απόδοση του LARS, προσομοιώνοντας το σε ad-hoc δίκτυα, όπου μια μερίδα των κόμβων δεν συνεργάζεται. Στα δίκτυα αυτά, θα υπάρχει κινητικότητα των κόμβων, υποθέτοντας ότι σε περιπτώσεις ομαδικής κίνησης κόμβων, οι κόμβοι που βρίσκονται στην ίδια ομάδα θα συνεργάζονται μεταξύ τους δίχως να τους επιβάλλεται. Στις προσομοιώσεις σκοπεύεται να πραγματοποιηθούν σενάρια βάσει διαφορετικών αριθμών κόμβων, μη συνεργάσιμων κόμβων και κινητικότητας. Οι μετρήσεις που σκοπεύουν οι κατασκευαστές να πραγματοποιήσουν όσον αφορά την απόδοση του LARS που βασίζεται στο DSR θα αφορούν:

- Τον **ρυθμό παράδοσης πακέτων δεδομένων**, που ορίζεται ως ο αριθμός των πακέτων δεδομένων που παραδόθηκαν στους κόμβους προορισμούς προς τον αριθμό των πακέτων δεδομένων που μεταδόθηκαν συνολικά από την πηγή. Ο παράγοντας αυτός, επηρεάζεται άμεσα από την απώλεια πακέτων που μπορεί να προκύψει είτε από γενικές βλάβες του δικτύου, είτε από μη συνεργασία κάποιων κόμβων.
- Την **επιβάρυνση overhead** του πρωτοκόλλου, που ορίζεται ως ο αριθμός των επιπλέον μηνυμάτων που εισάγονται από το LARS, όπως τα πακέτα ίχνους, οι καταγραφές των κόμβων που μεταδίδονται και τα μηνύματα WARNING, προς τον συνολικό αριθμό των μηνυμάτων που μεταδόθηκαν.

- Την **απ' άκρο σ άκρο καθυστέρηση**, που ορίζεται ως ο χρόνος που απαιτείται για την αποστολή ενός πακέτου επιτυχώς από τον κόμβο πηγή στον κόμβο προορισμό.

Οι προσομοιώσεις προορίζονται από τους δημιουργούς να πραγματοποιηθούν με τον προσομοιωτή ασύρματων κινητών ad-hoc δικτύων GloMoSim, και οι συγκρίσεις του LARS ως προς την απόδοση και την αποτελεσματικότητα του θα γίνουν σε σχέση με την λειτουργία ενός δικτύου που χρησιμοποιεί απλά το DSR χωρίς την προσθήκη κάποιου μηχανισμού υποστήριξης συνεργασίας.

2.8 E-HERMES

Το πρωτόκολλο E-Hermes(Extended-Hemes) [8] αποτελεί ένα δυνατό συνεργατικό σχήμα βασισμένο στην εγκαθίδρυση εμπιστοσύνης, που έχει σκοπό την βελτίωση της αξιοπιστίας στην διανομή πακέτων στα κινητά ασύρματα ad-hoc δίκτυα, κυρίως όταν υπάρχουν στο δίκτυο κακόβουλοι κόμβοι. Στο συγκεκριμένο σχήμα, κάθε κόμβος καθορίζει την αξιοπιστία των άλλων κόμβων όσον αφορά την προώθηση πακέτων, συνδυάζοντας την first-hand πληροφορία εμπιστοσύνης που λαμβάνεται ξεχωριστά από τους άλλους κόμβους, και την second-hand πληροφορία εμπιστοσύνης που λαμβάνεται μέσω συστάσεων από άλλους κόμβους. Για τους γειτονικούς κόμβους η first-hand πληροφορία εμπιστοσύνης λαμβάνεται μέσω απευθείας παρατήρησης στο επίπεδο MAC, ενώ για τους μη γειτονικούς κόμβους, λαμβάνεται μέσω επιβεβαιώσεων που αποστέλλονται από αυτούς ως απάντηση σε πακέτα δεδομένων. Το E-Hermes αξιοποιεί την ανταλλαγή πληροφοριών μεταξύ των κόμβων για την επιτάχυνση της σύγκλισης διαδικασιών εγκαθίδρυσης εμπιστοσύνης, αλλά είναι και ισχυρή κατά της διάδοσης λαθεμένων πληροφοριών εμπιστοσύνης από κακόβολους κόμβους.

Το E-Hermes αποτελεί επέκταση του πρωτοκόλλου Hermes. Στο Hermes η εγκαθίδρυση εμπιστοσύνης των μη γειτονικών κόμβων βασίζεται στις second-hand πληροφορίες εμπιστοσύνης, που λαμβάνονται από την διάδοση συστάσεων, πράγμα που κάνει το πρωτόκολλο ευάλωτο σε επιθέσεις κατά τις οποίες κόμβοι διαδίδουν εσφαλμένες πληροφορίες εμπιστοσύνης στο δίκτυο. Στο E-Hermes, τέτοιες επιθέσεις αποφεύγονται, με την επέκταση της έννοιας της first-hand απόδειξης μεταξύ των γειτονικών κόμβων, στους μη γειτονικούς κόμβους, μέσα από τη χρήση ενός ασφαλούς πρωτοκόλλου επιβεβαίωσης.

2.8.1 ΠΕΡΙΓΡΑΦΗ ΤΟΥ HERMES

Για την καλύτερη κατανόηση του E-Hermes, περιγράφεται σύντομα η λειτουργία εγκαθίδρυσης εμπιστοσύνης του Hermes. Στο πρωτόκολλο Hermes, οι first-hand πληροφορίες στην διάδοση πακέτων, είναι ότι μπορεί απευθείας να παρατηρηθεί από τον αποστολέα σε ένα μονοπάτι, ενώ οι second-hand πληροφορίες λαμβάνονται μέσω τρίτων, μέσω συστάσεων. Στο πρωτόκολλο συνδυάζονται οι έννοιες «εμπιστοσύνη» και «σιγουριά» σε μια νέα έννοια – την «αξιοπιστία». Παρακάτω περιγράφεται εν συντομία η λειτουργία εγκαθίδρυσης εμπιστοσύνης του Hermes:
Υποτίθεται ένας δοσμένος κόμβος του οποίου η λειτουργία παρατηρείται με βάση τη συμπεριφορά του όσον αφορά την προώθηση πακέτων. Ως A συμβολίζεται ο συσσωρευτικός αριθμός των πακέτων που προωθήθηκαν σωστά, και ως M, ο συσσωρευτικός αριθμός των πακέτων που εστάλησαν προς προώθηση από τον κόμβο, μέχρι τη συγκεκριμένη χρονική στιγμή. Η τιμή εμπιστοσύνης t με βάση τα παραπάνω ορίζεται ως:

$$t = \frac{A}{M}, \text{ όπου } 0 \le t \le 1$$

Όταν το t παίρνει την τιμή 1, υπάρχει απόλυτη εμπιστοσύνη, ενώ όταν προσεγγίζει το 0, υπάρχει χαμηλή εμπιστοσύνη. Από την άλλη, η τιμή της σιγουριάς, ορίζεται ως:

$$c = 1 - \sqrt{\frac{12A(M-A)}{M^2(M+1)}}\text{, όπου } 0 \le c \le 1$$

Όταν το c παίρνει την τιμή 1, υποδηλώνεται υψηλή σιγουριά όσον αφορά την υπολογισμένη εμπιστοσύνη, ενώ όταν προσεγγίζει το 0, υπάρχει χαμηλή σιγουριά. Η μέτρηση αυτή έχει μεγάλη σημασία, καθώς πρέπει να συλλεχθούν αρκετές πληροφορίες ώστε η εμπειρική τιμή της εμπιστοσύνης να έχει νόημα στατιστικά.
Με βάση τις δύο αυτές μετρήσεις, για κάθε κόμβος διατηρείται ένα ζευγάρι τιμών (t,c). Πιο συγκεκριμένα, ένας κόμβος i ορίζει την εμπιστοσύνη του σε ένα κόμβο j με το ζευγάρι (t_{ij}, c_{ij}). Έτσι για κάθε τέτοιο ζεύγος τιμών, μπορεί να δημιουργηθεί μια μοναδική τιμή αξιοπιστίας η οποία ορίζεται ως:

$$T(t,c) = 1 - \frac{\sqrt{(t-1)^2 + r^2(c-1)^2}}{\sqrt{1+r^2}}$$

, όπου r μια παράμετρος που ορίζει την σχετική σημασία της τιμής t έναντι της τιμής c.
Η προεπιλογή της τιμής της αξιοπιστίας, που αναπαριστά την άγνοια για την αξιοπιστία ενός κόμβου, και αναπαριστά την περίπτωση όπου t=0.5 και c=0.5, ορίζεται ως:

$$T_{def} = T(0.5, 0)$$

Η τιμή αυτή μπορεί να οριστεί ως αρχικό κατώφλι για την αξιοπιστία. Εάν η τιμή ξεπερνιέται από έναν κόμβο, αυτός θεωρείται αξιόπιστος, ενώ αντίθετα θεωρείται αναξιόπιστος.
Ακόμα ορίζεται η τιμή c_{acc}, ως ένα κατώφλι αποδοχής για το επίπεδο της εμπιστοσύνης. Έτσι, ένα ζεύγος τιμών (t, c) γίνεται αποδεκτό, μόνο όταν έχουν συλλεχθεί αρκετές πληροφορίες ώστε $c > c_{acc}$. Ο κάθε κόμβος μπορεί να ορίσει το κατώφλι αυτό με διαφορετική τιμή. Δίνοντας του μεγάλη τιμή, αυξάνει την ακρίβεια αλλά μεγαλώνει αρκετά τον χρόνο σύγκλισης.

2.8.2 ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ E-HERMES

Το E-Hermes αντιμετωπίζει μια βασική αδυναμία του Hermes με το μοντέλο επίθεσης του, αλλά προσφέρει και περισσότερες βελτιώσεις. Ακόμα και όταν το πρωτόκολλο δεν είναι ασφαλές, το E-Hermes μπορεί να μετριάσει τις επιθέσεις δρομολόγησης. Στο πρωτόκολλο Hermes θεωρείται ότι εάν ένας κόμβος προωθεί πακέτα σωστά, τότε θα διαδίδει και τιμές αξιοπιστίας σωστά, κάτι που δεν συμβαίνει πάντα, αφού οι δύο αυτές συμπεριφορές μπορεί να είναι ανεξάρτητες μεταξύ τους. Το E-Hermes επεκτείνει το μοντέλο επίθεσης, ώστε κάθε κόμβος να μπορεί να παρατηρεί αυτές τις κακόβουλες συμπεριφορές ξεχωριστά. Ακόμα, το E-Hermes εισάγει ένα νέο μηχανισμό για την άντληση της αξιοπιστίας μη γειτονικών κόμβων μέσω first-hand πληροφορίας από επιβεβαιώσεις. Συνοπτικά, οι ιδιότητες ασφαλείας που εισάγει το E-Hermes σε σχέση με το Hermes είναι οι εξής:

- Ικανότητα σύλληψης ανεξάρτητα, μη ομαλής συμπεριφοράς κατά την προώθηση πακέτων και κατά την διάδοση εμπιστοσύνης

- Ανθεκτικότητα έναντι κόμβων με κακή συμπεριφορά είτε ως προς την προώθηση πακέτων, είτε ως προς τις συστάσεις τους.
- Ανθεκτικότητα έναντι της τοποθέτησης του επιτιθέμενου κόμβου.

Στο E-Hermes θεωρείται ένα μοντέλο επιτιθέμενου κόμβου, κατά το οποίο ένας κόμβος μπορεί να απορρίψει, να επαναλάβει ή να στείλει σε λάθος διαδρομή δρομολόγησης, πακέτα δεδομένων που θα έπρεπε να προωθήσει σύμφωνα με ένα συγκεκριμένο πρωτόκολλο δρομολόγησης. Ένας κόμβος που διαπράττει τέτοιου είδους επιθέσεις με μια στατιστική συχνότητα ονομάζεται *κακός κόμβος*, ενώ ένας κόμβος που προωθεί σωστά τα πακέτα, *καλός κόμβος*. Κατ' αναλογία, ένας κόμβος που διαδίδει λανθασμένες συστάσεις με μια στατιστική συχνότητα ονομάζεται *κακός συνιστών*, ενώ αν διαδίδει σωστές συστάσεις, *καλός συνιστών*. Πιο συγκεκριμένα, αν οριστεί ως B_f^i την πιθανότητα ένας κόμβος i να προωθήσει λανθασμένα ένα πακέτο, και ως B_t^i την πιθανότητα ένας κόμβος i να διαδόσει λανθασμένα μια σύσταση, θεωρείται ότι ένας κόμβος είναι κακός αν $B_f^i < T_{def}$ (ενώ είναι καλός σε αντίθετη περίπτωση) και ότι ένας κόμβος είναι κακός συνιστών αν $B_t^i < T_{def}$ (ενώ είναι καλός συνιστών σε αντίθετη περίπτωση).
Γίνεται η υπόθεση επίσης, ότι κάθε κόμβος προωθεί πακέτα επιβεβαίωσης ACK και NACK, για πακέτα που έχει προωθήσει νωρίτερα, πράγμα που ισχύει καθώς ο κόμβος δεν έχει κανένα συμφέρον να μην το κάνει.

2.8.2.1 FIRST-HAND ΠΛΗΡΟΦΟΡΙΑ ΕΜΠΙΣΤΟΣΥΝΗΣ

Στο πρωτόκολλο Hermes οι κόμβοι εκτιμούν την αξιοπιστία των γειτονικών τους κόμβων ακούγοντας το κανάλι. Η περίπτωση σφάλματος, όπου ένας κόμβος δεν προωθεί σωστά ένα πακέτο στον επόμενο, μπορεί να δημιουργηθεί λόγω κακόβουλης συμπεριφοράς, αλλά και λόγω μη κακόβουλης συμπεριφοράς, εξαιτίας συμφόρησης του δικτύου, της κίνησης των κόμβων αλλά και κάποιας δυσλειτουργίας των κόμβων. Αν υποτεθεί ένα παράδειγμα διαδρομής δρομολόγησης {x,y,z}, ο κόμβος x διατηρεί μετρητές M_y και A_y, για τον γειτονικό κόμβο y, οι οποίοι ονομάζονται M-μετρητές και A-μετρητές. Ο μετρητής M_y, καταγράφει τον συνολικό αριθμό των πακέτων που στάλθηκαν από τον x στον y προς προώθηση στον κόμβο z πάνω από ένα παράθυρο παρατήρησης. Ο μετρητής A_y, καταγράφει τον συνολικό αριθμό πακέτων που προωθήθηκαν σωστά από τον κόμβο y στον z. Οι δύο αυτοί μετρητές ανανεώνονται ως εξής: Κάθε φορά που ένα πακέτο p προωθείται από τον x στον y, ο μετρητής M_y, αυξάνεται κατά ένα και εκκινεί ένα χρονόμετρο. Το χρονικό διάστημα μέχρι την λήξη του χρονομέτρου ορίζεται με μια τιμή μεγαλύτερη από τον χρόνο που χρειάζεται για να ληφθεί το πακέτο στον προορισμό και να ληφθεί στον αποστολέα η επιβεβαίωση λήψης(round-trip time – RTT), μεταξύ δύο γειτονικών κόμβων στο δίκτυο. Εάν ο κόμβος x ανιχνεύσει στο κανάλι ότι ο y προώθησε ένα αντίγραφο του πακέτου p στον επόμενο κόμβο εντός του χρονικού ορίου, ο μετρητής A_y, αυξάνεται κατά ένα, ενώ σε αντίθετη περίπτωση δεν ανανεώνεται. Στην περίπτωση αυτή, όπου αυξάνεται ο μετρητής M_y, και δεν ανανεώνεται ο μετρητής A_y, λέγεται ότι ο κόμβος x τιμωρεί τον κόμβο y.

Στο πρωτόκολλο E-Hermes χρησιμοποιείται ένα σχήμα επιβεβαίωσης για την εκτίμηση της first-hand πληροφορίας εμπιστοσύνης, όταν το εφαρμοζόμενο πρωτόκολλο δρομολόγησης είναι το DSR. Για τη λειτουργία του, οι κόμβοι πρέπει να

εγκαθιδρύουν εμπιστοσύνη για μη γειτονικούς κόμβους. Στο παράδειγμα του σχήματος που ακολουθεί, όταν ο κόμβος x προωθεί ένα πακέτο p στον κόμβο y_1, εκκινεί ένα χρονόμετρο επιβεβαίωσης με χρονικό διάστημα μέχρι τη λήξη του χρονομέτρου t^{ack}, και ανανεώνει τους M-μετρητές για τους επόμενους ενδιάμεσους κόμβους στη διαδρομή δρομολόγησης ως εξής:

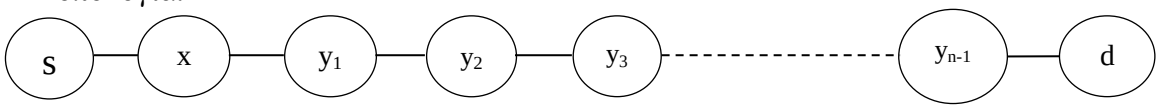
$$M_{y_i} \longleftarrow\!\!\!- M_{y_i} + 1 \text{ , όπου } 1 \le i \le n-1$$

Η τιμή του t^{ack}, πρέπει να είναι μεγαλύτερη από το μέγιστο RTT στο συγκεκριμένο μονοπάτι στο δίκτυο.
Εάν ο κόμβος x λάβει πακέτο επιβεβαίωσης ACK από τον y_1, μέσα στο χρονικό όριο, προωθεί το ACK στον προηγούμενο στη διαδρομή κόμβο και ανανεώνει τους A-μετρητές για όλους τους επόμενους στη στο μονοπάτι ενδιάμεσους κόμβους ως εξής:

$$A_{y_i} \longleftarrow\!\!\!- A_{y_i} + 1, \text{ όπου } 2 \le i \le n-1,$$

πράγμα που σημαίνει ότι όλοι οι επόμενοι κόμβοι έχουν προωθήσει σωστά το πακέτο p. Από τη στιγμή που ο y_1, είναι άμεσα γειτονικός κόμβος του x, ο μετρητής A_{y_1} αυξάνεται κατά ένα, όπως προαναφέρθηκε.

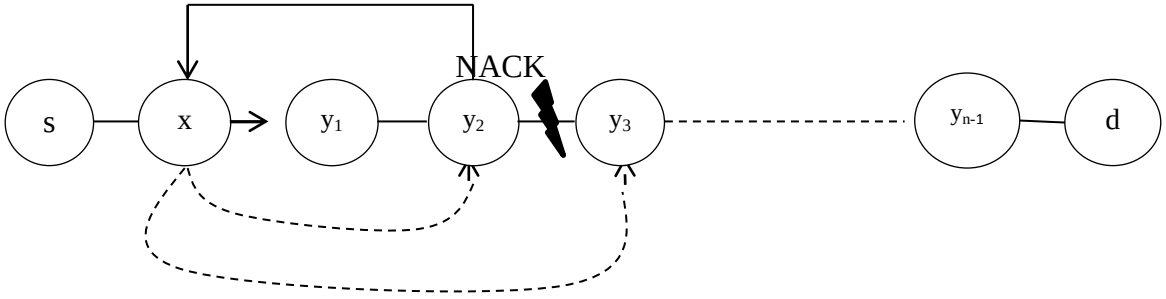
Τοπολογία:



Σχήμα 2.8.1

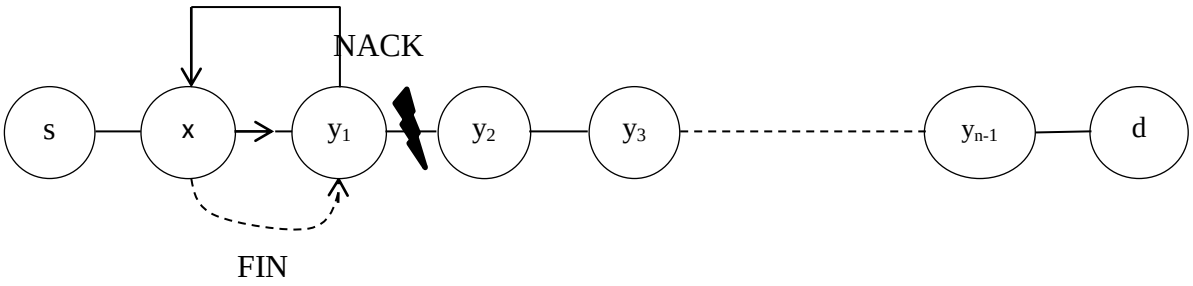
Στην περίπτωση που το πακέτο ACK δεν ληφθεί μέσα στο χρονικό όριο πριν τη λήξη του χρονομέτρου, ο κόμβος δημιουργεί ένα πακέτο αρνητικής επιβεβαίωσης NACK, και το αποστέλλει στον προηγούμενο στο μονοπάτι γειτονικό κόμβο. Η περίπτωση αυτή φαίνεται στα παρακάτω σχήματα, όπου στην πρώτη υποπερίπτωση ο κόμβος x λαμβάνει ένα πακέτο NACK από τον κόμβο y_2, ενώ στη δεύτερη ο κόμβος x λαμβάνει ένα NACK από τον κόμβο y_1.

Περίπτωση 1:



Σχήμα 2.8.2

Περίπτωση 2:



Σχήμα 2.8.3

Στα παραπάνω σχήματα, η μαύρη γραμμή συμβολίζει τη μετάδοση του NACK, ενώ η διακεκομμένη, την τιμωρία από τον κόμβο x στον εκάστοτε κόμβο, που σημείωσε το σφάλμα.

Στην περίπτωση όπου το πακέτο NACK προέρχεται από τον κόμβο y_i, όπου $2 \le i \le n-1$, ο κόμβος υποθέτει ότι το σφάλμα έγινε στην σύνδεση (y_i, y_{i+1}), αλλά δεν μπορεί να διαπιστώσει ποιος από τους δύο κόμβους έπραξε το σφάλμα (κάτι τέτοιο φαίνεται και στο σχήμα της Περίπτωσης 1). Στην περίπτωση αυτή, τιμωρεί και τους δύο κόμβους. Για να αποφευχθεί η τιμωρία των κόμβων που βρίσκονται στο μονοπάτι μετά από τον κόμβο y_{i+1}, οι Μ-μετρητές τους μειώνονται κατά 1 ως εξής:

$$M_{y_j} \longleftarrow\!\!- M_{y_j} - 1, \text{ όπου } \; i+2 \le j \le n-1$$

Αντίθετα, οι κόμβοι από y_1 μέχρι y_{i-1}, παίρνουν πόντους για την σωστή προώθηση, με τους Α-μετρητές τους να αυξάνονται κατά ένα ως εξής:

$$A_{y_j} \longleftarrow\!\!- A_{y_j} + 1, \text{ όπου } 1 \le j \le i-1$$

Στην περίπτωση πάλι που το πακέτο NACK προέρχεται από τον τερματικό κόμβο y_1, εάν ο x είχε ανιχνεύσει προηγουμένως στο επίπεδο MAC, ότι ο y_1 είχε προωθήσει σωστά το πακέτο p, τότε ο x υποθέτει ότι ο κόμβος y_2 απέτυχε να προωθήσει σωστά το πακέτο. Για να αποφευχθεί η τιμωρία των κόμβων που βρίσκονται στο μονοπάτι μετά από τον κόμβο y_2, οι Μ-μετρητές για τους κόμβους από y_3 μέχρι y_{n-1}, μειώνονται κατά 1 ως εξής:

$$M_{y_i} \longleftarrow\!\!- M_{y_i} - 1, \text{ όπου } \; 3 \le i \le n-1$$

Αντίθετα, εάν ο κόμβος x είχε παρατηρήσει στο επίπεδο MAC, ότι ο κόμβος y_1, δεν είχε προωθήσει σωστά το πακέτο p, τότε οι κόμβοι στο μονοπάτι μετά τον y_1, δεν τιμωρούνται, και για το λόγο αυτό ο x μειώνει τους Μ-μετρητές για τους κόμβους αυτούς κατά 1 ως εξής:

$$M_{y_i} \longleftarrow\!\!- M_{y_i} - 1, \text{ όπου } \; 2 \le i \le n-1$$

Και στις δύο περιπτώσεις, ο κόμβος x προωθεί το πακέτο NACK στον προηγούμενο στο μονοπάτι γειτονικό κόμβο.

Με βάση τα παραπάνω, έχοντας τους μετρητές A_y και M_y, για τους γειτονικούς και τους μη γειτονικούς κόμβους με τους οποίους επικοινωνεί ένας κόμβος πηγή, ο αριθμός των πακέτων που προωθήθηκαν λανθασμένα ορίζεται ως εξής:

$$B_y = M_y - A_y$$

Η εμπιστοσύνη και η σιγουριά που αποδίδει ο κόμβος x στον κόμβο y πάνω από ένα παράθυρο παρατήρησης δίνονται από τους παρακάτω τύπους αντίστοιχα, από τους οποίους μπορεί να υπολογισθεί και η τιμή της αξιοπιστίας T_y:

$$t_y = t(A_y, B_y) \quad \text{και} \quad c_y = c(A_y, B_y)$$

2.8.2.2 ΠΙΣΤΟΠΟΙΗΣΗ – ΠΑΚΕΤΑ ΣΤΟ E-HERMES

Η πιστοποίηση των δεδομένων, των συστάσεων, και των πακέτων ACK και NACK, είναι απαραίτητη για την προστασία του δικτύου από επιθέσεις τροποποίησης δεδομένων ή προσποίησης ψεύτικης ταυτότητας από κάποια οντότητα. Στο E-Hermes, χρησιμοποιείται ένα σύστημα πιστοποίησης βασισμένο στις αλυσίδες hash, όπου οι κόμβοι έχουν μεταξύ τους ένα ζεύγος κλειδιών (K, μεταξύ των κόμβων i και j), που διαχειρίζονται από ένα πρωτόκολλο διαχείρισης κλειδιών. Για την κατανόηση της διαδικασίας, θεωρείται μονοπάτι από κόμβο πηγή s σε κόμβο προορισμό d, $R = \{s, a_1, a_2, ..., a_{n-1}, a_n = d\}$ όπου $n \geq 2$, και k ο αριθμός σειράς ενός πακέτου δεδομένων που προωθείται μέσω του συγκεκριμένου μονοπατιού.

Στα πακέτα δεδομένων, το πεδίο πιστοποίησης A ενός πακέτου με πεδίο δεδομένων D, που αποστέλλεται πάνω από το μονοπάτι R, αποτελείται από μια σειρά κωδικών πιστοποίησης μηνύματος (MAC), ως εξής:

$$A = [M_n, M_{n-1}, ..., M_1]$$

Οι MAC ορίζονται ως εξής:

$$M_n = f(K_{s,a_n}, D)$$

Και για i από 1 έως n-1 ως εξής:

$$M_i = f(K_{s,a_i}, [D, M_n, ..., M_{i+1}])$$

όπου f (K, X), η συνάρτηση που παράγει ένα MAC από το κλειδί K και τα δεδομένα X. Το πεδίο πιστοποίησης επιτρέπει σε κάθε ενδιάμεσο κόμβο να πιστοποιήσει το πακέτο, και προστατεύει έναντι κακόβουλων ενδιάμεσων κόμβων που προσπαθούν να αλλάξουν το πεδίο MAC ενός επόμενου στη σειρά κόμβου. Στο E-Hermes, είναι αναγκαίο κάθε κόμβος να πιστοποιεί πακέτα δεδομένων, ώστε να συγκεντρώνει στατιστικά στοιχεία με σκοπό να εξάγει την first-hand πληροφορία εμπιστοσύνης. Τα πακέτα συστάσεων, αποτελούνται μόνο από ένα MAC, που υπολογίζεται από ένα διαμοιραζόμενο κλειδί μεταξύ του συνιστώντος κόμβου και της πηγής ενός πακέτου αίτησης σύστασης.

Ακόμα, τα πεδία πιστοποίησης των πακέτων ελέγχου ACK και NACK, αποτελούνται από μια συνάρτηση hash, και αλυσίδες hash μήκους ίσου με τρία., που χρησιμοποιούνται για την πιστοποίηση ενός πακέτου k για έναν ενδιάμεσο κόμβο α_i που ταξιδεύει μέσω μιας διαδρομής δρομολόγησης R. Για τον κόμβο α_i, όπου i από 1 έως n, το αρχικό στοιχείο της αλυσίδας hash για το πακέτο ACK, που υπολογίζεται από το κλειδί $K_s^{a_i}$, τον σειριακό αριθμό k του πακέτου, και το στοιχείο 0, είναι το $a_i^0(k)$. Τα υπόλοιπα δύο στοιχεία στην αλυσίδα είναι τα εξής:

$$a_i^1(k) = h[a_i^0(k)] \quad \text{και} \quad a_i^2(k) = h[a_i^1(k)].$$

Ως επέκταση στο Hermes, στο E-Hermes, για την πιστοποίηση για το εάν ένα πακέτο είναι ACK ή NACK, ορίζεται μία αλυσίδα hash τριών στοιχείων, για την πιστοποίηση των πακέτων NACK. Αντίστοιχα με το ACK, τα στοιχεία της συγκεκριμένης αλυσίδας είναι κατά σειρά τα:

$$\eta_i^0(k), \ \eta_i^1(k) = h[\eta_i^0(k)] \text{ και } \eta_i^2(k) = h[\eta_i^1(k)].$$

Κάθε φορά που ένας κόμβος s μεταδίδει ένα πακέτο δεδομένων k διαμέσου του μονοπατιού R, συνενώνει τα τρίτα στοιχεία των αλυσίδων ACK και NACK, που συνδέονται με τους ενδιάμεσους κόμβους. Έτσι, καθώς το πακέτο προωθείται μέσω του μονοπατιού, κάθε ενδιάμεσος κόμβος εξάγει και αποθηκεύει τα στοιχεία των αλυσίδων hash που συνδέονται με τους επόμενους σε σειρά κόμβους. Με την επέκταση αυτή, αποτρέπεται η επίθεση κατά την οποία ένας κόμβος μπορεί να δημιουργήσει ψευδώς ένα NACK με σκοπό να τιμωρηθούν οι επόμενοι στη σειρά κόμβοι, αφού πλέον δεν χρησιμοποιείται μια αλυσίδα hash και για τα ACK και για τα NACK πακέτα.

2.8.2.3 SECOND-HAND ΠΛΗΡΟΦΟΡΙΑ ΑΞΙΟΠΙΣΤΙΑΣ

Σε περιπτώσεις κόμβων με χαμηλές τιμές εμπιστοσύνης, κατά τη διαδικασία δρομολόγησης ή άλλων διαδικασιών στο δίκτυο, απαιτείται η αξιοποίηση της second-hand πληροφορίας αξιοπιστίας από τρίτους. Η μετάδοση της πληροφορίας αξιοπιστίας για τη διαμόρφωση απόψεων από έναν κόμβο, πραγματοποιείται μέσα από τις συστάσεις. Η σύσταση ενός συνιστώντος κόμβου j για ένα κόμβο m, ορίζεται ως $T_{j,m}$.

Ένας κόμβος i αναζητά συστάσεις για έναν κόμβο m, όταν η τιμή εμπιστοσύνης που έχει υπολογίσει για αυτόν, δεν ξεπερνά την τιμή c_{acc}. Ο i επιλέγει ανάμεσα σε πολλούς συνιστώντες κόμβους, με τη βοήθεια μιας μέτρησης, της *αξιοπιστίας σινιστώντος κόμβου*. Η τιμή αυτή που διατηρεί ένας κόμβος i για ένα κόμβο j, ορίζεται ως $T_{i,j}^R$, και δείχνει πόσο αξιόπιστα, ένας κόμβος μεταδίδει πληροφορίες αξιοπιστίας.

Ένας κόμβος j χαρακτηρίζεται από έναν κόμβο i ως:

1. ***Καλός συνιστών***, αν $T_{i,j}^R > T_{def}$

2. ***Κακός συνιστών***, αν $T_{i,j}^{R} < T_{def}$

Ένας κόμβος i μπορεί να ζητήσει από ένα σύνολο κόμβων D συστάσεις, για έναν κόμβο m. Το D (που έχει περιορισμένο μέγεθος d, για ον περιορισμό του overhead), επιλέγεται μεταξύ όλων των κόμβων του δικτύου με σειρά προτεραιότητας που έχει ως εξής:

1. Καλοί συνιστώντες κόμβοι
2. Κόμβοι για τους οποίους η τιμή εμπιστοσύνης του συνιστώντος c^{R}, είναι μικρότερη από την τιμή c_{acc}
3. Όλοι οι υπόλοιποι κακοί συνιστώντες κόμβοι, οι οποίοι επιλέγονται με σκοπό να ανανεωθεί η τιμή αξιοπιστίας τους.

Κατά τη διαδικασία αναζήτησης συστάσεων, ο κόμβος i θα λάβει το πολύ $f \le d$ συστάσεις, και δε θα λάβει σύσταση από έναν κόμβο j όταν η τιμή εμπιστοσύνης που έχει αυτός για έναν κόμβο m, είναι μικρότερη από c_{acc}. Οι συστάσεις πιστοποιούνται κι αυτές με χρήση MAC.

Μόλις ο κόμβος i λάβει ένα σετ $R_m = \{T_{j,m} : j \in D\}$ συστάσεων για τον κόμβο m, ακολουθεί τα εξής βήματα:

1. Αν η τιμή εμπιστοσύνης $c_{i,m}$, είναι μικρότερη από την c_{acc}, υπολογίζει μια προσωρινή τιμή αξιοπιστίας $\tilde{T}_{i,m}$, που θεωρείται ως η μεγαλύτερη τιμή αξιοπιστίας $T_{j,m}$, μεταξύ των συνιστούντων κόμβων. Η τιμή αυτή χρησιμοποιείται για δρομολόγηση ή άλλες αποφάσεις που αφορούν το δίκτυο, μέχρι η τιμή $c_{i,m}$, μέσω ανανέωσης να ξεπεράσει την c_{acc}.
2. Όταν η τιμή εμπιστοσύνης $c_{i,m}$, είναι μεγαλύτερη από την c_{acc}, μπορεί να εκτιμηθεί η αξιοπιστία των συνιστούντων κόμβων j, μέσω του λεγόμενου RC-τεστ που φαίνεται παρακάτω:

   $RC-test : |T_{i,m} - T_{j,m}| \le \eta$, όπου $\eta \in (0,1)$ μια τιμή κατωφλίου.

   Το τεστ θεωρείται επιτυχές, όταν η τιμή συνιστούμενης αξιοπιστίας είναι κοντά στην τιμή της first-hand αξιοπιστίας, όπως ορίζεται από το κατώφλι. Σε αντίθετη περίπτωση το τεστ δεν είναι επιτυχές. Η έξοδος που δίνει το τεστ για τον συνιστώντα κόμβο j, χρησιμοποιείται για την ανανέωση των μετρητών A^{R} και M^{R}, όπου A^{R} ο αριθμός των φορών που το τεστ επιτυγχάνει και M^{R}, ο συνολικός αριθμός των φορών που το τεστ εκτελείται. Με τη σειρά τους οι μετρητές αυτοί χρησιμοποιούνται για τον υπολογισμό της αξιοπιστίας συνιστώντος $T_{i,j}^{R}$.

Η έννοια της αξιοπιστίας γενικεύεται στην έννοια της ***γνώμης***, η οποία όρίζεται ως $P_{i,m}$, όταν την κατέχει ένας κόμβος i για ένα κόμβο m. Γενικότερα, μαθηματικώς ορίζεται ως:

$$P_{i,m} = \max_{j \in \Gamma} \{\omega_{i,j} T_{j,m}\} \quad \text{για} \quad P_{j,m} \neq T_{def}$$

όπου $\omega_{i,j} = \begin{cases} T_{i,j}^{R}, & i \neq j \\ 1, & i = j \end{cases}$ και Γ το σετ των συνιστούντων κόμβων που πέρασαν το RC-τεστ.

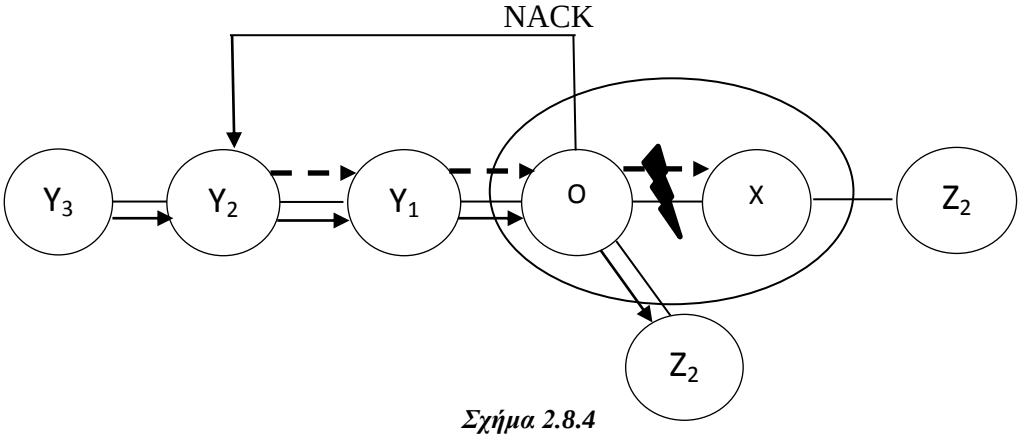
Σύμφωνα με τα παραπάνω και γενικεύοντας, ένας κόμβος j θεωρείται από έναν κόμβο i ως:

- ***Καλός***, όταν $P_{i,j} > T_{def}$
- ***Κακός***, όταν $P_{i,j} < T_{def}$

2.8.2.4 ΑΝΤΙΜΕΤΩΠΙΣΗ ΕΠΙΘΕΣΕΩΝ

Το πρωτόκολλο E-Hermes καταφέρνει να τιμωρήσει και τους κακούς κόμβους, και τους κακούς συνιστώντες. Ακόμη, η πολυμορφία στη δρομολόγηση, διασφαλίζει ότι ένας καλός κόμβος, μπορεί να θεωρηθεί κακός, μόνο με μια μικρή πιθανότητα. Το E-Hermes προσφέρει προστασία έναντι των εξής επιθέσεων:

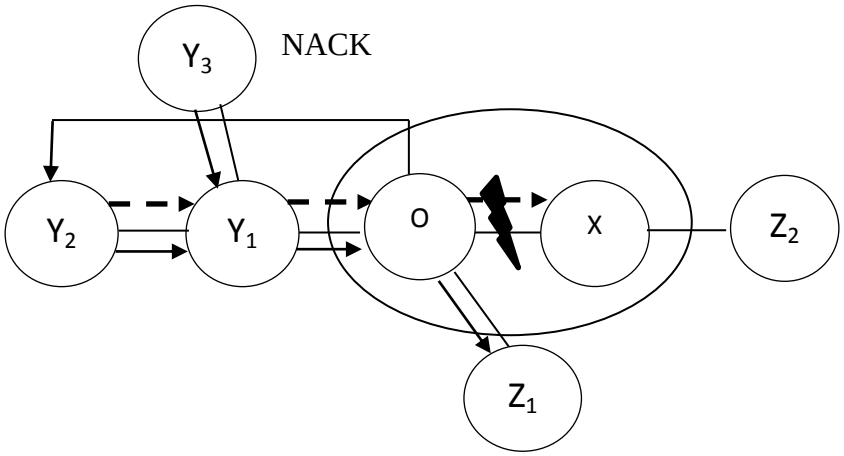
- **Επίθεση από κακούς κόμβους**. Όπως φαίνεται στο παρακάτω σχήμα, ο κόμβος X προωθεί λανθασμένα, πακέτα δεδομένων με μια πιθανότητα από 0 έως 1. Ο κόμβος γειτονικός κόμβος *O* αποκτά first-hand πληροφορίες, σχετικά με τη συμπεριφορά του X στη δρομολόγηση πακέτων. Οι προηγούμενοι στη στο μονοπάτι, κόμβοι του κόμβου O, συνάγουν first-hand πληροφορίες εμπιστοσύνης από τα πακέτα NACK που δημιουργεί ο O. Από τη στιγμή που ο κόμβος Y_1, είναι γειτονικός του O, αντιλαμβάνεται ότι αυτός προωθεί σωστά, και για το λόγο αυτό όταν λάβει το NACK τιμωρεί τον X. Αντίθετα ο κόμβος Y_2, που δεν είναι γειτονικός, μόλις λάβει το NACK που δημιούργησε ο O, θα τιμωρήσει και τον O και τον X. Καθώς το E-Hermes τιμωρεί και τα δύο άκρα μιας ζεύξης στην οποία παρουσιάζεται μη ομαλή συμπεριφορά, δεν συμφέρει κάποιον κόμβο να απορρίπτει πακέτα και να παράγει NACK για να κατηγορηθεί και να τιμωρηθεί ο επόμενος σε σειρά κόμβος.



Σχήμα 2.8.4

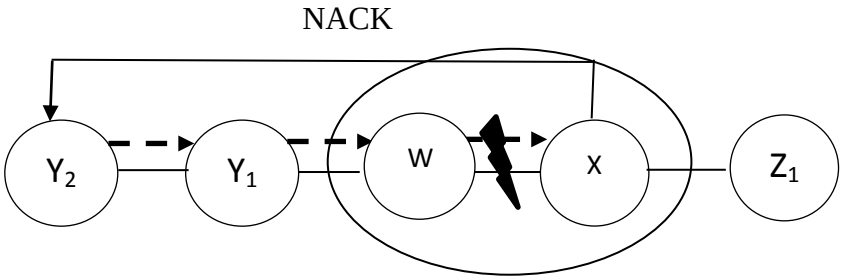
- **Επίθεση από κακούς συνιστώντες**. Όπως αναφέρθηκε παραπάνω, στο E-Hermes, με τη βοήθεια του RC-τεστ μπορούν να αναγνωριστούν οι κακοί συνιστώντες. Ακόμα και στην περίπτωση όπου ένας κόμβος κατηγορείται λανθασμένα ως κακός συνιστών, δεν επηρεάζεται η διαδικασία εγκαθίδρυσης εμπιστοσύνης, αφού οι κακές συστάσεις απορρίπτονται. Όπως φαίνεται στο παρακάτω σχήμα, ο κόμβος Y_2, εγκαθιδρύει τη διαδρομή δρομολόγησης $R_1 = \{Y_2, Y_1, O, X, Z_2, ...\}$. Ο κόμβος X προωθεί λανθασμένα πακέτα με πιθανότητα από 0 έως 1, και ο προηγούμενος στη σειρά κόμβος O, δημιουργεί πακέτα NACK, για τα πακέτα που δεν επιβεβαιώνονται από τον X. Στην περίπτωση αυτή, ο κόμβος Y_2, θα τιμωρήσει και τους δύο αυτούς κόμβους.. Στην περίπτωση που ο κόμβος Y_3, εγκαθιδρύει τη διαδρομή δρομολόγησης

$R_2 = \{Y_3, Y_1, O, Z_1, ...\}$, ο κόμβος Y_3, θεωρεί τον Ο ως καλό κόμβο. Εάν σε αυτή τη φάση, οι κόμβοι Y_2 και Y_3, ανταλλάξουν συστάσεις για τον κόμβο Ο, θα θεωρηθούν αναμεταξύ τους ως κακοί συνιστώντες, αλλά αυτό δεν θα επηρεάσει τις διαδικασίες εγκαθίδρυσης εμπιστοσύνης τους. Επίσης, αν ο κόμβος Y_2, συλλέξει περισσότερες παρατηρήσεις για τον Ο από διαδρομές που δεν εμπεριέχουν τον Χ, θα υπολογίσει για τον Ο υψηλή τιμή αξιοπιστίας.



Σχήμα 2.8.5

- **Επίθεση από συμπαιγνία μεταξύ κακού κόμβου και κακού συνιστώντος.** Στο παρακάτω σχήμα ο κόμβος Y_2, εγκαθιδρύει τη διαδρομή δρομολόγησης $R = \{Y_2, Y_1, W, X, Z_1, ...\}$. Παράλληλα, ο κόμβος Χ προωθεί λανθασμένα, πακέτα δεδομένων, και ο W μεταδίδει υπερβολικά υψηλές τιμές αξιοπιστίας για τον Χ, προσπαθώντας να πείσει τους προηγούμενους στο μονοπάτι κόμβους ότι ο κόμβος Χ είναι καλός κόμβος. Στην περίπτωση αυτή, ο κόμβος W δεν πρόκειται να δημιουργήσει και να μεταδώσει NACK για τα πακέτα που λανθασμένα προωθεί ο Χ, αφού έτσι θα προκαλούσε και την δική του τιμωρία. Έτσι, ο Χ στέλνει NACK ο ίδιος ενώ συνεχίζει να απορρίπτει και να προωθεί λανθασμένα πακέτα, με αποτέλεσμα να τιμωρηθεί ορθά, από τους προηγούμενους στο μονοπάτι κόμβους.



Σχήμα 2.8.6

- **Επίθεση σκουληκότρυπας**. Στην περίπτωση που δύο κόμβοι Χ και Υ δημιουργήσουν μια «σκουληκότρυπα», συνδεδεμένοι μέσω μιας ενσύρματης ή ασύρματης ζεύξης, μπορούν να αποτελέσουν μέρος μιας διαδρομής

δρομολόγησης, αν και δεν είναι γειτονικοί. Το σύστημα επιβεβαιώσεων του E-Hermes θα τιμωρήσει και τους δύο αυτούς κόμβους, εάν αυτοί δεν προωθούν σωστά τα πακέτα μέσω της σκουληκότρυπας.

- **Επίθεση προσποίησης ταυτότητας**. Εάν ένας κόμβος X προσποιείται έναν κόμβο Z, εάν αυτός απορρίψει πακέτα στη συγκεκριμένη διαδρομή δρομολόγησης, τότε ο Z θα τιμωρηθεί, με αποτέλεσμα να τιμωρηθεί και ο X που τον προσποιείται.
- **Επίθεση από κόμβο με κατευθυντική κεραία.** Εάν ένας κόμβος Y διαθέτει κατευθυντική κεραία και προωθεί πακέτα προς την κατεύθυνση του κόμβου X, ο δεύτερος θεωρεί λανθασμένα ότι ο Y προωθεί σωστά, πράγμα που δεν ισχύει αφού ο Y δεν προωθεί ουσιαστικά τα πακέτα στον επόμενο κόμβο στη διαδρομή δρομολόγησης. Ο κόμβος Y μπορεί να προσπαθήσει να εξαπατήσει τον X, είτε στέλνοντας ένα ACK, είτε δημιουργώντας και στέλνοντας του ένα NACK, είτε στέλνοντας του τίποτα από τα δύο. Η πρώτη περίπτωση αντιμετωπίζεται από το E-Hermes μέσω της αλυσίδας hash, στη δεύτερη θα τιμωρηθεί ο Y και ο επόμενος στη διαδρομή κόμβος, και στην τρίτη θα συμβεί το ίδιο καθώς θα λήξει το χρονόμετρο επιβεβαίωσης του X με αποτέλεσμα να τους τιμωρήσει.

2.8.3 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ E-HERMES

Για την πραγματοποίηση των απαραίτητων προσομοιώσεων οι δημιουργοί του E-Hermes, χρησιμοποίησαν το πρόγραμμα MATLAB, και πραγματοποίησαν πειράματα με ποικίλα δίκτυα και επιθέσεις. Το περιβάλλον προσομοίωσης διαμορφώθηκε ως εξής:

- Ορισμένο αριθμό ροών για κάθε προσομοίωση.
- Οι διαδρομές δρομολόγησης είναι τυχαίες.
- Οι ροές δεδομένων διαμορφώθηκαν συναρτήσει του αριθμού των κόμβων, του ελάχιστου και του μέγιστου αριθμού κόμβων σε μια διαδρομή.
- Οι κακοί κόμβοι μπορεί να είναι γειτονικοί ή μη.
- Κατώφλι του RC-τεστ 0.1.

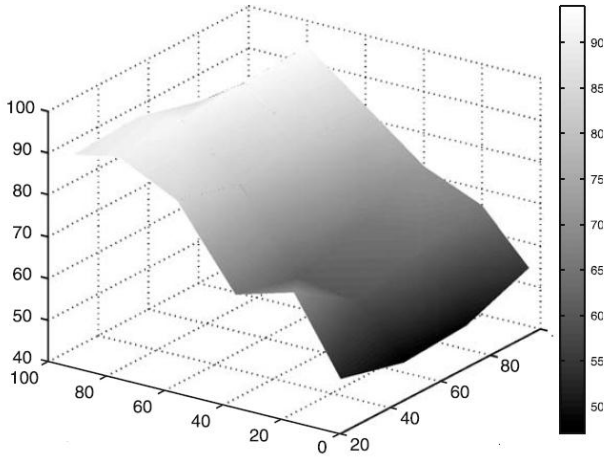
Οι κατασκευαστές του πρωτοκόλλου πραγματοποίησαν προσομοιώσεις που διέφεραν ως προς το ποσοστό σωστής προώθησης πακέτων από τους κόμβους. Έγινε ακόμα διάκριση μεταξύ των κόμβων σε τύπους, και διαφορετική παρουσία των τύπων αυτών σε κάθε σενάριο. Συγκεκριμένα, οι κόμβοι χωρίστηκαν στους εξής τύπους:

- Καλοί κόμβοι και καλοί συνιστώντες
- Κακοί κόμβοι και καλοί συνιστώντες
- Καλοί κόμβοι και κακοί συνιστώντες
- Κακοί κόμβοι και κακοί συνιστώντες

Ακόμα, τα σενάρια που προσομοιώθηκαν διέφεραν ως προς τη συμπεριφορά των κόμβων, αν θα είναι στατική ή δυναμική, ως προς τον αριθμό των κόμβων, τον χρόνο προσομοίωσης, ως προς το ποσοστό σωστής προώθησης πακέτων.
Από τις προσημειώσεις, προέκυψαν τα εξής συμπεράσματα:

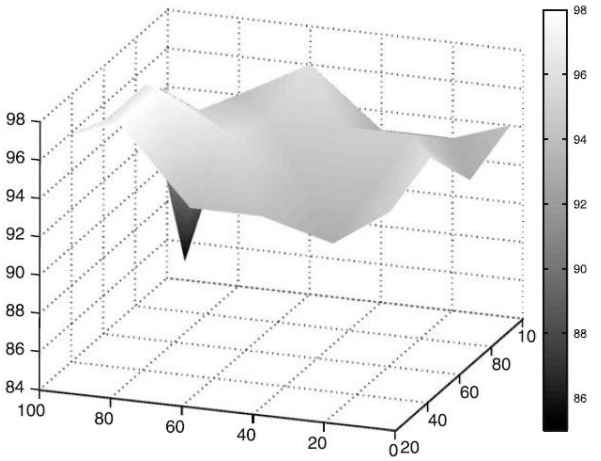
1. Μέσω του E-Hermes οι κακοί κόμβοι αναγνωρίζονται, όπως και οι καλοί, με μόνο πρόβλημα την πιθανά λανθασμένη θεώρηση για τη συμπεριφορά ενός κόμβου λόγω της τιμωρίας και των δύο άκρων μιας ζεύξης με σφάλμα.
2. Μέσω των συστάσεων οι κόμβοι έχουν σωστή άποψη φια το δίκτυο, πολύ πιο γρήγορα.

3. Μέσω του πρωτοκόλλου, γίνεται ακριβής εκτίμηση της εμπιστοσύνης και πραγματοποιούνται οι κατάλληλες αλλαγές στη συμπεριφορά των κόμβων.
4. Ο ρυθμός σύγκλισης εξαρτάται από το ποσοστό των μη ομαλά συμπεριφερόμενων κόμβων – όσο περισσότεροι είναι, τόσο πιο αργά το E-Hermes φτάνει σε μια σταθερή κατάσταση. Κάτι τέτοιο φαίνεται και από το παρακάτω διάγραμμα που στον κάθετο άξονα του έχει ***τη διάρκεια του χρονικού παραθύρου παρατήρησης***, στον οριζόντιο ***το ποσοστό των μη ομαλά συμπεριφερόμενων κόμβων*** και στον άξονα z την ***πραγματική συμπεριφορά των κόμβων*** (που δεν επηρεάζει ιδιαίτερα τη σύγκλιση).



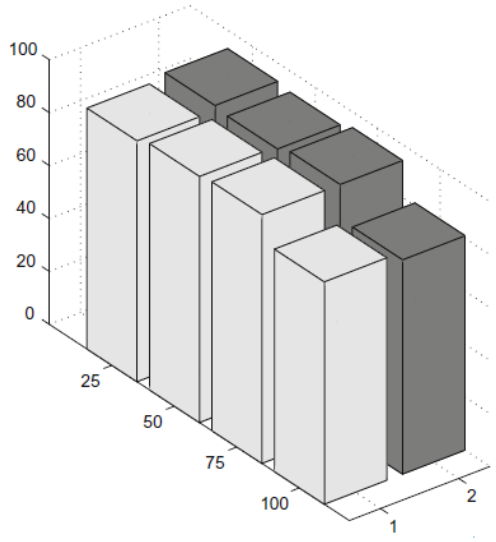
Διάγραμμα 2.8.1 (Πηγή [8])

5. Σε σταθερή κατάσταση, το E-Hermes ανιχνεύει τους μη ομαλά συμπεριφερόμενους κόμβους, σε ποσοστό 93-98%. Αυτό φαίνεται και από το παρακάτω εξαχθέν διάγραμμα που έχει στον κάθετο άξονα το ***ποσοστό αναγνώρισης μη ομαλής συμπεριφερόμενης συμπεριφοράς***, στον οριζόντιο άξονα ***το ποσοστό των μη ομαλά συμπεριφερόμενων κόμβων*** και στον άξονα z την ***πραγματική συμπεριφορά των κόμβων.***



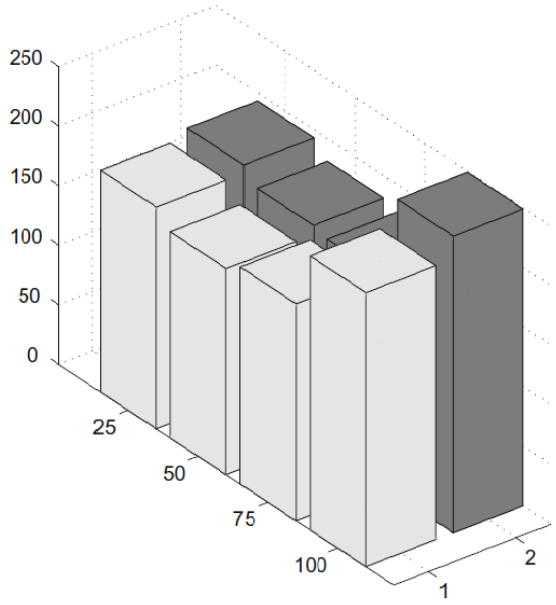
Διάγραμμα 2.8.2 (Πηγή [8])

6. Η ανταλλαγή κακών συστάσεων δεν επηρεάζει την απόδοση του πρωτοκόλλου,. Το συμπέρασμα αυτό εξάγεται από το παρακάτω διάγραμμα που έχει στον κάθετο άξονα το ***ποσοστό αναγνώρισης μη ομαλής συμπεριφερόμενης συμπεριφοράς***, στον οριζόντιο την ***πραγματική συμπεριφορά των κόμβων*** και στον άξονα z ***την περίπτωση όλοι οι κόμβοι να είναι κακοί συνισώντες (αχνό χρώμα) και την περίπτωση να μην ανταλλάσσονται καθόλου συστάσεις στο δίκτυο (σκούρο χρώμα).***



Διάγραμμα 2.8.3 (Πηγή [8])

7. Η δυνατότητα για ανταλλαγή καλών συστάσεων, επιταχύνει τη σύγκλιση των διαδικασιών εγκαθίδρυσης εμπιστοσύνης. Κάτι τέτοιο διαπιστώνεται από το παρακάτω διάγραμμα που έχει στον κάθετο άξονα ***τη διάρκεια του χρονικού παραθύρου παρατήρησης***, στον οριζόντιο την ***πραγματική συμπεριφορά των κόμβων*** και στον άξονα z ***την περίπτωση όλοι οι κόμβοι να είναι κακοί συνισώντες (αχνό χρώμα) και την περίπτωση να μην ανταλλάσσονται καθόλου συστάσεις στο δίκτυο (σκούρο χρώμα).*** Με άλλα λόγια, ακόμα και στην χειρότερη περίπτωση, όπου όλοι οι κόμβοι είναι κακοί συνιστώντες, ο χρόνος που απαιτείται για να φτάσει σε σταθερή κατάσταση δεν είναι διαφέρει ιδιαίτερα από την περίπτωση μη ύπαρξης συστάσεων.



Διάγραμμα 2.8.4 (Πηγή [8])

Συμπερασματικά, το E-Hermes αποτελεί έναν μηχανισμό εγκαθίδρυσης εμπιστοσύνης σε ασύρματα ad-hoc δίκτυα, που βελτιώνει την αξιοπιστία στην προώθηση των πακέτων. Στο σχήμα αυτό χρησιμοποιείται και η first-hand και η second-hand πληροφορία και γίνεται εκτίμηση της αξιοπιστίας των συνιστώντων κόμβων και των συστάσεων. Πραγματοποιεί επίσης συνδυασμό των δύο τύπων πληροφοριών, και εισάγει την έννοια της γνώμης, για την συμπεριφορά των κόμβων σχετικά με την προώθηση. Το E-Hermes επιτυχημένα πετυχαίνει την τιμωρία των ύποπτων κόμβων. Οι κατασκευαστές στοχεύουν να επεκτείνουν ακόμη περαιτέρω το σχήμα, για να μπορέσουν να αντιμετωπίσουν καταστάσεις κατά τις οποίες ένας κόμβος προωθεί σωστά σε συγκεκριμένες ροές, και λανθασμένα σε άλλες.

2.9 LRM

Το LRM [9] αποτελεί έναν απλό και αποτελεσματικό μηχανισμό τοπικής φήμης, ο οποίος μπορεί να χρησιμοποιηθεί στα ασύρματα ad-hoc δίκτυα, και σύμφωνα με τους δημιουργούς του, να υποστηρίξει τη συνεργασία μεταξύ των κόμβων και να μετριάσει την εγωιστική συμπεριφορά τους. Το LRM χρησιμοποιεί μόνο την τοπική πληροφορία για να παράγει την φήμη των κόμβων, καθιστώντας δυνατή την επιστροφή στο δίκτυο, κόμβων που έχει ανιχνευθεί ότι λειτουργούν εσφαλμένα.

2.9.1 ΛΕΙΤΟΥΡΓΙΑ

Η βασική διαφορά του LRM από άλλους γνωστούς και διαδεδομένους μηχανισμούς υποστήριξης συνεργασίας, είναι ότι απαγορεύεται ανταλλαγή πληροφορίας πέραν της τοπικής. Σύμφωνα με το πρωτόκολλο, η φήμη ενός κόμβου πέφτει εάν αυτός απορρίψει πακέτα δεδομένων, και θεωρείται εγωιστικός εάν η τιμή της φήμης του πέσει κάτω από ένα συγκεκριμένο κατώφλι. Το πρωτόκολλο θεωρεί την ύπαρξη δύο τύπων μη ομαλής συμπεριφοράς:

- Την ***Παραπλανητική***, κατά την οποία ένας κόμβος ανταποκρίνεται θετικά σε αιτήσεις δρομολόγησης, αλλά στην πραγματικότητα αποτυγχάνει να προωθήσει πακέτα, έτσι ώστε να παραπλανήσει τους άλλους κόμβους με σκοπό να θεωρήσουν ότι αυτός δεν μπορεί να προωθήσει επιτυχώς πακέτα.
- Την ***Εγωιστική***, κατά την οποία ένας κόμβος δεν αποκρίνεται σε αιτήσεις δρομολόγησης, αλλά συνεχίζει να αποστέλλει τα δικά του πακέτα στο δίκτυο, με αποτέλεσμα να επωφελείται από τους πόρους των άλλων κόμβων, χωρίς να παραχωρεί ο ίδιος τους δικούς του πόρους.

Θεωρώντας ότι το δίκτυο αποτελείται από Μ κόμβους, αυτοί χωρίζονται σε:

- **Καλούς κόμβους**, που ανταποκρίνονται θετικά σε αιτήσεις δρομολόγησης και προωθούν επιτυχώς πακέτα.
- **Παραπλανητικούς κόμβους**, που ανταποκρίνονται θετικά σε αιτήσεις δρομολόγησης αλλά δεν προωθούν ουσιαστικά τα πακέτα.
- **Εγωιστικούς κόμβους**, που δεν ανταποκρίνονται καν σε αιτήσεις δρομολόγησης.

Στο πρωτόκολλο LRM, κάθε κόμβος διατηρεί έναν πίνακα φήμης, στον οποίο αποθηκεύει την τιμή φήμης R, όλων των γειτονικών του κόμβων. Η τιμή αυτή ποικίλει και εκτείνεται από R_{min} έως R_{max}. Για την εξαγωγή συμπερασμάτων από την φήμη σχετικά με τη συμπεριφορά των κόμβων, ορίζονται τρία κατώφλια:

1. $\mathbf{R_w}$, που σηματοδοτεί την καλή φήμη
2. $\mathbf{R_t}$, που σηματοδοτεί την παραπλανητική φήμη
3. $\mathbf{R_v}$, που σηματοδοτεί την κακή φήμη

Για τις τιμές αυτές, ισχύει η σχέση $R_{\min} < R_v < R_t < R_w < R_{\max}$.

Έτσι, εξάγονται τα ακόλουθα συμπεράσματα σχετικά με τη συμπεριφορά των κόμβων:

- Ένας κόμβος θεωρείται καλός, αν $R_w \le R < R_{\max}$.
- Ένας κόμβος θεωρείται παραπλανητικός, αν $R_t \le R < R_w$.
- Ένας κόμβος θεωρείται εγωιστικός, αν $R_{\min} \le R < R_v$.

- Ένας κόμβος δεν μπορεί να αναγνωριστεί αν είναι εγωιστικός ή όχι, αν $R_v \le R < R_t$.

Κάθε νέος κόμβος που εισάγεται στο δίκτυο παίρνει τιμή φήμης που ανήκει στην τελευταία περίπτωση που αναφέρθηκε, αφού δεν υπάρχουν πληροφορίες σχετικά με τη συμπεριφορά του.
Κάθε κόμβος X διατηρεί για κάθε γειτονικό του κόμβο Y που ανήκει στη γειτονιά του N(X), μια τιμή φήμης R_{XY}, όπου ανανεώνεται βάσει άμεσων παρατηρήσεων. Ο κόμβος Y, θεωρείται εγωιστικός και εισάγεται στη λίστα σφαλμάτων, όταν η τιμή φήμης R_{XY}, πέσει κάτω από το κατώφλι κακής φήμης R_v.Την ίδια στιγμή, ένα μήνυμα προειδοποίησης WARNING αποστέλλεται για να ειδοποιήσει άλλους γειτονικούς κόμβους του X για την εγωιστική συμπεριφορά του Y.
Κατά τη λειτουργία του δικτύου, ένας κόμβος μπορεί λανθασμένα να αναφέρει την καλή συμπεριφορά άλλων κόμβων. Αν θεωρηθεί παραπλανητική η συμπεριφορά ενός καλού κόμβου, τότε ο κόμβος που έχει κατηγορηθεί λανθασμένα και η τιμή φήμης του έχει πέσει κάτω από το κατώφλι R_w, θα μπορεί ακόμα να συμμετέχει στην επόμενη απόκριση δρομολόγησης. Σε αντίθετη περίπτωση, αν ο καλός κόμβος κατηγορηθεί λανθασμένα και η τιμή φήμης του πέσει κάτω από το κατώφλι R_w,
θα συμπεριληφθεί στη λίστα σφαλμάτων.

2.9.1.1 ΥΠΟΛΟΓΙΣΜΟΣ ΦΗΜΗΣ

Κάθε φορά που ένας ενδιάμεσος κόμβος I συμμετέχει στο πρωτόκολλο δρομολόγησης, οι γειτονικοί του κόμβοι θα παρατηρήσουν τη συμπεριφορά του και θα ανανεώσουν ανάλογα την τιμή της φήμης του. Όσο ο I συνεχίζει να προωθεί πακέτα και να συμμετέχει θετικά στη διαδικασία δρομολόγησης και προώθησης, η φήμη του αυξάνεται, ενώ σε αντίθετη περίπτωση μειώνεται.
Πιο συγκεκριμένα, όταν ο κόμβος I προωθήσει ένα πακέτο δεδομένων, οι γειτονικοί του κόμβοι παρατηρούν την προώθηση και αυξάνουν την φήμη του I, κατά α Δηλαδή, η φήμη του γίνεται $R_{XI} = R_{XI} + a$, για κάθε κόμβο X που βρίσκεται στη γειτονιά του I.
Εάν, στη συνέχεια, ο κόμβος J που είναι ο επόμενος στο μονοπάτι μετά τον I, απορρίψει τα πακέτα που προωθεί ο I, οι γειτονικοί κόμβοι και των δύο, θα ανιχνεύσουν την απόρριψη και θα μειώσουν την τιμή φήμης του J, κατά β. Δηλαδή, η φήμη του γίνεται $R_{XJ} = R_{XJ} - \beta$, για κάθε κόμβο X που αποτελεί γείτονα και των δύο ταυτοχρόνως. Ο αριθμός β, είναι ίσος με $\beta = \alpha + k * h$, όπου k ο αριθμός των βημάτων που έχει ταξιδέψει ένα πακέτο και μπορεί να εκτιμηθεί από τους πίνακες δρομολόγησης τρων ενδιάμεσων κόμβων, και α και h θετικές σταθερές. Η τιμή β, δείχνει ότι όσο περισσότερα βήματα έχει διανύσει ένα πακέτο, τόσο μεγαλύτερη θα είναι η απώλεια φήμης για τον J, αν αποτύχει να προωθήσει το πακέτο.

Όπως αναφέρθηκε, όταν ένας κόμβος N ανακαλύπτει έναν νέο γειτονικό κόμβο, του αποδίδει μια αρχική τιμή φήμης R_0, καθώς δεν μπορεί να γνωρίζει τη συμπεριφορά του, και ανανεώνει στη συνέχεια δυναμικά τη φήμη του, ανάλογα με τα αποτελέσματα της προώθησης πακέτων από αυτόν. Μια σωστή προώθηση θα οδηγήσει τη φήμη του στο μέγιστο, ενώ μια λανθασμένη προώθηση θα μειώσει τη φήμη του, η οποία αν πέσει κάτω από το κατώφλι κακής φήμης, ο κόμβος θα θεωρηθεί εγωιστικός και θα εισαχθεί στη λίστα σφαλμάτων.

Στο LRM, έχει σημασία η επιλογή της τιμής $\Delta\tau \equiv R_0 - R_v$, αφού από αυτήν εξαρτάται η ευαισθησία στα γεγονότα απόρριψης πακέτων. Πιο συγκεκριμένα, μια μικρή τιμή του Δτ οδηγεί σε μεγάλη ευαισθησία που έχει ως αποτέλεσμα την γρήγορη απομόνωση των εγωιστικών κόμβων. Μεγάλη τιμή στο Δτ, θα έχει αντίθετα αποτελέσματα. Η τιμή του Δτ καθορίζεται από την πυκνότητα του δικτύου, από το φορτίο κίνησης, τον αναμενόμενο αριθμό εγωιστικών κόμβων κ.τ.λ. και μετά από προσομοιώσεις, έχει θεωρηθεί ως κατάλληλη τιμή η Δτ=15.

2.9.2 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ LRM

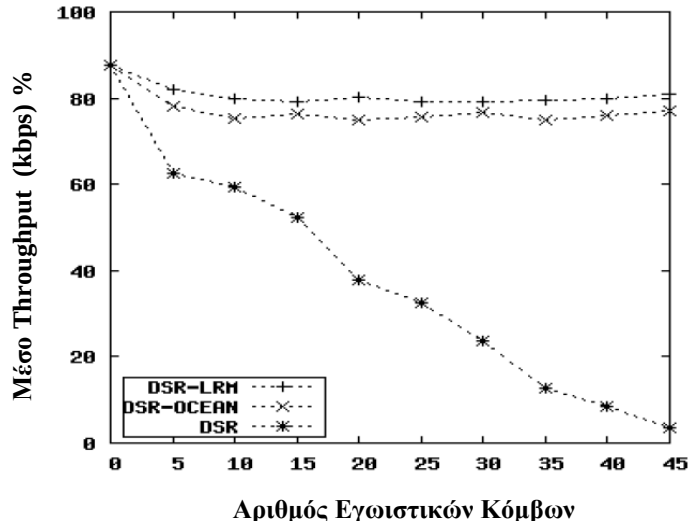
Οι δημιουργοί του πρωτοκόλλου LRM, χρησιμοποίησαν την έκδοση του διαδεδομένου προσομοιωτή δικτύων, NS2.28, με σκοπό να πραγματοποιήσουν τις απαραίτητες προσομοιώσεις ώστε να εξάγουν συμπεράσματα και τα αντίστοιχα διαγράμματα για το σχήμα. Ως πρωτόκολλο δρομολόγησης επιλέχθηκε το DSR. Το περιβάλλον της προσομοίωσης, διαμορφώθηκε ως εξής:

- Αριθμός κόμβων 50
- Περιοχή 1000 x 1000 m^2
- Ορισμένη τοπολογία και αρίθμηση κόμβων
- Πρωτόκολλο MAC, IEEE 802.11
- Ρυθμός μετάδοσης 2Mbps
- Μέγεθος πακέτου 512 bytes
- Χρόνος προσομοίωσης 900 s

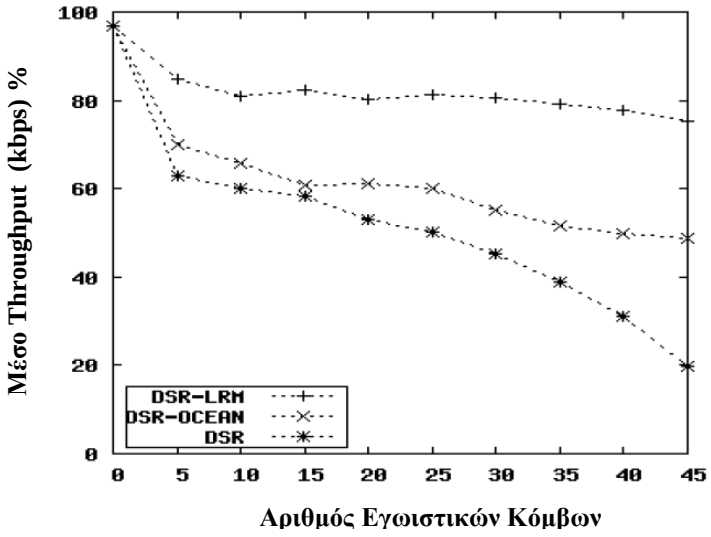
Οι απαραίτητες παράμετροι που εισάγονται από το LRM, πήραν τις παρακάτω τιμές κατά τη διάρκεια των προσομοιώσεων:

- $R_w = 80$
- $R_t = 60$
- $R_v = 20$
- $\alpha = 4$
- $h = 0.5$
- $R = \alpha + k*h$
- $\Delta\tau = 15$

Μετά από την πραγματοποίηση προσομοιώσεων κάτω από διαφορετικά σενάρια, οι κατασκευαστές του LRM, έκαναν μετρήσεις ως προς το throughput και το λόγο προώθησης πακέτων(λόγος μεταξύ των ληφθέντων στον προορισμό πακέτων και αποσταλμένων πακέτων από την πηγή. Από τις προσομοιώσεις προέκυψαν τα εξής διαγράμματα και συμπεράσματα σχετικά με την απόδοση του πρωτοκόλλου LRM:



Διάγραμμα 2.9.1 (Πηγή [9])



Διάγραμμα 2.9.2 (Πηγή [9])

Τα διαγράμματα αυτά έχουν στον κάθετο άξονα το ***μέσο throughput σε kbps και επί τοις εκατό***, αντίστοιχα με τη σειρά που εμφανίζονται, και στον οριζόντιο άξονα τον ***αριθμό των εγωιστικών κόμβων***, και σκοπεύουν στη σύγκριση δικτύων στα οποία εφαρμόζονται είτε το DSR με εφαρμογή του LRM, είτε το DSR με εφαρμογή του OCEAN, είτε το DSR μόνο του. Διαπιστώνονται τα εξής συμπεράσματα:

- Η ικανότητα του LRM να αναγνωρίζει και να απομονώνει αποτελεσματικά τους εγωιστικούς κόμβους, επιδρά στην αύξηση κατά 80% της τιμής του throughput σε δίκτυο που χρησιμοποιεί μόνο το DSR, όσο οι εγωιστικοί κόμβοι αυξάνουν.
- Η απόδοση του δικτύου σύμφωνα με τη μέτρηση του throughput, είναι ελαφρώς καλύτερη ακόμα και από δίκτυο που χρησιμοποιεί όχι μόνο το DSR, αλλά και τον μηχανισμό υποστήριξης συνεργασίας OCEAN, καθώς στο τελευταίο, οι παραπλανητικοί κόμβοι δεν μπορούν να επιστέψουν γρήγορα στο δίκτυο.

- Ο λόγος προώθησης πακέτων στο LRM έχει μόνο μια μικρή πτώση με την αύξηση των εγωιστικών κόμβων, σε αντίθεση με το DSR, που μειώνεται σημαντικά.

Συμπερασματικά, το LRM αποτελεί ένα σχετικά απλό μηχανισμό φήμης που χρησιμοποιεί μόνο την τοπική πληροφορία, με σκοπό να εντοπίσει και να απομονώσει τους εγωιστικούς κόμβους στο δίκτυο. Το LRM δίνει ακόμα τη δυνατότητα γρήγορης επιστροφής στο δίκτυο, των κατηγορημένων κόμβων. Από τις προσομοιώσεις των κατασκευαστών του φαίνεται, ότι το πρωτόκολλο μπορεί αποτελεσματικά να βελτιώσει την απόδοση ενός ασύρματου ad-hoc δικτύου.

2.10 E.R.B.M

Το συγκεκριμένο πρωτόκολλο, (που χάρη ευκολίας θα αποκαλείται στα πλαίσια της παρούσας εργασίας ως E.R.B.M.) [10] αποτελεί έναν μηχανισμό υποστήριξης συνεργασίας για κινητά ad-hoc δίκτυα βασιζόμενο στη φήμη, που βασίζεται στην συνεχή ανίχνευση και ανανέωση first-hand και second-hand πληροφορίας. Σύμφωνα με τη λειτουργία του πρωτοκόλλου, οι κόμβοι στο δίκτυο μπορούν να ανιχνεύσουν τους γειτονικούς τους κόμβους και να αποκτήσουν την first-hand πληροφορία που βασίζεται στην αντιληπτή συμπεριφορά τους, ενώ η second-hand πληροφορία αποκτάται από την ανταλλαγή first-hand πληροφορίας με άλλους κόμβους. Η συνολική τιμή φήμης στο πρωτόκολλο, αποτελεί μια συνάρτηση από τις δύο μορφές πληροφορίας, πράγμα που δίνει επιπρόσθετη αξιοπιστία.

2.10.1 ΛΕΙΤΟΥΡΓΙΑ

Όπως προαναφέρθηκε, το συγκεκριμένο πρωτόκολλο χρησιμοποιεί από τη μια την υποκειμενική φήμη, που υπολογίζεται από τις άμεσες παρατηρήσεις των κόμβων, και την έμμεση φήμη, η οποία εγκαθιδρύεται από άλλους κόμβους. Στην προσέγγιση αυτή, μόνο οι γειτονικοί κόμβοι που απέχουν μόνο ένα βήμα από έναν κόμβο, μπορούν να ελέγξουν τη συμπεριφορά του και να ανανεώσουν τη φήμη του. Η λογική είναι, ότι όλοι οι κόμβοι αρχικά έχουν την ίδια τιμή φήμης, η οποία αυξάνεται όταν ο κόμβος έχει καλή συμπεριφορά ενώ μειώνεται σε αντίθετη περίπτωση. Το παρόν πρωτόκολλο χρησιμοποιώντας ένα διαδικαστικό σύστημα προτεραιότητας, συνδυάζει την τιμωρία των μη ομαλά συμπεριφερόμενων κόμβων, με την προσφορά κινήτρων. Πιο συγκεκριμένα, οι κόμβοι που συνεργάζονται σωστά, λαμβάνουν υπηρεσίες νωρίτερα από τους εγωιστικούς κόμβους, οι αιτήσεις τους δηλαδή απαντώνται γρηγορότερα. Επίσης, από τη στιγμή που οι κόμβοι κατέχουν μόνο τις πληροφορίες για τους άμεσα γειτονικούς κόμβους και όχι για όλο το δίκτυο, υπάρχει σημαντική μείωση της επιβάρυνσης δικτύου – overhead.
Το πρωτόκολλο έχει τρεις βασικές λειτουργίες:

1. Την **ανίχνευση της συμπεριφοράς των γειτονικών κόμβων.**
2. Τον **υπολογισμό ης φήμης των κόμβων.**
3. Την **απόδοση προτεραιότητας για λήψη υπηρεσιών στους κόμβους.**

Για την υλοποίηση των λειτουργιών αυτών, διαθέτει τρεις θεμελιακούς μηχανισμούς που αντιστοίχως τις υλοποιούν:

1. Το **Monitoring System**
2. Το **Reputation System**
3. Το **Priority Processing System**

2.10.1.1 ΑΝΙΧΝΕΥΣΗ

Η λειτουργία της ανίχνευσης, πραγματοποιείται μέσω του συστήματος ανίχνευσης(Monitoring System), που διαθέτει το πρωτόκολλο. Σε κάθε κόμβο, υπάρχει ένα στοιχείο-φύλακας, που έχει ως καθήκον, την ανίχνευση των γειτονικών κόμβων και την παρακολούθηση της συμπεριφοράς τους. Οι παρατηρήσεις αυτές είναι οι first-hand πληροφορίες που είναι περιορισμένες από την ασύρματη εμβέλεια

του κόμβου. Η διαδικασία της ανίχνευσης, πιο συγκεκριμένα έχει ως εξής: Κάθε κόμβος ελέγχει τους άμεσα γειτονικούς του κόμβους, και στη συνέχεια αποθηκεύει τον αριθμό των πακέτων που αποστέλλονται και λαμβάνονται από τους κόμβους, ενώ ύστερα τους αποστέλλει στο μηχανισμό υπολογισμού φήμης, Reputation System. Οι συγκεκριμένες πληροφορίες ανανεώνονται ανά ένα ορισμένο χρονικό διάστημα.

2.10.1.2 ΦΗΜΗ

Η λειτουργία υπολογισμού της φήμης των κόμβων πραγματοποιείται μέσω του μηχανισμού Reputation System. Πιο συγκεκριμένα, το εργαλείο χρησιμοποιεί την αναλογία του αριθμού των πακέτων που έχουν αποσταλεί από έναν κόμβο προς τον αριθμό των πακέτων που έχουν ληφθεί από έναν κόμβο, ως τον συντελεστή συνεργασίας του κόμβου. Ο συντελεστής αυτός αναπαριστά ουσιαστικά φήμη ενός κόμβου, και μαθηματικά έχει τη μορφή:

$$a = \frac{\text{Αριθμός απεσταλμένων πακέτων}}{\text{Αριθμός ληφθέντων πακέτων}}$$

Σε κάθε κόμβο, υπάρχει ένας πίνακας που διατηρεί τη φήμη των κόμβων που πρέπει να ελεγχθούν και να ανιχνευθούν. Η πληροφορία του πίνακα αυτού ανανεώνεται ανάλογα με τις τιμές που αποστέλλονται από το Monitoring System. Ο συντελεστής συνεργασίας ενός κόμβου, είναι ένας αριθμός από το 0 έως το 1. Τιμές κοντά στο 0, δείχνουν ότι η συνεργασία του κόμβου είναι χαμηλή, και επομένως είναι ένας εγωιστικός κόμβος, ενώ τιμές κοντά στο 1 δείχνουν υψηλή συνεργασία και επομένως υψηλή φήμη. Στο συγκεκριμένο πρωτόκολλο, αντί της ανταλλαγής μηνυμάτων που εμπεριέχουν πληροφορίες φήμης και προειδοποιητικών μηνυμάτων, ενσωματώνεται στην αίτηση δρομολόγησης ένα πεδίο, που περιέχει τον συντελεστή συνεργασίας, με αποτέλεσμα να μειώνεται αισθητά ο αριθμός των μηνυμάτων.
Με τον τρόπο αυτό, ο κόμβος που θα λάβει την προαναφερθείσα αίτηση δρομολόγησης, συγκρίνει το πεδίο src-addr(αναζήτησης διεύθυνσης) του πακέτου, με το αντίστοιχο πεδίο άλλων πακέτων, και ακολουθεί μία εκ των παρακάτω επιλογών:

- Εάν υπάρχει μόνο ένα πακέτο με το ίδιο πεδίο, και ο κόμβος – πηγή ήταν μέρος των γειτονικών κόμβων που είχαν ανιχνευθεί από τον κόμβο, τότε τοποθετεί τον πραγματικό συντελεστή συνεργασίας του κόμβου στο σχετικό πεδίο του πακέτου.
- Εάν αρκετά πακέτα αίτησης διαδρομής δρομολόγησης RREQ με το ίδιο πεδίο src-addr, ληφθούν από τον κόμβο, τότε η νέα τιμή του συντελεστή συνεργασίας πρέπει να υπολογιστεί. Η τιμή υπολογίζεται βάσει του προσδιορισμένου βάρους για κάθε τιμή φήμης του πακέτου, το οποίο εξαρτάται από τον αριθμό των βημάτων – hops που έχει πραγματοποιήσει το πακέτο. Από όσο πιο μακριά προέρχεται το πακέτο, τόσο πιο πιθανό είναι να έχει αλλάξει η τιμή φήμης, άρα έχει και λιγότερο βάρος. Ο αριθμός των hops που πραγματοποιούνται από το πακέτο, μετριέται με έναν μετρητή που διαθέτει κάθε RREQ. Έτσι το Reputation System σε κάθε κόμβο, ανανεώνει την τιμή του συντελεστή συνεργασίας a, σύμφωνα με τη σχέση:

$$\alpha_{\mu} = \frac{\sum_{i=1}^{n} a_i w_i}{n}$$

Το n αναπαριστά τον αριθμό των πακέτων με το ίδιο πεδίο src-addr, το αναπαριστά το προσδιορισμένο βάρος στο i RREQ πακέτο και υπολογίζεται από τον τύπο:

$$w_i = \frac{s - c_i}{s}$$

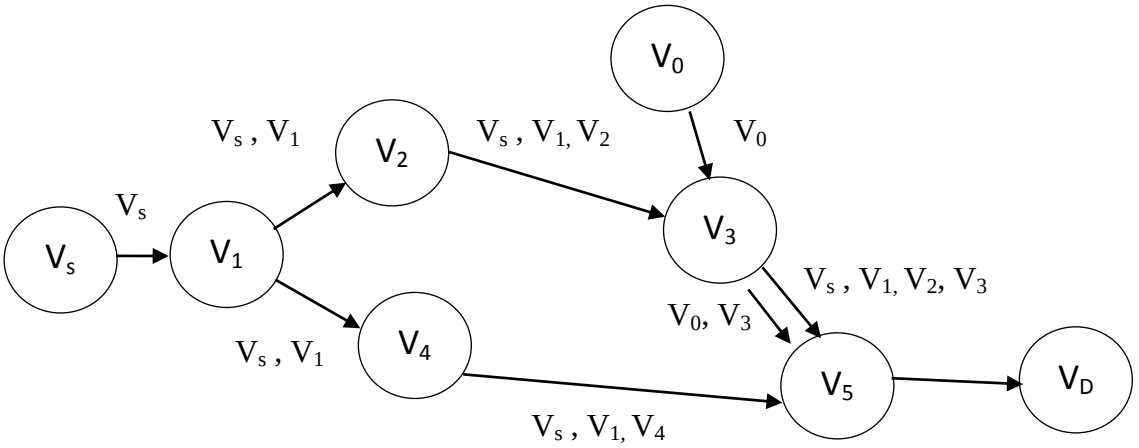
Αντίστοιχα το s υπολογίζεται αντίστοιχα από τη σχέση:

$$s = \sum_{i=1}^{n} c_i \ ,$$

,όπου c_i αναπαριστούν τον αριθμό των βημάτων που έχει διανύσει κάθε πακέτο.

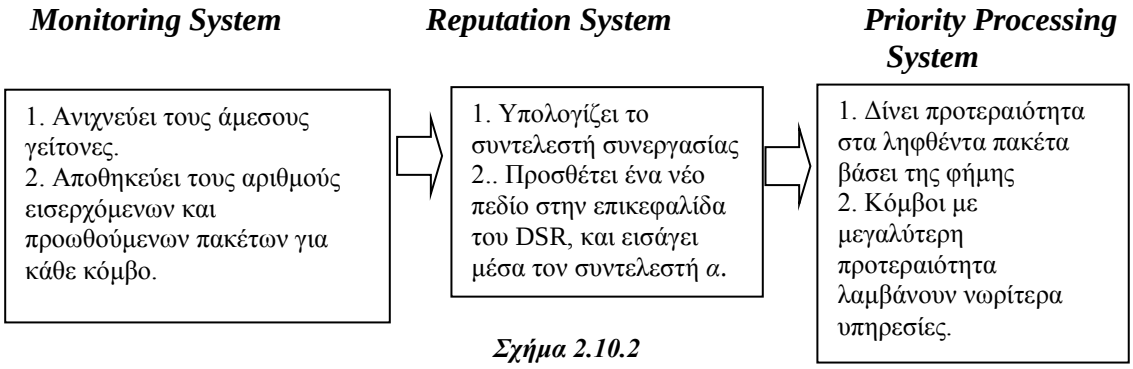
2.10.1.3 ΠΡΟΤΕΡΑΙΟΤΗΤΑ

Η λειτουργία αυτή που πραγματοποιείται με τη βοήθεια του Priority Processing System, οδηγεί στη λήψη αποφάσεων βασιζόμενη στις πληροφορίες που παράγονται από το Reputation System. Πιο συγκεκριμένα, κάθε αλλαγή στη φήμη των κόμβων μπορεί να προκαλέσει αλλαγές στην προτεραιότητα με βάση την οποία λαμβάνουν υπηρεσίες. Έτσι, κάθε κόμβος έχει μια ουρά για την προώθηση πακέτων, η οποία λειτουργεί και σαν ουρά προτεραιότητας. Βέβαια, το εργαλείο για την προτεραιότητα, ορίζει ότι η προτεραιότητα για κάθε πακέτο εξαρτάται από τον συντελεστή συνεργασίας που βρίσκεται στο αντίστοιχο πεδίο του. Στην περίπτωση που ο κόμβος λαμβάνει ένα πακέτο, είναι δυνατό να το προωθήσει άμεσα. Στην περίπτωση πάλι που λαμβάνει πολλαπλά πακέτα και δεν μπορεί να τα μεταδώσει αλλεπάλληλα, τα ληφθέντα πακέτα πρέπει να περιμένουν στη σειρά προτεραιότητας. Στην πραγματικότητα, στο Priority Processing System, πριν την εισαγωγή ενός πακέτου στην ουρά, λαμβάνεται υπ’ όψη ο συντελεστής συνεργασίας του. Με άλλα λόγια, το πακέτο που βρίσκεται στο έμπροσθεν μέρος της ουράς θα προωθηθεί νωρίτερα, καθώς ο κόμβος αποστολέας του έχει μεγαλύτερο συντελεστή συνεργασίας από τον κόμβο που απέστειλε το πακέτο που βρίσκεται στο πίσω μέρος της ουράς, που θεωρείται πιο εγωιστικός από τους υπόλοιπους. Με τον τρόπο αυτό, δίνονται κίνητρα στους κόμβους που συνεργάζονται σωστά, αφού θα λάβουν νωρίτερα υπηρεσίες. Η λειτουργία αυτή φαίνεται στο παρακάτω σχήμα: Αν υποθέσουμε ότι ο κόμβος V5 λαμβάνει πολλαπλά πακέτα αναζήτησης διαδρομής δρομολόγησης, και ότι ο κόμβος V0 έχει το μεγαλύτερο συντελεστή συνεργασίας, τότε ο κόμβος V5 θα περάσει πρώτα το πακέτο του V0.



Σχήμα 2.10.1

Επιγραμματικά, οι τρεις βασικοί μηχανισμοί που χρησιμοποιεί το πρωτόκολλο, λειτουργούν όπως σχηματικά φαίνεται παρακάτω:



Σχήμα 2.10.2

Τέλος, στην περίπτωση που ένας κόμβος δεν είναι πραγματικά εγωιστικός, αλλά η μη ομαλή συμπεριφορά του έχει να κάνει με άλλους παράγοντες, το πρωτόκολλο του δίνει την δυνατότητα επανένταξης. Συγκεκριμένα, αφού οι τιμές του συντελεστή συνεργασίας ανανεώνονται ανά συγκεκριμένες περιόδους, ένας κατηγορούμενος κόμβος μπορεί να αλλάξει μέσα σε αυτές συμπεριφορά. Με τον τρόπο αυτό, θα αυξηθεί ο συντελεστής του, και θα ενθαρρυνθεί μέσω των κινήτρων που περιγράφηκαν παραπάνω.

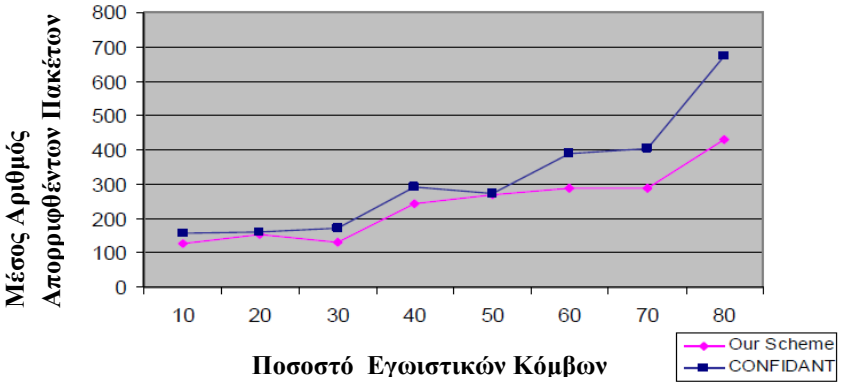
2.10.2 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ E.R.B.M.

Οι δημιουργοί του πρωτοκόλλου, έχουν πραγματοποιήσει προσομοιώσεις με σκοπό να ελέγξουν την λειτουργία του και την αποτελεσματικότητά του, και να βγάλουν συμπεράσματα για την απόδοση του ad-hoc δικτύου, όταν αυτό εφαρμόζεται. Οι προσομοιώσεις πραγματοποιήθηκαν με τον προσομοιωτή δικτύων GLOMOSIM. Το περιβάλλον προσομοίωσης κατά τη διαδικασία αυτή, διαμορφώθηκε όπως φαίνεται παρακάτω:

- Μέγεθος πακέτου 512 bytes
- Πρωτόκολλο MAC, IEEE 802.11
- Ρυθμός μετάδοσης 2Mbps
- Χρόνος προσομοίωσης 300s
- Κίνηση τυχαία

- Τοποθέτηση τυχαία
- Εμβέλεια 250 m
- Περιοχή 1000 x 1000 m^2

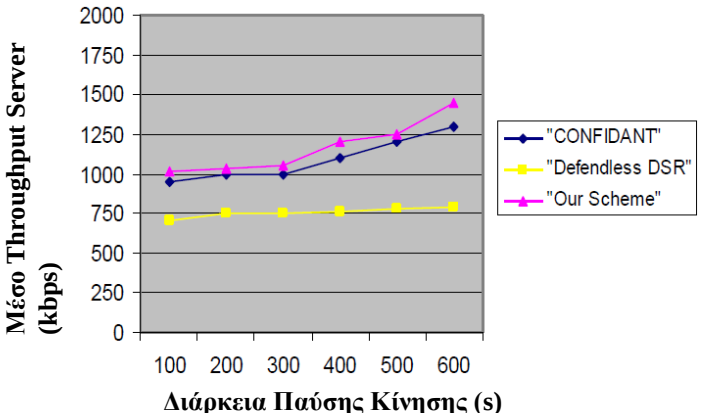
Οι προσομοιώσεις, πραγματοποιήθηκαν με σκοπό τη σύγκριση του παρόντος πρωτοκόλλου με το γνωστό μηχανισμό υποστήριξης συνεργασίας CONFIDANT, που περιγράφηκε στην παρούσα εργασία. Συγκεκριμένα, από τα πειράματα προέκυψαν τα εξής διαγράμματα και συμπεράσματα, σύμφωνα με τους δημιουργούς του σχήματος:
Το παρακάτω διάγραμμα δείχνει με ροζ γραμμή τα αποτελέσματα των προσομοιώσεων για το E.R.B.M. και με τη μπλε γραμμή τα αποτελέσματα των προσομοιώσεων για το CONFIDANT. Στον κάθετο άξονα έχει τον ***μέσο αριθμό των απορριφθέντων πακέτων*** και στον οριζόντιο άξονα ***το ποσοστό των εγωιστικών κόμβων στο δίκτυο***.



Διάγραμμα 2.10.1 (Πηγή [10])

Παρατηρείται ότι ο αριθμός των απορριφθέντων πακέτων, με τη αύξηση των εγωιστικών κόμβων, είναι μικρότερος από ότι στο πρωτόκολλο CONFIDANT, πράγμα που συμβαίνει καθώς στο παρόν πρωτόκολλο τα πακέτα δεν απορρίπτονται αλλά περιμένουν στην ουρά. Ένας άλλος παράγοντας για το γεγονός αυτό, είναι ότι οι διαδρομές που περιέχονται εγωιστικοί κόμβοι δεν απορρίπτονται, με αποτέλεσμα οι υπόλοιπες διαδρομές να μην αποκτούν υπερβολικά μεγάλο φόρτο.

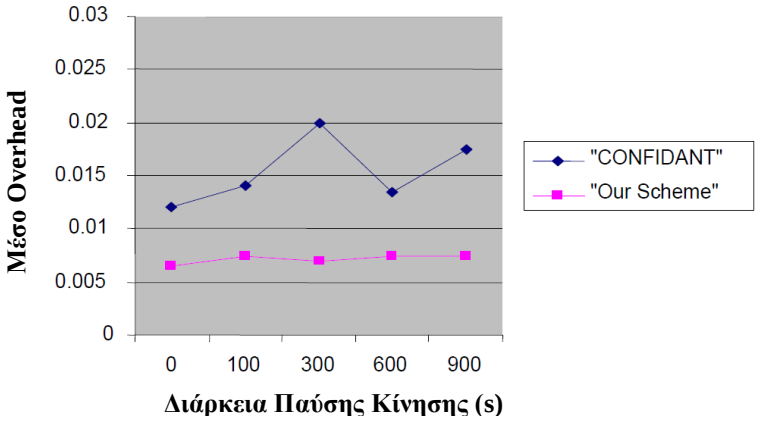
Ακόμη, παρήχθη το παρακάτω διάγραμμα για σύγκριση της απόδοσης δικτύων που εφαρμόζεται το E.R.B.M., το CONFIDANT ή απλώς το DSR(ροζ, μπλε και κίτρινη γραμμή για τα αποτελέσματα αντίστοιχα), που στον κάθετο άξονα έχει το ***μέσο throughput του server σε kbps***, και στον οριζόντιο άξονα ***τη διάρκεια της παύσης κίνησης σε δευτερόλεπτα***.



Διάγραμμα 2.10.2 (Πηγή [10])

Συμπεραίνεται ότι το throughput στο δίκτυο, μεγαλώνει αυξάνοντας την περίοδο στάσης, και είναι ελαφρώς μεγαλύτερο από το αντίστοιχο στο CONFIDANT.

Τέλος το παρακάτω διάγραμμα παρήχθη για σύγκριση μεταξύ του E.R.B.M και του CONFIDANT(ροζ και μπλε γραμμή αντίστοιχα), όσον αφορά την επιβάρυνση στο δίκτυο. Έχει στον κάθετο άξονα ***τη μέση επιβάρυνση overhead*** και στον οριζόντιο ***τη διάρκεια της παύσης κίνησης σε δευτερόλεπτα.***



Διάγραμμα 2.10.3 (Πηγή [10])

Διαπιστώνεται ότι η επιβάρυνση overhead στο δίκτυο, είναι αρκετά μικρότερη σε σχέση με τη χρήση του CONFIDANT, πράγμα που οφείλεται στα λιγότερα μηνύματα προειδοποίησης και μετάδοσης φήμης, που υπάρχουν στο παρουσιαζόμενο πρωτόκολλο. Το πεδίο που περιέχει τον συντελεστή συνεργασίας δεν εξαρτάται από τον αριθμό των εγωιστικών κόμβων, και δεν αλλάζει, με αποτέλεσμα να μην συνιστά σημαντικά στην επιβάρυνση.

Συμπερασματικά, το E.R.B.M. αποτελεί έναν μηχανισμό υποστήριξης συνεργασίας που αποφέρει αισθητή βελτίωση στην απόδοση του δικτύου σε σχέση και με άλλα παραπλήσια σχήματα, μεγαλώνει το throughput και μειώνει το overhead. Χρησιμοποιεί συνδυασμό υποκειμενικής και έμμεσης φήμης, και δίνει κίνητρα στους κόμβους ώστε να συνεργαστούν, με το σύστημα προτεραιότητας που διαθέτει.

2.11 FITS

Το πρωτόκολλο FITS [11] αποτελεί έναν μηχανισμό υποστήριξης συνεργασίας για ασύρματα ad-hoc δίκτυα βασιζόμενο στη φήμη, που δίνει βάρος στην προσφορά κινήτρων ώστε να προωθήσει τη συνεργασία μεταξύ των κόμβων. Προσδιορίζει τη διαφορά του με τους υπόλοιπους μηχανισμούς φήμης που διαθέτουν ακριβή και αυστηρή μαθηματική ανάλυση, στο γεγονός ότι αυτοί μελετούν την αλληλεπίδραση μεταξύ των κόμβων, ως ένα ατέρμονο παίγνιο φήμης. Το γεγονός αυτό, μπορεί από τη μία να είναι θεωρητικό σωστό, όμως στην πραγματικότητα δεν εξασφαλίζει την συνεργασία μεταξύ των κόμβων, αφού αυτή αποτελεί ένα επαναλαμβανόμενο παίγνιο φήμης που έχει αρχή και τέλος. Η λογική αυτή, γίνεται κατανοητή αν υποτεθεί μια διαδικασία επικοινωνίας – παίγνιο μεταξύ ενός κόμβου v_0 και v_1, που έχει αρχή και τέλος, και αποτελείται από ορισμένο αριθμό σταδίων μέχρι ο ένας κόμβος να τεθεί εκτός εμβέλειας του άλλου και να τελειώσει το παίγνιο. Η καλύτερη στρατηγική για τον εγωιστικό κόμβο v_0, είναι να συνεργαστεί φυσιολογικά μέχρι το τελευταίο στάδιο πριν τη λήξη του παιγνίου, και να μην συνεργαστεί στο τελευταίο. Ο κόμβος v_1 πάλι, που διαθέτει την ίδια νοημοσύνη και γνωρίζει τη στρατηγική του v_0, ακολουθεί ως πιο συμφέρουσα στρατηγική να μην συνεργαστεί στα δύο τελευταία στάδια, αφού έτσι κι αλλιώς δεν θα εξυπηρετηθεί στο τελευταίο στάδιο. Αν η συμπεριφορά αυτή από τους δύο κόμβους συνεχιστεί μελετώντας ο ένας τη στρατηγική του άλλου, στο τέλος δεν θα υπάρχει συνεργασία μεταξύ τους στο σύνολο του παιγνίου. Το πρωτόκολλο FITS αντιμετωπίζει τέτοια προβλήματα σε πρακτικά μοντέλα, χρησιμοποιώντας μια τεχνική που ονομάζεται TTI (Threat To Interfere). Η λογική της τεχνικής αυτής, είναι ότι δίνει τη δυνατότητα σε έναν κόμβο να απειλήσει έναν άλλο γειτονικό κόμβο ότι θα παρεμποδίσει την επικοινωνία του μετά τη λήξη ενός παιγνίου , εάν αυτός δεν συνεργαστεί στο τελευταίο στάδιο. Με τον τρόπο αυτό αποφεύγεται η μη συνεργασία από την αρχή.

Το FITS θεωρεί ότι κάθε κόμβος μπορεί να ακούσει τις μεταδόσεις των γειτονικών του κόμβων, ότι οι ζεύξεις είναι αμφίδρομες και ότι οι κόμβοι μπορεί να είναι εγωιστικοί μα όχι κακόβουλοι. Το παίγνιο της φήμης μεταξύ δύο κόμβων, μελετάται ως διαχωριζόμενο σε Τ στάδια, με Τ>0, όπου σε κάθε στάδιο ανταλλάσσεται μεταξύ των δύο κόμβων, μεγάλος αριθμός πακέτων. Πιο συγκεκριμένα σε κάθε παίγνιο, κάθε κόμβος v_i με $i \in \{0,1\}$, μπορεί σε κάθε στάδιο t να επιλέξει μια ενέργεια $\alpha_{i,t}$, από το σύνολο $A_i = \{a_i \mid 0 \le a_i \le 1\}$. Η ενέργεια αυτή, είναι ουσιαστικά η πιθανότητα ο κόμβος v_i, να προωθήσει κατά το στάδιο t τα πακέτα του κόμβου v_{1-i}. Ακόμα ορίζεται η «χρησιμότητα» του κόμβου v_i, ως εξής:

$$u_{i,t} = a_{1-i,t}u - a_{i,t}c$$

, όπου u το κέρδος που μπορεί να αποκομίσει εάν όλα τα πακέτα του προωθηθούν από τον v_{1-i}, καθ' όλη τη διάρκεια του σταδίου, και c το κόστος που χρειάζεται από τον v_i, για να προωθήσει στο στάδιο, όλα τα πακέτα του κόμβου v_{1-i}. Προφανώς τα u και c είναι ίδια για όλους τους κόμβους, με u>c>0. Η συνολική χρησιμότητα ενός κόμβου, είναι το άθροισμα των χρησιμοτήτων από όλα τα στάδια:

$$u_i = \sum_{t=1}^{T} u_{i,t}$$

Οι ενέργειες ενός κόμβου, δεν είναι ορατές από τους άλλους παίκτες, λόγω των πιθανών συγκρούσεων. Τα μόνο που είναι ορατό από τον κόμβο v_i, είναι η προσδιορισμένη πιθανότητα ο κόμβος v_{1-i}, να προωθήσει τα πακέτα τοθ στο στάδιο t, που ορίζεται μαθηματικά ως:

$$\hat{a}_{1-i,t} = (1 - p_c) a_{1-i,t}$$

Θωρείται ακόμα η παραδοχή PPA, που σημαίνει ότι και οι δύο κόμβοι μπορούν να δουν και τις δύο προσδιορισμένες ενέργειες($\hat{a}_{0,t}$ και $\hat{a}_{1,t}$) σε κάθε στάδιο. Επίσης με βάση το τελευταίο, για την ανάλυση του FITS, χρησιμοποιήθηκαν δύο ειδών στρατηγικές:

1. Η **PPA-εξαρτώμενη** στρατηγική, όπου αποτελεί συνάρτηση όλου του πιθανού ιστορικού προσδιορισμένων ενεργειών και των δύο κόμβων, από το στάδιο 1 μέχρι και το t, και προσδιορίζει στον κόμβο ποια θα είναι η επόμενη ενέργειά του.
2. Η **PPA-ανεξάρτητη** στρατηγική, όπου αποτελεί συνάρτηση όλου του πιθανού ιστορικού των ενεργειών του κόμβου v_i, και των προσδιορισμένων ενεργειών του κόμβου v_{1-i}, από το στάδιο 1 μέχρι και το t, και προσδιορίζει στον κόμβο ποια θα είναι η επόμενη ενέργειά του.

Το FITS, προτείνει δύο σχήματα, με βάση τα παραπάνω, το FITS-D που λαμβάνει υπ' όψη την παραδοχή PPA, και το FITS-I που δεν τη λαμβάνει υπ 'όψη, με την εφαρμογή των οποίων επιτυγχάνεται ότι η πιθανότητα προώθησης πακέτων από τους κόμβους, πλησιάζει το 1.

2.11.1 ΣΧΗΜΑ FITS-D

Η λογική του σχήματος, έγκειται στη δυνατότητα που έχει ένας κόμβος, να επιλέξει τη χειρότερη δυνατή ενέργεια που έχει καταγραφεί στο ιστορικό της επικοινωνίας. Στην περίπτωση που κανένας κόμβος δεν έχει διεξάγει την λεγόμενη ενέργεια ITF(που σημαίνει ότι ο κόμβος v_i, απορρίπτει όλα τα πακέτα του v_{1-i}, και παρεμποδίζει τις επικοινωνίες του), τότε ένας συνεργάσιμος κόμβος θα επιλέξει την μικρότερη δυνατή πιθανότητα για την προώθηση πακέτων, που έχει εμφανιστεί στο ιστορικό της επικοινωνίας. Η πιθανότητα αυτή μπορεί εύκολα να υπολογιστεί από τον κόμβο. Το πλεονέκτημα του σχήματος, έγκειται στο γεγονός, ότι αν ένα μη ομαλά συμπεριφερόμενος κόμβος απορρίπτει όλα τα πακέτα του γειτονικού του κόμβου με μια συγκεκριμένη πιθανότητα σε ένα στάδιο, τότε ο συνεργάσιμος κόμβος θα απορρίψει όλα τα πακέτα του με τουλάχιστον την ίδια πιθανότητα, σε όλα τα μελλοντικά στάδια. Η συγκεκριμένη απειλή για τιμωρία του μη ομαλά συμπεριφερόμενου κόμβου, τον αποτρέπει από το να απορρίψει πακέτα. Επίσης το σχήμα, εισάγει ένα επιπλέον στάδιο στο οποίο δεν πραγματοποιείται καμία μετάδοση δεδομένων, και χρησιμοποιεί την τεχνική TTI που περιγράφηκε παραπάνω. Κατά το στάδιο αυτό, ένας συνεργάσιμος κόμβος ελέγχει εάν ο άλλος κόμβος ήταν συνεργάσιμος στο τελευταίο στάδιο της μετάδοσης, και αν αυτό συμβαίνει, ο συνεργάσιμος κόμβος δεν κάνει τίποτα. Σε αντίθετη περίπτωση, παρεμποδίζει της επικοινωνίες του έτερου κόμβου. Με τον τρόπο αυτό παρεμποδίζονται οι απορρίψεις πακέτων μέσω της απειλής τιμωρίας, στο τελευταίο στάδιο της μετάδοσης δεδομένων. Ακόμα, με τη χρήση του σχήματος αυτού, δεν υπάρχει περίπτωση μη ομαλής συμπεριφοράς στο επιπλέον στάδιο, αφού κανένας κόμβος δεν μπορεί να αποκομίσει κέρδος σε ένα στάδιο που δεν πραγματοποιείται μετάδοση δεδομένων.

2.11.2 ΣΧΗΜΑ FITS-I

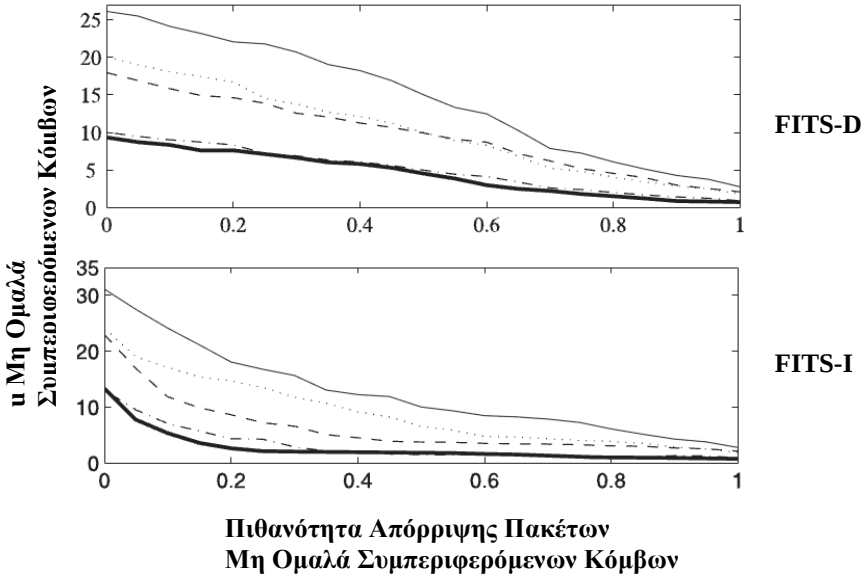
Το σχήμα FITS-I, χρησιμοποιείται σε περιπτώσεις δικτύων, όπου η παραδοχή PPA δεν είναι έγκυρη. Συγκεκριμένα, θεωρείται ότι στην αρχή κάθε σταδίου t, κάθε κόμβος v_i, αξιώνει την πραγματική πιθανότητα προώθησης του $\bar{a}_{i,t}$, στο στάδιο αυτό, στον κόμβο $v_{1\text{-}i}$. Εάν ο κόμβος v_i, είναι συνεργάσιμος, τότε ισχύει $\bar{a}_{i,t} = a_{i,t}$. Έτσι, μπορεί να εγκαθιδρυθεί ένα σχήμα παραπλήσιο με το FITS-D, χωρίς την χρήση προσδιορισμένων πιθανοτήτων, εφόσον μπορεί να εξασφαλιστεί ότι δεν υπάρχουν λάθος υποθέσεις στις πιθανότητες προώθησης. Για να εξασφαλιστεί αυτό, χωρίζεται κάθε στάδιο σε m μικρά χρονικά διαστήματα. Κάθε κόμβος είναι υπεύθυνος να διατηρεί μια λίστα των πακέτων που έχει προωθήσει στο τρέχον χρονικό διάστημα. Στο τέλος κάθε χρονικού διαστήματος, ο κόμβος v_i, με πιθανότητα p_v, επιλέγει να επικυρώσει την πιθανότητα προώθησης του κόμβου $v_{1\text{-}i}$, στο χρονικό διάστημα αυτό. Για να μην αυξηθεί σε μεγάλο βαθμό το overhead, η διαδικασία αυτή δεν γίνεται σε όλα τα χρονικά διαστήματα, αλλά σε κάποια που επιλέγονται τυχαία. Πιο συγκεκριμένα, ο κόμβος v_i, ζητά από στον κόμβο $v_{1\text{-}i}$, την λίστα με τα πακέτα, που προαναφέρθηκε. Στη συνέχεια, χρησιμοποιεί αυτή τη λίστα για να αποφασίσει αν ο $v_{1\text{-}i}$, όντως προώθησε τα πακέτα με πιθανότητα $\bar{a}_{1-i,t}$. Εάν αυτό δεν ισχύει, ο v_i, τιμωρεί τον κόμβο $v_{1\text{-}i}$, απορρίπτοντας τα πακέτα του και εμποδίζοντας τις επικοινωνίες του σε όλα τα μελλοντικά στάδια. Σε αντίθετη περίπτωση, ή στην περίπτωση που το τρέχον χρονικό διάστημα δεν έχει επιλεχθεί για επικύρωση, η λίστα με τα πακέτα απορρίπτεται ώστε να εξοικονομηθεί χώρος. Η επικύρωση των πιθανοτήτων προώθησης, πραγματοποιείται με τη χρήση ενός αλγορίθμου ονόματι VerProb.

2.11.3 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ FITS

Οι δημιουργοί του FITS, έχουν πραγματοποιήσει προσομοιώσεις και μετρήσεις για τον έλεγχο της αποτελεσματικότητας του FITS όσον αφορά την τιμωρία των μη ομαλά συμπεριφερόμενων κόμβων, την προσφορά κινήτρων για συνεργασία, την προστιθέμενη επιβάρυνση στο δίκτυο και την επίδραση της παρεμπόδισης επικοινωνιών που εισάγει το σχήμα. Ακόμα, μέσω των πειραμάτων επιχειρήθηκε η σύγκριση του FITS με άλλα υπάρχοντα σχήματα υποστήριξης συνεργασίας. Οι προσομοιώσεις πραγματοποιήθηκαν με τον προσομοιωτή δικτύων GLOMOSIM. Το περιβάλλον προσομοίωσης διαμορφώθηκε ως εξής:

- Πρωτόκολλο δρομολόγησης DSR
- Μοντέλο απωλειών μονοπατιού two-ray propagation
- Ισχύς μετάδοσης 12dBm
- Κατώφλι SNR 8dB
- Εύρος ζώνης 2Mbps
- Περιοχή 2000 x 2000 m^2
- Κόμβοι 50
- Μέγεθος πακέτου 512 bytes
- Χρονικά διαστήματα ανά στάδιο 20
- Πιθανότητα προώθησης 0.2

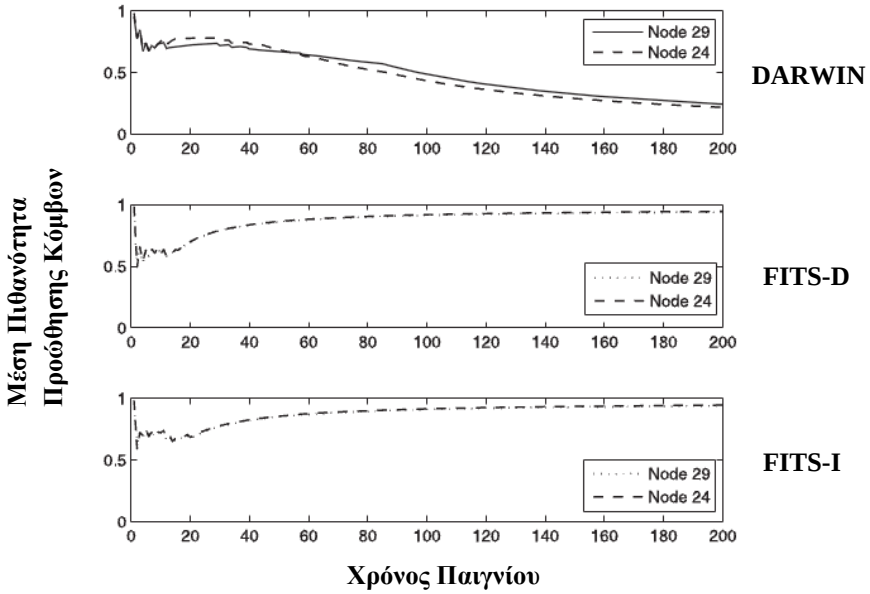
Από τα πειράματα που πραγματοποιήθηκαν από τους δημιουργούς του FITS προέκυψαν τα ακόλουθα συμπεράσματα από τα αντίστοιχα διαγράμματα των προσομοιώσεων:



Διάγραμμα 2.11.1 (Πηγή [11])

Τα παραπάνω διαγράμματα για το σχήμα FITS-D και FITS-I αντίστοιχα με την σειρά που εμφανίζονται, έχουν στον κάθετο άξονα τους ***τη χρησιμότητα u των μη ομαλά συμπεριφερόμενων κόμβων,*** και στον οριζόντιο άξονα ***την πιθανότητα απόρριψης πακέτων των μη ομαλά συμπεριφερόμενων κόμβων***, για τυχαίους κόμβους από τις προσομοιώσεις που πραγματοποιήθηκαν, στους οποίους ανταποκρίνονται οι διάφορες γραμμές των διαγραμμάτων. Παρατηρείται, ότι με τη χρήση των σχημάτων FITS-I και FITS-D, μειώνεται σημαντικά η χρησιμότητα u των μη ομαλά συμπεριφερόμενων κόμβων, όσο αυξάνεται η πιθανότητα απόρριψης πακέτων από αυτούς, πράγμα που σημαίνει ότι το FITS τους τιμωρεί αποτελεσματικά.

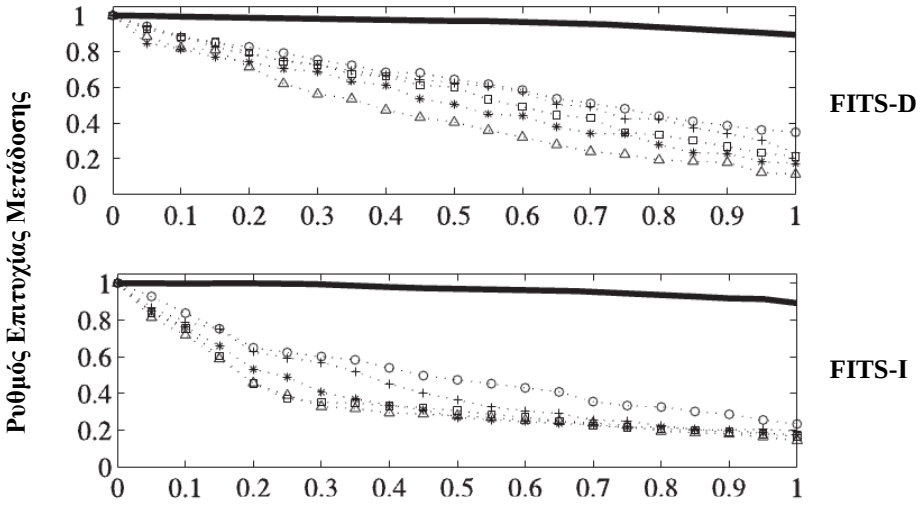
Ακόμα παρήχθησαν τα παρακάτω διαγράμματα που έχουν στον κάθετο άξονα τους ***τη μέση πιθανότητα προώθησης των κόμβων***, και στον οριζόντιο ***τον χρόνο του παιγνίου,*** για δίκτυα που εφαρμόζεται ο μηχανισμός φήμης DARWIN, το σχήμα FITS-D και το σχήμα FITS-I αντίστοιχα με τη σειρά που εμφανίζονται, για δύο τυχαίους κόμβους των δικτύων που προσομοιώθηκαν.



Διάγραμμα 2.11.2 (Πηγή [11])

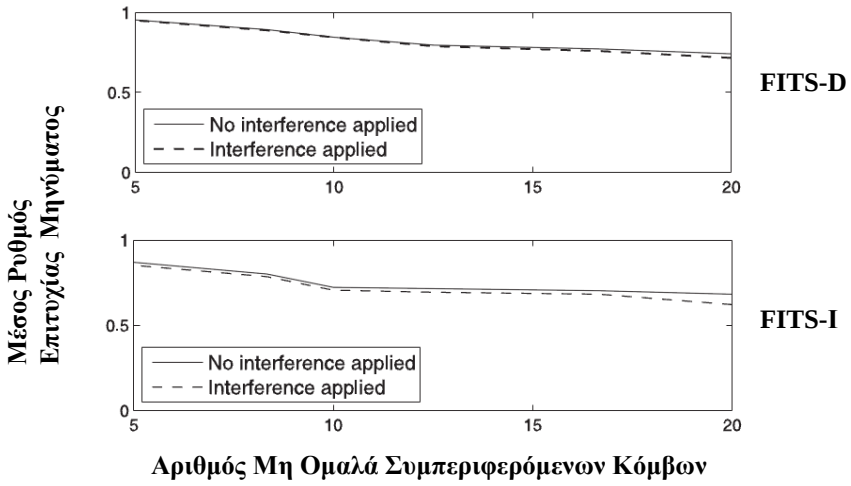
Συμπεραίνεται ότι Η πιθανότητα προώθησης των κόμβων και στα δύο σχήματα του FITS, έχει αυξητική πορεία συναρτήσει του χρόνου, σε σχέση και με τον μηχανισμό φήμης DARWIN, πράγμα που συμβαίνει, καθώς οι κόμβοι πραγματοποιούν όλες τις πιθανές προσπάθειες για να αυξήσουν τη χρησιμότητα u τους, και ανακαλύπτουν ότι δεν μπορούν να το κάνουν απορρίπτοντας πακέτα, με αποτέλεσμα σε όλο το υπόλοιπο πείραμα να επιλέγουν τη στρατηγική σύμφωνα με την οποία προωθούν πακέτα.

Επίσης, από τα παρακάτω διαγράμματα για το σχήμα FITS-D και FITS-I αντίστοιχα με την σειρά που εμφανίζονται, που έχουν στον κάθετο άξονα τους ***το ρυθμό επιτυχίας μετάδοσης***, και στον οριζόντιο ***την πιθανότητα απόρριψης πακέτων από τους μη ομαλά συμπεριφερόμενους κόμβους***, για τυχαίους κόμβους των δικτύων που προσομοιώθηκαν, διαπιστώθηκε ότι ο ρυθμός επιτυχίας της μετάδοσης μηνυμάτων από όλους τους μη ομαλά συμπεριφερόμενους κόμβους μειώνεται γρήγορα, ενώ ο αντίστοιχος των συνεργάσιμων κόμβων, μειώνεται ελάχιστα. Σημειώνεται ότι με τη σκούρα γραμμή αναπαριστώνται τα αποτελέσματα για τους συνεργάσιμους κόμβους.



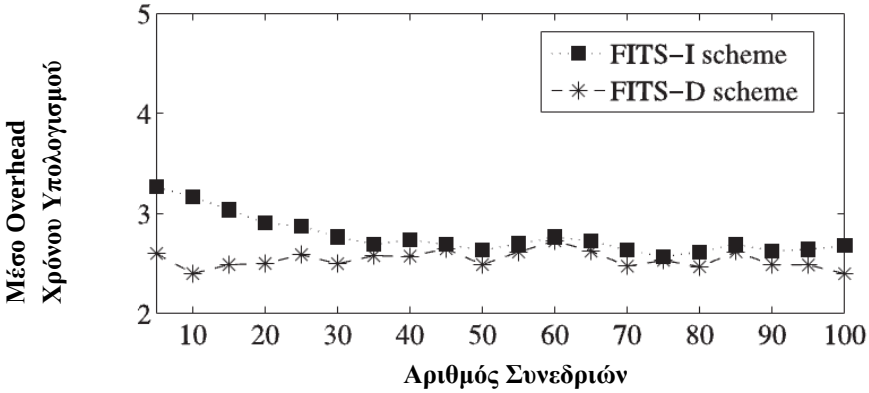
Διάγραμμα 2.11.3 (Πηγή [11])

Τέλος, από το διάγραμμα που ακολουθεί για το σχήμα FITS-D και FITS-I αντίστοιχα με την σειρά που εμφανίζονται, που έχουν στον κάθετο άξονα τους ***το μέσο ρυθμό επιτυχίας μηνύματος***, και στον οριζόντιο ***τον αριθμό των μη ομαλά συμπεριφερόμενων κόμβων***, για την περίπτωση ύπαρξης και μη, λειτουργίας παρεμπόδισης επικοινωνίας, διαπιστώνεται ότι η απώλεια στον μέσο ρυθμό επιτυχίας μετάδοσης μηνυμάτων, μειώνεται λόγω της λειτουργίας παρεμπόδισης επικοινωνίας, σε ελάχιστο βαθμό.



Διάγραμμα 2.11.4 (Πηγή [11])

Συμπεραίνεται επιπλέον από το παρακάτω διάγραμμα ότι και στα δύο σχήματα, το overhead που προκαλείται από την επικοινωνία, είναι αμελητέο σε σχέση με το αντίστοιχο υπολογιστικό. Συγκεκριμένα το διάγραμμα αυτό έχει στον κάθετο άξονα ***το μέσο overhead χρόνου υπολογισμού σε ms/συνεδρία***, και στον οριζόντιο άξονα τον ***αριθμό των συνεδριών*** για τα σχήματα FITS-D και FITS-I αντίστοιχα.



Διάγραμμα 2.11.5 (Πηγή [11])

Συμπερασματικά, το FITS αποτελεί έναν μηχανισμό φήμης που λύνει σε μεγάλο βαθμό το πρόβλημα της προσφοράς κινήτρων για συνεργασία μεταξύ των κόμβων στα ad-ho δίκτυα. Χρησιμοποιεί την θεωρία παιγνίων, για την ανάλυση της διαδικασίας επικοινωνίας σε ένα δίκτυο, και εισάγει δύο υποσχήματα , που με τη χρήση της τεχνικής TTI, τιμωρούν αποτελεσματικά τους μη ομαλά συμπεριφερόμενους κόμβους, αλλά προσφέρουν και κίνητρα για συνεργασία. Η

δημιουργία του FITS ωστόσο, έχει λάβει υπ’ όψη μόνο μια πλευρά των συστημάτων φήμης, και χρειάζεται περαιτέρω μελέτη για την εξέλιξή του και την εφαρμογή σε πραγματικές τοπολογίες δικτύων.

Κεφάλαιο 3

ΚΡΙΣΙΜΑ ΖΗΤΗΜΑΤΑ ΓΙΑ ΤΟΝ ΣΧΕΔΙΑΣΜΟ ΚΑΙ ΣΥΓΚΡΙΣΗ ΤΩΝ ΥΠΑΡΧΟΝΤΩΝ ΣΧΗΜΑΤΩΝ ΦΗΜΗΣ

3.1 ΚΡΙΣΙΜΑ ΖΗΤΗΜΑΤΑ

Το προηγούμενο κεφάλαιο της παρούσας εργασίας, διαπραγματεύτηκε την περιγραφή των πιο δημοφιλών μηχανισμών υποστήριξης συνεργασίας στα ad-hoc δίκτυα, βασιζόμενων στη φήμη. Παρουσιάζουν πλεονεκτήματα και μειονεκτήματα, μελετώντας τα από διαφορετικές σκοπιές και ανάλογα με το επιθυμητό αποτέλεσμα (ακρίβεια στη φήμη, επιβάρυνση στο δίκτυο, βελτίωση της απόδοσης, τιμωρία ή προσφορά κινήτρων συνεργασίας στους κόμβους κ.τ.λ.). Παρατηρείται ότι για τον σχεδιασμό ενός τέτοιου μηχανισμού, απαιτείται να παρθούν αποφάσεις και να πραγματοποιηθούν επιλογές σχετικά με ένα σύνολο κρίσιμων ζητημάτων, απαραίτητων για τη λειτουργία του. Η σύγκριση των μηχανισμών που περιγράφηκαν προκύπτει μέσα από την διάκριση και διαφοροποίησή τους πάνω στα ζητήματα αυτά. Στα υποκεφάλαια που ακολουθούν πραγματοποιείται ανάλυση των κρίσιμων αυτών σημείων και αναδεικνύονται οι βασικές διαφορές των παρουσιασθέντων σχημάτων, ώστε να γίνει σαφής η βασική λογική της λειτουργίας τους, τα θετικά και αρνητικά τους στοιχεία. Παρακάτω αναλύονται με τη σειρά τα βασικότερα ζητήματα.

3.1.1 ΧΡΗΣΙΜΟΠΟΙΟΥΜΕΝΗ ΠΛΗΡΟΦΟΡΙΑ ΣΤΗΝ ΑΡΧΙΤΕΚΤΟΝΙΚΗ ΣΧΗΜΑΤΟΣ

Μια βασική επιλογή κατά τον σχεδιασμό ενός μηχανισμού υποστήριξης συνεργασίας στα ασύρματα ad-hoc δίκτυα, είναι ο τύπος της πληροφορίας που θα χρησιμοποιηθεί, για την δημιουργία σε κάθε κόμβο, της άποψης του για τους υπόλοιπους κόμβους που συμμετέχουν στην επικοινωνία, ή με άλλα λόγια, για τη φήμη τους. Κάποιοι μηχανισμοί επιλέγουν τη χρήση μόνο first – hand πληροφορίας, είτε αυτή προκύπτει από την άμεσα εμπειρία του κόμβου, είτε από την παρατήρηση της συμπεριφοράς άλλων κόμβων στο δίκτυο, ενώ άλλοι επιλέγουν επιπλέον και τη χρήση της second – hand πληροφορίας, της πληροφορίας φήμης δηλαδή που μεταδίδεται από τους υπόλοιπους κόμβους. Η αξιοποίηση μόνο της first-hand πληροφορίας, βοηθάει από τη μια σε έναν πιο απλό σχεδιασμό και σε μικρότερη επιβάρυνση στο δίκτυο, όμως από την άλλη δεν αξιοποιείται όλη η διατιθέμενη πληροφορία που υπάρχει στο δίκτυο, με αποτέλεσμα η αναγνώριση και τιμωρία των μη ομαλά συμπεριφερόμενων κόμβων, να πραγματοποιείται με πιο αργούς ρυθμούς και με μικρότερη ακρίβεια. Αντίθετα, μηχανισμοί που χρησιμοποιούν συν τοις άλλοις, και second-hand πληροφορία, αξιοποιούν την εμπειρία των κόμβων όλου του δικτύου, με αποτέλεσμα η εκτίμηση της συμπεριφοράς κάθε κόμβου να πραγματοποιείται με μεγαλύτερη ακρίβεια, και ταχύτερα, ώστε ένας μη ομαλά συμπεριφερόμενος κόμβος να μην προλάβει να επηρεάσει τις λειτουργίες και την επικοινωνίας στο δίκτυο σε μεγάλο βαθμό. Η ανταλλαγή βέβαια της second-hand πληροφορίας με επιπρόσθετα μηνύματα και πακέτα πληροφορίας φήμης, επιβαρύνει αρκετά το δίκτυο, αυξάνει το συνολικό overhead. Έγκειται σε πειραματικές μετρήσεις κατά πόσο είναι προτιμότερο για την απόδοση του δικτύου, να είναι πιο επιβαρυμένο από άποψη φόρτου, ή να υποφέρει σε μεγαλύτερο βαθμό ή για μεγαλύτερο χρονικό διάστημα από τις μη επιθυμητές ενέργειες κακόβουλων ή μη ομαλά συμπεριφερόμενων κόμβων. Η συγκεκριμένη επιλογή για τους μηχανισμούς που περιγράφηκαν, φαίνεται στον παρακάτω πίνακα.

ΣΧΗΜΑ	ΧΡΗΣΙΜΟΠΟΙΟΥΜΕΝΗ ΠΛΗΡΟΦΟΡΙΑ	
	FIRST-HAND	SECOND-HAND
CONFIDANT	†	†
IM. CONFIDANT	†	†
SORI	†	†
CORE	†	†
OCEAN	†	-
WATCHDOG - PATHRATER	†	†
LARS	†	-
E-HERMES	†	†
LRM	†	†
E.R.B.M.	†	†
FITS	†	-

Πίνακας 3.1.1

3.1.2 ΜΕΤΑΔΟΣΗ ΠΛΗΡΟΦΟΡΙΩΝ ΦΗΜΗΣ

Όπως αναφέρθηκε τα περισσότερα σχήματα υποστήριξης συνεργασίας στα ad-hoc δίκτυα, χρησιμοποιούν και second-hand πληροφορία. Η μετάδοση της πληροφορίας αυτής ποικίλει σε μορφές και τρόπους, και αποτελεί βασικό στοιχείο διαφοροποίησης των διάφορων μηχανισμών. Κατά την απόφαση για τον τρόπο με τον οποίο θα πραγματοποιηθεί η μετάδοση, προσδιορίζεται σε ποιους κόμβους θα μεταδοθεί η πληροφορία φήμης. Οι κόμβοι αυτοί, μπορεί να είναι είτε οι γειτονικοί κόμβοι ενός κόμβου, είτε κόμβοι σε ένα συγκεκριμένο μονοπάτι δρομολόγησης, είτε κόμβοι αποθηκευμένοι σε μια λίστα «φίλων» σε κάθε κόμβο, είτε και σε όλους τους κόμβους του δικτύου. Η επιλογή αυτή εξαρτάται από τον τρόπο λειτουργίας του πρωτοκόλλου, αλλά και από παράγοντες όπως η επιθυμία για ελαχιστοποίηση της επιβάρυνσης στο δίκτυο και η εμπιστοσύνη μεταξύ των κόμβων. Για το λόγο αυτό είναι σπάνιο φαινόμενο η πληροφορία φήμης να μεταδίδεται σε όλους τους κόμβους ενός δικτύου, ενώ πιο συχνά συναντάται η μετάδοση στη «γειτονιά» ή σε μια λίστα με φιλικούς κόμβους, που περιορίζουν τη μετάδοση στους κόμβους με τους οποίους ο κόμβος που μεταδίδει, έχει άμεση επαφή και ανταλλάσει πιο συχνά δεδομένα. Ένας άλλος κρίσιμος παράγοντας για τη μετάδοση πληροφορίας φήμης, είναι ο χρονική στιγμή αποστολής της πληροφορίας. Η αποστολή μπορεί να εκκινήσει αμέσως με την

αναγνώριση μιας μη ομαλής συμπεριφοράς, να πραγματοποιείται σε συγκεκριμένα χρονικά διαστήματα ή μετά από την πάροδο συγκεκριμένου αριθμού γεγονότων, ή όταν η βαθμολογία φήμης ενός κόμβου είναι κάτω από ένα ορισμένο κατώφλι ή το υπερβαίνει. Η αποστολή μπορεί ακόμα να γίνεται και ταυτόχρονα με την διαδικασία αναζήτησης διαδρομής δρομολόγησης. Η διαφορά στον χρόνο εκκίνησης αποστολής πληροφορίας φήμης, έγκειται στην επιλογή της γρήγορης ενημέρωσης του δικτύου για την μη ομαλή συμπεριφορά ενός κόμβου, που ενέχει τον κίνδυνο αναξιοπιστίας, ή από την άλλη πλευρά, της πιο εμπεριστατωμένης απόδειξης μιας μη ομαλής συμπεριφοράς που χρειάζεται περισσότερο χρόνο για να παραχθεί, αποφεύγοντας όμως τις περιπτώσεις συμπτώσεων όπως η σύγκρουση πακέτων. Τέλος, ποικιλία υπάρχει και στη μορφή της μεταδιδόμενης πληροφορίας ,που μπορεί να αποτελείται είτε από μηνύματα προειδοποίησης ALARM-WARNING για μια μη ομαλή συμπεριφορά, από θετικές και αρνητικές πληροφορίες σχετικές με τη φήμη, αλλά και από βαθμολογίες φήμης, και ενσωματωμένες πληροφορίες φήμης στη δρομολόγηση. Τα μηνύματα ALARM δεν μπορούν να περιέχουν θετικές πληροφορίες για την φήμη ενός κόμβου, και κυρίως αποτελούν απλές αναφορές για την μη ομαλή συμπεριφορά και την ταυτότητα του κόμβου που την κατέχει, ενώ οι άλλες μορφές παρέχουν πιο σαφή εικόνα για τη συμπεριφορά ενός κόμβου και την αξιοπιστία του για την επιλογή του σε μια διαδρομή δρομολόγησης αλλά αυξάνουν το overhead. Τα ζητήματα αυτά εντοπίζονται στα πρωτόκολλα που μελετήθηκαν όπως φαίνεται στους τρεις παρακάτω υποπίνακες.

ΣΧΗΜΑ	**ΜΕΤΑΔΟΣΗ ΠΛΗΡΟΦΟΡΙΑΣ ΦΗΜΗΣ**					
	1. ΚΟΜΒΟΙ ΟΠΟΥ ΓΙΝΕΤΑΙ Η ΜΕΤΑΔΟΣΗ					
	ΚΑΝΕΙΣ	**ΓΕΙΤΟΝΙΚΟΙ**	**ΠΗΓΗ ΜΟΝΟΠΑΤΙΟΥ**	**ΛΙΣΤΑ ΦΙΛΩΝ**	**ΟΛΟ ΤΟ ΔΙΚΤΥΟ**	**ΜΟΝΟΠΑΤΙ**
CONFIDANT	-	-	-	†	-	-
IM. CONFIDANT	-	-	-	†	-	-
SORI	-	†	-	-	-	-
CORE	-	†	-	-	-	-
OCEAN	†	-	-	-	-	-
WATCHDOG-PATHRATER	-	-	†	-	-	-
LARS	-	-	-	-	-	-
E-HERMES	-	-	-	†	-	-
LRM	-	†	-	-	-	-
E.R.B.M.	-	-	-	-	-	†
FITS	†	-	-	-	-	-

Πίνακας 3.1.2

ΣΧΗΜΑ	ΜΕΤΑΔΟΣΗ ΠΛΗΡΟΦΟΡΙΑΣ ΦΗΜΗΣ				
	2. ΧΡΟΝΙΚΗ ΣΤΙΓΜΗ ΕΚΚΙΝΗΣΗΣ ΜΕΤΑΔΟΣΗΣ				
	ΜΟΛΙΣ ΑΝΑΓΝΩΡΙΣΤΕΙ ΜΗ-ΟΜΑΛΗ ΣΥΜΠΕΡΙΦΟΡΑ	ΣΥΓΚΕΚΡΙΜΕΝΑ ΧΡΟΝΙΚΑ ΔΙΑΣΤΗΜΑΤΑ	ΜΕ ΤΟ ΠΕΡΑΣ ΣΥΓΚΕΚΡΙΜΕΝΟΥ ΑΡΙΘΜΟΥ ΓΕΓΟΝΟΤΩΝ	ΟΤΑΝ Η ΦΗΜΗ ΞΕΠΕΡΑΣΕΙ ΕΝΑ ΚΑΤΩΦΛΙ	ΚΑΤΑ ΤΗ ΔΡΟΜΟΛΟ-ΓΗΣΗ
CONFIDANT	-	-	-	†	-
IM. CONFIDANT	-	†	-	-	-
SORI	-	-	-	†	-
CORE	-	†	-	-	-
OCEAN	-	-	-	-	-
WATCHDOG-PATHRATER	-	-	†	-	-
LARS	-	-	-	-	-
E-HERMES	-	-	-	†	-
LRM	-	-	-	†	-
E.R.B.M.	-	-	-	-	†
FITS	-	-	-	-	-

Πίνακας 3.1.3

ΣΧΗΜΑ	ΜΕΤΑΔΟΣΗ ΠΛΗΡΟΦΟΡΙΑΣ ΦΗΜΗΣ			
	3. ΜΟΡΦΗ ΠΛΗΡΟΦΟΡΙΑΣ ΦΗΜΗΣ			
	ALARM-WARNING	ΣΧΕΤΙΖΟΜΕΝΕΣ ΜΕ ΦΗΜΗ ΠΛΗΡΟΦΟΡΙΕΣ	ΒΑΘΜΟΛΟΓΙΕΣ ΦΗΜΗΣ	ΕΝΣΩΜΑΤΩΜΕΝΗ ΣΕ ΜΗΝΥΜΑΤΑ ΔΡΟΜΟΛΟΓΗΣΗΣ
CONFIDANT	†	-	-	-
IM. CONFIDANT	-	-	†	-
SORI	-	-	†	-
CORE	-	-	†	-
OCEAN	-	-	-	-
WATCHDOG-PATHRATER	†	-	-	-
LARS	-	-	-	-
E-HERMES	-	†	-	-
LRM	†	-	-	-
E.R.B.M.	-	-	-	†
FITS	-	-	-	-

Πίνακας 3.1.4

3.1.3 ΤΡΟΠΟΣ ΤΙΜΩΡΙΑΣ ΚΑΙ ΕΠΑΝΕΝΤΑΞΗ

Οι διάφοροι μηχανισμοί υποστήριξης συνεργασίας έχουν επιλέξει διαφορετικές μορφές τιμωρίας για τους μη ομαλά συμπεριφερόμενους ή κακόβουλους κόμβους. Μια πιο χαλαρή ή μια πιο αυστηρή προσέγγιση μπορεί να επιλεχθεί, είτε για την αποφυγή αιώνιων τιμωριών που μπορεί να προκύψουν από λανθασμένες κατηγορίες και διαπιστώσεις λόγω συμπτώσεων στο δίκτυο, μειώνοντας πάντως την αρνητική επίδραση της μη ομαλής συμπεριφοράς, είτε για την συμμόρφωση των κακόβουλων κόμβων και την προσφορά κινήτρων για βελτίωση της συμπεριφοράς τους αντιστοίχως. Έτσι, η τιμωρία μπορεί να είναι η απομόνωση του μη ομαλά συμπεριφερόμενου κόμβου από το δίκτυο, η άρνηση ή μειωμένη προτεραιότητα στην παροχή υπηρεσιών και η απόρριψη των πακέτων του, είτε από την άλλη η αποφυγή των μη ομαλά συμπεριφερόμενων κόμβων στις διαδρομές δρομολόγησης. Τα περισσότερα σχήματα, εμπεριέχουν μηχανισμούς για την επανένταξη των κόμβων στο δίκτυο και στην επικοινωνία, ώστε να αξιοποιούνται όλες οι δυνατότητες του δικτύου στην επικοινωνία, ώστε να δίνεται η δυνατότητα στους κόμβους να βελτιώσουν τη συμπεριφορά τους έχοντας υποστεί τιμωρία λόγω αρνητικής συμπεριφοράς και να συνεισφέρουν θετικά στην απόδοση του δικτύου. Τα κριτήρια για την επανένταξη ενός κόμβου είναι διαφορετικά σε κάθε μηχανισμό. Ένας κόμβος μετά την τιμωρία του, μπορεί να επανέλθει σε κάποιες περιπτώσεις στο δίκτυο μετά από ένα χρονικό διάστημα αδράνειας, μετά από τη λήξη της επικοινωνίας με έναν άλλο κόμβο, ή μετά από ένα διάστημα ομαλής συμπεριφοράς που μπορεί να τον απαλλάξει από τις κατηγορίες που του είχαν ανατεθεί. Οι προαναφερθείσες επιλογές για τους μηχανισμούς που αναλύθηκαν φαίνονται στους παρακάτω δύο πίνακες.

ΣΧΗΜΑ	ΤΡΟΠΟΣ ΤΙΜΩΡΙΑΣ				
	ΑΠΟΜΟΝΩΣΗ ΑΠΟ ΤΟ ΔΙΚΤΥΟ	ΑΠΟΦΥΓΗ ΑΠΟ ΤΙΣ ΔΙΑΔΡΟΜΕΣ ΔΡΟΜΟΛΟΓΗΣΗΣ	ΑΡΝΗΣΗ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ	ΧΑΜΗΛΗ ΠΡΟΤΕΡΑΙΟΤΗΤΑ ΣΤΗΝ ΠΑΡΟΧΗ ΥΠΗΡΕΣΙΩΝ	ΔΕΝ ΟΡΙΖΕΤΑΙ
CONFIDANT	-	†	†	-	-
IM. CONFIDANT	-	†	†	-	-
SORI		-	†	-	-
CORE	†	-	†	-	-
OCEAN		†	†	-	-
WATCHDOG-PATHRATER	-	†	-	-	-
LARS	-	-	†	-	-
E-HERMES	-	-	-	-	†
LRM	†	-	-		-
E.R.B.M.	-	-	-	†	-
FITS	-	-	†	-	-

Πίνακας 3.1.5

ΣΧΗΜΑ	ΜΗΧΑΝΙΣΜΟΣ ΕΠΑΝΕΝΤΑΞΗΣ			
	ΚΑΝΕΙΣ	ΜΕΤΑ ΑΠΟ ΔΙΑΣΤΗΜΑ ΟΜΑΛΗΣ ΣΥΜΠΕΡΙΦΟΡΑΣ	ΜΕΤΑ ΑΠΟ ΔΙΑΣΤΗΜΑ ΑΔΡΑΝΕΙΑΣ	ΣΕ ΚΑΘΕ ΝΕΑ ΑΛΛΗΛΕΠΙΔΡΑΣΗ
CONFIDANT	-	†	-	-
IM. CONFIDANT	-	†	†	-
SORI	†	-	-	-
CORE	†	-	-	-
OCEAN		-	†	-
WATCHDOG-PATHRATER	-	-	†	-
LARS	-	†	†	-
E-HERMES	†	-	-	-
LRM	†	-	-	-
E.R.B.M.	-	†	-	-
FITS	-	-	-	†

Πίνακας 3.1.6

3.1.4 ΑΡΧΙΚΟΠΟΙΗΣΗ ΤΙΜΩΝ ΦΗΜΗΣ ΓΙΑ ΝΕΟΕΙΣΑΧΘΕΝΤΕΣ ΚΟΜΒΟΥΣ

Όλοι οι μηχανισμοί φήμης που περιγράφηκαν είναι βασισμένοι στη φήμη, και χρησιμοποιούν διαφορετικές μεθόδους για την ανανέωσή τους κατά τη διαδικασία της επικοινωνίας. Ένα κρίσιμο ζήτημα στην διαμόρφωση της φήμης, είναι η αρχική τιμή φήμης που ανατίθεται σε έναν νέο κόμβο όταν αυτός για πρώτη φορά εισάγεται στο δίκτυο, η οποία με την πάροδο του χρόνου ανανεώνεται βάσει των άμεσων ή αποκτημένων από άλλους κόμβους πληροφοριών φήμης. Η αρχική τιμή μπορεί να είναι είτε ουδέτερη, δηλαδή ούτε θετική αλλά ούτε και αρνητική, είτε 0 και να διαμορφώνεται στη συνέχεια με βάση την προωθητική συμπεριφορά του κόμβου, είτε να είναι τυχαία και να εκτείνεται από την μικρότερη δυνατή τιμή μέχρι τη μεγαλύτερη δυνατή τιμή, στη λογική ότι ένας άγνωστος κόμβος μπορεί να έχει οποιουδήποτε είδους συμπεριφορά. Μια ουδέτερη τιμή από τη μία, μπορεί να αδικήσει είτε τους νεοεισαχθέντες κόμβους είτε τους παλαιότερους ανάλογα με το μοντέλο διαμόρφωσης φήμης που χρησιμοποιείται. Μια υψηλή αρχική τιμή προσφέρει κίνητρα για αλλαγή ταυτοτήτων ώστε να απαλλαχθεί η επικοινωνία από πιθανή κακή συμπεριφορά, ενώ μια χαμηλή αρχική τιμή φήμης μεγαλώνει τη δυσκολία για γρήγορα απόκτηση μιας ακριβούς εικόνας σχετικά με τη συμπεριφορά ενός κόμβου. Η αρχική τιμή 0 πάλι, είναι αποδεκτή μόνο στην περίπτωση που δίνονται από το πρωτόκολλο κίνητρα για διατήρηση της ταυτότητας των κόμβων. Η

αρχικοποίηση της φήμης νεοεισαχθέντων κόμβων στα πρωτόκολλα που αναλύθηκαν φαίνεται στον παρακάτω πίνακα.

ΣΧΗΜΑ	ΑΡΧΙΚΗ ΤΙΜΗ ΦΗΜΗΣ			
	ΟΥΔΕΤΕΡΗ	ΤΥΧΑΙΑ ΣΕ ΕΝΑ ΕΥΡΟΣ ΤΙΜΩΝ	ΔΕΝ ΑΝΑΦΕΡΕΤΑΙ	0
CONFIDANT	-	-	†	-
IM. CONFIDANT	†	-	-	-
SORI	-	-	-	†
CORE	†	-	-	-
OCEAN	-	-	-	†
WATCHDOG-PATHRATER	†	-	-	-
LARS	-	†	-	-
E-HERMES	†	-	-	-
LRM	-	†	-	-
E.R.B.M.	†	-	-	-
FITS	-	-	†	-

Πίνακας 3.1.7

3.1.5 ΠΙΣΤΟΠΟΙΗΣΗ ΤΑΥΤΟΤΗΤΑΣ ΔΕΔΟΜΕΝΩΝ

Στους περισσότερους μηχανισμούς υποστήριξης συνεργασίας, δεν χρησιμοποιούνται μηχανισμοί ασφαλείας και πιστοποίησης, καθώς προσθέτουν πολυπλοκότητα αλλά και μεγάλη επιβάρυνση στα ήδη επιβαρυμένα από τους μηχανισμούς φήμης, δίκτυα. Παρόλα αυτά, στα ad-hoc δίκτυα, που κάνουν την εμφάνισή τους κακόβουλοι ή άλλοι μη ομαλά συμπεριφερόμενοι κόμβοι, είναι πολύ πιθανή η πραγματοποίηση επιθέσεων αλλαγής ταυτότητας (όπου ένας κακόβουλος κόμβος προσποιείται έναν κόμβο με καλή φήμη για να προωθήσει τα συμφέροντα του), αλλά και επιθέσεις τροποποίησης δεδομένων, είτε αυτά αποτελούν πραγματικά δεδομένα, είτε μηνύματα επιβεβαίωσης ή προειδοποίησης, απαραίτητα για την εύρυθμη λειτουργία του δικτύου και την αποτελεσματικότητα των σχημάτων υποστήριξης συνεργασίας. Για το λόγο αυτό, κάποια πρωτόκολλα έχουν ενσωματωμένους μηχανισμούς πιστοποίησης ταυτότητας και πιστοποίησης δεδομένων, που χρησιμοποιούν hash αλυσίδες και συναρτήσεις, και κρυπτογραφικές μεθόδους όπως οι ψηφιακές υπογραφές. Ανάλογα με την ιδιότητα τους αυτή, τα σχήματα που περιγράφηκαν φαίνονται παρακάτω.

ΣΧΗΜΑ	ΠΙΣΤΟΠΟΙΗΣΗ		
	ΤΑΥΤΟΤΗΤΑΣ	ΔΕΔΟΜΕΝΩΝ	
	ONE-WAY HASH ΑΛΥΣΙΔΕΣ	HASH ΑΛΥΣΙΔΕΣ	ΨΗΦΙΑΚΕΣ ΥΠΟΓΡΑΦΕΣ
CONFIDANT	-	-	-
IM. CONFIDANT	-	-	-
SORI	†	-	-
CORE	-	-	-
OCEAN	-	-	-
WATCHDOG-PATHRATER	-	-	-
LARS	-	-	†
E-HERMES	-	†	-
LRM	-	-	-
E.R.B.M.	-	-	-
FITS	-	-	-

Πίνακας 3.1.8

3.1.6 ΧΡΟΝΙΚΗ ΒΑΡΥΤΗΤΑ ΣΤΗ ΦΗΜΗ

Πολλοί μηχανισμοί υποστήριξης συνεργασίας στα ad-hoc δίκτυα, δίνουν διαφορετική βαρύτητα στις παρατηρήσεις ανάλογα με την προέλευσή τους χωρικά, αλλά και ανάλογα με τη μορφή των παρατηρήσεων, αν αυτές είναι first-hand ή second-hand. Μια άλλη σημαντική παράμετρος στην οποία διαφοροποιούνται τα διάφορα σχήματα, είναι η απόδοση διαφορετικής βαρύτητας στις παρατηρήσεις ανάλογα με τον χρόνο πραγματοποίησής τους. Έτσι, οι περισσότεροι μηχανισμοί δίνουν ίδιο βάρος σε όλες τις παρατηρήσεις στο χρονικό της επικοινωνίας, παρέχοντας έτσι μια πιο ασφαλή εικόνα σε σχέση με την συμπεριφορά των κόμβων σε όλη τη διαδικασία της επικοινωνίας, και αναγκάζοντας τους κόμβους να βελτιώσουν ή να μειώσουν τη φήμη τους ανάλογα με συμπεριφορά τους όσον αφορά την προώθηση πακέτων καθ' 'όλο αυτό το χρονικό διάστημα. Με τον τρόπο αυτό, κάθε ενέργεια του κόμβου συνεισφέρει ίσα στην διαμόρφωση της φήμης του. Μια άλλη μερίδα μηχανισμών από την άλλη, επιλέγει μέσω συντελεστών χρονικής βαρύτητας, να δίνει μεγαλύτερο βάρος σε παρατηρήσεις που έχουν πραγματοποιηθεί πιο πρόσφατα. Η λογική αυτής της τεχνικής, έγκειται στην δυνατότητα που θέλει να προσδώσει το σχήμα στους κατηγορούμενους για μη ομαλή συμπεριφορά κόμβους για επανένταξη τους στο δίκτυο μετά από την τιμωρία τους, στο σταδιακό ξεθώριασμα της μνήμης ώστε οι κατηγορίες που έχουν απαγγελθεί σε έναν κόμβο να μην μένουν αιώνια. Τέλος, κάποια σχήματα επιλέγουν να δώσουν μεγαλύτερη βαρύτητα σε παρατηρήσεις που έχουν γίνει στο παρελθόν σε σχέση με πιο πρόσφατες, όσον αφορά την προωθητική συμπεριφορά των κόμβων. Η συγκεκριμένη επιλογή πραγματοποιείται, ώστε να αποφευχθεί η μεγάλη συνεισφορά στη διαμόρφωση της φήμης, σποραδικών μη ομαλών συμπεριφορών ή δυσλειτουργιών ενός κόμβου σε πρόσφατες παρατηρήσεις, που μπορεί να οφείλεται σε συμπτώσεις, όπως οι συγκρούσεις και οι ζεύξεις με βλάβη. Παρακάτω φαίνεται το συγκεκριμένο κρίσιμο ζήτημα, όπως αυτό έχει

επιλεχθεί για τους μηχανισμούς φήμης που περιγράφηκαν. Σημειώνεται ότι στο σχήμα FITS, η ίδια βαρύτητα δίνεται σε όλα τα στάδια μιας αλληλεπίδρασης μεταξύ των κόμβων, ενώ η διαμόρφωση της φήμης ξεκινά από την αρχή για κάθε νέα αλληλεπίδραση.

ΣΧΗΜΑ	ΧΡΟΝΙΚΗ ΒΑΡΥΤΗΤΑ		
	ΙΣΗ ΓΙΑ ΟΛΕΣ ΤΙΣ ΠΑΡΑΤΗΡΗΣΕΙΣ	ΜΕΓΑΛΥΤΕΡΗ ΓΙΑ ΠΡΟΣΦΑΤΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ	ΜΕΓΑΛΥΤΕΡΗ ΓΙΑ ΠΑΡΕΛΘΟΝΤΙΚΕΣ ΠΑΡΑΤΗΡΗΣΕΙΣ
CONFIDANT	†	-	-
IM. CONFIDANT	-	†	-
SORI	†	-	-
CORE	-	-	†
OCEAN	†	-	-
WATCHDOG-PATHRATER	†	-	-
LARS	-	†	-
E-HERMES	†	-	-
LRM	†	-	-
E.R.B.M.	†	-	-
FITS	†	-	-

Πίνακας 3.1.9

3.1.7 ΠΕΡΙΕΧΟΜΕΝΟ ΤΗΣ ΦΗΜΗΣ

Για τους διάφορους μηχανισμούς υποστήριξης συνεργασίας, η φήμη των κόμβων μπορεί να υπολογίζεται με διαφορετικούς τρόπους, να λαμβάνει υπόψη διαφορετικούς παράγοντες, να κρατείται από διαφορετικές ομάδες κόμβων. Πιο συγκεκριμένα, η φήμη, ανάλογα με τον τρόπο λειτουργίας του εκάστοτε πρωτοκόλλου, μπορεί να διατηρείται είτε μόνο για γειτονικούς κόμβου του κάθε κόμβου, είτε για όλους τους κόμβους του δικτύου, είτε για μερίδες κόμβων που ο κόμβος επικοινωνεί και γνωρίζει ή τον αφορούν στην επικοινωνία. Όσο μεγαλύτερος είναι ο αριθμός των κόμβων για τους οποίους διατηρεί τιμές φήμης ένας κόμβος, τόσο πιο πολύπλοκη και χρονοβόρα είναι η διαδικασία διαμόρφωσης της φήμης, ενώ είναι και πιο επιβαρυντική όσον αφορά τις αποθηκευτικές ανάγκες και εύρος ζώνης. Διατήρηση τιμών για περισσότερους κόμβους από την άλλη, δίνει σαφή εικόνα για ολόκληρο το δίκτυο, που μπορεί να βοηθάει στην διαδικασία της δρομολόγησης. Η διάκριση αυτή για τα πρωτόκολλα που περιγράφηκαν φαίνεται παρακάτω.

ΣΧΗΜΑ	ΔΙΑΤΗΡΗΣΗ ΤΙΜΩΝ ΦΗΜΗΣ ΚΟΜΒΟΥ				
	ΓΙΑ ΤΟΥΣ ΓΕΙΤΟΝΙΚΟΥΣ ΚΟΜΒΟΥΣ	ΓΙΑ ΜΕΡΙΔΑ ΚΟΜΒΩΝ ΠΟΥ ΤΟΝ ΑΦΟΡΟΥΝ	ΓΙΑ ΤΟΥΣ ΚΟΜΒΟΥΣ ΠΟΥ ΓΝΩΡΙΖΕΙ	ΓΙΑ ΟΛΟΥΣ ΤΟΥΣ ΚΟΜΒΟΥΣ ΣΤΟ ΔΙΚΤΥΟ	ΔΕΝ ΑΝΑΦΕΡΕΤΑΙ
CONFIDANT	-	-	-	-	†
IM. CONFIDANT	-	†	-	-	-
SORI	†	-	-	-	-
CORE	†	-	-	-	-
OCEAN	†	-	-	-	-
WATCHDOG-PATHRATER	-	-	†	-	-
LARS	†	-	-	-	-
E-HERMES	-	-	-	†	-
LRM	†	-	-	-	-
E.R.B.M.	†	-	-	-	-
FITS	-	-	†	-	-

Πίνακας 3.1.10

Ένα άλλο κρίσιμο ζήτημα διαφοροποίησης των σχημάτων ως προς τη διαμόρφωση της φήμης και το περιεχόμενό της, είναι οι παράγοντες που λαμβάνει υπόψη το πρωτόκολλο για τον υπολογισμό της. Πιο συγκεκριμένα μπορεί η φήμη να υπολογίζεται λαμβάνοντας υπόψη την συμπεριφορά του κόμβου ως προς την προώθηση πακέτων, ως προς τη διαδικασία τη δρομολόγησης, ή ως προς άλλες λειτουργίες. Στην παρούσα διάκριση, θεωρείται στην εργασία, ότι σε ένα πρωτόκολλο κατά το οποίο ελέγχεται η προωθητική συμπεριφορά ενός κόμβου και με βάση αυτή δημιουργούνται βαθμολογίες φήμης για τις εκάστοτε διαδρομές δρομολόγησης, υπάρχει εμπλοκή και των δύο λειτουργιών στη φήμη. Από τη μία, η εξάρτηση της φήμης από διαφορετικές λειτουργίες, καθιστά πολύπλοκη τη δημιουργία καθολικής φήμης για κάθε κόμβο, ενώ αν η συνολική φήμη υπολογίζεται συναθροίζοντας τις φήμες ενός κόμβου που αφορούν διαφορετικές λειτουργίες, ένα κόμβος μπορεί να κρύψει τη μη ομαλή συμπεριφορά του όσον αφορά κάποια λειτουργία. Αντιθέτως μια τιμή φήμης που αναπαριστά συνολικά τη συμπεριφορά ενός κόμβου στο δίκτυο, χωρίς να διαχωρίζεται σε επιμέρους λειτουργίες, είναι μια πιο απλή λύση που καταναλώνει λιγότερους πόρους. Εξάλλου η αντιμετώπιση μιας μη ομαλής συμπεριφοράς για ένα σχήμα, θα είναι παρόμοια, ανεξάρτητα από τη μορφή της δυσλειτουργίας. Στον παρακάτω πίνακα φαίνεται η επιλογή αυτή για τα υπό μελέτη σχήματα.

ΣΧΗΜΑ	ΑΝΑΦΟΡΑ ΠΕΡΙΕΧΟΜΕΝΟΥ ΦΗΜΗΣ		
	ΠΡΟΩΘΗΣΗ ΠΑΚΕΤΩΝ	ΔΙΑΔΙΚΑΣΙΑ ΔΡΟΜΟΛΟΓΗΣΗΣ	ΑΛΛΕΣ ΛΕΙΤΟΥΡΓΙΕΣ
CONFIDANT	†	†	-
IM. CONFIDANT	-	†	†
SORI	†	-	-
CORE	†	†	†
OCEAN	†	-	-
WATCHDOG-PATHRATER	†	-	-
LARS	†	-	-
E-HERMES	†	-	-
LRM	†	†	-
E.R.B.M.	†	-	-
FITS	†	-	-

Πίνακας 3.1.11

3.1.8 ΑΞΙΟΠΙΣΤΙΑ

Όπως αναφέρθηκε, αρκετοί μηχανισμοί υποστήριξης συνεργασίας που βασίζονται στη φήμη, χρησιμοποιούν και μετάδοση second – hand πληροφοριών φήμης, αξιοποιώντας έτσι όλες τις δυνατές πληροφορίες στο δίκτυο, για την ασφαλέστερη εξαγωγή συμπερασμάτων για τη συμπεριφορά των κόμβων και την ανάλογη διαμόρφωση της φήμης τους. Είναι προφανές, ότι όλοι αυτοί οι μηχανισμοί, δίνουν μεγαλύτερο βάρος στις first – hand πληροφορίες στη διαμόρφωση της φήμης, αφού είναι σίγουρα πιο αξιόπιστες, δεν ενέχει ο κίνδυνος μετατροπής ή αλλοίωσης τους, ή και ο κίνδυνος ψευδών αναφορών για τη φήμη κάποιου κόμβου (εκτός βέβαια από την περίπτωση συγκρούσεων στο δίκτυο). Για την εξακρίβωση της αξιοπιστίας των πληροφοριών λοιπόν που μεταδίδονται από τους κόμβους στους υπόλοιπους κόμβους του δικτύου, πολλά σχήματα του είδους, διατηρούν εκτός των πληροφοριών φήμης, και τιμές αξιοπιστίας των κόμβων στο δίκτυο, ώστε η επιρροή στη φήμη, να είναι πιο έγκυρη. Με άλλα λόγια, με τη χρήση της αξιοπιστίας, οι second – hand πληροφορίες που μεταδίδει ένας λιγότερο αξιόπιστος κόμβος, επηρεάζουν λιγότερο τη φήμη από τις second – hand πληροφορίες που μεταδίδει ένας περισσότερο αξιόπιστος κόμβος. Μπορεί να εξαχθεί το συμπέρασμα, ότι από τη μια, με τη χρήση της αξιοπιστίας μεγαλώνει σε μεγάλο βαθμό η ακρίβεια στην διαμόρφωση της φήμης των κόμβων, ενώ από την άλλη επιφέρεται αύξηση της πολυπλοκότητας στους μηχανισμούς και της επιβάρυνσης στο δίκτυο. Στον παρακάτω πίνακα φαίνεται η διάκριση των

μηχανισμών υποστήριξης συνεργασίας που βασίζονται στη φήμη, με γνώμονα την χρήση ή όχι αξιοπιστίας.

ΣΧΗΜΑ	ΧΡΗΣΗ ΑΞΙΟΠΙΣΤΙΑΣ	
	NAI	OXI
CONFIDANT	-	†
IM. CONFIDANT	†	-
SORI	†	-
CORE	-	†
OCEAN	-	-
WATCHDOG-PATHRATER	-	†
LARS	-	-
E-HERMES	†	-
LRM	-	†
E.R.B.M.	-	†
FITS	-	-

Πίνακας 3.1.12

Κεφάλαιο 4

ΜΗΧΑΝΙΣΜΟΙ ΥΠΟΣΤΗΡΙΞΗΣ ΣΥΝΕΡΓΑΣΙΑΣ ΒΑΣΙΖΟΜΕΝΟΙ ΣΤΙΣ ΠΙΣΤΩΣΕΙΣ

Οι μηχανισμοί υποστήριξης συνεργασίας που βασίζονται στις πιστώσεις, λειτουργούν με διαφορετικό τρόπο από ότι οι μηχανισμοί φήμης. Εδώ, η συνεργασία των κόμβων πετυχαίνεται δίνοντας τους οικονομικά κίνητρα για την παροχή υπηρεσιών. Με λίγα λόγια, οι κόμβοι οι οποίοι προωθούν τα πακέτα των υπολοίπων αποκτούν πιστώσεις που τους βοηθούν να προωθήσουν τα δικά τους πακέτα, ενώ κόμβοι οι οποίοι δε συμβάλουν στη διαδικασία της επικοινωνίας, σταδιακά απομονώνονται εφόσον μείνουν δίχως πιστώσεις για να εξυπηρετήσουν τα δικά τους συμφέροντα στην επικοινωνία. Όπως παρατηρείται, και μηχανισμοί του ίδιου είδους, παρουσιάζουν ιδιαιτερότητες και διακρίνονται σε μια σειρά ζητήματα. Παρακάτω αναλύεται ο τρόπος λειτουργίας των γνωστότερων μηχανισμών πιστώσεων, τα αποτελέσματα που προέκυψαν από τα πειράματα πάνω στη λειτουργία τους, και η αποτελεσματικότητα στην υποστήριξη της συνεργασίας και την επιρροή τους στην απόδοση των δικτύων.

4.1 NUGLETS

Ο μηχανισμός υποστήριξης συνεργασίας για ad-hoc δίκτυα, Nuglets [12], αποτελεί ένα από τα βασικότερα σχήματα υποστήριξης συνεργασίας βασισμένων σε πιστώσεις, σε χρέωση της προσφερόμενης υπηρεσίας στους κόμβους. Στον μηχανισμό αυτό, εισάγεται η έννοια ενός εικονικού νομίσματος, των nuglets, και μηχανισμοί χρέωσης και επιβράβευσης για την προσφερόμενη υπηρεσία. Για να επιτευχθεί λοιπόν επικοινωνίας μεταξύ των κόμβων, τα nuglets είναι απαραίτητα, και για το λόγο αυτό κάθε κόμβος ενδιαφέρεται να αυξάνει συνεχώς τον αριθμό των nuglets που έχει στην κατοχή του. Ένας τρόπος για την απόκτηση nuglets, είναι η παροχή υπηρεσιών για τους άλλους κόμβους. Κάτι τέτοιο προτρέπει τους κόμβους να συνεργαστούν, ενώ παράλληλα τους ενθαρρύνει να χρησιμοποιούν το δίκτυο με φειδώ, καθώς και να διατηρούν σε λειτουργία τις συσκευές τους με σκοπό την εξυπηρέτηση άλλων κόμβων, ακόμα και αν δεν περιμένουν κάποιο πακέτο τη συγκεκριμένη χρονική στιγμή. Το σχήμα Nuglets, έχει στόχο την ενίσχυση της παροχής μιας στγκεκριμένης υπηρεσίας, της προώθησης πακέτων, ενώ μπορεί θεωρητικά να χρησιμοποιηθεί σε συνδυασμό με οποιονδήποτε αλγόριθμο δρομολόγησης.

4.1.1 ΜΟΝΤΕΛΑ ΧΡΕΩΣΗΣ

Η προώθηση πακέτων, αποτελεί μια υπηρεσία που εκτελείται από ενδιάμεσουε κόμβους προς όφελος της πηγής και του παραλήπτη ενός πακέτου. Έτσι, το μοντέλο χρέωσης της υπηρεσίας μπορεί να επιβαρύνει είτε τον αποστολέα είτε τον παραλήπτη. Με βάση την διαφοροποίηση αυτήν, είναι δυνατή η χρήση τριών διαφορετικών χρεωστικών μοντέλων:

1. Το μοντέλο ***PPM(Packet Purse Model)***, όπου υλοποιείται η πρώτη περίπτωση, χρεώνεται δηλαδή η πηγή του πακέτου για την υπηρεσία της προώθησης. Η χρέωση των κόμβων που προωθούν το πακέτο γίνεται ως εξής: Με την αποστολή του πακέτου, η πηγή φορτώνει το πακέτο με έναν αριθμό nuglets αρκετό ώστε να φτάσει στον προορισμό, καθώς κάθε ενδιάμεσος κόμβος που προωθεί το πακέτο, χρειάζεται έναν αριθμό nuglets ως κόστος προώθησης. Ο αριθμός των nuglets που χρειάζεται κάθε ενδιάμεσος κόμβος μπορεί να

εξαρτάται από την ποσότητα ενέργειας που σπαταλά για την προώθηση του πακέτου, από την κατάσταση της μπαταρίας την εκάστοτε στιγμή και τον αριθμό των nuglets που διαθέτει σε αυτήν. Στην περίπτωση που το πακέτο δεν διαθέτει αρκετά nuglets ώστε να προωθηθεί, απορρίπτεται. Το συγκεκριμένο μοντέλο χρέωσης, έχει το πλεονέκτημα ότι πέρα από την ενίσχυση της συνεργασίας των κόμβων, τους αποτρέπει από την αποστολή άχρηστων δεδομένων, πράγμα που συμβάλλει στην εξοικονόμηση bandwidth. Δυσκολία παρουσιάζεται στην εκτίμηση του αριθμού των πακέτων που απαιτούνται για να φτάσει το πακέτο στον προορισμό. Χρειάζεται ιδιαίτερη προσοχή καθώς εάν ο αρχικός αριθμός των nuglets δεν είναι αρκετός, το πακέτο μπορεί να χαθεί, επομένως είναι καλό ο αρχικός αριθμός να είναι λίγο μεγαλύτερος από ότι χρειάζονται, και αν περισσέψουν nuglets να μένουν στον προορισμό. Ωστόσο κάτι τέτοιο πρέπει να γίνεται με φειδώ, ώστε σε περίπτωση που το πακέτο χαθεί σε έναν ενδιάμεσο κόμβο με γεμάτη μνήμη, να μην υπάρχει τεράστια απώλεια nuglets.

2. Το μοντέλο ***PTM(Packet Trade Model)***, στο οποίο το πακέτο δεν τροφοδοτείται από την αρχή με nuglets αλλά αγοράζεται για κάποιον αριθμό nuglets από τους ενδιάμεσους κόμβους (εκτός από τον πρώτο μετά την πηγή που το παίρνει δωρεάν). Έτσι, κάθε ενδιάμεσος κόμβος αγοράζει το πακέτο από τον προηγούμενο για κάποια nuglets, και το πουλάει στον επόμενο για περισσότερα. Με τον τρόπο αυτό κάθε ενδιάμεσος κόμβος που προσφέρει υπηρεσίες προώθησης, αυξάνει τον αριθμό των nuglets του ενώ το το συνολικό κόστος μεταφοράς καλύπτεται από τον προορισμό. Στην περίπτωση που κάποιος ενδιάμεσος κόμβος δεν προτίθεται να αγοράσει το πακέτο, ο προηγούμενος έχει τη δυνατότητα να το πουλήσει σε χαμηλότερη τιμή, να επιλέξει κάποιον άλλο επόμενο κόμβο, ή να το απορρίψει. Το κύριο πλεονέκτημα του συγκεκριμένου μοντέλου είναι ότι η πηγή αποστολής δεν χρειάζεται να γνωρίζει από την αρχή τον αριθμό των nuglets που απαιτούνται για τη μεταφορά, ενώ η ανάληψη του κόστους από τον προορισμό, επιτρέπει την πολυδιανομή πακέτων. Αντίθετα στα μειονεκτήματα συγκαταλέγεται η μη πρόληψη της υπερφόρτωσης του δικτύου.

3. Το ***υβριδικό μοντέλο*** που συνδυάζει τα δύο προαναφερθέντα μοντέλα χρέωσης. Σύμφωνα με αυτό, το πακέτο αρχικά τροφοδοτείται με κάποια nuglets, και συνεχίζει να χρησιμοποιείται το PPM, μέχρι αυτά να τελειώσουν. Μόλις συμβεί αυτό, χρησιμοποιείται το PTM, μέχρι και την αγορά του πακέτου από τον προορισμό. Έτσι, αξιοποιούνται τα πλεονεκτήματα και των δύο πρώτων χρεωστικών μοντέλων: από τη μία η πηγή από τη στιγμή που απαιτείται να τροφοδοτήσει το πακέτο με nuglets θα αποφύγει την αποστολή άχρηστων πληροφοριών, ενώ από την άλλη δεν δημιουργείται πρόβλημα αν υποτιμήσει τον απαιτούμενο αριθμό nuglets, αφού το πακέτο δεν πρόκειται να απορριφθεί.

Για την χρήση των μοντέλων αυτών, πρέπει να λαμβάνεται υπόψιν και η ανάλογη προστασία από επιθέσεις όπως: η παράνομη τροποποίηση του πακέτου κατά τη μετάδοση, η αποκόλληση των nuglets από το πακέτο και η χρήση τους για την αποστολή άλλου πακέτου, η εξασφάλιση ότι ένας κόμβος επιβραβεύεται (ή χρεώνεται αντίστοιχα) με nuglets, μόνο στην περίπτωση που προωθεί το πακέτο.

4.1.1.1 ΕΠΕΚΤΑΣΕΙΣ ΤΟΥ PPM

Ο παρών μηχανισμός Nuglets, χρησιμοποιεί το μοντέλο χρέωσης PPM, ενώ γίνεται η παραδοχή ότι ο κόμβος πηγή μπορεί να υπολογίσει τον ελάχιστο αριθμό nuglets που απαιτούνται για την μεταφορά του πακέτου, βασιζόμενος στους παράγοντες που προαναφέρθηκαν (απαιτούμενη ενέργεια, μπαταρία κ.λ.π.). Για την αντιμετώπιση του ενδεχόμενου προβλήματος, ένας ενδιάμνεσος κόμβος να απαιτεί όλο το περιεχόμενο σε nuglets του πακέτου για να το προωθήσει, έχουν προστεθεί δύο επεκτάσεις στο βασικό μοντέλο PPM:

- Το ***PPM με καθορισμένες χρεώσεις ανά βήμα.*** Στην προσέγγιση αυτή, η πηγή πέρα από τα nuglets, τοποθετεί στο πακέτο και έναν ακριβή αριθμό u, που αναπαριστά τον αριθμό nuglets, που με τη βοήθεια ενός μηχανισμού προστασίας, θα παίρνει κάθε ενδιάμεσος κόμβος για την προώθηση του πακέτου. Ο αριθμός των απαιτούμενων nuglets, δεν εξαρτάται από τους προαναφερθέντες παράγοντες, αλλά ο κάθε ενδιάμεσος κόμβος έχει τη δυνατότητα να μην προωθήσει το πακέτο αν κρίνει ότι η προώθηση δεν είναι συμφέρουσα για αυτόν. Η συγκεκριμένη προσέγγιση είναι απλή στην υλοποίηση, ενώ μπορεί να εφαρμοστεί πάνω σε οποιονδήποτε αλγόριθμο δρομολόγησης όπως ο DSR και ο AODV, ενώ το μειονέκτημά του έγκειται στην πιθανότητα κάποιος κόμβος να απαιτήσει περισσότερα nuglets από την προκαθορισμένη τιμή με αποτέλεσμα να απορριφθεί το πακέτο. Κάτι τέτοιο, μπορεί να αντιμετωπιστεί μέσω μηχανισμών ελέγχου των απαιτήσεων των κόμβων, αλλά και από το ίδιο το ενδιαφέρον των κόμβων να συμμετέχουν στις διαδρομές δρομολόγησης ώστε να αποκτούν nuglets.
- Το ***PPM με δημοπρασίες.*** Στην επέκταση αυτή, κάθε κόμβος που προωθεί πακέτο συμπεριλαμβανομένης και της πηγής, πραγματοποιεί μια δημοπρασία σφραγισμένης προσφοράς. Οι προσφέροντες κόμβοι, είναι οι πιθανοί επόμενοι στη σειρά κόμβοι προς τον προορισμό. Κάθε προσφέρων κόμβος b_i, προσδιορίζει μια τιμή p_i, για την οποία προτίθεται να προωθήσει το πακέτο, και την αποστέλλει στον προωθούντα κόμβο σε σφραγισμένη μορφή. Όταν ο δεύτερος συλλέξει όλες τις προσφορές και διαπιστώνει τον νικητή της δημοπρασίας, που είναι ο προσφέρων κόμβος b_j, με την χαμηλότερη προσφορά $p_j = \min_i p_i$. Στην συνέχεια ο προωθών κόμβος τοποθετεί την τιμή p_k, στο πακέτο, και το αποστέλλει στον b_j, όπου $p_k = \min_{i,i\neq j} p_i$, η δεύτερη χαμηλότερη προσφορά. Με τη βοήθεια ενός προστατευτικού μηχανισμού εξασφαλίζεται ότι ο κόμβος b_j, αποκτά p_k nuglets για να προωθήσει παραπέρα το πακέτο. Βάσει αυτής της προσέγγισης, κάθε προωθών κόμβος ενθαρρύνεται να προσφέρει την μικρότερη δυνατή τιμή για ένα πακέτο, στο βαθμό βέβαια που είναι συμφέρουσα για αυτόν. Με τη μέθοδο αυτήν, όπου επιλέγεται ως επόμενος κόμβος, ο κόμβος που απαιτεί τα λιγότερα nuglets, καταφέρνεται να αποσπώνται το δυνατόν λιγότερα nuglets από το πακέτο, ελαχιστοποιώντας την πιθανότητα αυτό να απορριφθεί λόγω έλλειψης nuglets. Ακόμα εξαρτώντας την απαίτηση των κόμβων σε nuglets από την κατάσταση της μπαταρίας τους, μεγαλώνει ο χρόνος ζωής του δικτύου, αφού η δρομολόγηση και η κατανάλωση μπαταρίας, ισορροπείται μεταξύ των κόμβων. Από την άλλη, η προσέγγιση του PPM με δημοπρασίες, επιβαρύνει το δίκτυο με ανταλλασσόμενα μηνύματα για την πραγματοποίηση των

δημοπρασιών (κάτι που μπορεί να αντιμετωπιστεί με ανταλλαγή προγραμμάτων – πρακτόρων που πραγματοποιούν τη δημοπρασία), ενώ επίσης μπορεί να εφαρμοστεί πάνω σε πρωτόκολλα δρομολόγησης που επιτρέπουν την επιλογή διαφορετικών επόμενων κόμβων, για τον ίδιο προορισμό.

4.1.2 ΜΗΧΑΝΙΣΜΟΙ ΠΡΟΣΤΑΣΙΑΣ

Στον παρόντα μηχανισμό υποστήριξης συνεργασίας με χρήση nuglets, τα nuglets δεν αναπαριστώνται με εικονικά νομίσματα, καθώς μια τέτοια λύση θα απαιτούσε την ύπαρξη μιας αρχής υπεύθυνης για την έκδοση νομισμάτων και την εγκαθίδρυση λογαριασμών για τους χρήστες, καθώς και servers για on-line ή off-line συναλλαγές με την αρχή. Κάτι τέτοιο δεν υλοποιείται εύκολα στα ad-hoc δίκτυα που δεν έχουν μια κεντρική εσωτερική δομή. Για το λόγο αυτό, τα nuglets αναπαριστώνται από μετρητές σε κάθε κόμβο, η τιμή των οποίων αντιπροσωπεύει τον πλούτο του κάθε κόμβο. Για να αποτραπεί η αέναη αύξηση του μετρητή κάθε κόμβου, χρησιμοποιείται ένα αξιόπιστο και μη αλλοιώσιμο εργαλείο hardware, το ***Εργαλείο Ασφαλείας***. Ακόμα για την αποτροπή παράνομων μετατροπών και αποκοπής από το πακέτο, του «πορτοφολιού» που περιέχει τα nuglets, χρησιμοποιούνται κρυπτογραφικές μέθοδοι. Αντίστοιχα, για να εξασφαλιστεί ότι ο κόμβος αποκτά τα απαραίτητα nuglets από το πακέτο, μόνο όταν το προωθήσει, χεσιμοποιούνται πακέτα επιβεβαίωσης που αποστέλλονται από τον επόμενο κόμβο μετά την προώθηση του πακέτου. Ο επόμενος κόμβος ενθαρρύνεται να στέλνει τέτοιες επιβεβαιώσεις αποκτώντας μερικά ακόμα nuglets.

Το **Εργαλείο Ασφαλείας** είναι το μόνο σημείο του κόμβου το οποίο μπορεί κανείς να εμπιστευτεί για σωστή συμπεριφορά, καθώς προμηθεύεται από αξιόπιστο κατασκευαστή και δεν είναι αλλοιώσιμο. Λειτουργεί σαν ένας ασφαλής βοηθητικός επεξεργαστής που υλοποιεί λίγες συγκεκριμένες συναρτήσεις ,ενώ η πλειοψηφία των συναρτήσεων βρίσκονται στον ίδιο τον κόμβο. Με τον τρόπο αυτό, η αλλοίωση των συναρτήσεων στον κόμβο δεν δίναι πλεονεκτήματα στον χρήστη του κόμβου.
Το Εργαλείο Ασφαλείας περιέχει τα εξής δεδομένα:

- Ένα μοναδικό αναγνωριστικό του εργαλείου
- Τον μετρητή των nuglets του κόμβου
- Το ιδιωτικό κλειδί του εργαλείου
- Το πιστοποιητικό δημοσίου κλειδιού του εργαλείου που εκδίδεται από τον κατασκευαστή του
- Τα πιστοποιητικά δημοσίου κλειδιού του εργαλείου όλων των κατασκευαστών που εκδίδονται από τον κατασκευαστή του
- Το δημόσιο κλειδί του κατασκευαστή του εργαλείου ασφαλείας.

Ακόμα, περιέχει έναν πίνακα, κάθε εγγραφή του οποίου αντιστοιχεί σε ένα γειτονικό εργαλείο ασφαλείας που απαρτίζεται από:

- Το **μοναδικό αναγνωριστικό** του γειτονικού εργαλείου στο σύστημα.
- Το **κλειδί συνεδρίας**. Όταν ο κόμβος του εργαλείου ασφαλείας Α, και ο κόμβος ενός εργαλείου ασφαλείας Β, γίνονται γειτονικοί, τρέχουν το πρωτόκολλο γνωριμίας τους, εγκαθιδρύοντας ένα συμμετρικό κλειδί συνεδρίας k_{AB}, το οποίο χρησιμοποιείται για την προστασία του «πορτοφολιού» και των επιβεβαιώσεων των πακέτων που ανταλλάσσονται μεταξύ Α και Β. Η προστασία αυτή βασίζεται σε συμμετρική κρυπτογράφηση

ενώ η εγκαθίδρυση του κλειδιού συνεδρίας βασίζεται σε κρυπτογράφηση δημοσίου κλειδιού.

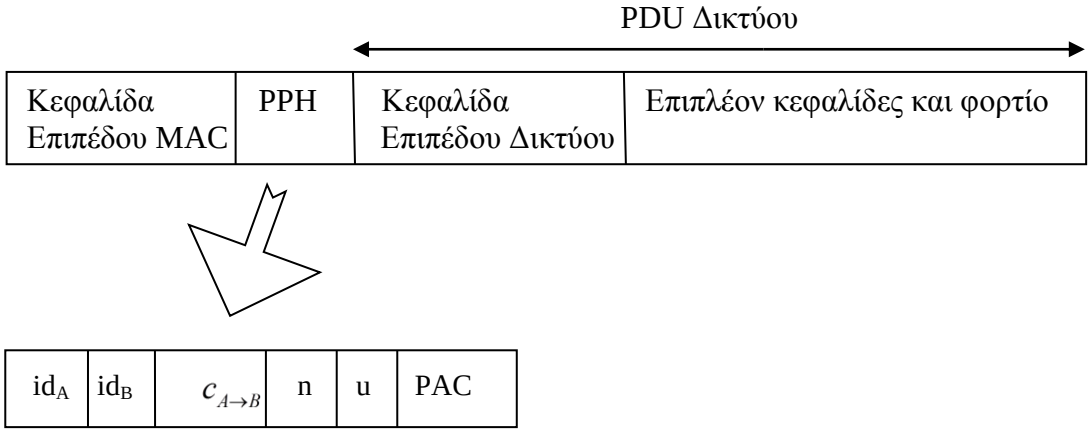
- Τους **αριθμούς ακολουθίας**, που ανταλλάσσονται μεταξύ Α και Β για τον εντοπισμό πορτοφολιών πακέτων που έχουν επαναληφθεί. Ο αριθμός ακολουθίας του Α που σχετίζεται με το Β ορίζεται ως $c_{A\to B}$, ενώ αντίστοιχα ο αριθμός ακολουθίας που λαμβάνει ορίζεται ως $c_{A\leftarrow B}$. Αντίστοιχα για τους αριθμούς ακολουθίας του Β που σχετίζονται με το Α, ορίζονται ως $c_{B\to A}$ και $c_{B\leftarrow A}$. Τα Α και Β αρχικοποιούν τους αριθμούς ακολουθίας τους με τυχαίες τιμές, και μετά το τρέξιμο του πρωτοκόλλου γνωριμίας, τους ορίζουν ως $c_{A\to B}=c_{B\leftarrow A}+1$ και $c_{B\to A}=c_{A\leftarrow B}+1$ αντίστοιχα. Κάθε φορά που το Α αποστέλλει ένα πορτοφόλι πακέτου στο Β, προσθέτει την τρέχουσα τιμή του αριθμού ακολουθίας του στο πορτοφόλι και αυξάνει τον αριθμό. Όταν το Α λαμβάνει ένα πορτοφόλι από το Β, επιβεβαιώνει αν αυτό περιέχει έναν αριθμό ακολουθίας που είναι κατά ένα μεγαλύτερος από τον τρέχοντα αριθμό ακολουθίας λήψης $c_{A\leftarrow B}$. Εάν αυτό συμβαίνει, αποδέχεται το πορτοφόλι και αυξάνει την τιμή του αριθμού ακολουθίας λήψης στην τιμή που λαμβάνει, αλλιώς το απορρίπτει.
- Τον **μετρητή χρέους**. Το Α διατηρεί έναν μετρητή $d_{A\to B}$ που σχετίζεται με το Β, και κρατά την τιμή του χρέους του Α προς το Β. Όταν ο κόμβος του Α προωθεί ένα πακέτο στον κόμβο του Β, το Α δεν αυξάνει τον μετρητή των nuglets του απευθείας, αλλά περιμένει επιβεβαίωση από το Β, ώστε να είναι σίγουρο ότι το πακέτο έχει προωθηθεί. Για να ενθαρρυνθεί ο κόμβος του Β ώστε να στέλνει επιβεβαιώσεις, φιλοδωρείται από το Α με έναν μικρό αριθμό nuglets, αυξάνοντας το $d_{A\to B}$, μόλις φτάσει η επιβεβαίωση. Τα Α και Β μηδενίζουν τα χρέη τους ανα τακτά χρονικά διαστήματα και επανεκινούν το πρωτόκολλο γνωριμίας τους.

4.1.3 ΜΟΡΦΗ ΠΑΚΕΤΟΥ ΠΟΡΤΟΦΟΛΙΟΥ ΚΑΙ ΕΠΙΒΕΒΑΙΩΣΗΣ

Τα nuglets σε κάθε πακέτο που απαιτούνται για την προώθηση του, αποθηκεύονται στην κεφαλίδα πορτοφολιού πακέτου(PPH), μια επιπλέον κεφαλίδας μεταξύ της κεφαλίδας το επιπέδου MAC και του επιπέδου Δικτύου. Το PPH δημιουργείται από το Εργαλείο Ασφαλείας της πηγής, επαναυπολογίζεται από το Εργαλείο Ασφαλείας κάθε κόμβου που προωθεί το πακέτο, και προστατεύεται με κρυπτογραφικές μεθόδους για να αποφευχθούν παράνομες αλλαγές στο περιεχόμενο. Το PPH περιέχει τα εξής:

- Το αναγνωριστικό του εργαλείου ασφαλείας Α που το δημιούργησε.
- Το αναγνωριστικό του εργαλείου ασφαλείας Β του επόμενου κόμβου.
- Τον αριθμό ακολουθίας αποστολής $c_{A\to B}$.
- Τον αριθμό nuglets, u, που επιτρέπεται το Β να αποσπάσει από το πακέτο.
- Έναν Κωδικό Πιστοποίησης Πορτοφολιού(PAC), που υπολογίζεται από τα πεδία του PPH, και την τιμή hash του περιεχομένου του πακέτου, με χρήση κρυπτογραφικής συνάρτησης g, με το κλειδί συνεδρίας k_{AB} μεταξύ του Α και του Β.

Σχηματικά η μορφή του πακέτου και του PPH φαίνεται παρακάτω:

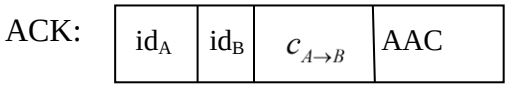


Σχήμα 4.1.1

Αντίστοιχα η επιβεβαίωση ACK, υπολογίζεται από το εργαλείο ασφαλείας Β του κόμβου και προσκολλάται στην επιβεβαίωση του επιπέδου MAC που επιστρέφεται στον αποστολέα. Η επιβεβαίωση περιέχει:

- Το αναγνωριστικό του εργαλείου ασφαλείας Α του προηγούμενου βήματος.
- Το αναγνωριστικό του εργαλείου ασφαλείας Β.
- Τον αριθμό ακολουθίας αποστολής $c_{A\to B}$, που λήφθηκε στο PPH.
- Έναν Κωδικό Πιστοποίησης Επιβεβαίωσης (AAC) που υπολογίζεται από το ληφθλεν PPH, με χρήση κρυπτογραφικής συνάρτησης g, με το κλειδί συνεδρίας k_{AB} μεταξύ του Α και του Β.

Σχηματικά η μορφή του πακέτου και του PPH φαίνεται παρακάτω:



Σχήμα 4.1.2

4.1.4 ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ NUGLETS

Για την κατανόηση της λειτουργίας του πρωτοκόλλου δρομολόγησης με χρήση PPM με καθορισμένες χρεώσεις ανά βήμα, γίνεται η παρακάτω περιγραφή:
Υποτίθεται ότι ο κόμβος N_A λαμβάνει ένα πακέτο από τον N_B, έχει καθορίσει ότι ο επόμενος κόμβος είναι ο N_C, και προτίθεται να προωθήσει το πακέτο για την καθορισμένη χρέωση στο PPH. Για την απόκτηση nuglets από το πακέτο, ο N_B πρέπει να περάσει το PPH στο εργαλείο ασφαλείας του Β μαζί με το αναγνωριστικό του εργαλείου ασφαλείας C του επόμενου βήματος και την κρυπτογραφικά τιμή hash του περιεχομένου του πακέτου. Στη συνέχεια το Β επιβεβαιώνει το PPH ελέγχοντας αν ο αριθμός ακολουθίας αποστολής του PPH είναι μεγαλύτερος κατά ένα από τον αριθμό ακολουθίας $c_{B\leftarrow A}$ που σχετίζεται με το Α. Εάν αυτό ισχύει, το Β τον $c_{B\leftarrow A}$ στην τιμή του αριθμού ακολουθίας που λαμβάνεται. Επίσης το Β επικυρώνει την αυθεντικότητα του PPH με επαναυπολογισμό του PAC και σύγκρισης της τιμής του με την τιμή που λαμβάνεται. Επιβεβαιώνεται έτσι ότι το PPH έχει όντως υπολογιστεί από το Α.

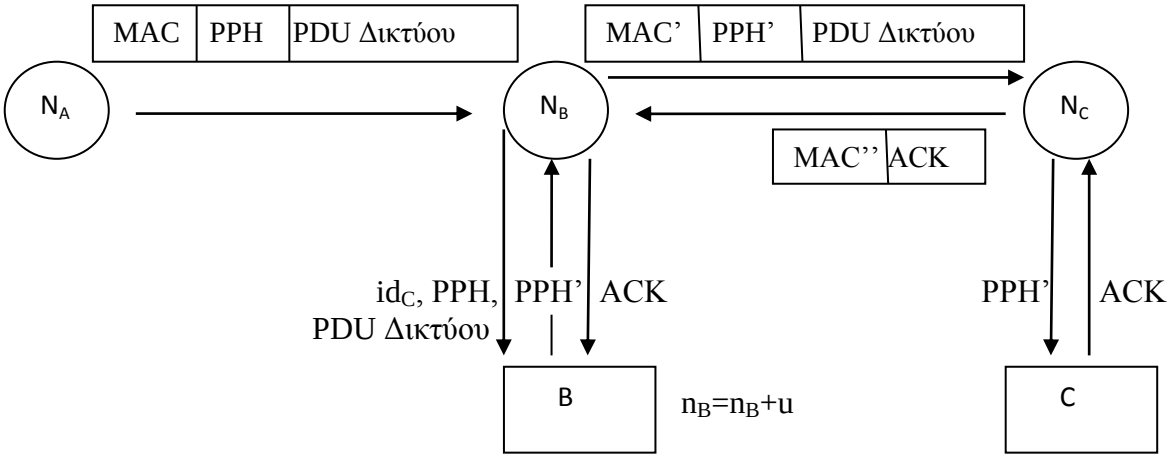
Μετά την επιτυχή επιβεβαίωση το Β υπολογίζει ένα νέο PPH ενσωματώνοντας τα αναγνωριστικά των Β και C, και τον αριθμό ακολουθίας αποστολής $c_{B\to C}$, μειώνοντας τον αριθμό των nuglets κατά την καθορισμένη τιμή, και υπολογίζοντας νέο PAC με χρήση κρυπτογραφικής συνάρτησης g, με το κλειδί συνεδρίας k_{BC}. Τέλος το Β αυξάνει τον αριθμό ακολουθίας αποστολής $c_{B\to C}$, και αποθηκεύοντας το PPH εσωτερικά και εξάγοντας ένα αντίγραφο για τον N_B.

Μόλις συμβεί αυτό, ο N_B επικολλά το νέο PPH στο πακέτο και το αποστέλλει στον N_C, ο οποίος πρέπει να επιβεβαιώσει τη λήψη του πακέτου. Για το λόγο αυτό, αποστέλλει το PPH στο εργαλείο ασφαλείας του για τον υπολογισμό του ACK, το οποίο επιστρέφει στον κόμβο N_C, που με τη σειρά του το αποστέλλει στον N_B επικολλημένο στην επιβεβαίωση του επιπέδου MAC.

Με τη σειρά του ο N_B, ο οποίος λαμβάνει το ACK και το αποστέλλει στο εργαλείο ασφαλείας του. Το Β προσπαθεί να βρει το ανταποκρινόμενο PPH στην εσωτερική του μνήμη ταιριάζοντας το αναγνωριστικό του C και τον αριθμό ακολουθίας αποστολής που λήφθηκε από το ACK, με τα αναγνωριστικά και τους αριθμούς ακολουθίας αποστολής στα αποθηκευμένα PPH. Στην περίπτωση που το βρει, επικυρώνει την αυθεντικότητα της επιβεβαίωσης επαναυπολογίζοντας το AAC του PPH και συγκρίνοντας το με την τιμή που λήφθηκε από το ACK. Εάν ταυτίζονται, το Β αυξάνει τον μετρητή των nuglets κατά την καθορισμένη τιμή, διαγράφει το PPH από την εσωτερική του μνήμη και φιλοδωρεί τον N_C με λίγα nuglets αυξάνοντας τον μετρητή χρέους $d_{B\to C}$.

Στην περίπτωση του PPM με δημοπρασίες, το εργαλείο ασφαλείας πραγματοποιεί τη δημοπρασία μεταξύ των πρακτόρων των πιθανών επόμενων κόμβων, και δημιουργεί το νέο PPH ανάλογα με το αποτέλεσμα της δημοπρασίας, το εξάγει μαζί με το αναγνωριστικό του επόμενου βήματος και προωθεί το πακέτο. Η υπόλοιπη διαδικασία είναι ίδια με το PPM με καθορισμένες χρεώσεις ανά βήμα.

Η λειτουργία του πρωτοκόλλου δρομολόγησης που περιγράφηκε, φαίνεται σχηματικά παρακάτω:



Σχήμα 4.1.3

4.1.5 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ NUGLETS

Οι δημιουργοί του μηχανισμού Nuglets, πραγματοποίησαν προσομοιώσεις συγγράφοντας κώδικα C++, με σκοπό να μελετήσουν την αποδοτικότητα του, καθώς και την απόδοση του δικτύου όταν εφαρμόζονται τα διάφορα μοντέλα χρέωσης. Για την ακρίβεια χρησιμοποιήθηκε κατά τις προσομοιώσεις, ένας αλγόριθμος προώθησης πακέτων, όπου κάθε κόμβος γνωρίζει τη γεωγραφική του θέση καθώς και τη γεωγραφική θέση των γειτόνων του, ενώ η πηγή του πακέτου γνωρίζει την γεωγραφική θέση του προορισμού. Κάθε κόμβος προωθεί το πακέτο στον κοντινότερο στον προορισμό, ενώ όταν ο κόμβος που προωθεί δεν έχει κοντά του κάποιον κόμβο που είναι κοντινότερα στον προορισμό από τον ίδιο, απορρίπτει το πακέτο. Οι κατασκευαστές του Nuglets, πραγματοποίησαν προσομοιώσεις με χρήση και των δύο επεκτάσεων του σχήματος(PPM με καθορισμένες χρεώσεις ανά βήμα, PPM με δημοπρασίες). Με βάση το συγκεκριμένο αλγόριθμο οι κόμβοι, λειτουργούν με βάση δύο συναρτήσεις:

- Την συνάρτηση χρησιμότητας της μπαταρίας u, που εξαρτάται από το επίπεδο της μπαταρίας b και τον αριθμό των nuglets n. Ο μαθηματικός τύπος που δίνει την u είναι ο παρακάτω:

$$u(b,n) = k\frac{\min(n^{a}, N^{a})}{\min(b^{\beta}, \mathrm{B}^{\beta})}$$

,όπου α, β, k, N και B, κατάλληλες σταθερές με α,β > 0.

- Την συνάρτηση χρησιμότητας των nuglets v, που εξαρτάται από το επίπεδο της μπαταρίας b και τον αριθμό των nuglets n. Ο μαθηματικός τύπος που δίνει την v είναι ο παρακάτω:

$$v(n,b) = \tilde{k}\frac{\min(b^{\tilde{a}}, \tilde{B}^{\tilde{a}})}{\min(n^{\tilde{\beta}}, \tilde{N}^{\tilde{\beta}})}$$

,όπου $\tilde{a}$, $\tilde{\beta}$, $\tilde{k}$, $\tilde{N}$ και $\tilde{B}$, οι κατάλληλες σταθερές με $\tilde{a}, \tilde{\beta} > 0$.

Το κόστος σε χρησιμοποιούμενη ισχύ μπαταρίας για την προώθηση πακέτου από έναν κόμβο είναι c και ως p ορίζεται ο αριθμός των nuglets με το οποίο επιβραβεύεται για την προωθητική του δραστηριότητα. Ο μίνιμουμ αριθμός nuglets για τον οποίο συμφέρει έναν κόμβο να προωθήσει ένα πακέτο δίνεται από την παρακάτω σχέση:

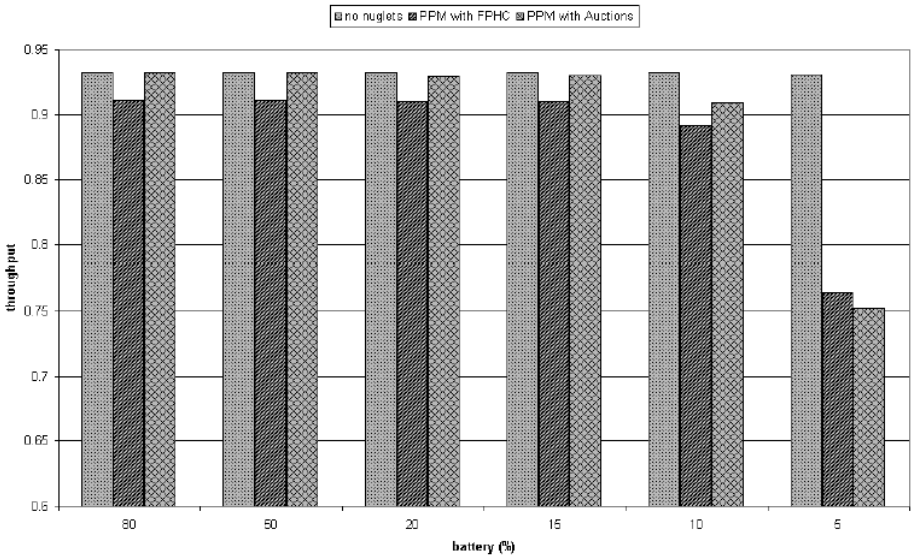
$$p_0 = \begin{cases} c\dfrac{u(b,n)}{v(n,b)} + 1 \\ \left\lceil c\dfrac{u(b,n)}{v(n,b)} \right\rceil \end{cases}$$

,με την πάνω παράμετρο να ισχύει για $c\dfrac{u(b,n)}{v(n,b)}$ ακέραιο, και την δεύτερη για όλες τις άλλες περιπτώσεις.

Για τις προσομοιώσεις του Nuglets, διαμορφώθηκε το εξής περιβάλλον προσομοίωσης:

- Κόμβοι 400
- Περιοχή 1000m x 1000m
- Εμβέλεια ισχύος 100m
- Δεν υπάρχει κίνηση
- Ρυθμός δημιουργίας πακέτου 0.5 πακέτο/second
- Τυχαία επιλογή του προορισμού
- 4kbits μέγεθος πακέτου
- 4.4kbits μέγεθος πακέτου σε περίπτωση ύπαρξης επεκτάσεων στο πρωτόκολλο
- Ρυθμός μετάδοσης 1Mbps
- Αρχικός αριθμός nuglets 800000

Οι κατασκευαστές του Nuglets πραγματοποίησαν 10 προσομοιώσεις για κάθε επίπεδο μπαταρίας μεταξύ 80%, 50%, 20%, 15%, 10% και 5%, ενώ για κάθε περίπτωση πραγματοποιήθηκε προσομοίωση λειτουργίας του δικτύου 2.5 ωρών.
Τα αποτελέσματα που εξήγαγαν σχετικά με το throughput του δικτύου σε σχέση με το επίπεδο μπαταρίας, στις περιπτώσεις που δεν χρησιμοποιούνται nuglets, που χρησιμοποιείται PPM με καθορισμένες χρεώσεις ανά βήμα και PPM με δημοπρασίες αντίστοιχα, φαίνονται στο παρακάτω διάγραμμα:



Διάγραμμα 4.1.1 (Πηγή [11])

Φαίνεται ότι στις περιπτώσεις που χρησιμοποιούνται nuglets, το throughput είναι μικρότερο σε σχέση με ένα δίκτυο που δεν χρησιμοποιεί nuglets, κάτι που είναι φυσιολογικό, αφού τα πακέτα στην πρώτη περίπτωση έχουν μεγαλύτερο μέγεθος και υπάρχει περίπτωση να απορριφθούν λόγω της χαμηλής τιμής του πορτοφολιού ή της καθορισμένης χρέωσης ανά βήμα. Τέλος, εκτός από τις περιπτώσεις χαμηλού επιπέδου μπαταρίας, οι επεκτάσεις που χρησιμοποιούν nuglets διαφέρουν μεταξύ τους ως προς την απόδοση αμελητέα, ενώ και σε σχέση με δίκτυο που δεν κάνει χρήση nuglets, υστερούν ως προς την απόδοση μόνο κατά 5%.

Συμπερασματικά, ο μηχανισμός υποστήριξης συνεργασίας Nuglets, ενισχύει την συνεργασία των κόμβων όσον αφορά την προώθηση πακέτων, προωθεί την εκλογικευμένη χρήση του δικτύου ενώ παράλληλα ενθαρρύνει τους κόμβους να είναι σε λειτουργία ακόμα και όταν δεν περιμένουν κάποιο πακέτο, ώστε να εξυπηρετήσουν τους υπόλοιπους. Τα nuglets μπορούν να χρησιμοποιηθούν για την ενίσχυση υπηρεσιών επικοινωνίας και πληροφορίας, αλλά και για την πληρωμή της χρήσης backbone δικτύων ή δορυφορικών ζεύξεων. Πλεονέκτημα του Nuglets, αποτελεί το ότι μπορεί να χρησιμοποιηθεί πάνω από οποιοδήποτε πρωτόκολλο δρομολόγησης, ενώ δεν επηρεάζει σε μεγάλο βαθμό αρνητικά το throughput του δικτύου.

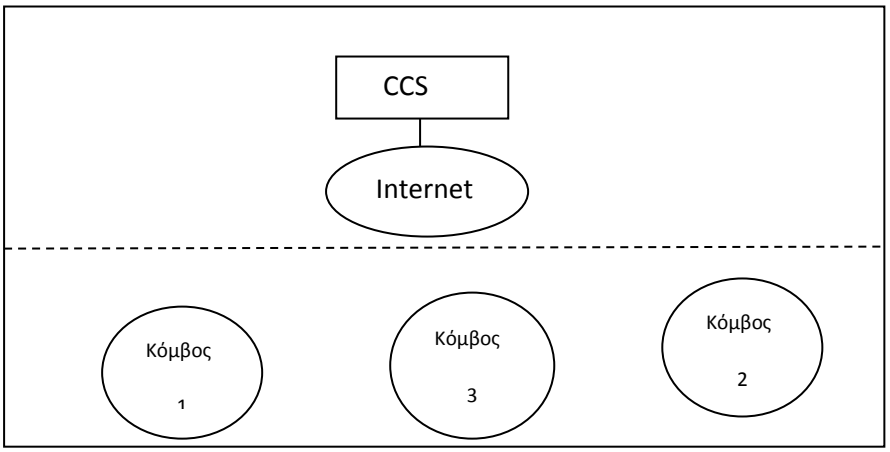
4.2 SPRITE

Το SPRITE [13] αποτελεί έναν μηχανισμό υποστήριξης συνεργασίας για ad-hoc δίκτυα με παρουσία εγωιστικών κόμβων, βασισμένο σε πιστώσεις, που δεν χρησιμοποιεί ειδικό hardware στους κόμβους. Σε γενικές γραμμές το σχήμα λειτουργεί ως εξής:
Όταν ένας κόσμος λαμβάνει ένα μήνυμα, διατηρεί μια «απόδειξη είσπραξης» του. Στη συνέχεια, όταν ο κόμβος διαθέτει γρήγορη σύνδεση σε μια Υπηρεσία Εκκαθάρισης Πιστώσεων (CCS), αναφέρει σε αυτήν τα μηνύματα που έχει παραλάβει και προωθήσει, ανεβάζοντας σε αυτήν τις αποδείξεις είσπραξής του. Με βάση τις αναφερόμενες απόδειξης του μηνύματος, η CCS καθορίζει την χρέωση και τις πιστώσεις για κάθε κόμβο που συμμετέχει στη μετάδοση.
Βασικό ζήτημα που συναντάται κατά την υλοποίηση του σχήματος αποτελεί, το ότι οι κόμβοι δε διαθέτουν ειδικό hardware, με αποτέλεσμα να υπάρχει πιθανότητα ένας εγωιστικός κόμβος να προσπαθήσει να πλανέψει το σύστημα ώστε να μεγιστοποιήσει τους πόρους του. Για παράδειγμα θα μπορούσε ένας κόμβος να αποκρύψει την απόδειξη είσπραξής του, ή να δημιουργήσει συμπαιγνία με άλλους κόμβους για να πλαστογραφήσει αποδείξεις. Ένα άλλο ζήτημα είναι η ανάγκη του κόμβου να λάβει αρκετές πιστώσεις για να προωθήσει ένα μήνυμα, ώστε να μπορεί να στείλει τα δικά του μηνύματα με τις ληφθείσες αυτές πιστώσεις, εκτός αν οι πόροι του κόμβου είναι εξαιρετικά χαμηλοί.

4.2.1 ΠΕΡΙΓΡΑΦΗ ΤΟΥ SPRITE

Το Sprite αποτελείται από την CCS και από μια ομάδα κινητών κόμβων, οι οποίοι είναι εφοδιασμένοι με διεπαφές δικτύου που τους επιτρέπουν να στέλνουν και να λαμβάνουν μηνύματα μέσω ενός ασύρματου δικτύου. Για την αναγνώριση κάθε κόμβου υποτίθεται ότι καθένας τους διαθέτει ένα πιστοποιητικό που εκδίδεται από μια κλιμακούμενη αρχή πιστοποιητικών, ενώ κατά την υλοποίηση του σχήματος υποτέθηκε ότι ο αποστολέας γνωρίζει το πλήρες μονοπάτι προς τον προορισμό, χρησιμοποιώντας ένα ασφαλές πρωτόκολλο δρομολόγησης βασισμένο στο DSR.
Όταν ένας κόμβος αποστέλλει τα μηνύματα του, χάνει πιστώσεις στο δίκτυο, καθώς άλλοι κόμβοι επιβαρύνουν με ένα κόστος για την προώθηση του μηνύματος. Με την ίδια λογική όταν ένας κόμβος προωθεί μηνύματα άλλων κόμβων, λαμβάνει πιστώσεις για να είναι ικανός να αποστείλει αργότερα μηνύματα.
Στο Sprite υπάρχουν δύο τρόποι ώστε ένας κόμβος να αποκτήσει περισσότερες πιστώσεις. Ο πρώτος είναι, η πληρωμή ενός κόμβου σε αληθινά χρήματα ώστε να αγοράσει πιστώσεις ή η πληρωμή της χρέωσής του, βασιζόμενος στην τρέχουσα απόδοση του συστήματος. Ο δεύτερος που είναι και ο επικρατέστερος, είναι η προώθηση μηνυμάτων άλλων κόμβων. Για να καταφέρει να αποκτήσει πιστώσεις από την προώθηση μηνυμάτων, ένας κόμβος πρέπει να αναφέρει στην CCS, ποιά μηνύματα έχει βοηθήσει να προωθηθούν. Με σκοπό να ελαττώσει τον αποθηκευτικό χώρο, ο κόμβος αναφέρει στην CCS πότε αλλάζει σε γρήγορη σύνδεση, και διαθέτει εφεδρική ισχύ. Η αναφορά στην CCS μπορεί να πραγματοποιηθεί μέσω ενός υπολογιστή ή ενός proxy. Επίσης, για την εξοικονόμηση εύρους ζώνης και αποθηκευτικού χώρου, χρησιμοποιούνται στις αναφορές μικρές αποδείξεις είσπραξης, παράγονται από τα μηνύματα και δεν αποκαλύπτουν το συνολικό περιεχόμενο του μηνύματος, και όχι ολόκληρα τα μηνύματα. Αυτό έχει ως αποτέλεσμα, οι κόμβοι να μην χρειάζεται να εμπιστεύονται την CCS για θέματα

εμπιστευτικότητας μηνυμάτων. Σε γενικές γραμμές η αρχιτεκτονική του Sprite φαίνεται παρακάτω:



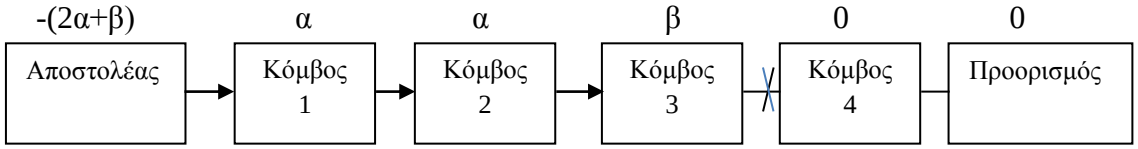
Σχήμα 4.2.1

Βασικά ζητήματα που λαμβάνονται υπόψη για την λειτουργία του Sprite είναι τα εξής:

1. Ο τρόπος χρέωσης. Σύμφωνα με το Sprite στις ανταλλαγές μηνυμάτων χρεώνεται μόνο ο αποστολέας, και όχι ο παραλήπτης, πρώτον επειδή χρεώνοντας τον προορισμό επιτρέπεται σε άλλους κόμβους να εκτοξεύσουν μια επίθεση άρνησης παροχής υπηρεσιών στέλνοντας του μια τεράστια ποσότητα κίνησης. Κάτι τέτοιο μπορεί να συμβεί ακόμα και αν η χρέωση μοιραστεί σε παραλήπτη και προορισμό, καθώς ο αποστολέας έχει τη δυνατότητα να δημιουργήσει συμπαιγνία με ενδιάμεσους κόμβους, ώστε να επιστραφεί σε αυτόν η πληρωμή του, και όλη η χρέωση να επιβαρύνει τον παραλήπτη. Χρεώνοντας μόνο τον αποστολέα πετυχαίνεται να μην αποστέλλει και άχρηστα μηνύματα, αλλά και να μπορεί να ζητήσει αποζημίωση από τον προορισμό.
   Αντίστοιχα, όσον αφορά τις πιστώσεις, ο κόμβος θα τις λάβει μόνο στην περίπτωση που η προώθηση του μηνύματος από αυτόν είναι επιτυχημένη, δηλαδή όταν ο επόμενος κόμβος στο μονοπάτι λάβει το μήνυμα. Με άλλα λόγια, η CCS θεωρεί ότι ένας κόμβος έχει προωθήσει το μήνυμα μόνο όταν υπάρχει διάδοχος στο μονοπάτι που αναφέρει την έγκυρη απόδειξη είσπραξης του μηνύματος.
2. Οι στόχοι του συστήματος πληρωμών. Βασικός στόχος, είναι η πρόληψη ενεργειών εξαπάτησης και η παροχή κινήτρων στους κόμβους ώστε να συνεργαστούν. Για το λόγο αυτό δεν απαιτείται μια ισορροπημένη πληρωμή, δεν απαιτείται η συνολική χρέωση του αποστολέα να είναι ίση με τις συνολικές πιστώσεις που λαμβάνουν άλλοι κόμβοι για ένα μήνυμα. Πιο συγκεκριμένα η CCS χρεώνει τον αποστολέα περισσότερο από ότι δίνει στους άλλους κόμβους, και για να αντισταθμιστεί η μακρόχρονη εκροή πιστώσεων από αυτούς προς την CCS, σε ένα μεγάλο δίκτυο, η CSS περιοδικά επιστρέφει τις πιστώσεις σε αυτούς ομοιόμορφα. Σε αντίθετη περίπτωση, η CSS περιοδικά δίνει στους κόμβους ένα καθορισμένο αριθμό πιστώσεων. Μια τέτοια κίνηση ούτε δίνει τη δυνατότητα σε κόμβους να εξαπατήσουν το σύστημα, ούτε μειώνει τα κίνητρα προς τους κόμβους.
3. Οι ενέργειες εξαπάτησης κατά την διαδικασία καταχώρησης αποδείξεων είσπραξης. Κάθε εγωιστικός κόμβος, εάν δεν υπάρχει το κατάλληλο σύστημα

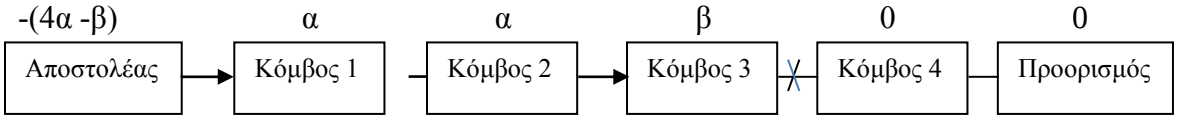
πληρωμών, μπορεί να μην προωθεί τα μηνύματα άλλων κόμβων ή να προβεί σε ενέργειες εξαπάτησης του συστήματος με σκοπό να μεγιστοποιήσει τους πόρους του. Μπορεί για παράδειγμα μετά τη λήψη του μηνύματος να αποθηκεύσει την απόδειξη είσπραξης αλλά να μην προωθήσει το μήνυμα, να μην αναφέρει την απόδειξη είσπραξης, ή στην περίπτωση που δε λάβει το μήνυμα να ισχυριστεί ψευδώς ότι το έχει λάβει. Το σύστημα πληροί συγκεκριμένες προϋποθέσεις ώστε να προλαμβάνονται τέτοιες ενέργειες.

4. Η προσφορά κινήτρων στους κόμβους ώστε να προωθήσουν μηνύματα.. Για το σκοπό αυτό, η CCS προσφέρει στους κόμβους που προωθούν μηνύματα, περισσότερες πιστώσεις από ότι σε κόμβους που δεν προωθούν. Η διαδικασία αυτή πραγματοποιείται ως εξής. Αρχικά η CCS καθορίζει τον τελευταίο κόμβο στο μονοπάτι που έχει λάβει το μήνυμα, και στη συνέχεια ζητάει από τον αποστολέα να πληρώσει β πιστώσεις στον κόμβο και α πιστώσεις στους προκατόχους του, όπου $\beta<\alpha$. Η διαδικασία γίνεται πιο κατανοητή από το παρακάτω παράδειγμα. Στο παρακάτω σχήμα μόνο οι τρεις πρώτοι ενδιάμεσοι κόμβοι καταχωρούν τις αποδείξεις είσπραξης τους, και για το λόγο αυτό, οι κόμβοι 1 και 2 λαμβάνουν α πιστώσεις, ενώ ο κόμβος 3 λαμβάνει β πιστώσεις. Από τη στιγμή που ο κόμβος 4 και ο προορισμός δεν καταχωρούν καμία απόδειξη είσπραξης, δεν λαμβάνουν καμία πίστωση, και ο αποστολέας πληρώνει συνολικά $2\alpha + \beta$ πιστώσεις. Στο παρακάτω σχήμα φαίνεται σχηματικά το αντίστοιχο παράδειγμα.



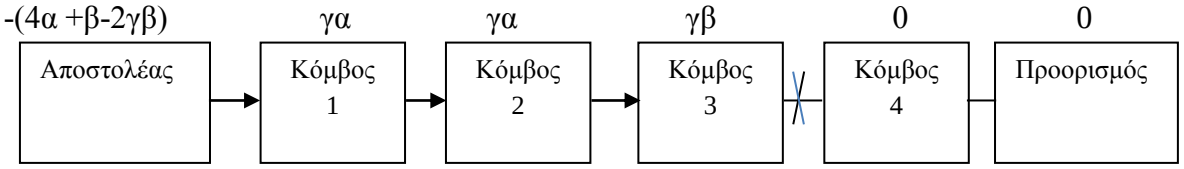
Σχήμα 4.2.2

5. Η προσφορά κινήτρων στους κόμβους ώστε να καταχωρούν τις αποδείξεις είσπραξης τους. Στην πραγματικότητα κάθε κόμβος που έχει παραλάβει ένα μήνυμα, έχει κίνητρο να αναφέρει την απόδειξη πληρωμής του, εάν οι πιστώσεις β είναι μικρότερες από το κόστος καταχώρησης μιας απόδειξης είσπραξης, το οποίο είναι γενικά χαμηλό. Παρόλα αυτά υπάρχει η περίπτωση ο τελευταίος κόμβος να πραγματοποιήσει συμπαιγνία με τον αποστολέα. Πιο συγκεκριμένα, αν ο τελευταίος κόμβος δεν αναφέρει την απόδειξη είσπραξης του, ο αποστολέας γλιτώνει α πιστώσεις ενώ ο τελευταίος κόμβος χάνει β πιστώσεις. Ωστόσο, αν ο αποστολέας δώσει κρυφά στον τελευταίο κόμβο $\beta+\varepsilon$ πιστώσεις όπου $\varepsilon>0$, ο τελευταίος κόμβος ευνοείται ενώ και ο αποστολέας απολαμβάνει ένα κέρδος $\alpha-(\beta+\varepsilon)$ πιστώσεων. Έτσι συνολικά οι δύο κόμβοι, έχουν κέρδος $\alpha - \beta$ πιστώσεων.
   Για να αποφευχθεί κάτι τέτοιο, η CCS χρεώνει τον αποστολέα με ένα έξτρα ποσό πιστώσεων, τις οποίες λαμβάνει η ίδια, αν ο προορισμός δεν αναφέρει την απόδειξη είσπραξης ενός μηνύματος. Η συνολική χρέωση του αποστολέα πρέπει να είναι $k\beta$ πιστώσεις λιγότερες από ότι από το ποσό που χρεώνεται ο αποστολέας όταν λαμβάνεται ένα μήνυμα από τον προορισμό, όπου k ο αριθμός των κόμβων που δεν καταχωρούν αποδείξεις. Βάσει του παραδείγματος που χρησιμοποιήθηκε παραπάνω, βλέπουμε τη συνολική χρέωση το αποστολέα που ανέρχεται σε $(4\alpha + \beta) - 2\beta$ πιστώσεις.



Σχήμα 4.2.3

6. Η πρόληψη ψευδών αποδείξεων είσπραξης. Όπως αναφέρθηκε υπάρχει περίπτωση για λόγους εξοικονόμησης εύρους ζώνης και αποθηκευτικού χώρου, ένας κόμβος να καταχωρήσει μόνο την απόδειξη ενός μηνύματος. Έτσι, κάποιος κόμβος μπορεί να προωθεί μόνο την απόδειξη αντί για όλο το μήνυμα στον επόμενο κόμβο, πράγμα που είναι αρκετό για να λάβει πιστώσεις. Ακόμα, είναι δυνατό ένας ενδιάμεσος κόμβος να περιμένει μέχρι να έχει γρήγορη σύνδεση προς τον επόμενο κόμβο, ώστε να προωθήσει μια ψεύτικη απόδειξη είσπραξης, ώστε να εξοικονομήσει πόρους. Η αντιμετώπιση τέτοιων επιθέσεων βασίζεται στον προορισμό. Εάν ο προορισμός πραγματοποιήσει συμπαιγνία με ενδιάμεσους κόμβους, και καταχωρήσει μια απόδειξη είσπραξης ακόμα και αν δεν λάβει ολόκληρο το μήνυμα, υποτίθεται ότι οι ενδιάμεσοι κόμβοι και ο προορισμός πρέπει να πληρωθούν σαν να μην έχουν πραγματοποιήσει ενέργεια εξαπάτησης. Αν ο αποστολέας χρειάζεται να σιγουρευτεί ότι ο προορισμός έλαβε ολόκληρο το πακέτο, υλοποιείται ένα πρωτόκολλο υψηλότερου επιπέδου για την επιβεβαίωση της απόδειξης είσπραξης ολόκληρου του μηνύματος από τον προορισμό.
   Στην περίπτωση πάλι που ο προορισμός δεν πραγματοποιεί συμπαιγνία με ενδιάμεσους κόμβους, αν οι ενδιάμεσοι κόμβοι προωθήσουν μόνο την απόδειξη είσπραξης του μηνύματος, τότε ο προορισμός δεν θα δύναται να λάβει ένα έγκυρο φορτίο μηνύματος, και συνεπώς δεν θα δύναται να καταχωρήσει μια απόδειξη είσπραξης του μηνύματος. Βάσει αυτού του γεγονότος, οι ενέργειες εξαπάτησης των ενδιάμεσων κόμβων μπορούν να αποφευχθούν μειώνοντας κατά πολύ την ποσότητα πιστώσεων που δίνονται στους ενδιάμεσους κόμβους, αν το μήνυμα δεν αναφέρεται ότι λήφθηκε από τον προορισμό. Με τον τρόπο αυτό, οι κόμβοι που διαπράττουν εξαπάτηση, δεν μπορούν να λάβουν πιστώσεις ικανές να καλύψουν ούτε στο ελάχιστο τις ενέργειες εξαπάτησης τους. Με βάσει πάντα το παράδειγμα που αναφέρθηκε, πιο συγκεκριμένα, αν ο προορισμός δεν αναφέρει την απόδειξη είσπραξης ενός μηνύματος, πολλαπλασιάζονται οι πιστώσεις που πληρώνονται σε κάθε κόμβο με γ, όπου $\gamma<1$. Σύμφωνα με τα παραπάνω, μειώνεται η χρέωση του αποστολέα κατά $\gamma\beta$ αντί για β, για κάθε κόμβο στο μονοπάτι που δεν αναφέρει την απόδειξη είσπραξης.



Σχήμα 4.2.4

4.2.2 ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ ΠΡΩΤΟΚΟΛΛΟΥ ΠΡΟΩΘΗΣΗΣ ΜΗΝΥΜΑΤΩΝ

Κατά την εξειδίκευση του πρωτοκόλλου προώθησης στο Sprite, θεωρούνται ως PK_i και SK_i, το ιδιωτικό και το δημόσιο κλειδί αντίστοιχα, του κόμβου n_i. Κάθε κόμβος n_i, διατηρεί έναν αριθμό ακολουθίας seq_i, όπου seq_i (j,k) είναι οι αριθμοί ακολουθίας των μηνυμάτων του κόμβου αποστολέα n_j, στον προορισμό n_k. Θεωρείται ακόμα ότι ($sign_{SK}$(), $verify_{PK}$ ()) αποτελεί ένα σχήμα ψηφιακής υπογραφής.
Παρακάτω περιγράφονται οι διάφορες λειτουργίες του πρωτοκόλλου:

- **Αποστολή μηνύματος**. Υποθέτοντας ότι ο κόμβος n_0 προτίθεται να αποστείλει φορτίο μηνύματος m με αριθμό ακολουθίας seq_0(0,d) στον προορισμό n_d, μέσω του μονοπατιού p, ο κόμβος n_0 αρχικά υπολογίζει μια υπογραφή s, μέσω του σχήματος (MD(m), p, seq_0 (0,d)), όπου MD() μια συνάρτηση κρυπτογράφησης μηνύματος όπως οι αλγόριθμοι MD5 και SHA-1. Στη συνέχεια μεταφέρει το σύνολο (m, p, seq_0(0,d), s) στον επόμενο κόμβο στο μονοπάτι, και αυξάνει το seq_0(0,d) κατά 1.
- **Λήψη μηνύματος**. Υποθέτοντας ότι ο κόμβος n_i λαμβάνει το σύνολο (m, p, seq, s), ελέγχει αρχικά τρεις παραμέτρους: Πρώτον ότι ο n_i είναι στο μονοπάτι. Δεύτερον ότι το μήνυμα διαθέτει αριθμό ακολουθίας μεγαλύτερο από τον seq_i (0,d). Τρίτον ότι η υπογραφή είναι έγκυρη. Αν οποιαδήποτε από αυτές τις υποθέσεις δεν ικανοποιείται, το πακέτο απορρίπτεται, αλλιώς, ο κόμβος αποθηκεύει το σύνολο (MD(m), p, seq, s) ως απόδειξη είσπραξης του μηνύματος. Αν ο κόμβος n_i δεν είναι ο προορισμός και αποφασίσει να προωθήσει το μήνυμα, στέλνει το (m, p, seq, s), στο επόμενο βήμα.
- **Υπολογισμός πληρωμών**. Μια απόδειξη είσπραξης (D, p, seq, s) καταχωρημένη από έναν κόμβο n_i θεωρείται έγκυρη όταν ισχύει (σύμφωνα με το σχήμα ψηφιακής υπογραφής που αναφέρθηκε), $verify_{PK0}$((D, p, seq), s) = TRUE, όπου PK_0, το δημόσιο κλειδί του αποστολέα. Υποτίθεται ακόμα ότι p = (n_0, n_1, …., n_e,…., n_d), όπου ο n_e είναι ο τελευταίος κόμβος στο μονοπάτι p, που καταχωρεί μια έγκυρη απόδειξη είσπραξης με αριθμό ακολουθίας seq. Στη συνέχεια η CCS χρεώνει C πιστώσεις από τον κόμβο n_0, και πληρώνει P_i, στον κόμβο n_i, όπου:

  $C = (d - 1)\alpha + \beta - (d - e)\gamma\beta$ και $P_i = \begin{cases} a \\ \beta \\ \gamma\alpha \\ \gamma\beta \end{cases}$

  , αν i < e = d, αν i = e = d, αν i < e < d και αν i = e < d αντίστοιχα.

  Η απόδοση πιστώσεων από την CCS γίνεται βαθμιαία.

Για την καλύτερη κατανόηση της λειτουργίας του πρωτοκόλλου προώθησης μηνυμάτων του Sprite, θεωρείται η διαδικασία καταχώρησης των αποδείξεων είσπραξης σαν ένα παίγνιο ενός γύρου, με d + 1 παίκτες (κόμβοι n_0, n_1, …., n_d) από τον αποστολέα στον προορισμό. Ορίζεται ως T_i η πληροφορία που κρατά ο κόμβος n_i και δεν είναι γνωστή στην CCS. Για i > 0 ισχύει T_i = TRUE αν ο κόμβος έχει λάβει το μήνυμα m, ειδάλλως ισχύει T_i = FALSE. Προφανώς ο κόμβος n_0 και οι κόμβοι που έχουν λάβει το μήνυμα m συνιστούν ένα πρόθεμα του μονοπατιού. Επομένως ισχύει:

$$T_i = \begin{cases} TRUE & \alpha\nu \quad 0 < i \le e' \\ FALSE & \alpha\nu \quad e' < i \le d \end{cases}$$

, όπου e' το περιεχόμενο του τελευταίου κόμβου που έχει λάβει το μήνυμα m, και παραμένει άγνωστο στην CCS στην αρχή του παιγνίου. Επίσης αρχικοποιείται T_0 = TRUE.

Κάθε κόμβος παίκτης n_i, έχει δύο επιλογές. Πρώτον να αναφέρει ότι έλαβε το μήνυμα m, καταχωρώντας μια έγκυρη απόδειξη είσπραξης, ή δεύτερον να μην κάνει αναφορά. Η ενέργεια αυτή ορίζεται ως A_0 και μπορεί να είναι TRUE ή FALSE. Μόνο ο κόμβος n_0 δεν έχει δυνατότητα επιλογής. Η A_0 αρχικοποιείται TRUE.

Το κόστος για την ενέργεια αυτή του κόμβου n_i, ορίζεται ως U_i. Ισχύει:

$$U_i = \begin{cases} \delta \quad \alpha\nu\, T_i = FALSE \quad \kappa\alpha\iota\, \mathrm{A}_i = TRUE \\ \\ 0 \qquad\qquad\qquad\qquad\qquad\qquad \alpha\lambda\lambda\iota\acute{\omega}\varsigma \end{cases}$$

, όπου δ το κόστος για την προώθηση μιας απόδειξης είσπραξης από έναν κινητό κόμβο σε έναν άλλο.

Το σύστημα πληρωμής αναφέρθηκε παραπάνω, ενώ για τον κόμβο n_0, η χρέωση σε C, θεωρείται σαν αρνητική πληρωμή και έχει ως εξής:

$$P_0 = -C = -((d - 1)\alpha + \beta - (d - e)\gamma\beta)$$

Η ευημερία σε πόρους κάθε κόμβου n_i, δίνεται από τον τύπο:

$$W_i = P_i - U_i$$

Η υλοποίηση του Sprite χρησιμοποιεί κάποιες βασικές παραδοχές:

- Ένας κόμβος n_i, λέει την αλήθεια όταν $A_i = T_i$, ενώ σε αντίθετη περίπτωση ψεύδεται.
- Κάθε παίγνιο είναι ανθεκτικό ενάντια σε συμπαιγνίες.
- Η βέλτιστη στρατηγική για κάθε κόμβο, είναι να λέει την αλήθεια.
- Κάθε παίγνιο είναι ανθεκτικό ενάντια στην εξαπάτηση.
- Κάθε ενδιάμεσος κόμβος περιμένει κέρδος ίσο με $(p_1 - p_2)\gamma\alpha + (1 - p_1)\gamma\beta - \gamma\beta$, όπου p_1 η πιθανότητα το μήνυμα να φτάσει στον επόμενο κόμβο, και p_2 η πιθανότητα να φτάσει στον προορισμό. Αν το κέρδος αυτό είναι αρκετό για να καλύψει το κόστος προώθησης του μηνύματος, ο κόμβος έχει κίνητρο ώστε να προωθήσει το μήνυμα.

Όπως αναφέρθηκε, το Sprite μπορεί να εφαρμοστεί πάνω στο πρωτόκολλο δρομολόγησης DSR, να το βελτιώσει ως προς την ενίσχυση της συνεργασίας των κόμβων. Περιληπτικά, η λειτουργία του ενισχυμένου DSR έχει ως εξής:

- Όταν ένας κόμβος ξεκινά την αποστολή ενός μηνύματος ROUTE REQUEST, το μήνυμα περιέχει την διεύθυνση της πηγής και έναν αριθμό ακολουθίας. Στη συνέχεια, ο κόμβος υπογράφει και μεταδίδει το μήνυμα, αυξάνοντας τον μετρητή αριθμών ακολουθίας του κατά 1.
- Όταν ένας κόμβος λαμβάνει ένα μήνυμα ROUTE REQUEST, αποφασίζει αρχικά αν αυτό έχει επαναληφτεί, ελέγχοντας τον αριθμό ακολουθίας του. Ύστερα, αποθηκεύει το μήνυμα αυτό, ώστε να λάβει πληρωμή στο μέλλον.

Όταν ο κόμβος αποφασίζει να αναμεταδώσει το ROUTE REQUEST, επισυνάπτει τη δική του διεύθυνση και υπογράφει το εκτεταμένο μήνυμα.

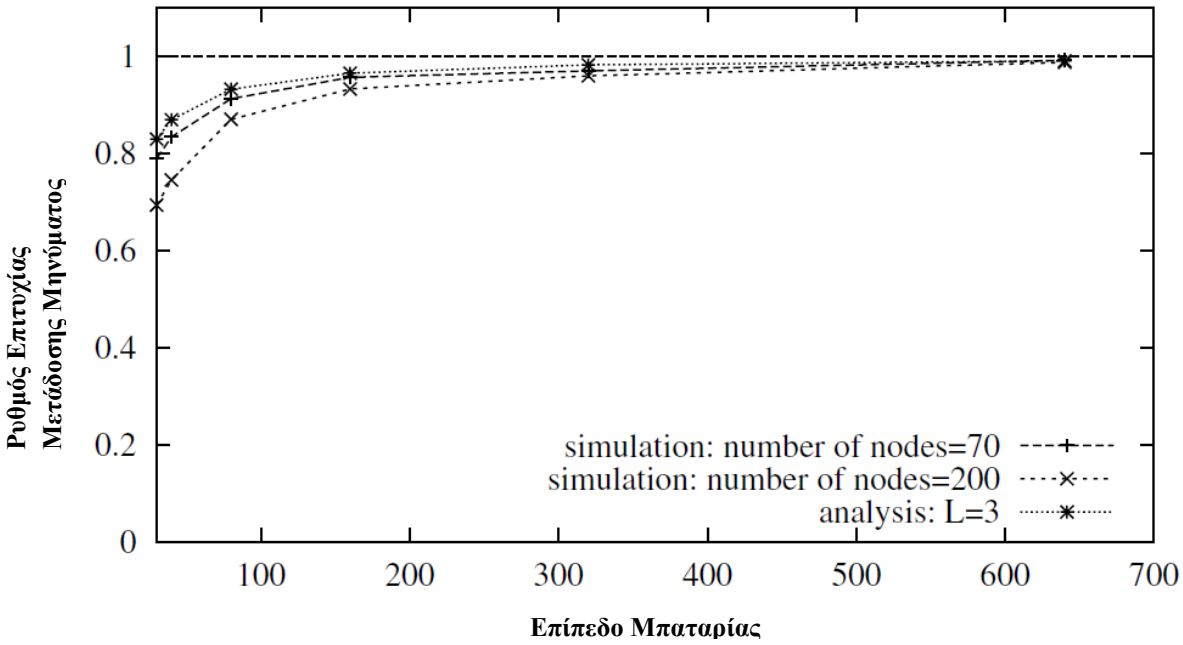
- Όταν η CCS υπολογίζει κάποια πληρωμή, απορρίπτει το μήνυμα ROUTE REQUEST, αν κάποια υπογραφή στο μήνυμα δεν είναι έγκυρη. Το ίδιο συμβαίνει, και όταν ένα μήνυμα ROUTE REQUEST που έχει καταχωρηθεί από έναν κόμβο, είναι μέρος κάποιου άλλου ROUTE REQUEST που έχει καταχωρηθεί από τον ίδιο. Τέλος, η CCS χτίζει ένα δέντρο βασιζόμενο στα αποδεκτά ROUTE REQUEST. Ο αποστολέας πληρώνει *α* πιστώσεις σε κάθε κόμβο που δεν είναι φύλλο του δέντρου και *β* πιστώσεις σε κάθε κόμβο που είναι. Για κάθε κόμβο έξω από το δέντρο, ο αποστολέας πληρώνει *α-β* πιστώσεις στην CCS.

4.2.3 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ SPRITE

Η υλοποίηση του σχήματος Sprite για την υποστήριξη συνεργασίας στα ad-hoc δίκτυα, από τους δημιουργούς του, έγινε με χρήση της βιβλιοθήκης Crypto++4.0, σε λογισμικό Windows XP. Κατά τις προσομοιώσεις χρησιμοποιήθηκε σαν κινητός κόμβος ένα laptop με επεξεργαστή Intel Mobile Premium III στα 866 Mhz. Για τις προσομοιώσεις του Sprite χρησιμοποιήθηκε το ακόλουθο περιβάλλον προσομοίωσης:

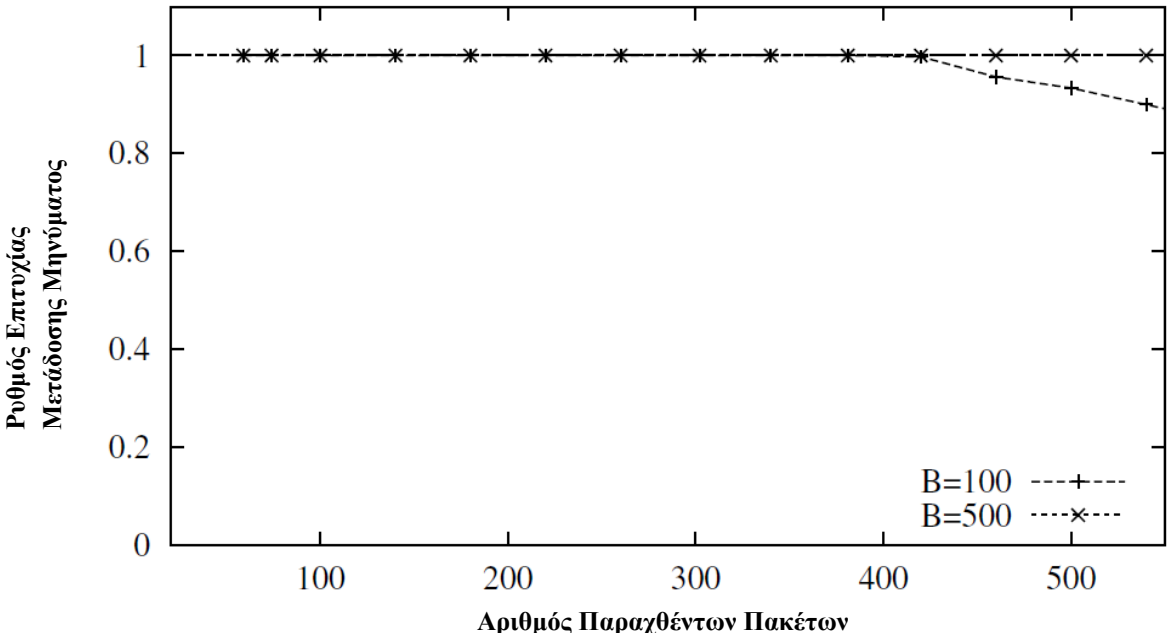
- Μήκος φορτίου μηνύματος 1000 bytes
- Αλγόριθμος κρυπτογράφησης MD5
- Σχήματα ψηφιακής υπογραφής RSA με υπόλοιπο 1024 bits και ECNR
- Μέσο μήκος μονοπατιού 8 βήματα
- Πρωτόκολλο δρομολόγησης DSR
- Περιοχή 1000m x 1000m - 70 κόμβοι
- Περιοχή 2000m x 2000m - 200 κόμβοι
- Ακτίνα επικοινωνία 250
- C=10
- Μέγιστη μπαταρία 640
- Αρχικές πιστώσεις κόμβου 3

Πραγματοποιώντας προσομοιώσεις για τα δύο σχήματα ψηφιακής υπογραφής και τα δύο σενάρια όσον αφορά τον αριθμό των κόμβων και το εύρος της περιοχής, οι δημιουργοί του Sprite κατέληξαν στα ακόλουθα συμπεράσματα για την απόδοση του δικτύου, όπως φαίνονται και μέσα από τα διαγράμματα που εξήγαγαν:



Διάγραμμα 4.2.1 (Πηγή **[13]**)

Από το παραπάνω διάγραμμα που στον κάθετο άξονα του φαίνεται ο **ρυθμός επιτυχίας μετάδοσης μηνύματος** και στον οριζόντιο άξονα το **επίπεδο της μπαταρίας του δικτύου**, διαπιστώνεται ότι όσο αυξάνονται οι πόροι μπαταρίας, τόσο αυξάνεται και ο ρυθμός επιτυχίας μετάδοσης του μηνύματος, που στο μέγιστο επίπεδο μπαταρίας αγγίζει και το 1. Αντίστοιχα στο παρακάτω διάγραμμα που στον κάθετο άξονα του φαίνεται ο **ρυθμός επιτυχίας μετάδοσης μηνύματος** και στον οριζόντιο **ο αριθμός των παραχθέντων πακέτων,** διαπιστώνεται ότι όσο δεν εισάγονται νέοι κόμβοι στο δίκτυο, και καταναλώνεται η μπαταρία, οι κόμβοι τείνουν να είναι πιο συντηρητική, ενώ παρόλα αυτά, ακόμα και για χαμηλή μπαταρία παράγονται αρκετά πακέτα πριν πέσει ο ρυθμός επιτυχίας μετάδοσης των μηνυμάτων.



Διάγραμμα 4.2.1 (Πηγή **[13]**)

Κατά τις προσομοιώσεις υποτέθηκε ότι οι κόμβοι μπορούν να στείλουν μόνο ένα περιορισμένο ποσό μηνυμάτων με την εναπομείνασα ισχύ τους.

Συμπεραίνεται από τα παραπάνω πειράματα, ότι η εφαρμογή του Sprite σε ένα ασύρματο δίκτυο ad-hoc δεν επηρεάζει αρνητικά την απόδοση του δικτύου ενώ επιτυγχάνεται σε μεγάλο βαθμό και η επιτυχής μετάδοση των μηνυμάτων. Το Sprite αποτελεί έναν μηχανισμό υποστήριξης συνεργασίας, που ενισχύει την συνεργασία μεταξύ των κόμβων, και δίνει κίνητρα για την προώθηση των πακέτων άλλων κόμβων, εκτός από την περίπτωση που οι πόροι ενέργειας είναι πάρα πολύ χαμηλοί. Τέλος, το Sprite εισάγει και ασφάλεια, χωρίς την χρήση κάποιου hardware.

4.3 PIFA

Ο μηχανισμός υποστήριξης συνεργασίας PIFA [14], βασίζεται σε πιστώσεις ώστε να ενισχύσει τη συνεργασία των κόμβων στα ad-hoc δίκτυα. Πρόκειται για ένα σχήμα πληρωμής που σκοπό έχει την εθελοντική προώθηση πακέτων από τους κόμβους και την πρόληψη της υποβάθμισης του δικτύου, όταν σε αυτό υπάρχουν εγωιστικοί κόμβοι, που δεν προωθούν πακέτα με στοχεύοντας στην εξοικονόμηση ενέργειας. Σε δίκτυα που εφαρμόζεται ο αλγόριθμος PIFA, οι κόμβοι χρειάζονται πιστώσεις για να μεταδώσουν τα δικά τους πακέτα, και οι οποίες μπορούν να αποκτηθούν μέσω της προώθησης πακέτων των υπόλοιπων κόμβων. Σημαντικό πλεονέκτημα του σχήματος, αποτελεί το γεγονός ότι μπορεί να εφαρμοστεί πάνω από οποιοδήποτε πρωτόκολλο δρομολόγησης, σε αντίθεση με ομοειδή σχήματα που εφαρμόζονται μόνο πάνω από το DSR, και χρειάζεται να γνωρίζουν πληροφορίες για το συνολικό μονοπάτι για να εφαρμοστούν.

4.3.1 ΠΕΡΙΓΡΑΦΗ ΤΟΥ PIFA

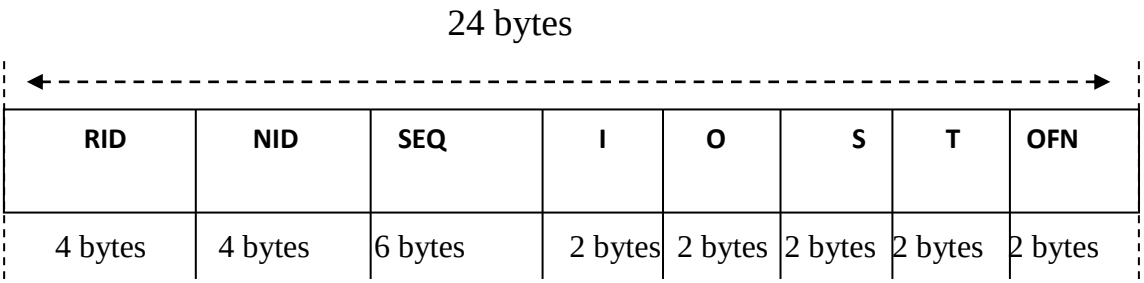
Σε ένα ασύρματο ad-hoc πάνω στο οποίο εφαρμόζεται το PIFA, οι κόμβοι γεννούν πακέτα, μόνο όταν διαθέτουν αρκετές πιστώσεις, οι οποίες μπορούν να αποκτηθούν μέσω της προώθησης πακέτων άλλων κόμβων. Το PIFA έχει τη δυνατότητα να ανιχνεύσει και να απομονώσει κάθε κόμβο που προσπαθεί να εξαπατήσει τους υπόλοιπους όσον αφορά τον αριθμό των προωθούμενων πακέτων, με σκοπό να αποκτήσει περισσότερες πιστώσεις από ότι πραγματικά πρέπει να λάβει. Έχει επίσης τη δυνατότητα να εντοπίσει πολλαπλούς κακόβουλους κόμβους, με την προϋπόθεση ότι δεν έχουν σχηματίσει μεταξύ τους κάποια συμπαιγνία. Θεωρείται ότι οι κόμβοι δεν γνωρίζουν πληροφορίες για το συνολικό μονοπάτι από την πηγή στον προορισμό, και ότι η μετάδοση πακέτου μεταξύ δύο γειτονικών κόμβων, πετυχαίνει πάντα.
Για τη λειτουργία του PIFA απαιτείται ένας κόμβος server που ονομάζεται **Διαχειριστής Πιστώσεων(CM)**, ο οποίος διαχειρίζεται την **Βάση Δεδομένων Πιστώσεων(CDB)** των κόμβων. Κάθε κόμβος που συμμετέχει στο ad-hoc δίκτυο, αναφέρει περιοδικά στον CM τον αριθμό των πακέτων που προώθησε στο συγκεκριμένο χρονικό διάστημα, και αυτός με τη σειρά του επικυρώνει την αξιοπιστία των αναφορών και συνάγει από αυτούς την τρέχουσα τοπολογία του δικτύου. Ο CM μπορεί να είναι είτε ο κόμβος του δικτύου με τους μεγαλύτερους πόρους σε ισχύ, είτε κάποιο access point.

Το πακέτο αναφοράς που αποστέλλουν οι κόμβοι στο διαχειριστή, αποτελείται από τα εξής πεδία:

- Το **RID,** το ID του αναφέροντα κόμβου
- Το **NID,** το ID ενός γειτονικού κόμβου
- Το **SEQ,** τον αριθμό ακολουθίας των αναφορών του τρέχοντος κόμβου για τον συγχρονισμό των μηνυμάτων αναφορών
- Το **I**, τον αριθμό των εισερχόμενων πακέτων από τον γειτονικό κόμβο
- Το **O**, τον αριθμό των εξερχόμενων προς τον γειτονικό κόμβο
- Το **S**, τον αριθμό των πακέτων που ξεκινούν στον τρέχοντα κόμβο ανάμεσα στα εξερχόμενα πακέτα προς τον γειτονικό κόμβο
- Το **T**, τον αριθμό των πακέτων που τερματίζουν στον τρέχοντα κόμβο ανάμεσα στα εισερχόμενα πακέτα από τον γειτονικό κόμβο

- Το **OFN**, τον αριθμό των πακέτων που δημιουργούνται από τον γειτονικό κόμβο ανάμεσα στα εισερχόμενα πακέτα από τον γειτονικό κόμβο

Σχηματικά το πακέτο αναφοράς φαίνεται παρακάτω.



Σχήμα 4.3.1

Όπως αναφέρθηκε, ο διαχειριστής CM έχοντα συλλέξει τα μηνύματα αναφοράς με τον ίδιο αριθμό ακολουθίας, επικυρώνει την αξιοπιστία των αναφορών σε τρία διαφορετικά στάδια.

1. Αρχικά, ελέγχει αν ο αριθμός των εξερχόμενων πακέτων από έναν κόμβο είναι ίδιος με τον αριθμό των εισερχόμενων πακέτων από τον απέναντι κόμβο στη ζεύξη για κάθε ζεύξη. Ορίζεται ως $\mathbf{Q_{n,m}}$, το πεδίο του πακέτου αναφοράς όπου n και m τα πεδία RID και NID αντίστοιχα, και οι κόμβοι n και m είναι γειτονικοί αναμεταξύ τους. Ισχύει τότε ότι $\mathbf{O_{n,m} = I_{n,m}}$.
2. Δεύτερον, ελέγχεται αν ισχύει ότι $F_n = \sum_{m \in A_n} I_{n,m} - \sum_{m \in A_n} T_{n,m} = \sum_{m \in A_n} O_{n,m} - \sum_{m \in A_n} S_{n,m}$,

   όπου F_n, ο αριθμός των πακέτων που προωθήθηκαν από τον κόμβο n σε μια περίοδο, και A_n, η ομάδα των γειτονικών κόμβων του n.

   Η διαφορά μεταξύ του συνολικού αριθμού των εισερχόμενων πακέτων και του συνολικού αριθμού των πακέτων που τερματίζουν σε έναν κόμβο, είναι ο αριθμός των πακέτων που προωθούνται. Επίσης, η διαφορά μεταξύ του συνολικού αριθμού των εξερχόμενων πακέτων και του συνολικού αριθμού των πακέτων που εκκινούν είναι η ίδια με τον αριθμό των προωθούμενων πακέτων. Ο CM, αυξάνει τις πιστώσεις για κάθε κόμβο κατ' αναλογία με το F_n, και όλοι οι κόμβοι οφείλουν να πληρώσουν αυτές τις πιστώσεις ανάλογα με την τιμή $\sum S \times H_{avg}$, σύμφωνα με τον αριθμό των πακέτων που παράγουν, όπου H_{avg}, είναι ο μέσος αριθμός βημάτων μεταξύ δύο κόμβων στο δίκτυο.

   Κατ' αρχήν οι πιστώσεις ενός κόμβου μειώνονται κατ' αναλογία με τον αριθμό των κόμβων των οποίων τα πακέτα διασχίζουν το δίκτυο μέχρι να φτάσουν στον προορισμό. Αν ο αριθμός των πιστώσεων ενός κόμβου μειώνεται κάτω από ένα καθορισμένο κατώφλι τ_c, ο CM αποστέλλει στον κόμβο ένα μήνυμα για να τον προειδοποιήσει ότι πρέπει να αποκτήσει πιστώσεις προωθώντας πακέτα άλλων κόμβων. Το μήνυμα προειδοποίησης αποστέλλεται περιοδικά μέχρι ο αριθμός των πιστώσεων να ξεπεράσει τ_c. Αν ένας κόμβος επιχειρήσει να στείλει δεδομένα αφού τελειώσουν οι πιστώσεις του, ο CM καταχωρεί τον κόμβο σε μια μαύρη λίστα και το ανακοινώνει σε όλους τους κόμβους του ad-hoc δικτύου ώστε να απορρίψουν τις αιτήσεις για προώθηση πακέτων τους. Όταν οι κόμβοι αποκτήσουν αρκετές πιστώσεις ώστε να στείλουν πάλι πακέτα δεδομένων, μπορούν να βγουν από τη μαύρη λίστα.

3. Τρίτον, το πεδίο S στην αναφορά ενός κόμβου πρέπει να είναι ίδιο με το πεδίο OFN, του επόμενου κόμβου. Ο σκοπός του πεδίου OFN είναι η πρόληψη της αλλαγής του F_n, από κάποιον κακόβουλο κόμβο, αλλάζοντας τον συνολικό αριθμό των πακέτων που εκκινούν από έναν κόμβο και τον συνολικό κόμβο των πακέτων που τερματίζουν. Το OFN καταγράφεται μετρώντας τον αριθμό των πακέτων που γεννιούνται σε ένα γειτονικό κόμβο ανάμεσα στα εισερχόμενα πακέτα στον γειτονικό κόμβο.

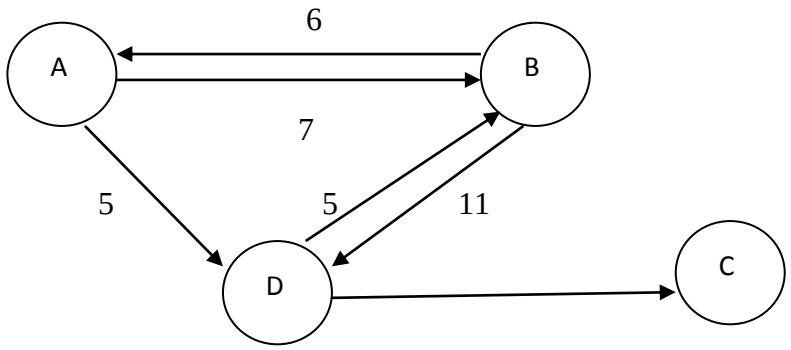
Από τη στιγμή που θα γίνει η επικύρωση και στα τρία αυτά στάδια, ο CM μπορεί να συμπεράνει την τοπολογία του δικτύου. Η τοπολογία μπορεί να μην είναι ακριβώς ίδια με την τρέχουσα τοπολογία λόγω της κίνησης των κόμβων, πράγμα που δεν έχει τόση σημασία, αφού δεν επηρεάζει τον υπολογισμό των αριθμών των προωθούμενων πακέτων, καθώς η τοπολογία δεν αφορά την δρομολόγηση αλλά την αξιοπιστία των αναφορών των κόμβων. Γνωρίζοντας την τοπολογία στην αρχή μιας περιόδου και στο τέλος της, μπορεί να εξαχθεί η τρέχουσα τοπολογία. Παρακάτω φαίνεται σχηματικά ένα παράδειγμα της παραπάνω διαδικασίας:

Μηνύματα αναφοράς προς τον CM

RID	***NID***	***SEQ***	***I***	***O***	***S***	***T***	***OFN***
A	B	128	6	7	7	2	2
A	B	128	0	5	1	0	0
B	A	128	7	6	2	3	7
B	D	128	5	11	7	1	3
C	D	128	3	0	0	3	2
D	A	128	5	0	0	4	1
D	B	128	11	5	3	9	7
D	C	128	0	3	2	0	0

Σχήμα 4.3.2

Υπολογιζόμενη τοπολογία από τις αναφορές



Σχήμα 4.3.3

4.3.2 ΑΝΙΧΝΕΥΣΗ ΚΑΚΟΒΟΥΛΩΝ ΚΟΜΒΩΝ

Στην περίπτωση που το πεδίο S στην αναφορά ενός κόμβου δεν σχετίζεται με το OFN του επόμενου κόμβου, ο διαχειριστής CM αρχικά υιοθετεί το OFN αφού στις περισσότερες φορές ο επόμενος κόμβος δεν έχει κίνητρο να εξαπατήσει όσον αφορά τον αριθμό των προωθούμενων πακέτων από τον προηγούμενο κόμβο. Παρόλα αυτά, υπάρχει περίπτωση ένας κόμβος να αποστέλλει συνεχώς λανθασμένες πληροφορίες με σκοπό να προκαλέσει σύγχυση στο δίκτυο. Για το λόγο αυτό το σχήμα PIFA διαθέτει μια μέθοδο που σκοπό έχει να απομονώσει τους κακόβουλους κόμβους, χρησιμοποιώντας αναφορές αποτυχιών του τεστ αξιοπιστίας. Στα πλαίσια της μεθόδου αυτής, ο CM διαθέτει τον ***Πίνακα Ασυνέπειας Καταγραφής(IRT)***, ο οποίος καταγράφει τον αριθμό των φορών που κάθε κόμβος φέρεται να έχει αλλάξει τις καταγραφές του. Ο πίνακας IRT έχει την εξής μορφή:

	a	b	c	d	…	Σύνολο
a	-	$m_{a,b}$	$m_{a,c}$	$m_{a,d}$	…	$\sum m_{a,i}$
b	$m_{b,a}$	-	$m_{b,c}$	$m_{b,d}$	…	$\sum m_{b,i}$
c	$m_{c,a}$	$m_{c,b}$	-	$m_{c,d}$	…	$\sum m_{c,i}$
d	$m_{d,a}$	$m_{d,b}$	$m_{d,c}$	-	…	$\sum m_{d,i}$
.	.	.	.	.	.	.
.	.	.	.	.	.	.
.	.	.	.	.	.	.

Σχήμα 4.3.4

Ως $m_{i,j}$, ορίζονται οι ***Αριθμοί Υποτιθέμενου Χειρισμού(NAM)*** που πιθανώς ο κόμβος i έχει επιχειρήσει με σκοπό να εξαπατήσει τον CM πάνω σε πληροφορίες εισερχόμενων και εξερχόμενων πακέτων μεταξύ αυτού και του κόμβου j. Αν το σύνολο των NAM κάθε κόμβου που φαίνονται στον πίνακα, είναι μεγαλύτερο ή ίσο από μια τιμή κατωφλίου, ο κόμβος αυτός αποκλείεται από το δίκτυο. Οι υπόλοιποι κόμβοι αγνοούν τα πακέτα του κόμβου αυτού αλλά και δε χρησιμοποιούν τον κόμβο αυτό ως ενδιάμεσο κόμβο για τα δικά τους πακέτα.

Στην περίπτωση που αναφορές δύο κόμβων, υποδεικνύουν ότι οι κόμβοι *α* και *β* δεν σχετίζονται μεταξύ τους, δεν είναι γνωστός ποιος από τους δύο μετέτρεψε τις αναφορές, και για τον λόγο αυτό αυξάνονται τα NAM και των δύο ως εξής:

$$m_{a,b} = m_{a,b} + 1 \quad \text{και} \quad m_{b,a} = m_{b,a} + 1.$$

Για να αποφευχθεί η άδικη τιμωρία κάποιων κόμβων, το πρωτόκολλο PIFA διαθέτει μια πολιτική για τα μείωση των NAM, στη λογική ότι ένας κακόβουλος κόμβος πραγματοποιεί επαναλαμβανόμενες ενέργειες για να εξαπατήσει άλλους. Έτσι, αν οι κόμβοι *α* και *β* αναφέρουν αβάσιμες πληροφορίες, τα NAM άλλων κόμβων που σχετίζονται με τους κόμβους αυτούς, μειώνονται στο μισό ως εξής:

$$m_{i,a} = \left\lfloor \frac{m_{i,a}}{2} \right\rfloor, \forall i \notin \{a,b\} \quad \text{και} \quad m_{i,b} = \left\lfloor \frac{m_{i,b}}{2} \right\rfloor, \forall i \notin \{a,b\}$$

4.3.3 ΠΟΛΥΠΛΟΚΟΤΗΤΑ ΤΟΥ PIFA

Σε ένα δίκτυο στο οποίο εφαρμόζεται το PIFA, κάθε κόμβος στέλνει μηνύματα αναφοράς στον CM στο τέλος κάθε περιόδου. Οι αναφορές αυτές δεν αφορούν μόνο τους γειτονικούς κόμβους, αλλά και τους κόμβους που βγήκαν από την εμβέλεια μετάδοσης κατά τη διάρκεια της περιόδου. Έτσι, ένας κόμβος i στέλνει αναφορές στους εξής τρεις τύπους κόμβων:

- Τους κόμβους που παραμένουν στην εμβέλεια του κόμβου i από την αρχή μέχρι το τέλος της περιόδου.
- Τους κόμβους που βγήκαν από την εμβέλεια του κόμβου i στη διάρκεια της περιόδου.
- Τους κόμβους που εισήχθησαν στην εμβέλεια του κόμβου i στη διάρκεια της περιόδου.

Υποθέτοντας ότι οι κόμβοι είναι πάντα ομοιόμορφα κατανεμημένοι, ο κόμβος i έχει πάντα τον ίδιο αριθμό γειτόνων στο τέλος κάθε περιόδου, με αποτέλεσμα οι κόμβοι των τελευταίων δύο τύπων κόμβων που αναφέρθηκαν, να έχουν πάντα τον ίδιο αριθμό. Έτσι, αν n είναι ο μέσος αριθμός γειτονικών κόμβων σε κάθε περίοδο και *α* ο αριθμός των κόμβων που εισήχθησαν ή βγήκαν στην εμβέλεια του κόμβου κατά τη διάρκεια μιας περιόδου, ο συνολικός αριθμός των αναφορών του κόμβου i, είναι ίσος με $n + a$. Τα n και α, εξάγονται από τους εξής μαθηματικούς τύπους:

$n = \frac{N\pi r^2}{A} - 1$, όπου N ο συνολικός αριθμός των κόμβων, r η εμβέλεια μετάδοσης και A η συνολική περιοχή του δικτύου.

$a = nP$, όπου P η πιθανότητα δύο κόμβοι που είναι γειτονικοί στη διάρκεια μιας περιόδου, να μην είναι γειτονικοί στην επόμενη περίοδο.

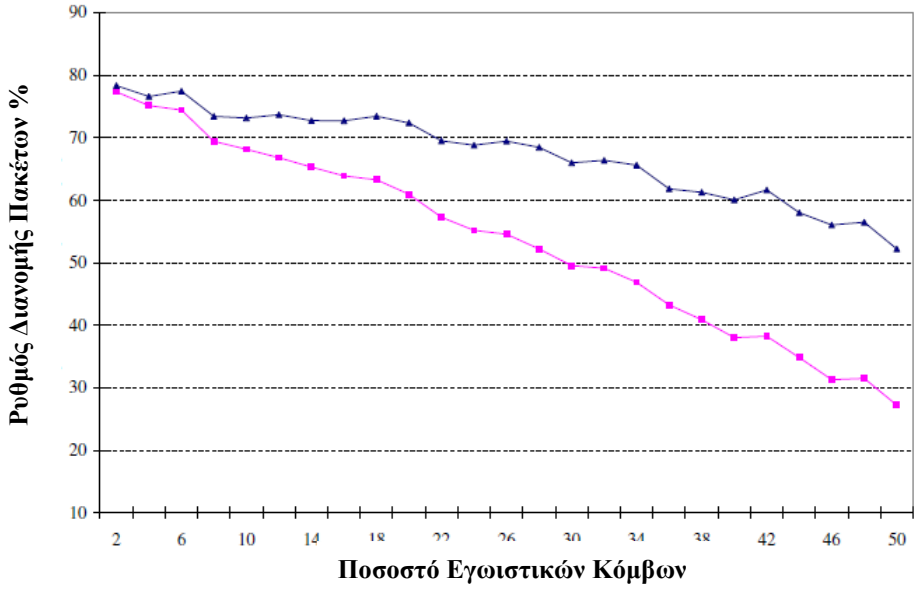
Αποδεικνύεται μαθηματικά, ότι σε ένα δίκτυο που αποτελείται από N κόμβους, ο συνολικος αριθμός αναφορών που πρέπει να διαχειριστεί ο CM είναι ίσος με $N\left(\frac{N\pi r^2}{A} - 1\right) \times 1.036$ (έχοντας παραδεχτεί ορισμένες καθορισμένες τιμές), μια χαμηλή σχετικά πολυπλοκότητα από τη στιγμή που κάθε κόμβος στο PIFA αποστέλλει αναφορά περιοδικά αφού συλλέξει πληροφορίες.

4.3.4 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ PIFA

Οι δημιουργοί του σχήματος PIFA, χρησιμοποίησαν τον προσομοιωτή δικτύων ns-2 με σκοπό να πραγματοποιήσουν προσομοιώσεις, ώστε να βγάλουν συμπεράσματα για την αποτελεσματικότητα του PIFA στην αντιμετώπιση των εγωιστικών κόμβων και την επιρροή του στην απόδοση του δικτύου. Οι προσομοιώσεις πραγματοποιήθηκαν στο παρακάτω περιβάλλον προσομοίωσης:

- Αριθμός κόμβων 50
- Περιοχή 1000m x 1000m
- Τυχαία κίνηση
- Μέγιστη ταχύτητα 20 m/s
- Εμβέλεια μετάδοσης 250 m
- Χωρητικότητα καναλιού 2 Mbps
- Μείωση ισχύος για απόσταση d, κατά $1/d^4$
- Πρωτόκολλο δρομολόγησης AODV
- Πρωτόκολλο MAC 802.11
- Τυχαία επιλογή πηγής-προορισμού
- Δημιουργία από την πηγή δύο πακέτων CBR των 512 bytes ανά δευτερόλεπτο
- Αρχική ενέργεια κόμβου 95 Joule
- Περίοδος μηνυμάτων αναφοράς 1s
- Αρχικές πιστώσεις κόμβου 10
- Χρόνος προσομοίωσης 1000s
- 30 προσομοιώσεις για κάθε μέτρηση – μέσος όρος

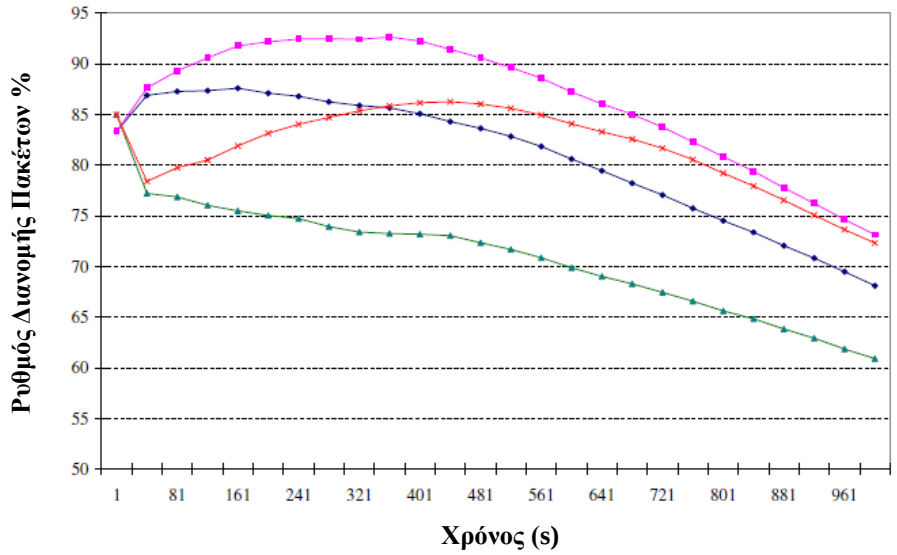
Από τις προσομοιώσεις οι κατασκευαστές του PIFA εξήγαγαν τα εξής συμπεράσματα που φαίνονται στα αντίστοιχα γραφήματα:



Διάγραμμα 4.3.1 (Πηγή **[14]**)

Στο διάγραμμα αυτό, που στον κάθετο άξονα έχει τον ***ρυθμό διανομής των πακέτων επί τοις εκατό***, και στον οριζόντιο άξονα ***το ποσοστό των εγωιστικών κόμβων στο***

δίκτυο, με την ροζ γραμμή ορίζονται τα αποτελέσματα για ένα δίκτυο στο οποίο δεν εφαρμόζεται το PIFA, ενώ με τη μπλε γραμμή ένα δίκτυο που εφαρμόζεται το PIFA. Συμπεραίνεται αρχικά ότι όσο αυξάνεται το ποσοστό των εγωιστικών κόμβων, μειώνεται ο ρυθμός διανομής των πακέτων. Παρόλα αυτά, στο δίκτυο που εφαρμόζεται το PIFA πετυχαίνεται σύμφωνα με τα αποτελέσματα, η διατήρηση του ρυθμού διανομής πάνω από το 50% ακόμα και όταν οι μισοί κόμβοι στο δίκτυο είναι εγωιστικοί. Κάτι τέτοιο οφείλεται στο γεγονός ότι το PIFA υποχρεώνει τους εγωιστικούς κόμβους να προωθούν τα πακέτα άλλων κόμβων τουλάχιστον όταν οι ίδιοι χρειάζονται πιστώσεις, ενώ στην περίπτωση μη εφαρμογής του δεν θα προωθούσαν καθόλου πακέτα.



Διάγραμμα 4.3.2 (Πηγή **[14]**)

Στο παραπάνω διάγραμμα που στον κάθετο άξονα έχει τον ***ρυθμό διανομής των πακέτων επί τοις εκατό***, και στον οριζόντιο άξονα τον ***χρόνο σε δευτερόλεπτα,*** ορίζονται:
- Με τη μπλε γραμμή ένα δίκτυο που δεν χρησιμοποιεί PIFA και έχει ένα 10% εγωιστικούς κόμβους.
- Με την πράσινη γραμμή ένα δίκτυο που δεν χρησιμοποιεί PIFA και έχει ένα 20% εγωιστικούς κόμβους.
- Με τη ροζ γραμμή, ένα δίκτυο που χρησιμοποιεί PIFA και έχει ένα 10% εγωιστικούς κόμβους.
- Με την κόκκινη γραμμή, ένα δίκτυο που χρησιμοποιεί PIFA και έχει ένα 20% εγωιστικούς κόμβους.

Παρατηρείται αρχικά ότι σε όλες τις περιπτώσεις, με την πάροδο του χρόνου και την αύξηση των εγωιστικών κόμβων, μειώνεται ο ρυθμός διανομής πακέτων, λόγω της εξάντλησης της ενέργειας των μη εγωιστικών κόμβων, και τη συγκέντρωση της προωθητικής διαδικασίας σε αυτούς. Παρόλα αυτά, φαίνεται, ότι στην περίπτωση εφαρμογής του PIFA, αυξάνεται για ένα χρονικό διάστημα ο ρυθμός διανομής, λόγω της ανάγκης των εγωιστικών κόμβων για πιστώσεις, που τους αναγκάζει να προωθήσουν πακέτα άλλων κόμβων.

Συμπερασματικά, το PIFA αποτελεί έναν μηχανισμό υποστήριξης συνεργασίας για ad-hoc δίκτυα, βασισμένο στις πιστώσεις, που μπορεί να εφαρμοστεί πάνω από

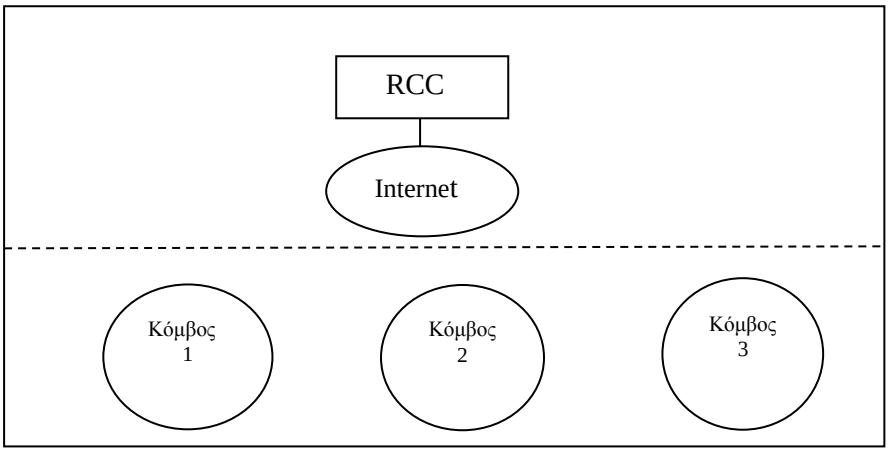
οποιοδήποτε πρωτόκολλο δρομολόγησης, και ενισχύει την εθελοντική προώθηση πακέτων από τους εγωιστικούς κόμβους, πετυχαίνοντας βελτίωση της απόδοσης του ad-hoc δικτύου στην περίπτωση ύπαρξης εγωιστικών κόμβων.

4.4 EXPRESS

Το Express [15], αποτελεί μηχανισμό υποστήριξης συνεργασίας βασισμένο σε πιστώσεις, που δεν χρησιμοποιεί ειδικό hardware στη λειτουργίας του. Επιδίωξη του είναι η μείωση του υπολογιστικού overhead στους κινητούς κόμβους, αλλά και η παροχή ασφάλειας ενάντια σε πιθανή απάτη κάποιων κόμβων. Αυτό πετυχαίνεται με χρήση αλυσίδων hash, ώστε να μειωθούν οι λειτουργίες που απαιτούν ψηφιακές υπογραφές. Πιο συγκεκριμένα, κάθε κόμβος πηγή χρησιμοποιεί ψηφιακή υπογραφή μόνο στην πρώτη συναλλαγή με κάποιον συνεργάσιμο ενδιάμεσο κόμβο, ενώ όλες οι άλλες συναλλαγές πραγματοποιούνται από τους κόμβους με λειτουργίες hash. Η αρχιτεκτονική του Express είναι παρόμοια με αυτή του σχήματος Sprite, με την ύπαρξη μιας κεντρικής CCS που αναλαμβάνει την απόδοση πιστώσεων στους κόμβους που συνεργάζονται στην προώθηση πακέτων, και την μείωση των πιστώσεων στους κόμβους που μεταδίδουν τα δικά τους πακέτα μέσα από το δίκτυο.

4.4.1 ΠΕΡΙΓΡΑΦΗ ΤΟΥ EXPRESS

Το σχήμα Express αποτελείται ένα **Αξιόπιστο Κέντρο Εκτελωνισμού(RCC)** και έναν αριθμό κινητών κόμβων που συνεργάζονται μεταξύ τους για την προώθηση της κίνησης του δικτύου. Το RCC έχει παρόμοια λειτουργία με την CCS του σχήματος Sprite αλλά οι μέθοδοι ελέγχου και τα μοντέλα απόδοσης κινήτρων διαφέρουν. Οι κόμβοι του δικτύου είναι εφοδιασμένοι με διεπαφές δικτύου ώστε να μπορούν να μεταδώσουν και να παραλάβουν μηνύματα στο ασύρματο δίκτυο, πράγμα που πετυχαίνεται με χρήση του πρωτοκόλλου GPRS σε εξωτερικούς χώρους, και του 802.11 ή του Bluetooth σε εσωτερικούς χώρους. Σε αντίθεση με τους κινητούς κόμβους, το RCC δεν ενέχει περιορισμό σε πόρους ενέργειας και υπολογιστικούς πόρους. Στο Express, για να γίνει δυνατή η αναγνώριση των κόμβων που ανήκουν σε ένα δίκτυο, θεωρείται ότι κάθε κόμβος έχει λάβει ένα πιστοποιητικό από μια Αρχή Πιστοποίησης (CA), ενώ χρησιμοποιείται επίσης το πρωτόκολλο δρομολόγησης DSR. Η αρχιτεκτονική του Express σχηματικά φαίνεται στο παρακάτω σχήμα.



Σχήμα 4.4.1

Το κέντρο RCC διαχειρίζεται τους λογαριασμούς πιστώσεων των κόμβων του δικτύου. Σε κάθε μονοπάτι μετάδοσης, κάθε ενδιάμεσος κόμβος δίνει μια αναφορά για την συνεργασία του στην προώθηση πακέτων στο RCC, και ομοίως ο κόμβος

πηγή. Στο τέλος προκαθορισμένων χρονικών περιόδων, το RCC εκκαθαρίζει τις πιστώσεις βασιζόμενο στις αναφορές. Έτσι, ο κόμβος πηγή χάνει πιστώσεις για την μετάδοση του πακέτου, και οι ενδιάμεσοι κόμβοι που έχουν συμμετάσχει στην προώθηση του πακέτου, αποκτούν πιστώσεις. Με τον τρόπο αυτό, οι κόμβοι μπορούν να αυξήσουν τον λογαριασμό πιστώσεων τους, είτε με καταβολή πιστώσεων στο λογαριασμό τους, είτε με την προώθηση πακέτων άλλων κόμβων, και με τις πιστώσεις αυτές προωθούν τα δικά τους πακέτα.
Η αποστολή των αναφορών των κόμβων στο RCC, στον μηχανισμό υποστήριξης συνεργασίας Express, πραγματοποιείται ως εξής: Οι κόμβοι αποθηκεύουν τις αναφορές τους σε έναν αποθηκευτικό χώρο, και τις καταθέτουν στο RCC, μέσω ενός υπολογιστή proxy, περιοδικά, πάνω από ένα ασφαλές κανάλι. Για τη δημιουργία μιας σωστής αναφοράς, κάθε ενδιάμεσος κόμβος χρειάζεται να έχει μια επίσημη αίτηση για συνεργασία από την πηγή. Έτσι, για κάθε μήνυμα ο κόμβος πηγή, δημιουργεί την αίτηση αυτήν και την αποστέλλει μέσω του μηνύματος στους κόμβους του μονοπατιού. Στη συνέχεια, κάθε ενδιάμεσος κόμβος διαλέγει την δική του αίτηση από το μήνυμα και αποφασίζει αν θα προωθήσει το μήνυμα στον επόμενο κόμβο. Οι αιτήσεις που αναφέρθηκαν για κάθε κόμβο, αποτελούν στοιχεία μιας αλυσίδας hash και αποστέλλονται από την πηγή στον κόμβο, η μια μετά την άλλη, κατά την επικοινωνία τους. Με τον τρόπο αυτό, οι ενδιάμεσοι κόμβοι δεν είναι δυνατό να απομιμηθούν την αίτηση, και ο κόμβος πηγή δεν μπορεί να αρνηθεί την έκδοση της αίτησης. Φαίνεται εδώ η διαφορά από το σχήμα Sprite, που σε κάθε πακέτο οι αιτήσεις υποστηρίζονται από ψηφιακές υπογραφές.
Για τη λειτουργία του RCC, στο Express, θεωρείται ότι το RCC ανοίγει έναν λογαριασμό πιστώσεων και εκδίδει ένα ψηφιακά υπογεγραμμένο πιστοποιητικό με ημερομηνία λήξης, για κάθε κόμβο που προτίθεται να μπει στο δίκτυο. Ο κόμβος πηγή προωθεί τα πακέτα μόνο μέσω των ενδιάμεσων κόμβων που διαθέτουν έγκυρο πιστοποιητικό από το RCC. Λόγω της ικανότητας του RCC να ανιχνεύει την συνεργασιμότητα των κόμβων μέσω των αναφορών, αποτρέπονται από το πρωτόκολλο οι ανανεώσεις των πιστοποιητικών από κακόβουλους ή μη συνεργάσιμους κόμβους.

Παρακάτω περιγράφεται η λειτουργία των κόμβων στον μηχανισμό υποστήριξης συνεργασίας Express:
Σε ένα τυπικό σενάριο μετάδοσης πακέτου, ο κόμβος πηγή S βρίσκει το μονοπάτι προς τον προορισμό D μέσω n ενδιάμεσων κόμβων m_i(για i = 1,…,n). Ο D αποτελεί τον τελευταίο κόμβο στο μονοπάτι, δηλαδή τον m_n. Η πηγή S σε κάθε συναλλαγή με κάθε ενδιάμεσο κόμβο m_i, παράγει μια συγκεκριμένη αλυσίδα hash για τον κόμβο, και την διατηρεί για μελλοντικές συναλλαγές. Η αλυσίδα hash $H_i^s = (w_0^{s\to i}, w_1^{s\to i}, ..., w_{n'}^{s\to i})$, αποτελεί ένα διάνυσμα από τιμές σύνοψης $w_k^{s\to i}$ (για j = 1,….,k). Η πηγή S χρησιμοποιεί κάθε τέτοια τιμή ως αίτηση συνεργασίας. Έτσι, η τιμή $w_k^{s\to i}$ ορίζει την jκοστή τιμή που εκδίδεται από την S για τον iκοστό ενδιάμεσο κόμβο. Η τιμή αυτή έχει την ακόλουθη ιδιότητα:

$w_k^{s\to i} = h(w_{k+1}^{s\to i})$ για κάθε k = 0,1,….,n’ – 1, όπου h μια ισχυρή συνάρτηση hash όπως ο MD5 ή ο SHA.
Ένα διάνυσμα $H_s = (H_1^s, ..., H_i^s, ..., H_n^s)$ όλων των αλυσίδων hash που έχει παράξει για τους ενδιάμεσους κόμβους, κρατείται από την πηγή. Για την αποφυγή εξάντλησης

μεγάλου χώρου μνήμης με την αύξηση του n, το Express χρησιμοποιεί δένδρα hash αλυσίδων.

Για την κατανόηση της λειτουργίας του Express παρουσιάζεται το παρακάτω παράδειγμα:

Έστω ότι ο κόμβος πηγή S επιθυμεί να αποστείλει το t-οστό του πακέτο p_t^s. Προσθέτει κάποιες επιπλέον πληροφορίες στο πακέτο μέσω της παρακάτω διαδικασίας. Για κάθε κόμβο m_i στο μονοπάτι του p_t^s, η πηγή πραγματοποιεί μια εκ των δύο ενεργειών που ακολουθούν:

1. Εάν είναι η πρώτη φορά που ο κόμβος m_i, συμμετέχει στην προώθηση ενός πακέτου της πηγής S, η πηγή παράγει την αλυσίδα H_i^s, δημιουργεί το συμβόλαιο C_i^s και το περιλαμβάνει στο πακέτο p_t^s. Το συμβόλαιο, περιέχει την τιμή $w_0^{s\to i}$, την ταυτότητα της πηγής S, και υπογράφεται ψηφιακά από την πηγή.
2. Εάν ο κόμβος m_i, έχει προωθήσει στο παρελθόν κάποιο πακέτο του κόμβου S, η αντίστοιχη αλυσίδα έχει ήδη δημιουργηθεί. Έτσι, αν η τιμή $w_{l-1}^{s\to i}$ είναι η τελευταία τιμή που έχει σταλεί στον m_i από τον S, η πηγή περιλαμβάνει το ζεύγος ($w_{l-1}^{s\to i}$, l) στο πακέτο.

Στη συνέχεια ο κόμβος πηγή S μεταδίδει το τροποποιημένο πακέτο στον πρώτο ενδιάμεσο κόμβο του μονοπατιού. Κάθε ενδιάμεσος κόμβος m_i, κρατά τα δικά του δεδομένα από το πακέτο και τα επικυρώνει. Αν αυτή είναι η πρώτη συναλλαγή μεταξύ των κόμβων m_i και S, ο πρώτος επικυρώνει τα δεδομένα C_i^s ελέγχωντας την υπογραφή του S σε αυτά. Για επόμενες συναλλαγές, ο m_i επικυρώνει την τιμή $w_l^{s\to i}$ εξετάζοντας αν είναι μετατρέψιμη στην προηγούμενη τιμή $w_{l-1}^{s\to i}$ που λήφθηκε. Με τον τρόπο αυτό ο m_i μπορεί να είναι σίγουρος ότι το πακέτο προέρχεται από τον S. Αν η επικύρωση αποτύχει, το πακέτο απορρίπτεται, αλλιώς ο κόμβος m_i, δημιουργεί μια αναφορά $R_i^{s,t}$ του πακέτου και την αποθηκεύει μαζί και με την τιμή $w_l^{s\to i}$. Τελικά, ο m_i προωθεί το πακέτο στον επόμενο κόμβο στο μονοπάτι, και η διαδικασία αυτή συνεχίζεται μέχρι το πακέτο να φτάσει στον προορισμό. Η αναφορά που παράγει ο κόμβος m_i, για το πακέτο p_t^s παράγεται ως εξής:

$$R_i^{s,t} = h'(p_t^s, w_l^{s\to i})$$

, όπου $w_l^{s\to i}$ είναι η τιμή σύνοψης που λαμβάνει ο m_i, για την προώθηση του πακέτου p_t^s.

Η h’ , που είναι ίδια για όλους τους κόμβους, αποτελεί μια ισχυρή συνάρτηση hash που λειτουργεί όπως η h αλλά δέχεται δύο εισόδους, το περιεχόμενο του πακέτου και την τιμή σύνοψης. Η h’ συνδυάζει τις δύο αυτές τιμές και κρυπτογραφεί το αποτέλεσμα.

Το μήκος της αλυσίδας hash βασίζεται στην διαθέσιμη μνήμη, και να δεν καλυφθεί από τα καταχωρημένα πακέτα, μπορεί να χρησιμοποιηθεί και για μελλοντικές συναλλαγές. Αντίθετα, αν το μήκος ξεπεραστεί, η πηγή S πρέπει να εκκινήσει μια καινούρια αλυσίδα hash.

4.4.2 ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ RCC

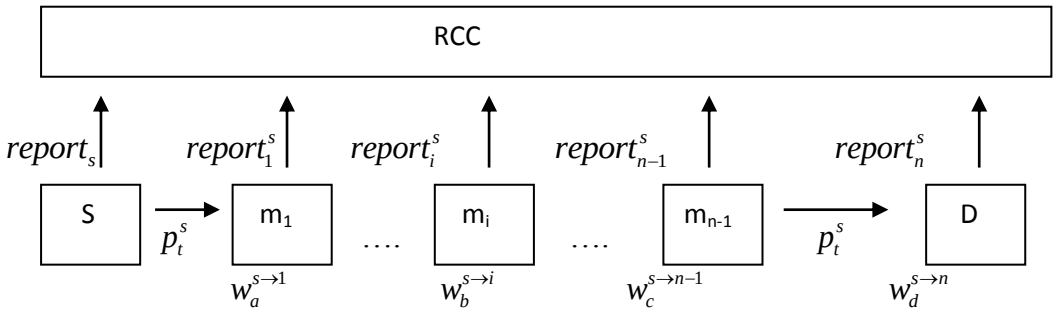
Όπως αναφέρθηκε, το RCC απαιτεί αναφορές από τους κινητούς κόμβους για να διαχειριστεί τις πιστώσεις. Η αναφορά που δίδεται από έναν ενδιάμεσο κόμβο m_i, έχει την εξής μορφή:

$$report_i^s = \{w_l^{s\to 1}, l_i^s, C_i^s, \{R_i^{s,t}, R_i^{s,t'}, ...\}\}$$

, όπου $w_l^{s\to 1}$ η τελευταία τιμή σύνοψης που λαμβάνεται στον m_i, από τον S, l_i^s ο αριθμός των τιμών σύνοψης που λαμβάνονται στον m_i, από τον S, C_i^s ένα συμβόλαιο που υπογράφεται από τον S για τον m_i, και περιλαμβάνει την τιμή $w_0^{s\to i}$, και $\{R_i^{s,t}, R_i^{s,t'}, ...\}$ περιλαμβάνει τις αποδείξεις είσπραξης για τα πακέτα $(p_t^s, p_{t'}^s, ...)$ του S, που έχει προωθήσει ο m_i.
Αναφορά στο RCC δίνει και ο κόμβος πηγή S, και η αναφορά αυτή έχει την παρακάτω μορφή:

$$report_s = \{\{Path_1^s, R'^{s,1}_a, R'^{s,1}_b, ...\}, ..., \{Path_t^s, R'^{s,t}_i, R'^{s,t}_j, ...\}, ..., \{Path_{n''}^s, R'^{s,n''}_u, R'^{s,n''}_v, ...\}\},$$

όπου το σετ $\{Path_t^s, R'^{s,t}_i, R'^{s,t}_j, ...\}$ σχετίζεται με το πακέτο p_t^s. Συγκεκριμένα, το $Path_t^s$ είναι το μονοπάτι μετάδοσης για το πακέτο, ενώ τα άλλα στοιχεία του σετ είναι οι αποδείξεις είσπραξης που σχετίζονται με το πακέτο, τις οποίες παράγει ο S για τους ενδιάμεσους κόμβους του μονοπατιού. Παρακάτω φαίνεται σχηματικά η αλληλεπίδραση των κόμβων με το RCC:



Σχήμα 4.4.2

Όπως αναφέρθηκε, το RCC εκκαθαρίζει πιστώσεις περιοδικά. Οι αποφάσεις του εξαρτώνται από τις ληφθέντες αναφορές και για το λόγο αυτό, πρέπει να γνωρίζει αν είναι αληθείς. Χρησιμοποιώντας την αναφορά $report_i^s$ το RCC επικυρώνει την τιμή $w_l^{s\to i}$ προσδιορίζοντας πόσες εφαρμογές της h απαιτούνται για να καθοριστεί η τιμή $w_l^{s\to i}$ στην $w_0^{s\to i}$. Ο αριθμός αυτών των βημάτων πρέπει να είναι ίσος με l_i^s
Το RCC παρατηρώντας την αναφορά της πηγής $report_s$ πρέπει να σιγουρευτεί ότι η πηγή δεν έχει πραγματοποιήσει απάτη στην αναφορά του μονοπατιού $Path_t^s$, και για το λόγο αυτό υπολογίζει τον αριθμό των διαδρομών δρομολόγησης των πακέτων του S, στις οποίες συμμετέχει ο κόμβος m_i. Η τιμή αυτή ορίζεται όπως φαίνεται παρακάτω:

$$x_i^s = \sum_{t=1}^{n''} E(i,t)$$

, όπου $E(i,t) = \begin{cases} 1 & αν\ m_i\ ανήκει\ στο\ Path_t^s \\ 0 & αλλιώς \end{cases}$

Εάν υπάρχει $x_i^s < l_i^s$, τότε το RCC θεωρεί ότι ο S προσπάθησε να εξαπατήσει, αναφέροντας λανθασμένες διαδρομές δρομολόγησης πακέτων.
Το RCC για να αναγνωρίσει ποιοι ενδιάμεσοι κόμβοι έχουν συμμετάσχει στην προώθηση του πακέτου p_t^s, ακολουθεί τα εξής δύο βήματα. Πρώτον, αν όταν λάβει το $R_i^{s,t}$, διαπιστώσει ότι δεν έχει διαφορά με το $R'^{s,t}_i$, συμπεραίνει ότι ο κόμβος m_i, έχει λάβει το πακέτο. Δεύτερον, ελέγχει αν το πακέτο έφτασε στον προορισμό, προσδιορίζοντας αν ο κόμβος m_k που είναι ο τελευταίος στο μονοπάτι, ταυτίζεται με τον D. Με την πάροδο των δύο αυτών βημάτων, το RCC α πιστώσεις στους κόμβους από m_1 έως m_{k-1}, και β πιστώσεις στον m_k (όπου $\alpha>\beta$). Τέλος, αφαιρεί το άθροισμα των πληρωμένων πιστώσεων από το λογαριασμό του S.

4.4.3 ΜΗΧΑΝΙΣΜΟΙ ΠΡΟΛΗΨΗΣ

Σε ένα δίκτυο που εφαρμόζεται το Express, οι εγωιστικοί κόμβοι μπορεί να πραγματοποιήσουν κάποιες εκ των παρακάτω εγωιστικών ενεργειών:

- Μετά τη λήψη ενός μηνύματος, ο κόμβος αποθηκεύει μια απόδειξη πληρωμής και μια τιμή σύνοψης προς αναφορά στο RCC, αλλά τελικά δεν προωθεί το μήνυμα
- Ο κόμβος έχει λάβει το μήνυμα αλλά δεν αναφέρει την απόδειξη πληρωμής .
- Ο κόμβος πηγή παραποιεί τη λίστα των διαδρομών δρομολόγησης των πακέτων που αναφέρει.
- Οι κόμβοι παραποιούν τις δικές τους αποδείξεις είσπραξης.

Με τις κατάλληλες συναρτήσεις στους πράκτορες και τα κατάλληλα κίνητρα που προσφέρονται σε αυτούς, **το Express καθιστά δυνατό να πειστούν οι εγωιστικοί κόμβοι ώστε να χρησιμοποιούν τους διαθέσιμους πόρους τους για να προωθούν τα πακέτα άλλων κόμβων και να αναφέρουν τις αποδείξεις είσπραξης των ληφθέντων πακέτων**. Για να υπάρχουν τα κατάλληλα κίνητρα, χρειάζεται οι πιστώσεις που λαμβάνει ένας συνεργάσιμος κόμβος να είναι περισσότερες από αυτές ενός μη συνεργάσιμου κόμβου. Για τους κόμβους των οποίων οι πόροι ενέργειας είναι εξαιρετικά λίγοι και δεν μπορούν να προωθήσουν μηνύματα, δεν είναι δυνατό να συμμετέχουν στην προώθηση πακέτων, και για το λόγο αυτό χάνουν τις πιστώσεις τους με αποτέλεσμα να μην μπορούν να προωθήσουν ούτε τα δικά τους μηνύματα, με αποτέλεσμα σταδιακά να εξάγονται από το δίκτυο μέχρι να ανακτήσουν τους ενεργειακούς τους πόρους. Με σκοπό να μην επιλέγονται τέτοιοι κόμβοι για τις διαδρομές δρομολόγησης, οι αλγόριθμοι δρομολόγησης που χρησιμοποιούνται είναι οι MTPR, MMBCR και CMMBCR.
Ακόμα το Express διαθέτει μηχανισμό για απόδοση κινήτρων στην πηγή ώστε να αναφέρει τα μονοπάτια ορθώς. Όπως αναφέρθηκε, το RCC μπορεί να επικυρώσει το μονοπάτι $Path_t^s$ χρησιμοποιώντας την αναφορά $report_i^s$. Αν ο S πραγματοποιήσει

απάτη κατά την αναφορά διαδρομών δρομολόγησης, θα αναγκαστεί να πληρώσει για όλες τις τιμές σύνοψης που έχουν λάβει από αυτόν οι ενδιάμεσοι κόμβοι. Επιπλέον, ο κόμβος S, θα τιμωρηθεί από το RCC με πληρωμή ε πιστώσεων, όπου ε μια μικρή θετική τιμή. Έτσι, σε περίπτωση απάτης, ο κόμβος S χάνει τις ακόλουθες πιστώσεις:

$$C_f^s = \left[\sum_{i=1}^{n} (l_i^s \times a) \right] + \varepsilon$$

, όπου l_i^s ο αριθμός των τιμών σύνοψης που έχει λάβει ο κόμβος m_i, από τον S, α οι πιστώσεις που λαμβάνει ένας κόμβος για την προώθηση του μηνύματος και ε η ποινή που επιβάλλεται στον S όπως αναφέρθηκε.
Ωστόσο, αν οι διαδρομές δρομολόγησης έχουν αναφερθεί σωστά στο RCC, ελέγχοντας τις αποδείξεις είσπραξης, το RCC μπορεί να προσδιορίσει για ποια από τις τιμές σύνοψης που έχει αναφέρει ένας κόμβος, είχε συνάμα προωθήσει και το μήνυμα. Στη συνέχεια, μεταφέρει τις πιστώσεις από τον λογαριασμό του S, στους άλλους κόμβους, μόνο για τις τιμές σύνοψης των οποίων το αντίστοιχο μήνυμα προωθήθηκε. Επίσης, όταν ένα πακέτο δεν έχει φτάσει στον προορισμό, ο τελευταίος κόμβος που έχει αναφέρει την απόδειξη είσπραξης, λαμβάνει β πιστώσεις αντί για α, πράγμα το οποίο μειώνει το ποσό των πιστώσεων που θα χάσει ο κόμβος S. Έτσι, οι πιστώσεις που χάνει τελικά ο κόμβος S, ορίζεται ως:

$$C_h^s \le \sum_{i=1}^{n} (k_i^s \times a)$$

, όπου k_i^s ο αριθμός των μηνυμάτων που έχει προωθήσει ο κόμβος m_i, για τον S, και $k_i^s \le l_i^s$. Προφανώς είναι βέλτιστη στρατηγική για τον S να αναφέρει τις σωστές λίστες διαδρομών δρομολόγησης.

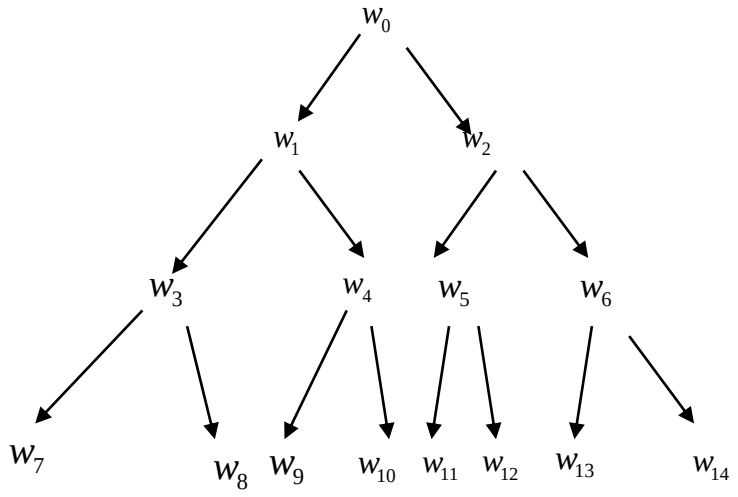
Τέλος, **το Express φροντίζει και για την πρόληψη των ψευδών αποδείξεων** είσπραξης. Κατά τη διαδικασία αυτή, γίνονται δύο παραδοχές. Πρώτον ότι όταν οι αποδείξεις είσπραξης είναι διαφορετικές, μια εκ των δύο πλευρών πραγματοποιεί απάτη, και δεύτερον ότι όταν είναι ίδιες, ο ενδιάμεσος κόμβος ήταν στη διαδρομή δρομολόγησης του πακέτου και έλαβε σωστά το πακέτο της πηγής.
Ένας ενδιάμεσος κόμβος δεν μπορεί να μην αναφέρει σωστά μια απόδειξη είσπραξης για ένα πακέτο που δεν έχει λάβει ο κόμβος, ή για ένα πακέτο για το οποίο ο κόμβος δεν ήταν στη διαδρομή δρομολόγησης του, για τους παρακάτω λόγους:

- Ο κόμβος m_i, δεν μπορεί να παράξει μια απόδειξη είσπραξης για ένα μήνυμα ώστε αυτή να είναι ίδια με την απόδειξη είσπραξης της πηγής, εκτός αν έχει το μήνυμα p_t^s και την σχετιζόμενη τιμή σύνοψης $w_l^{s \to i}$.
- Ο ενδιάμεσος κόμβος m_i, μπορεί να παράγει τις αποδείξεις είσπραξης για όλους τους επόμενους κόμβους στο μονοπάτι, και τους τις αποστέλλει, πράγμα που προσθέτει overhead από επιπλέον λειτουργίες hash, χωρίς όμως αυτό να του δίνει κάποιο όφελος.

Ο κόμβος πηγή επίσης δεν έχει κίνητρο να παραποιήσει την απόδειξη είσπραξης του, καθώς αν το RCC λάβει διαφορετικές αποδείξεις από τον m_i και τον S, ο m_i όχι μόνο δεν λαμβάνει πιστώσεις για την προώθηση του αντίστοιχου μηνύματος αλλά τιμωρείται και με πληρωμή ε πιστώσεων. Ακόμα σε αυτή την περίπτωση το RCC χρεώνει πηγή με $\alpha+\varepsilon$ πιστώσεις, των οποίων η τιμή είναι μεγαλύτερη από το κόστος για την προώθηση ενός πακέτου.

4.4.4 ΔΕΝΔΡΑ ΑΛΥΣΙΔΩΝ HASH

Όπως προαναφέρθηκε, το Express διαθέτει μια μέθοδο για τη διατήρηση αρκετών αλυσίδων hash σε πολύ μικρό χώρο μνήμης. Για την παραγωγή των τιμών σύνοψης χρησιμοποιούνται δύο συναρτήσεις hash που ονομάζονται h_1 και h_2. Ένα **δέντρο αλυσίδας hash**, είναι ένα δυαδικό δέντρο του οποίου οι κόμβοι είναι τιμές σύνοψης. Ξεκινώντας από οποιονδήποτε κόμβο του, αν η τιμή του κόμβου έχει κρυπτογραφηθεί με την h_1, το αριστερό «παιδί» έχει φταστεί ενώ αν ο κόμβος έχει κρυπτογραφηθεί με την h_2, συμβαίνει το αντίστοιχο για το δεξιό «παιδί». Με τον τρόπο αυτό, κάθε μονοπάτι στο δέντρο, από τη ρίζα στα φύλλα, είναι μια πιθανή αλυσίδα hash που μπορεί να αναθέσει ο κόμβος S σε κάποιον ενδιάμεσο κόμβο του δικτύου.
Για την αποθήκευση του συνολικού σετ αλυσίδων hash, ο S χρειάζεται μόνο να αποθηκεύσει την ρίζα του δέντρου, και για την ανάθεση μιας αλυσίδας σε έναν κόμβο, ο S χρειάζεται να αποθηκεύσει έναν αριθμό k bit για τον κόμβο αυτό, όπου k είναι το ύψος του δέντρου. Ο αριθμός αυτός ορίζει το μονοπάτι μιας συγκριμένης αλυσίδας στο δέντρο. Έχοντας τη ρίζα του δέντρου και τον αριθμό, μπορεί να παραχθεί η συνολική αλυσίδα hash.
Για καλύτερη κατανόηση δίδεται το εξής παράδειγμα. Στο δέντρο του παρακάτω σχήματος, που έχει ύψος 3, με έναν αριθμό 3 bit, όπως ο 010, μπορεί να παραχθεί μια αλυσίδα hash όπως η $w_0 \rightarrow w_1 \rightarrow w_4 \rightarrow w_9$. Στη μέθοδο αυτή, η επικύρωση μιας νεοληφθείσας τιμής σύνοψης είναι απλή: αν μια από τις συναρτήσεις hash μετατρέψει την νέα αυτή τιμή στην προηγούμενη έγκυρη τιμή, τότε και η νέα είναι έγκυρη.



Σχήμα 4.4.3

4.4.5 ΛΕΙΤΟΥΡΓΙΑ ΤΟΥ EXPRESS

Ο μηχανισμός υποστήριξης συνεργασίας Express αναλύεται μέσω της θεωρίας παιγνίων και για το λόγο αυτό καθορίζονται οι παίκτες που συμμετέχουν στο παίγνιο, τις δυνατές ενέργειες, και τις απολαβές των παικτών όταν επιλέγουν να ακολουθήσουν τη στρατηγική μιας συγκεκριμένης ενέργειας. Σε ένα τυπικό σενάριο μετάδοσης οι στρατηγικοί παίκτες είναι ο κόμβος πηγής S, και ένας αριθμός

ενδιάμεσων κόμβων m_i. Για ευκολία περιγράφεται εδώ ένα παίγνιο μεταξύ του κόμβου S και ενός αυθαίρετου ενδιάμεσου κόμβου. Για την μοντελοποίηση της πιθανότητας ένα πακέτο να απορριφθεί σε κάποιο βήμα της μετάδοσης, θεωρείται ένας τρίτος παίκτης που ονομάζεται ***Φύση***, ο οποίος αποφασίζει αν θα προωθήσει ή όχι το πακέτο σε κάποιον ενδιάμεσο κόμβο με μια πιθανότητα P. Κάθε παίγνιο ξεκινά με την απόφαση του παίκτη Φύση σχετικά με τη μετάδοση, και αφού πραγματοποιηθεί αυτή η απόφαση, ο ενδιάμεσος κόμβος M μπορεί να επιλέξει μια από τις παρακάτω ενέργειες:

- FPCR: Προώθηση πακέτου και αναφορά μιας σωστής απόδειξης είσπραξης
- FPNR: Προώθηση πακέτου και μη αναφορά απόδειξης είσπραξης
- NFNR: Μη προώθηση του πακέτου και μη αναφορά απόδειξης είσπραξης
- NFMR: Μη προώθηση του πακέτου και αναφορά μιας τροποποιημένης απόδειξης είσπραξης με σκοπό την εξαπάτηση του RCC ώστε να πιστέψει ότι ο κόμβος συμμετείχε στην προώθηση του πακέτου
- NFCR: Μη προώθηση του πακέτου και αναφορά μιας σωστής απόδειξης είσπραξης

Στην περίπτωση που ο παίκτης Φύση δεν μεταδώσει το πακέτο, ο M μπορεί να επιλέξει ανάμεσα στις εξής ενέργειες:

- MR: Αναφορά μιας παραποιημένης απόδειξης είσπραξης με σκοπό την εξαπάτηση του RCC ώστε να πιστέψει ότι ο κόμβος παρέλαβε το πακέτο
- NR: Μη αναφορά απόδειξης είσπραξης υποδηλώνοντας ότι δεν έχει παραλάβει το πακέτο

Τέλος, η πηγή πραγματοποιεί την ενέργειά της ανεξάρτητα από τις αποφάσεις του παίκτη Φύση και του ενδιάμεσου κόμβου. Οι δυνατές ενέργειες για την πηγή είναι οι εξής:

- CR: Αναφορά μιας σωστής απόδειξης είσπραξης
- MR: Αναφορά μιας παραποιημένης απόδειξης είσπραξης έτσι ώστε να αποφύγει την πληρωμή στον ενδιάμεσο κόμβο

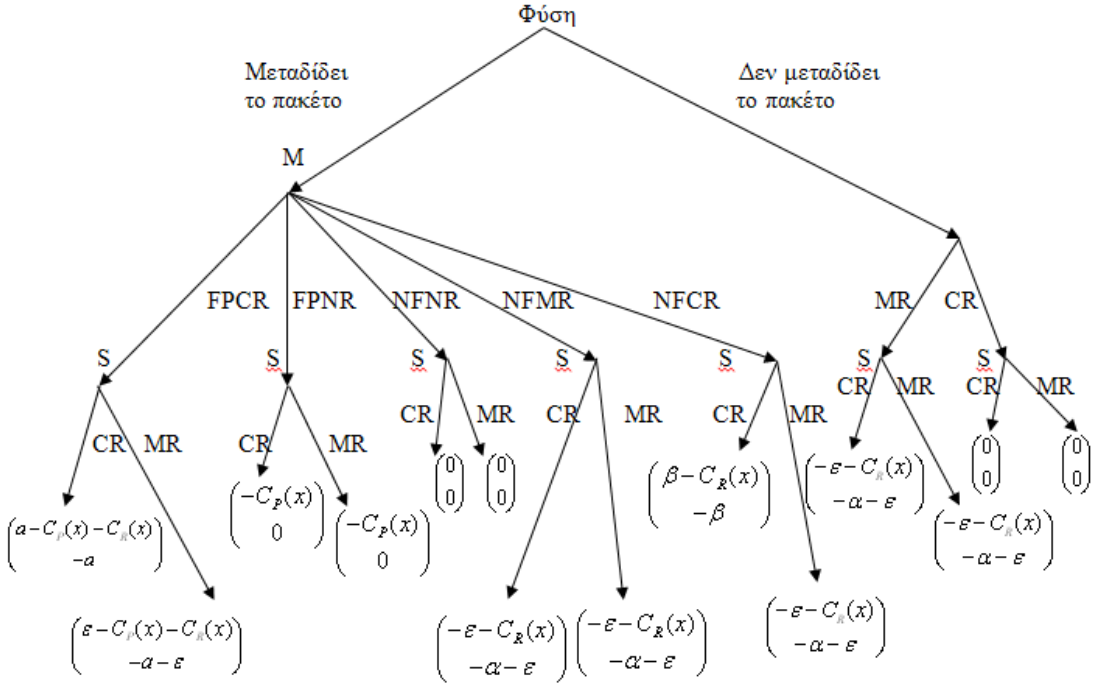
Θεωρείται επίσης ότι το κόστος για την προώθηση ενός πακέτου ή για την αποστολή μιας αναφοράς, εξαρτάται από την διαθέσιμη ισχύ ενός κόμβου, με μόνη εξαίρεση τον κόμβο πηγή. Πιο συγκεκριμένα τα δύο παραπάνω κόστη εκφράζονται ως $C_P(x)$ και $C_R(x)$ και μαθηματικά ορίζονται ως:

$$C_i(x) = A_i \frac{1-x}{x} + \rho_i$$

, όπου A_i και ρ_i θετικές σταθερές, $x \in [0,1]$ και $i \in [P,R]$.

Υποτίθεται επίσης ότι $\rho_R < \rho_P$ αφού η αποστολή μιας αναφοράς προκαλεί λιγότερο φόρτο στον κόμβο από ότι η προώθηση πακέτου. Παρόμοια, η αλλαγή στην τρέχουσα ισχύ έχει μικρότερη επίδραση στο κόστος της μετάδοσης αναφοράς από ότι στο κόστος προώθησης πακέτου, επομένως ισχύει ότι $A_R < A_P$.

Σχηματικά, η διαδικασία του παιγνίου που παρουσιάστηκε φαίνεται παρακάτω (όπου S η πηγή, και από κάτω οι πληροφορίες που τίθενται από αυτήν όταν παίρνει μια απόφαση) :



Σχήμα 4.4.4

Σύμφωνα με τη θεωρία παιγνίων, για κάθε τιμή του x, το παίγνιο έχει ένα ισοζύγιο στρατηγικής. Τα ισοζύγια αυτά είναι τα εξής:

1. ((FPCR,NR),CR): Ο ενδιάμεσος κόμβος προωθεί το πακέτο και αναφέρει μια σωστή απόδειξη είσπραξης αν λάβει το πακέτο, ενώ δεν αναφέρει απόδειξη είσπραξης αν δεν το λάβει. Ο κόμβος πηγή δίνει σωστή απόδειξη είσπραξης για το πακέτο του. Η στρατηγική αυτή είναι το ισοζύγιο του παιγνίου αν $C_P(x)+C_R(x)<a$ και $C_R(x)<\beta$.
2. ((NFCR,NR),CR): Ο ενδιάμεσος κόμβος δεν προωθεί το πακέτο αλλά αναφέρει ότι έχει λάβει το πακέτο, ενώ δεν στέλνει απόδειξη είσπραξης αν δεν λάβει το πακέτο. Ο κόμβος πηγή δίνει σωστή απόδειξη είσπραξης για το πακέτο του. Η στρατηγική αυτή είναι το ισοζύγιο του παιγνίου αν $C_P(x)+C_R(x)>a$ και $C_R(x)<\beta$.
3. ((NFNR,NR),CR): Ο ενδιάμεσος κόμβος ούτε προωθεί το πακέτο, ούτε αναφέρει κάποια απόδειξη είσπραξης. Ο κόμβος πηγή δίνει σωστή απόδειξη είσπραξης για το πακέτο του. Η στρατηγική αυτή είναι το ισοζύγιο του παιγνίου αν $C_P(x)+C_R(x)>a$ και $C_R(x)>\beta$.

Φαίνεται, ότι η συνεργασία επιτυγχάνεται όταν η πληρωμή α για την προώθηση ενός πακέτου είναι μεγαλύτερη από το κόστος για την προώθηση του πακέτου συν το κόστος για την αποστολή αναφοράς. Επίσης, οι πιστώσεις β που χρειάζονται για τον τελευταίο κόμβο στο μονοπάτι, πρέπει να είναι περισσότερες από το κόστος για την αποστολή αναφοράς.

Ακόμα, υποθέτοντας ότι ο λόγος της τρέχουσας ισχύος προς την μέγιστη ισχύ μοιράζεται ομοιόμορφα μεταξύ 0 και 1, η πιθανότητα συνεργασίας δίδεται από τον τύπο:

$$P_C = 1 - \max\left\{\frac{A_P + A_R}{a + A_P + A_R - \rho_P - \rho_R}, \frac{A_P}{\beta + A_R - \rho_R}\right\}$$

ή $$P_C = \min\left\{\frac{a - \rho_P - \rho_R}{a + A_P + A_R - \rho_P - \rho_R}, \frac{\beta - \rho_R}{\beta + A_R - \rho_R}\right\}.$$

Θέτοντας $a - \rho_P - \rho_R = r(A_P + A_R)$ και $\beta - \rho_R = sA_R$, συνάγεται ότι:

$$P_C = \min\left\{\frac{r}{r+1}, \frac{s}{s+1}\right\}.$$

Προκύπτει ότι $P_C \to 1$ αν $r, s \to \infty$, επομένως κάθε επίπεδο συνεργασίας μεταξύ των κόμβων είναι εφικτό αν τεθούν οι σωστές τιμές πιστώσεων *α* και *β*.

4.4.6 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ EXPRESS

Οι δημιουργοί του Express δεν έχουν δημοσιεύσει κάποια προσομοίωση για την απόδειξη της αποτελεσματικότητας του. Παρόλα αυτά, έχουν πραγματοποιήσει εκτιμήσεις σχετικά με την απόδοση του σε σύγκριση με μηχανισμούς υποστήριξης συνεργασίας που χρησιμοποιούν ψηφιακές υπογραφές, όπως το Sprite. Συγκεκριμένα, υπέθεσαν σενάριο επικοινωνίας στο οποίο ο κόμβος πηγή S επιθυμεί να αποστείλει πακέτα *p* στον προορισμό D μέσω *n* ενδιάμεσων κόμβων. Κατέληξαν στα εξής συμπεράσματα σύμφωνα με την παρακάτω λογική:
Στο Express, *n* παραγωγές ψηφιακών υπογραφών(G) από τον S, και *n* επικυρώσεις υπογραφών(V) από τους ενδιάμεσους κόμβους συμπεριλαμβανομένου και του D, απαιτούνται για τη διαδικασία της χειραψίας και της πραγματοποίησης του συμβολαίου συνεργασίας, ή με άλλα λόγια $n(G+V)$ κόστος. Αυτό συμβαίνει διότι στο Express απαιτούνται ψηφιακές υπογραφές μόνο για τις πρώτες συναλλαγές μεταξύ του S και των άλλων κόμβων. Για κάθε πακέτο, ο κόμβος πηγή πραγματοποιεί μια λειτουργία hash για κάθε κόμβο με σκοπό να δημιουργήσει τα αντίστοιχα στοιχεία αλυσίδων hash (pnH). Κάθε ενδιάμεσος κόμβος πραγματοποιεί δύο λειτουργίες hash για να ελέγξει την εγκυρότητα κάθε τιμής σύνοψης(2 pnH). Επίσης, για την παραγωγή των αποδείξεων είσπραξης, κάθε ενδιάμεσος κόμβος πραγματοποιεί μια λειτουργία hash για κάθε πακέτο (pnH) και ο κόμβος S πραγματοποιεί μια λειτουργία hash για κάθε πακέτο ανά κόμβο. Θεωρώντας τις τιμές στις παρενθέσεις ως κόστος υπολογισμού, το συνολικό κόστος υπολογισμού που εισάγει το Express στους κόμβους είναι:

$$O_E = nG + nV + 5pnH$$

Από την άλλη στον μηχανισμό υποστήριξης συνεργασίας Sprite, όπως υποστηρίζουν οι δημιουργοί του Express, όταν ο κόμβος S επιθυμεί να αποστείλει p πακέτα στον κόμβο προορισμό D μέσω *n* ενδιάμεσων κόμβων, ο S πραγματοποιεί μια παραγωγή ψηφιακής υπογραφής και μια λειτουργία hash(H) για κάθε πακέτο ή με άλλα λόγια $p(G+H)$ κόστος. Επίσης κάθε ενδιάμεσος κόμβος πραγματοποιεί μια επικύρωση ψηφιακής υπογραφής και μια λειτουργία hash για κάθε πακέτο($pn(V+H)$). Όπως και παραπάνω, συμπεραίνεται ότι το συνολικό κόστος υπολογισμού που εισάγει το Sprite στους κόμβους είναι:

$$O_S = pG + pnV + p(n+1)H$$

- Συγκρίνοντας τα παραπάνω, οι κατασκευαστές του Express, καταλήγουν στο συμπέρασμα ότι το υπολογιστικό overhead του μηχανισμού Sprite είναι πολύ μεγαλύτερο από το Express καθώς η υπολογιστική πολυπλοκότητα των λειτουργιών ψηφιακών υπογραφών είναι πολύ υψηλότερη από την αντίστοιχη των λειτουργιώνhash, και ο αριθμός των μεταδιδόμενων πακέτων είναι συνήθως πολύ μεγαλύτερος από τον αριθμό των κόμβων στο δίκτυο.

Συμπερασματικά, το Express αποτελεί έναν μηχανισμό υποστήριξης συνεργασίας, που προσφέρει υπηρεσίες ασφαλείας και κίνητρα για προώθησης της συνεργασίας των κόμβων, ενώ παράλληλα επιτυγχάνει πρόληψη ενάντια στις γνωστές ενέργειες εξαπάτησης, και οι διαδικασίες του επιφέρουν σχετικά μικρή επιβάρυνση στο δίκτυο, πράγμα που επιτυγχάνεται με τη χρήση αλυσίδων hash. Παρόλα αυτά, η κρίση του συγκεκριμένου πρωτοκόλλου είναι επισφαλής, αφού δεν είναι γνωστές τυχόν προσομοιώσεις ώστε να υπάρχουν επαρκή στοιχεία για την αποτελεσματικότητα του.

Κεφάλαιο 5

ΚΡΙΣΙΜΑ ΖΗΤΗΜΑΤΑ ΓΙΑ ΤΟΝ ΣΧΕΔΙΑΣΜΟ ΚΑΙ ΣΥΓΚΡΙΣΗ ΤΩΝ ΥΠΑΡΧΟΝΤΩΝ ΣΧΗΜΑΤΩΝ ΠΙΣΤΩΣΕΩΝ

5.1 ΚΡΙΣΙΜΑ ΖΗΤΗΜΑΤΑ

Στο κεφάλαιο αυτό παρουσιάζονται μερικά βασικά ζητήματα που απασχολούν την ανάλυση και τη σχεδίαση των μηχανισμών υποστήριξης συνεργασίας βασισμένων στις πιστώσεις για ad-hoc δίκτυα. Πάνω στα συγκεκριμένα ζητήματα διακρίνονται και διαφοροποιούνται τα σχήματα πιστώσεων που παρουσιάσθηκαν, παίρνονται κρίσιμες αποφάσεις για το σχεδιασμό των μηχανισμών, ανάλογα με την απόδοση που επιθυμείται να επιτευχθεί και τα χαρακτηριστικά που απαιτούνται. Παρακάτω αναλύονται κάποια από αυτά τα θέματα, τα θετικά και αρνητικά τους στοιχεία σε κάθε επίπεδο, και πραγματοποιείται μια σύγκριση των μηχανισμών που παρουσιάσθηκαν.

5.1.1 ΑΣΦΑΛΕΙΑ ΕΝΑΝΤΙΑ ΣΤΙΣ ΑΛΛΟΙΩΣΕΙΣ

Βασικό ζήτημα κατά τον σχεδιασμό ενός σχήματος πίστωσης αποτελεί η επιλογή για χρήση ή όχι, ειδικού hardware ενάντια στην αλλοίωση. Είναι προφανές ότι από τη στιγμή που οι μηχανισμοί χρησιμοποιούν πιστώσεις, υπάρχει ο κίνδυνος για αλλοίωση, μετατροπή του αριθμού πιστώσεων στους κόμβους με σκοπό την καλύτερη μονομερή εκμετάλλευση του δικτύου από κάποιον εγωιστικό κόμβος. Για το λόγο αυτό, απαιτείται στα δίκτυα η εύρεση κάποιου τρόπου με σκοπό την απόδοση ασφάλειας σε τέτοια φαινόμενα. Μια επιλογή, που φυσικά εισάγει κόστος, αποτελεί η εισαγωγή στο σύστημα ειδικού hardware, που με φυσικό τρόπο αποτρέπει εισβολείς από το να εισβάλλουν και να τροποποιήσουν πληροφορίες στο σύστημα, όπως για παράδειγμα η μη εξουσιοδοτημένη αύξηση των πιστώσεων ή και άλλες λειτουργίες. Η χρήση του hardware είναι η πλέον ασφαλής, με το μειονέκτημα όμως ότι πρέπει να κατέχεται από όλους τους χρήστες και είναι ακριβό, με αποτέλεσμα να προτιμάται λιγότερο σε μεγάλα δίκτυα. Από την άλλη, ασφάλεια μπορεί να εισαχθεί σε ένα πρωτόκολλο και με χρήση αποκλειστικά και μόνο λογισμικού. Κάτι τέτοιο απαιτεί χρήση κρυπτογραφικών μεθόδων με αλυσίδες hash και ψηφιακών υπογραφών. Το μειονέκτημα σε αυτόν τον τρόπο εισαγωγής ασφαλείας, είναι η αύξηση του υπολογιστικού overhead στους κόμβους, με ότι συνέπειες μπορεί αυτό να έχει, ενώ το πλεονέκτημα, ότι είναι δωρεάν και μπορεί να χρησιμοποιηθεί πλατιά στα δίκτυα. Επομένως η λύση που θα επιλεχθεί ενάντια στις αλλοιώσεις, βασίζεται στις επιθυμίες του σχεδιαστή όσον αφορά το βαθμό ασφάλειας, το κόστος και την απόδοση του δικτύου. Στους μηχανισμούς υποστήριξης συνεργασίας βασισμένων στις πιστώσεις, που χρησιμοποιήθηκαν, η επιλογή όσον αφορά το ζήτημα της ασφάλειας φαίνεται στον παρακάτω πίνακα.

ΣΧΗΜΑ	**ΑΣΦΑΛΕΙΑ**	
	HARDWARE	**ΛΟΓΙΣΜΙΚΟ**
NUGLETS	†	†
SPRITE	-	†
PIFA	-	†
EXPRESS	-	†

Πίνακας 5.1.1

5.1.2 ΣΥΜΒΑΤΟ ΠΡΩΤΟΚΟΛΛΟ ΔΡΟΜΟΛΟΓΗΣΗΣ

Άλλο σημαντικό ζήτημα για το σχεδιασμό ενός σχήματος βασισμένου στις πιστώσεις για την υποστήριξη συνεργασίας στα ad-hoc δίκτυα, είναι το πρωτόκολλο δρομολόγησης με το οποίο είναι συμβατός ο μηχανισμός. Γενικότερα, τα περισσότερα σχήματα βασίζονται στον αλγόριθμο δρομολόγησης DSR, ο οποίος είναι ευρέως διαδεδομένος στα δίκτυα και απλός στην υλοποίηση του, ή σε άλλους αλγόριθμους δρομολόγησης πηγής. Παρόλα αυτά είναι δελεαστικό ο κάθε μηχανισμός υποστήριξης συνεργασίας να μπορεί να εφαρμοστεί πάνω σε οποιοδήποτε πρωτόκολλο δρομολόγησης, ο σχεδιασμός να είναι ανεξάρτητος από τα χαρακτηριστικά δρομολόγησης του εκάστοτε δικτύου. Ακόμα, η χρήση του DSR απαιτεί τη γνώση πληροφοριών για το σύνολο του μονοπατιού, πράγμα το οποίο εισάγει καθυστέρηση και επιβάρυνση, ενώ δεν μπορεί να παίξει σωστά το ρόλο του σε ένα δίκτυο όπου υπάρχουν εγωιστικοί κόμβοι. Από την άλλη, για να μπορεί ένας μηχανισμός να εφαρμοστεί πάνω από οποιοδήποτε πρωτόκολλο δρομολόγησης απαιτείται μεγαλύτερη πολυπλοκότητα, απαιτεί κεντρικό server που να δέχεται τις αναφορές κόμβων σχετικά με την προώθηση πακέτων. Επομένως για το σχεδιασμό λαμβάνεται υπόψη το βάθος που επιθυμείται να στην υλοποίηση του σχήματος, το εύρος των δικτύων στα οποίο μπορεί να υλοποιηθεί και η απόδοση του δικτύου.

ΣΧΗΜΑ	**ΣΥΜΒΑΤΟ ΠΡΩΤΟΚΟΛΛΟ ΔΡΟΜΟΛΟΓΗΣΗΣ**	
	ΠΡΩΤΟΚΟΛΛΟ ΔΡΟΜΟΛΟΓΗΣΗΣ ΠΗΓΗΣ	**ΟΠΟΙΟΔΗΠΟΤΕ ΠΡΩΤΟΚΟΛΛΟ ΔΡΟΜΟΛΟΓΗΣΗΣ**
NUGLETS	†	-
SPRITE	†	-
PIFA	-	†
EXPRESS	†	-

Πίνακας 5.1.2

5.1.3 ΑΝΑΠΑΡΑΣΤΑΣΗ ΠΙΣΤΩΣΕΩΝ

Στα σχήματα που βασίζονται στις πιστώσεις, ζήτημα στο σχεδιασμό αποτελεί και ο τρόπος αναπαράστασης των πιστώσεων. Στα ad-hoc δίκτυα ως γνωστόν, δεν υπάρχει μια κεντρική εσωτερική υποδομή, επομένως μια άποψη για την αναπαράσταση των πιστώσεων είναι η αναπαράσταση τους ως μετρητών στους κόμβους, ώστε να μην απαιτείται κάποια αρχή που θα εκδίδει και θα διαχειρίζεται ψηφιακά νομίσματα. Παρόλα αυτά, κάτι τέτοιο είναι επικίνδυνο, καθώς κάποιος κόμβος μπορεί να μετατρέψει την τιμή του μετρητή του ώστε να αποκτήσει περισσότερες πιστώσεις, και για να αποφευχθεί αυτό απαιτείται ειδικό hardware ενάντια στις αλλοιώσεις όπως προαναφέρθηκε. Απαιτούνται επίσης κρυπτογραφικές μέθοδοι. Από την άλλη, διαφορετική λύση πάνω στο συγκεκριμένο ζήτημα αποτελεί η εισαγωγή της έννοιας του ψηφιακού νομίσματος. Στον σχεδιασμό ενός μηχανισμού με τον τρόπο αυτό, απαιτείται ο ορισμός ενός κόμβου ως κεντρικού server-διαχειριστή στον οποίο

αναφέρονται οι κόμβοι σχετικά με την συμπεριφορά τους. Ο διαχειριστής αυτός διαχειρίζεται τους λογαριασμούς των κόμβων, αυξάνει ή μειώνει τις πιστώσεις τους. Η λύση αυτή βέβαια εισάγει μεγάλη κίνηση λόγω των αναφορών, μεταξύ των κόμβων και της τράπεζας, πράγμα που μεταφράζεται σε επιπλέον επιβάρυνση στο δίκτυο. Ακόμα σε κάποια σχήματα μπορεί να απαιτηθεί και η έκδοση πιστοποιητικών για τους κόμβους που συμμετέχουν στο δίκτυο και κατέχουν λογαριασμούς πιστώσεων. Είναι παρά ταύτα ασφαλής λύση όσον αφορά την ακεραιότητα των πιστώσεων. Με βάση τα παραπάνω, στο σχεδιασμός ενός μηχανισμού υποστήριξης συνεργασίας βάσει πιστώσεων, πρέπει να ληφθούν αποφάσεις σχετικά με την ισορροπία μεταξύ ασφάλειας, overhead και κόστους. Τα σχήματα που περιγράφηκαν επιλέγουν την αναπαράσταση και τη διαχείριση των πιστώσεων, όπως φαίνεται στον παρακάτω πίνακα.

ΣΧΗΜΑ	**ΑΝΑΠΑΡΑΣΤΑΣΗ ΠΙΣΤΩΣΕΩΝ**	
	ΨΗΦΙΑΚΑ ΝΟΜΙΣΜΑΤΑ	**ΜΕΤΡΗΤΕΣ**
NUGLETS	-	†
SPRITE	†	-
PIFA	†	-
EXPRESS	†	-

Πίνακας 5.1.3

5.1.4 ΤΡΟΠΟΣ ΧΡΕΩΣΗΣ

Ο τρόπος χρέωσης των κόμβων για την προσφορά και την απόλαυση υπηρεσιών προώθησης πακέτων, διαφέρει μεταξύ των μηχανισμών υποστήριξης συνεργασίας. Οι επιλογές είναι από τη μία η χρέωση αποκλειστικά του κόμβου – πηγή που επιθυμεί να αποστείλει κάποιο πακέτο με τη συμβολή των υπόλοιπων κόμβων στο δίκτυο, και από την άλλη, η χρέωση όλων των κόμβων που συμμετέχουν στην μετάδοση του πακέτου, με χρήση αγοράς και επαναπώλησης του. Τα περισσότερα σχήματα που βασίζονται στις πιστώσεις, χρησιμοποιούν την πρώτη επιλογή. Κάτι τέτοιο, αποτρέπει τους κόμβους που επιθυμούν να αποστείλουν πακέτα, από το να στέλνουν άχρηστες πληροφορίες, καθώς κάτι τέτοιο επιφέρει σπατάλη εύρους ζώνης. Επίσης, η επιλογή αυτή αντιτίθεται στην χρέωση του παραλήπτη, ή και την χρέωση αποστολέα και παραλήπτη, αφού από την μία ελλοχεύουν κίνδυνοι άρνησης παροχής υπηρεσιών από τους ενδιάμεσους κόμβους και από την άλλη υπάρχει περίπτωση δημιουργίας συμπαιγνίας από τα δύο άκρα του μονοπατιού. Ο συγκεκριμένος τρόπος χρέωσης βέβαια, έχει και μειονεκτήματα, όπως το γεγονός ότι εάν δεν επαρκούν οι πιστώσεις του αποστολέα για την μετάδοση του πακέτου, αυτό μπορεί να απορριφθεί. Ο τρόπος χρέωσης που επιβαρύνει και τους ενδιάμεσους κόμβους, έχει κι αυτός πλεονεκτήματα και μειονεκτήματα. Ως πλεονέκτημα συγκαταλέγεται το γεγονός ότι δεν είναι αναγκαία η γνώση του απαιτούμενου αριθμού πιστώσεων για την μετάδοση ενός πακέτου μέσω ενός μονοπατιού, ενώ ταυτόχρονα μειώνεται και ο κίνδυνος απώλειας του πακέτου που έχει σταλεί . Αντίθετα, με βάση τη χρέωση αυτή, δεν λαμβάνεται καθόλου υπόψη, η πιθανή επιβάρυνση του δικτύου από κάθε είδους λιγότερο σημαντικές πληροφορίες και δεδομένα. Επομένως κατά το σχεδιασμό, λαμβάνεται

υπόψη το overhead και το εύρος ζώνης, αλλά και η ασφάλεια όσον αφορά τη σίγουρη άφιξη του πακέτου στον προορισμό. Οι μηχανισμοί υποστήριξης συνεργασίας που περιγράφηκαν, επιλέγουν τον τρόπο χρέωσης ως ακολούθως.

ΣΧΗΜΑ	**ΤΡΟΠΟΣ ΧΡΕΩΣΗΣ**		
	ΧΡΕΩΣΗ ΠΗΓΗΣ	**ΧΡΕΩΣΗ ΠΡΟΟΡΙΣΜΟΥ**	**ΧΡΕΩΣΗ ΟΛΩΝ ΤΩΝ ΣΥΜΜΕΤΕΧΟΝΤΩΝ ΚΟΜΒΩΝ**
NUGLETS	†	-	†
SPRITE	†	-	-
PIFA	†	-	-
EXPRESS	†	-	-

Πίνακας 5.1.4

Κεφάλαιο 6

ΥΒΡΙΔΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ ΥΠΟΣΤΗΡΙΞΗΣ ΣΥΝΕΡΓΑΣΙΑΣ

Όπως αναφέρθηκε, η πιο νέα ομάδα υποστήριξης συνεργασίας, οι υβριδικοί, αποτελούν μια προσπάθεια αξιοποίησης των θετικών στοιχείων από τις δύο βασικές κατηγορίες μηχανισμών υποστήριξης συνεργασίας, και η απαλοιφή των αδυναμιών τους. Οι υβριδικοί μηχανισμοί διατηρούν σύστημα φήμης όπως οι μηχανισμοί φήμης, αλλά και σύστημα πιστώσεων όπως οι μηχανισμοί πιστώσεων. Ο συνδυασμός των δύο αυτών ιδιοτήτων, πραγματοποιείται, χρεώνοντας την υπηρεσία προώθησης ανάλογα με την φήμη κάθε κόμβου. Η υποστήριξη συνεργασίας εξασφαλίζεται, δίνοντας κίνητρα στους κόμβους να συνεργαστούν, ώστε να αποκτήσουν καλή φήμη, και να απολαύσουν την υπηρεσία προώθησης πακέτων από άλλους κόμβους, με λιγότερο κόστος. Παρακάτω παρουσιάζοντα χαρακτηριστικά παραδείγματα υβριδικών μηχανισμών, καθώς και τα πειραματικά αποτελέσματα για τη λειτουργία και την αποτελεσματικότητα τους όπως αυτά εξήχθησαν από τους δημιουργούς τους.

6.1 ARM

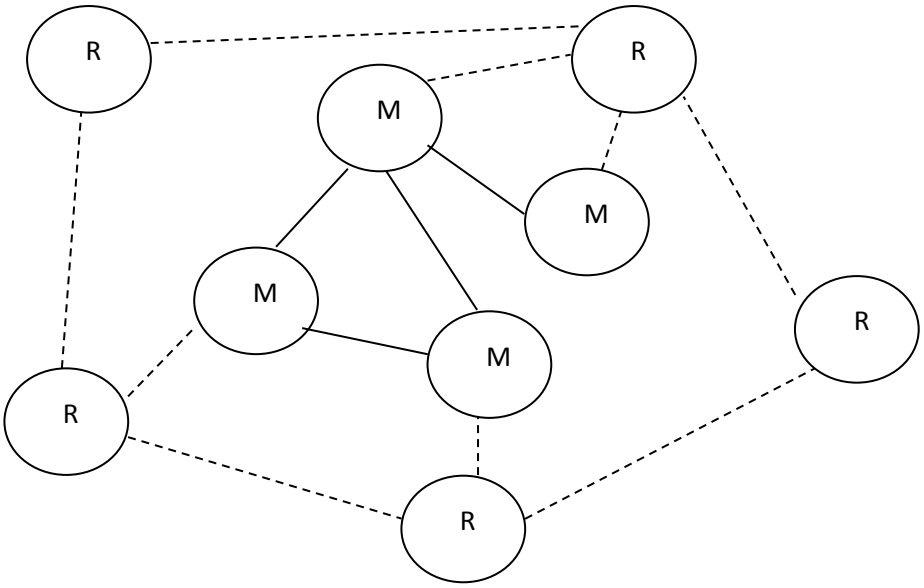
Το ARM [16] αποτελεί έναν υβριδικό μηχανισμό υποστήριξης συνεργασίας για ad-hoc δίκτυα, που έχει ως στόχο την ανίχνευση και εκμηδένιση της εγωιστικής συμπεριφοράς, καθώς και την ενίσχυση της συνεργασίας των κόμβων με αποτελεσματικό τρόπο, χωρίς να αυξάνεται η πολυπλοκότητα. Το ARM συνδυάζει στοιχεία των μηχανισμών υποστήριξης συνεργασίας που βασίζονται στη φήμη, καθώς και αυτών που βασίζονται στις πιστώσεις. Πιο συγκεκριμένα:

- Δεν επιβαρύνει κάθε κόμβο με πίνακες φήμης, αλλά επιλέγει ως ***διαχειριστές της φήμης(RMN)***, τους κόμβους χαμηλής κινητικότητας, χτίζοντας μια ιεραρχική δομή με τους RMN στο υψηλό επίπεδο, και τους υπόλοιπους κόμβους στο χαμηλό επίπεδο. Αφήνοντας τους RMN να διαχειρίζονται τις τιμές φήμης(***RV***) εξοικονομεί υπολογιστικούς πόρους, ενώ απαλλάσσει και τους υπόλοιπους κόμβους από το φορτίο της διαχείρισης φήμης, έτσι ώστε να χρησιμοποιούν περισσότερους πόρους για μετάδοση πακέτων.
- Συγκροτεί τους RMN σε μια δομή ***DHT*(Distributed Hash Table)**, για την αποτελεσματική ανταλλαγή και συλλογή πληροφοριών φήμης.
- Χρησιμοποιεί ένα μοντέλο βασισμένο σε χρεώσεις, κατά το οποίο κάθε υπηρεσία χρεώνεται με βάση τη φήμη, πράγμα που αποτρέπει τους εγωιστικούς κόμβους από το να κρατάν χαμηλά τις τιμές φήμης τους λίγο πάνω από το κατώφλι, ώστε να αποφεύγουν την τιμωρία.
- Αντίθετα με τα σχήματα που βασίζονται σε πιστώσεις, δεν χρησιμοποιεί νομίσματα, με αποτέλεσμα να μην καταστρέφει την παραδοσιακή μορφή των IP πακέτων.

6.1.1 ΠΕΡΙΓΡΑΦΗ ΤΟΥ ARM

Παρακάτω φαίνεται σχηματικά η ιεραρχική δομή του ARM. Με R συμβολίζονται οι κόμβοι RMN που συγκροτούν τη δομή DHT, και με M οι υπόλοιποι κινητοί κόμβοι.

Επίσης με σκούρα γραμμή συμβολίζονται οι ζεύξεις για προώθηση πακέτων και με διακεκομμένη οι ζεύξεις για την διαχείριση της φήμης.



Σχήμα 6.1.1

Τα παρακάτω σύνολο αποτελεί το ***Καθολικό Σύστημα Διαχείρισης Φήμης(GRMS)***, για τη διαχείριση των τιμών των λογαριασμών και της φήμης. Η λειτουργία διαχείρισης φήμης χρησιμοποιείται για τη διαχείριση των RV του κάθε αυτόνομου κινητού κόμβου. Κάθε τέτοιος κόμβος διαθέτει έναν μηχανισμό – φύλακα για τον υπολογισμό των RV των γειτονικών του κόμβων και την αναφορά τους στο GRMS περιοδικά, μετά από μια περίοδο T. Οι τιμές RV συγχωνεύονται στο GRMS για τον προσδιορισμό μιας καινούριας RV για έναν κόμβο.

Η λειτουργία διαχείρισης λογαριασμών, χρησιμοποιείται για την ενίσχυση της συνεργασίας όλων των κόμβων στο δίκτυο. Οι τιμές λογαριασμού AV ενός κόμβου N, αφαιρούνται από μια συγκεκριμένη τιμή, από το GRMS ανάλογα με τον αριθμό των πακέτων που δημιουργήθηκαν από τον κόμβο, ενώ αυξάνονται ανάλογα με τον αριθμό των πακέτων που προωθήθηκαν από τον κόμβο. Όταν ο κόμβος N έχει υψηλότερη φήμη, χρειάζεται να πληρώσει λιγότερο στο GRMS. Οι κόμβοι στο δίκτυο επίσης, διαθέτουν διπλές διεπαφές, με αποτέλεσμα να μπορούν να χρησιμοποιήσουν διεπαφή χαμηλής ισχύος μετάδοσης για την προώθηση πακέτων, και διεπαφή υψηλής ισχύος μετάδοσης για τα δεδομένα φήμης. Σύμφωνα με το ARM, μόνο ο κόμβος πηγή χρεώνεται για την μετάδοση του πακέτου στον επόμενο κόμβο, ενώ οι ενδιάμεσοι κόμβοι, όχι μόνο δεν χρεώνονται αλλά επιβραβεύονται όταν προωθούν το πακέτο.

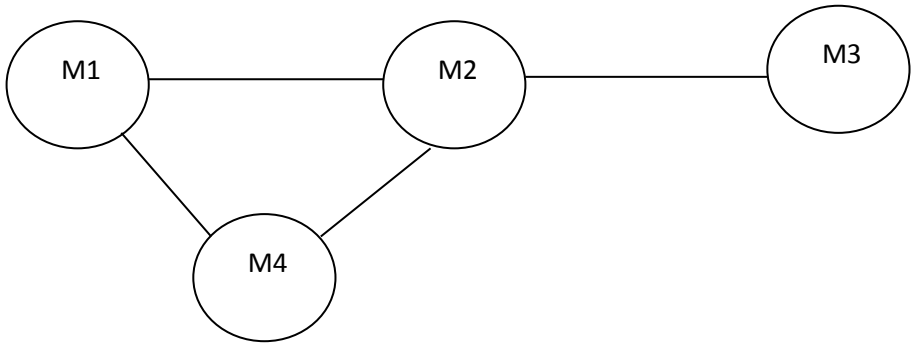
Οι λογαριασμοί, διαχειρίζονται από το GRMS, και δεν χρησιμοποιείται κάποια μορφή νομίσματος που περιφέρεται στο δίκτυο. Το GRMS, αγνοεί τις ανανεωμένες τιμές RV που αναφέρονται από κόμβους με μη ομαλή συμπεριφορά ή από κόμβους με AV μικρότερες του 0. Πιο συγκεκριμένα, όταν ο κόμβος N1 λαμβάνει μια αίτηση από τον κόμβο N2 για την προώθηση ενός αριθμού πακέτων, ο N1 θα επικοινωνήσει με κάποιον κοντινό RMN, τον R1, για να ζητήσει τις τιμές RV και AV του N2. Εάν αυτός δεν τις έχει, ο R1 μπορεί να ρωτήσει άλλους RMN με βάση τον αλγόριθμο δρομολόγησης του DHT. Εάν οι τιμές RV του N2 είναι κάτω από ένα κατώφλι Th ή οι τιμές AV του N2 είναι μικρότερες του 0, τότε ο N1 αρνείται να προωθήσει πακέτα για τον N2.Αν πάλι οι RV του N2 είναι υψηλότερες από το κατώφλι, ο N1 χρεώνει

την προώθηση από τον N2 βασιζόμενος στις τιμές RV του. Ανά κάθε χρονικό διάστημα T, όλοι οι κόμβοι συγχωνεύουν τις νέες τιμές RV άλλων κόμβων στο GRMS.

6.1.2 ΛΕΙΤΟΥΡΓΙΑ ΣΥΣΤΗΜΑΤΟΣ ΔΙΑΧΕΙΡΙΣΗΣ ΦΗΜΗΣ

Στο σύστημα διαχείρισης φήμης, χρησιμοποιούνται συχνά οι εξής λειτουργίες:

1. Ανίχνευση γειτόνων και Ανανέωση φήμης. Στο ARM, η ανίχνευση των γειτονικών κόμβων χρησιμοποιείται για την συλλογή πληροφοριών σχετικά με την προωθητική συμπεριφορά των γειτονικών κόμβων. Ακούγοντας το κανάλι, ένας κόμβος μπορεί να αντιληφθεί τις μεταδόσεις άλλων γειτονικών κόμβων. Κάθε κόμβος διατηρεί μια τρέχουσα λίστα(NNL) με τους γείτονές του, η οποία περιέχει τις ταυτότητες ID τους και τις πληροφορίες τους συμπεριλαμβανομένων των RV και AV. Με τον τρόπο αυτό καταφέρεται να μην απαιτείται να ρωτά διαρκώς το GRMS. Η λίστα NNL, χρησιμοποιεί μια συνάρτηση TTL για να διατηρεί την φρεσκάδα των πληροφοριών των γειτονικών κόμβων. Όταν ένας γειτονικός κόμβος βγει από την εμβέλεια μετάδοσης του κόμβου, οι πληροφορίες του γείτονα αυτού διαγράφονται από την NNL. Η χρονική περίοδος T κατά την οποία οι κόμβοι αναφέρουν τις RV στο GRMS, παίρνει μικρή τιμή αν το δίκτυο αλλάζει γρήγορα τοπολογία, ενώ παίρνει μεγάλη τιμή όταν οι αλλαγές είναι αργές. Επίσης στο ARM, οι κόμβοι χρησιμοποιούν ένα μηχανισμό φύλακα για να ανιχνεύσουν την προωθητική συμπεριφορά των γειτονικών κόμβων, διατηρώντας δύο μετρητές. Ο μετρητής $\mathbf{RF_i(j)}$(Request for Forwarding), μετρά τον συνολικό αριθμό πακέτων που έχει προωθήσει ο κόμβος i στον κόμβο j, και ο μετρητής $\mathbf{HF_i(j)}$(Has Forwarded) μετρά τον συνολικό αριθμό των πακέτων που έχουν προωθηθεί από τον j και το έχει αντιληφθεί ο i.



Σχήμα 6.1.2

Με βάση το παραπάνω παράδειγμα – σχήμα, ο μηχανισμός φύλακας λειτουργεί ως εξής: Όταν ο κόμβος M1 μεταδίδει πακέτα στον M2, ο M4 λαμβάνει επίσης πακέτα. Όταν ο κόμβος M2 προωθεί πακέτα στον M3, ο M1 λαμβάνει επίσης πακέτα. Έτσι, όταν ο M2 λαμβάνει ένα πακέτο που πρέπει να προωθηθεί, είτε από τον M1 είτε από τον M4, οι δύο τελευταίοι θα ακούσουν την μετάδοση και θα αποθηκεύσουν το πακέτο στη μνήμη τους, θα θέσουν ένα χρονόμετρο και θα ακούσουν τη μετάδοση του M2, και τέλος θα αυξήσουν τον μετρητή RF κατά 1.

Αν πάλι ο κόμβος M2 προωθήσει το πακέτο, αυτό διαγράφεται από τη μνήμη και αυξάνεται κατά 1 ο μετρητής HF. Ειδάλλως, το πακέτο αφαιρείται όταν τερματίσει το χρονόμετρο.

Περιοδικά, το εργαλείο ανίχνευσης δημιουργεί μια τιμή που ονομάζεται **Τοπική Τιμή(LV),** που βασίζεται στους δύο μετρητές που αναφέρθηκαν για όλους τους γειτονικούς κόμβους των οποίων γίνεται αντιληπτή η μετάδοση, και για όλες τις αναφορές LV, στον κοντινότερο RMN ανά κάθε χρονική περίοδο $t_0 + nT$, όπου t_0 η χρονική που ένας κινητός κόμβος εισάγεται στο σύστημα, και n είναι θετικός ακέραιος. Ουσιαστικά η τιμή LV παράγεται από τον παρακάτω μαθηματικό τύπο:

$$LV_i(j) = \frac{HF_i(j)}{RF_i(j)}$$

Οι τιμές των μετρητών $RF_i(j)$ και $HF_i(j)$ αναφέρονται επίσης στο GRMS για τον υπολογισμό της τιμής λογαριασμού, ενώ μετά την ανανέωση οι μετρητές μηδενίζονται.

2. <u>Λειτουργία συστήματος διαχείρισης φήμης.</u> Το δίκτυο DHT όπως αναφέρθηκε, αποτελεί μια κλάση αποκεντρωμένων συστημάτων που μοιράζονται την ιδιοκτησία ενός σετ αντικειμένων ανάμεσα στους συμμετέχοντες κόμβους. Πετυχαίνει χρόνο πολυπλοκότητας O(log n) για κάθε αίτηση αναζήτησης, χρησιμοποιώντας O(log n) γειτονικούς κόμβους ανά κόμβο, όπου n είναι ο αριθμός των κόμβων. Κάθε αντικείμενο ή κόμβος, ανατίθεται μια ταυτότητα ID(ή κλειδί) που είναι η κρυπτογραφημένη τιμή της διεύθυνσης IP του, με χρήση μιας συνάρτησης hash. Κάθε αντικείμενο αποθηκεύεται στον κόμβο του οποίου το ID ταυτίζεται ή ταιριάζει με το ID του αντικειμένου. Το δίκτυο παρέχει δύο βασικές λειτουργίες:
   - Την Εισαγωγή, **Insert(κλειδί, αντικείμενο)**, για την αποθήκευση ενός αντικειμένου σε ένα κόμβο υπεύθυνο για το κλειδί.
   - Την Αναζήτηση, **Lookup(κλειδί)**, για την ανάκτηση του αντικειμένου.

   Το μήνυμα για τις δύο λειτουργίες, προωθείται με βάση τον αλγόριθμο δρομολόγησης του DHT. Κάθε κόμβος διατηρεί ένα πίνακα δρομολόγησης για τους γειτονικούς κόμβους στο δίκτυο.

   Στο ARM, υλοποιείται η κατασκευή μιας υποδομής δικτύου βασισμένη στο DHT και που εξαρτάται από την τοποθεσία, όπου η λογική εγγύτητα που παράγει ο RMN ταιριάζει με την φυσική εγγύτητα στην πραγματικότητα. Χρησιμοποιείται μια μέθοδος με δείκτες, για την αναπαράσταση της εγγύτητας των κόμβων. Κάθε RMN μετρά την διαχείριση φήμης του, τις φυσικές αποστάσεις του ως $<d_1, d_2,\ldots, d_m>$ σαν συντεταγμένες σε ένα καρτεσιανό σύστημα. Δύο κοντινοί στον πραγματικό χώρο RMN έχουν παρόμοια διανύσματα. Με χρήση της μαθηματικής καμπύλης Hilbert, αντιστοιχίζονται διανύσματα χώρου m διαστάσεων σε αληθινούς αριθμούς, ώστε να διατηρείται η σχέση εγγύτητας. Οι αριθμοί αυτοί ονομάζονται ***αριθμοί Hilbert*** των RMN.

   Ο αριθμός Hilbert κάθε κόμβου χρησιμοποιείται ως το DHT ID του, και εκχωρείται ένα ID στις πληροφορίες φήμης ενός κόμβου, κρυπτογραφώντας την IP διεύθυνση του κόμβου μέσω μιας συνάρτησης hash. Έτσι, το GRMS συγκροτεί μια DHT δομή που εξαρτάται από την τοποθεσία, όπου οι κοντινοί στην πραγματικότητα, κόμβοι, είναι κοντινοί λόγω του χαρακτηριστικού του αριθμού Hilbert. Με βάση την πολιτική εκχώρησης κλειδιών DHT, οι τιμές RV κάθε κόμβου αποθηκεύονται στον ιδιοκτήτη τους. Έτσι, αν ο κόμβος i επιθυμεί να ρωτήσει για τις RV του κόμβου j, ρωτά τον κοντινότερο RMN. Εάν πάλι οι κόμβοι αυτοί δεν έχουν τις πληροφορίες φήμης, ο i στέλνει μια αίτηση Lookup με

την κρυπτογραφημένη τιμή της IP του j, ως κλειδί. Με τη σειρά της η αίτηση προωθείται στον κόμβο που έχει τις πληροφορίες φήμης του j χρησιμοποιώντας τον αλγόριθμο δρομολόγησης του DHT. Στην περίπτωση που ο κόμβος πηγή δεν είναι στην εμβέλεια ενός RMN, μπορεί να χρησιμοποιήσει πληροφορίες που αναζητήθηκαν πρόσφατα. Με τον τρόπο αυτό, ένας κόμβος μπορεί πάντα να έχει πρόσβαση στην φήμη ενός άλλου κόμβου αποτελεσματικά.

Στο σχήμα ARM όπως αναφέρθηκε, κάθε κινητός κόμβος κρατά μια λίστα των γειτονικών του κόμβων για να διευκολύνει την τακτική εγκαθίδρυση ζεύξεων. Αν ένας γειτονικός κόμβος N_i του κόμβου N, ζητήσει από τον N την προώθηση ενός πακέτου, ο κόμβος N ρωτάει τις τιμές RV και AV του N_i από τον κοντινότερο R1, αν βέβαια δεν υπάρχουν πληροφορίες για τον N_i, στην NNL του. Αν πάλι ο R1 δεν έχει τις απαραίτητες RV που χρειάζεται ο N, ο πρώτος θα ζητήσει τις πληροφορίες φήμης από κάποιον άλλο RMN με βάση τον αλγόριθμο αναζήτησης του DHT. Τέλος, αφού λάβει RV του N_i, ο κόμβος N θα τις κρατήσει, μέχρι ο N_i, να βγει εκτός εμβέλειας του κόμβου N.

3. <u>Διαχείριση φήμης.</u> Όπως ειπώθηκε, κάθε κόμβος αναφέρει περιοδικά στο GRMS τις τιμές LVπου έχει ανιχνεύσει, ωστόσο κάθε περίοδο T, πολλοί κόμβοι παρατηρούν τη συμπεριφορά ενός συγκεκριμένου κόμβου και την αναφέρουν στο GRMS. Για το λόγο αυτό, δίδεται περισσότερος βάρος στον κόμβος με υψηλή φήμη για να υπολογιστεί η τρέχουσα RV για τον κόμβο N. Μαθηματικά, αυτό δίνεται από τον τύπο:

$$RV_{Current}(N) = \frac{\sum_{i \in N \cup (LV_i(N) > Th)} LV_i(N) \cdot RV_{table}(i)}{\sum_{i=1}^{n} LV_i(N)}$$

, όπου Th το κατώφλι φήμης κάτω από το οποίο ο κόμβος θεωρείται ως μη ομαλά συμπεριφερόμενος, και RV_{table}, ορίζει τις παρελθοντικές τιμές RV. Όταν αναφέρονται αυτές οι τιμές, το GRMS αγνοεί τις τιμές RV που αναφέρονται από κάποιον εγωιστικό κόμβο, ώστε να αποφευχθεί η κατηγορία άλλων κόμβων επειδή αρνούνται να προωθήσουν πακέτα.

Ωστόσο, για να αποφεύγονται οι λανθασμένες κατηγορίες στην περίπτωση που απορρίπτονται πακέτα λόγω θορύβου στο δίκτυο, οι παρελθοντικές τιμές RV λαμβάνονται υπόψη στον RV_{table}, αλλά και στον υπολογισμό της νέας RV, ως εξής:

$$RV_{new}(N) = aRV_{table}(N) + (1-a)RV_{Current}(N)$$

Αλλάζοντας την τιμή του *α,* μπορεί ανάλογα με το περιβάλλον, να αλλάξει και το βάρος που δίνεται στην παρελθοντική ή στην τρέχουσα συμπεριφορά των κόμβων. Στο μηχανισμό ARM, η επίδραση της λανθασμένης αναφοράς φήμης στο συνολικό υπολογισμό της φήμης, είναι μικρή, και οι καθολικές τιμές RV στο GRMS με ακρίβεια αντανακλούν την συμπεριφορά των κόμβων.

6.1.3 ΛΕΙΤΟΥΡΓΙΑ ΔΙΑΧΕΙΡΙΣΗΣ ΛΟΓΑΡΙΑΣΜΩΝ

Ο μηχανισμός υποστήριξης συνεργασίας ARM διαθέτει μια λειτουργία διαχείρισης λογαριασμών για να αποφεύγεται η ίση αντιμετώπιση των κόμβων με υψηλή φήμη, η οποία παρέχει κίνητρα για συνεργασία μεταξύ των κόμβων, και αποτρέπει την εγωιστική συμπεριφορά.

Με βάση αυτή τη λειτουργία, η πολιτική χρέωσης βασίζεται στις τιμές RV στον πίνακα φήμης, ως εξής:

$$P(N) = \frac{\gamma}{RV_{table}(N)}$$

, όπου γ μια σταθερά τιμή βαρύτητας και P η τιμή για τη μετάδοση ενός πακέτου. Όσο υψηλότερη RV διαθέτει ένας κόμβος, τόσο λιγότερο πρέπει να πληρώσει για την μετάδοση. Επιπλέον, το GRMS διατηρεί έναν λογαριασμό ψηφιακών μετρητών για κάθε κόμβο στο σύστημα. Το GRMS αρχικά αναθέτει σε κάθε νεοεισαχθέντα στο δίκτυο κόμβο, ένα συγκεκριμένο ποσό ψηφιακών μετρητών στον λογαριασμό Sum. Κάθε φορά που ένας κόμβος N παράγει πακέτα στο σύστημα, για άλλους κόμβους, η τιμή του λογαριασμού του μειώνεται κατά ένα συγκεκριμένο αριθμό ψηφιακών μετρητών ίσο με $P_i(N) \cdot RFS_i(N)$, όπου $RFS_i(N)$ ο αριθμός των πακέτων που ο κόμβος πηγή N στέλνει στους γειτονικούς του σε μια περίοδο T. Από την άλλη, αν ο κόμβος N βοηθήσει άλλους κόμβους να προωθήσουν πακέτα, η τιμή AV του N αυξάνεται κατά $\lambda \cdot HF_i$, όπου λ μια σταθερά – επιβράβευση για κάθε πακέτο που προώθησε ο N, και HF_i ο αριθμός των πακέτων που προώθησε ο κόμβος σε μια περίοδο T. Έτσι, η τιμή AV του κόμβου N υπολογίζεται από τον παρακάτω τύπο:

$$AV = Sum - \sum_{i=t_0}^{t_0+mT} (P_i(N) \cdot RF_i(N) + \lambda \cdot HF_i)$$

Ο κόμβος που προωθεί πακέτα, δεν χρειάζεται να πληρώσει για τα πακέτα που προωθεί στο επόμενο βήμα. Στο ARM, ένας πιο συνεργάσιμος κόμβος έχει μεγαλύτερη AV, ενώ ένας λιγότερο συνεργάσιμος κόμβος μπορεί να έχει αρνητική τιμή AV, πράγμα που δεν του επιτρέπει να αποστέλλει πακέτα. Με τον τρόπο αυτό πετυχαίνεται η συνεργασιμότητα των κόμβων στο δίκτυο.

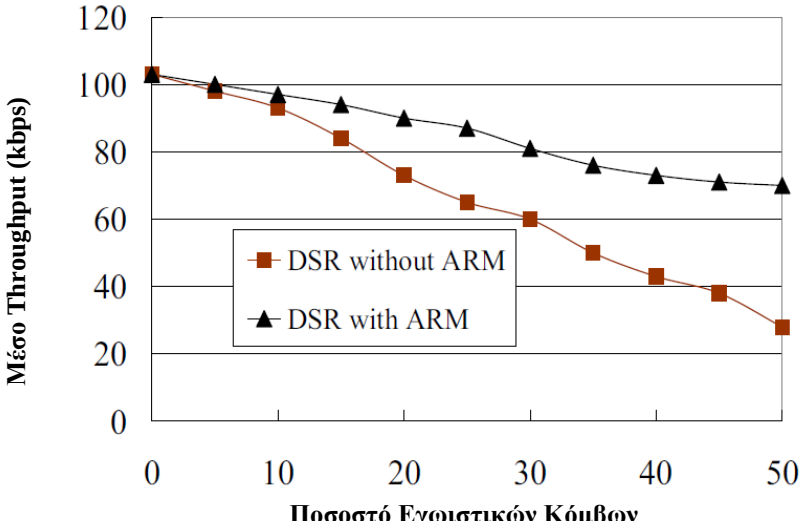
6.1.4 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ ARM

Για την εξακρίβωση της αποτελεσματικότητας του ARM, οι δημιουργοί του πραγματοποίησαν προσομοιώσεις με χρήση του προγράμματος προσομοίωσης δικτύων, NS-2, με σκοπό και τη σύγκριση έναντι ενός δικτύου που χρησιμοποιεί απλό DSR. Πιο συγκεκριμένα χρησιμοποιήθηκε κατά τα πειράματα, το παρακάτω περιβάλλον προσομοίωσης:

- Πρωτόκολλο δρομολόγησης DSR
- Κόμβοι 50
- Περιοχή 1000m x 1000m
- Πρωτόκολλο MAC 802.11 – DCF
- Εμβέλεια μετάδοσης 250m
- Εύρος ζώνης 2Mbps
- Ύψος κεραιών 1.5m
- Εφαρμογή CBR – 2 πακέτα ανά δευτερόλεπτο
- Κίνηση τυχαία
- Τυχαία τοποθέτηση κόμβων
- Χρόνος παύσης κίνησης 1 – 5 δευτερόλεπτα
- Ταχύτητα 1 – 10 m/s

- 10 νέα ζευγάρια πηγής – προορισμού επιλέγονται κάθε 40s
- Προσομοιώσεις 10
- Χρόνος προσομοίωσης 200s
- Κατώφλι φήμης 0.4

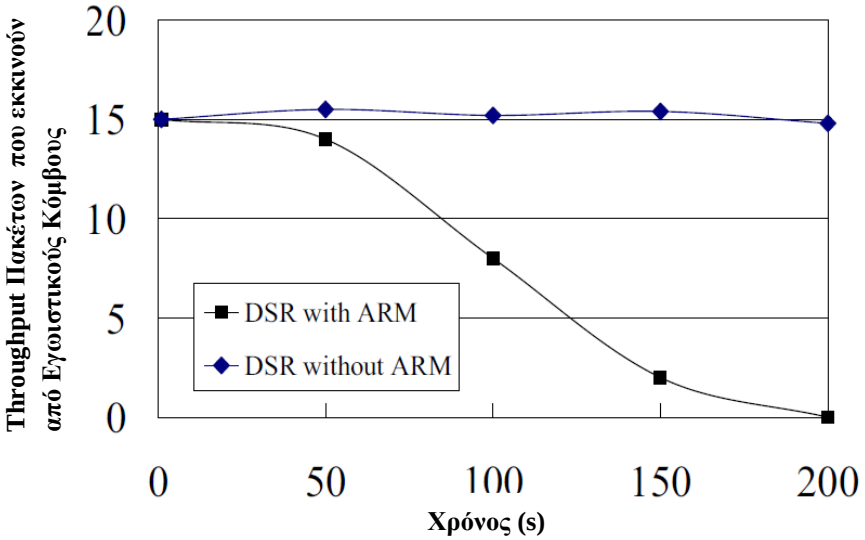
Μετά την πραγματοποίηση των προσομοιώσεων, παράχθηκαν τα παρακάτω διαγράμματα και εξήχθησαν τα αντίστοιχα συμπεράσματα για την απόδοση του μηχανισμού ARM:
Το παρακάτω διάγραμμα που έχει στον κάθετο άξονα ***το μέσο throughput του δικτύου σε kbps***, και στον οριζόντιο ***το ποσοστό των εγωιστικών κόμβων***, φαίνεται με την κόκκινη γραμμή το αποτέλεσμα για ένα δίκτυο που δεν χρησιμοποιεί ARM πάνω από το DSR, ενώ με την μαύρη ένα δίκτυο που χρησιμοποιεί το ARM.



Διάγραμμα 6.1.1 (Πηγή [16])

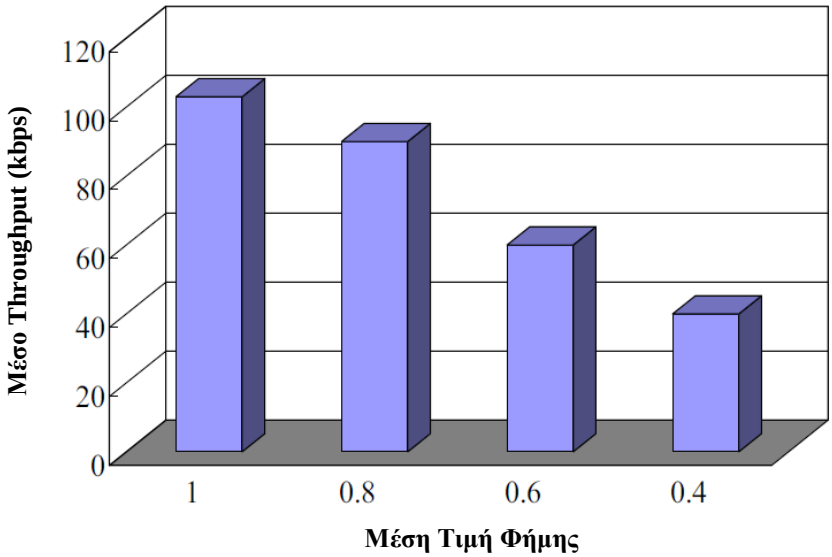
Παρατηρείται, ότι το δίκτυο που χρησιμοποιεί ARM έχει μεγαλύτερο throughput από ένα δίκτυο με DSR που δεν το χρησιμοποιεί, όσο ανεβαίνει και το ποσοστό των εγωιστικών κόμβων, πράγμα που συμβαίνει λόγω της ικανότητας του ARM να εξαιρεί τους εγωιστικούς κόμβους από τις διαδρομές δρομολόγησης. Παρόλα αυτά το throughput του δικτύου με ARM, μειώνεται και αυτό με την αύξηση του ποσοστού των εγωιστικών κόμβων, αφού όταν δεν υπάρχουν εγωιστικοί κόμβοι, το μήκος μονοπατιού είναι μεγαλύτερο άρα και το throughput.

Ακολουθεί εξαχθέν διάγραμμα που έχει στον κάθετο άξονα ***το throughput των πακέτων που εκκινούν από εγωιστικούς κόμβους*** , και στον οριζόντιο ***το χρόνο σε δευτερόλεπτα***. Φαίνεται με την μπλε γραμμή το αποτέλεσμα για ένα δίκτυο που δεν χρησιμοποιεί ARM πάνω από το DSR, ενώ με την κόκκινη ένα δίκτυο που χρησιμοποιεί το ARM. Συμπεραίνεται ότι όταν δεν χρησιμοποιείται το ARM οι εγωιστικοί κόμβοι διατηρούν σταθερό throughput στα 15 kbps, ενώ σε δίκτυο που χρησιμοποιείται ARM, το throughput των εγωιστικών κόμβων μειώνεται με το χρόνο καθώς το ARM τους εντοπίζει με αποτέλεσμα οι άλλοι κόμβοι να μην προωθούν τα πακέτα τους.



Διάγραμμα 6.1.2 (Πηγή [16])

Τέλος το παρακάτω διάγραμμα που εξήχθη από τα πειράματα, έχει στον κάθετο άξονα ***το μέσο throughput του δικτύου σε kbps***, και στον οριζόντιο ***τη μέση τιμή φήμης***. Παρατηρείται ότι όσο μειώνεται η μέση RV, μειώνεται και το μέσο throughput του δικτύου, αφού ένας κόμβος με χαμηλή φήμη έχει μεγαλύτερες πιθανότητες απόρριψης πακέτων.



Διάγραμμα 6.1.3 (Πηγή [16])

Συμπερασματικά, ο υβριδικός μηχανισμός υποστήριξης συνεργασίας ARM, με τη χρήση του GRMS, καταφέρνει να μειώσει τον αποθηκευτικό χώρο και την υπολογιστική ισχύ που χρειάζονται οι κόμβοι για τη διαχείριση της φήμης, ενώ αυξάνει την κλιμάκωση της διάδοσης της φήμης. Επίσης, χρησιμοποιώντας και τη λειτουργία διαχείρισης λογαριασμών, αποτρέπει ενέργειες εγωιστικών κόμβων που παραποιούν τη φήμη τους για να αποφύγουν την τιμωρία. Σε γενικές γραμμές, βελτιώνεται η απόδοση του δικτύου σε σχέση με την περίπτωση ύπαρξης μόνο του DSR, και δρα αποτελεσματικά έναντι των εγωιστικών κόμβων, ως αποτέλεσμα της

παράλληλης χρήσης στοιχείων των μηχανισμών υποστήριξης συνεργασίας με βάση τη φήμη αλλά και τις χρεώσεις.

6.2 S.A.R.C.I.S.

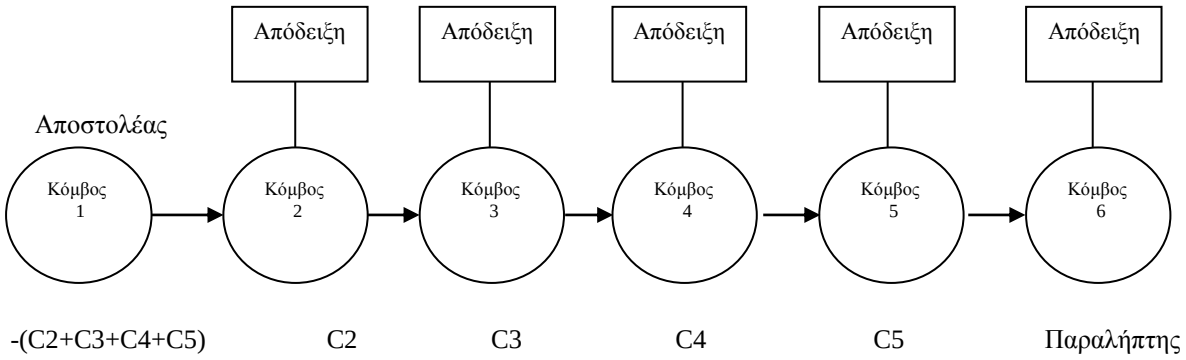
Ο συγκεκριμένος μηχανισμός υποστήριξης συνεργασίας, που στα πλαίσια της παρούσας διπλωματικής εργασίας για ευκολία, θα αναφέρεται ως S.A.R.C.I.S. [17], αποτελεί ένα υβριδικό σχήμα που ενσωματώνει τις λειτουργίες προώθησης και αναζήτησης διαδρομής δρομολόγησης χρησιμοποιώντας στοιχεία μηχανισμών υποστήριξης βασισμένων στη φήμη αλλά και σε πιστώσεις. Το σχήμα αυτό, στη φάση της προώθησης, ένας συνδυασμένος μηχανισμός φήμης και πιστώσεων προσφέρει κίνητρα με μια απλή και με λιγότερο overhead διαδικασία. Από την άλλη, στη φάση της αναζήτησης διαδρομής δρομολόγησης εισάγεται μια νέα μέτρηση που λαμβάνει υπόψη την εναπομείνασα ενέργεια καθώς και τη σχέση της ενέργεια με τις πιστώσεις. Στόχος του S.A.R.C.I.S. είναι η επίτευξης της συνεργασίας των κόμβων με αλλαγή των περιορισμών φήμης και πιστώσεων, και από την άλλη η αποθάρρυνση των κόμβων από τρεις τύπους εγωιστικής συμπεριφοράς. Η φιλοσοφία πάνω στην οποία δουλεύει το σχήμα, είναι να γίνεται βέλτιστη στρατηγική για τους κόμβους, η συνεργατική και ειλικρινής συμπεριφορά των κόμβων.

6.2.1 ΠΕΡΙΓΡΑΦΗ ΤΟΥ S.A.R.C.I.S.

Το S.A.R.C.I.S. λειτουργεί βάσει μιας κεντρικοποιημένης αρχιτεκτονικής, όπου ένας κόμβος CCS λειτουργεί σαν τράπεζα, που είναι υπεύθυνη για τον υπολογισμό της αύξησης ή μείωσης των πιστώσεων, καθώς και για την κράτηση καταγραφής σχετικής με τους λογαριασμούς των κόμβων. Θεωρείται ότι η πληρωμή, είναι η τιμή που παίρνει κάθε κόμβο κατά τη φάση της δρομολόγησης, και ότι οι μη συνεργάσιμοι κόμβοι τιμωρούνται με μείωση των πιστώσεων τους.
Κατά τη φάση της αναζήτησης διαδρομής δρομολόγησης, χρησιμοποιείται πρωτόκολλο δρομολόγησης όπως το DSR. Όταν ένας χρήστης προσπαθεί να μεταδώσει ένα μήνυμα σε ένα συγκεκριμένο κόμβο, αποστέλλει πλατιά μια αίτηση με τις διευθύνσεις της πηγής και του προορισμού, και ο κόμβος που το λαμβάνει ελέγχει αν είναι στο μονοπάτι. Σε αντίθετη περίπτωση, προσθέτει τις δικές του πληροφορίες (που περιέχουν την τιμή που δηλώνει και βασίζεται στην εναπομείνασα ενέργεια και τις πιστώσεις που διαθέτει) στην αίτηση, και επαναμεταδίδει πλατιά το μήνυμα. Όταν ο κόμβος προορισμός ανακαλυφθεί, μαθαίνει την συνολική τιμή κάθε μονοπατιού, και διαλέγει το μονοπάτι με την μικρότερη τιμή, και στη συνέχεια απαντά πίσω μέσω του αντίστροφου μονοπατιού.
Για να ενισχύσει την αναγγελία αληθινών τιμών από τους κόμβους, το S.A.R.C.I.S., χρησιμοποιεί εγκατάσταση ενός εργαλείου ανίχνευσης στους κόμβους. Υπάρχει η περίπτωση ένας κόμβος να δηλώσει χαμηλότερη τιμή ώστε να επιλεχθεί σε μονοπάτι, πράγμα που δεν συμφέρει πάντα όμως αφού η πληρωμή μπορεί να μην είναι αρκετή για την κάλυψη του κόστους. Το εργαλείο ανίχνευσης από την άλλη, ανιχνεύει τις περιπτώσεις όπου ένας κόμβος δηλώνει μεγαλύτερη τιμή ώστε να μην επιλεχθεί και να συλλέγει πιστώσεις. Όταν το εργαλείο ανίχνευσης ανιχνεύει ότι η αναφερόμενη τιμή ενός κόμβου αλλάζει πάνω από 15% σε σχέση με την τελευταία αναφερθείσα τιμή, μειώνει τις πιστώσεις του κόμβου κατά την τιμή που απαιτεί. Έτσι, αν ένας κόμβος αναφέρει μια πολύ ψηλή τιμή, και αποφύγει την συνεργασία για προώθηση, την επόμενη φορά πρέπει να διατηρήσει αυτή την ψηλή τιμή. Αποτέλεσμα, μετά από κάποιους γύρους ο κόμβος αυτός να μην μπορεί να συμμετέχει στις διαδικασίες επικοινωνίας λόγω του υψηλού κόστους, χάνοντας έτσι τη δυνατότητα να αποκτά πιστώσεις. Για το λόγο αυτό στο S.A.R.C.I.S., η ειλικρινής αναφορά τιμών γίνεται η βέλτιστη στρατηγική για τους κόμβους.

6.2.2 ΦΑΣΗ ΠΡΟΩΘΗΣΗΣ ΔΕΔΟΜΕΝΩΝ

Στο σχήμα S.A.R.C.I.S., η πολιτική πληρωμής που χρησιμοποιείται, προϋποθέτει την πληρωμή των μεταδιδόμενων κόμβων στους ενδιάμεσους που προσφέρουν την υπηρεσία τους, με σκοπό να μην αυξάνεται το overhead λόγω άσκοπων μεταδόσεων από τους κόμβους.
Σε αντιστοιχία με τον αναφερθέντα μηχανισμό υποστήριξης συνεργασίας Sprite, ο κόμβος CCS στο S.A.R.C.I.S., διαχειρίζεται ανάθεση πιστώσεων, βασισμένος στις αναφορές που λαμβάνει από αυθαίρετους κόμβους. Ο κόμβος που προωθεί, βασίζεται στον παραλήπτη ή τον κόμβο στο επόμενο βήμα για να αποστείλει μια αναφορά στο CCS μετά την λήψη των πακέτων. Το παρακάτω σχήμα, δείχνει τη λειτουργία του πρωτοκόλλου.



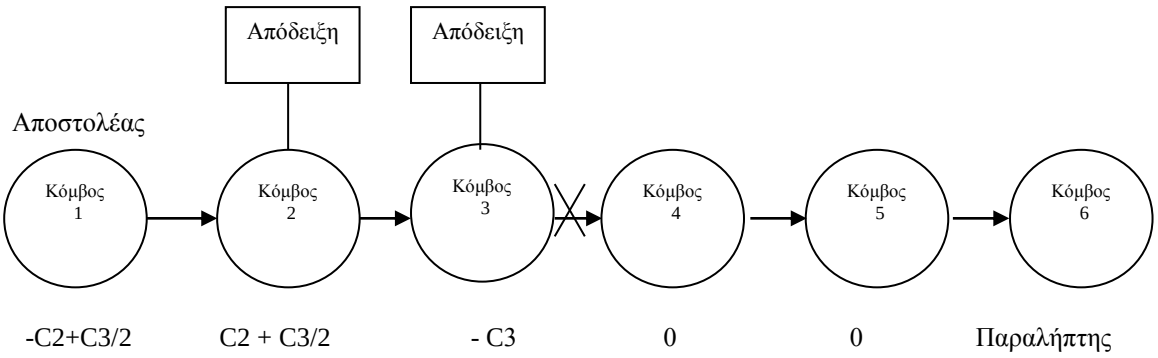
Σχήμα 6.2.1

Παραπάνω φαίνεται ο κόμβος 1 να αποστέλλει πακέτα στον κόμβο 6. Ως C2 ορίζεται που ο κόμβος 2 απαιτεί και έχει συμφωνηθεί με το σύστημα στη φάση δρομολόγησης. Αναλόγως ορίζονται και οι άλλες τιμές. Αφού, όλοι οι άλλοι χρήστες έχουν καταχωρήσει τις αποδείξεις είσπραξης, το πακέτο έχει ληφθεί επιτυχώς από τον κόμβο προορισμό. Λόγω της συμβολής όλων των ενδιάμεσων κόμβων, καθένας αποκτά τις πιστώσεις που χρειάζεται, και σε αντάλλαγμα για τις υπηρεσίες που λαμβάνονται από άλλους, ο κόμβος 1χρεώνεται με το σύνολο των πληρωμών για κάθε κόμβο. Το σύνολο αυτό είναι ίσο με –(C2+C3+C4+C5), όπου το « - » συμβολίζει την χρέωση ή την τιμωρία που μειώνει τις πιστώσεις του αντίστοιχου κόμβου. Ο κόμβος 6 λαμβάνει τα δεδομένα, και δεν χρεώνεται πιστώσεις.

Σε ένα δίκτυο ad-hoc που χρησιμοποιεί το S.A.R.C.I.S., μπορεί να υπάρξουν τρία είδη μη ομαλής συμπεριφοράς:
-Η μη προώθηση πακέτων
-Η μη αναφορά απόδειξης είσπραξης
-Η δημιουργία συμπαιγνίας μεταξύ των κόμβων
Καθώς δεν υπάρχουν επιπλέον χρεώσεις από τον αποστολέα ή επιπλέον πληρωμές προς τους ενδιάμεσους κόμβους, η συμπαιγνία κάποιων λίγων γειτονικών κόμβων δεν είναι αποτελεσματική στο να κερδίσουν πιστώσεις. Επομένως συμπεραίνεται ότι το S.A.R.C.I.S. μειώνει την πιθανότητα εμφάνισης μη συνεργατικών συμπεριφορών από τους κόμβους. Οι μη ομαλές συμπεριφορές που αναφέρθηκαν, αντιμετωπίζονται από το πρωτόκολλο, όπως αναλύεται με τα παρακάτω παραδείγματα:

1. Το πρωτόκολλο προσφέρει κίνητρα στους κόμβους ώστε να προωθήσουν μηνύματα. Στο παράδειγμα δικτύου του προηγούμενου σχήματος, έστω ότι ο

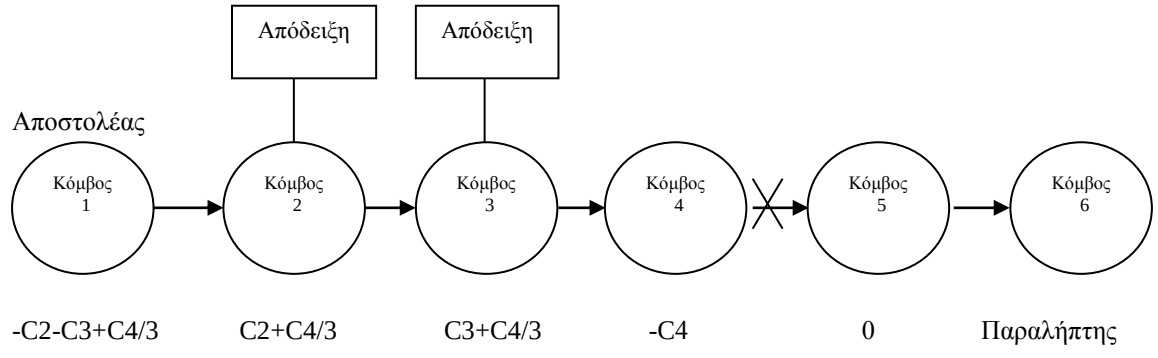
κόμβος 3 απορρίπτει το πακέτο. Οι πληρωμές διαμορφώνονται όπως φαίνεται παρακάτω.



Σχήμα 6.2.2

Από τη στιγμή που ο κόμβος 4 δεν λαμβάνει το μήνυμα, δύο μόνο αποδείξεις είσπραξης καταχωρούνται. Έτσι ο κόμβος 3 τιμωρείται με μια μείωση πιστώσεων ίση με C3, ενώ ο κόμβος 2 επιβραβεύεται με αύξηση ίση C2 πιστώσεις. Οι κόμβοι 4 και 5 δεν επηρεάζονται, αφού δεν συμμετέχουν στη διαδικασία. Οι πιστώσεις C3 που αφαιρούνται από τον κόμβο 3, μοιράζονται ισόποσα στους κόμβους 1 και 2, κάτι που μεταφράζεται ως αποζημίωση στους 1 και 2 για την ενέργεια που έχασαν λόγω της μη ομαλής συμπεριφοράς του κόμβου 3. Τέτοιου είδους τιμωρίες ενθαρρύνουν τους κόμβους να συμμετέχουν στην προώθηση πακέτων.

2. <u>Το πρωτόκολλο προσφέρει κίνητρα στους κόμβους ώστε να αναφέρουν τις αποδείξεις είσπραξης.</u> Στο ίδιο παράδειγμα δικτύου, έστω ότι ο κόμβος 4 ψεύδεται όσον αφορά την απόδειξη είσπραξης, και το σύστημα διαθέτει ένα μηχανισμό για την εγκαθίδρυση του επιπέδου ειλικρίνειας των κόμβων όπως φαίνεται παρακάτω:

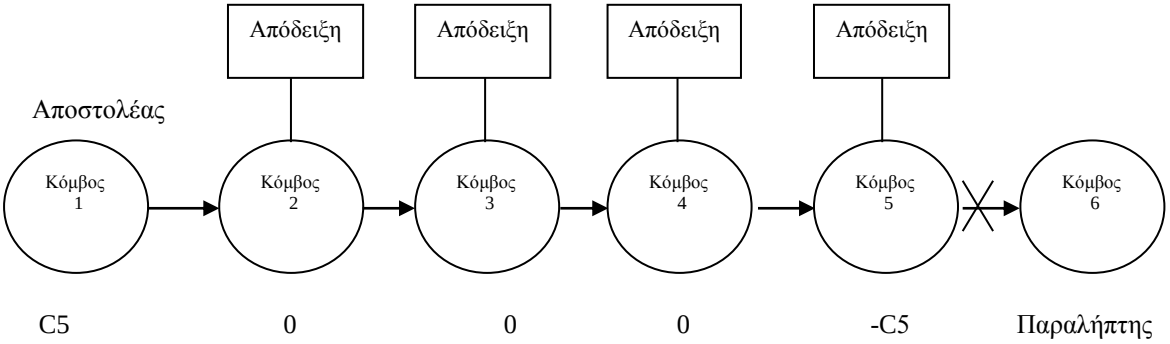


Σχήμα 6.2.3

Στην περίπτωση αυτή, θα αφαιρεθούν C4 πιστώσεις από το λογαριασμό του κόμβου 4, που θα μοιραστούν στους προηγούμενους κόμβους και τον αποστολέα. Ο αποστολέας βέβαια πρέπει να πληρώσει τους 2 και 3 για τη συμβολή τους στην προώθηση. Ο φόβος τέτοιων τιμωριών που εισάγει το S.A.R.C.I.S., αποθαρρύνει τους κόμβους από τη μη αναφορά αποδείξεων είσπραξης.

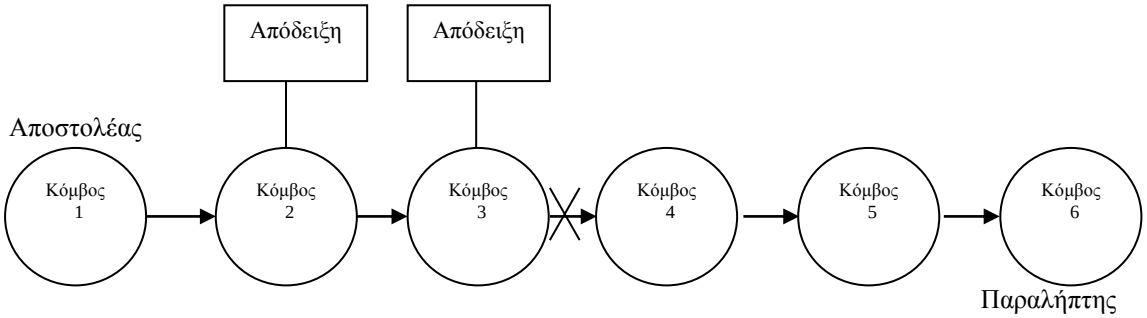
3. <u>Το πρωτόκολλο προσφέρει πρόληψη ενάντια στη δημιουργία συμπαιγνιών.</u> Στο παρακάτω σχήμα φαίνεται ότι όταν συμβαίνει συμπαιγνία μεταξύ των κόμβων, ο κόμβος 6 δεν καταχωρεί την απόδειξη είσπραξης. Αν όλοι οι

κόμβοι ισχυρίζονται ότι έχουν λάβει τα μηνύματα, είναι πιθανό όλοι οι κόμβοι μαζί πραγματοποιούν εξαπάτηση. Προφανώς είτε συμβαίνει αυτό είτε όχι, από τη στιγμή που ο κόμβος 5 δεν έχει προωθήσει το μήνυμα, σύντομα χρεώνεται. Παρόλα αυτά, για τους άλλους κόμβους , επειδή υπάρχει η πιθανότητα μόνο ο κόμβος 5 να έχει παρουσιάσει μη ομαλή συμπεριφορά, θα ήταν άδικο να τιμωρηθούν και οι άλλοι κόμβοι. Για το λόγο αυτό πληρώνονται μόνο C5 πιστώσεις στον αποστολέα. Στην περίπτωση πάλι που οι κόμβοι πραγματοποιούν όντως συμπαιγνία, αυτή, δεν φέρνει κάποια επιβράβευση στους κόμβους, ενώ δεν καλύπτει ούτε το κόστος για την καταχώρηση των αποδείξεων είσπραξης τους.



Σχήμα 6.2.4

Γίνεται κατανοητό ότι κρίσιμο ζήτημα για το σχήμα αποτελεί η ανίχνευση της συμπεριφοράς των κόμβων και η απόφαση για επιβράβευση ή τιμωρία τους. Σε γενικές γραμμές στο S.A.R.C.I.S., το CCS καταγράφει τις μη ομαλές συμπεριφορές, και βασίζεται στους ειλικρινείς κόμβους που χαρακτηρίζονται ανάλογα με το επίπεδο φήμης τους. Παράλληλα, χρησιμοποιείται ένας απλός μετρητής για την καταγραφή ης αναφερόμενης κατάστασης των κόμβων.
Περιληπτικά, κάθε φορά που μια μετάδοση είναι ανεπιτυχής όπως φαίνεται στο παρακάτω παράδειγμα, το CCS καταγράφει τους κόμβους στις θέσεις του τελευταίου που καταχώρησε την απόδειξη είσπραξης (κόμβος 3) και του πρώτου που δεν το έκανε (κόμβος 4). Έτσι, εκτός από έναν λογαριασμό πιστώσεων που κρατάται στο CCS, υπάρχει για κάθε χρήστη και ένας λογαριασμός φήμης. Όλες οι μη ομαλές συμπεριφορές συσσωρεύονται και ανανεώνονται με το χρόνο.



Σχήμα 6.2.5

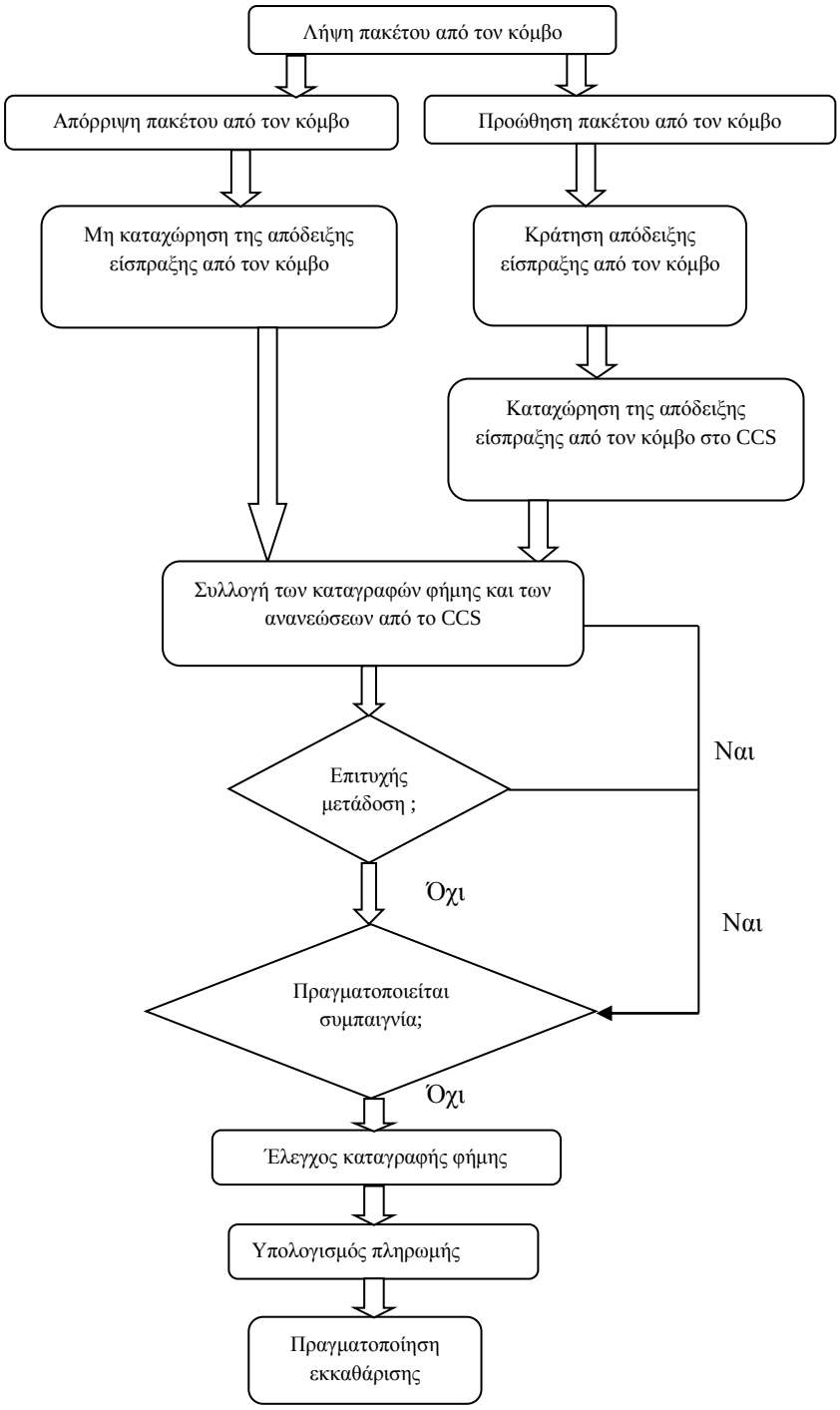
Στην περίπτωση που ο κόμβος 3 είναι πάντα ο τελευταίος που αναφέρει την απόδειξη είσπραξης, μπορεί να απορρίπτει πακέτα και να είναι μη συνεργάσιμος. Ως αποτέλεσμα, το CCS αποφασίζει να τιμωρήσει τον κόμβο 3. Ωστόσο, αν ο κόμβος 4

παρουσιάζει συχνά τέτοια συμπεριφορά σε αντίθεση με τον κόμβο 3, μεγαλώνει πολύ η πιθανότητα ο κόμβος 4 να ψεύδεται όσον αφορά την απόδειξη είσπραξης, και επομένως τιμωρείται ο 4 αντί του 3.
Στο S.A.R.C.I.S., χρησιμοποιούνται δύο τιμές κατωφλίου για τη συχνότητα των αναφορών. Πιο συγκεκριμένα, οι τιμές x και y χρησιμοποιούνται για την αναπαράσταση των κατωφλίων της συχνότητας ένας κόμβος να είναι ο τελευταίος που αναφέρει, και για την αναπαράσταση της συχνότητας ένας κόμβος να είναι ο πρώτος που δεν αναφέρει, αντίστοιχα. Επίσης ορίζονται ως F1 και F2, οι συχνότητες με τις οποίες ένας κόμβος βρίσκεται σε αυτές τις δύο καταστάσεις αντιστοίχως. Στον παρακάτω πίνακα φαίνεται η λήψη της απόφασης, για τους κόμβους 3 και του παραδείγματος που προηγήθηκε.

Καταγραφή Φήμης	Σχήμα Πληρωμής	
	Κόμβος 3	Κόμβος 4
F1<x, F2<y	0	0
F1>x, F2<y	-C3	0
F1<x, F2>y	C3	-C4
F1>x, F2>y	-C3	-C4

Πίνακας 6.2.1

Το επίπεδο φήμης, ορίζεται ως μέσος όρος στο χρόνο, και ανανεώνεται με την πάροδο του χρόνου, και για το λόγο αυτό ένας κόμβος με χαμηλή φήμη, δε μένει για πάντα σε αυτή την κατάσταση. Παρέχεται λοιπόν, ένα καλό κίνητρο ώστε οι κόμβοι να συνεργάζονται για να ανεβάζουν τη φήμη τους ώστε να μην τιμωρούνται από τις αποφάσεις του CCS. Τα κατώφλια x και y ορίζονται ανάλογα με τις συνθήκες (μεγαλύτερος ρυθμός απόρριψης πακέτων – μεγαλύτερη τιμή του x), όπως και η τοπολογία. Η συνολική λειτουργία του υβριδικού μηχανισμού S.A.R.C.I.S., κατανοείται απλά από το παρακάτω διάγραμμα ροής:



Σχήμα 6.2.6

6.2.3 ΦΑΣΗ ΑΝΑΖΗΤΗΣΗΣ ΔΙΑΔΡΟΜΗΣ ΔΡΟΜΟΛΟΓΗΣΗΣ

Οι αλγόριθμοι δρομολόγησης πρέπει όχι μόνο να αυξάνουν τις πιθανότητες των κόμβων για μετάδοση μηνυμάτων δίδοντας τους πιστώσεις, αλλά και να αυξάνουν τον χρόνο ζωής του δικτύου εξοικονομώντας ενέργεια στα κρίσιμα μονοπάτια του.

Ο αλγόριθμος δρομολόγησης του S.A.R.C.I.S. εξυπηρετεί αυτούς τους σκοπούς και λειτουργεί ως εξής, υποθέτοντας ότι ο κόμβος v_i αποστέλλει ένα πακέτο στον κόμβο v_j:

Αν ο v_i, συμπεριλάβει την ισχύ μετάδοσης που χρησιμοποιείται, στην κεφαλίδα του πακέτου, και ο κόμβος v_j, ορίζει την ελάχιστη ισχύ λήψης που απαιτείται, τότε η ελάχιστη ισχύς μετάδοσης του v_i, $P_{i,j}^{\min}$, μπορεί να υπολογιστεί. Η ισχύς αυτή, είναι η πραγματική ενέργεια μετάδοσης, και εξαρτάται από την απόσταση μεταξύ των δύο κόμβων. Όταν ένας κόμβος μεταδίδει πλατιά μια αίτηση διαδρομής δρομολόγησης, ο κόμβος παραλήπτης μπορεί να αναγγείλει το μικρότερο επίπεδο ισχύος , στην κεφαλίδα του πακέτου. Ύστερα, όταν ο κόμβος προορισμός ανακαλυφθεί, αποκτάται η συνολική πληροφορία του μονοπατιού.

Στην περίπτωση που ένας κόμβος έχει ένα πολύ χαμηλό επίπεδο εναπομείνασας ενέργειας, δεν επιθυμεί να προωθήσει πακέτα άλλων. Έτσι, υπάρχει μια μεταβλητή για την περιγραφή της θέλησης ενός κόμβου για συνεργασία, που συμπεριλαμβάνει και τον παράγοντα εναπομείνασας ενέργειας. Ορίζεται ως *E* η εναπομείνασα ενέργεια στον κόμβο, και ως *1/E*, η μη επιθυμία του κόμβου να προωθήσει. Επιπλέον, η τελευταία τιμή αναπαριστά την τιμή που απαιτεί ο κόμβος στην φάση της δρομολόγησης. Εάν η εναπομείνασα ενέργεια είναι χαμηλή, το σύστημα χρειάζεται μεγαλύτερη πληρωμή για την υπηρεσία. Αν η συνεργασία είναι επιτυχής, χρειάζεται μεγαλύτερη αντιστάθμιση λόγω των σκληρών θυσιών που έχουν γίνει.

Ακόμα, εισάγεται μια νέα μέτρηση NE για την αναπαράσταση του αριθμού των πακέτων που επιτρέπεται να αποσταλούν με την εναπομείνασα ενέργεια ενός κόμβου, και μια μέτρηση NC για την αναπαράσταση του αριθμού των πακέτων που επιτρέπεται να αποσταλούν βάσει των υπαρχόντων πιστώσεων. Όταν λοιπόν, είναι NE > NC, οι πιστώσεις που διαθέτει ένας κόμβος, είναι αρκετές για να υποστηρίξουν τη μετάδοση των πακέτων που μπορούν να σταλούν με την εναπομείνασα ενέργεια. Έτσι, οι κόμβοι επιθυμούν να συνεργαστούν για να αυξήσουν τη διαθεσιμότητα της ενέργειας παίρνοντας περισσότερες πιστώσεις.

Για το λόγο αυτό, στον αλγόριθμο δρομολόγησης του S.A.R.C.I.S., μοντελοποιείται ο βαθμός μη επιθυμίας για προώθηση με την μέτρηση NC/NE. Όσο αυξάνεται αυτή η τιμή, ο χρήστης επιθυμεί λιγότερο να προσφέρει υπηρεσίες και απαιτεί μεγαλύτερη αποζημίωση για να συνεργαστεί. Για να λαμβάνονται υπόψη όλοι οι παράγοντες που καθορίζουν την μη επιθυμία ενός κόμβου να προωθήσει, χρησιμοποιείται η παρακάτω έκφραση:

$$C_i = \left(a * \frac{1}{E} + b * \frac{NC}{NE} \right) * P_{i,j}^{\min}$$

, όπου *a* και *b* δύο σταθερές – βάρη, που αλλάζουν ανάλογα με την απόδοση του συστήματος. Με την ίδια έκφραση αναπαριστάται και το κόστος για την αναζήτηση διαδρομής δρομολόγησης. Το συνολικό κόστος για ένα μονοπάτι δίνεται από το άθροισμα του κόστους όλων των κόμβων σε αυτό και ορίζεται ως $C = \sum_i C_i$.

Το μονοπάτι με το μικρότερο κόστος επιλέγεται ως μονοπάτι δρομολόγησης. Όλες οι αποφάσεις στο S.A.R.C.I.S. αντιμετωπίζονται αυτόματα από τον αλγόριθμο δρομολόγησης.

6.2.4 ΑΠΟΤΕΛΕΣΜΑΤΙΚΟΤΗΤΑ ΤΟΥ S.A.R.C.I.S.

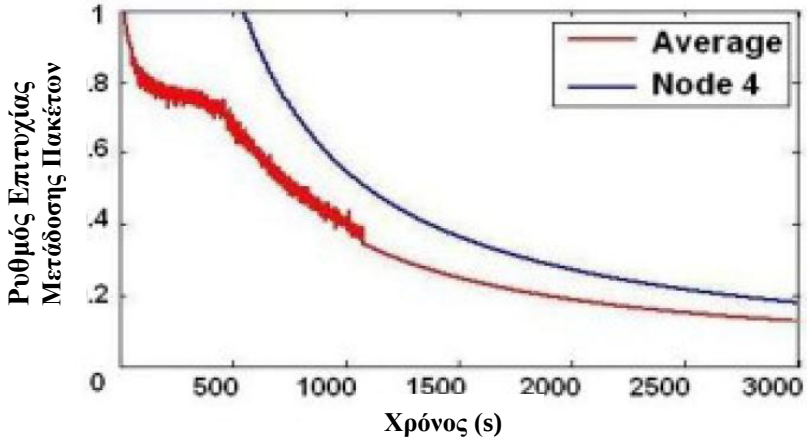
Οι δημιουργοί του S.A.R.C.I.S., έχουν πραγματοποιήσει πειράματα για την εξακρίβωση τη αποτελεσματικότητας του πρωτοκόλλου, χωρίς όμως να διευκρινίζουν τον προσομοιωτή που χρησιμοποιήθηκε. Το περιβάλλον προσομοίωσης που χρησιμοποιήθηκε για τα πειράματα είναι το εξής:

- Περιοχή 100m x 100m
- Κόμβοι 10
- Απλό μοντέλο κίνησης στο δίκτυο
- Ιδανικές συνθήκες δικτύου
- Διάρκεια προσομοίωσης 50 λεπτά
- Ρυθμός μετάδοσης κόμβου 20 πακέτα / δευτερόλεπτο
- Τυχαία επιλογή πηγής – προορισμού
- Σταθερές $\alpha = 200$ και $\beta = 3$
- Αρχική ενέργεια κόμβου 5000 μονάδες
- Αρχικές πιστώσεις κόμβου 20

Βασικές μετρήσεις έγιναν προσομοιώνοντας δίκτυο αρχικά για την κατάσταση όπου όλοι οι κόμβοι επιθυμούν να συνεργαστούν, και μετά για δίκτυο όπου εισάγεται κόμβος που έχει μη ομαλή συμπεριφορά, χωρίς να αλλάζει η συμπεριφορά των άλλων κόμβων. Ο κόμβος αυτός (ονομάζεται κόμβος 4 στις προσομοιώσεις), απορρίπτει πακέτα, ψεύδεται όσον αφορά τις αποδείξεις είσπραξης και πείθει κόμβους στο ίδιο μονοπάτι για πραγματοποίηση συμπαιγνίας. Από τις προσομοιώσεις προέκυψαν τα παρακάτω διαγράμματα και τα αντίστοιχα συμπεράσματα για την αποτελεσματικότητα του S.A.R.C.I.S. και την αποδοτικότητα του δικτύου. Αρχικά, με τη σειρά που εμφανίζονται τα διαγράμματα, προσομοιώνουν δίκτυα με τα εξής χαραχτηριστικά:

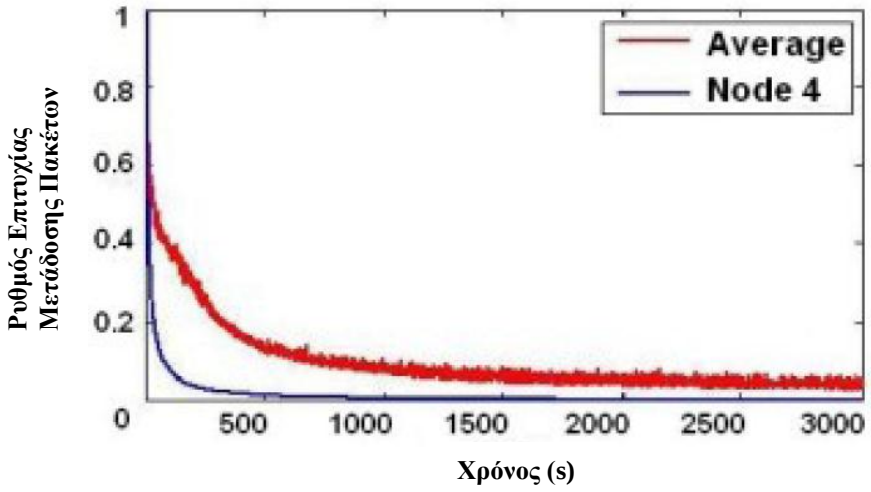
1. Όλοι οι κόμβοι είναι συνεργάσιμοι
2. Κόμβος που δεν προωθεί μηνύματα
3. Κόμβος που δεν αναφέρει αποδείξεις είσπραξης
4. Συμπαιγνία κόμβων

Τα διαγράμματα αυτά, έχουν στον κάθετο άξονα τον ***ρυθμό επιτυχίας μετάδοσης των πακέτων***, και στον οριζόντιο άξονα ***το χρόνο σε δευτερόλεπτα.*** Με την κόκκινη γραμμή συμβολίζεται ο μέσος όρος των αποτελεσμάτων όλων των κόμβων και με τη μπλε τα αποτελέσματα για τον κόμβο 4.



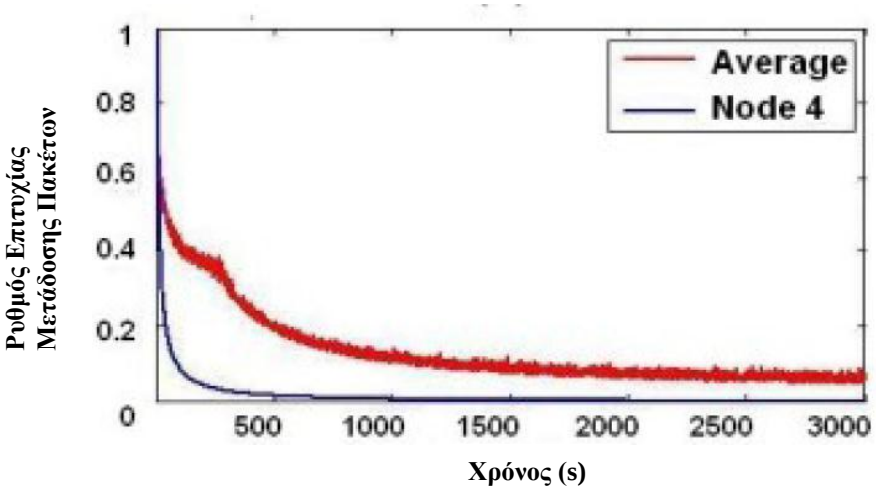
Όλοι οι κόμβοι είναι συνεργάσιμοι

Διάγραμμα 6.2.1 (Πηγή [17])



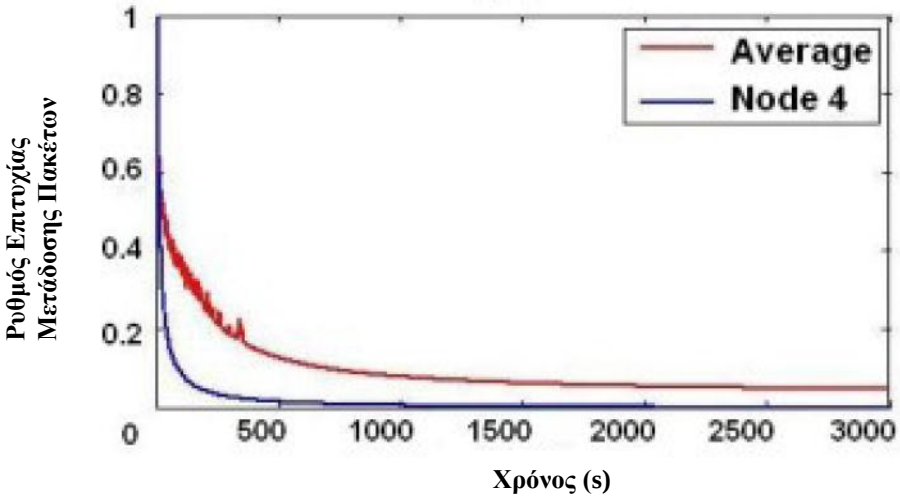
Κόμβος που δεν προωθεί μηνύματα

Διάγραμμα 6.2.2 (Πηγή [17])



Κόμβος που δεν αναφέρει αποδείξεις είσπραξης

Διάγραμμα 6.2.3 (Πηγή [17])



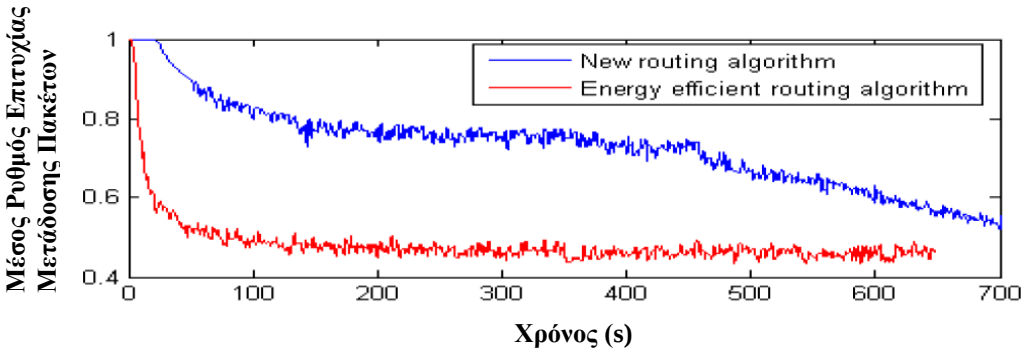
Συμπαιγνία Κόμβων

Διάγραμμα 6.2.4 (Πηγή [17])

Συμπεραίνεται ότι με την εισαγωγή εγωιστικής συμπεριφοράς ο ρυθμός επιτυχίας μετάδοσης πακέτων μειώνεται σημαντικά για όλο το σύστημα αλλά και για τον

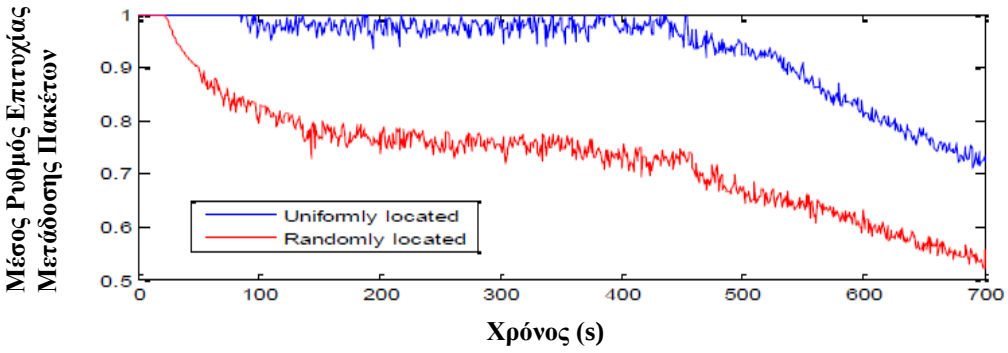
κόμβο 4. Οι εγωιστικές συμπεριφορές του κόμβου 4 μπορούν να εντοπιστούν και να τιμωρηθούν αποτελεσματικά μειώνοντας τις πιστώσεις. Φαίνεται ότι η εγωιστική συμπεριφορά, οι ψευδείς αναφορές δεν μπορούν να αυξήσουν το ρυθμό επιτυχίας μηνύματος του κόμβου, επομένως δεν είναι συμφέρουσα από τους κόμβους η επιλογή εγωιστικής συμπεριφοράς, και άρα το σύστημα πιστώσεων λειτουργεί αποτελεσματικά στην απόδοση κινήτρων για συνεργασία.

Το παρακάτω εξαχθέν διάγραμμα δείχνει τη σύγκριση μεταξύ δικτύου που χρησιμοποιεί αλγόριθμο δρομολόγησης βασιζόμενο στην υπάρχουσα ενέργεια (κόκκινη γραμμή) και δικτύου με τον αλγόριθμο δρομολόγησης του S.A.R.C.I.S. Έχει στον κάθετο άξονα τον ***μέσο ρυθμό επιτυχίας μετάδοσης πακέτων***, και στον οριζόντιο άξονα ***το χρόνο σε δευτερόλεπτα***. Είναι εμφανές ότι λόγω της ιδιότητας του αλγόριθμου του S.A.R.C.I.S. που συνδυάζει εναπομείνασα ενέργεια και πιστώσεις, να μην σταματάνε τη λειτουργία τους οι κόμβοι λόγω υπερχρησιμοποίησης πόρων. Αποτέλεσμα, ο ρυθμός επιτυχίας μετάδοσης πακέτου να είναι με τον αλγόριθμο του S.A.R.C.I.S. 10% μεγαλύτερος από ότι με τον άλλον.



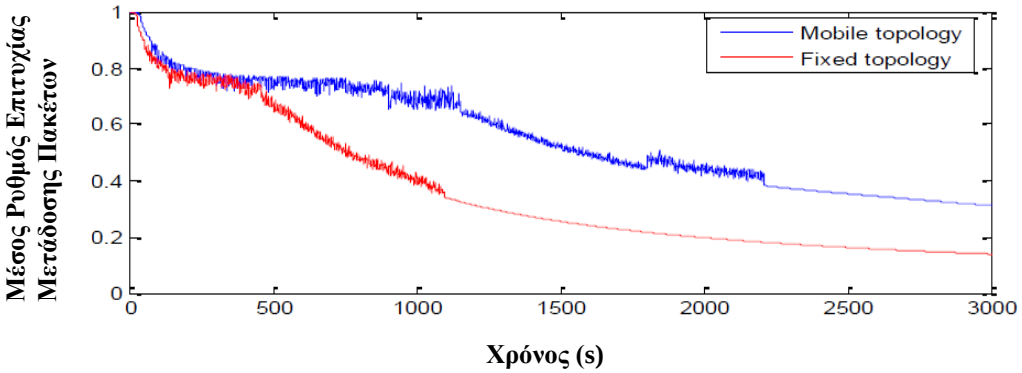
Διάγραμμα 6.2.5 (Πηγή [17])

Ακόμα συμπεραίνεται ότι η εφαρμογή συγκεκριμένης τοπολογίας όπως η ομοιόμορφη τοποθέτηση των κόμβων (μπλε γραμμή) είναι καλύτερη όσον αφορά το ρυθμό επιτυχίας μετάδοσης πακέτων, από μια τυχαία τοπολογία, πράγμα που εξηγείται από το γεγονός ότι στην τυχαία τοπολογία οι πολύ απομακρυσμένοι κόμβοι δεν μπορούν να συμμετέχουν στο δίκτυο εύκολα ή να συμμετέχουν στην προώθηση. Αυτό φαίνεται και από το παρακάτω διάγραμμα, που έχει στον κάθετο άξονα τον ***μέσο ρυθμό επιτυχίας μετάδοσης πακέτων***, και στον οριζόντιο άξονα ***το χρόνο σε δευτερόλεπτα.***



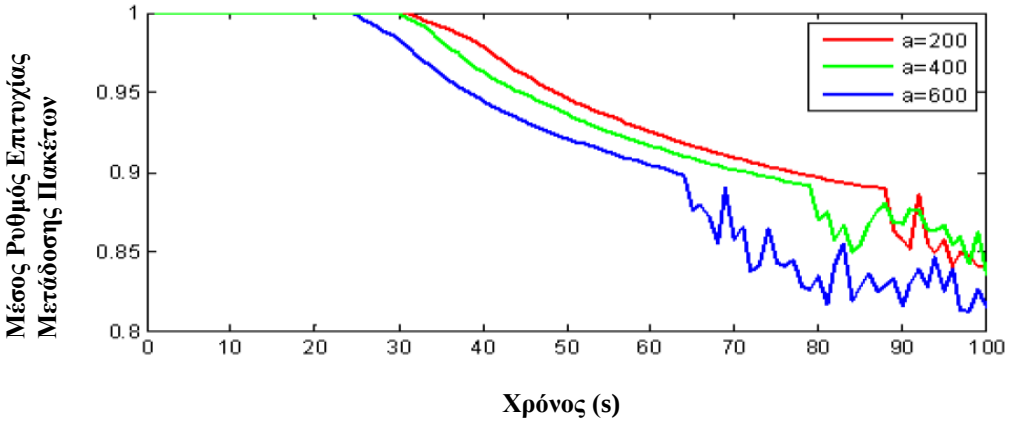
Διάγραμμα 6.2.6 (Πηγή [17])

Κάτι αντίστοιχο συμβαίνει και στην περίπτωση που οι κόμβοι είναι κινητοί (μπλε γραμμή) σε σχέση με ένα δίκτυο που χρησιμοποιεί καθορισμένη τοπολογία (κόκκινη γραμμή). Αυτό συμπεραίνεται από το παρακάτω εξαχθέν διάγραμμα, που όπως και τα υπόλοιπα, έχει στον κάθετο άξονα τον ***μέσο ρυθμό επιτυχίας μετάδοσης πακέτων***, και στον οριζόντιο άξονα ***το χρόνο σε δευτερόλεπτα.***



Διάγραμμα 6.2.7 (Πηγή [17])

Τέλος, στο παρακάτω διάγραμμα που έχει στον κάθετο άξονα τον ***μέσο ρυθμό επιτυχίας μετάδοσης πακέτων***, και στον οριζόντιο άξονα ***το χρόνο σε δευτερόλεπτα***, γίνεται σύγκριση ανάμεσα σε δίκτυα με διαφορετικές τιμές του παράγοντα *α*, και πιο συγκεκριμένα για *α* = 200 (κόκκινη γραμμή), *α* = 400 (πράσινη γραμμή) και *α* = 600 (μπλε γραμμή). Συμπεραίνεται ότι ο χρόνος ζωής του δικτύου μεγαλώνει όσο μεγαλώνει το *α* που αναπαριστά το βάρος της εναπομείνασας ενέργειας, πράγμα όμως που μειώνει τον ρυθμό επιτυχίας μετάδοσης των πακέτων.



Διάγραμμα 6.2.8 (Πηγή [17])

Συμπερασματικά, ο υβριδικός μηχανισμός υποστήριξης συνεργασίας S.A.R.C.I.S., με την λειτουργία προώθησης που χρησιμοποιεί χαρακτηριστικά βασισμένα ταυτόχρονα στη φήμη και τις πιστώσεις, και τον αλγόριθμο δρομολόγησης που ισορροπεί την εναπομείνασα ενέργεια και τις πιστώσεις, προωθεί τη συνεργασία μεταξύ των κόμβων, αποθαρρύνει τρεις τύπους εγωιστικής συμπεριφοράς με αρκετά μικρό overhead. Τέλος, η ισορροπία μεταξύ κατανάλωσης ενέργειας και πιστώσεων, μεγαλώνει το χρόνο ζωής του δικτύου, δίνοντας τη δυνατότητα για επιλογή μεταξύ αυτού, και του ρυθμού επιτυχίας μετάδοσης πακέτων.

Κεφάλαιο 7

ΥΒΡΙΔΙΚΟΙ ΜΗΧΑΝΙΣΜΟΙ ΥΠΟΣΤΗΡΙΞΗΣ ΣΥΝΕΡΓΑΣΙΑΣ ΕΝΑΝΤΙ ΜΗ ΥΒΡΙΔΙΚΩΝ

7.1 ΠΡΟΣΘΕΝΤΑ ΠΡΟΣΟΝΤΑ ΥΒΡΙΔΙΚΩΝ ΜΗΧΑΝΙΣΜΩΝ ΥΠΟΣΤΗΡΙΞΗΣ ΣΥΝΕΡΓΑΣΙΑΣ

Στα πλαίσια της παρούσας διπλωματικής εργασία, παρουσιάστηκε η λειτουργία μηχανισμών υποστήριξης συνεργασίας, των δύο θεμελιωδών κατηγοριών: των σχημάτων που βασίζονται στη φήμη, και των σχημάτων που βασίζονται στην τιμολόγηση και τις πιστώσεις. Είναι εμφανές από τα αποτελέσματα των πειραμάτων που έχουν πραγματοποιήσει οι δημιουργοί των αναφερόμενων σχημάτων, ότι οι μηχανισμοί αυτοί, έως ένα σημαντικό βαθμό, καταφέρνουν να ενισχύσουν τη συνεργασία μεταξύ των κόμβων στα αυτοοργανούμενα ad-hoc δίκτυα με κίνητρα, να ελαττώσουν την κακόβουλη δράση των εγωιστικών και μη ομαλά συμπεριφερόμενων κόμβων. Παρόλα αυτά, τα εν λόγω σχήματα υποφέρουν από αρκετά μειονεκτήματα. Για το λόγο αυτό, έντονη έρευνα διεξάγεται τα τελευταία χρόνια πάνω στο σχεδιασμό υβριδικών μηχανισμών υποστήριξης συνεργασία, όπως αυτοί που αναλύθηκαν στην προηγούμενη ενότητα, οι οποίοι χρησιμοποιούν συνδυασμό των χαρακτηριστικών των δύο βασικών κατηγοριών, δηλαδή της φήμης και των πιστώσεων.

Η ανάπτυξη υβριδικών μηχανισμών υποστήριξης συνεργασίας για ad-hoc δίκτυα, πατάει πάνω στην αντιμετώπιση των βασικών μειονεκτημάτων των δύο βασικών κατηγοριών σχημάτων, όπως αυτό φαίνεται παρακάτω:

1. **Βασικό Μειονέκτημα Σχημάτων Φήμης:** Τα περισσότερα πρωτόκολλα συνεργασίας που βασίζονται στη φήμη, θέτουν ένα κατώφλι φήμης, για την διάκριση συνεργάσιμων και εγωιστικών κόμβων. Όσοι κόμβοι διατηρούν φήμη μεγαλύτερη από αυτό το κατώφλι, θεωρούνται συνεργάσιμοι, ενώ όσοι έχουν φήμη χαμηλότερη από αυτό το κατώφλι θεωρούνται εγωιστικοί κόμβοι. Όλη η λειτουργία αυτών των μηχανισμών βασίζεται σε αυτήν την παραδοχή, από την οποία και πηγάζει το κύριο μειονέκτημα τους: Κόμβοι με φήμη λίγο πάνω από το κατώφλι, απολαμβάνουν ίδιας ποιότητας υπηρεσίες προώθησης πακέτων, με τους κόμβους που διαθέτουν εξαιρετικά υψηλή φήμη. Κάτι τέτοιο εισάγει αδικίες στο σύστημα, καθώς ένας κόμβος δεν αναγκάζεται να συνεργάζεται διαρκώς, αλλά αρκείται στη συνεργασία μέχρι του σημείου που θα κρατά τη φήμη του, ελάχιστα πάνω από το κατώφλι. Με τον τρόπο αυτό αδικείται ο κόμβος που προσφέρει τις προωθητικές του υπηρεσίες όποτε του ζητηθούν, και η μεγάλη φήμη του δεν του επιφέρει μια επιπλέον επιβράβευση.

2. **Βασικό Μειονέκτημα Σχημάτων Πιστώσεων:** Τα πρωτόκολλα συνεργασίας που βασίζονται στην τιμολόγηση και τις πιστώσεις, θεωρούν την προώθηση πακέτων ως μια υπηρεσία που μπορεί να τιμολογηθεί και εισάγουν μια μορφή ψηφιακών νομισμάτων για τη ρύθμιση σχέσεων προώθησης ανάμεσα στους κόμβους. Παρόλα αυτά, βασιζόμενοι μόνο στις πιστώσεις, οι κόμβοι δεν μπορούν να γνωρίζουν σε βάθος την ποιότητα της υπηρεσίας που προσφέρουν οι άλλοι κόμβοι, πράγμα που σημαίνει ότι ένας κόμβος που έχει αποκτήσει μεγάλα αποθέματα πιστώσεων, μπορεί να είναι επίσης εγωιστικός, και να μην επιθυμεί να συνεργαστεί πλέον.

Η νέα λογική που εισάγεται από τους υβριδικούς μηχανισμούς, είναι σε γενικές γραμμές, να λαμβάνεται υπόψη η φήμη των κόμβων κατά τον καθορισμό της

χρέωσης τους για την λήψη μιας υπηρεσίας. Με άλλα λόγια, οι κόμβοι με υψηλή φήμη χρεώνονται λιγότερο για την προώθηση των πακέτων τους, σε αντίθεση με τους κόμβους με χαμηλή φήμη που χρεώνονται περισσότερο. Με τον τρόπο αυτό αποτρέπεται ένας κόμβος από το να κρατά τη φήμη του λίγο πάνω από το κατώφλι όπως αναφέρθηκε.
Από την άλλη, στα υβριδικά σχήματα, για κάθε πακέτο που αποστέλλει ένας κόμβος πηγή, του αφαιρούνται και πιστώσεις, ενώ όταν αυτός προωθεί πακέτα άλλων, αυξάνονται οι πιστώσεις του. Με τον τρόπο αυτό προσφέρονται κίνητρα στους κόμβους, ώστε να προσφέρουν τις προωθητικές τους υπηρεσίες με σκοπό να έχουν πάντα στη διάθεση τους πιστώσεις ικανές για να στείλουν τα δικά τους πακέτα. Άλλος τρόπος για την αντιμετώπιση του βασικού μειονεκτήματος των σχημάτων πιστώσεων από τα υβριδικά, είναι η ενσωμάτωση του πλούτου σε πιστώσεις που κατέχει ένας κόμβος, στο κόστος διαδρομής δρομολόγησης, στο κόστος μονοπατιού. Όταν το μονοπάτι το οποίο περιέχει κόμβους με πολύ μεγάλο πλήθος πιστώσεων γίνεται πιο ακριβό για την αποστολή πακέτων, από ότι άλλα μονοπάτια, είναι λογικό να μην επιλέγεται από κάποιον κόμβο που θέλει να προωθήσει τα πακέτα του. Με τον τρόπο αυτό, αποφεύγεται το φαινόμενο, κάποιοι κόμβοι να δημιουργούν μεγάλο απόθεμα πιστώσεων και στη συνέχεια να μην συνεργάζονται, αφού σταδιακά οι πιστώσεις τους θα πέφτουν, αν αυτοί δεν προσφέρουν υπηρεσίες προώθησης, ως αποτέλεσμα της μη επιλογής τους.

Ακόμα:

- Τα περισσότερα υβριδικά σχήματα, σε αντίθεση με τα σχήματα φήμης, δεν υποχρεώνουν τους κινητούς κόμβους να κρατούν πίνακες φήμης, αλλά αντιθέτως αναθέτουν την λειτουργία της διαχείρισης σε κάποια τρίτη έμπιστη οντότητα. Με τον τρόπο αυτό εξασφαλίζεται η εξοικονόμηση υπολογιστικών πόρων, ενώ επιτρέπεται στους κόμβους η χρήση περισσότερων πόρων για τη μετάδοση πακέτων, πράγμα που ενισχύει και διευκολύνει τη συνεργασία μεταξύ τους.
- Κάτι ανάλογο συμβαίνει και με τους λογαριασμούς πιστώσεων, πράγμα που μειώνει το overhead στο δίκτυο.

Σήμερα, δεν έχει διεξαχθεί μεγάλος αριθμός πειραμάτων για την εξαγωγή ασφαλών συμπερασμάτων σχετικά με την ανωτερότητα των υβριδικών μηχανισμών υποστήριξης συνεργασίας σε σχέση με τα σχήματα φήμης και πιστώσεων. Παρόλα αυτά, από την θεωρητική σύγκριση, τα διεξαχθέντα πειράματα, αλλά και με βάση τη θεωρία παιγνίων, φαίνεται ότι στα υβριδικά σχήματα, η συνεργασία των κόμβων, γίνεται πολύ πιο γρήγορα βέλτιστη στρατηγική των κόμβων, από ότι στους υπόλοιπους μηχανισμούς υποστήριξης συνεργασίας στα ad-hoc. Για το λόγο αυτό, η κατεύθυνση της σύγχρονης έρευνας πάνω σε νέους μηχανισμούς, δίνει βάρος στις υβριδικές λύσεις. Παράλληλα, από τα αποτελέσματα των προσομοιώσεων για την αποτελεσματικότητα των υβριδικών μηχανισμών, συμπεραίνεται η ικανότητα των σχημάτων αυτών, στην σημαντική αύξηση του throughput του δικτύου έναντι σε δίκτυα που δεν χρησιμοποιούν κάποιο πρωτόκολλο συνεργασίας, αλλά και στον εντοπισμό και την τιμωρία των υπαρχόντων εγωιστικών κόμβων.

Κεφάλαιο 8

ΣΥΜΠΕΡΑΣΜΑΤΑ

8.1 ΣΥΝΟΨΗ ΚΑΙ ΣΥΜΠΕΡΑΣΜΑΤΑ

Συνοψίζοντας τα όσα παρουσιάστηκαν στην παρούσα εργασία, τονίζονται εδώ τα σημαντικότερα σημεία που απασχόλησαν κατά τη συγγραφή.
Αρχικά, περιγράφηκαν τα βασικά στοιχεία της αρχιτεκτονικής και της λειτουργίας των ad-hoc δικτύων, ο σημαντικός ρόλος της ενέργειας που καταναλώνουν οι κόμβοι και η δρομολόγηση. Τονίστηκε η διαφορετικά τους από τα υπόλοιπα δίκτυα, λόγω της έλλειψης κάποιας εσωτερικής υποδομής, πράγμα που δημιουργεί και την ανάγκη για ενίσχυση της συνεργασίας μεταξύ των κόμβων.
Στη συνέχεια παρουσιάστηκαν με τη σειρά, οι τρεις βασικές κατηγορίες μηχανισμών υποστήριξης συνεργασίας για την αντιμετώπιση των εγωιστικών κόμβων οι οποίοι δεν προσφέρουν προωθητικές υπηρεσίες για να εξυπηρετήσουν τα συμφέροντα τους, και για την τόνωση της συνεργασίας των κόμβων. Ανάλογα με τις βασικές αρχές λειτουργίας τους διακρίθηκαν οι εξής αυτές κατηγορίες:

1. Οι Μηχανισμοί Υποστήριξης Συνεργασίας που βασίζονται στη φήμη, όπου οι κόμβοι διατηρούν και ανταλλάσσουν τιμές φήμης για τους υπόλοιπους κόμβους, ανάλογα με τις οποίες ένας κόμβος απολαμβάνει ή όχι τις υπηρεσίες του δικτύου.
2. Οι Μηχανισμοί Υποστήριξης Συνεργασίας που βασίζονται στις πιστώσεις, όπου οι προωθητικές υπηρεσίες κοστίζουν και αγοράζονται από τους κόμβους με πιστώσεις, έτσι ώστε ένας κόμβος ο οποίο διαθέτει πιστώσεις να μπορεί να προωθήσει τα πακέτα του σε αντίθεση με κάποιον που δεν έχει.
3. Οι Υβριδικοί Μηχανισμοί Υποστήριξης Συνεργασίας, όπου χρησιμοποιούνται στοιχεία και από τις δύο προηγούμενες κατηγορίες.

Για κάθε βασική κατηγορία παρουσιάστηκαν κάποια από τα δημοφιλέστερα πρωτόκολλα, που ακόμα και για την ίδια κατηγορία διατηρούν αρκετές διαφορές στη λειτουργία τους. Είναι φυσικό, να μην μπορούν να παρουσιαστούν όλα τα πρωτόκολλα που έχουν δημιουργηθεί, καθώς ο αριθμός τους είναι τεράστιος και έχουν δημιουργηθεί από δεκάδες ομάδες εργασίας. Για το λόγο αυτό επιλέχθηκαν μηχανισμοί δημοφιλείς, που έχουν δημοσιευτεί σε διακεκριμένα επιστημονικά περιοδικά και συνέδρια. Στην παρουσίαση κάθε μηχανισμού, παρατίθενται στην εργασία οι υποθέσεις που έγιναν κατά την σχεδίαση τους, αλλά και τα αποτελέσματα που εξήγαγαν οι δημιουργοί τους, ώστε να εξαχθούν συμπεράσματα όσον αφορά την αποτελεσματικότητα τους.

Στην διπλωματική εργασία, διενεργήθηκε επίσης πρωτότυπη έρευνα πάνω στην εύρεση των κρίσιμων ζητημάτων που λαμβάνονται υπόψη κατά των σχεδιασμό των μηχανισμών υποστήριξης συνεργασίας στα ad-hoc, και η σύγκριση των παρουσιασθέντων σχημάτων με βάση αυτά. Πιο συγκεκριμένα, για την πρώτη κατηγορία διακρίθηκαν ζητήματα όπως ο τρόπος, ο αποστολέας και η μορφή των πληροφοριών φήμης, ο τύπος της πληροφορίας, ο τρόπος τιμωρίας των εγωιστικών κόμβων και η ύπαρξη ασφάλειας στα δεδομένα. Για την δεύτερη κατηγορία, διακρίθηκαν ζητήματα όπως ο τρόπος αναπαράστασης των πιστώσεων, ο τύπος της ασφάλειας ενάντια στις αλλοιώσεις, ο τρόπος χρέωσης και το πρωτόκολλο δρομολόγησης με το οποίο είναι συμβατά τα σχήματα. Τέλος, μελετώντας τους υβριδικούς μηχανισμούς, εντοπίστηκαν τα πρόσθετα στοιχεία, που τους καθιστούν πιο αποτελεσματικούς από τις δύο πρώτες κατηγορίες σχημάτων.

Από τη μελέτη των παρουσιασθέντων μηχανισμών υποστήριξης συνεργασίας, εξάγονται χρήσιμα συμπεράσματα. Τονίζεται ότι η σύγκριση ενέχει αντικειμενικές δυσκολίες, εφόσον οι δημιουργοί κάθε πρωτοκόλλου έχουν κάνει διαφορετικές υποθέσεις σχετικά με τη λειτουργία του δικτύου, έχουν χρησιμοποιήσει διαφορετικά προγράμματα και περιβάλλοντα προσομοίωσης. Παρόλα αυτά, μπορούν ασφαλώς να εξαχθούν αδιαμφισβήτητα συμπεράσματα όσον αφορά την επίτευξη του σκοπού για τον οποίο δημιουργήθηκαν. Συγκεκριμένα, από την παρουσίαση και μελέτη των μηχανισμών υποστήριξης συνεργασίας όλων των κατηγοριών συμπεραίνεται ότι:

- Μειώνεται σημαντικά ο αριθμός των πακέτων που απορρίπτονται κατά την επικοινωνία στο δίκτυο, αφού ενισχύεται η συνεργασία, εντοπίζονται και αποβάλλονται οι εγωιστικοί κόμβοι που απορρίπτουν πακέτα.
- Αυξάνεται σημαντικά το μέσο throughput του δικτύου, λόγω της μεγαλύτερης επιτυχούς μετάδοσης και προώθησης πακέτων που επιτυγχάνει η τόνωση της συνεργασίας.
- Αυξάνεται η επιβάρυνση overhead στο δίκτυο, λόγω της έξτρα ανταλλασσόμενης πληροφορίας είτε αυτή είναι πληροφορία φήμης είτε άλλη πληροφορία για τις πρόσθετες λειτουργίες που εισάγουν τα πρωτόκολλα.
- Εντοπίζονται οι εγωιστικοί κόμβοι, και είτε αποβάλλονται από το δίκτυο, είτε ωθούνται να συμμετέχουν στην προωθητική διαδικασία.
- Οι υβριδικοί μηχανισμοί καθιστούν τη συνεργασία των κόμβων γρηγορότερη, αλλά και εξοικονομούν πολύτιμους υπολογιστικούς πόρους που μπορούν να χρησιμοποιηθούν στην προώθηση.

Ακόμα, συμπεραίνεται ότι όλοι οι υπάρχοντες μηχανισμοί υποστήριξης συνεργασίας, πρέπει να πατάνε πάνω σε συγκεκριμένες υποθέσεις και ζητήματα σχεδιασμού, και απαιτούν την υιοθέτηση παραδοχών κατά την προσομοίωση τους, λόγω της μεγάλης πολυπλοκότητας που εισάγεται στα ad-hoc δίκτυα.
Σε γενικές γραμμές, η σύγκριση μεταξύ των μηχανισμών των δύο πρώτων κατηγοριών, δεν μπορεί να οδηγήσει σε ασφαλή συμπεράσματα σχετικά με το ποια κατηγορία είναι πιο αποτελεσματική, καθώς απαιτούνται αφενός συγκριτικές μελέτες μεταξύ των καλύτερων πρωτοκόλλων και από τις δύο κατηγορίες, καθώς και εφαρμογή σε αληθινά δίκτυα. Κάτι τέτοιο έχει πραγματοποιηθεί μόνο για λίγα από τα σχήματα που έχουν δημοσιευτεί.

Συμπερασματικά, φαίνεται ότι οι μηχανισμοί υποστήριξης συνεργασίας, μπορούν να προσφέρουν σημαντικές λύσεις στο πρόβλημα του εγωισμού που προκαλείται από την ίδια τη φύση των ad-hoc δικτύων, ενισχύουν έμπρακτα τη συνεργασία και εντοπίζουν τους μη ομαλά συμπεριφερόμενους κόμβους, αυξάνοντας έτσι αποτελεσματικά την απόδοση του δικτύου σε σημαντικό βαθμό. Το μέλλον της έρευνας πάνω στους μηχανισμούς υποστήριξης συνεργασίας τελικά, διαγράφεται μεγάλο, λόγω και της όλο και περισσότερο ευρύτερης χρήσης των ad-hoc που επιτάσσεται από την εισαγωγή νέας τεχνολογίας στους υπολογιστές και τα δίκτυα.

ΒΙΒΛΙΟΓΡΑΦΙΑ

ΒΙΒΛΙΟΓΡΑΦΙΑ

[1] Sonja Buchegger, Jean-Yves Le Boudec, *Performance Analysis of the CONFIDANT Protocol (Cooperation Of Nodes: Fairness In Dynamic Adhoc NeTworks)*, MobiHoc, 2002

[2] Sonja Buchegger, Jean-Yves Le Boudec, *A Robust Reputation System for P2P and Mobile Ad-hoc Networks*, Second Workshop on the Economics of Peer-to-Peer Systems, 2004

[3] Qi He, Dapeng Wu, Pradeep Khosla, *SORI: A Secure and Objective Reputation-based Incentive Scheme for Ad-hoc Networks*, Wireless Communications and Networking Conference, 2004

[4] Pietro Michiardi, Refik Molva, *CORE: A Collaborative Reputation Mechanism to enforce node cooperation in Mobile Ad hoc Networks*, IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, 2006

[5] Sorav Bansal, Mary Baker, *Observation-based Cooperation Enforcement in Ad hoc Networks*, CoRR, 2003

[6] Sergio Marti, T.J. Giuli, Kevin Lai, Mary Baker, *Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*, MobiCom, 6th annual international conference on Mobile computing and networking, 2000

[7] Jiangyi Hu, *Cooperation in Mobile Ad Hoc Networks*, Guide to Wireless Ad Hoc Networks, 2005

[8] Charikleia Zouridaki, Brian L. Mark, Marek Hejmo, Roshan K. Thomas, *E-Hermes: A robust cooperative trust establishment scheme for mobile ad hoc networks*, Ad Hoc Networks, 2009

[9] Fang Liu, Rongsheng Dong, Jianming Liu, Xuliang Xu, *A Reputation Mechanism to Stimulate Node Cooperation in Ad Hoc Networks*, Third International Conference on Genetic and Evolutionary Computing, 2009

[10] Zahra Safaei, Masoud Sabaei, Fatemeh Torgheh, *An Efficient Reputation-Based Mechanism to Enforce Cooperation in MANETs*, Application of Information and Communication Technologies, 2009

[11] Tingting Chen, Fan Wu, Sheng Zhong, *FITS: A Finite-Time Reputation System for Cooperation in Wireless Ad Hoc Networks*, IEEE Transactions on computers, Vol. 60, No. 7, July 2011

[12] Levente Buttyan, Jean-Pierre Hubaux, *Nuglets: a Virtual Currency to Stimulate Cooperation in Self-Organized Mobile Ad Hoc Networks*, Technical Report DSC/2001/001, 2001

[13] Sheng Zhong, Jiang Chen, Yang Richard Yang, *Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks*, INFOCOM, 2003

[14] Younghwan Yoo, Sanghyun Ahn, Dharma P. Agrawal, *A Credit-Payment Scheme for Packet Forwarding Fairness in Mobile Ad Hoc Networks,* Communications, 2005

[15] Hamed Janzadeh, Kaveh Fayazbakhsh, Mehdi Dehghan_, Mehran S. Fallah, *A secure credit-based cooperation stimulating mechanism for MANETs using hash chains*, Future Generation Computer Systems, Volume 25 Issue 8, September, 2009

[16] Haiying Shen, Ze Li, *ARM: An Account-based Hierarchical Reputation Management System for Wireless Ad Hoc Networks,* Distributed Computing Systems Workshops, 2008

[17] Luyang Zhang, Mahesh Sooriyabandara, Zhong Fan, *A Simple and Reliable Credit-Balanced Incentive Scheme for Wireless Ad-hoc Networks*, Wireless Communications and Mobile Computing Conference (IWCMC), 2011

[18] Ze Li, Haiying Shen, *Analysis the Cooperation Strategies in Mobile Ad hoc Networks*, Mobile Ad Hoc and Sensor Systems, 2008

[19] Louta Malamati, Kraounakis Stylianos, Michalas Angelos, *A survey on reputation-based cooperation enforcement schemes in wireless ad hoc networks*, Wireless Information Networks and Systems (WINSYS), 2010

[20] Mohamed Tamer Refaei, Luiz A. DaSilva, Mohamed Eltoweissy, Tamer Nadeem, *Adaptation of Reputation Management Systems to Dynamic Network Conditions in Ad Hoc Networks*, IEEE Transactions on computers, Vol. 59, No. 5, May 2010

[21] Po-Wah Yau and Chris J. Mitchell, *Reputation Methods for Routing Security for Mobile Ad Hoc Networks,* Mobile Future and Symposium on Trends in Communications, 2003

[22] Andrew S. Tanenbaum, *Computer Networks, Fourth Edition*, Pearson Education, 2003

[23] Lu Han, *Wireless Ad-hoc Networks*, October 8, 2004

[24] Alex Song, *Piconet II - A Wireless Ad Hoc Network for Mobile Handheld Devices*, 2001

[25] G. F. Marias, P. Georgiadis, D. Flitzanis, K. Mandalas, *Cooperation enforcement schemes for MANETs: A survey*, Wiley InterScience, 2006