ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μελέτη των απειλών και προκλήσεων σε θέματα ασφάλειας των ασύρματων δικτύων αισθητήρων (Wireless Sensor Networks - WSNs) και των υλοποιήσεων τους στο Διαδίκτυο των Πραγμάτων (Internet of Things – IoT)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΤΙΓΚΟΥ ΣΤΕΡΓΙΟΥ

(ΑΕΜ: 2494)

Επιβλέπων : Σπυρίδων Νικολάου

Λέκτορας

Καστοριά Απρίλιος 2023

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Μελέτη των απειλών και προκλήσεων σε θέματα ασφάλειας των ασύρματων δικτύων αισθητήρων (Wireless Sensor Networks - WSNs) και των υλοποιήσεων τους στο Διαδίκτυο των Πραγμάτων (Internet of Things – IoT)

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

του

ΤΙΓΚΟΥ ΣΤΕΡΓΙΟΥ

(ΑΕΜ: 2494)

Επιβλέπων : Σπυρίδων Νικολάου
Λέκτορας

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 7/4/2023

Σπυρίδων Νικολάου	**Βέργαδος Δημήτριος**	**Βαρδάκας Ιωάννης**
Λέκτορας	**Επίκουρος Καθηγητής**	**Αναπληρωτής Καθηγητής**

Καστοριά Απρίλιος 2023

Ευχαριστίες

Η παρούσα διπλωματική εργασία συντάχθηκε στα πλαίσια του προπτυχιακού προγράμματος σπουδών του τμήματος Πληροφορικής του Πανεπιστημίου Δυτικής Μακεδονίας. Πρωτίστως, θα ήθελα να ευχαριστήσω τον λέκτορα κύριο Σπυρίδων Νικολάου, ο οποίος ανέλαβε την επίβλεψη της εργασίας, για την υποστήριξη και καθοδήγηση του. Επιπλέον, θα ήθελα να ευχαριστήσω την οικογένεια μου, η οποία με στήριξε ανελλιπώς με τον καλύτερο δυνατό τρόπο, καθώς και τους καθηγητές και τους συμφοιτητές μου, με τους οποίους είχα μία εποικοδομητική συνεργασία κατά τη διάρκεια των σπουδών μου.

Περίληψη

Τα ασύρματα δίκτυα αισθητήρων (Wireless Sensor Networks) είναι μια δικτυακή υποδομή με μεγάλο αριθμό συσκευών χαμηλού αλλά και υψηλού κόστους—κόμβους που αναπτύσσονται σε περιοχές ενδιαφέροντος. Στόχος τους είναι ο εντοπισμός, η παρακολούθηση και η καταγραφή δεδομένων από την περιοχή. Οι διαδρομές του WSN συνέλεγαν πληροφορίες και μηνύματα διαχείρισης στους σταθμούς βάσης μέσω των κόμβων που το αποτελούν. Οι κόμβοι που συμμετέχουν σε ασύρματα δίκτυα αισθητήρων περιορίζονται σοβαρά όσον αφορά τον υπολογισμό, την αποθήκευση και την ενέργεια λόγω της ανάγκης ελέγχου του κόστους δικτύου και εξοικονόμησης ενέργειας για την αύξηση των ορίων λειτουργίας του δικτύου. Με βάση τους περιορισμούς της αρχιτεκτονικής δικτύου, αναπτύχθηκαν πρωτόκολλα επικοινωνίας που λαμβάνουν υπόψη το μοντέλο OSI. Αυτά τα πρωτόκολλα υλοποιούν στοίβες πρωτοκόλλων που βασίζονται σε αυτήν την αρχιτεκτονική και αποτελούν τη βάση για την ανάπτυξη προτύπων επικοινωνίας.

Οι περιοριστικοί παράγοντες στα WSN σε συνδυασμό με το μέσο ασύρματης μετάδοσης και την απομακρυσμένη λειτουργία χωρίς επίβλεψη καθιστούν το δίκτυο ευάλωτο σε πιθανές επιθέσεις. Οι επιθέσεις αυτές αμφισβητούν τις απαιτήσεις ασφάλειας του δικτύου στοχεύοντας στις λειτουργίες αυτού με βάση την αρχιτεκτονική τους, η πιο σημαντική από τις οποίες είναι η επίθεση Denial of Service (DoS). Το πρωτόκολλο που αναπτύχθηκε βασίζεται σε έναν απλό και ενεργειακά αποδοτικό σχεδιασμό. Για το λόγο αυτό, έχουν αναπτυχθεί μηχανισμοί που παρέχουν διασφάλιση όσον αφορά τον εντοπισμό επιθέσεων, τη δρομολόγηση και τη συλλογή δεδομένων. Επιπλέον, προς αυτή την κατεύθυνση αναπτύσσονται επίσης μηχανισμοί ελέγχου ταυτότητας και κρυπτογράφησης απορρήτου. Ωστόσο, οι παραπάνω μηχανισμοί παρέχουν ασφάλεια στο δίκτυο με κόστος αυξημένης πολυπλοκότητας δικτύου και κατανάλωσης ενέργειας.

Η εποχή του Διαδικτύου των Πραγμάτων (IoT) έχει ξεκινήσει και θα φέρει επανάσταση στον τρόπο που ζούμε. Ενώ το IoT μας παρέχει πολλά πολύτιμα οφέλη, το IoT μας εκθέτει επίσης σε πολλούς διαφορετικούς τύπους απειλών για την ασφάλεια στην καθημερινή μας ζωή. Πριν από το IoT, οι περισσότερες απειλές για την ασφάλεια σχετίζονταν με διαρροή πληροφοριών και απώλεια υπηρεσίας. Με το Διαδίκτυο των πραγμάτων, οι απειλές για την ασφάλεια έχουν συνδεθεί στενά με τις

μη εικονικές ζωές μας και μπορούν να επηρεάσουν άμεσα τους κινδύνους φυσικής ασφάλειας.

Λέξεις Κλειδιά: *«ασύρματοι αισθητήρες, σταθμός βάσης, αρχιτεκτονική WSN, πρωτόκολλα επικοινωνίας, απαιτήσεις ασφαλείας, επιθέσεις – απειλές ασφαλείας, άρνηση εξυπηρέτησης, ασφαλής δρομολόγηση, κρυπτογράφηση»*

Abstract

Wireless Sensor Networks are a network infrastructure with a large number of low-cost but also high-cost devices—nodes deployed in areas of interest. Their goal is to locate, monitor and record data from the area. The routes of the WSN collected information and management messages to the base stations through its constituent nodes. Nodes participating in wireless sensor networks are severely constrained in terms of computation, storage, and energy due to the need to control network costs and save energy to increase network operating limits. Based on these limitations, communication protocols were developed based on the network architecture of the OSI model. These protocols implement protocol stacks based on this architecture and form the basis for developing communication standards.

The limiting factors in WSNs combined with the wireless transmission medium and unattended remote operation make the network vulnerable to potential attacks. These attacks challenge network security requirements. In a specific manner attacks target network functions based on their architecture, the most important of which is the Denial of Service (DoS) attack. The developed protocol is based on a simple and energy efficient design. For this reason, mechanisms have been developed that provide assurance in terms of attack detection, routing and data collection. In addition, authentication and privacy encryption mechanisms are also being developed in this direction. However, the above mechanisms provide network security at the cost of increased network complexity and power consumption.

The era of the Internet of Things (IoT) has begun and will revolutionize the way we live. While IoT provides us with many valuable benefits, IoT also exposes us to many different types of security threats in our daily lives. Before IoT, most security threats were related to information leakage and loss of service. With the Internet of Things, security threats have become closely connected to our non-virtual lives and can directly affect physical security risks.

Key Words: *«wireless sensors, base station, WSN architecture, communication protocols, security requirements, security attacks - security threats, denial of service, secure routing, cryptography»*

Πίνακας Περιεχομένων

Λίστα Εικόνων

Λίστα Πινάκων

Εισαγωγή

Πρόλογος

Τα ασύρματα δίκτυα αισθητήρων (WSN) συνδέουν το φυσικό και ψηφιακό κόσμο συγκεντρώνοντας πληροφορίες από το επιθυμητό περιβάλλον αποτελώντας μια δικτυακή υποδομή. Αυτές οι πληροφορίες μεταφέρονται μέσω των κόμβων του δικτύου σε μια κυρίαρχη υπολογιστική μονάδα, η οποία τις επεξεργάζεται κατάλληλα, με στόχο την αποστολή τους στον τελικό χρήστη. Επίσης, χωρίς ανθρώπινη επίβλεψη, τα δίκτυα WSN έχουν τη δυνατότητα να λειτουργούν για μεγάλο χρονικό διάστημα. Χάρη σε αυτό, η ανάπτυξή τους είναι ταχύρρυθμη κυρίως σε περιβάλλοντα μη ασφαλείς πρόσβασης για τον άνθρωπο στα οποία όμως η συγκέντρωση πληροφοριών κρίνεται σημαντική.

Σκοπός

Η παρούσα εργασία έχει ως στόχο να διερευνήσει ζητήματα ασφάλειας σε δίκτυα WSN και ειδικότερα στην υλοποίησή τους στο Διαδίκτυο των Πραγμάτων. Η διερεύνηση γίνεται μέσω τις οπτικής των ιδιαιτεροτήτων ενός δικτύου WSN, ως προς τη δομή, τις δυνατότητες των συσκευών και κόμβων, των μεθόδων δρομολόγησης πληροφοριών κλπ. Συγκεκριμένα, εξετάζονται οι απειλές, οι οποίες

μπορούν να αμφισβητήσουν την ασφάλεια ενός δικτύου WSN καθώς επίσης και οι μηχανισμοί αντιμετώπισής τους, οι οποίοι είναι καίριας σημασίας ως προς την εξασφάλιση των προκαθορισμένων απαιτήσεων ασφάλειας. Τέλος, διερευνάται η εφαρμογή των μηχανισμών ασφάλειας και διαχείρισης δικτύων WSN στο Διαδίκτυο των Πραγμάτων.

Δομή εργασίας

Στο Κεφάλαιο 1 γίνεται αναφορά στα ασύρματα δίκτυα αισθητήρων (WSN), με έμφαση στη δομή τους, στην αρχιτεκτονική τους και τη συνδεσιμότητά τους με το Διαδίκτυο των Πραγμάτων.

Στο Κεφάλαιο 2 γίνεται αναφορά στο Διαδίκτυο των Πραγμάτων (Internet of Things) και πιο συγκεκριμένα στην αρχιτεκτονική του, στις τεχνολογίες δικτύωσής του, αλλά και στις βασικές τεχνολογίες και πρότυπα τα οποία χρησιμοποιούνται για τη παροχή ενός μέσου συνδεσιμότητας μεταξύ των κόμβων αισθητήρων και του Διαδικτύου των Πραγμάτων.

Στο Κεφάλαιο 3 γίνεται ανάλυση των βασικών απαιτήσεων ασφαλείας του Διαδικτύου των Πραγμάτων, με βάση τα επίπεδα της αρχιτεκτονικής του.

Στο Κεφάλαιο 4 γίνεται ανάλυση των απαιτήσεων ασφαλείας των δικτύων WSN, οι οποίες είναι δύσκολο να εφαρμοστούν λόγω των ιδιαιτεροτήτων αυτού του τύπου δικτύου. Αυτές οι ιδιαιτερότητες καθιστούν τα δίκτυα ευάλωτα σε κακόβουλες ενέργειες (επιθέσεις). Επιπλέον, οι πιθανές επιθέσεις σε δίκτυα WSN εξετάζονται από την άποψη της αρχιτεκτονικής του δικτύου και των επηρεαζόμενων λειτουργιών.

Στο Κεφάλαιο 5 παρουσιάζονται μηχανισμοί ασφαλείας για την αντιμετώπιση επιθέσεων σε δίκτυα WSN. Αρχικά, εξετάζεται το πρόβλημα της ανίχνευσης κακόβουλης συμπεριφοράς και, έπειτα, τα αντίμετρα στις επιθέσεις που αναφέρονται στο προηγούμενο κεφάλαιο. Επιπλέον, εξετάζεται το ζήτημα της ασφαλής δρομολόγησης και συνάρθρωσης δεδομένων, της κρυπτογράφησης, της αυθεντικοποίησης και της προστασίας απορρήτου.

1. Ασύρματα Δίκτυα Αισθητήρων

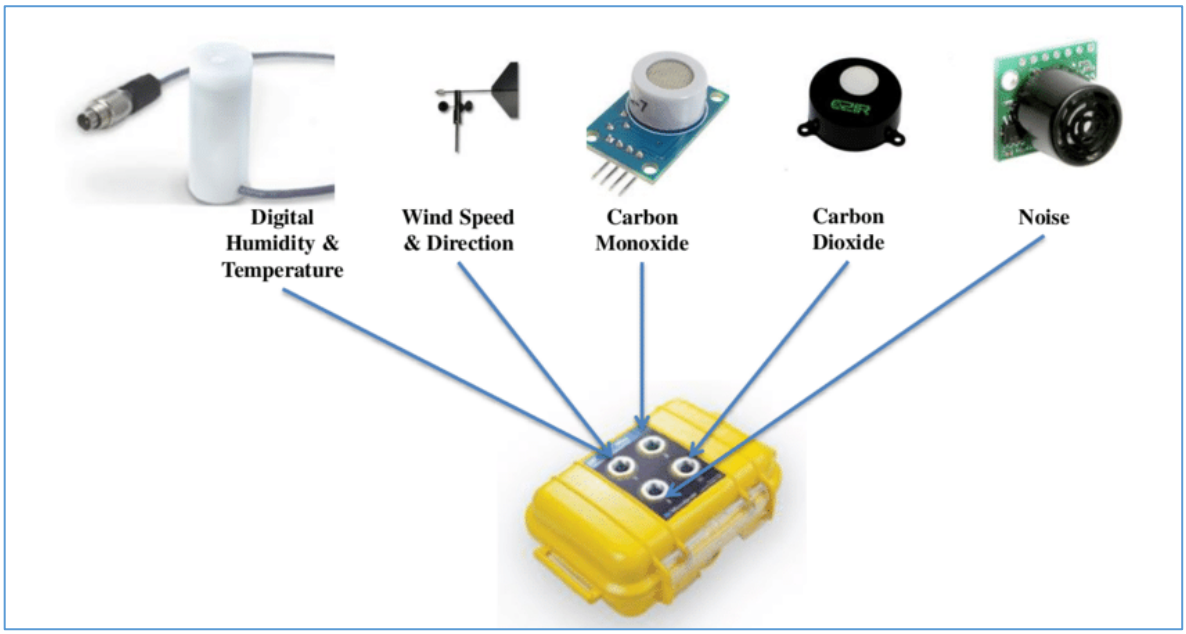
1.1 Εισαγωγή

Ασύρματο δίκτυο αισθητήρων (Wireless Sensor Network – WSN) ονομάζεται μια δικτυακή υποδομή η οποία αποτελείται από εκατοντάδες η ακόμα και χιλιάδες αισθητήριους κόμβους ικανούς ως προς την συλλογή δεδομένων μέσω εξωτερικών ερεθισμάτων, την επεξεργασία των συλλεγμένων δεδομένων, την συνεχή επικοινωνία μεταξύ τους αλλά και με το διαχειριστή του δικτύου. Ο διαχειριστής, ως παρατηρητής, έχει τη δυνατότητα να αλληλεπιδρά με το δίκτυο σύμφωνα με τις απαιτήσεις της εκάστοτε εφαρμογής. Τα WSNs μπορούν επίσης να ερμηνευτούν ως μια ειδική μορφή δικτύων ad hoc. Η ανάπτυξη των δικτύων ad hoc δεν απαιτεί προϋπάρχουσα υποδομή και πραγματοποιείται χωρίς προσχεδιασμένο τρόπο στα σημεία ενδιαφέροντος. Με αντίστοιχο τρόπο σχεδιάζονται και τα δίκτυα WSN έτσι ώστε να απαιτείται ελάχιστη, αλλά ακόμη και μηδενική, υποδομή για την ανάπτυξή τους. Αυτός ο τύπος δικτύων WSN ονομάζεται μη δομημένος (unstructured). Επίσης, ως δομημένος (structured), ορίζεται ένας ακόμη τύπος δικτύων WSN όπου οι θέσεις ανάπτυξης του δικτύου των κόμβων είναι προεπιλεγμένες.

Μεγαλύτερη ευελιξία προσδίδει η υλοποίηση μη δομημένων δικτύων WSN , ωστόσο είναι πιο επιρρεπή σε ζητήματα συντήρησης και διαχείρισης συγκριτικά με τα δομημένα. Επιπλέον, λόγο του τυχαίου τρόπου ανάπτυξης η κάλυψη της περιοχής ενδιαφέροντος δεν είναι επαρκής. Περαιτέρω διάκριση των δικτύων WSN προκύπτει σύμφωνα με το περιβάλλον ανάπτυξής τους και τα αντίστοιχα πεδία τοποθέτησης αισθητηρίων όπως στο έδαφος, υπόγεια, υποθαλάσσια, κινητά και πολυμέσων. Η αιτία της διάκρισης αυτής είναι οι διαφορετικές απαιτήσεις κάθε εφαρμογής σε θέματα λογισμικού, υλικού και πρωτοκόλλων επικοινωνίας.

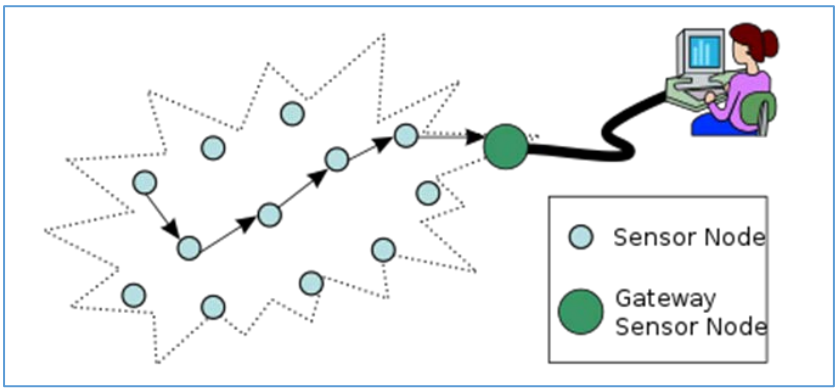
Τα δίκτυα αισθητήρων διαφέρουν σε σύγκριση με τα υπόλοιπα είδη δικτύων, καθώς οι κόμβοι λόγω των περιβαλλοντικών φθορών, περιορισμών ενέργειας, αποθηκευτικών, επικοινωνιακών και υπολογιστικών πόρων ενδέχεται να σταματήσουν να λειτουργούν. Κατά την απώλεια κόμβων ενός WSN προκαλούνται αλλαγές ως προς την τοπολογία του δικτύου. Σε εφαρμογές WSN με κύριο γνώρισμα την ικανότητα αυτόνομης φορητότητας των κόμβων (mobility), η διατήρηση της σταθερότητας και μη ευρωστίας του δικτύου γίνεται ακόμη πιο σημαντική.

Ως αποτέλεσμα, για αποδοτικότερη αξιοποίηση των λιγοστών και συχνά τροποποιημένων πόρων είναι απαραίτητη η δυνατότητα αυτό-οργάνωσης (self organizing) του δικτύου WSN. Για να εκπληρωθούν οι παραπάνω προϋποθέσεις αναπτύχθηκε η τεχνολογία ZigBee και τα πρότυπα επικοινωνίας IEE 802.15.4 καθώς και πλήθος άλλων εξειδικευμένων πρωτοκόλλων στα οποία θα γίνει εκτενής συσχέτιση στη συνέχεια. Στην Εικόνα 1.1 απεικονίζεται η συσκευή ENV-Link -Mini της MicroStrain [1] η οποία διαθέτει διαφόρων τύπων αισθητήρων για την παρακολούθηση περιβαλλοντολογικών συνθηκών, όπως η θερμοκρασία, η υγρασία, η ταχύτητα και κατεύθυνση του αέρα, ο ήχος αλλά και τα επίπεδα μονοξειδίου και διοξειδίου του άνθρακα.



Εικόνα 1.1. Συσκευή περιβαλλοντικής παρακολούθησης ENV-Link -Mini της MicroStrain [1]

Πηγή: https://www.researchgate.net/publication/303093555/figure/fig1/AS:614230990549034@1523455488981/The-Microstrain-ENVI-Link-Mini-wireless-sensor-node-and-associated-sensors.png



Εικόνα 1.2. Τυπική αρχιτεκτονική ασύρματου δικτύου αισθητήρων πολλαπλών βημάτων

Πηγή: https://commons.wikimedia.org/wiki/File:WSN.svg

1.2 Ιστορική αναδρομή

Όπως και πολλές άλλες προηγμένες τεχνολογίες, η προέλευση των WSN μπορεί να εντοπιστεί σε στρατιωτικές και βαριές βιομηχανικές εφαρμογές, πολύ απόμακρα από τις εφαρμογές WSN της ελαφριάς βιομηχανίας και των καταναλωτών που επικρατούν σήμερα.

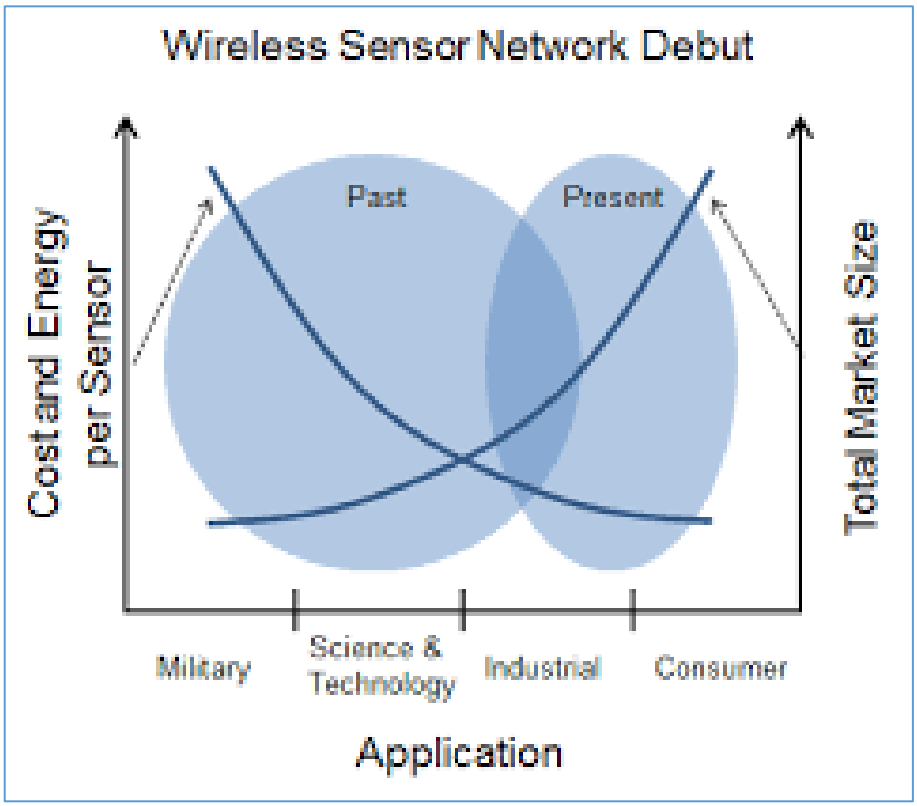
Το πρώτο ασύρματο δίκτυο που είχε οποιαδήποτε πραγματική ομοιότητα με ένα σύγχρονο WSN είναι το Sound Surveillance System (SOSUS), που αναπτύχθηκε από τον Στρατό των Ηνωμένων Πολιτειών τη δεκαετία του 1950 για τον εντοπισμό και την παρακολούθηση σοβιετικών υποβρυχίων. Αυτό το δίκτυο χρησιμοποίησε βυθισμένους ακουστικούς αισθητήρες - υδρόφωνα - που διανεμήθηκαν στον Ατλαντικό και τον Ειρηνικό ωκεανό. Οι δυνατότητες του ARPA NET (προκάτοχος του Διαδικτύου) και του πρόσφατα αναπτυγμένου τότε πρωτοκόλλου TCP/IP στο πεδίο της μάχης με τη μορφή δικτύων αισθητήρων διερευνήθηκαν τη δεκαετία του 1980, με έμφαση στην έρευνα που διεξήχθη από τις Ηνωμένες Πολιτείες και την DARPA (υπηρεσία προχωρημένων ερευνών άμυνας).

Κατά τη δεκαετία του 1990 αναπτύχθηκαν κατάλληλοι αλγόριθμοι με οδηγό το πρόγραμμα DSN, με στόχο την υλοποίηση ενός δικτύου DSN αποτελούμενου από πολύπλοκους αισθητήρες, χρησιμοποιώντας τεχνολογίες και πρότυπα δικτύου που είναι ήδη διαθέσιμα στην αγορά. Ως αποτέλεσμα προέκυψε η δημιουργία του δικτυοκεντρικού πολέμου (Network Centric Warfare – NCW) με την πλήρη ενσωμάτωση των δικτύων αισθητήρων στο πεδίο της μάχης. Ουσιαστικά, το NCW μεταφράζει την υπεροχή πληροφοριών σε δύναμη μάχης συνδέοντας αποτελεσματικά οντότητες με “γνώσεις” στον χώρο της μάχης

Αυτή η τεχνολογία ανίχνευσης εξακολουθεί να χρησιμοποιείται σήμερα, αν και εξυπηρετεί πιο ειρηνικές λειτουργίες όπως παρακολούθηση της υποθαλάσσιας άγριας ζωής και της ηφαιστειακής δραστηριότητας. Με τη γέννηση του (DSN) και την εξέλιξή του στον ακαδημαϊκό χώρο μέσω των συνεργαζόμενων πανεπιστημίων όπως το Πανεπιστήμιο Carnegie Mellon και το Massachusetts Institute of Technology Lincoln Labs, η τεχνολογία σύντομα βρήκε μια στέγη στον ακαδημαϊκό χώρο και στην επιστημονική έρευνα των πολιτών. Οι κυβερνήσεις και τα πανεπιστήμια άρχισαν τελικά να χρησιμοποιούν WSN σε εφαρμογές όπως η παρακολούθηση ποιότητας του αέρα, ανίχνευση δασικών πυρκαγιών, πρόληψη φυσικών καταστροφών, μετεωρολογικοί σταθμοί και δομική παρακολούθηση.

Ενώ η ζήτηση της αγοράς για WSN ήταν ισχυρή, η μετάβαση πέρα από αυτές τις περιορισμένες εφαρμογές αποδείχθηκε πρόκληση. Ο στρατός, η επιστήμη/τεχνολογία και οι βαριές βιομηχανικές εφαρμογές των προηγούμενων δεκαετιών βασίζονται σε ογκώδεις, ακριβούς αισθητήρες και ιδιόκτητα πρωτόκολλα δικτύωσης.

Αυτά τα WSN έθεσαν ένα πρότυπο υψηλής ποιότητας όσο αφορά τη λειτουργικότητα και την απόδοση, ενώ άλλοι παράγοντες όπως το κόστος υλικού και εγκατάστασης, η δικτύωση η κατανάλωση ενέργειας και η επεκτασιμότητα έπεσαν στο περιθώριο με αποτέλεσμα την αποστασιοποίηση της ευρείας υιοθέτησης και ανάπτυξης των WSN σε ένα ευρύτερο φάσμα εφαρμογών [2]. Ωστόσο, με την εξέλιξη στα υπολογιστικά συστήματα και στις επικοινωνίες προέκυψε μια νέα γενιά τεχνολογίας δικτύων αισθητήρων. Η ευρεία χρήση προτύπων ασύρματης δικτύωσης (οικογένεια προτύπων IEEE 802, Bluetooth, τεχνολογία ZigBee, WiMax) και η ενσωμάτωση ηλεκτρονικών συσκευών σε κλίμακα μικρομέτρου (και πρόσφατα νανομέτρου) σε συσκευές αισθητήρων (motes ή sensor boards) μείωσε το κόστος και έκανε δυνατή την ευρεία χρήση των ασύρματων δικτύων αισθητήρων.

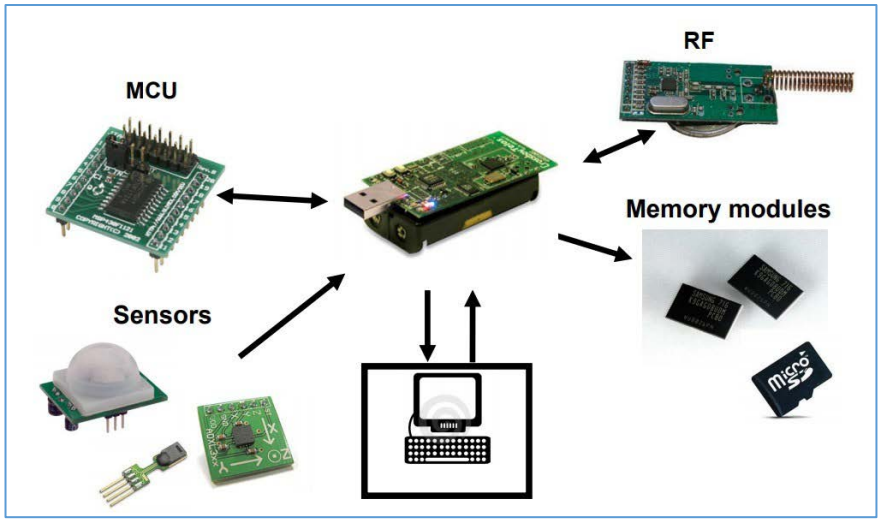


Εικόνα 1.3. Τα WSN κερδίζουν έλξη στην αγορά με μείωση του κόστους αισθητήρων

Πηγή: https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf

1.3 Δομή δικτύων WSNs

Ένα δίκτυο WSN αποτελείται από έναν αριθμό συσκευών που αναπτύσσονται σε μια περιοχή ενδιαφέροντος και τουλάχιστον μια συσκευή σταθμού βάσης (base station) ή καταβόθρα (sink) που είναι υπεύθυνη για τη συλλογή πληροφοριών από τους κόμβους αισθητήρων.



Εικόνα 1.4. Δομικά στοιχεία αισθητήριου κόμβου

Πηγή: https://polynoe.lib.uniwa.gr/xmlui/bitstream/handle/11400/513/Kyriakakis_18040.pdf?sequence=1&isAllowed=y

1.3.1 Κόμβοι δικτύου WSN

Η τεχνολογική πρόοδος μικροηλεκτρικών συστημάτων MEMS (Micro Electro Machines Systems) επίσπευσε την εξέλιξη των έξυπνων αισθητήρων (smart sensors). Οι αισθητήρες αυτοί είναι διατάξεις με δυνατότητα ασύρματης δικτύωσης, χαμηλού κόστους και μεγέθους με συγκρατημένες επεξεργαστικές, υπολογιστικές και αποθηκευτικές ικανότητες.

Οι κόμβοι εξαιτίας του μικρού μεγέθους τους μπορούν να αξιοποιηθούν για τη παρατήρηση φαινομένων σε μεγάλη εγγύτητα, καθώς η αυτονομία που διαθέτουν επιτρέπει την ανάπτυξή τους σε περιοχές δύσβατες χωρίς υποδομή. Έχουν τη δυνατότητα ενσωμάτωσης πολλαπλών αισθητήρων ικανών προς μέτρηση ποικίλων διαφορετικών παραμέτρων, όπως ηλεκτρικά σήματα (ένταση ρεύματος, τάση, φορτίο), μαγνητικά σήματα (μαγνητική ροή, μαγνητικό πεδίο), θερμικά σήματα (θερμοκρασία, θερμότητα, ροή θερμότητας), μηχανικά σήματα (ταχύτητα, επιτάχυνση, κίνηση, πίεση, δύναμη), ακτινοβολίας (ενέργεια, ένταση, ισχύ) και χημικά σήματα (σύνθεση, συγκέντρωση υλικών).

Οι κόμβοι χωρίζονται σε γενικούς κόμβους πολλαπλών χρήσεων (generic-multi purpose), κόμβους πύλης (gateway) και κόμβους αναμετάδοσης (relay). Η διαφορά έγκειται στις υπολογιστικές και επικοινωνιακές δυνατότητες που τα διαφοροποιούν. Ο κόμβος πύλης είναι υπεύθυνος για τη μετάδοση αυτών των δεδομένων στο σταθμό βάσης, όπου υφίσταται επεξεργασία και ελέγχει το WSN.

1.3.2 Σταθμός βάσης

Ένας σταθμός βάσης είναι το βασικό στοιχείο ενός WSN, το οποίο είναι μια οντότητα με βελτιωμένες δυνατότητες υπολογισμού και αποθήκευσης που μπορεί να λειτουργήσει ως σημείο πρόσβασης (human interface) για το διαχειριστή εφαρμογής ή ένας κόμβος ενός άλλου δικτύου - μια πύλη (gateway). Οι κόμβοι που ανήκουν στο δίκτυο WSN επικοινωνούν με το σταθμό βάσης μέσω άλλων κόμβων ή απευθείας σύμφωνα με τη διάταξή τους στο πεδίο. Τα δεδομένα υποβάλλονται σε τοπική επεξεργασία πριν σταλούν στον σταθμό βάσης. Αυτή η επεξεργασία μπορεί να περιλαμβάνει τεχνικές συμπίεσης, κρυπτογράφησης και συλλογής πληροφοριών. Τα δεδομένα πρέπει να είναι σωστά καταχωρημένα και διευθυνσιοδοτημένα (timestamp-position), ώστε να μπορούν να βρεθούν όταν υποβάλλεται ένα ερώτημα. Επιπλέον, οι σταθμοί βάσης μπορούν να στείλουν στοχευμένα ερωτήματα σε ομάδες κόμβων που βρίσκονται πιο κοντά σε μια περιοχή ενδιαφέροντος καθώς οι κόμβοι έχουν τη δυνατότητα εντοπισμού της θέσης τους με τη χρήση GPS, διαφορετικά η θέση τους είναι εξαρχής γνωστή σε περίπτωση προκαθορισμένης ανάπτυξης του δικτύου.

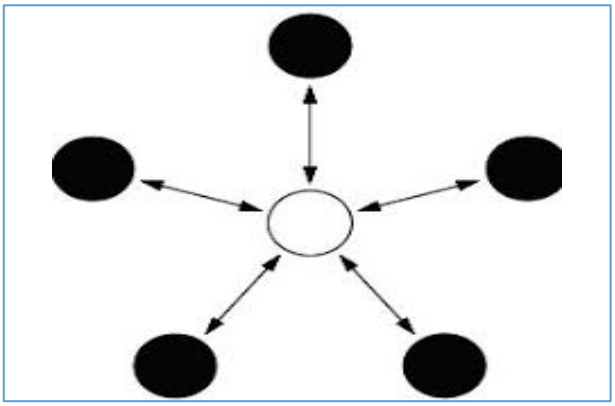
Η διεπαφή μεταξύ μακρινών κόμβων και του σταθμού βάσης αποφεύγεται λόγω των περιορισμών εμβέλειας των κόμβων αλλά και για εξοικονόμηση ενέργειας. Οι τρόποι δρομολόγησης των δεδομένων χωρίζονται σε δύο κατηγορίες, με σκοπό την ελαχιστοποίηση κατανάλωσης ενέργειας, όπως: α) δρομολόγηση δεδομένων με πολλαπλά άλματα - αναπηδήσεις (multi-hop) και β) δρομολόγηση δεδομένων σε ομάδες κόμβων (clusters). Επίσης είτε με πολλαπλά άλματα, είτε χωρίς, η δρομολόγηση με βάση την ομαδοποίηση των κόμβων μπορεί να υλοποιηθεί.

1.4 Βασικές τοπολογίες δικτύων WSNs

Ένα ασύρματο δίκτυο αισθητήρων είναι ένα δίκτυο κόμβων που ανταλλάσσουν μηνύματα ασύρματα. Υπάρχουν πολλές διαφορετικές τοπολογίες που μπορεί να ακολουθήσει ένα ασύρματο δίκτυο αισθητήρων και η καθεμία έχει τα δικά της πλεονεκτήματα και μειονεκτήματα.

1.4.1 Τοπολογία αστέρα (Star)

Ένα δίκτυο «αστέρα» (Star topology) [3] είναι ένας τύπος τοπολογίας επικοινωνιών στην οποία ένας μεμονωμένος σταθμός βάσης μπορεί να στέλνει και/ή να λαμβάνει μηνύματα σε έναν αριθμό απομακρυσμένων κόμβων. Οι απομακρυσμένοι κόμβοι δεν επιτρέπεται να στέλνουν μηνύματα ο ένας στον άλλο. Το πλεονέκτημα αυτού του τύπου δικτύου για ασύρματα δίκτυα αισθητήρων περιλαμβάνει την απλότητα διαχείρισης και τη δυνατότητα διατήρησης της κατανάλωσης ενέργειας του απομακρυσμένου κόμβου στο ελάχιστο. Αυτό το δίκτυο επιτρέπει επικοινωνίες χαμηλής καθυστέρησης μεταξύ του απομακρυσμένου κόμβου και του σταθμού βάσης. Το μειονέκτημα αυτού του δικτύου είναι ότι ο σταθμός βάσης πρέπει να βρίσκεται εντός του εύρους ραδιομετάδοσης όλων των μεμονωμένων κόμβων και δεν είναι τόσο ισχυρός όσο άλλα δίκτυα λόγω της εξάρτησής του από έναν μόνο κόμβο για τη διαχείριση του δικτύου.



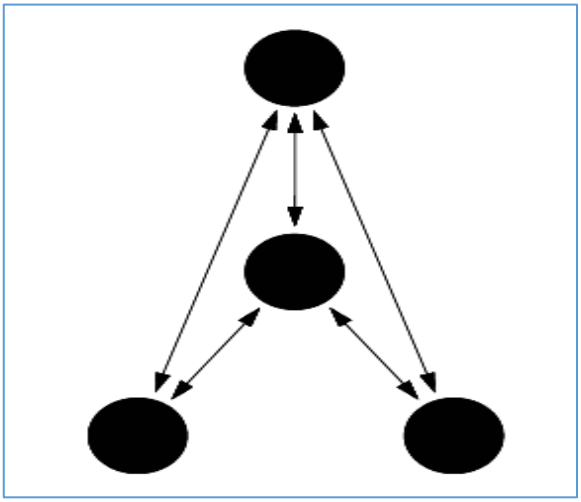
Εικόνα 1.5. Μια τοπολογία δικτύου Star

Πηγή: https://www.researchgate.net/figure/A-Star-network-topology_fig2_272832872

1.4.2 Τοπολογία πλέγματος (Mesh)

Ένα δίκτυο πλέγματος (Mesh topology) [3] επιτρέπει τη μετάδοση δεδομένων μεταξύ ενός κόμβου και ενός άλλου κόμβου στο δίκτυο που βρίσκεται εντός του εύρους ραδιομετάδοσης του. Αυτό επιτρέπει την επικοινωνία πολλαπλού άλματος, η οποία είναι χρήσιμη εάν ένας κόμβος θέλει να στείλει ένα μήνυμα σε έναν άλλο κόμβο που βρίσκεται εκτός εμβέλειας ραδιοεπικοινωνιών. Αυτή η τοπολογία δικτύου έχει το πλεονέκτημα του πλεονασμού και της επεκτασιμότητας. Εάν ένας μεμονωμένος κόμβος αποτύχει, ένας απομακρυσμένος κόμβος μπορεί ακόμα να επικοινωνήσει με οποιονδήποτε άλλο κόμβο στην περιοχή του, ο οποίος με τη σειρά του μπορεί να προωθήσει το μήνυμα στην επιθυμητή θέση. Επιπλέον, το εύρος του δικτύου δεν περιορίζεται απαραίτητα από το εύρος μεταξύ μεμονωμένων κόμβων. Μπορεί απλά να επεκταθεί προσθέτοντας

περισσότερους κόμβους στο σύστημα. Το μειονέκτημα αυτού του τύπου δικτύου είναι ότι η κατανάλωση ενέργειας για τους κόμβους που υλοποιούν επικοινωνίες πολλαπλών αλμάτων είναι γενικά υψηλότερη από ό,τι για τους κόμβους που δεν το υλοποιούν, περιορίζοντας συχνά τη διάρκεια ζωής της μπαταρίας. Επιπλέον, καθώς αυξάνεται ο αριθμός των μεταπηδήσεων επικοινωνίας σε έναν προορισμό, αυξάνεται και ο χρόνος παράδοσης του μηνύματος, ειδικά εάν απαιτείται λειτουργία χαμηλής ισχύος των κόμβων.

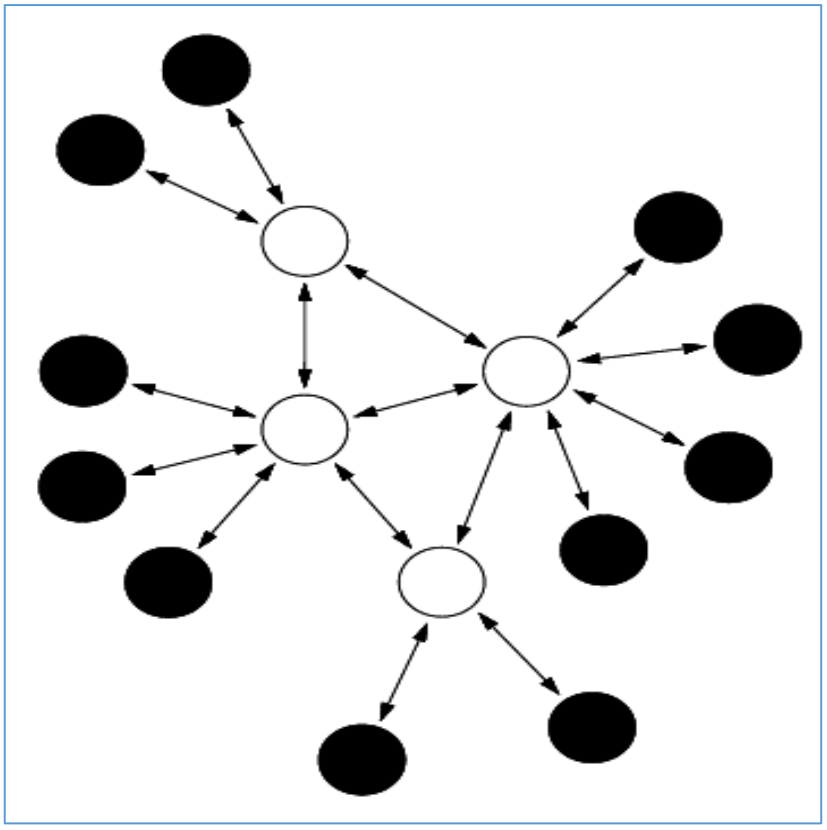


Εικόνα 1.6. Μια τοπολογία δικτύου Mesh

Πηγή: https://www.intechopen.com/media/chapter/38793/media/image3.png

1.4.3 Υβριδική τοπολογία (Star – Mesh)

Ένας υβριδικός μετασχηματισμός μεταξύ των τοπολογιών δικτύου star και mesh παρέχει ένα ισχυρό και ευέλικτο δίκτυο επικοινωνιών, διατηρώντας παράλληλα τη δυνατότητα να διατηρείται η κατανάλωση ενέργειας ασύρματου κόμβου αισθητήρα στο ελάχιστο [3]. Σε αυτήν την τοπολογία δικτύου, οι κόμβοι αισθητήρων με τη χαμηλότερη απόδοση δεν ενεργοποιούνται με την προώθηση μηνυμάτων. Αυτό επιτρέπει τη διατήρηση της ελάχιστης κατανάλωσης ενέργειας. Ωστόσο, άλλοι κόμβοι στο δίκτυο είναι ικανοί πολλαπλών βημάτων, γεγονός που τους επιτρέπει να προωθούν μηνύματα από τους κόμβους χαμηλής απόδοσης σε άλλους κόμβους του δικτύου. Γενικά, οι κόμβοι με την ικανότητα πολλαπλών βημάτων έχουν υψηλότερη ισχύ και, εάν είναι δυνατόν, συχνά συνδέονται στη γραμμή ηλεκτρικού δικτύου. Αυτή είναι η τοπολογία που εφαρμόζεται από το ανερχόμενο πρότυπο δικτύωσης πλέγματος γνωστό ως ZigBee.



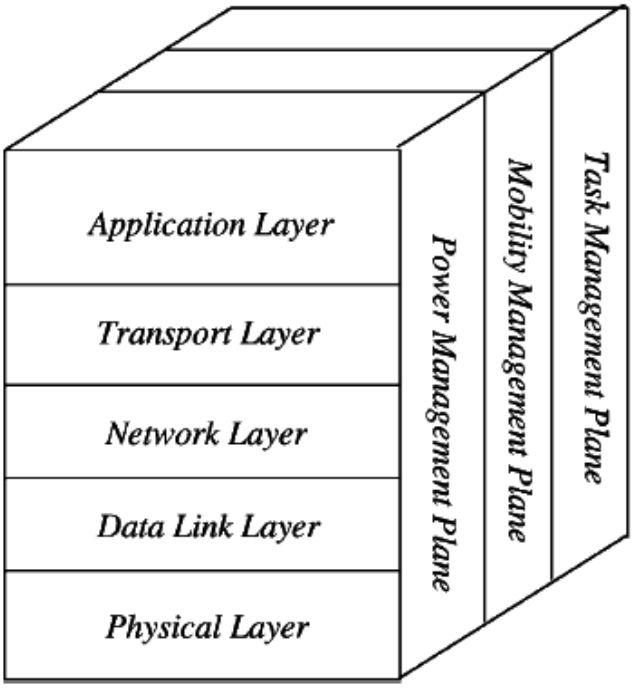
Εικόνα 1.7. Μια τοπολογία δικτύου Hybrid Star – Mesh

Πηγή: https://www.intechopen.com/media/chapter/38793/media/image4.png

1.5 Αρχιτεκτονική – Πρότυπα Wireless Sensor Networks

Τα ασύρματα δίκτυα αισθητήρων ακολουθούν συνήθως το μοντέλο αναφοράς OSI (Open Systems Interconnection), το οποίο είναι ένα μοντέλο επτά επιπέδων (φυσικό, ζεύξης και μετάδοσης δεδομένων, δικτύου, μεταφοράς, συνδιάλεξης, παρουσίασης και εφαρμογής). Το μοντέλο αυτό αναπτύχθηκε σύμφωνα με το Διεθνές Οργανισμό Τυποποίησης (ISO - International Standards Organization) με σκοπό τη διεθνή τυποποίηση των πρωτοκόλλων που χρησιμοποιούνται στο επίπεδο σχεδιασμού δικτύων. Τα αλληλένδετα αυτά επίπεδα, συμβάλουν στην υλοποίηση τις κατακόρυφης στοίβας επιπέδων όπου κάθε επίπεδο επωφελείται από τις λειτουργίες του επιπέδου κάτω από αυτό καθώς και παρέχοντας λειτουργικότητα στο επίπεδο πάνω από αυτό.

Σε ένα WSN, τα επίπεδα παρουσίασης και επικοινωνίας του μοντέλου OSI δεν υλοποιούνται, αλλά το υλοποιούμενο μοντέλο περιλαμβάνει τα υπόλοιπα τέσσερα επίπεδα του μοντέλου σχεδίασης καθώς και τρία διασταυρούμενα επίπεδα (cross layers/planes), όπως απεικονίζονται στην Εικόνα 1.8.



Εικόνα 1.8. Μοντέλο αρχιτεκτονικής WSN

Πηγή: https://www.elprocus.com/architecture-of-wireless-sensor-network-and-applications/

Ο σχεδιασμός των διασταυρούμενων επιπέδων του δικτύου αισθητήρων στοχεύει στη διαχείριση του δικτύου έτσι ώστε οι κόμβοι να συνεργάζονται με τρόπο που να μεγιστοποιεί την αποτελεσματικότητα και το χρόνο λειτουργίας του δικτύου. Τα τρία διασταυρούμενα επίπεδα (cross layers / planes) αποτελούνται από τα επίπεδα διαχείρισης ενέργειας (power management plane), φορητότητας (mobility management plane) και λειτουργιών (task management plane). Αυτά τα επίπεδα χρησιμοποιούνται για τη βέλτιστη συνεργασία των αισθητήρων με στόχο την αύξηση της πλήρης απόδοσης του δικτύου [4].

Τα πρωτόκολλα επικοινωνίας που χρησιμοποιούνται σε ένα ασύρματο δίκτυο αισθητήρων εξαρτώνται από το επίπεδο του μοντέλου WSN και αποτελούν τη στοίβα πρωτοκόλλων του δικτύου (protocol stack). Είναι σημαντικό η στοίβα πρωτοκόλλων να είναι ενεργειακά αποδοτική και να μπορεί να υποστηρίξει τη συνεργασία μεγάλου αριθμού κόμβων.

Υπάρχουν 2 τύποι αρχιτεκτονικών ασύρματων αισθητήρων: Επίπεδη αρχιτεκτονική δικτύου (Layered Network Architecture) και αρχιτεκτονική συμπλέγματος (Clustered Network Architecture). Αυτά εξηγούνται ως εξής παρακάτω.

1.5.1 Επίπεδη αρχιτεκτονική δικτύου - Layered Network Architecture

Αυτό το είδος δικτύου χρησιμοποιεί εκατοντάδες κόμβους αισθητήρων καθώς και έναν σταθμό βάσης. Εδώ η διάταξη των κόμβων δικτύου μπορεί να γίνει σε ομόκεντρα στρώματα. Αποτελείται από πέντε στρώματα καθώς και τρία διασταυρούμενα επίπεδα που περιλαμβάνουν τα ακόλουθα.

1.5.1.1 Επίπεδο εφαρμογής (application layer)

Το επίπεδο εφαρμογής διαχειρίζεται το λογισμικό της εκάστοτε εφαρμογής, το οποίο βοηθά στη διαμόρφωση των πακέτων δεδομένων (messages) σε σαφή μορφή για τον διαχειριστή, ανάλογα με τις απαιτήσεις της εφαρμογής (π.χ. ιατρικής, περιβαλλοντικής, στρατιωτικής κλπ).

Ο κύριος στόχος αυτού του πρωτοκόλλου επιπέδου εφαρμογής είναι να ορίσει πώς οι εντολές ελέγχου αποστέλλονται από το σταθμό βάσης στους κόμβους δικτύου (downlink), και ο δευτερεύων στόχος είναι να ορίσει πώς τα δεδομένα αποστέλλονται πίσω από τους κόμβους του δικτύου στον σταθμό βάσης. Η εφαρμογή καθορίζει τις λεπτομέρειες του τρόπου με τον οποίο τα δύο συστήματα τερματισμού - σταθμοί βάσης και κόμβοι - ανταλλάσσουν μηνύματα κατά τις διαδικασίες της. Πρέπει να καθοριστούν οι τύποι των μηνυμάτων που θα ανταλλάσσονται, η σύνταξή τους και ο χρόνος κατά τον οποίο μια διεργασία λαμβάνει ή στέλνει μηνύματα.

1.5.1.2 Επίπεδο μεταφοράς (transport layer)

Το επίπεδο μεταφοράς εξασφαλίζει αξιόπιστη επικοινωνία μεταξύ του επιπέδου εφαρμογής και του δικτύου, ανεξάρτητα από την αξιοπιστία του υποκείμενου δικτύου. Αυτό προκύπτει διαιρώντας τα μηνύματα από το επίπεδο εφαρμογής σε μικρότερα τμήματα δεδομένων (segments) και προσθέτοντας κεφαλίδες επιπέδου μεταφοράς σε αυτά. Στη συνέχεια, το επίπεδο μεταφοράς στέλνει αυτά τα τμήματα δεδομένων στο δίκτυο. Όταν το δίκτυο λαμβάνει ένα τμήμα δεδομένων, εξάγει τα δεδομένα από το δεδομενόγραμμα και τα αποστέλλει στο επίπεδο μεταφοράς. Με τη σειρά του, το επίπεδο μεταφοράς επεξεργάζεται τα δεδομένα και τα μεταβιβάζει στο επίπεδο εφαρμογής. Το υλικό και το λογισμικό που συνθέτουν τις λειτουργίες του επιπέδου μεταφοράς αποτελούν μέρος των οντοτήτων μεταφοράς (transport entities).

Τα πρωτόκολλα επιπέδου μεταφοράς είναι απαραίτητα για αξιόπιστες μεταφορές δεδομένων σε διαφορετικές εφαρμογές. Ακόμα κι αν το υποκείμενο πρωτόκολλο δικτύου δεν είναι αξιόπιστο, αυτά τα πρωτόκολλα διασφαλίζουν ότι τα δεδομένα είναι αξιόπιστα.

Η επίτευξη αξιοπιστίας διασφαλίζει ότι τα μεταδιδόμενα bit δεδομένων δεν θα καταστραφούν, θα χαθούν και θα παραδοθούν όλα με τη σειρά με την οποία στάλθηκαν. Η απώλεια πακέτων μπορεί να προκληθεί από μια ποικιλία αστοχιών δικτύου, οι οποίες μπορεί να είναι αναξιόπιστη επικοινωνία κόμβου, συμφόρηση ή σύγκρουση πακέτων, εξάντληση της χωρητικότητας αποθήκευσης κόμβου και αποτυχίες κόμβου. Οποιαδήποτε απώλεια πακέτων έχει αρνητικό αντίκτυπο στην ενεργειακή απόδοση και την Ποιότητα Υπηρεσιών (QoS).

1.5.1.3 Επίπεδο δικτύου (network layer)

Το επίπεδο δικτύου είναι υπεύθυνο για τη δρομολόγηση των πακέτων δεδομένων και οι κύριες προκλήσεις είναι η εξοικονόμηση ενέργειας, η υπέρβαση των δυσκολιών που προκαλούνται από τους περιορισμούς της μνήμης των κόμβων και η διασφάλιση της αυτοοργάνωσης των κόμβων. Κατά την αποστολή δεδομένων, το επίπεδο δικτύου λαμβάνει κομμάτια δεδομένων από το επίπεδο μεταφοράς, συγκεντρώνει κάθε κομμάτι σε ένα συγκεντρωτικό δεδομενόγραμμα και το στέλνει στον πλησιέστερο δρομολογητή. Κατά τη λήψη, το επίπεδο δικτύου λαμβάνει δεδομενογράμματα από τον πλησιέστερο δρομολογητή, εξάγει τα τμήματα δεδομένων και τα διαβιβάζει στο επίπεδο μεταφοράς.

Τα πρωτόκολλα επικοινωνίας του επιπέδου δικτύου παρέχουν αξιόπιστες διαδρομές δρομολόγησης για πακέτα, όπως ορίζονται από κάθε πρωτόκολλο. Επιπλέον, διαφέρουν από τα κλασικά πρωτόκολλα δρομολόγησης στο ότι οι κόμβοι στα WSN δεν διαθέτουν διευθύνσεις IP (Internet Protocol) και επομένως δεν μπορούν να χρησιμοποιήσουν πρωτόκολλα που βασίζονται σε IP.

Ο σχεδιασμός των πρωτοκόλλων δρομολόγησης για ένα WSN θα πρέπει να επικεντρωθεί στη διαχείριση της επικοινωνίας πολλών κόμβων και στη διάδοση δεδομένων από αυτούς στο σταθμό βάσης, λαμβάνοντας υπόψη τους περιορισμούς του δικτύου (ενέργεια, μνήμη, εύρος ζώνης και υπολογιστικές δυνατότητες των κόμβων). Με αυτόν τον τρόπο, παρατείνεται η διάρκεια ζωής του δικτύου.

1.5.1.4 Επίπεδο ζεύξης (data link layer)

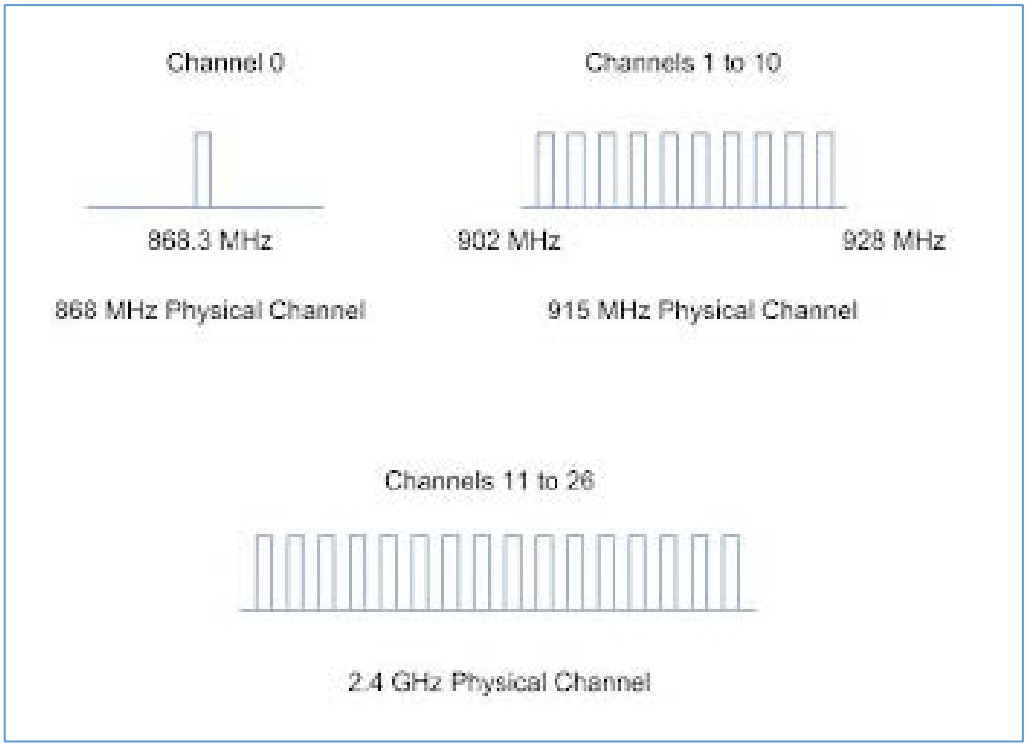
Στο αυτό το επίπεδο, ο κόμβος δεδομένων αποστολής ενθυλακώνει το δεδομενόγραμμα σε ένα πλαίσιο επιπέδου ζεύξης και ο κόμβος λήψης εξάγει το αντίστοιχο δεδομενόγραμμα από το πλαίσιο που έλαβε. Κάθε πλαίσιο περιλαμβάνει το επίμετρο (trailer) και την επικεφαλίδα, τα οποία προστίθενται από το επίπεδο ζεύξης, και το ωφέλιμο φορτίο, που είναι το δεδομενόγραμμα του επιπέδου δικτύου.

Το πρωτόκολλο επιπέδου χρησιμοποιείται κυρίως για λειτουργίες όπως η ανίχνευση πλαισίων δεδομένων και η διασφάλιση της αξιοπιστίας της υπηρεσίας. Είναι πιθανό να ανιχνευθούν σφάλματα λόγω παρεμβολών συν-καναλιού (co-channel interference) στο επίπεδο MAC (Media Access Control) ή δυσμενών παραγόντων του περιβάλλοντος διάδοσης, όπως η διάδοση πολλαπλών διαδρομών, η απώλεια και η σκίαση. Προκειμένου να επιλυθούν οι δυσκολίες που θέτουν σε κίνδυνο την αξιοπιστία του δικτύου, το πρωτόκολλο MAC έχει σχεδιαστεί για να λύνει το πρόβλημα παρεμβολών μεταξύ καναλιών όπως επίσης, έχουν σχεδιαστεί και οι τεχνολογίες FEC (Forword Error Correction) [5] και ARQ (Automatic Repeat Request) [5], οι οποίες μειώνουν τις αρνητικές επιπτώσεις του περιβάλλοντος διάδοσης. Σε πολλά πρότυπα, το επίπεδο διασύνδεσης χωρίζεται σε δύο υποστρώματα, το επίπεδο Λογικού Ελέγχου Σύνδεσης (Logical Link Control - LLC) και το επίπεδο MAC. Το επίπεδο MAC είναι υπεύθυνο για την πρόσβαση στο μέσο μετάδοσης, ενώ το επίπεδο LLC διαχειρίζεται την πολυπλεξία και την αποπολυπλεξία των δεδομενογραμμάτων του επιπέδου δικτύου.

1.5.1.5 Physical Layer – Φυσικό επίπεδο

Το φυσικό επίπεδο καθορίζει τη συχνότητα της εφαρμογής, τον εντοπισμό και την επεξεργασία του σήματος (διαμόρφωση, κωδικοποίηση δεδομένων, κρυπτογράφηση). Ορίζει επίσης μια διεπαφή για τη μετάδοση ψηφιακών ακολουθιών σε φυσικά μέσα. Το πρότυπο IEEE 802.15.4 χρησιμοποιείται ευρέως σε ασύρματα δίκτυα αισθητήρων, με στόχο το χαμηλό κόστος, την πολυπλοκότητα και τη χαμηλή κατανάλωση δικτύου. Αναπτύχθηκε από το IEEE (Institute of Electrical and Electronics Engineers) για την παροχή υπηρεσιών φυσικού επιπέδου και επιπέδου MAC σε δίκτυα μικρής απόστασης που υποστηρίζουν χαμηλούς ρυθμούς μετάδοσης. Αυτό το πρότυπο είναι η βάση του προτύπου ZigBee, το οποίο παρέχει υπηρεσίες στο ανώτερο επίπεδο της αρχιτεκτονικής δικτύου WSN.

Το πρωτόκολλο 802.15.4 λειτουργεί σε τρείς ζώνες συχνοτήτων α) 868 MHz (ρυθμός δεδομένων 20 kbps), β) 915 MHz (ρυθμός δεδομένων 40 kbps) και γ) 2,4 GHz (ρυθμός μετάδοσης δεδομένων 250 kbps). Αυτό φαίνεται στην Εικόνα 1.9. Με ρυθμό μετάδοσης δεδομένων μικρότερο από 250 kbps, υποστηρίζει έως και 254 κόμβους σε εμβέλεια 75 μέτρων. Το δίκτυο που χρησιμοποιεί αυτό το πρωτόκολλο μπορεί να “επιβιώσει” από 6 μήνες έως 2 χρόνια με δύο μπαταρίες AA.



Εικόνα 1.9. Κανάλια πρωτοκόλλου 802.15.4 στο φυσικό επίπεδο.

Πηγή: http://sensors-and-networks.blogspot.com/2011/08/physical-layer-for-wireless-sensor.html

1.5.1.6 Διασταυρούμενα επίπεδα (cross layers)

Προκειμένου να λειτουργεί πιο αποτελεσματικά και να παραταθεί ο κύκλος ζωής του δικτύου, η συνεργασία μεταξύ των κόμβων είναι απαραίτητη. Τα διασταυρούμενα επίπεδα λειτουργούν σε συντονισμό με τα επίπεδα σχεδίασης και αποτρέπουν τους κόμβους να λειτουργούν ατομικά.

Το επίπεδο διαχείρισης ισχύος (power management plane) διαχειρίζεται την ενέργεια των κόμβων του δικτύου. Για παράδειγμα, εάν ένας κόμβος έχει ανεπαρκή υπολειπόμενη ενέργεια, δεν θα μπορεί να συμμετέχει στη δρομολόγηση πακέτων στο σταθμό βάσης. Με αυτόν τον τρόπο εξοικονομείται ενέργεια ώστε να μπορεί να αφιερωθεί στη λειτουργία του ως πηγή πληροφοριών.

Το επίπεδο διαχείρισης φορητότητας (mobility management plane) διατηρεί ένα αρχείο της κίνησης των κόμβων και της θέσης τους σε σχέση με το σταθμό βάσης. Αυτά τα δεδομένα είναι χρήσιμα στη διαχείριση της ενεργειακής κατάστασης των κόμβων.

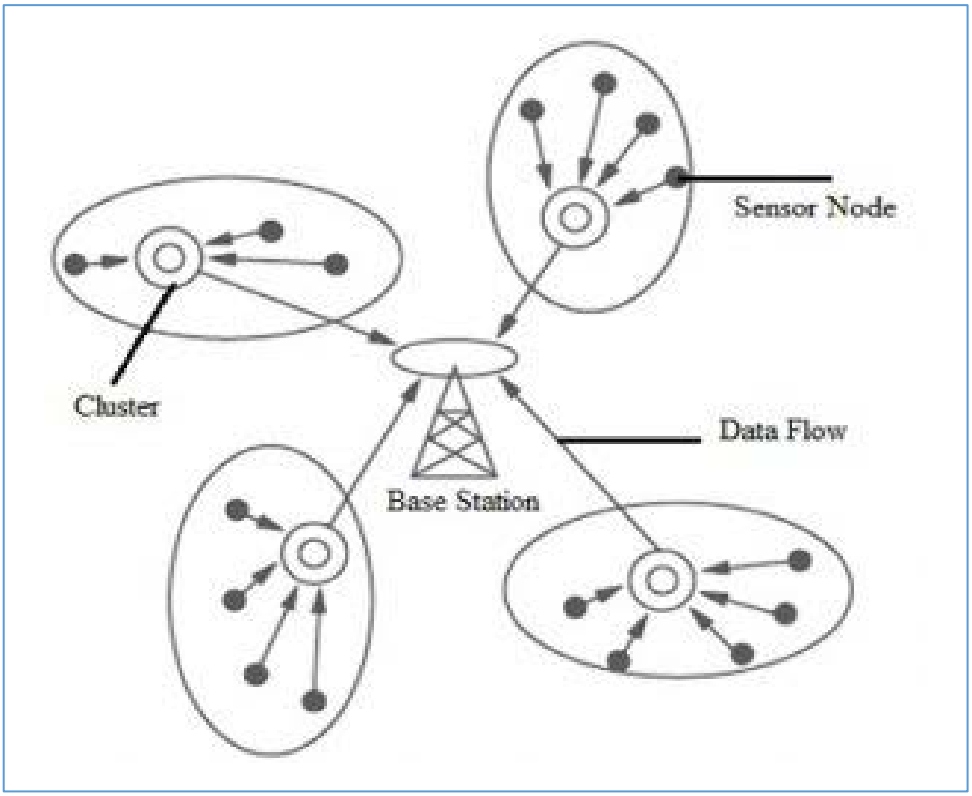
Τέλος, το επίπεδο διαχείρισης εργασιών (task management plane) ελέγχει και διαχειρίζεται κατάλληλα τις λειτουργίες των κόμβων (δρομολόγηση ή παρακολούθηση του κατάλληλου περιβάλλοντος) με βάση τα αποθέματα ισχύος τους.

1.5.2 Clustered Network Architecture

Με την χρήση αυτής της αρχιτεκτονικής , οι κόμβοι αισθητήρων ομαδοποιούνται αυτόνομα σε ομάδες που ονομάζονται συμπλέγματα. Βασίζεται στο Πρωτόκολλο Leach που χρησιμοποιεί συμπλέγματα. (Low Energy Adaptive Clustering Hierarchy – Ιεραρχία Προσαρμοστικής Ομαδοποίησης Χαμηλής Ενέργειας) [6]

Ιδιότητες του Πρωτοκόλλου Leach:

- Είναι μια αρχιτεκτονική ομαδοποίησης ιεραρχίας 2 επιπέδων.
- Είναι ένας κατανεμημένος αλγόριθμος για την οργάνωση των κόμβων αισθητήρων σε ομάδες που ονομάζονται συστάδες.
- Οι κόμβοι κεφαλής συμπλέγματος σε κάθε ένα από τα αυτόνομα σχηματισμένα συμπλέγματα δημιουργούν τα χρονοδιαγράμματα πολλαπλής πρόσβασης διαίρεσης χρόνου (TDMA).
- Χρησιμοποιεί τη μέθοδο Data Fusion, όπου τα συμπλέγματα που σχηματίζονται μοιράζονται τις πληροφορίες που έχουν συλλέξει στο σταθμό βάσης, επομένως το καθιστά ενεργειακά αποδοτικό.



Εικόνα 1.10. Clustered Network Architecture

Πηγή: https://www.geeksforgeeks.org/sensor-network-architecture/

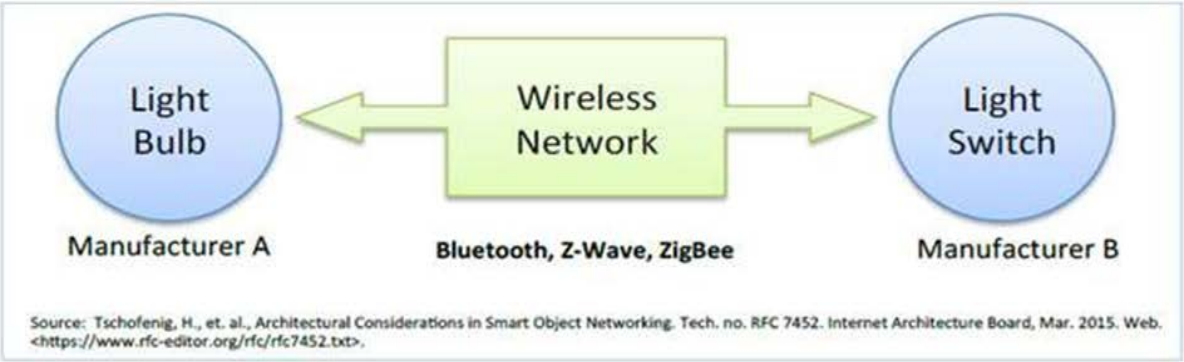
1.6 Συνδεσιμότητα και Διαδίκτυο των Πραγμάτων

Καθώς αναπτύσσεται το Διαδίκτυο των Πραγμάτων (Internet of Things) εξελίσσονται και οι ποικιλίες υπηρεσιών.

1.6.1 Συσκευή προς Συσκευή (Device-to-Device)

Στις επικοινωνίες συσκευής με συσκευή (D2D), οι συσκευές επικοινωνούν μεταξύ τους αυτόνομα χωρίς κεντρικό έλεγχο και συνεργάζονται για τη συλλογή, κοινή χρήση και προώθηση πληροφοριών σε δίκτυα μικρής εμβέλειας, όπως ασύρματα δίκτυα αισθητήρων (WSN), LTEDirect, Wi-Fi Direct ή Bluetooth Low Energy (BLE). Οι επικοινωνίες και η δικτύωση D2D είναι μια πολλά υποσχόμενη ιδέα για τη βελτίωση της χρήσης πόρων και τη βελτίωση της ποιότητας εμπειρίας χρήστη (QoE). [7] Επίσης, έχουν τη δυνατότητα να επεκτείνουν την κάλυψη του δικτύου και να διευκολύνουν νέους τύπους ασύρματων υπηρεσιών ομότιμων δικτύων (peer-to-peer), ενώ ταυτόχρονα αυξάνουν την ενεργειακή απόδοση των επικοινωνιών.

Αυτό το μοντέλο επικοινωνίας χρησιμοποιείται συνήθως σε εφαρμογές όπως τα συστήματα οικιακού αυτοματισμού, τα οποία συνήθως χρησιμοποιούν μικρά πακέτα πληροφοριών για την επικοινωνία μεταξύ συσκευών με σχετικά χαμηλές απαιτήσεις ρυθμού δεδομένων. Οι οικιακές συσκευές IoT, όπως λαμπτήρες, διακόπτες φώτων, θερμοστάτες και κλειδαριές θυρών συνήθως στέλνουν μικρές ποσότητες πληροφοριών μεταξύ τους (π.χ. μήνυμα κατάστασης κλειδαριάς πόρτας ή φως κατά την εντολή) σε ένα σενάριο οικιακού αυτοματισμού. Από την πλευρά του χρήστη, αυτό σημαίνει συχνά ότι τα υποκείμενα πρωτόκολλα επικοινωνίας μεταξύ συσκευών είναι ασύμβατα, αναγκάζοντας τον χρήστη να επιλέξει μια οικογένεια συσκευών που χρησιμοποιούν ένα κοινό πρωτόκολλο.



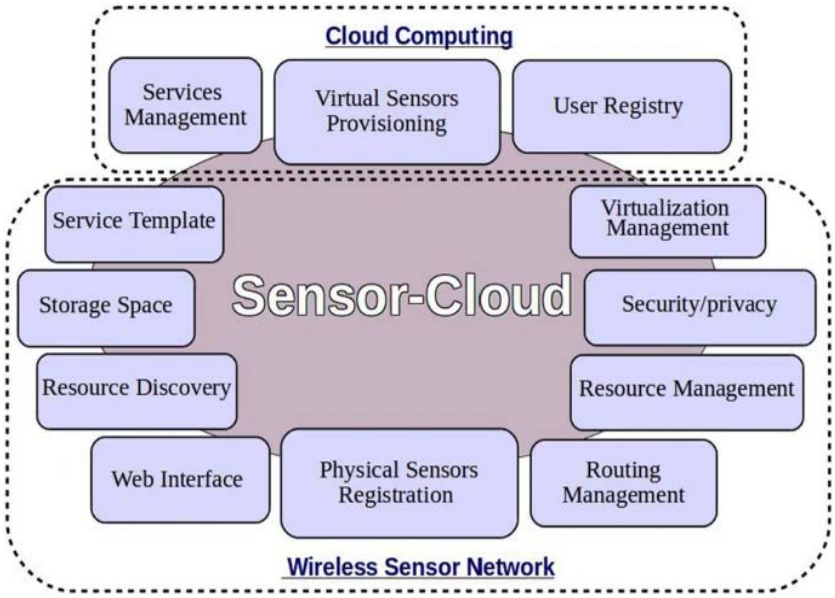
Εικόνα 1.11. Παραδείγματα διαδραστικών υπηρεσιών IoT από συσκευή σε συσκευή.

1.6.2 Συσκευή προς Υπολογιστικό Νέφος (Device-to-Cloud)

Με τις αλλαγές γενεών στα WSN που βασίζονται στο IoT, τα συνδεδεμένα μηχανήματα και οι αισθητήρες μπορούν να λαμβάνουν αυτόνομες αποφάσεις. Χρησιμοποιώντας έξυπνους αισθητήρες και τεχνητή νοημοσύνη, ένα μηχάνημα μπορεί να ενημερώσει ένα άλλο μηχάνημα όταν συμβαίνει ένα συγκεκριμένο συμβάν, επομένως η κατάλληλη ενέργεια μπορεί να αποφασιστεί ανεξάρτητα και, στη συνέχεια, ο ιδιοκτήτης μπορεί να ειδοποιηθεί [8]. Η σχέση μεταξύ της ιδιοκτησίας και της χρήσης των συλλεγόμενων δεδομένων είναι ένα πρόσφατο αναδυόμενο ζήτημα σε τέτοια κυβερνο-φυσικά συστήματα, όπου αυτά τα δεδομένα συλλέγονται από ετερογενείς αισθητήρες που βρίσκονται σε διαφορετικά σημεία, ενοποιούνται, υποβάλλονται σε επεξεργασία και αναλύονται για περαιτέρω χρήση.

Στα "παραδοσιακά" WSN [9], τα μοντέλα δικτύωσης έχουν ορισμένους περιορισμούς που τα περιορίζουν στη χρήση τους στις σημερινές καινοτόμες εφαρμογές. Κάθε WSN εκχωρείται σε μία εφαρμογή, στην οποία ο χρήστης/κάτοχος είναι ο μόνος υπεύθυνος για τη διαγραφή του δικτύου, την κατανομή πόρων, τον προγραμματισμό και τη συντήρηση.

Το Sensor-Cloud [10] είναι ένα νέο παράδειγμα WSN που αντιμετωπίζει αυτό το πρόβλημα και αποσυνδέει τους κατόχους των φυσικών αισθητήρων από τους χρήστες του δικτύου. Πολλά δίκτυα αισθητήρων που μπορεί να ανήκουν σε διαφορετικές οντότητες και να αναπτύσσονται σε διαφορετικές γεωγραφικές περιοχές, συνδέονται μεταξύ τους μέσω του υπολογιστικού νέφους, επιτρέποντάς τους να λειτουργούν μεταξύ τους ταυτόχρονα για πολλαπλές εφαρμογές.



Εικόνα 1.12. Βασικά στοιχεία του παραδείγματος αισθητήρα-νέφους

Πηγή: https://link.springer.com/article/10.1007/s12652-021-03515-z/figures/4

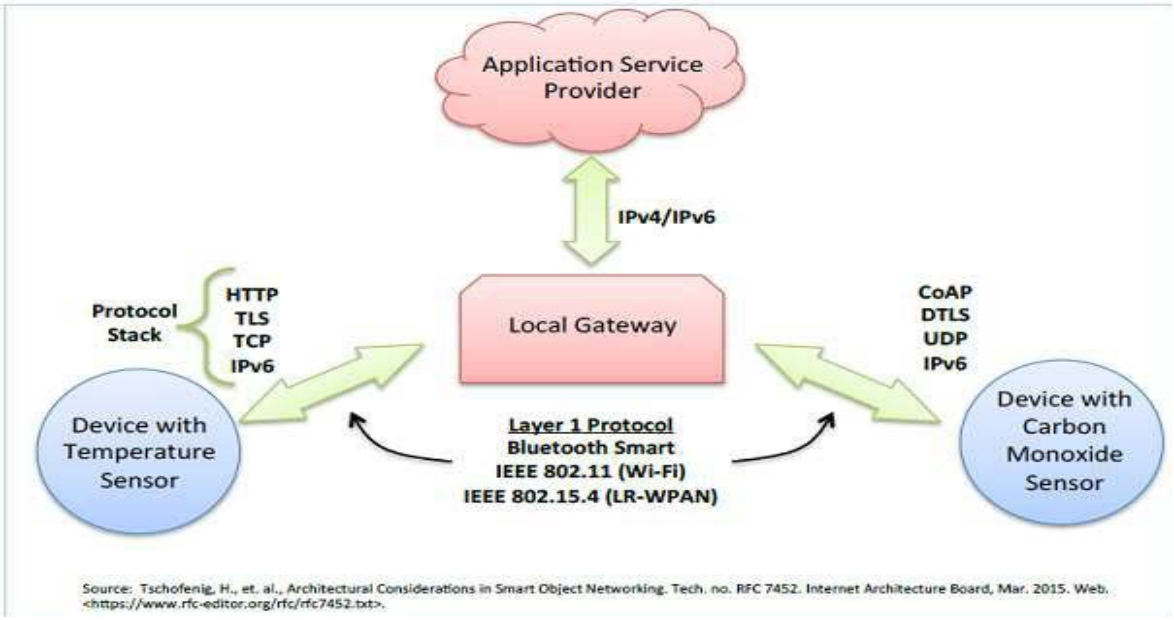
Γενικά, το **Sensor-Cloud** είναι μια εκτεταμένη υποδομή που προέρχεται από δύο κύριες τεχνολογίες **IoT-WSN** και **Virtualization** που βασίζεται στην Υπολογιστική Νέφους (Cloud Computing).

Τα βασικά στοιχεία του Sensor-Cloud περιγράφονται ως εξής:

- Web interface (Διασύνδεση Ιστού): Αυτή η ενότητα επιτρέπει στους χρήστες των εφαρμογών να εγγραφούν στο cloud και να στείλουν αίτημα για εικονικούς αισθητήρες μέσω ενός προγράμματος περιήγησης ιστού.
- User registry (Μητρώο χρηστών): Εγγραφή των χρηστών μαζί με τις εφαρμογές τους στη βάση δεδομένων cloud.
- Physical sensors registration (Καταχώριση φυσικών αισθητήρων): Αποθηκεύει τα χαρακτηριστικά των συσκευών αισθητήρων (όπως αναγνωριστικό αισθητήρα, χωρητικότητα πόρων, τοποθεσία, διεύθυνση IP) στη βάση δεδομένων cloud.
- Routing management (Διαχείριση δρομολόγησης): Μια μέθοδος απόφασης διαδρομής για τη μετάδοση δεδομένων από το φυσικό επίπεδο στο επίπεδο του cloud.
- Resource management (Διαχείριση πόρων): Αυτή η ενότητα χρησιμοποιείται για τη διαχείριση πόρων όπως η κατανομή πόρων, ο προγραμματισμός εργασιών με βάση την προτεραιότητά τους και ο προγραμματισμός του προϋπολογισμού και του κόστους.
- Resource discovery (Ανακάλυψη πόρων): Αναζήτηση ικανών αισθητήρων που πληρούν τις απαιτήσεις των εφαρμογών των χρηστών.
- Storage space (Αποθηκευτικός χώρος): Η χωρητικότητα αποθήκευσης που είναι διαθέσιμη στο cloud για την αποθήκευση των δεδομένων ανίχνευσης.
- Security and privacy (Ασφάλεια και απόρρητο): Διασφάλιση προστασίας του απορρήτου των δικτύων Sensor-Cloud από οποιαδήποτε παραβίαση.
- Virtualization management (Διαχείριση εικονικών αισθητήρων): Υπεύθυνο για τον έλεγχο της διαδικασίας δημιουργίας, παρακολούθησης και συντήρησης των εικονικών αισθητήρων.
- Service template (Πρότυπο υπηρεσίας): Ένας κατάλογος ο οποίος περιέχει μια λίστα με τις διαθέσιμες υπηρεσίες που είναι έτοιμες να εξυπηρετήσουν εφαρμογές.
- Service management (Διαχείριση υπηρεσιών): Έλεγχος και παρακολούθηση της παροχής διαφόρων υπηρεσιών

1.6.3 Συσκευή προς Πύλη (Device-to-Gateway)

Στο μοντέλο συσκευής προς πύλη, που ονομάζεται επίσης μοντέλο πύλης από συσκευή σε εφαρμογή επιπέδου (Application-Level Gateway), η συσκευή IoT συνδέεται μέσω μιας υπηρεσίας ALG ως αγωγός για να φτάσει σε μια υπηρεσία cloud. Με απλούστερους όρους, αυτό σημαίνει ότι υπάρχει λογισμικό εφαρμογής που εκτελείται σε μια τοπική συσκευή πύλης που λειτουργεί ως ενδιάμεσος μεταξύ της συσκευής και της υπηρεσίας cloud, παρέχοντας ασφάλεια και άλλες λειτουργίες, όπως μετάφραση δεδομένων ή πρωτοκόλλου.



Εικόνα 1.13. Παράδειγμα μοντέλου Device to Gateway

Πολλές παραλλαγές αυτού του μοντέλου βρίσκονται σε καταναλωτικές συσκευές. Σε πολλές περιπτώσεις, η τοπική συσκευή πύλης είναι ένα smartphone που εκτελεί μια εφαρμογή για επικοινωνία με τη συσκευή και μεταφορά δεδομένων σε μια υπηρεσία cloud. Πολλές φορές αυτό το μοντέλο έχει χρησιμοποιηθεί σε δημοφιλή καταναλωτικά προϊόντα όπως προσωπικοί ιχνηλάτες γυμναστικής (fitness trackers). Αυτές οι συσκευές δεν διαθέτουν ενσωματωμένη απευθείας συνδεσιμότητα στο cloud, επομένως συχνά βασίζονται σε λογισμικό εφαρμογών smartphone ως πύλη για τη σύνδεση της συσκευής γυμναστικής στο cloud.

Μια άλλη μορφή αυτού του μοντέλου συσκευής σε πύλη είναι η εμφάνιση συσκευών "hub" σε εφαρμογές οικιακού αυτοματισμού. Πρόκειται για συσκευές που χρησιμεύουν ως τοπική πύλη μεταξύ μεμονωμένων συσκευών IoT και μιας υπηρεσίας cloud.

Αυτό το μοντέλο επικοινωνίας χρησιμοποιείται σε περιπτώσεις όπου τα έξυπνα αντικείμενα απαιτούν διαλειτουργικότητα με συσκευές που δεν χρησιμοποιούν IP (Internet protocol). Αυτή η προσέγγιση χρησιμοποιείται μερικές φορές για την ενσωμάτωση συσκευών IPv6, πράγμα που σημαίνει ότι απαιτείται πύλη για συσκευές και υπηρεσίες IPv4 παλαιού τύπου.

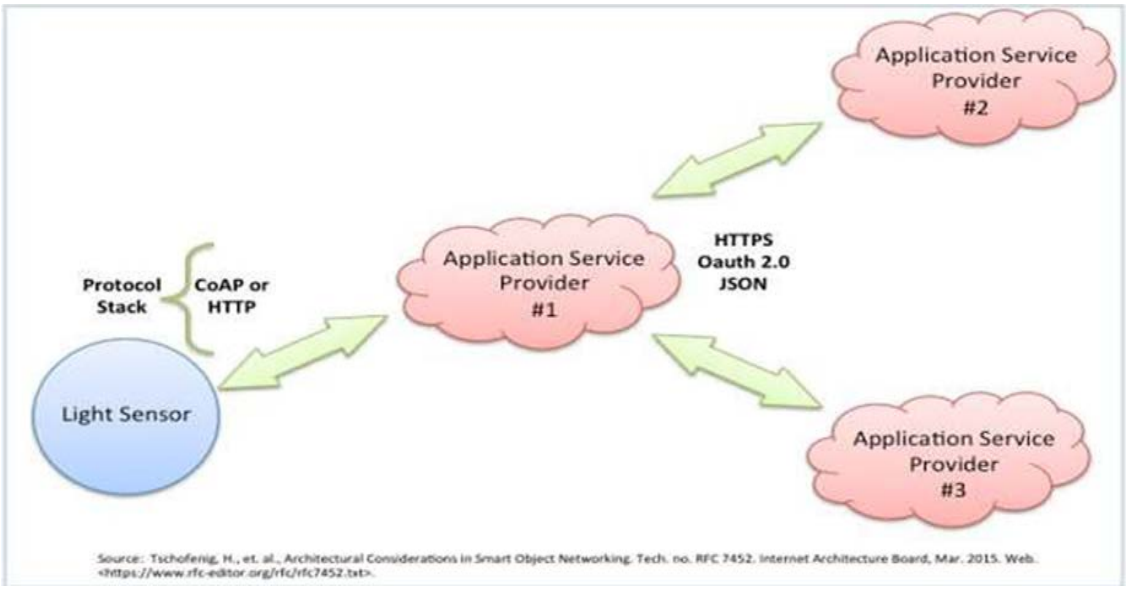
Αυτό το μοντέλο επικοινωνίας χρησιμοποιείται συχνά για την ενσωμάτωση νέων έξυπνων συσκευών σε ένα παλαιού τύπου σύστημα με συσκευές που δεν είναι εγγενώς συμβατές με αυτές. Ένα μειονέκτημα αυτής της προσέγγισης είναι ότι η απαραίτητη ανάπτυξη του λογισμικού επιπέδου εφαρμογής και του συστήματος πύλης προσθέτει πολυπλοκότητα και κόστος στο συνολικό σύστημα.

1.6.4 Back-End μοντέλο μετάδοσης δεδομένων (Back-End Data-Sharing Model)

Το μοντέλο κοινής χρήσης δεδομένων back-end επιτρέπει στους χρήστες να εξάγουν και να αναλύουν δεδομένα έξυπνων αντικειμένων από μια υπηρεσία cloud σε συνδυασμό με δεδομένα από άλλες πηγές. Αυτή η αρχιτεκτονική επιτρέπει στους χρήστες να παραχωρούν πρόσβαση στα μεταφορτωμένα δεδομένα αισθητήρων σε εξουσιοδοτημένα τρίτα μέρη.

Για παράδειγμα, ένας εταιρικός χρήστης υπεύθυνος για ένα συγκρότημα γραφείων θα ενδιαφερόταν να ενοποιήσει και να αναλύσει την κατανάλωση ενέργειας και τα δεδομένα κοινής ωφέλειας που παράγονται από όλους τους αισθητήρες IoT και τα βοηθητικά συστήματα με δυνατότητα Internet στις εγκαταστάσεις. Μια αποτελεσματική αρχιτεκτονική κοινής χρήσης δεδομένων back-end θα επέτρεπε στην εταιρεία να έχει εύκολη πρόσβαση και να αναλύει τα δεδομένα στο cloud που παράγονται από όλο το φάσμα των συσκευών στο κτίριο. Επίσης, αυτού του είδους η αρχιτεκτονική διευκολύνει τις ανάγκες φορητότητας δεδομένων. Η αποτελεσματική αρχιτεκτονική κοινής χρήσης δεδομένων back-end επιτρέπει στους χρήστες να μετακινούν τα δεδομένα τους όταν κάνουν εναλλαγή μεταξύ υπηρεσιών IoT, καταρρίπτοντας τα παραδοσιακά εμπόδια σιλό δεδομένων [11].

Το μοντέλο κοινής χρήσης δεδομένων back-end προτείνει μια προσέγγιση ομόσπονδων υπηρεσιών cloud ή διεπαφές προγραμματιστών εφαρμογών cloud (API) για την επίτευξη διαλειτουργικότητας δεδομένων έξυπνων συσκευών που φιλοξενούνται στο cloud. Μια γραφική αναπαράσταση αυτού του σχεδίου φαίνεται στην Εικόνα 1.14.



Εικόνα 1.14. Παράδειγμα Back-End Data-Sharing Model

1.7 Λειτουργία WSNs

Όπως προαναφέραμε, τα WSN μπορούν να οριστούν ως ένα ασύρματο δίκτυο χωρίς υποδομή που έχει ρυθμιστεί για την παρατήρηση φυσικών ή περιβαλλοντικών συνθηκών, όπως θερμοκρασία, πίεση, κίνηση, ήχο, κραδασμούς ή ρύπους, και για απευθείας μετάδοση δεδομένων ή πληροφοριών μέσω το δίκτυο σε ένα σταθμό βάσης όπου συχνά παρατηρούνται και αναλύονται οι πληροφορίες. Ένας σταθμός βάσης λειτουργεί σαν μια διεπαφή μεταξύ των χρηστών και του δικτύου. Μπορεί να μετατρέψει και να επιστρέψει πίσω ορισμένες απαιτούμενες πληροφορίες από το δίκτυο εισάγοντας ορισμένα queries και συλλέγοντας αποτελέσματα από το σταθμό βάσης. Συνήθως ένα ασύρματο δίκτυο αισθητήρων περιέχει πολλές χιλιάδες κόμβους αισθητήρων.

Οι αισθητήριοι κόμβοι μπορούν να επικοινωνούν μεταξύ τους χρησιμοποιώντας ραδιοσήματα. Είναι εξοπλισμένοι με αισθητήρες και πομποδέκτες ραδιοφώνου, υπολογιστικές συσκευές και εξαρτήματα ισχύος. Ένας κόμβος αισθητήρα σε ένα ασύρματο δίκτυο αισθητήρων είναι εγγενώς περιορισμένος σε πόρους, επίσης έχει περιορισμένη ταχύτητα επεξεργασίας, χωρητικότητα αποθήκευσης και εύρος ζώνης επικοινωνίας. Αφού εγκατασταθούν οι κόμβοι αισθητήρων, είναι υπεύθυνοι για την αυτο-οργάνωση μιας κατάλληλης υποδομής δικτύου συχνά με επικοινωνία πολλαπλών βημάτων μεταξύ τους.

Αρχικά, οι ενσωματωμένοι αισθητήρες αρχίζουν να συλλέγουν πληροφορίες διάφορου τύπου ενδιαφέροντος. Και στη συνέχεια, οι ειδικά σχεδιασμένες συσκευές ασύρματων δικτύων αισθητήρων απαντούν σε αυτά τα queries που αποστέλλονται από

μια "θέση ελέγχου" για να εκτελέσουν συγκεκριμένες οδηγίες ή να παράσχουν δείγματα ανίχνευσης.

Ο τρόπος λειτουργίας των κόμβων αισθητήρων θα μπορούσε επίσης να είναι είτε συνεχής είτε βάσει συμβάντων. GPS (Global Positioning System) και LPA (Local Positioning Algorithms) μπορούν να χρησιμοποιηθούν για τη λήψη πληροφοριών τοποθεσίας και θέσης. Οι συσκευές ασύρματου αισθητήρα είναι συχνά εξοπλισμένες με ενεργοποιητές για να «ενεργούν» υπό ορισμένες συνθήκες. Αυτά τα δίκτυα συνήθως ονομάζονται ασύρματο δίκτυο αισθητήρων (Sensors Network) και δίκτυο ενεργοποιητών (Actuators Network) [12].

1.8 Τύποι WSNs

Υπάρχουν πέντε τύποι ασύρματων δικτύων αισθητήρων ανάλογα με το περιβάλλον. Οι διαφορετικοί τύποι WSN είναι οι εξής:

1. **Επίγεια ασύρματα δίκτυα αισθητήρων:** Τα επίγεια WSN χρησιμοποιούνται για την αποτελεσματική επικοινωνία σταθμών βάσης και περιλαμβάνουν χιλιάδες ασύρματους κόμβους αισθητήρων που αναπτύσσονται είτε με μη δομημένο (ad hoc) είτε με δομημένο (Προσχεδιασμένο) τρόπο.

   Σε μια μη δομημένη λειτουργία (ad hoc), οι κόμβοι αισθητήρων κατανέμονται τυχαία εντός της περιοχής στόχου. Η ισχύς της μπαταρίας είναι περιορισμένη, ωστόσο, η μπαταρία παρέχεται με ηλιακές κυψέλες ως δευτερεύουσα πηγή ενέργειας. Η διατήρηση της ενέργειας των WSN επιτυγχάνεται χρησιμοποιώντας λειτουργίες χαμηλού κύκλου λειτουργίας, βέλτιστη δρομολόγηση, ελαχιστοποίηση καθυστερήσεων κ.λπ.

2. **Υπόγεια ασύρματα δίκτυα αισθητήρων:** Όσον αφορά την ανάπτυξη, τη συντήρηση, το κόστος του εξοπλισμού και τον προσεκτικό σχεδιασμό, τα υπόγεια ασύρματα δίκτυα αισθητήρων είναι πιο ακριβά από τα επίγεια WSN. Τα UWSN (Underground Wireless Sensor Networks) περιλαμβάνουν αρκετούς αισθητήριους κόμβους που είναι κρυμμένοι στο έδαφος για να παρατηρήσουν υπόγειες συνθήκες. Οι κόμβοι αισθητήρων που είναι εξοπλισμένοι με περιορισμένη ισχύ μπαταρίας είναι επίσης δύσκολο να επαναφορτιστούν. Επιπλέον, το υπόγειο περιβάλλον καθιστά την ασύρματη επικοινωνία πρόκληση λόγω του υψηλού επιπέδου εξασθένησης και απώλειας σήματος.

3. **Υποβρύχια ασύρματα δίκτυα αισθητήρων**: Περίπου περισσότερο από το 70% του πλανήτη της γης είναι κατειλημμένο με νερό. Αυτά τα δίκτυα περιέχουν αρκετούς κόμβους αισθητήρων και οχήματα τοποθετημένα υποβρύχια. Χρησιμοποιούνται αυτόνομες υποβρύχιες συσκευές και οχήματα για τη συλλογή δεδομένων από αυτούς τους κόμβους αισθητήρων.

   Μια πρόκληση της υποβρύχιας επικοινωνίας είναι η μεγάλη καθυστέρηση μετάδοσης και αστοχίες εύρους ζώνης και αισθητήρα. Υποβρύχια, τα WSN είναι εξοπλισμένα με περιορισμένη μπαταρία που δεν μπορεί να επαναφορτιστεί ή να αντικατασταθεί. Η δυσκολία εξοικονόμησης ενέργειας για τα υποβρύχια WSN περιλαμβάνει την ανάπτυξη τεχνικών υποβρύχιας επικοινωνίας και δικτύωσης.

4. **Ασύρματα δίκτυα αισθητήρων πολυμέσων**: Τα ασύρματα δίκτυα αισθητήρων πολυμέσων προτείνονται για τον εντοπισμό και την παρακολούθηση γεγονότων στο είδος των πολυμέσων, όπως βίντεο, απεικόνισης και ήχου. Αυτά τα δίκτυα περιέχουν κόμβους αισθητήρα χαμηλού κόστους εξοπλισμένους με κάμερες και μικρόφωνα. Αυτοί οι αισθητήριοι κόμβοι των πολυμέσων WSN διασυνδέονται μεταξύ τους μέσω μιας ασύρματης σύνδεσης για ανάκτηση δεδομένων, συμπίεση δεδομένων και συσχέτιση. Οι προκλήσεις με τα WSN πολυμέσων περιλαμβάνουν απαιτήσεις υψηλού εύρους ζώνης, υψηλή κατανάλωση ενέργειας, τεχνικές επεξεργασίας και συμπίεσης. Επιπλέον, τα περιεχόμενα πολυμέσων χρειάζονται υψηλό εύρος ζώνης για να παραδοθούν σωστά και εύκολα.

5. **Κινητά ασύρματα δίκτυα αισθητήρων**: Τα δίκτυα κινητών WSN περιλαμβάνουν μια ομάδα κόμβων αισθητήρων που μπορούν να μετακινηθούν μόνοι τους και μπορούν να αλληλεπιδράσουν με το φυσικό περιβάλλον. Είναι πολύ πιο ευέλικτα από τα στατικά δίκτυα αισθητήρων. Τα οφέλη των φορητών WSN έναντι των στατικών WSN περιλαμβάνουν καλύτερη και βελτιωμένη κάλυψη, ανώτερη χωρητικότητα καναλιού, καλύτερη ενεργειακή απόδοση κ.λπ.

1.9 Εφαρμογές WSNs

Τα ασύρματα δίκτυα αισθητήρων έχουν κερδίσει μεγάλη δημοτικότητα λόγω της ευελιξίας τους στην επίλυση προβλημάτων σε διαφορετικούς τομείς εφαρμογών και έχουν τη δυνατότητα να αλλάξουν τη ζωή μας με πολλούς διαφορετικούς τρόπους. Τα WSN έχουν εφαρμοστεί με επιτυχία σε διάφορους τομείς εφαρμογών, όπως:

Στρατιωτικές εφαρμογές: Τα ασύρματα δίκτυα αισθητήρων είναι πιθανότατα αναπόσπαστο μέρος των συστημάτων στρατιωτικής διοίκησης, ελέγχου, επικοινωνιών, υπολογιστών, πληροφοριών, επιτήρησης πεδίου μάχης, αναγνώρισης και στόχευσης [13].

Παρακολούθηση περιοχής: Στην παρακολούθηση περιοχής, οι κόμβοι αισθητήρων αναπτύσσονται σε μια περιοχή όπου πρέπει να παρακολουθείται κάποιο φαινόμενο. Όταν οι αισθητήρες ανιχνεύουν το συμβάν που παρακολουθείται (θερμότητα, πίεση κ.λπ.), το συμβάν αναφέρεται σε έναν από τους σταθμούς βάσης, ο οποίος στη συνέχεια λαμβάνει τα κατάλληλα μέτρα [14].

Μεταφορά: Οι πληροφορίες κυκλοφορίας σε πραγματικό χρόνο συλλέγονται από τα WSN για να τροφοδοτήσουν αργότερα μοντέλα μεταφοράς και να ειδοποιήσουν τους οδηγούς για κυκλοφοριακή συμφόρηση και προβλήματα κυκλοφορίας [15] [16].

Εφαρμογές υγείας: Ορισμένες από τις εφαρμογές υγείας για δίκτυα αισθητήρων υποστηρίζουν διεπαφές για άτομα με ειδικές ανάγκες, ενσωματωμένη παρακολούθηση ασθενών, διαγνωστικά και χορήγηση φαρμάκων σε νοσοκομεία, τηλεπαρακολούθηση ανθρώπινων φυσιολογικών δεδομένων και παρακολούθηση γιατρών ή ασθενών εντός νοσοκομείου [17].

Περιβαλλοντική ανίχνευση: Ο όρος Environmental Sensor Networks έχει αναπτυχθεί για να καλύψει πολλές εφαρμογές των WSN στην έρευνα της επιστήμης της γης. Αυτό περιλαμβάνει αισθητήρια ηφαίστεια, ωκεανούς, παγετώνες, δάση κ.λπ. Μερικές άλλες σημαντικές περιοχές παρατίθενται παρακάτω:

- Παρακολούθηση ατμοσφαιρικής ρύπανσης
- Ανίχνευση δασικών πυρκαγιών
- Παρακολούθηση θερμοκηπίου
- Ανίχνευση κατολισθήσεων

Δομική παρακολούθηση: Μπορούν να χρησιμοποιηθούν ασύρματοι αισθητήρες για την παρακολούθηση της κίνησης εντός κτιρίων και υποδομών όπως γέφυρες, αερογέφυρες, αναχώματα, σήραγγες κ.λπ., επιτρέποντας στους αρμόδιους να παρακολουθούν τα δομικά αυτά έργα εξ αποστάσεως χωρίς την ανάγκη δαπανηρών επισκέψεων [18].

Βιομηχανική παρακολούθηση: Τα ασύρματα δίκτυα αισθητήρων έχουν αναπτυχθεί για συντήρηση βάσει συνθηκών (Condition-Based Maintenance), καθώς προσφέρουν σημαντική εξοικονόμηση κόστους και επιτρέπουν νέες λειτουργίες. Στα ενσύρματα

συστήματα, η εγκατάσταση πολλών αισθητήρων μπορεί να είναι απαγορευτικά δαπανηρή λόγω του κόστους καλωδίωσης, περιορίζοντας τις πιθανές λειτουργίες που μπορούν να επιτευχθούν [19].

Αγροτικός τομέας: η χρήση ασύρματου δικτύου απαλλάσσει τον αγρότη από τη συντήρηση της καλωδίωσης σε ένα δύσκολο περιβάλλον. Ο αυτοματισμός άρδευσης επιτρέπει την αποτελεσματικότερη χρήση του νερού και μειώνει τη σπατάλη.

2. Διαδίκτυο των Πραγμάτων (Internet of Things - IoT)

Το Διαδίκτυο των Πραγμάτων (Internet of Things) αποτελεί ένα δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Με λίγα λόγια, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους ή στο Διαδίκτυο [20].

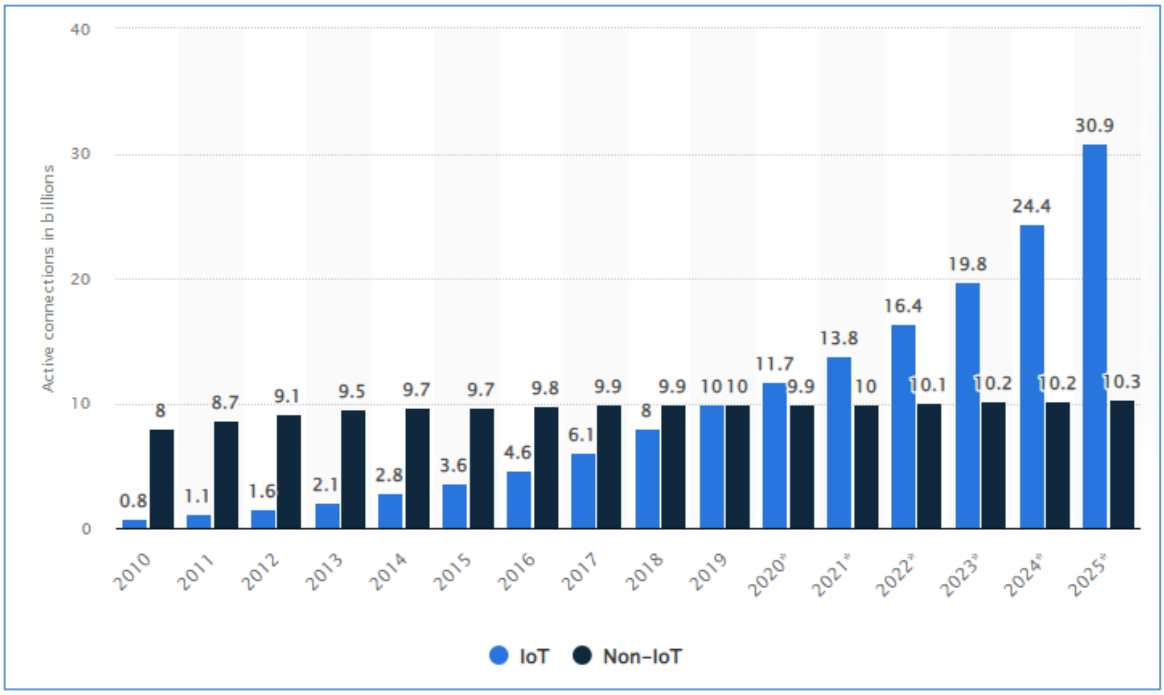
Το Διαδίκτυο των Πραγμάτων μπορεί να θεωρηθεί ως μια τεράστια γκάμα διασυνδεδεμένων συσκευών και τεχνολογιών, με πιθανές κοινωνικές και τεχνολογικές προεκτάσεις, ενώ ο όρος Διαδίκτυο των Πραγμάτων επινοήθηκε τη δεκαετία του 1990 από τον Kevin Ashton (2020) [21]. Χρησιμοποιώντας δυνατότητες ανίχνευσης, καταγραφής δεδομένων, επεξεργασίας και επικοινωνίας, το IoT επιτρέπει την πρόσβαση στις υπηρεσίες από όλα τα είδη εφαρμογών, πληρώντας τις απαιτήσεις εγγύτητας και ασφάλειας.

2.1 Εισαγωγή στο Διαδίκτυο των Πραγμάτων (IoT)

Η τεχνολογία IoT αποτελείται από ένα πολύπλοκο δίκτυο το οποίο διασυνδέει τα «αντικείμενα-πράγματα» με το Διαδίκτυο μέσω της χρήσης τυποποιημένων πρωτοκόλλων επικοινωνίας. Τα διασυνδεδεμένα «πράγματα» έχουν φυσική ή εικονική αναπαράσταση στον ψηφιακό κόσμο, δυνατότητα ανίχνευσης και ενεργοποίησης, δυνατότητα προγραμματισμού, είναι μοναδικώς αναγνωρίσιμα και προσφέρουν υπηρεσίες μέσω της αξιοποίησης των παραπάνω χαρακτηριστικών [22].

Οι πρόοδοι που έχουν σημειωθεί στις τεχνολογίες επικοινωνίας και πληροφοριών, εισάγουν το Διαδίκτυο των Πραγμάτων στις υπηρεσίες ασφάλειας των κρίσιμων υποδομών. Οι ευπάθειες, ωστόσο, των συστημάτων αυτών περιλαμβάνουν τη γρήγορη εξάντληση των πόρων ενέργειας και την πιθανότητα της δολιοφθοράς μέσω λογισμικών υποκλοπών ή κακόβουλων ιών. Ως εκ τούτου, η φύση των ασύρματων αισθητήρων και του IoT επιτρέπει τη διεξαγωγή του ρόλου αυτής της οντότητας για το σκοπό της προστασίας των υποδομών· από την άλλη όμως επιβάλλει την προστασία του ίδιου συστήματος από κακόβουλες επιθέσεις και δολιοφθορά [23].

Η αγορά του Διαδικτύου των Πραγμάτων συνεχίζει να αναπτύσσεται. Το 2020, για πρώτη φορά, υπήρχαν περισσότερες συνδέσεις IoT από ό,τι οι συνδέσεις εκτός IoT (smartphones, φορητοί υπολογιστές και υπολογιστές). Από τα 21,7 δισεκατομμύρια ενεργές συνδεδεμένες συσκευές παγκοσμίως, τα 11,7 δισεκατομμύρια (ή 54%) εκτιμήθηκαν ως συνδέσεις συσκευών IoT περί το τέλος του 2020. Μέχρι το 2025, αναμένεται ότι θα υπάρξουν περισσότερες από 30 δισεκατομμύρια συνδέσεις IoT, σχεδόν 4 συσκευές IoT ανά άτομο κατά μέσο όρο [24] (Εικόνα 2.1).



Εικόνα 2.1. Συνδέσεις ενεργών συσκευών Internet of Things (IoT) και μη IoT παγκοσμίως από το 2010 έως το 2025

Πηγή: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/

2.2 Αρχιτεκτονική IoT

Η αρχιτεκτονική των εφαρμογών IoT είναι απαραίτητη για τη λειτουργικότητά τους. Μπορεί να επηρεάσει την καθημερινή ζωή με διάφορους τρόπους, και έτσι η επιτυχία του IoT βασίζεται σε ένα σύστημα που είναι δυναμικό, ασφαλές και επεκτάσιμο. Διάφορες αρχιτεκτονικές έχουν προταθεί στη βιβλιογραφία, αλλά υπάρχουν ακόμη κάποια ανοιχτά ζητήματα που πρέπει να επιλυθούν. Ωστόσο, κάθε αρχιτεκτονική στοχεύει να εξασφαλίσει ένα σύνολο σημαντικών ιδιοτήτων [25] :

- **Διαλειτουργικότητα**: Οι συσκευές από διαφορετικούς προμηθευτές θα πρέπει να λειτουργούν αρμονικά για την επίτευξη κοινών στόχων. Επιπλέον, τα συστήματα και τα πρωτόκολλα επικοινωνίας θα πρέπει να σχεδιάζονται με τέτοιο τρόπο ώστε

να μπορούν να ανταλλάσσονται δεδομένα μεταξύ αντικειμένων από διαφορετικούς κατασκευαστές.

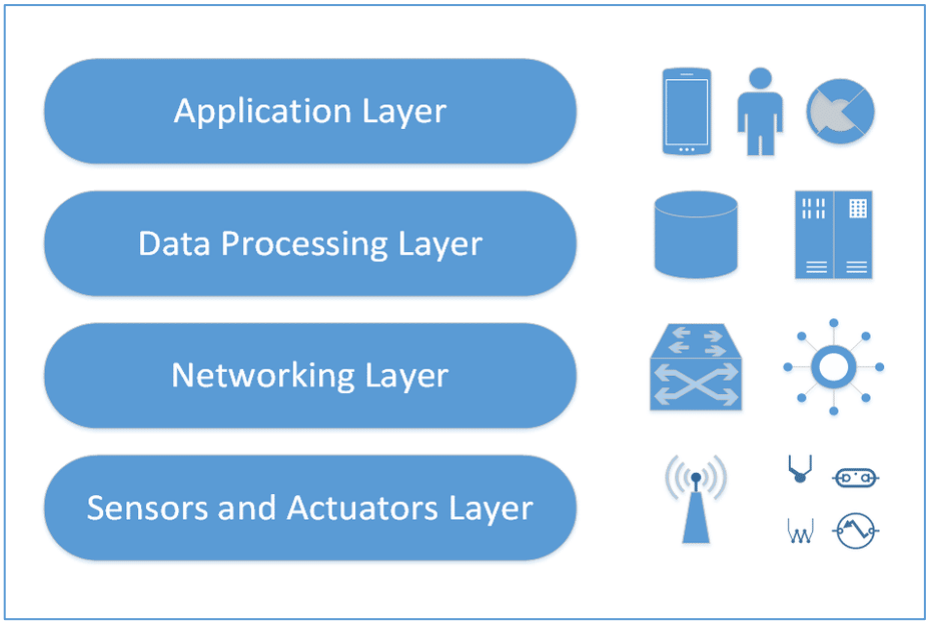
- **Επεκτασιμότητα**: Δισεκατομμύρια αντικείμενα αναμένεται να είναι μέρος του ίδιου δικτύου. Για το λόγο αυτό, τα συστήματα που ελέγχουν και υποστηρίζουν αυτά τα αντικείμενα πρέπει να είναι σε θέση να διαχειρίζονται μεγάλες ποσότητες δεδομένων.
- **Δυνατότητες Κατανομής**: Το IoT εξελίσσεται σε ένα μεγάλο, διασυνδεδεμένο σύστημα όπου τα δεδομένα θα συλλέγονται από διαφορετικές πηγές και θα υποβάλλονται σε επεξεργασία από διαφορετικές οντότητες με κατανεμημένο τρόπο.
- **Έλλειψη πόρων**: Τόσο η ενέργεια όσο και η υπολογιστική ισχύς των αντικειμένων IoT που εμπλέκονται είναι σημαντικά περιορισμένη.
- **Ασφάλεια**: Οι χρήστες μπορεί να αισθάνονται ότι παρακολουθούνται και πως η καθημερινότητά τους καταγράφεται από εξωτερικούς παράγοντες, γεγονός που ίσως εμποδίσει τη δημιουργία εφαρμογών IoT.

Διαφορετικές αρχιτεκτονικές IoT έχουν και αντίστοιχα διαφορετική κάλυψη των ιδιοτήτων που προαναφέρθηκαν, αλλά οι περισσότερες συγκλίνουν στην κατασκευή του IoT σε διάφορα επίπεδα, ανάλογα με τις τεχνολογίες που χρησιμοποιούνται. Τα βασικά επίπεδα αρχιτεκτονικής του IoT είναι τα ακόλουθα:

- Επίπεδο Αντίληψης (perception/sensing layer),
- Επίπεδο Δικτύωσης (network layer)
- Επίπεδο Εφαρμογών (application layer)

Διαφορετικές προσεγγίσεις προσθέτουν και ένα επιπλέον ενδιάμεσο επίπεδο υποστήριξης μεταξύ του επιπέδου δικτύωσης και του επιπέδου εφαρμογών:

- Επίπεδο Αντίληψης (perception/sensing layer),
- Επίπεδο Δικτύωσης (network layer)
- Επίπεδο Υποστήριξης/Επεξεργασίας Δεδομένων (supporting/data processing layer)
- Επίπεδο Εφαρμογών (application layer)



Εικόνα 2.2. Μοντέλο IoT τεσσάρων επιπέδων

Πηγή: https://www.hiotron.com/wp-content/uploads/2019/07/The-architectural-layers-of-IoT-systems.png

Το επίπεδο αντίληψης είναι υπεύθυνο για την αναγνώριση αντικειμένων και τη συλλογή δεδομένων από αισθητήρες (sensors) και ενεργοποιητές (actuators). Το επίπεδο δικτύωσης περιλαμβάνει ιδιωτικά δίκτυα, το Διαδίκτυο, δίκτυα κινητής τηλεφωνίας, τοπικά και δίκτυα ευρείας περιοχής. Έχει σχεδιαστεί για την ασφαλή και αξιόπιστη μεταφορά και μετάδοση δεδομένων. Το επίπεδο υποστήριξης υιοθετεί ομοιόμορφη κωδικοποίηση, διάδοση, διαχείριση και αποθήκευση δεδομένων και «υπολογιστικό νέφος». Τέλος, το επίπεδο των εφαρμογών αφορά εμπορικές δραστηριότητες, αλυσίδες εφοδιασμού, «έξυπνα» σπίτια, «έξυπνες» πόλεις κ.λπ.

2.2.1 Επίπεδο Αντίληψης

Σε αυτό το επίπεδο αρχιτεκτονικής IoT, οι αισθητήρες και οι ενεργοποιητές παίζουν πολύ σημαντικό ρόλο. Οι συσκευές αυτές συνδέονται μεταξύ τους είτε ενσύρματα είτε ασύρματα και χρησιμοποιούνται για την αναγνώριση αντικειμένων, τη συλλογή πληροφοριών και την εκτέλεση διεργασιών χωρίς την ανάγκη ανθρώπινης παρουσίας. Τα βασικότερα χαρακτηριστικά του επιπέδου αντίληψης είναι τα εξής:

- **Αντίληψη**: Διάφοροι αισθητήρες έχουν την ικανότητα να ανιχνεύουν χαρακτηριστικά και ιδιότητες του εξωτερικού περιβάλλοντος. Αυτά τα δεδομένα μπορούν να χρησιμοποιηθούν για την ενεργοποίηση ενεργειών και την εκκίνηση διεργασιών.

- **Επικοινωνία**: Οι αισθητήρες και οι ενεργοποιητές συνδέονται ασύρματα και ενσύρματα με άλλα αντικείμενα για να δημιουργήσουν ένα δίκτυο. Μπορούν επίσης να συνδεθούν σε ετερογενή δίκτυα μεταξύ διασυνδεδεμένων αντικειμένων.
- **Ταυτοποίηση**: Οι αισθητήρες είναι σε θέση να αναγνωρίζουν αντικείμενα εκπέμποντας ένα σήμα ή μέσω των συγκεκριμένων ιδιοτήτων τους (π.χ. μέγεθος, θέση, θερμοκρασία). Τα φυσικά χαρακτηριστικά των αντικειμένων μπορούν στη συνέχεια να ενοποιηθούν με τα αντίστοιχα εικονικά τους.

2.2.1.1 Αισθητήρες και Ενεργοποιητές

Οι αισθητήρες είναι συσκευές που χρησιμοποιούνται για την ανίχνευση φυσικών αντικειμένων στο περιβάλλον. Είναι συνήθως χαμηλού κόστους και έχουν χαμηλή ενεργειακή χωρητικότητα. Έχουν επίσης περιορισμούς όσον αφορά την υπολογιστική τους ισχύ και τις δυνατότητες δικτύωσης. Ωστόσο, ορίζονται χρήσιμοι στην ανίχνευση εξωτερικών περιβαντολογικών ιδιοτήτων όπως ταχύτητα, επιτάχυνση, δόνηση, οι ηλεκτρομαγνητικά πεδία, θερμοκρασία και υγρασία.

Αυτοί οι αισθητήρες βασίζονται στην ανίχνευση φυσικών χαρακτηριστικών (non - ID based sensors). Επίσης, υπάρχουν και αισθητήρες που ανιχνεύουν ορισμένα σήματα από τα αντικείμενα (ID based sensors). Οι αισθητήρες αυτού του είδους διαβάζουν ετικέτες RFID και κωδικούς QR. Σε διαφορετικά σενάρια IoT, οι εμπλεκόμενοι αισθητήρες μπορεί να έχουν διαφορετικές ταυτότητες. Γενικά, οι αισθητήρες ετεροσύνδεσης των δύο παραπάνω κατηγοριών είναι οργανωμένοι με τέτοιο τρόπο ώστε να επιτρέπουν την υβριδική ανίχνευση και αναγνώριση φυσικών αντικειμένων.

Οι ενεργοποιητές είναι συσκευές που αυτοματοποιούν και ελέγχουν συγκεκριμένες διαδικασίες, συχνά ως μηχανικές ή ηλεκτρικές συσκευές (διακόπτες, βαλβίδες). Συνήθως χρησιμοποιούνται για τη μετατροπή των συλλεγόμενων δεδομένων σε εντολές ενεργειών. Σε πολλές περιπτώσεις, οι αισθητήρες και οι ενεργοποιητές βρίσκονται στην ίδια συσκευή. Μια συσκευή ελέγχου ποιότητας του αέρα, για παράδειγμα, κατά τη στιγμή που θα ανιχνεύσει μη επιτρεπτά επίπεδα διοξειδίου του άνθρακα θα ενεργοποιήσει αυτόματα το κλιματιστικό ώστε να αποκατασταθούν οι φυσιολογικές συνθήκες. Οι ενεργοποιητές μπορούν επίσης να βρίσκονται σε απόσταση από τους αντίστοιχους αισθητήρες και να επικοινωνούν με το επίπεδο δικτύου χρησιμοποιώντας πρωτόκολλα επικοινωνίας [26].

2.2.2 Επίπεδο Δικτύωσης

Το επίπεδο δικτύωσης είναι υπεύθυνο για την τοπική επεξεργασία των δεδομένων που συλλέγονται από το επίπεδο αντίληψης μέσω υπολογιστικής άκρου, καθώς και για την προώθηση και μετάδοση αυτών των δεδομένων στα ανώτερα επίπεδα μέσω διαφόρων τεχνολογιών δικτύου. Οι τεχνολογίες κυψελωτών δικτύων κινητών τηλεπικοινωνιών (3G, 4G, 5G), τα πρωτόκολλα δικτύωσης σε δίκτυα αισθητήρων (WSN) και στο διαδίκτυο των πραγμάτων (IoT), αλλά και η υπέρυθρη ακτινοβολία, είναι οι πιο βασικές μορφές δικτυακών τεχνολογιών.

2.2.2.1 Wi – Fi

Το Wi – Fi, βασισμένο σε IEEE 802.11 πρότυπα, αποτελεί την τεχνολογία που χρησιμοποιούν τα τοπικά δίκτυα (WLANs). Είναι μία ασύρματη τεχνολογία που επιτρέπει στις ηλεκτρονικές συσκευές να ανταλλάσσουν δεδομένα σε υψηλές ταχύτητες, συνήθως μέσω ενός δικτύου υπολογιστών (πχ Διαδίκτυο). Οι πιο κοινές ζώνες Wi - Fi είναι 2,4 GHz, 5 GHz και 6 GHz. Οι υψηλότερες συχνότητες επιτρέπουν μεγαλύτερες ταχύτητες, ωστόσο έχουν μειωμένο εύρος εκπομπής σήματος.

2.2.2.2 Bluetooth

Το Bluetooth είναι μία ασύρματη τεχνολογία μετάδοσης ραδιοσυχνοτήτων μικρής εμβέλειας (<10m), που βασίζεται στα πρότυπα IEEE 802.15.1. Χρησιμοποιείται κυρίως σε προσωπικά δίκτυα (PAN) για τη ζεύξη κινητών τηλεφώνων, έξυπνων ρολογιών (Smartwatches), ασύρματων ακουστικών, κ.α. Διαθέτει χαμηλές ταχύτητες, απαιτεί υψηλή ασφάλεια και συνεπή κωδικοποίηση.

2.2.2.3 ZigBee

Το ZigBee είναι μια τεχνολογία ασύρματης μετάδοσης δεδομένων που λειτουργεί σε μικρές αποστάσεις και σύμφωνα με τα πρότυπα IEEE 802.15.4. Η εγκατάσταση συσκευών ZigBee σε επίπεδο σπιτιού (Home Area Network) γίνεται συνήθως με κατανεμημένη τοπολογία προκειμένου να επιτευχθεί επικοινωνία σε μεγαλύτερες αποστάσεις μέσω ενδιάμεσων συσκευών. Αυτή η τεχνολογία έχει πολλά χαρακτηριστικά, συμπεριλαμβανομένης της δυνατότητας ταυτόχρονης σύνδεσης πολλών αισθητήρων. Υποστηρίζει τοπολογίες όπως peer-to-peer (P2P) και peer to multi-peer (P2M). Έχει χαμηλές απαιτήσεις ενέργειας και πολυπλοκότητας αλλά και μηχανισμούς κρυπτογράφησης (AES 128-bit).

2.2.2.4 Υπέρυθρη Ακτινοβολία

Η υπέρυθρη ακτινοβολία μπορεί να χρησιμοποιηθεί για την κοινή χρήση δεδομένων μεταξύ συσκευών (P2P). Έχει χαμηλό οικονομικό και ενεργειακό κόστος, αλλά και χαμηλό ποσοστό σφάλματος (low-BER – Bit Error Rate). Το μειονέκτημά του είναι ότι απαιτεί οπτική επαφή (LOS – Line Of Sight) για να λειτουργήσει. Υποστηρίζει επίσης ad-hoc συνδεσιμότητα. Χρησιμοποιείται κυρίως σε εφαρμογές πληρωμής από κινητά τηλέφωνα και φορητούς υπολογιστές.

2.2.2.5 Ασύρματα Τοπικά Δίκτυα (WLAN)

Το WLAN εφαρμόζει τεχνολογίες ασύρματης διαμόρφωσης, όπως η διασπορά φάσματος (spread spectrum) και πολυπλεξία συχνότητας ορθογωνίων φερουσών (OFDM – Orthogonal Frequency-Division Multiplexing), ώστε να διασυνδεθούν πολλές συσκευές παράλληλα, στα πλαίσια ενός περιβάλλοντος IoT. Προσφέρει υψηλές ταχύτητες μετάδοσης δεδομένων, καθιστώντας το ιδανικό για χρήση σε οικιακά δίκτυα. Δεν υπάρχει κόστος εγκατάστασης και προωθεί τη διασύνδεση πολλών συσκευών, βασιζόμενο στα πρότυπα IEEE 802.11.

2.2.2.6 Κινητές Τηλεπικοινωνίες

Η κινητή τηλεφωνία ξεκίνησε με τη χρήση αναλογικών κυψελωτών δικτύων (1G) και στη συνέχεια ακολούθησαν τα ψηφιακά κυψελωτά δίκτυα (2G-GSM) και το GPRS (General Packet Radio Service). Στην παρούσα φάση επικρατούν τα πρότυπα 3G, ενώ το 4G εξαπλώνεται σταδιακά.

Η τεχνολογία 3G είναι ένα σύνολο προτύπων που ενσωματώνουν τις προτάσεις IMT-2000 (International Mobile Telecommunications 2000) της διεθνούς ένωσης τηλεπικοινωνιών (ITU) για κινητά τηλέφωνα και τηλεπικοινωνιακές υπηρεσίες. Αυτές οι υπηρεσίες είναι για παράδειγμα πρόσβαση στο Διαδίκτυο από κινητές συσκευές, τηλεφωνικές κλήσεις και βιντεοκλήσεις μέσω Διαδικτύου, αλλά και τηλεόραση σε κινητά τηλέφωνα. Τα πρότυπα 3G περιλαμβάνουν την πολυπλεξία κώδικα (WCDMA) και την πολυπλεξία διαίρεσης χρόνου (TDMA). Ουσιαστικά, το IMT-2000 επιχειρεί να συνδυάσει τα πλεονεκτήματα του GSM και του GPRS με αυτά του Διαδικτύου δημιουργώντας το παγκόσμιο πρότυπο συστήματος τηλεπικοινωνιών UMTS (Universal Mobile Telecommunications System).

Η τεχνολογία 4G αναμένεται να κυριαρχήσει στον τομέα των κινητών επικοινωνιών. Ουσιαστικά είναι ένας συνδυασμός τεχνολογιών 3G και WLAN, η εξέλιξη του 3G με

έμφαση στο εύρος ζώνης. Στο περιβάλλον IoT, η σύγκλιση σταθερών, κινητών και ασύρματων επικοινωνιών καθίσταται απαραίτητη για την επίτευξη υψηλών ταχυτήτων και φορητότητας. Θα πρέπει να υπάρχουν υβριδικοί συνδυασμοί τεχνολογιών δικτύου. Σε ένα σύστημα 4G, η πολιτική είναι ότι κάθε κόμβος δικτύου έχει μια μοναδική διεύθυνση IP. Αυτός ο σχεδιασμός επιτρέπει την τηλεφωνία IP σε πραγματικό χρόνο και τη ροή πολυμέσων. Ο σχεδιασμός 4G ακολουθεί τα πρότυπα Long-Term Evolution (LTE)-Advanced και WirelessMAN – Advanced (IEEE 802.16m). Το 4G βασίζεται στη μετάδοση πακέτων δεδομένων, επομένως θα πρέπει να λαμβάνεται υπόψη η διαχείριση της κυκλοφορίας, ο έλεγχος των «χαμένων» πακέτων και η ποιότητα της υπηρεσίας (QoS).

Το πρότυπο 5G για δίκτυα κινητής τηλεφωνίας αναπτύχθηκε από το 3rd Generation Partnership Project (3GPP) το 2016. Το 3GPP είναι μια διεθνής κοινοπραξία οργανισμών τυποποίησης και βιομηχανικών ομάδων που ανέπτυξαν πρότυπα για προηγούμενες γενιές δικτύων. Το πρότυπο 5G ξεκίνησε την παγκόσμια ανάπτυξη το 2019, με αυξήσεις στις ταχύτητες και τις ικανότητες μετάδοσης δεδομένων σε σχέση με τα προηγούμενα πρότυπα.

Το ασύρματο δίκτυο επικοινωνίας 6G θα είναι ο διάδοχος του 5G και αναμένεται να ξεκινήσει το 2030. Σημαντικές διαφοροποιήσεις του 6G από το 5G περιλαμβάνουν βελτιωμένη επεκτασιμότητα, μεγαλύτερη χρήση του ραδιοφάσματος και δυναμική πρόσβαση σε διαφορετικούς τύπους σύνδεσης. Αυτό θα επιτρέψει μεγαλύτερη αξιοπιστία και θα περιορίσει τις πτώσεις στη σύνδεση, κάτι που είναι κρίσιμο για την υποστήριξη προηγμένων τεχνολογιών όπως τα drones και τα ρομπότ. Αυτή η δυναμική πρόσβαση θα επιτρέψει στις συνδεδεμένες συσκευές να χρησιμοποιούν πολλές συνδέσεις ταυτόχρονα (π.χ. Wi-Fi και κινητής τηλεφωνίας) για να παραμείνουν συνδεδεμένες ακόμα και αν διακοπεί μία από της συνδέσεις.

2.2.3 Επίπεδο Υποστήριξης και Επεξεργασίας Δεδομένων

Ο όγκος των δεδομένων που πρέπει να μεταφερθούν από το επίπεδο δικτύου είναι τεράστιος, και επομένως είναι απαραίτητο να υπάρχει μια ενδιάμεση υποδομή υλικού και λογισμικού (middleware) για την αποθήκευση και την επεξεργασία των δεδομένων. Middleware ονομάζεται το λογισμικό που βρίσκεται μεταξύ του επιπέδου δικτύωσης και των εφαρμογών. Παρέχει λύσεις σε ζητήματα ετερογένειας, διαλειτουργικότητας και ασφάλειας. Το cloud computing είναι μια βασική τεχνολογία για το σκοπό αυτό [27],

καθώς και για τη διαχείριση της υποδομής των αντικειμένων που συμμετέχουν στο περιβάλλον IoT.

Συγκεκριμένα, όσον αφορά τη διαχείριση οντοτήτων IoT, συμπεριλαμβάνονται αισθητήρες, ενεργοποιητές, πύλες και τερματικοί σταθμοί. Αυτά μπορεί να κατανεμηθούν σε διαφορετικές γεωγραφικές περιοχές. Παράλληλα, εξετάζεται η φυσική υποδομή των αντικειμένων και των απαιτήσεων ενέργειάς τους. Τα στατιστικά στοιχεία αποθηκεύονται για μελλοντική χρήση και λαμβάνονται μέτρα για την προστασία του απορρήτου και της ασφάλειας. Όσον αφορά τη διαχείριση του δικτύου, δίνεται ιδιαίτερη έμφαση στη διαχείριση της υποδομής του δικτύου, στα πρωτόκολλα επικοινωνίας και στις διαδικασίες απόκτησης πρόσβασης. Ειδικότερα, διαχειρίζεται την τοπολογία του δικτύου και τις δομικές του σχέσεις, προκειμένου να διασφαλίζει την αξιοπιστία και τη διαθεσιμότητά του, σε όλα τα κανάλια διανομής δεδομένων. Επιπλέον, δημιουργούνται ετερογενείς μορφές δικτύων, χωρίς να διακυβεύεται η ασφάλεια, προς όφελος της συμβατότητας σε περιβάλλον IoT.

Όπως έχει αναφερθεί προηγουμένως, ο κύριος σκοπός του επιπέδου υποστήριξης ενδιάμεσου λογισμικού είναι η επεξεργασία και αποθήκευση δεδομένων που συλλέγονται από συσκευές IoT. Το IoT είναι ένα παράδειγμα που βασίζεται σε μεμονωμένους διασυνδεδεμένους κόμβους, αλλά αυτοί οι κόμβοι έχουν συνήθως χαμηλές υπολογιστικές δυνατότητες. Αυτό κάνει την αξιοπιστία, την ασφάλεια και την απόδοση να αποτελούν μεγάλο ζήτημα για το IoT. Αντιθέτως, το cloud computing έχει τη δυνατότητα να χειρίζεται πολλά περισσότερα δεδομένα από το IoT, καθώς είναι μια πιο ώριμη τεχνολογία.

Κύριο χαρακτηριστικό του «υπολογιστικού νέφους» είναι η δυνατότητα που προσφέρει η αρχιτεκτονική του, η οποία χωρίζεται σε τρία κύρια επίπεδα, τα οποία αναλύονται διαδοχικά. Αυτές οι υπηρεσίες περιλαμβάνουν ουσιαστικά την παροχή μιας υποδομής (IaaS), την παροχή ενός συνόλου υπηρεσιών (SaaS) και την παροχή ενός συνόλου πλατφορμών εργασίας (PaaS). Το IaaS (Υποδομή ως Υπηρεσία) αναφέρεται στην παροχή επεξεργαστικής ισχύος, χώρου αποθήκευσης και υποδομής δικτύου, δίνοντας έτσι τη δυνατότητα στους καταναλωτές να ελέγχουν το αντίστοιχο λειτουργικό σύστημα και όλες τις λειτουργίες του. Το SaaS (Λογισμικό ως Υπηρεσία) αναφέρεται στην πρόσβαση σε εφαρμογές που «τρέχουν» σε περιβάλλον «νέφους». Η πρόσβαση σε αυτές τις εφαρμογές γίνεται συνήθως μέσω ενός προγράμματος περιήγησης ιστού. Το PaaS (Πλατφόρμα ως Υπηρεσία) αναφέρεται στην παροχή πλατφορμών που υποστηρίζουν διάφορα λειτουργικά συστήματα, υλικολογισμικό και πλήρη πλαίσια

εργασίας. Στο παρακάτω σχήμα φαίνονται παραδείγματα υπηρεσιών «υπολογιστικού νέφους» [28] τα οποία αποτελούν υποκατηγορίες των τριών παραπάνω επιπέδων:

Πίνακας 2.1 Υπηρεσίες «υπολογιστικού νέφους»

Anything as a service	Description
Things as a service	Συγκέντρωση και αφαίρεση ετερογενών πόρων σύμφωνα με προσαρμοσμένη σημασιολογία
Sensing as a service	Παροχή πανταχού παρούσας πρόσβασης σε δεδομένα αισθητήρων
Sensing and Actuation as a service	Ενεργοποίηση λογικών αυτόματου ελέγχου που εφαρμόζονται στο Cloud
Sensor Event as a service	Αποστολή υπηρεσιών ανταλλαγής μηνυμάτων που ενεργοποιούνται από συμβάντα αισθητήρων
Sensor as a service	Επιτρέποντας την πανταχού παρούσα διαχείριση των απομακρυσμένων αισθητήρων
DataBase as a service	Ενεργοποίηση της πανταχού παρούσας διαχείρισης βάσεων δεδομένων
Data as a service	Παροχή πανταχού παρούσας πρόσβασης σε κάθε είδους δεδομένα
Ethernet as a service	Παροχή πανταχού παρούσας συνδεσιμότητας επιπέδου-2 σε απομακρυσμένες συσκευές
Identify and Policy Management as a service	Επιτρέποντας την πανταχού παρούσα πρόσβαση σε λειτουργίες διαχείρισης πολιτικής και ταυτότητας
Video Surveillance as a service	Παροχή πανταχού παρούσας πρόσβασης σε εγγεγραμμένο βίντεο και υλοποίηση σύνθετων αναλύσεων στο Cloud

Το IoT και το «υπολογιστικό νέφος» είναι δύο τεχνολογίες στις οποίες γίνεται αντιληπτό ότι αλληλοσυμπληρώνονται, παρόλο που έχουν ακολουθήσει ανόμοια πορεία ανάπτυξης. Η συμπληρωματικότητά τους επιδεικνύεται με κάποια παραδείγματα στο παρακάτω πίνακα:

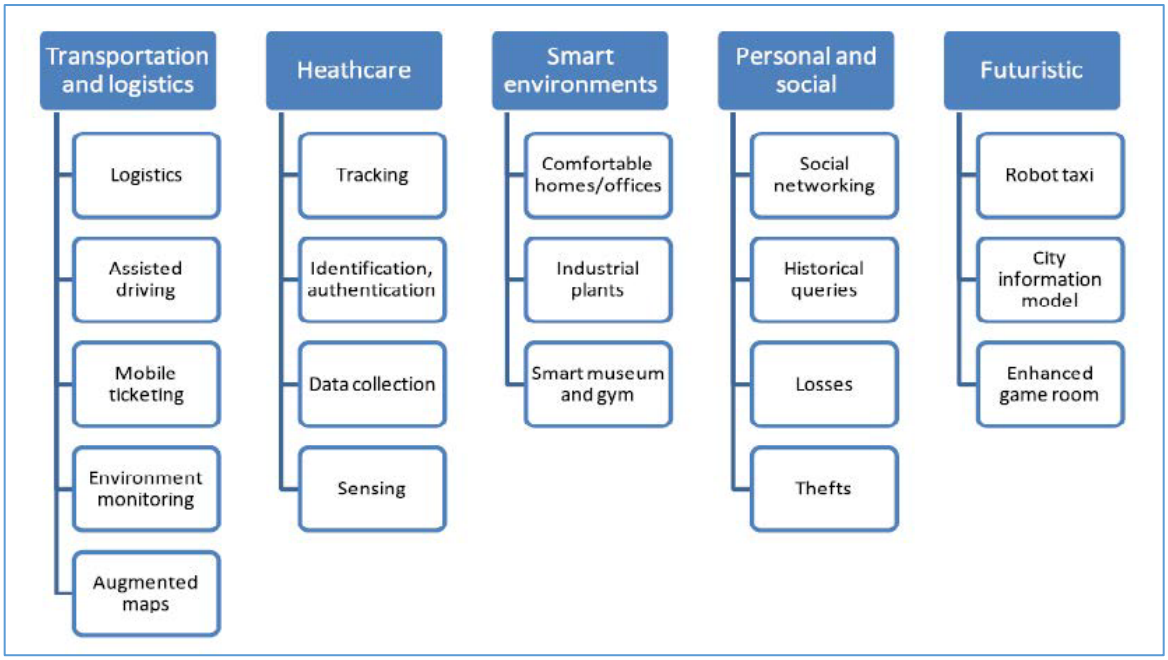
Πίνακας 2.2 Συμπληρωματικότητα IoT & Cloud

	IoT	Cloud
Μετατόπιση	Διαχυτική	Συγκεντρωτική
Προσβασιμότητα	Περιορισμένη	Από παντού
Εξαρτήματα	Πραγματικά πράγματα	Εικονικοί πόροι
Υπολογιστικές δυνατότητες	Περιορισμένες	Εικονικά απεριόριστες
Χώρος αποθήκευσης	Περιορισμένος ως καθόλου	Εικονικά απεριόριστος
Ρόλος του Διαδικτύου	Σημείο σύγκλισης	Μέσα για παροχή υπηρεσιών
Μεγάλα δεδομένα	Πηγή	Μέσα διαχείρισης

Συμπερασματικά, η συν-ολοκλήρωση και συγκερασμός των δύο αυτών τεχνολογιών οδηγούν στο γνωστό και ως CloudIoT. Οι δύο αυτές πτυχές γίνονται επαρκώς ευδιάκριτες στο τομέα του αποθηκευτικού χώρου, των επικοινωνιών και των υπολογιστικών δυνατοτήτων.

2.2.4 Επίπεδο Εφαρμογών

Το επίπεδο των εφαρμογών είναι αυτό που αναμορφώνει τα δεδομένα και τις πληροφορίες που επεξεργάστηκαν στο προγενέστερο επίπεδο. Ουσιαστικά, ο μέσος άνθρωπος μέσα από το επίπεδο αυτό συνειδητοποιεί τη δυναμική του IoT. Η συνεισφορά του IoT γίνεται με αυτόν τον τρόπο αισθητή στην καθημερινότητα και σε τομείς όπως η υγεία, τα κοινωνικά δίκτυα, οι μεταφορές, οι εμπορικές εφοδιαστικές αλυσίδες αλλά και η «ευφυία» που αποκομίζουν οι συσκευές ενός «έξυπνου περιβάλλοντος». Στην Εικόνα 2.3 φαίνονται ενδεικτικά κάποιο κάθετοι τομείς και οι IoT πιθανές εφαρμογές τους [29].



Εικόνα 2.3. Τομείς εφαρμογών IoT

Πηγή: https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/1324973/theFile

Οι διάφορες αυτές εφαρμογές και οι τομείς στους οποίους διασκορπίζεται η IoT τεχνολογία, αποδεικνύεται με σιγουριά πως δεν έχουν όμοιες ανάγκες σε δίκτυα, υποδομές και άλλους πόρους, όπως επίσης υπερέχουν και στις συνδεσιμότητες που χρησιμοποιούν. Στο ακόλουθο σχήμα διακρίνονται ενδεικτικά κάποια χαρακτηριστικά των εφαρμογών IoT.

Πίνακας 2.3 Χαρακτηριστικά εφαρμογών IoT

	Smart Home	**Smart Retail**	**Smart City**	**Smart Agriculture**	**Smart Water**	**Smart Transportation**
Network Size	Small	Small	Medium	Medium / Large	Large	Large
Users	Very few (family)	Few (community)	Many (general public)	Few (landowners)	Few (government)	Large (general public)
Energy	Rechargeable battery	Rechargeable battery	Rechargeable battery, Energy harvesting	Energy harvesting	Energy harvesting	Rechargeable battery, Energy harvesting
Internet Connectivity	WiFi, 3G, 4G LTE backbone	WiFi, 3G, 4G LTE backbone	WiFi, 3G, 4G LTE backbone	WiFi, Satellite	Satellite, Microwave links	WiFi, Satellite
Data Management	Local server	Local server	Shared server	Local & shared servers	Shared server	Shared server
IoT devices	RFID, WSN	RFID, WSN	RFID, WSN	WSN	Single sensors	RFID, WSN, Single sensor
Bandwidth Requirement	Small	Small	Large	Medium	Medium	Medium / Large
Examples	Aware Home	SAP future solutions	Smart Santander	Vineyards with Waspmotes	GBROOS	LocalMotion

2.3 Είδη Αισθητήρων IoT

Προκειμένου οι ασύρματοι αισθητήρες που αποτελούν το δίκτυο IoT να λειτουργούν σωστά, το πρότυπο IEEE 14517 καθιέρωσε την προσθήκη μιας συσκευής μνήμης στο σχεδιασμό τους. Η συσκευή μνήμης αποθηκεύει ένα φύλλο δεδομένων βαθμονόμησης (TEDS - Transducer Electronic Data Sheet) που περιέχει την αναγνώριση του αισθητήρα, τα δεδομένα διόρθωσης και πληροφορίες κατασκευαστή.

Το πρωτόκολλο IEEE 14518 δημιουργήθηκε με στόχο να διευκολύνει τους ανθρώπους να έχουν πρόσβαση σε δεδομένα αισθητήρων από δίκτυα υπολογιστών. Με την αυξανόμενη ισχύ των μικροεπεξεργαστών και την αυξανόμενη δημοτικότητα της τεχνολογίας IoT, το πρωτόκολλο έχει εξελιχθεί ώστε να επιτρέπει ακόμη πιο εξελιγμένους αισθητήρες. Η δυνατότητα της τοπικής επεξεργασίας σημάτων επέτρεψε την επεξεργασία δεδομένων, την ερμηνεία και τη λήψη αποφάσεων [30].

Υπάρχουν πολλοί και διαφορετικοί αισθητήρες IoT για συγκεκριμένους σκοπούς. Στη συνέχεια γίνεται αναφορά σε κάθε έναν από αυτούς.

1. **Αισθητήρας θερμοκρασίας**

   Ένας αισθητήρας θερμοκρασίας είναι, εξ ορισμού, μια συσκευή που χρησιμοποιείται για την αξιολόγηση της ποσότητας θερμικής ενέργειας που επιτρέπει στον χρήστη να

ανιχνεύσει μια φυσική αλλαγή στη θερμοκρασία από μια συγκεκριμένη πηγή, μετασχηματίζοντας τα δεδομένα για μια συσκευή ή χρήστη. Αυτοί οι αισθητήρες IoT χρησιμοποιήθηκαν ως επί το πλείστων για τον έλεγχο του κλιματισμού, των ψυγείων και άλλων συσκευών περιβαλλοντικού ελέγχου μόλις πριν από λίγα χρόνια. Όμως, καθώς το IoT έχει αναπτυχθεί, οι αισθητήρες θερμοκρασίας αξιοποιούνται στους τομείς της μεταποίησης, της γεωργίας και της υγειονομικής περίθαλψης.

2. **Αισθητήρας εγγύτητας (proximity sensor)**

   Ο αισθητήρας εγγύτητας είναι μια συσκευή, χωρίς επαφή, που ανιχνεύει την παρουσία ενός αντικειμένου όταν εισέρχεται στο οπτικό του πεδίο, γνωστό και ως «στόχος». Ανάλογα με τον τύπο του αισθητήρα εγγύτητας, ο αισθητήρας μπορεί να ανιχνεύσει έναν στόχο μέσω ήχου, φωτός, υπέρυθρης ακτινοβολίας (IR) ή ηλεκτρομαγνητικών πεδίων. Τηλέφωνα, εγκαταστάσεις ανακύκλωσης, αυτο-οδηγούμενα αυτοκίνητα, αντιαεροπορικά συστήματα και γραμμές παραγωγής χρησιμοποιούν αισθητήρες εγγύτητας.

3. **Αισθητήρας πίεσης**

   Ο αισθητήρας πίεσης είναι μια συσκευή που ανιχνεύει την πίεση και τη μετατρέπει σε ηλεκτρικό σήμα. Η συσκευή ειδοποιεί τον διαχειριστή του συστήματος για τυχόν αποκλίσεις από το κανονικό εύρος πίεσης και για τυχόν προβλήματα που πρέπει να διορθωθούν. Λόγω της ευκολίας χρήσης τους για τον εντοπισμό αλλαγών πίεσης, αυτοί οι αισθητήρες χρησιμοποιούνται στην παραγωγή και στη συντήρηση ολοκληρωμένων συστημάτων νερού και θέρμανσης.

4. **Αισθητήρας υπερύθρων (infrared – IR)**

   Ο αισθητήρας υπερύθρων είναι ένας αισθητήρας που ανιχνεύει ή εκπέμπει υπέρυθρη ακτινοβολία με σκοπό την ανίχνευση συγκεκριμένων πτυχών του περιβάλλοντός του. Επί του παρόντος χρησιμοποιούνται ιδιαίτερα στην υγειονομική περίθαλψη, διότι διευκολύνουν την παρακολούθηση της ροής του αίματος και της πίεσης. Επίσης, χρησιμοποιούνται σε μια τεράστια ποικιλία κοινών έξυπνων προϊόντων, συμπεριλαμβανομένων των smartphones και των smartwatches.

5. **Γυροσκόπιο**

   Τα γυροσκόπια χρησιμοποιούνται για τη μέτρηση του γωνιακού ρυθμού ή της ταχύτητας γύρο από έναν άξονα. Συχνά χρησιμοποιούνται σε αυτοκίνητα, συστήματα ελέγχου ευστάθειας, ανίχνευση κίνησης για βιντεοπαιχνίδια, προστασία ανθρώπου

από πτώση (man-down) [31], συστήματα ανίχνευσης μετατόπισης κάμερας ή κινητών τηλεφώνων, tablets, κλπ.

6. **Αισθητήρας ανίχνευσης κίνησης**

   Ο ανιχνευτής κίνησης είναι μια ηλεκτρική συσκευή που ανιχνεύει φυσική κίνηση σε μια συγκεκριμένη περιοχή και μετατρέπει αυτή την κίνηση σε ηλεκτρικό σήμα. Μπορεί να ανιχνεύσει την κίνηση οποιουδήποτε αντικειμένου ή προσώπου.

   Χρησιμοποιούνται κυρίως σε εφαρμογές όπως συστήματα ανίχνευσης εισβολής, αυτόματα χειριστήρια θυρών, έξυπνες κάμερες (λήψη / εγγραφή βάσει κίνησης), θέσεις διοδίων, αυτόματα συστήματα στάθμευσης, αυτοματοποιημένοι νεροχύτες, στεγνωτήρια χεριών, συστήματα διαχείρισης ενέργειας (αυτοματοποιημένος φωτισμός, AC , Fan, Appliances Control).

2.4 Ενσωμάτωση δικτύων WSNs στο IoT

Τα WSNs μπορούν να συνδεθούν σε ένα δίκτυο IP χρησιμοποιώντας τρεις διαφορετικές λύσεις: αρχιτεκτονική διακομιστή μεσολάβησης, δίκτυα με ανοχή καθυστέρησης και μικρο-υλοποίηση TCP/IP.

2.4.1 Proxy Architecture

Η αρχιτεκτονική του διακομιστή μεσολάβησης (Proxy Architecture) είναι ο πιο συνηθισμένος τρόπος σύνδεσης WSN σε δίκτυα IP. Σε αυτή τη μέθοδο, ένα πρόγραμμα ρουτίνας που εκτελείται σε έναν υπολογιστή πύλης αναπτύσσεται μεταξύ του ασύρματου δικτύου αισθητήρων και του δικτύου IP.

Ο διακομιστής μεσολάβησης μπορεί να εκτελεστεί σε δύο λειτουργίες: ως μεταγωγέας ή ως front-end διεπαφή (πρόσθιο άκρο). Στη λειτουργία αναμετάδοσης, ο διακομιστής μεσολάβησης αναμεταδίδει τα δεδομένα IP που προέρχονται από το WSN σε έναν συγκεκριμένο πελάτη στο Διαδίκτυο. Ο πελάτης πρέπει να δηλώσει ενδιαφέρον για ορισμένα δεδομένα με έναν διαθέσιμο διακομιστή μεσολάβησης και, στη συνέχεια, ο διακομιστής μεσολάβησης θα μεταδώσει αυτά τα δεδομένα στον προορισμό. Στη δεύτερη περίπτωση, ο διακομιστής μεσολάβησης θα συλλέξει όλα τα δεδομένα που προέρχονται από το WSN στη βάση δεδομένων και στη συνέχεια θα λειτουργήσει ως διακομιστής βάσης δεδομένων για τον πελάτη σε ένα δίκτυο IP. Οι πελάτες Διαδικτύου μπορούν να υποβάλουν ερωτήματα στον διακομιστή μεσολάβησης για δεδομένα αισθητήρα με διάφορους τρόπους, όπως μέσω ερωτημάτων δομημένης γλώσσας (SQL) ή διεπαφών που βασίζονται στον ιστό.

2.4.2 Delay Tolerant Networks

Τα δίκτυα με ανοχή καθυστέρησης (DTN) έχουν σχεδιαστεί για να χειρίζονται δύσκολες συνθήκες δικτύου, όπως μεγάλη καθυστέρηση, συχνή κοινή χρήση και υψηλά ποσοστά σφαλμάτων bit. Το DTN χρησιμοποιεί μια γενική αρχιτεκτονική όπου τα μηνύματα αποθηκεύονται και στη συνέχεια προωθούνται χρησιμοποιώντας δέσμες (bundles). Το στρώμα δέσμης εφαρμόζεται ως το κορυφαίο στρώμα (top layer). Στην πραγματικότητα, αυτό υλοποιείται στο στρώμα εφαρμογής του πρωτοκόλλου TCP/IP.

Ουσιαστικά το DTN είναι ένα σύνολο διακομιστών που μεταφράζει φιλικά προς τον άνθρωπο ονόματα τομέα σε διευθύνσεις IP. Το DTN είναι υπεύθυνο για τη διατήρηση μιας λίστας διακομιστών με τους οποίους μπορείτε να επικοινωνήσετε για να επιλύσετε ένα όνομα τομέα, τμηματοποίηση μηνυμάτων και αξιοπιστία από άκρο σε άκρο. Κάθε περιοχή έχει μία ή περισσότερες πύλες DTN που θα προωθήσουν μηνύματα πακέτων μεταξύ περιοχών για να φτάσουν στην τελική πύλη DTN που θα παραδώσει το μήνυμα σε κεντρικούς υπολογιστές (host computers) στην περιοχή της.

2.4.3 Micro TCP/IP Implementations

Το uIP (micro-IP) είναι μία υλοποίηση ανοικτού κώδικα της στοίβας πρωτοκόλλου δικτύου TCP/IP που προορίζεται για χρήση με μικροσκοπικούς μικροελεγκτές 8 και 16 bits, καθώς απαιτεί πολύ μικρές ποσότητες κώδικα και μνήμης RAM. Το πρωτόκολλο αρχικά αναπτύχθηκε από τον Adam Dunkels [32] του ομίλου "Networked Embedded Systems" στο Σουηδικό Ινστιτούτο Πληροφορικής, ενώ η ανάπτυξη συνεχίστηκε περαιτέρω από μια ευρεία ομάδα προγραμματιστών [33]. Τον Οκτώβριο του 2008, η Cisco, η Atmel και η SICS ανακοίνωσαν μια πλήρως συμβατή επέκταση IPv6 στο uIP, που ονομάζεται uIPv6.

2.5 Βασικές τεχνολογίες Δικτύωσης WSN & IoT

Οι συσκευές IoT δεν μπορούν να λειτουργήσουν χωρίς τη σύνδεση δικτύου. Για να ενεργοποιηθεί η συνδεσιμότητα μεταξύ ετερογενών έξυπνων συσκευών, χρησιμοποιούνται διάφορες τεχνολογίες δικτύωσης και επικοινωνίας.

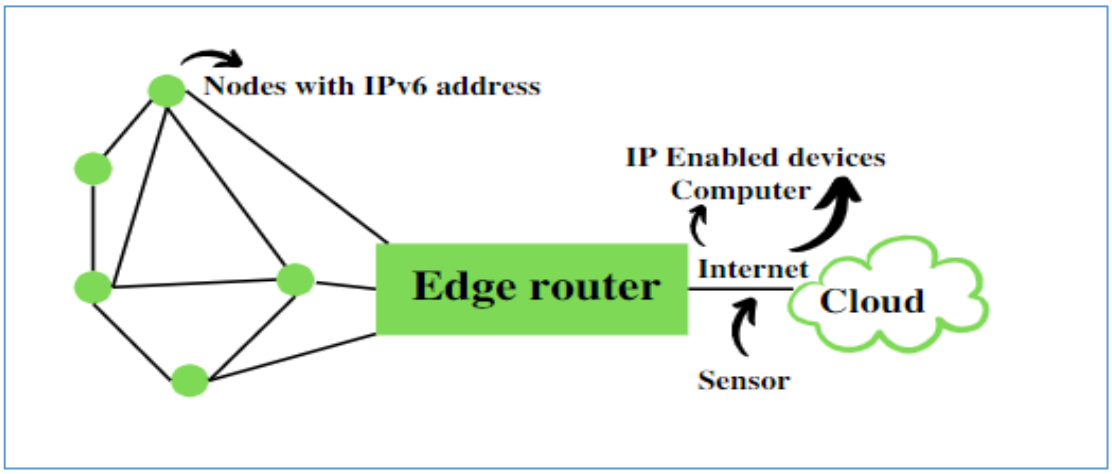
2.5.1 Πρωτόκολλο IPv6 over low-power wireless personal area networks

Το 6LoWPAN είναι ένα πρωτόκολλο IPv6 και επεκτείνεται από το IPv6 μέσω του Προσωπικού Δικτύου Περιοχής χαμηλής ισχύος. Δημιουργήθηκε αρχικά για να ξεπεράσει τις συμβατικές μεθοδολογίες που είχαν προσαρμοστεί για τη μετάδοση

πληροφοριών. Ωστόσο, δεν είναι τόσο αποτελεσματικό, καθώς επιτρέπει μόνο στις μικρότερες συσκευές με πολύ περιορισμένη ικανότητα επεξεργασίας να δημιουργούν επικοινωνία χρησιμοποιώντας ένα από τα Πρωτόκολλα Διαδικτύου, δηλαδή το IPv6. Έχει πολύ χαμηλό κόστος, μικρή εμβέλεια, χαμηλή χρήση μνήμης και χαμηλό ρυθμό μετάδοσης bit. Χρησιμοποιείται με IEEE 802.15.4 στη ζώνη των 2.4 GHz.

- Εύρος εξωτερικού χώρου: ~200 m (μέγιστο)
- Ρυθμός δεδομένων: 200 kbps (μέγιστος)
- Μέγιστος αριθμός κόμβων: ~100

Αποτελείται από έναν δρομολογητή Edge και έναν κόμβο αισθητήρα. Χρησιμοποιείται στον οικιακό αυτοματισμό, σε έξυπνες γεωργικές τεχνικές και στη βιομηχανική παρακολούθηση.



Εικόνα 2.4. Παράδειγμα λειτουργίας 6LoWPAN

Πηγή: https://media.geeksforgeeks.org/wp-content/uploads/20220714142105/Screenshot20220714141952.png

Ακόμη και η μικρότερη από τις συσκευές IoT μπορεί πλέον να είναι μέρος του δικτύου και οι πληροφορίες μπορούν να μεταδοθούν και στον έξω κόσμο. Για παράδειγμα, ένας LED οδικός σηματοδότης.

Πλεονεκτήματα 6LoWPAN:

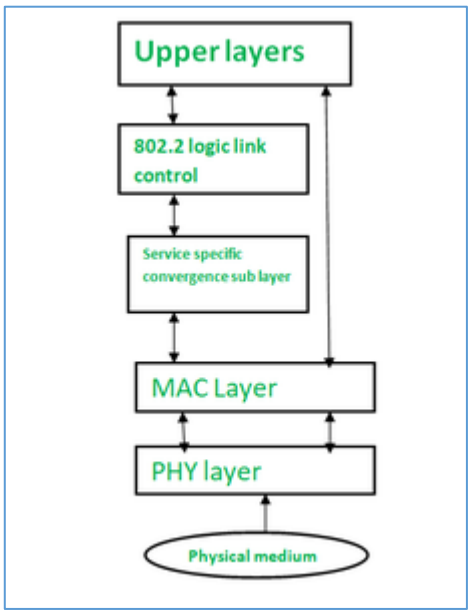
1. Είναι ένα δίκτυο πλέγματος που είναι ισχυρό, επεκτάσιμο και μπορεί να "επουλωθεί" μόνο του.
2. Παρέχει χαμηλού κόστους και ασφαλή επικοινωνία σε συσκευές IoT.
3. Χρησιμοποιεί πρωτόκολλο IPv6 και έτσι μπορεί να δρομολογηθεί απευθείας σε πλατφόρμες cloud.
4. Προσφέρει δρομολόγηση ένα προς πολλά και πολλά προς ένα.

Μειονεκτήματα του 6LoWPAN:

1. Είναι συγκριτικά λιγότερο ασφαλές από το Zigbee.
2. Μεγαλύτερη ευαισθησία σε παρεμβολές σε σύγκριση με το Wi-Fi και το Bluetooth.
3. Αν δεν εφαρμοστεί η τοπολογία πλέγματος, υποστηρίζει μικρή εμβέλεια.

2.5.2 ZigBee & IEEE 802.15.4

Το IEEE 802.15.4 είναι ένα τεχνικό πρότυπο που ορίζει τη λειτουργία ενός ασύρματου προσωπικού δικτύου χαμηλής συχνότητας (LR-WPAN). Καθορίζει το φυσικό επίπεδο (PHY) και τον έλεγχο πρόσβασης μέσων (MAC) για τα LR-WPAN και διατηρείται από την ομάδα εργασίας IEEE 802.15, η οποία καθόρισε το πρότυπο το 2003 [39].



Εικόνα 2.5. Αρχιτεκτονική συσκευής LR-WPAN

Πηγή: https://media.geeksforgeeks.org/wp-content/uploads/20210609162405/iee802154-230x300.png

Η τεχνολογία ZigBee είναι ένα πρωτόκολλο ασύρματης δικτύωσης χαμηλού ρυθμού μετάδοσης δεδομένων, χαμηλής κατανάλωσης ενέργειας, χαμηλού κόστους, που στοχεύει σε εφαρμογές αυτοματισμού και τηλεχειρισμού. Η επιτροπή IEEE 802.15.4 άρχισε να εργάζεται σε ένα πρότυπο χαμηλού ρυθμού δεδομένων λίγο αργότερα. Τότε η ZigBee Alliance και η IEEE αποφάσισαν να ενώσουν τις δυνάμεις τους και το ZigBee είναι το εμπορικό όνομα αυτής της τεχνολογίας.

Το ZigBee παρέχει συνδεσιμότητα χαμηλού κόστους και χαμηλής ισχύος για εξοπλισμό που χρειάζεται διάρκεια μπαταρίας από αρκετούς μήνες έως αρκετά χρόνια,

αλλά δεν απαιτεί ταχύτητες μεταφοράς δεδομένων τόσο υψηλές όσο αυτές που ενεργοποιούνται από το Bluetooth.

Επιπλέον, το ZigBee μπορεί να εφαρμοστεί σε δίκτυα πλέγματος μεγαλύτερα από ό,τι είναι δυνατό με το Bluetooth. Οι ασύρματες συσκευές συμβατές με ZigBee εκπέμπουν σε εμβέλεια 10-75 μέτρων, ανάλογα με το περιβάλλον και την κατανάλωση ισχύος εξόδου που απαιτείται για μια δεδομένη εφαρμογή, και λειτουργούν σε μη αδειοδοτημένη ραδιοσυχνότητα παγκοσμίως (2,4 GHz παγκόσμια, 915 MHz Αμερική ή 868 MHz Ευρώπη). Ο ρυθμός μετάδοσης δεδομένων είναι 250 kbps στα 2,4 GHz, 40 kbps στα 915 MHz και 20 kbps στα 868 MHz.

Για μετάδοση στα 868 MHz, υπάρχουν τρία σχήματα διαμόρφωσης: Δυαδική Μεταλλαγή Μετατόπισης Φάσης (BPSK), μετατόπισης πλάτους (ASK) και Μετατόπιση Τετραγωνικής Φάσης (O-QPSK). Το φυσικό επίπεδο υψηλής ζώνης χρησιμοποιεί συχνότητες που κυμαίνονται από 2,4 GHz έως 2,483 GHz. Παρέχει 16 κανάλια με μέγεθος βήματος 5 MHz και μέγιστο ρυθμό μετάδοσης 250 kb/s. Η διαμόρφωση που χρησιμοποιείται σε αυτή τη ζώνη είναι O-QPSK (Offset Quadrature Phase Shift Keying).

Πίνακας 2.4 Συχνότητες λειτουργίας και ρυθμοί μετάδοσης προτύπου IEEE802.15.4

	Συχνότητα (MHz)	Αριθμός καναλιών	Διαμόρφωση	Chip Rate (Kchip/s)	Bit Rate (kb/s)	Symbol Rate (Ksymbol/s)	Μέθοδος Διασποράς
	868-868.6	1	BPSK	300	20	20	Binary DSSS
	902-928	10	BPSK	600	40	40	Binary DSSS
Προαιρετικά	868-868.6	1	ASK	400	250	12.5	20-bit PSSS
	902-928	10	ASK	1600	250	50	5-bit PSSS
Προαιρετικά	868-868.6	1	O-QPSK	400	100	25	16-array orthogonal
	902-928	10	O-QPSK	1000	250	62.5	16-array orthogonal
	2400-2483.5	16	O-QPSK	2000	250	62.5	16-array orthogonal

Το πρότυπο 802.15.4 ορίζει τις απαιτήσεις ευαισθησίας του δέκτη στα -92 dBm στη χαμηλή ζώνη και στα -85 dBm στην υψηλή ζώνη. Απαιτεί επίσης ικανότητα μετάδοσης ισχύος 1 mW, η οποία μπορεί να διαφέρει ανάλογα με τους υφιστάμενους κανονισμούς και τους περιορισμούς ισχύος μετάδοσης. Η ανάγκη για όλο και υψηλότερους ρυθμούς μετάδοσης και η δυνατότητα χρήσης περισσότερων καναλιών έχει οδηγήσει στη υιοθέτηση ραδιοπομπών που χρησιμοποιούν ζώνες υψηλών συχνοτήτων. Επιπλέον, η τεχνολογία ZigBee χρησιμοποιεί άμεσο φάσμα διασποράς ακολουθίας (Direct – sequence spread spectrum – DSSS) για την αποφυγή παρεμβολών.

Η IEEE και η ZigBee Alliance συνεργάζονται στενά για να καθορίσουν ολόκληρη τη στοίβα πρωτοκόλλων. Το IEEE 802.15.4 εστιάζει στις προδιαγραφές των δύο κατώτερων επιπέδων του πρωτοκόλλου (φυσικό επίπεδο και επίπεδο σύνδεσης δεδομένων). Από την άλλη πλευρά, η ZigBee Alliance στοχεύει να παρέχει τα ανώτερα επίπεδα της στοίβας πρωτοκόλλων (από το δίκτυο στο επίπεδο εφαρμογής) για διαλειτουργική δικτύωση δεδομένων, υπηρεσίες ασφαλείας και μια σειρά ασύρματων λύσεων ελέγχου οικιών και κτιρίων, παροχή δοκιμών συμμόρφωσης διαλειτουργικότητας, μάρκετινγκ , προηγμένη μηχανική για την εξέλιξη του προτύπου. Αυτό διαβεβαιώνει τους καταναλωτές πως αν αγοράσουν προϊόντα από διαφορετικούς κατασκευαστές τα προϊόντα θα συνεργαστούν.

Το IEEE 802.15.4 αναλύει τις προδιαγραφές των PHY και MAC, προσφέροντας δομικά στοιχεία για διαφορετικούς τύπους δικτύωσης γνωστά ως «star, mesh και cluster tree». Τα σχήματα δρομολόγησης δικτύου έχουν σχεδιαστεί για να διασφαλίζουν εξοικονόμηση ενέργειας και χαμηλό λανθάνοντα χρόνο μέσω εγγυημένων χρονοθυρίδων. Ένα μοναδικό χαρακτηριστικό του επιπέδου δικτύου ZigBee είναι ο πλεονασμός της επικοινωνίας που εξαλείφει το "μοναδικό σημείο αστοχίας" σε δίκτυα πλέγματος.

Τα βασικά χαρακτηριστικά του PHY [30]περιλαμβάνουν ανίχνευση ενέργειας και ποιότητας σύνδεσης, σαφή αξιολόγηση καναλιών για βελτιωμένη συνύπαρξη με άλλα ασύρματα δίκτυα. Το υπόστρωμα MAC παρέχει δύο υπηρεσίες: α) την υπηρεσία δεδομένων MAC και β) την υπηρεσία διαχείρισης MAC όπου πραγματοποιείται διασύνδεση με το σημείο πρόσβασης υπηρεσίας οντότητας διαχείρισης υποστρώματος MAC (MLME – MAC Layer Management Entity) (SAP – Service Access Point) (MLMESAP). Η μονάδα δεδομένων πρωτοκόλλου MAC (MPDU – MAC Protocol Data Unit) επιτρέπει τη μετάδοση και λήψη δεδομένων μεταξύ επιπέδων MAC και PHY.
Τα χαρακτηριστικά του υποστρώματος MAC είναι η διαχείριση φάρων, πρόσβαση καναλιών, διαχείριση GTS (Global Trade Services), επικύρωση πλαισίου, αναγνωρισμένη παράδοση πλαισίου, συσχέτιση και αποσύνδεση.

2.5.3 Πρότυπο Bluetooth Low Energy (Bluetooth LE)

Το πρότυπο Bluetooth LE [41] σχεδιάστηκε για εφαρμογές WPAN όπου η χαμηλή κατανάλωση ενέργειας είναι κρίσιμη. Το πρότυπο βασίζεται στο πρωτόκολλο IEEE 802.15.1 και χρησιμοποιεί την ελεύθερη ζώνη συχνοτήτων 2,4 GHz. Η πρόσβαση στα κανάλια γίνεται μέσω πολλαπλής πρόσβασης διαίρεσης συχνότητας (Frequency-division multiple access - FDMA) ή πολλαπλής πρόσβασης διαίρεσης χρόνου (Time-divison multiple access - TDMA). Χρησιμοποιώντας τη πολλαπλή πρόσβαση διαίρεσης

συχνότητας, εκχωρούνται 40 κανάλια εύρους 2 MHz, ενώ χρησιμοποιώντας τη πολλαπλή πρόσβαση διαίρεσης χρόνου, το φυσικό κανάλι χωρίζεται σε χρονικές μονάδες που ονομάζονται γεγονότα (events). Το πρότυπο Bluetooth LE υποστηρίζει ρυθμό μετάδοσης 1 Mbps, που είναι υψηλότερος από την τεχνολογία ZigBee (250 Kbps) και χρησιμοποιεί διαμόρφωση GFSK.

Οι συσκευές που χρησιμοποιούν το πρότυπο αυτό έχουν εμβέλεια έως 50 m και ισχύ εκπομπής κόμβου 10 mW. Για την αποφυγή παρεμβολών, χρησιμοποιείται η τεχνική μεταπήδησης συχνότητας (Adaptive Frequency Hopping - AFH). Τέλος, το πρότυπο έχει τη δυνατότητα υποστήριξης εγκαταστάσεων 232 συσκευών σε τοπολογίες αστεριού, σημείου προς σημείο ή ad hoc. Η συγκριτική παρουσίαση των προτύπων ZigBee και Bluetooth LE αποτυπώνεται στον Πίνακα 2.5

Πίνακας 2.5 Σύγκριση προτύπου ZigBee και Bluetooth LE

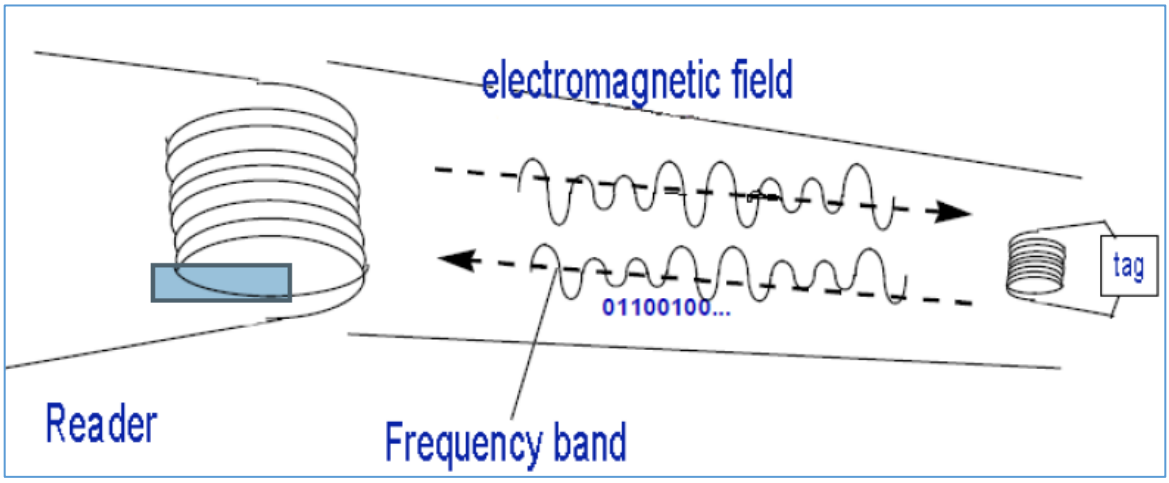
Χαρακτηριστικά	**ZigBee**	**Bluetooth LE**
Συχνότητα λειτουργίας	2400 / 915 / 868 MHz	2.4 GHz
Εμβέλεια	100 m	50 m
Ρυθμός μετάδοσης	20 – 2500 Kbps	1 Mbps
Ισχύς εκπομπής	Έως 30 mW	10 mW
Μέγεθος πακέτου δεδομένων	127 bytes	27 bytes
Μηχανισμός αποφυγής παρεμβολών	DSSS	AFH
Πλήθος υποστηριζόμενων συσκευών	2^{16}	2^{32}
Τοπολογίες	Star, Mesh, Cluster-Tree	Star, Ad hoc, Point-to-Point
Διαμόρφωση	O-QPSK / BPSK	GFSK
Ασφάλεια	AES 128 bit	AES 128 bit
Χρόνος ζωής	6 μήνες – 2 χρόνια	1 – 2 χρόνια

2.5.4 RFID (Radio Frequency Identification)

Στην τεχνολογία RFID, οι ετικέτες (tags) χρησιμοποιούνται για την αποθήκευση δεδομένων και οι αναγνώστες (readers) για την ανάκτηση αυτών των δεδομένων από τις ετικέτες, ενώ η τεχνολογία ασύρματου δικτύου αισθητήρων περιλαμβάνει μικρές έξυπνες διασυνδεδεμένες συσκευές ανίχνευσης με εκτεταμένες εγκαταστάσεις ασύρματης επικοινωνίας. Από τα αρχικά τους στάδια, τα συστήματα RFID έχουν χρησιμοποιηθεί επιτυχώς για την επισήμανση ζώων [40], τη συλλογή διοδίων [41], τα συστήματα WSN

στην περιβαλλοντική παρακολούθηση [42], τη ρομποτική [43], και τα WSN που βασίζονται σε πλατφόρμες κινητικής ανίχνευσης έχουν χρησιμοποιηθεί για πιο ποικίλες εφαρμογές.

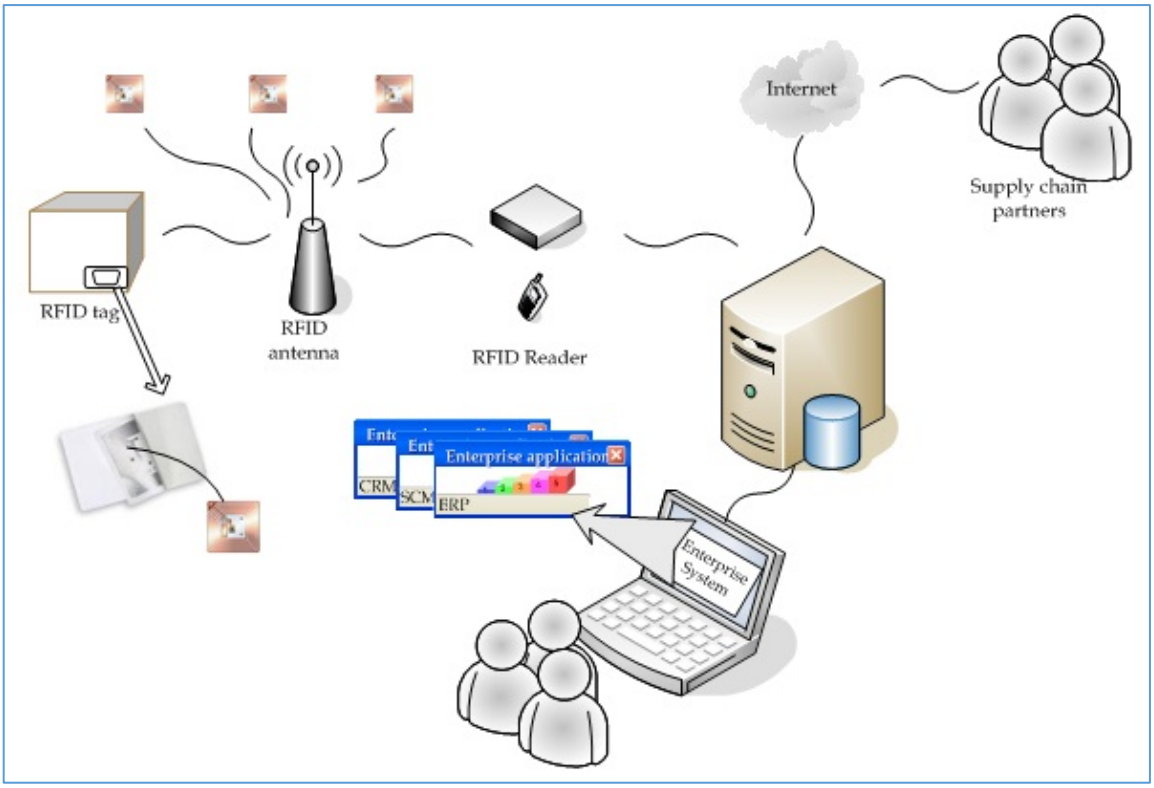
Οι ετικέτες RFID είναι μικροτσίπ συνδυασμένα με κεραία ραδιοφώνου, προσαρτημένα σε αντικείμενα ή συνδεδεμένα με άτομα για αναγνώριση και παρακολούθηση. Δίνουν περιοδικά τον μοναδικό ηλεκτρονικό κωδικό προϊόντος τους (Electronic Product Code) μέσω σήματος RF όταν βρίσκονται στην περιοχή ανάγνωσης των συσκευών ανάγνωσης RFID. Οι συσκευές ανάγνωσης που ενεργοποιούνται π.χ. σε έξυπνα κτίρια αναζητούν και διαβάζουν EPC από ετικέτες μέσω σήματος RF, ενημερώνουν το EPC στις υπηρεσίες πληροφοριών EPC που αποτελούν μέρος της διαμόρφωσης RFID ή ενός αυτόνομου συστήματος [44].



Εικόνα 2.6. RFID Αναγνώστης και Ετικέτα

Πηγή: https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/1324973/theFile

Η ρύθμιση διαμόρφωσης υποστηρίζεται από ένα HIDSS (Hybrid Intelligent Decision Support System), το οποίο είναι ένα υβριδικό έξυπνο σύστημα υποστήριξης αποφάσεων που αποτελείται από στοιχεία παρακολούθησης και λήψης αποφάσεων σε πραγματικό χρόνο. Αυτές οι δύο τεχνολογίες βασίζονται στη χρήση συμβατικών τεχνολογιών αισθητήρων. Στα WSN, οι περιορισμοί της ενεργειακής ικανότητας των κόμβων αισθητήρων μπορούν να αντισταθμιστούν με τη χρήση πολύ φθηνών ετικετών RFID για την κοντινή τους ανάγνωση, ενώ οι ικανότητές τους ανίχνευσης δεν είναι τόσο καλές όσο αυτές των κόμβων αισθητήρων WSN.



Εικόνα 2.7. Χρήση RFID στη Διαχείριση Εφοδιαστικής Αλυσίδας για Κατασκευαστική Ψηφιακή Επιχείρηση

Πηγή: https://www.intechopen.com/media/chapter/18524/media/image3.jpeg

Μεγάλη σημασία στο ενσωματωμένο εννοιολογικό πλαίσιο WSN-RFID είναι οι προδιαγραφές του αναγνώστη RFID που επιτρέπουν τη δημιουργία εκτεταμένων δυνατοτήτων υποστήριξης που θα διαμορφωθούν στο HIDSS [45]. Ο κόμβος αισθητήρα WSN συνδέεται με τη συσκευή ανάγνωσης RFID για να επιτρέψει στον κόμβο αισθητήρα να επικοινωνεί με συμβατές συσκευές. Το μοντέλο δεδομένων έχει σχεδιαστεί για να υποστηρίζει αποτελεσματικά το πρωτόκολλο επικοινωνίας κατά την ανάγνωση των διαφορετικών ετικετών που χρησιμοποιούνται στη ρύθμιση. Αυτό απαιτεί την ανάπτυξη περίτεχνων πολυτροπικών διεπαφών για έναν εξαιρετικά πανταχού παρόν και διάχυτο υπολογισμό για τη μείωση της πολυπλοκότητας της υλοποίησης τέτοιων διαμορφώσεων και τη βελτίωση της αποτελεσματικότητας και της λειτουργικότητας των ενεργοποιημένων υπηρεσιών. Οι απαιτήσεις διεπαφής παρατίθενται παρακάτω [46]:

- Η ενσωμάτωση ετικετών RFID και συσκευών ανάγνωσης στη διαμόρφωση του συστήματος απαιτεί ασύρματη ή ενσύρματη σύνδεση μέσω USB/σειριακής θύρας μεταξύ της συσκευής ανάγνωσης, ετερογενών συσκευών και του συστήματος που

θα ανοίξει χρησιμοποιώντας μια διεπαφή προγραμματισμού εφαρμογής για την υλοποίηση μιας κατανεμημένης ενοποιημένης διεπαφής .

- Η ανταλλαγή δεδομένων μεταξύ των ετικετών RFID και του συστήματος απαιτεί την αποθήκευση στο σύστημα όλων των δεδομένων ανίχνευσης μεμονωμένης διαδρομής, εμφανίζοντας τη μεμονωμένη θέση εντοπισμού.
- Μοναδικό αναγνωριστικό ανά ετικέτα σε πολλαπλές αναγνώσεις ετικετών.
- Το φιλτράρισμα δεδομένων για την εξάλειψη ασήμαντων δεδομένων που πρέπει να μεταδοθούν στον διακομιστή.
- Πλήρης κάλυψη ζώνης αναγνώστη RFID.
- Ανίχνευση ετικετών "παιδιών" σε οποιοδήποτε μέρος της ζώνης κάλυψης του αναγνώστη.
- Το HIDSS πρέπει να μπορεί να δημιουργεί και να στέλνει ειδοποιήσεις σε ετικέτες RFID (δόνηση), έξυπνες συσκευές υπολογιστών και συσκευές χειρός μέσω SMS και email.
- Το ολοκληρωμένο σύστημα RFID αναπτύσσεται σε ένα WSN και η ανάπτυξη και η διαμόρφωσή τους υποστηρίζονται από το HIDSS.

2.5.5 NFC (Near Field Communication)

Σύμφωνα με το υπάρχον σύστημα WSN, ο χρήστης συλλέγει δεδομένα μόνο από το Operation Center Server. Ωστόσο, αυτού του είδους η παραδοσιακή μέθοδος συλλογής έχει ορισμένα μειονεκτήματα. Δεν είναι τόσο εύκολο στη χρήση, επειδή ο χρήστης χρειάζεται κάποιες βασικές γνώσεις δικτύου για τη λήψη δεδομένων από τον διακομιστή. Κάθε υποκόμβος αισθητήρα εξαρτάται από τον κύριο κόμβο και τον διακομιστή (βάση δεδομένων), με αποτέλεσμα ο χρήστης να μη μπορεί να λάβει δεδομένα απευθείας από τον κόμβο αισθητήρα. Επίσης, δεν είναι εύκολη η αλλαγή των παραμέτρων συλλογής δεδομένων αισθητήρα μέσα στον υποτελή κόμβο από τον χρήστη. Έτσι δημιουργήθηκε η ανάγκη για βελτίωση ως προς την ανάκτηση δεδομένων και την αλλαγή των παραμέτρων. Ο σχεδιασμός ενός πιο απλού, ασφαλούς, εύκολου και διαισθητικού τρόπου λήψης δεδομένων από κόμβους αισθητήρων ή αλλαγής εσωτερικών παραμέτρων κόμβων είναι απαιτητικός. Το Near Field Communication (NFC) είναι μια τεχνολογία ασύρματης συνδεσιμότητας μικρής εμβέλειας που παρέχει διαισθητική, απλή και ασφαλή επικοινωνία μεταξύ ηλεκτρονικών συσκευών. Η επικοινωνία πραγματοποιείται όταν δύο συσκευές συμβατές με NFC βρίσκονται σε απόσταση τεσσάρων εκατοστών η μία από

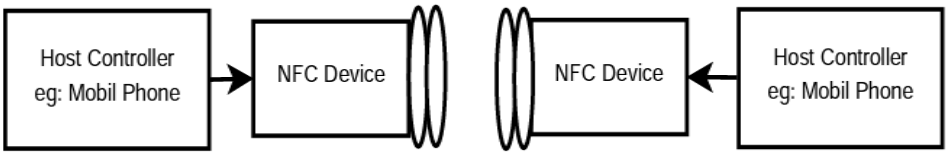
την άλλη. [47] Με αυτό το σύστημα, δημιουργείται ένα εξαιρετικά φιλικό προς τον χρήστη σύστημα όπου ο χρήστης μπορεί να χρησιμοποιήσει το NFC για να ανακτήσει δεδομένα απευθείας από τον κόμβο αισθητήρα μέσω tablet ή έξυπνου τηλεφώνου. [48]

Το NFC είναι μια τεχνολογία ανοιχτής πλατφόρμας, η οποία λειτουργεί στα 13,56 MHz (εκτείνεται σε RFID) και συνήθως απαιτεί απόσταση 10 cm ή μικρότερη. Έχει εμπλακεί στην καθημερινότητά μας ασυνείδητα όπως σε ανέπαφες πληρωμές, έκδοση εισιτηρίων, σύζευξη συσκευών bluetooth και εάν διαθέτετε έξυπνη κλειδαριά στο σπίτι σας, μπορείτε να χρησιμοποιήσετε την ετικέτα (tag) NFC για να κλειδώσετε ή να ξεκλειδώσετε την πόρτα σας [49] [50]. Επομένως, αρκετοί οργανισμοί δημιουργούν τα δικά τους πρότυπα που ορίζονται από τον Διεθνή Οργανισμό Τυποποίησης (ISO), την Ecma International και τη Sony. Αυτά τα πρότυπα καθορίζουν όχι μόνο το περιβάλλον λειτουργίας "Άμεσης επαφής", όπως οι φυσικές απαιτήσεις των κεραιών, αλλά και τη μορφή των δεδομένων που θα μεταφερθούν και τους ρυθμούς δεδομένων για τη μεταφορά αυτή.

Το ISO/IEC 18092 είναι το πρώτο επίσημο πρότυπο για το NFC, το οποίο ορίζει τρόπους επικοινωνίας για τη διεπαφή και το πρωτόκολλο Near Field Communication Interface and Protocol (NFCIP-1) με χρήση επαγωγικών συζευγμένων συσκευών που λειτουργούν στην κεντρική συχνότητα των 13,56 MHz για συσκευές. Αυτό το πρότυπο δημιουργείται για την επικοινωνία μεταξύ συσκευών peer-to-peer. Αυτό το πρότυπο καθορίζει τη διεπαφή RF, την προετοιμασία, το πρωτόκολλο μεταφοράς και τις μεθόδους ανταλλαγής δεδομένων. Επίσης, το πρότυπο Ecma-340 είναι εναρμονισμένο με το ISO/IEC 18092 και αναφέρονται στα πρότυπα μεθόδου δοκιμής NFCIP-1, ECMA-356 και ECMA-352. Έτσι, το ISO/IEC 180092 και το ECMA-340 [51] είναι σχεδόν τα ίδια πρότυπα. Το πρωτόκολλο NFCIP – 1 έχει τρεις τρόπους λειτουργίας για την ικανοποίηση διαφορετικών απαιτήσεων χρήστη και η ταχύτητα μετάδοσης δεδομένων κυμαίνεται από 106Kbit/s έως 424Kbit/s.

- **Λειτουργία Peer-to-Peer** [52]: σε αυτή τη λειτουργία, δύο συσκευές NFC μπορούν να επικοινωνούν μαζί, μια συσκευή λειτουργεί ως εκκινητής, μια άλλη συσκευή ως ο στόχος. Για να ξεκινήσει η επικοινωνία με τον στόχο είτε σε ενεργή είτε σε παθητική λειτουργία επικοινωνίας, ένας εκκινητής απαιτεί συνεχώς την παρουσία ενός εξωτερικού πεδίου ραδιοσυχνοτήτων. Σε λειτουργία ενεργής επικοινωνίας, και οι δύο συσκευές δημιουργούν το δικό τους πεδίο RF. Έτσι, σε αυτήν τη λειτουργία, και οι δύο συσκευές πρέπει να έχουν τροφοδοτικό. Ενώ υπό παθητική λειτουργία, μόνο η συσκευή εκκινητή δημιουργεί πεδίο

ραδιοσυχνοτήτων, η συσκευή στόχος λαμβάνει τη λειτουργική της ισχύ από το πεδίο RF του εκκινητή, γεγονός που κάνει τη συσκευή-στόχο να μην χρειάζεται τροφοδοσία ρεύματος.



Εικόνα 2.8. Παράδειγμα επικοινωνίας peer-to-peer με χρήση NFC

Πηγή: https://www.diva-portal.org/smash/get/diva2:613332/FULLTEXT01.pdf

- **Λειτουργία ανάγνωσης/εγγραφής**: σε αυτή τη λειτουργία, η συσκευή NFC μπορεί να διαβάζει/εγγράφει δεδομένα από/προς μια ανέπαφη έξυπνη κάρτα που είναι συμβατή με τα πρωτόκολλα ISO14443 ή FeliCa [53]
- **Λειτουργία εξομοίωσης κάρτας NFC**: σε αυτή τη λειτουργία, μια συσκευή βλέπει μια άλλη συσκευή NFC ως ανέπαφη κάρτα.

2.5.6 Ανταγωνιστικά πρότυπα WSN

Έχουν επίσης αναπτυχθεί για εφαρμογές WSN, τα ανταγωνιστικά πρότυπα EnOcean, DASH7, RuBee και Isa100.11.a [54] και στον Πίνακα 2.6 αποτυπώνεται η συγκριτική παρουσίαση των βασικών χαρακτηριστικών τους, σε σχέση αυτά των 6LoWPAN, ZigBee και Bluetooth LE που έχουν ήδη αναφερθεί σε προηγούμενες ενότητες.

Πίνακας 2.6 Σύγκριση προτύπων WSN

Πρότυπο	Συχνότητα λειτουργίας	Ρυθμός μετάδοσης	Εμβέλεια
6LoWPAN	2.4 GHz	20 – 250 Kbps	10 – 30 m
RuBee	131 KHz	1.2 Kbps	30 m
Bluetooth LE	2.4 GHz	1 Mbps	50 m
Isa100.11.a	2.4 GHz	250 Kbps	100 m
ZigBee	2400 / 915 / 868 MHz	Έως 250 Mbps	100 m
EnOcean	868 / 315 MHz	125 Kbps	300 m
DASH7	433 KHz	200 Kbps	2 km

3. Ασφάλεια και ιδιωτικότητα στο Διαδίκτυο των Πραγμάτων

Ένα περιβάλλον Διαδικτύου των Πραγμάτων θα πρέπει να σχεδιαστεί με τρόπο που να διασφαλίζει την ασφάλεια, ενώ παράλληλα να είναι εύκολο στη χρήση. Οι πιθανοί χρήστες πρέπει να πειστούν για αυτές τις ιδιότητες προκειμένου να απολαμβάνουν τα οφέλη του IoT αποφεύγοντας παράλληλα μη ασφαλείς λύσεις.

Στο πλαίσιο του IoT, όλα τα «έξυπνα» αντικείμενα έχουν τη δυνατότητα να συνδέονται στο Διαδίκτυο και να επικοινωνούν με άλλα «έξυπνα» αντικείμενα, δημιουργώντας έτσι νέα είδη ζητημάτων ασφάλειας και απορρήτου. Υπό αυτές τις συνθήκες, όλο και περισσότερα ζητήματα ασφάλειας προκύπτουν καθώς τα αντικείμενα γίνονται πιο αυτόνομα και αναλαμβάνουν πρωτοβουλίες. Στο πλαίσιο της ασφάλειας του υπολογιστικού συστήματος, και συνεπώς του IoT, οι βασικές αρχές που πρέπει να διασφαλιστούν είναι οι εξής:

- Εμπιστευτικότητα
- Ιδιωτικότητα
- Ακεραιότητα
- Διαθεσιμότητα
- Πιστοποίηση Ταυτότητας
- Έλεγχος Πρόσβασης
- Αξιοπιστία

3.1 Βασικές Απαιτήσεις Ασφάλειας στο Διαδίκτυο των Πραγμάτων

Οι βασικές απαιτήσεις ασφάλειας στο Διαδίκτυο των Πραγμάτων [34] [35] [36] συνοψίζονται ως εξής:

- ***Εμπιστευτικότητα***

  Οι υπηρεσίες IoT είναι πιθανό να περιέχουν «ευαίσθητα» δεδομένα και πληροφορίες, για το λόγο αυτό, όλα τα αντικείμενα IoT πρέπει να είναι ασφαλισμένα σε σχέση με τους χρήστες που τα διαχειρίζονται. Η εμπιστευτικότητα μπορεί να επιτευχθεί μέσω συμμετρικής ή ασύμμετρης κρυπτογράφησης (κρυπτογράφηση δημόσιου κλειδιού). Ωστόσο, ο τύπος κρυπτογράφησης που θα επιλεγεί εξαρτάται από τις υπολογιστικές δυνατότητες κάθε αντικειμένου. Για παράδειγμα, στο περιβάλλον ενός «έξυπνου» σπιτιού, όπου υπάρχουν πληροφορίες για τις δραστηριότητες των ενοίκων, οι ίδιοι δεν θα ήθελαν κανένας επισκέπτης να έχει πρόσβαση σε τέτοια δεδομένα παρατηρώντας απλώς «έξυπνες» συσκευές.

- ***Ιδιωτικότητα***

  Το IoT μπορεί να χρησιμοποιηθεί σε πολλούς διαφορετικούς τομείς της ζωής όπου εμπλέκονται προσωπικά δεδομένα των χρηστών, όπως η διαχείριση της κυκλοφορίας, η παροχή ιατρικής περίθαλψης και η κατηγοριοποίηση των καταναλωτών σύμφωνα με τις αγοραστικές τους προτιμήσεις. Οι τεχνικές που χρησιμοποιούνται για τον έλεγχο ροής πληροφοριών (Information Flow Control), επιτρέπουν στα μεταδιδόμενα δεδομένα να χαρακτηρίζονται με στοιχεία που καθορίζουν τον λόγο μεταφοράς και ύπαρξής τους, προστατεύοντας έτσι το απόρρητο του χρήστη με μόνο μειονέκτημα την απαίτηση σημαντικής υπολογιστικής ισχύος. Ταυτόχρονα, μπορούν να χρησιμοποιηθούν πρωτόκολλα ελέγχου πρόσβασης, βασισμένα σε τεχνικές που προστατεύουν την ανωνυμία (context-aware k-anonymity). Επιπλέον, μπορεί να χρησιμοποιηθεί μια τεχνική για την επίτευξη ανωνυμίας. Αυτό ονομάζεται CASTLE (Continuously Anonymizing Streaming data via adaptive cLuestEring) και δίνει έμφαση στη «φρεσκάδα» και τον περιορισμό των καθυστερήσεων δεδομένων. Στη συνέχεια, ένα βελτιωμένο σύστημα DNS προστατεύει το απόρρητο με το να μην εκχωρεί ένα όνομα τομέα σε έναν κόμβο IoT και να απαιτεί έλεγχο ταυτότητας χρήστη πριν από την παραχώρηση πρόσβασης.

- ***Ακεραιότητα***

  Στο πλαίσιο του Διαδικτύου των Πραγμάτων, σημαντικά δεδομένα ανταλλάσσονται επίσης με οντότητες όπως κυβερνητικές υπηρεσίες, πάροχοι υπηρεσιών Διαδικτύου (ISP) και μηχανισμοί ελέγχου, κάτι που απαιτεί τα δεδομένα που μεταδίδονται και αποθηκεύονται να μην παραβιάζονται. Η ακεραιότητα των δεδομένων είναι πρωταρχικής σημασίας κατά τη δημιουργία αξιόπιστων συστημάτων IoT, και αυτό επιτυγχάνεται με κωδικούς ελέγχου ταυτότητας μηνυμάτων (MAC) που χρησιμοποιούν συναρτήσεις κατακερματισμού. Η επιλογή αυτών των τεχνικών καθορίζεται από τις δυνατότητες κάθε συσκευής. Ένα χαρακτηριστικό παράδειγμα όπου η ακεραιότητα των δεδομένων είναι εξ ορισμού απαραίτητη είναι το «έξυπνο» σπίτι το οποίο είναι συνδεδεμένο σε ένα «έξυπνο» δίκτυο ηλεκτρικής ενέργειας. Στην περίπτωση αυτή, η ηλεκτρονική και αυτόματη έκδοση των λογαριασμών δεν συνάδει με πιθανή αλλοίωση των στοιχείων κατανάλωσης ηλεκτρικής ενέργειας.

- ***Διαθεσιμότητα***

  Σε ένα σύγχρονο περιβάλλον IoT, είναι αναπόφευκτο οι κόμβοι να λειτουργούν ως διακομιστές. Στο πλαίσιο ενός «έξυπνου» σπιτιού, για παράδειγμα, θα υπάρχουν

συσκευές – κόμβοι που θα αναμεταδίδουν δεδομένα δικτύου όπως κατανάλωση ενέργειας, εικόνες από οικιακές κάμερες και την κατάσταση του συναγερμού. Είναι πολύ σημαντικό αυτές οι πληροφορίες να είναι διαθέσιμες ανά πάσα στιγμή σε όσους τις χρειάζονται. Ωστόσο, κανένα πρωτόκολλο ασφαλείας από μόνο του δεν διασφαλίζει τη διαθεσιμότητα δεδομένων και υπηρεσιών στα ενδιαφερόμενα μέρη. Απαιτείται ένας συνδυασμός τεχνικών και πολλαπλών μετρήσεων πραγματικών δεδομένων για τον προσδιορισμό του ποσοστού διαθεσιμότητας. Αυτό μπορεί να είναι δύσκολο να γίνει και συχνά γίνεται ως μέρος συμφωνιών επιπέδου υπηρεσιών (service level agreements - SLAs) μεταξύ παρόχων και πελατών.

- ***Πιστοποίηση Ταυτότητας***

  Οι συσκευές IoT απαιτούν πιστοποίηση ταυτότητας (ή αλλιώς αυθεντικοποίηση), προκειμένου να διασφαλιστεί ότι τόσο ο αποστολέας όσο και ο παραλήπτης είναι σίγουροι για την ταυτότητα του άλλου. Αυτό είναι ιδιαίτερα σημαντικό κατά την αποστολή δεδομένων μεταξύ δύο μερών, καθώς η συσκευή που παρέχει τα δεδομένα πρέπει επίσης να διασφαλίζει ότι ο παραλήπτης είναι νόμιμος. Το πρωτόκολλο που χρησιμοποιείται για την παροχή αυτού του ελέγχου ταυτότητας, που ονομάζεται Datagram Transport Layer Security (DTLS), χρησιμοποιείται ήδη και μπορεί να λειτουργήσει τόσο σε IPv4 όσο και σε IPv6.

  Επιπλέον, άλλες πολλά υποσχόμενες μέθοδοι για την αναγνώριση αντικειμένων IoT είναι τα πρότυπα κωδικοποίησης (Electronic Product Code – EPC) και ucode. Με τον όρο EPC εννοούμε τον Ηλεκτρονικό Κωδικό Προϊόντος, ο οποίος είναι ένα παγκόσμιο πρότυπο για την αναγνώριση προϊόντων μέσω αναγνώσιμων ετικετών. Έχει τη μορφή URI. Το ucode είναι επίσης ένας μηχανισμός αναγνώρισης αντικειμένου ή τοποθεσίας που χρησιμοποιεί 128 bit. Ωστόσο, η έλλειψη υπολογιστικών πόρων των συσκευών IoT αποτελεί εμπόδιο για την υιοθέτηση αυτών των προτύπων.

- ***Έλεγχος Πρόσβασης***

  Οι μηχανισμοί ελέγχου πρόσβασης είναι υπεύθυνοι για την επιβολή του μοντέλου ώστε να διασφαλίζεται η εξουσιοδοτημένη πρόσβαση σε δεδομένα και πόρους, λαμβάνοντας αποφάσεις με βάση το μοντέλο ελέγχου πρόσβασης. Με το Διαδίκτυο των πραγμάτων πλέον πανταχού παρών, η ιδιωτική και περιορισμένη πρόσβαση στα δεδομένα καθίσταται επιτακτική. Το βασικό στοιχείο που χρησιμοποιείται για τον έλεγχο πρόσβασης είναι οι λίστες ελέγχου πρόσβασης (ACL) που ορίζουν τα

δικαιώματα του χρήστη. Συμπληρωματικά, υπάρχει επίσης έλεγχος πρόσβασης βάσει ρόλου χρήστη (RBAC). Οι ρόλοι μπορεί να διαφέρουν σύμφωνα με το περιεχόμενο κάθε εφαρμογής, είναι δυναμικοί και μπορούν να τροποποιηθούν σε πραγματικά σενάρια IoT. Για παράδειγμα, ένας γιατρός μπορεί να διαχειρίζεται εξ αποστάσεως τα μηχανήματα των διαφόρων νοσοκομείων στα οποία ανήκει, υπό την προϋπόθεση ότι «κερδίζει» την εμπιστοσύνη των οντοτήτων IoT που βρίσκονται στο περιβάλλον εργασίας. Το μειονέκτημα των δηλώσεων είναι ότι σε ευρέως διανεμημένα συστήματα IoT με πολλούς χρήστες που αλληλεπιδρούν, δεν δίνουν σε κάθε χρήστη όσο το δυνατόν λιγότερα δικαιώματα. Στο έργο FP7 IoT@Work, η ανάπτυξη του CapBAC (Capability Based Access Control) αντιμετωπίζει αυτό το ζήτημα.

- ***Αξιοπιστία***

  Πολλές εφαρμογές και υπηρεσίες είναι εγγενώς ευάλωτες, όπως οι υπηρεσίες υγειονομικής περίθαλψης. Όταν βασίζονται σε συσκευές IoT, θα πρέπει να διασφαλίζεται η αξιοπιστία που παρέχουν. Η αξιοπιστία σχετίζεται επίσης με τη «φρεσκάδα» των μεταδιδόμενων δεδομένων. Δυνητικά λανθασμένα δεδομένα, είτε μέσω απάτης είτε λόγω λάθους, μπορεί να οδηγήσουν σε κακές καταστάσεις. Για να εξασφαλιστεί η αξιοπιστία, ορίζεται ένας μηχανισμός «διαπραγμάτευσης εμπιστοσύνης» (trust negotiation). Αυτό βασίζεται στην ανταλλαγή διαπιστευτηρίων μέσω P2P πριν από τη μεταφορά πληροφοριών.

3.2 Ασφάλεια στην Αρχιτεκτονική του IoT

Στο Διαδίκτυο των πραγμάτων, εκτός από τα θέματα ασφάλειας των δικτύων αισθητήρων, των κινητών επικοινωνιών και του Διαδικτύου, προκύπτουν άλλα σημαντικά ζητήματα ασφάλειας που είναι εξειδικευμένα και περιλαμβάνουν την προστασία δεδομένων, τον έλεγχο πρόσβασης, τη διαχείριση δεδομένων και την αποθήκευση. Τα συστήματα RFID και τα ασύρματα δίκτυα αισθητήρων είναι τα πρώτα που έχουν πρόσβαση σε πληροφορίες, επομένως χρησιμοποιούν τεχνικές όπως η κρυπτογράφηση και οι ψηφιακές υπογραφές για την επίτευξη εμπιστευτικότητας και ακεραιότητας.

Προκειμένου να διασφαλιστεί η ασφάλεια και η εμπιστοσύνη στη μετάδοση δεδομένων μεταξύ κόμβων IoT, τα πρωτόκολλα επικοινωνίας και οι τεχνολογίες δικτύου μπορεί να είναι πολύπλοκα και ποικίλα. Αυτό καθιστά δύσκολη την οικοδόμηση εμπιστοσύνης στις επικοινωνίες των κόμβων IoT και μπορεί να οδηγήσει σε συμφόρηση

και άλλα ζητήματα στο δίκτυο κορμού. Σε επίπεδο μεμονωμένων εφαρμογών IoT, εγείρονται επίσης ανησυχίες σχετικά με την αυθεντικότητα και τον έλεγχο πρόσβασης.

3.2.1 Ασφάλεια Επιπέδου Αντίληψης

Το εν λόγω επίπεδο είναι υπεύθυνο για τη συλλογή πληροφοριών. Περιλαμβάνει RFID, WSN, RSN, GPS και άλλες τεχνολογίες.

3.2.1.1 Ζητήματα ασφαλείας στα RFID συστήματα

Η τεχνολογία RFID που χρησιμοποιείται ευρέως στο IoT για την ανέπαφη ταυτοποίηση αντικειμένων βρίσκεται αντιμέτωπη σε μια σειρά από προβλήματα.

- ***Ενιαία κωδικοποίηση:*** Δεν υπάρχει διεθνώς συμφωνημένο πρότυπο για την κωδικοποίηση ετικετών RFID, το οποίο μπορεί να οδηγήσει σε προβλήματα όπως μη έγκυρες αναγνώσεις ή αδυναμία ανάγνωσης της ετικέτας από συσκευή ανάγνωσης RFID. Τα πιο ευρέως χρησιμοποιούμενα είναι το UID και το EPC.
- ***«Συνωστισμός» δεδομένων:*** Σε σενάρια πραγματικού κόσμου, είναι λογικό για περισσότερες από μία ετικέτες να στέλνουν δεδομένα στους αναγνώστες ταυτόχρονα. Αυτό μπορεί να οδηγήσει σε σύγχυση κατά την ανάγνωση, με αποτέλεσμα να μην ολοκληρωθούν οι εργασίες. Θα πρέπει να χρησιμοποιούνται τεχνικές αποφυγής σύγκρουσης δεδομένων, οι οποίες θα φέρουν σε τάξη τις μεταδιδόμενες πληροφορίες. Ταυτόχρονα, πρέπει να υπάρχουν αλγόριθμοι για να αποτρέπεται η επικάλυψη των πληροφοριών της ετικέτας.
- ***Ιδιωτικότητα στο RFID:*** Η ανάγκη για χαμηλού κόστους ετικέτες RFID έχει περιορίσει τους υπολογιστικούς τους πόρους, επομένως θα πρέπει να αναζητηθούν αξιόπιστες λύσεις σε ζητήματα απορρήτου που δεν απαιτούν μεγάλη επεξεργαστική ισχύ. Οι εναλλακτικές λύσεις για την αποθήκευση δεδομένων στις ασφαλείς περιοχές αποθήκευσης των ετικετών μπορεί να περιλαμβάνουν τη χρήση φυσικών μεθόδων ή τη χρήση κωδίκων που είναι λιγότερο απαιτητικοί για την επεξεργαστική ισχύ των ετικετών. Επιπλέον, οι βάσεις δεδομένων υψηλότερου επιπέδου μπορούν να αποθηκεύουν σημαντικά δεδομένα αντί να βασίζονται στις ασφαλείς περιοχές αποθήκευσης των ετικετών. Για παράδειγμα, στην περίπτωση των ετικετών που έχουν πληροφορίες οχημάτων GNSS (Δορυφορικό σύστημα πλοήγησης), είναι δυνατόν αυτό να μπορεί να εντοπιστεί [37].

- ***Διαχείριση εμπιστευτικότητας:*** Το απόρρητο και η εμπιστευτικότητα αποτελούν αναπόσπαστο κομμάτι των συστημάτων RFID. Οι ψηφιακές υπογραφές διαδραματίζουν σημαντικό ρόλο στη διασφάλιση της αυθεντικότητας των δεδομένων που ανταλλάσσονται μεταξύ ετικετών και σταθμών βάσης. Οι αλγόριθμοι και τα πρωτόκολλα κρυπτογραφίας μπορούν να συμβάλουν σε αυτό, αλλά απαιτούν χώρο αποθήκευσης και επεξεργαστική ισχύ από την πλευρά των ετικετών. Η έρευνα θα πρέπει να κατευθύνεται προς την ανάπτυξη αλγορίθμων όσο το δυνατόν λιγότερο απαιτητικών [37].

3.2.1.2 Το πρόβλημα της ετερογένειας

Είναι γνωστό ότι υπάρχουν πολλά δεδομένα προς συλλογή, επεξεργασία και αποθήκευση σε περιβάλλον IoT. Ωστόσο, αυτά τα δεδομένα συλλέγονται με διαφορετικούς τρόπους, μορφές και πρωτόκολλα, γεγονός που καθιστά δύσκολη την ανάλυσή τους. Συχνά προκύπτουν ζητήματα συμβατότητας μεταξύ μορφών δεδομένων και πρωτοκόλλων επικοινωνίας. Τα δίκτυα RFID (RSN) και τα δίκτυα αισθητήρων έχουν διαφορετικές φιλοσοφίες, πράγμα που σημαίνει ότι πρέπει να αναπτυχθεί λογισμικό και υλικό που θα προωθεί την ομοιόμορφη και κοινή κωδικοποίησή τους. Μερικά κοινά παραδείγματα είναι ο μεμονωμένος κόμβος ενός αισθητήρα με ενσωματωμένη τεχνολογία RFID ή οι ετικέτες RFID που λειτουργούν και ως ασύρματοι αισθητήρες παράλληλα. Ωστόσο, λόγω της έλλειψης υποδομής και της υψηλής πυκνότητας των δικτύων, τα δεδομένα από πολλούς κόμβους είναι συχνά αναξιόπιστα [37].

Όσον αφορά την αντίληψη του IoT, η πολυπλοκότητα είναι μια πρόκληση, με τα θέματα ασφάλειας να είναι το κύριο πρόβλημα. Υπάρχουν επίσης ζητήματα με την επεξεργαστική ισχύ και την ετερογένεια, καθώς και το γεγονός ότι οι κόμβοι IoT δεν μπορούν εύκολα να αντιμετωπιστούν μεμονωμένα. Ακόμα κι αν οι προτεινόμενες λύσεις παρέχουν κάποιο επίπεδο ασφάλειας σε επίπεδο αντίληψης, δεν εγγυώνται ασφάλεια σε ένα σύστημα Διαδικτύου των Πραγμάτων.

3.2.2 Ασφάλεια Επιπέδου Δικτύωσης και Μεταφοράς

Το επίπεδο δικτύωσης και μεταφοράς παρέχει ένα περιβάλλον πρόσβασης για το επίπεδο αντίληψης, το οποίο μεταδίδει πληροφορίες και τις αποθηκεύει για χρήση από εφαρμογές υψηλότερου επιπέδου. Ανάλογα με τις λειτουργίες, το επίπεδο μεταφοράς μπορεί να χωριστεί σε τρία επιπλέον υποστρώματα: το δίκτυο πρόσβασης, το δίκτυο κορμού και τα τοπικά δίκτυα. Είναι μια συμβολή διαφορετικών ετερογενών δικτύων.

3.2.2.1 Δίκτυο Πρόσβασης

Το δίκτυο πρόσβασης έρχεται πρώτα σε επαφή με τα δεδομένα του επιπέδου αντίληψης. Αυτό σημαίνει ότι θα είναι υπεύθυνο για τη "φιλοξενία" τυχόν εκκρεμών ζητημάτων ασφαλείας που ενδέχεται να υπάρχουν ακόμη από το προηγούμενο επίπεδο. Αυτό περιλαμβάνει ασύρματα δίκτυα Wi-Fi, δίκτυα ad hoc και δίκτυα κινητής τηλεφωνίας 3G/4G. Ανάλογα με τα δομικά τους στοιχεία, τα ασύρματα δίκτυα μπορούν να διακριθούν μεταξύ αυτών που απαιτούν σταθμό βάσης, όπως Wi-Fi και κινητής τηλεφωνίας, και εκείνων που δεν απαιτούν σταθμό βάσης, όπως ad hoc.

- ***Ζητήματα ασφάλειας δικτύων Wi-Fi:*** Γνωστά και ως IEEE802.11, τα δίκτυα Wi-Fi είναι ο πιο κοινός τύπος ασύρματου δικτύου. Στο πλαίσιο του IoT, οι εφαρμογές Wi-Fi χρησιμοποιούνται για την περιήγηση στο Διαδίκτυο την ανταλλαγή ηλεκτρονικών μηνυμάτων (email) και την κοινή χρήση μεγάλων αρχείων. Η ασφάλεια είναι ένα σημαντικό μέρος των δικτύων Wi-Fi και έχουν καταγραφεί αρκετές επιθέσεις, όπως phishing, επιθέσεις άρνησης υπηρεσίας (DDos/Dos) και σημεία πρόσβασης χωρίς έλεγχο ταυτότητας. Για την αντιμετώπιση αυτών των συγκεκριμένων ζητημάτων, ο έλεγχος πρόσβασης και η κρυπτογράφηση δικτύου καθίστανται σημαντικά. Ο έλεγχος πρόσβασης διασφαλίζει ότι μόνο οι πιστοποιημένοι χρήστες μπορούν να εισέλθουν στο Διαδίκτυο, ενώ η κρυπτογράφηση διασφαλίζει ότι μόνο ο παραλήπτης που έχει πρόσβαση στο κοινόχρηστο κλειδί μπορεί να αποκρυπτογραφήσει τα δεδομένα. Συγκεκριμένα πρωτόκολλα που χρησιμοποιούνται για κρυπτογράφηση και έλεγχο ταυτότητας σε δίκτυα Wi-Fi είναι το WPA/WPA2, με βάση το πρωτόκολλο TKIP και το πρότυπο AES. Ταυτόχρονα, τα πιστοποιητικά τύπου PPPoE χρησιμοποιούνται για σκοπούς ελέγχου ταυτότητας.

- ***Ζητήματα ασφάλειας δικτύων ad hoc:*** Τα ad hoc ασύρματα δίκτυα είναι μη συνδεδεμένοι κόμβοι που δεν είναι συνδεδεμένοι με άλλους κόμβους ή με σταθερή υποδομή. Είναι δίκτυα D2D, που σημαίνει ότι είναι αυτοδιαχειριζόμενα και μπορούν να αυτό-οργανωθούν. Είναι επίσης χρήσιμα για το IoT επειδή δεν είναι ευαίσθητα σε υποκλοπές ή παρεμβολές. Οι κύριες απειλές ασφαλείας για τα ad hoc δίκτυα είναι τα κανάλια μέσω των οποίων μεταδίδονται τα δεδομένα και οι διαδρομές που ακολουθούν τα δεδομένα. Στο IoT, η ασφάλεια στα ad hoc δίκτυα είναι σημαντική στους κόμβους, στα δεδομένα και επίσης στις διαδρομές που ακολουθούν τα δεδομένα. Όσον αφορά την ασφάλεια των κόμβων, για να αποφευχθεί η παράνομη επικοινωνία, κάθε κόμβος θα πρέπει να προσδιορίζει άλλους κόμβους με τους

οποίους επικοινωνεί. Διαφορετικά, η μη εξουσιοδοτημένη ιδιοκτησία κόμβου θα παρείχε πρόσβαση στα μεταδιδόμενα δεδομένα. Ο έλεγχος ταυτότητας μεταξύ τους αποκαλύπτει ποιος είναι νόμιμος και ικανός να επικοινωνήσει. Όσον αφορά τα ίδια τα δεδομένα, σε ένα ad hoc δίκτυο, λόγω της δομής του, είναι εύκολο να διαρρεύσουν και να παραβιαστούν με κακόβουλο τρόπο. Στην περίπτωση αυτή υπάρχουν βασικοί μηχανισμοί διαχείρισης. Όσον αφορά τη δρομολόγηση σε ένα ad hoc δίκτυο, προκειμένου να αποφευχθούν επιθέσεις άρνησης πρόσβασης, μπορούν να εφαρμοστούν τεχνικές κρυπτογράφησης.

- ***Ζητήματα Ασφάλειας κυψελωτών δικτύων 3G/4G:*** Όταν τα κυψελωτά δίκτυα χρησιμοποιούνται ως δίκτυο πρόσβασης σε περιβάλλον IoT, υπάρχει κίνδυνος διαρροής προσωπικών δεδομένων και απώλειας πακέτων δεδομένων. Η διαχείριση κλειδιών, ο έλεγχος ταυτότητας προέλευσης δεδομένων και η κρυπτογράφηση μπορούν όλα να βοηθήσουν στη μείωση αυτών των κινδύνων. Επιπλέον, συγκεκριμένα δίκτυα έχουν τη δυνατότητα να χρησιμοποιούν κάρτες SIM ως μέσο ελέγχου ταυτότητας χρηστών και συσκευών IoT. Οι πληροφορίες αναγνώρισης και οι κωδικοί πρόσβασης επαληθεύονται αμοιβαία από τους διακομιστές και τα τερματικά, γεγονός που συμβάλλει στην προώθηση της νομιμότητας της επικοινωνίας τους.

3.2.2.2 Δίκτυο Κορμού

Σε ένα περιβάλλον IoT, το κεντρικό δίκτυο είναι υπεύθυνο για τη μετάδοση δεδομένων. Πιο συγκεκριμένα, το βασικό δίκτυο, στο πλαίσιο του IoT, είναι το Διαδίκτυο. Επομένως, τυχόν ζητήματα ασφάλειας που αφορούν το Διαδίκτυο εμπίπτουν φυσικά στη ραχοκοκαλιά του IoT.

Όπως ήδη αναφέρθηκε, ο τεράστιος αριθμός διευθύνσεων IP που απαιτεί το IoT καθιστά το πρωτόκολλο IPv4 ανεπαρκές. Δεν μπορεί να αντιμετωπίσει τον όγκο των δικτυωμένων αισθητήρων IoT. Η εξέλιξη στο IPV6 είναι επιτακτική. Έτσι, σε αυτό το πρωτόκολλο, η τεχνολογία που διατηρεί χαμηλή κατανάλωση ενέργειας είναι το 6LowPAN, το οποίο υιοθετείται στο φυσικό επίπεδο (PHY) και μεσαίου ελέγχου πρόσβασης (MAC).

Επιπλέον, προτείνεται να υπάρχει ένα επίπεδο προσαρμογής (adaptation layer) μεταξύ του επιπέδου IEEE 802.15.4 MAC και του δικτύου IPv6. Η τεχνολογία 6LowPAN περιλαμβάνει κατακερματισμό (hash), επανασυναρμολόγηση, συμπίεση και διευθυνσιοδότηση κεφαλίδων (header).

3.2.2.3 Τοπικά Δίκτυα Περιοχής

Στο πλαίσιο του IoT, είναι σημαντικό να ληφθεί υπόψη η διαρροή πληροφοριών και η προστασία των διακομιστών σε τοπικά δίκτυα (LAN). Ο έλεγχος πρόσβασης δικτύου είναι μια από τις πιο βασικές στρατηγικές για την αποφυγή ανεπιθύμητων καταστάσεων και ταυτόχρονα, η κάλυψη τυχόν ευπάθειας ασφαλείας που μπορεί να υπάρχουν στις υπηρεσίες δικτύου, σε συνδυασμό με την αφαίρεση κακόβουλου λογισμικού ή σφαλμάτων λογισμικού δικτύου, βοηθά σε κάποιο βαθμό την προστασία του συστήματος. Επιπλέον, για την ασφάλεια των τοπικών δικτύων IoT, συνιστάται η ενημέρωση του λειτουργικού συστήματος σε τακτά χρονικά διαστήματα και η χρήση κωδικών ασφαλείας.

Συμπερασματικά, το επίπεδο μεταφοράς μεταξύ συστημάτων IoT θεωρείται πολύ σημαντικό από άποψη ασφάλειας. Ανησυχίες για την ασφάλεια προκύπτουν κατά τη προσπάθεια ενοποίησης των διάφορων ετερογενών δικτύων (ad-hoc, Internet, 3G) που συνθέτουν ένα σύστημα IoT. Για το λόγο αυτό, χρησιμοποιούνται ορισμένες τεχνικές (όπως η στενή σύζευξη tight & loose coupling και οι συνεργασίες πανεπιστημίων όπως το ACENET) για να προσπαθήσουν να μετριάσουν αυτές τις ανησυχίες.

Σε επίπεδο μεταφορών, το IoT είναι ευάλωτο σε επιθέσεις Άρνησης Εξυπηρέτησης (DoS). Αυτές οι επιθέσεις μπορεί να είναι δύσκολο να αποφευχθούν, καθώς εκμεταλλεύονται την πολυπλοκότητα των συστημάτων IoT. Οι μηχανισμοί ελέγχου ταυτότητας και ανίχνευσης βοηθούν στην προστασία από ιομορφικά λογισμικά, Trojan, spam κ.α.

3.2.3 Ασφάλεια Επιπέδου Εφαρμογών

Το επίπεδο υποστήριξης εφαρμογών είναι τοποθετημένο ένα στρώμα πάνω από το επίπεδο μεταφοράς και είναι υπεύθυνο για την υποστήριξη σχεδόν όλων των τύπων επιχειρηματικών λειτουργιών. Εφαρμόζει «έξυπνους» υπολογισμούς, επεξεργάζεται τα εισερχόμενα δεδομένα και συμβάλλει στη διαδικασία λήψης αποφάσεων. Είναι επίσης σε θέση να αναγνωρίσει και να φιλτράρει τα έγκυρα από τα κακόβουλα δεδομένα που φθάνουν. Ανάλογα με τις λειτουργίες, το επίπεδο εφαρμογής μπορεί να χωριστεί σε διάφορα τμήματα, όπως ενδιάμεσο λογισμικό, επικοινωνίες M2M και υπολογιστικό νέφος.

Η έννοια του ενδιάμεσου λογισμικού περιλαμβάνει προφανώς διάφορες πλατφόρμες και λειτουργικά συστήματα. Ο όγκος των δεδομένων στο IoT, τον οποίο θα κληθεί να υποστηρίξει, είναι τεράστιος και δυναμικός. Επιπλέον, αυτά τα δεδομένα θα πρέπει να

μπορούν να επεκταθούν γραμμικά, για να καλύψουν τις επερχόμενες ανάγκες. Ταυτόχρονα, αυτό το λογισμικό θα πρέπει να μπορεί να χειρίζεται εισερχόμενα αιτήματα που φτάνουν την ίδια στιγμή και έχουν μια ορισμένη διάρκεια ζωής, επομένως θα πρέπει να εισάγει στις λειτουργίες του τεχνικές που θα δίνουν προτεραιότητα στη σειρά με την οποία διεκπεραιώνονται τα αιτήματα, έτσι ώστε τα επείγοντα αιτήματα μην μπαίνουν σε ουρά αναμονής. Οι επικοινωνίες M2M, ένα δημοφιλές μοντέλο εφαρμογής στο IoT, αντιμετωπίζουν κινδύνους ασφάλειας καθώς βασίζονται σε ηλεκτρικά καλώδια, ασύρματα ή κυψελωτά δίκτυα. Αυτό σημαίνει ότι το επίπεδο backend (middleware & M2M) θα πρέπει να πληροί όλες τις υψηλές επιχειρηματικές απαιτήσεις για ασφάλεια. Ο έλεγχος πρόσβασης, η αναγνώριση χρήστη, η ακεραιότητα και η διαθεσιμότητα των δεδομένων είναι αναπόσπαστα στοιχεία για τη διασφάλιση του απορρήτου και της αξιοπιστίας πληροφοριών των χρηστών. Η έρευνά μας επικεντρώνεται στην ανάπτυξη τεχνικών για τη διασφάλιση της ανωνυμίας k-anonymity (μοντέλο διαφύλαξης ευαίσθητων δεδομένων) [38], τυχαιοποίησης των δεδομένων και ανανέωσης των κλειδιών αυθεντικοποίησης. Επιπλέον, οι αρχές κάθε κράτους θα πρέπει να φροντίζουν για τις περιπτώσεις που οι χρήστες αλλάζουν παρόχους υπηρεσιών Διαδικτύου (ISP), ώστε να μην κινδυνεύουν τα δεδομένα τους.

Όσον αφορά την επεξεργασία δεδομένων στο νέφος, υπάρχουν επίσης αρκετοί κίνδυνοι. Αυτοί οι κίνδυνοι αφορούν πιθανές απομονώσεις δεδομένων και εσφαλμένη ιεράρχηση προτεραιοτήτων καθώς και προβλήματα στην ανάκτηση δεδομένων. Οι πλατφόρμες υπολογιστικού νέφους συχνά περιέχουν κρίσιμες πληροφορίες εμπορικών εταιρειών, επομένως συχνά αποτελούν στόχο επιθέσεων στον κυβερνοχώρο. Εταιρείες με ευαίσθητα δεδομένα, όπως μεσιτείες και ιατρικές κλινικές, μπορεί να διστάζουν να υιοθετήσουν το «σύννεφο» ως τρόπο επεξεργασίας και αποθήκευσης των ηλεκτρονικών τους αρχείων. Επιπλέον, οι επιθέσεις άρνησης πρόσβασης (DDoS) είναι κοινές στο cloud computing. Προκαλούν ασυνέχεια στη ροή πληροφοριών, τερματισμό λειτουργίας σε απροσδόκητες στιγμές και δυσκολία πρόσβασης σε ιδιωτικές αποθηκευμένες πληροφορίες, κατανάλωση μνήμης cache και διαθέσιμο εύρος ζώνης. Ένα άλλο ζήτημα ασφάλειας στο cloud computing σχετίζεται με το γεγονός ότι είναι προσβάσιμο από οπουδήποτε. Ιδιαίτερη αναφορά πρέπει να γίνει στην επαλήθευση των διαπιστευτηρίων των λογαριασμών χρηστών, καθώς είναι σχετικά δύσκολο να εντοπιστούν (tracing) τα ηλεκτρονικά δακτυλικά αποτυπώματα των χρηστών με πλαστά διαπιστευτήρια.

4. Θέματα Ασφάλειας στα WSNs και μοντέλα επιθέσεων

Τα ζητήματα ασφαλείας είναι κρίσιμης σημασίας διότι οι απαιτήσεις αξιοπιστίας είναι αυξημένες, όπως για παράδειγμα σε ιατρικές και στρατιωτικές εφαρμογές. Τα περισσότερα από τα υπάρχοντα πρωτόκολλα δρομολόγησης WSN και οι υπάρχουσες λύσεις ασφαλείας είναι ακατάλληλα. Αυτό οφείλεται στον περιορισμό πόρων που σχετίζεται με τα WSN [55]. Αυτοί οι περιορισμοί καθορίζουν σε μεγάλο βαθμό το είδος των προσεγγίσεων ασφαλείας που μπορούν να υιοθετηθούν για τα WSN. Η ασφάλεια αυτού του δικτύου λαμβάνει μέτρα για την πρόληψη δυσμενών καταστάσεων, όπως η ακεραιότητα δεδομένων, η υποκλοπή και η παρεμβολή, καθώς και η εισαγωγή και μετάδοση ψευδών ή τροποποιημένων μηνυμάτων. Για να διατηρηθεί ένα ασφαλές και αξιόπιστο σύστημα, όλες οι συσκευές και οι μηχανισμοί πρέπει να συνεργάζονται με ασφάλεια. Οποιαδήποτε απόκλιση από αυτή την αρχή θα μπορούσε να οδηγήσει σε επιθέσεις στο δίκτυο. Διάφορα ζητήματα ασφαλείας και οι λύσεις τους περιγράφονται σε αυτήν την ενότητα.

4.1 Προκλήσεις Ασφαλείας στα WSNs

Οι προκλήσεις ασφαλείας στα ασύρματα δίκτυα αισθητήρων προκύπτουν από τα κενά ασφαλείας αυτών των δικτύων, τα οποία οφείλονται στα μοναδικά χαρακτηριστικά αυτών των συστημάτων και αναφέρονται παρακάτω:

- ***Αναξιόπιστο μέσο μετάδοσης:*** Το δίκτυο είναι επιρρεπές σε επιθέσεις και κακόβουλες ενέργειες τρίτων λόγω της ασύρματης σύνδεσης των κόμβων. Για την προστασία κάθε κόμβου, είναι απαραίτητο να ληφθούν τα κατάλληλα μέτρα ασφαλείας. Αυτό είναι ιδιαίτερα σημαντικό καθώς για τη μετάδοση πληροφοριών χρησιμοποιείται η δρομολόγηση πολλαπλών βημάτων μέσω των κόμβων (multi-hop routing).
- ***Περιορισμοί των κόμβων σε θέματα υπολογιστικών δυνατοτήτων, ενέργειας και αποθήκευσης:*** Οι κόμβοι ενός δικτύου WSN έχουν σχεδιαστεί για να είναι χαμηλού κόστους και περιορισμένων πόρων, γεγονός που μπορεί να δημιουργήσει προβλήματα αξιοπιστίας στο δίκτυο. Οι περισσότεροι αλγόριθμοι ασφάλειας δικτύου δεν είναι συμβατοί με WSN, επειδή είναι πολύ περίπλοκοι για τα δίκτυα αυτά.

- ***Δυσκολία συγχρονισμού συσκευών δικτύου:*** Σε ορισμένους μηχανισμούς ασφαλείας ο συγχρονισμός μεταξύ των συσκευών είναι κρίσιμης σημασίας και η επίτευξή του γίνεται πιο δύσκολη λόγω δρομολόγησης πακέτων με πολλαπλά άλματα.
- ***Απομακρυσμένη λειτουργία:*** Ο συνήθης τρόπος υλοποίησης των WSN είναι, για μεγάλο χρονικό διάστημα, χωρίς ανθρώπινη επίβλεψη γεγονός που τα καθιστά ευάλωτα σε φυσικές επιθέσεις.

4.2 Απαιτήσεις Ασφαλείας στα WSNs

Η ασφάλεια ενός WSN βασίζεται στην προστασία των δεδομένων από αλλοίωση ή καταστροφή, στην ασφάλεια των πόρων του δικτύου και στην ικανότητα των κόμβων αισθητήρων να παρέχουν αξιόπιστες πληροφορίες. Σύμφωνα με αυτά, προκύπτουν επίσης και οι προδιαγραφές ασφαλείας του δικτύου. Οι προδιαγραφές που θα πρέπει να πληρούνται τόσο κατά την συνηθισμένη λειτουργία όσο και σε περίπτωση κακόβουλης ενέργειας (επίθεσης), είναι οι εξής:

- ***Διαθεσιμότητα (availability):*** Διαθεσιμότητα ορίζεται ως η δυνατότητα προσπέλασης της πληροφορίας από εξουσιοδοτημένο χρήστη και από όλους τους κόμβους του δικτύου. Η διαθεσιμότητα της πληροφορίας πρέπει να υφίσταται ακόμα και σε περιπτώσεις διαταραχών (φυσικές καταστροφές, επιθέσεις, εξάντληση πόρων), δηλαδή οι κόμβοι δεν πρέπει να τίθενται σε κατάσταση άρνησης εξυπηρέτησης (Denial of Service – DoS). Η εξασφάλιση της διαθεσιμότητας γίνεται με καταπολέμηση επιθέσεων DoS, όπως θα δούμε στη συνέχεια.
- **Εμπιστευτικότητα (confidentiality):** Εμπιστευτικότητα καλείται η προστασία των μεταδιδόμενων μηνυμάτων από μη εξουσιοδοτημένη αποκάλυψη. Η εξασφάλιση της εμπιστευτικότητας υλοποιείται με χρήση κρυπτογραφικών μεθόδων συμμετρικού κλειδιού, όπως θα δούμε στη συνέχεια.
- **Ακεραιότητα (integrity):** Η ακεραιότητα είναι η διασφάλιση της ορθότητας των δεδομένων που κυκλοφορούν μέσω των κόμβων του δικτύου. Κρίνεται αναγκαία η εξασφάλιση η μη αλλοίωση των δεδομένων κατά την προώθηση τους από το αισθητήριο κόμβο προς το σταθμό βάσης.
- **Πιστοποίηση ταυτότητας – Αυθεντικότητα (authentication):** Ο έλεγχος ταυτότητας επιβεβαιώνει την ταυτότητα του αποστολέα και δίνει τη δυνατότητα στο

κόμβο παραλήπτη να επαληθεύσει πως η πληροφορία στάλθηκε από συγκεκριμένο κόμβο αποστολέα του δικτύου.

- **Ιδιωτικότητα ή απόρρητο επικοινωνίας (privacy):** Το απόρρητο προστατεύει την ανωνυμία της επικοινωνίας μεταξύ οντοτήτων δικτύου. Διασφαλίζει την εμπιστευτικότητα των μηνυμάτων, η οποία προστατεύει το περιεχόμενο των μηνυμάτων και το πλαίσιο στο οποίο ανταλλάχθηκαν, καθώς και την απαίτηση για ελεγχόμενη πρόσβαση σε πληροφορίες που συλλέγονται σχετικά με το απόρρητο των ευαίσθητων πληροφοριών. Η απαίτηση προστασίας πλαισίου επικοινωνίας διασφαλίζει ότι οι πληροφορίες σχετικά με τον αποστολέα, τον παραλήπτη και το περιεχόμενο του μηνύματος δεν αποκαλύπτονται σε έναν εισβολέα.
- ***Μη αποποίηση (non-repudiation):*** Η μη αποποίηση αποτελεί εγγύηση ότι ο αποστολέας και ο παραλήπτης των πληροφοριών συμμετέχουν και οι δύο στη μετάδοση. Αυτό είναι σημαντικό για τον εντοπισμό κόμβων που έχουν παραβιαστεί από κακόβουλη δραστηριότητα.
- ***Φρεσκάδα δεδομένων (data freshness):*** Διασφάλιση πως τα δεδομένα που διακινούνται στο δίκτυό είναι όσο το δυνατόν πιο πρόσφατα ενσωματώνοντας έναν μετρητή χρόνου στα πακέτα. Με αυτόν τον τρόπο, αποφεύγουμε τη σπατάλη ενέργειας σε αναμεταδόσεις παλαιών δεδομένων και διατηρούμε τη λειτουργία του δικτύου όσο το δυνατόν πιο ομαλή.
- ***Ευρωστία (robustness):*** Ένα δίκτυο ανθεκτικό στις επιθέσεις μπορεί να ελαχιστοποιήσει τις αρνητικές συνέπειες των κακόβουλων ενεργειών. Αυτό επιτυγχάνεται ελαχιστοποιώντας τον αντίκτυπο σε ολόκληρο το δίκτυο μιας πιθανής επίθεσης σε πολλούς κόμβους.
- ***Αυτό-οργάνωση (self-organization):*** Η αυτο-οργάνωση των WSN αποτελεί πρόκληση λόγω των αυστηρών περιορισμών στο εύρος ζώνης και στους ενεργειακούς πόρους που διατίθενται στα δίκτυα αυτά, καθώς οι κρυπτογραφικοί μηχανισμοί πρέπει να είναι συμβατοί με αυτές τις ιδιότητες.
- ***Συγχρονισμός (synchronization):*** Οι μηχανισμοί ασφαλείας απαιτούν το συγχρονισμό των συσκευών που αποτελούν ένα WSN, όπως οι περισσότερες λειτουργίες των δικτύων αυτών.

4.3 Επιθέσεις σε WSNs

Οι απειλές ασφαλείας (security attacks) κατά των ασύρματων δικτύων ορίζονται ως ενέργειες από εξωτερικές οντότητες με σκοπό τη διακοπή ή την παρέμβαση σε μηνύματα που διακινούνται μέσω του δικτύου. Στη βιβλιογραφία οι επιθέσεις αναφέρονται συχνά και ως απειλές, ωστόσο στο Λεξικό Ασφαλείας Διαδικτύου (Internet Security Glossary) RFC 2828 [56] γίνεται διαχωρισμός αυτών των δύο εννοιών.

Απειλή (threat): «Μια απειλή είναι η πιθανότητα παραβίασης ενός συστήματος ασφάλειας όπου μπορεί να συμβεί ένα περιστατικό, ευκαιρία, πράξη ή γεγονός που καθιστά επιτρεπτή τη παραβίαση ασφάλειας με πιθανή εκμετάλλευση ευπάθειας ενός συστήματος.».

Επίθεση (attack): «Μια επίθεση είναι μια παραβίαση ενός συστήματος ασφάλειας που προέρχεται από μια προμελετημένη απειλή. Στην ουσία, ορίζεται ως μια σκόπιμη προσπάθεια (ειδικά με την έννοια της μεθόδου ή της τεχνικής) να παρακαμφθούν οι υπηρεσίες ασφαλείας και να διαταραχθεί το σύστημα». Η ταξινόμηση των επιθέσεων πραγματοποιείται σε δύο μορφές, α) ενεργητικής και β) παθητικής μορφής.

- Στις επιθέσεις ενεργητικής μορφής (active attacks), ο επιτιθέμενος επιδιώκει να θέσει σε κίνδυνο την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των δεδομένων (τροποποίηση δεδομένων ή δημιουργία ψεύτικων δεδομένων, άρνηση εξυπηρέτησης). Πραγματοποιούνται τροποποιώντας δεδομένα (modification of messages) ή δημιουργώντας πλαστά δεδομένα (masquerades), επανεκπομπές (replays) καθώς και προκαλώντας αρνήσεις εξυπηρέτησης (denial of service) [57] [58].
- Στις επιθέσεις παθητικής μορφής (passive attacks) ο επιτιθέμενος δεν μεταδίδει τροποποιημένα δεδομένα εντός του δικτύου, αντίθετα στοχεύει στην υποκλοπή δεδομένων με σκοπό τη μείωση εμπιστευτικότητας στο δίκτυο. Η υποκλοπή (eavesdropping) και η παρακολούθηση (monitoring) μιας ασύρματης σύνδεσης είναι οι πιο συνήθεις παθητικές επιθέσεις, με στόχο την εξαγωγή μεταδιδόμενων πληροφοριών από άλλους χρήστες.

Επιπρόσθετα, οι επιθέσεις ασφάλειας κατηγοριοποιούνται σε εσωτερικές και εξωτερικές.

- Οι εσωτερικές επιθέσεις προέρχονται από κακόβουλα προσβεβλημένων συσκευών του δικτύου, και καθιστούν δυσκολότερη την ανίχνευσή τους.

- Στις εξωτερικές επιθέσεις μία ,εκτός δικτύου, συσκευή παρακολουθεί την κυκλοφορία και/ή εισάγει μη έγκυρα πακέτα στο δίκτυο προκειμένου να διαταράξει τις λειτουργίες του.

Οι επιθέσεις μπορούν επίσης να κατηγοριοποιηθούν με βάση τις απαιτήσεις ασφαλείας που στοχεύουν. Με αυτή τη λογική, προκύπτουν επιθέσεις ασφαλείας κατά α) αυθεντικότητας, β) διαθεσιμότητας ή γ) ακεραιότητας δεδομένων δικτύου.

- Οι επιθέσεις ελέγχου ταυτότητας δικτύου στοχεύουν στην τροποποίηση ή την υποκλοπή δεδομένων και αντιμετωπίζονται με κρυπτογραφία που διαφυλάσσει το απόρρητο.
- Ως επιθέσεις άρνησης εξυπηρέτηση (Denial of Service– DoS Attacks) αναφέρονται οι επιθέσεις κατά της διαθεσιμότητας.
- Τέλος, οι επιθέσεις ακεραιότητας στοχεύουν στην εισαγωγή ψευδών ή τροποποιημένων δεδομένων στο δίκτυο μέσω κόμβων αισθητήρων.

Για να επιτύχει τους στόχους του, ο εισβολέας στοχεύει τις λειτουργίες δικτύου οι οποίες υλοποιούνται σύμφωνα με την αρχιτεκτονική των δικτύων WSN, στην οποία έγινε περιγραφή στο Κεφάλαιο 2, και όχι μεμονωμένα.

4.3.1 Επιθέσεις Άρνησης Εξυπηρέτησης (Denial of Service – DoS Attacks)

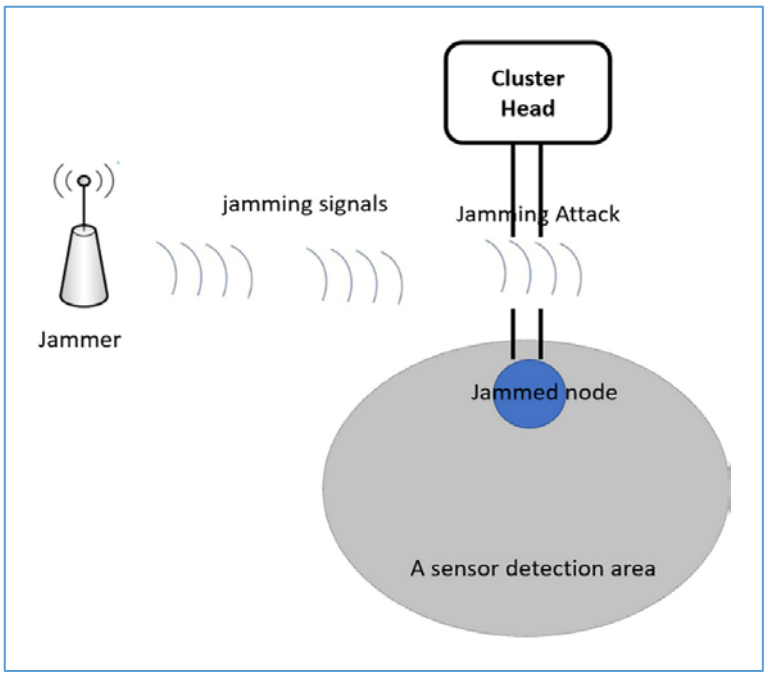
Οι επιθέσεις άρνησης υπηρεσίας είναι επιθέσεις που μπορούν να διαταράξουν τη διαθεσιμότητα του δικτύου. Έχουν τη δυνατότητα δημιουργίας σφαλμάτων υλικού και λογισμικού, εξάντληση πόρων ή συνδυασμό αυτών.

4.3.1.1 Φυσικό επίπεδο

Το φυσικό επίπεδο, όπως έχει αναφερθεί στο Κεφάλαιο 2, είναι υπεύθυνο για το καθορισμό της χρησιμοποιούμενης συχνότητας λειτουργίας, ανίχνευσης και επεξεργασίας σημάτων (διαμόρφωση, κωδικοποίηση δεδομένων, κρυπτογράφηση). Ένα δίκτυο WSN τίθεται ευάλωτο σε κακόβουλες παρεμβολές ή τροποποίηση δεδομένων καθώς χρησιμοποιείται το μέσο ασύρματης μετάδοσης στο οποίο έχει πρόσβαση ο εισβολέας. Αυτό μπορεί να συμβεί μέσω επιθέσεων παρεμβολής (jamming attacks) και επιθέσεων παραβίασης (tampering attacks), οι οποίες εξηγούνται στη συνέχεια.

- ***Επίθεση παρεμβολής (jamming attack):*** Σκοπός της επίθεσης παρεμβολής είναι η άρνηση εξυπηρέτησης. Ο επιτιθέμενος δημιουργεί θόρυβο, με παρόμοια εκπομπή σήματος από το δίκτυο μπάντα συχνοτήτων, και στοχεύει στη μη ορθή ανταλλαγή

μηνυμάτων μεταξύ των κόμβων. Χρησιμοποιούνται διάφοροι μηχανισμοί αντιμετώπισης όπως η τεχνική μεταπήδησης συχνότητας FHSS (Frequency – hopping spread spectrum) και η διαμόρφωση φάσματος (Code spreading).



Εικόνα 4.1. Επίθεση παρεμβολής (jamming)

Πηγή: https://www.researchgate.net/figure/Jamming-attack-in-wireless-communications-of-cyber-physical-systemss_fig1_357981233

- ***Επίθεση αλλοίωσης και υποκλοπής (tampering attack):*** Στόχος της επίθεσης αυτής είναι η φυσική καταστροφή των κόμβων και η υποκλοπή ευαίσθητων δεδομένων, όπως κρυπτογραφικά κλειδιά, με σκοπό ο επιτιθέμενος να αποκτήσει τον έλεγχο του κόμβου που δέχεται την επίθεση. Ο επιτιθέμενος, επιπλέον, μπορεί να τροποποιήσει ή να αντικαταστήσει κόμβους (αναπαραγωγή κόμβου), φέρνοντας τους επηρεαζόμενους κόμβους υπό τον έλεγχό του. Η άμυνα έναντι αυτής της επίθεσης είναι η χρήση μηχανισμών προστασίας από παραβίαση, οι κόμβοι μικρού μεγέθους και η απόκρυψή τους στο φυσικό περιβάλλον.

4.3.1.2 Επίπεδο Ζεύξης Δεδομένων

Υπεύθυνο για τον εντοπισμό και την πολυπλεξία δεδομένων, την πρόσβαση στα μέσα και τον έλεγχο σφαλμάτων ορίζεται το επίπεδο ζεύξης. Οι επιθέσεις, με στόχο τις λειτουργίες του επιπέδου, δημιουργούν είτε συμφόρηση δεδομένων είτε εξάντληση ενεργειακών πόρων σε εκτεθειμένα σημεία του δικτύου θέτοντας υπό αμφισβήτηση την αξιόπιστη επικοινωνία των κόμβων.

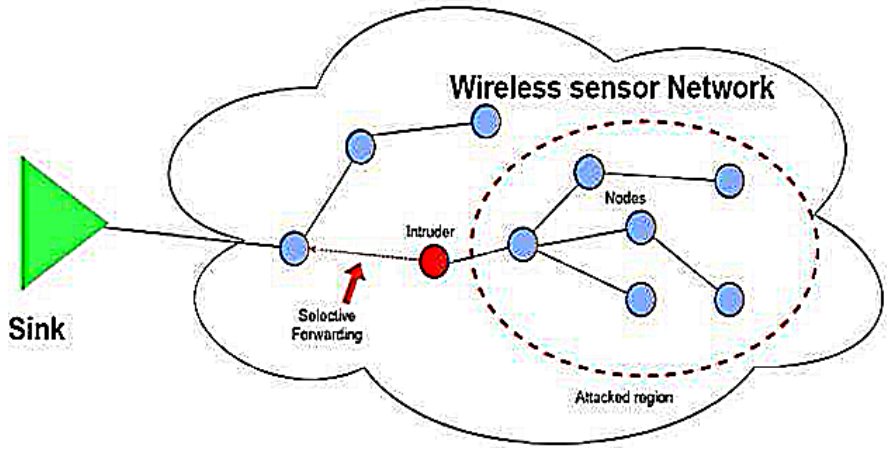
- ***Σύγκρουση δεδομένων (collision):*** Συγκρούσεις δεδομένων μπορεί να προκύψουν καθώς δύο ή περισσότεροι κόμβοι στέλνουν πακέτα δεδομένων, ταυτόχρονα, στο ίδιο κανάλι επικοινωνίας. Η επίθεση σκοπεύει σε απώλεια πακέτων, που προκαλείται από επίθεση πρωτοκόλλου MAC, η οποία με τη σειρά της προκαλεί σφάλματα δικτύου και απαιτεί αναμεταδόσεις δεδομένων. Ο μηχανισμός σηματοδότησης RTS/CTS (Ready-to-Send/Clear-to-Send) χρησιμοποιείται από το πρωτόκολλο MAC, το οποίο είναι επιρρεπές σε επιθέσεις σύγκρουσης δεδομένων. Ένας εισβολέας μπορεί να τοποθετήσει κακόβουλους κόμβους στην περιοχή κάλυψης του δικτύου, οι οποίοι θα λαμβάνουν τα μηνύματα RTS/CTS και θα προσποιούνται ότι είναι οι εξουσιοδοτημένοι δέκτες. Αυτοί οι κόμβοι δεν επιβεβαιώνουν την παραλαβή, επομένως ο μεσολαβητής κόμβος τους στέλνει συνεχώς πακέτα RTS. Κύρια μέθοδος για την καταπολέμηση της επίθεσης αυτής είναι η χρήση κωδικών διόρθωσης σφαλμάτων (error-correcting codes) και η χρήση πρωτοκόλλων MAC τα οποία δεν επιτρέπουν συγκρούσεις δεδομένων.
- ***Εξάντληση ενεργειακών πόρων (exhaustion):*** Οι ενεργειακοί πόροι στο δίκτυο εξαντλούνται λόγω της συμφόρησης που προκαλείται από τις επαναλαμβανόμενες αναμεταδόσεις δεδομένων. Αυτή η συμφόρηση μπορεί να αποφευχθεί με τη χρήση πολλαπλής πρόσβασης διαίρεσης χρόνου (TDMA), τη δρομολόγηση πακέτων εφόσον πραγματοποιηθεί επαλήθευση του αποστολέα και τον περιορισμό του μεγέθους των πακέτων που επιτρέπονται.
- ***Μεροληψία (unfairness):*** Ο εισβολέας οδηγεί το δίκτυο σε προκατειλημμένη συμπεριφορά κόμβων χρησιμοποιώντας διαδοχικά επιθέσεις συμφόρησης δεδομένων και εξάντλησης ενεργειακών πόρων. Αυτό θα αποτρέψει την πρόσβαση των κόμβων στο κανάλι επικοινωνίας, γεγονός που θα προκαλέσει καθυστερήσεις και απώλεια πακέτων.

4.3.1.3 Επίπεδο Δικτύου

Υπεύθυνο για τη δρομολόγηση πακέτων εντός του δικτύου, ορίζεται το επίπεδο δικτύου. Κατά συνέπεια, οι επιθέσεις που κατευθύνονται προς τις λειτουργίες αυτού του επιπέδου προκαλούν αστοχίες στη δρομολόγηση πακέτων.

- ***Επιλεκτική προώθηση (selective forwarding):*** Αφού ένας κόμβος δικτύου WSN λάβει ένα πακέτο δεδομένων από τον γειτονικό του κόμβο, προωθεί το πακέτο δεδομένων σύμφωνα με τη διαδρομή πολλαπλών αλμάτων που ορίζει το

πρωτόκολλο δρομολόγησης. Οι προσβεβλημένοι κόμβοι προωθούν επιλεκτικά ορισμένα πακέτα, χάνοντας τα υπόλοιπα πακέτα καθώς απορρίπτονται (Εικόνα 4.2). Μια επέκταση της επίθεσης επιλεκτικής προώθησης είναι η επίθεση μαύρης τρύπας (blackhole attack), στην οποία ένας προσβεβλημένος κόμβος ρίχνει κάθε πακέτο που λαμβάνει χωρίς να το προωθήσει. Η προστασία από την επιλεκτική προώθηση παρέχεται από τεχνικές δρομολόγησης πολλαπλών διαδρομών, οι οποίες παρέχουν εναλλακτικές διαδρομές για τη ροή πληροφοριών μέσω του δικτύου.



Εικόνα 4.2. Επίθεση επιλεκτικής προώθησης (selective forwarding)

Πηγή: https://d3i71xaburhd42.cloudfront.net/ffc6915014740dbcbc83401eec96ce26ea5b522f/2-Figure3-1.png

- ***Πλαστογράφηση, τροποποίηση, ή αντικατάσταση πληροφοριών δρομολόγησης – επίθεση παραπλάνησης (misdirection):*** Η πλαστογράφιση, η τροποποίηση και η αντικατάσταση πληροφοριών δρομολόγησης είναι μέθοδοι επιθέσεων κατά των πρωτοκόλλων δρομολόγησης. Στόχος του εισβολέα είναι να διαταράξει τη ροή των μηνυμάτων στο δίκτυο. Οι επιθέσεις αυτές προσελκύουν ή απωθούν την κυκλοφορία μηνυμάτων και προκαλούν εξάντληση της ενέργειας του κόμβου λόγω συνεχούς μετάδοσης καθυστερημένων μηνυμάτων, δημιουργούν ανεπιθύμητους βρόχους δρομολόγησης καθώς και καθυστερήσεις επικοινωνίας μεταξύ κόμβων αισθητήρων και σταθμών βάσης.
- ***Επίθεση homing:*** Υπάρχουν κόμβοι, σε ένα δίκτυο WSN, με αυξημένες ευθύνες (όπως συντονιστές, επικεφαλής ομάδων, δρομολογητές). Αυτή η επίθεση χαρτογραφεί τη δρομολόγηση των πακέτων στο δίκτυο και, εάν εντοπίσει ότι ορισμένοι κόμβοι είναι κρίσιμης σημασίας, ο εισβολέας μπορεί να προσπαθήσει να βλάψει αυτούς τους κόμβους.

- ***Πλαστογράφηση αναγνώρισης (acknowledgment spoofing):*** Αυτή η επίθεση εξαπατά τα πρότυπα που προβλέπουν την πιθανή ανταλλαγή μηνυμάτων αναγνώρισης μεταξύ κόμβων. Ο επιτιθέμενος στοχεύει στην δημιουργία δυσλειτουργιών στη διακίνηση δεδομένων στο δίκτυο αντιγράφοντας ή μετασχηματίζοντας τα μηνύματα αυτών.

4.3.1.4 Επίπεδο Μεταφοράς

Το επίπεδο μεταφοράς ορίζεται αρμόδιο για τη διασφάλιση της αξιόπιστης σύνδεσης μεταξύ δύο κόμβων. Το πλημμύρισμα (flooding) και ο αποσυγχρονισμός είναι επιθέσεις που προσπαθούν να διακόψουν αυτή τη σύνδεση.

- ***Πλημμύρισμα (flooding):*** Ο εισβολέας προσπαθεί να συνδεθεί με τον κόμβο στόχο (destination) ξανά και ξανά, σε μια προσπάθεια να τον ελέγξει. Ο κόμβος στόχος δεχόμενος πακέτα από τον κακόβουλο κόμβο (initiating node) μπορεί να συμβαδίσει με τη σύνδεση, αφού διαθέτει πόρους για να το κάνει.
- ***Αποσυγχρονισμός (desynchronization):*** Η σύνδεση μεταξύ δύο συσκευών διακόπτεται ως αποτέλεσμα της επίθεσης αποσυγχρονισμού. Αυτό είναι εφικτό με την αποστολή πλαστών μηνυμάτων σε μία από τις συσκευές, η οποία ζητά την αναμετάδοση των χαμένων μηνυμάτων.

4.3.1.5 Επίπεδο Εφαρμογής

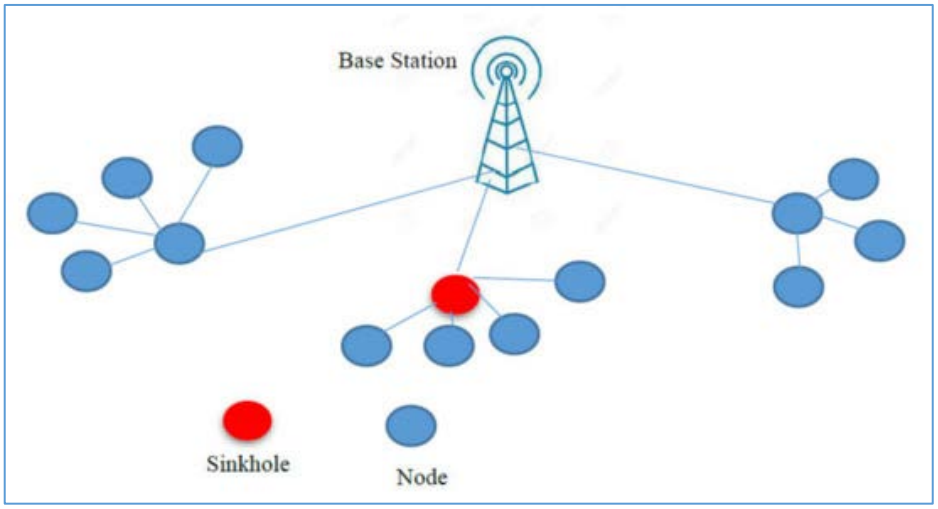
Η επίθεση καταπίεσης (overwhelm attack) και η επίθεση επαναπρογραμματισμού (reprogram attack) είναι δύο τύποι επιθέσεων DoS, σε επίπεδο εφαρμογής.

- ***Επίθεση καταπίεσης (overwhelm attack):*** Αυτή η επίθεση στοχεύει στη δημιουργία συμφόρησης πακέτων και εξάντλησης πόρων του δικτύου (ενέργεια κόμβων, εύρος ζώνης) χρησιμοποιώντας τους κόμβους του δικτύου ώστε να αποστείλουν μεγάλο όγκο πληροφοριών στο σταθμό βάσης.
- ***Επίθεση επαναπρογραμματισμού (reprogram attack):*** Όταν ο διαχειριστής προσπαθεί να επαναπρογραμματίσει εξ αποστάσεως μια συσκευή στο δίκτυο, είναι πιθανό ένας εισβολέας να μπει στον υπολογιστή του και να προσπαθήσει να καταλάβει τη συσκευή ή μέρος του δικτύου.

4.3.2 Επίθεση καταβόθρας (sinkhole)

Ένας κόμβος που δέχεται επίθεση μπορεί να χειριστεί τις πληροφορίες δρομολόγησης που αναχαιτίζει από το δίκτυο προκειμένου να φανεί πιο ελκυστικός σε άλλους κόμβους,

οδηγώντας αυτούς τους κόμβους να επιλέξουν να στείλουν μηνύματα στον κόμβο που δέχεται επίθεση αντί για τον επιδιωκόμενο παραλήπτη. Με τον τρόπο αυτό, ο εισβολέας μπορεί να χειραγωγήσει τη ροή πληροφοριών εντός του δικτύου μέσω του παραβιασμένου κόμβου (Εικόνα 4.3).

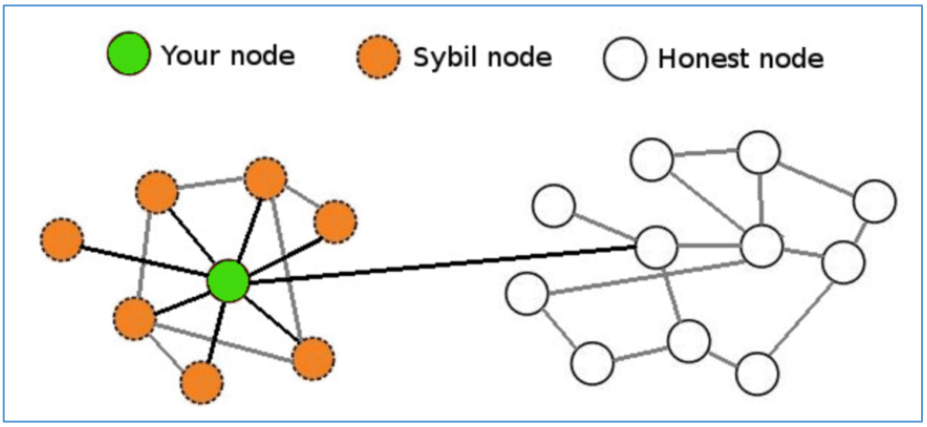


Εικόνα 4.3. Επίθεση καταβόθρας (sinkhole)

Πηγή: https://www.mdpi.com/2224-2708/9/3/39

4.3.3 Σιβυλλική επίθεση (sybil attack)

Σιβυλλική επίθεση είναι ένας τύπος επίθεσης που στοχεύει στη δημιουργία πολλαπλών ταυτοτήτων σε έναν κόμβο. Με αυτόν τον τρόπο, ο κόμβος μπορεί να δημιουργήσει νέες πλαστές ταυτότητες που υλοποιούν ίσο αριθμό εικονικών κόμβων ή να μιμηθεί τις ταυτότητες άλλων κόμβων. Αυτοί οι κόμβοι συνήθως συμμετέχουν σε ένα δίκτυο WSN, αλλά στην πραγματικότητα είναι μόνο μία συσκευή. Το αποτέλεσμα της επίθεσης αυτής είναι ότι ο κόμβος επιβαρύνεται με περισσότερη ενέργεια από τους άλλους κόμβους του δικτύου (Εικόνα 4.4).

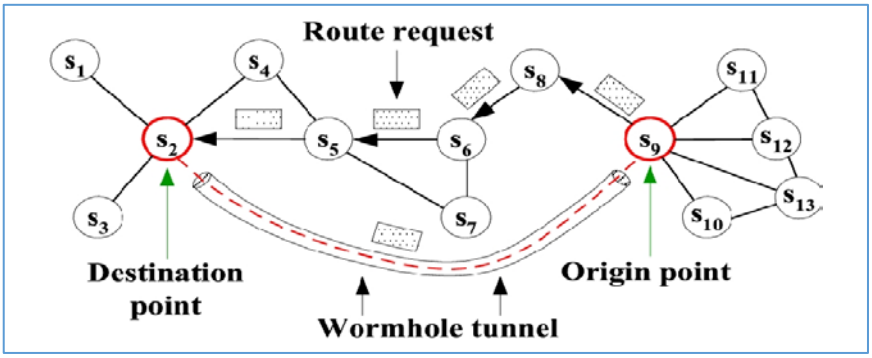


Εικόνα 4.4. Σιβυλλική επίθεση (sybil attack)

Πηγή: https://coincentral.com/wp-content/uploads/2018/08/Screenshot-2018-08-30-at-15.21.56-874x395.png

4.3.4 Σκουληκότρυπες (wormholes)

Η επίθεση σκουληκότρυπας είναι ένας τρόπος παραπλάνησης δύο απομακρυσμένων κόμβων, έτσι ώστε να αναγνωρίζονται ως γειτονικοί. Αυτή η επίθεση χρησιμοποιείται συνδυάζοντας κι άλλα είδη επιθέσεων, όπως η επιλεκτική προώθηση και η επίθεση με καταβόθρα.

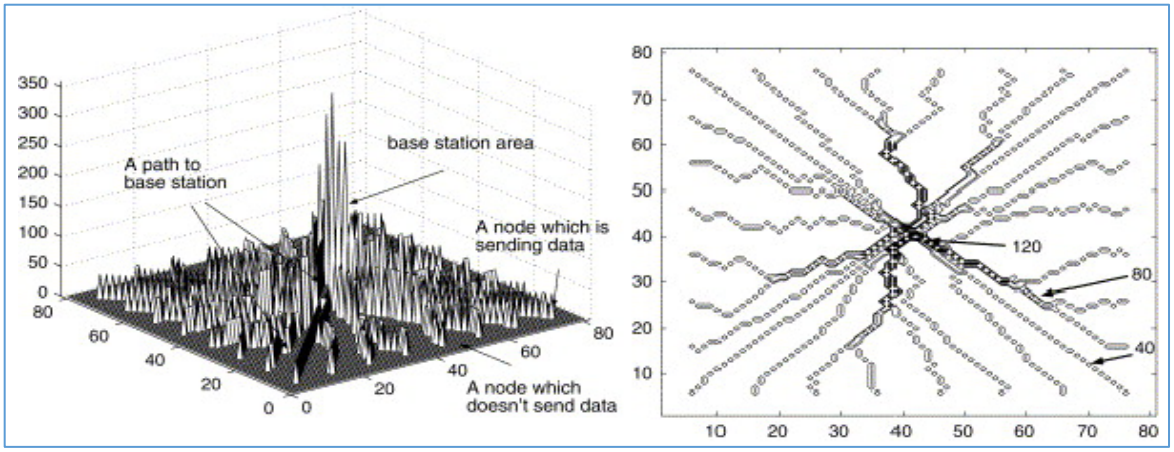


Εικόνα 4.5. Επίθεση σκουληκότρυπας (wormhole)

Πηγή: https://d3i71xaburhd42.cloudfront.net/62f9acd579414838df1e0a0344070fe46b082c79/13-Figure1.2-1.png

4.3.5 Επίθεση ανάλυσης κίνησης (traffic analysis)

Η επίθεση ανάλυσης κυκλοφορίας χρησιμοποιείται για τον εντοπισμό και την απενεργοποίηση ενός σταθμού βάσης WSN, με σκοπό τη πραγματοποίηση επιβλαβών ενεργειών εναντίον του. Η υλοποίηση ανάλυσης κίνησης είναι εφικτή με δύο τρόπους. Με το πρώτο τρόπο, ο επιτιθέμενος, εκμεταλλεύεται το γεγονός ότι οι πλησιέστεροι κόμβοι ως προς τους σταθμούς βάσης έχουν τη φυσική ιδιότητα να διαχειρίζονται περισσότερα πακέτα. Με την επίθεση καταγραφής ρυθμού (rate monitoring attack) [59], ο εισβολέας εντοπίζει τελικά το σταθμό βάσης με τη βοήθεια των κόμβων που στέλνουν περισσότερα πακέτα (Εικόνα 4.6).



Εικόνα 4.6. Εντοπισμός θέσης σταθμού βάσης με επίθεση καταγραφής ρυθμού

Πηγή: https://www.sciencedirect.com/science/article/abs/pii/S1574119205000726

Με το δεύτερο τρόπο, σύμφωνα με την επίθεση συσχέτισης χρόνου (time correlation attack) [59], ο επιτιθέμενος δημιουργεί γεγονότα ανιχνεύσιμα από τους κόμβους αισθητήρες και αναλύει την πορεία αποστολής των πακέτων.

4.3.6 Επίθεση HELLO flood

Η επίθεση αυτή χρησιμοποιεί έναν κακόβουλο κόμβο που εκπέμπει σε υψηλότερη ισχύ από άλλους κόμβους, και αυτό μπορεί να ξεγελάσει άλλους κόμβους ώστε να πιστεύουν ότι είναι γειτονικοί. Αυτό επιτρέπει στον εισβολέα να ελέγχει τη δρομολόγηση των πακέτων.

4.3.7 Επιθέσεις κατά του απορρήτου

Οι επιθέσεις αυτές σκοπεύουν στην εξαγωγή ευαίσθητων δεδομένων από ένα δίκτυο, όπως δεδομένα που σχετίζονται με τη λειτουργία του δικτύου ή τα δεδομένα κίνησης. Αυτές οι επιθέσεις θεωρούνται μορφές παρακολούθησης και υποκλοπής.

- **Παρατήρηση και κρυφάκουσμα (monitoring and eavesdropping):** Αυτή η επίθεση έχει σχεδιαστεί για την κλοπή πληροφοριών που είναι σημαντικές για την ασφάλεια του δικτύου, όπως δεδομένα κυκλοφορίας και πληροφορίες ελέγχου.
- **Επίθεση ανάλυσης κίνησης (traffic analysis):** Η επίθεση ανάλυσης κυκλοφορίας εξετάζει τη διακίνηση πληροφοριών στο δίκτυο και μπορεί να αποκαλύψει πού βρίσκεται ο σταθμός βάσης, όπως αναφέρθηκε στην υπό ενότητα 4.3.5.
- **Επίθεση παραλλαγής (camouflage):** Η επίθεση παραλλαγής στοχεύει στη προσέλκυση πακέτων με σκοπό την εξαγωγή απόρρητων πληροφοριών του δικτύου, μέσω εισαγόμενων και ελεγχόμενων από τον επιτιθέμενο κόμβων.

4.3.8 Φυσικές επιθέσεις – Αναπαραγωγή κόμβου

Στόχος της φυσικής επίθεσης είναι η καταστροφή ενός κόμβου. Ένας κόμβος υπό φυσική επίθεση μπορεί να αντικατασταθεί από τον εισβολέα με έναν κόμβο υπό τον έλεγχό του (επίθεση αντιγραφής κόμβου) και προγραμματισμένο από τον ίδιο. Με αυτόν τον τρόπο, ένας εισβολέας αποκτά τη δυνατότητα ελέγχου ενός τμήματος του δικτύου ώστε να το χρησιμοποιήσει για να εξαπολύσει επίθεση στο υπόλοιπο δίκτυο. Η προστασία φυσικών επιθέσεων γίνεται εφικτή με τη χρήση φυσικής απόκρυψης των κόμβων στο περιβάλλον ανάπτυξης του δικτύου.

4.4 Σύνοψη

Σε αυτό το κεφάλαιο, έγινε αναφορά στις σημαντικές απαιτήσεις και τα κενά ασφαλείας των δικτύων WSN και εξετάστηκαν ορισμένες πιθανές επιθέσεις ασφαλείας που θα μπορούσαν να θέσουν υπό αμφισβήτηση την ασφάλεια και την αξιοπιστία του δικτύου.

Ακολουθεί ανασκόπηση (Πίνακας 4.1) των επιθέσεων σύμφωνα με τις προδιαγραφές που θέτουν υπό αμφισβήτηση και τους αντίστοιχους στόχους τους.

Πίνακας 4.1 Στόχοι επιθέσεων δικτύων WSN

Επίθεση	Επίπεδο σχεδίασης	DoS	Προδιαγραφή	Στόχος επίθεσης
Παρεμβολή (jamming)	Φυσικό επίπεδο	*	Διαθεσιμότητα Ακεραιότητα	Πλημμύρισμα τμήματος του δικτύου με θόρυβο
Αλλοίωση και υποκλοπή (tampering)		*	Διαθεσιμότητα Ακεραιότητα Πιστοποίηση Ταυτότητας	Καταστροφή κόμβων και υποκλοπή ευαίσθητων δεδομένων
Φυσική επίθεση			Διαθεσιμότητα	Καταστροφή κόμβου
Αναπαραγωγή κόμβου		*	Αυθεντικοποίηση	Αντικατάσταση κόμβου με κόμβο υπό τον έλεγχο του επιτιθέμενου
Σύγκρουση δεδομένων (collision)	Επίπεδο Ζεύξης Δεδομένων	*	Διαθεσιμότητα	Απώλεια δεδομένων
Εξάντληση ενεργειακών πόρων (exhaustion)		*		Εξάντληση ενεργειακών πόρων
Μεροληψία (unfairness)		*		Απώλεια δεδομένων
Καταβόθρα (sinkhole)	Επίπεδο Ζεύξης Δεδομένων, Επίπεδο Δικτύου		Πιστοποίηση Ταυτότητας	Έλεγχος δρομολόγησης
Σκουληκότρυπα			Πιστοποίηση Ταυτότητας	Έλεγχος δρομολόγησης
Παραπλάνηση (misdirection)	Επίπεδο Δικτύου	*	Διαθεσιμότητα Ακεραιότητα	Έλεγχος δρομολόγησης
Επιλεκτική προώθηση (selective forwarding)		*	Διαθεσιμότητα Ακεραιότητα	Απώλεια δεδομένων
Μαύρη τρύπα (black hole)		*		Απώλεια δεδομένων
HELLO flood			Πιστοποίηση Ταυτότητας	Έλεγχος δρομολόγησης
Σιβυλλική επίθεση (sybil				Δυσλειτουργία στη

attack)				ταυτοποίηση κόμβου και έλεγχος δρομολόγησης
Επίθεση homing		*	Διαθεσιμότητα	Ανίχνευση κόμβων κρίσιμης σημασίας
Πλαστογράφηση αναγνώρισης (acknowledgment spoofing)		*	Διαθεσιμότητα Ακεραιότητα	Διακίνηση ψευδών μηνυμάτων
Πλημμύρισμα (flooding)	Επίπεδο Μεταφοράς	*	Διαθεσιμότητα Ακεραιότητα	Εξάντληση πόρων
Αποσυγχρονισμός (desynchronization)		*		Δυσλειτουργίες σύνδεσης
Καταπίεση (overwhelm)	Επίπεδο Εφαρμογής	*		Εξάντληση πόρων δικτύου
Επαναπρογραμματισμός (reprogram)		*		Έλεγχος τμήματος δικτύου
Παρακολούθηση & Υποκλοπή (monitoring & eavesdropping)			Πιστοποίηση Ταυτότητας	Υποκλοπή κρίσιμων πληροφοριών
Ανάλυση κίνησης (traffic analysis)				Ανίχνευση κόμβων κρίσιμης σημασίας
Παραλλαγή (camouflage)				Εξαγωγή πληροφοριών απορρήτου

5. Μηχανισμοί Ασφαλείας Ασύρματων Δικτύων Αισθητήρων

Στο προηγούμενο κεφάλαιο, έγινε αναφορά επιθέσεων που αμφισβητούν την ασφάλεια των επικοινωνιών σε ένα δίκτυο WSN. Όπως προαναφέρθηκε, στόχοι του εισβολέα είναι να δημιουργήσει δυσκολίες στην εκπλήρωση των προδιαγραφών ασφαλείας του δικτύου. Η κακόβουλη ενέργεια, με αυτό το τρόπο, επηρεάζει τόσο την αξιοπιστία όσο και την ασφάλεια του δικτύου. Για το λόγο αυτό, είναι απαραίτητο να προβλεφθούν μηχανισμοί ασφαλείας, που λειτουργούν ως αντίμετρα στις επιθέσεις. Η αυξημένη πολυπλοκότητα είναι αποτέλεσμα των περισσότερων μηχανισμών ασφαλείας καθώς χρησιμοποιούν περισσότερους από έναν αλγόριθμους ή πρωτόκολλα επικοινωνίας. Επιπλέον, είναι απαραίτητη η χρήση μυστικών κλειδιών κρυπτογράφησης για τις συσκευές δικτύου, γεγονός που περιπλέκει περαιτέρω τον σχεδιασμό, όσον αφορά τον χειρισμό και την προστασία αυτών των μυστικών πληροφοριών. Ένας μηχανισμός ασφαλείας πρέπει να πληροί ορισμένες απαιτήσεις για να είναι κατάλληλος για χρήση σε ένα ασύρματο δίκτυο .Στη συνέχεια γίνεται αναφορά των απαιτήσεων.

- **Ασφάλεια:** Οι μηχανισμοί ασφαλείας θα πρέπει να πληρούν τις απαιτήσεις ασφαλείας, που αναφέρθηκαν στο προηγούμενο κεφάλαιο.
- **Ανθεκτικότητα:** Ο μηχανισμός ασφαλείας, σε περίπτωση πιθανής επίθεσης κόμβου, οφείλει να μην επηρεάζεται (ευρωστία) και να έχει τη δυνατότητα να διατηρεί τη λειτουργία του.
- **Εξοικονόμηση ενέργειας:** Σε ένα WSN, είναι σημαντικό να διασφαλιστεί ότι ο μηχανισμός ασφαλείας είναι συμβατός με τον στόχο της μεγιστοποίησης της διάρκειας ζωής του δικτύου. Αυτό είναι ιδιαίτερα σημαντικό αν ληφθούν υπόψιν οι περιορισμοί ενεργειακών πόρων που μπορεί να έχουν οι κόμβοι στο δίκτυο.
- **Ευελιξία:** Λόγω των διαφορετικών τύπων ανάπτυξης δικτύου, η διαχείριση κρυπτογραφικών κλειδιών και η συνολική ασφάλεια πρέπει να είναι προσαρμόσιμες.
- **Δυνατότητα κλιμάκωσης:** Η δυνατότητα αυτή αποτελεί σημαντικό μέρος ενός μηχανισμού ασφαλείας, καθώς το WSN είναι επεκτάσιμο.
- **Ανοχή σε σφάλματα:** Παρά το ενδεχόμενο ύπαρξης σφαλμάτων (ή καταστάσεων που τα προκαλούν) στο δίκτυο, ο μηχανισμός ασφαλείας οφείλει να διαθέτει ικανότητα παροχής ασφάλειας στο δίκτυο (π.χ. καταστροφή κόμβων ή παρουσία κακόβουλης ενέργειας).

5.1 Ανίχνευση Εισβολών (intrusion detection)

Οι μηχανισμοί ασφαλούς δρομολόγησης και συγκέντρωσης δεδομένων είναι σημαντικοί, αλλά δεν επαρκούν για την προστασία ενός WSN από επιθέσεις. Οι μηχανισμοί ανίχνευσης και αποτροπής εισβολών, είναι επίσης απαραίτητοι για τη διασφάλιση της πλήρους κάλυψης των απαιτήσεων ασφαλείας. Για τη παρακολούθηση και τον εντοπισμό ασυνήθιστων συμπεριφορών στο δίκτυο χρησιμοποιείται το σύστημα ανίχνευσης εισβολής (Intrusion Detection System - IDS) [60], [61]. Αυτά τα συστήματα εισβολής κατηγοριοποιούνται ως βασισμένα σε κανόνες (rule – based) [56] και βασισμένα σε ανωμαλίες (anomaly – based) [56].

Η πρώτη κατηγορία συστημάτων IDS έχει σχεδιαστεί για να ανιχνεύει γνωστά μοτίβα εισβολής, ενώ τα συστήματα IDS που βασίζονται σε ανωμαλίες αναπτύσσονται για τον εντοπισμό άγνωστων στο δίκτυο μορφών ανωμαλιών. Ορισμένα συστήματα διαθέτουν κάποιου είδους ανατροφοδότηση, όπως συναγερμό, στο δίκτυο με σκοπό την αντίδραση και την ταχύτερη επίλυση προβλημάτων. Ένα σύστημα IDS που βασίζεται σε κανόνες χαρακτηρίζεται από χαμηλότερο ποσοστό ψευδών συναγερμών ωστόσο διαθέτει λιγότερη αποτελεσματικότητα ανίχνευσης από ένα αντίστοιχο σύστημα που βασίζεται σε ανωμαλίες.

Στα ασύρματα δίκτυα αισθητήρων, λόγω των περιορισμών των υπολογισιμότητας, της αποθήκευσης και της ενέργειας, η ενημέρωση των κόμβων σχετικά με την ορθή συμπεριφορά του δικτύου δεν είναι πρακτική, λόγω του ότι είναι αναποτελεσματική ενεργειακά. Αυτό καθιστά δύσκολο τον σχεδιασμό μηχανισμών ανίχνευσης εισβολής σε ασύρματα δίκτυα αισθητήρων. Στη βιβλιογραφία γίνεται αναφορά σε τεχνικές όπως IHOP [62], LIDS [63] και SEF [64], ως λύσεις.

Η τεχνολογία IHOP (Interleaved Hop-by-Hop Authentication) βρίσκει εφαρμογή σε δίκτυα ιεραρχικής δρομολόγησης για τη διασφάλιση ικανότητας ανίχνευσης των σταθμών βάσης λανθασμένων δεδομένων που εισάγονται στο δίκτυο, με την απαίτηση πως δεν υπάρχει κακόβουλη συμπεριφορά από έναν ελάχιστο αριθμό κόμβων. Η συγκεκριμένη τεχνολογία ορίζει πως ο σταθμός βάσης μοιράζεται ένα κλειδί με τον κάθε κόμβο, και πως κάθε κόμβος μαθαίνει για τους γείτονές του (απόστασης one-hop) ανταλλάσσοντας κλειδιά μαζί του και πως κάθε κόμβος μπορεί ακόμη και να προσδιορίσει ένα κλειδί εάν απαιτείται, χωρίς παρακείμενους κόμβους. Επιπλέον, το τοπικό σύστημα ανίχνευσης εισβολών (Local Intrusion Detection System - LIDS) είναι το βασικό τμήμα του μηχανισμού που περιγράφει ο Camp.O (2002) [63]. Αυτός ο

μηχανισμός είναι συμβατός με δομημένα WSN, παρόλο που έχει σχεδιαστεί για εφαρμογές ad-hoc δικτύων [61].

Το φίλτρο στατικής δρομολόγησης (Statistical Route Filtering - SEF) έχει σχεδιαστεί για να ανιχνεύει και να απορρίπτει ψευδή δεδομένα κατά την προώθηση μηνυμάτων στο σταθμό βάσης. Η λειτουργία του μηχανισμού βασίζεται στη προϋπόθεση πως τουλάχιστον ένα ψευδές συμβάν γίνεται αντιληπτό από πολλούς κόμβους αισθητήρων που συνεργάζονται για τον εντοπισμό και την αντιμετώπιση της επίθεσης. Η ποσοστιαία απόρριψη ψευδών δεδομένων ξεπερνά το 70% σε διάστημα πέντε αλμάτων και η επίτευξη σημαντικής εξοικονόμησης ενέργειας είναι εφικτή, σύμφωνα με τους Fan Ye, Haiyun Luo, Songwu Lu and Lixia Zhang (2005) [64].

Τρείς αρχιτεκτονικές ανίχνευσης παρείσφρησης προτείνονται από τον O Brutch P. (2003) [65]. Σύμφωνα με τη πρώτη προσέγγιση αυτόνομης (stand-alone) αρχιτεκτονικής, κάθε κόμβος εντοπίζει από μόνος του κακόβουλη δραστηριότητα. Σύμφωνα με τη δεύτερη προσέγγιση κατανεμημένης και συνεργατικής αρχιτεκτονικής, σε κάθε κόμβο ορίζονται ευθύνες συνεργασίας με τους γείτονές του για την ανταλλαγή δεδομένων σχετικά με μια πιθανή εισβολή αλλά και για τον εντοπισμό τοπικών απειλών ασφαλείας. Αναφορά γίνεται, επίσης, στην αρχιτεκτονική ιεραρχίας όπου κρίνεται κατάλληλη για εφαρμογή στα ιεραρχικά δομημένα δίκτυα WSN. Τέλος, ένας μηχανισμός που προσδιορίζει εάν έχει δεχθεί επίθεση ένας ή περισσότεροι κόμβοι δικτύου από κακόβουλο εισβολέα προτείνουν οι Wang G. ,Zhang W. και Cao C. (2003) [66]. Το αποτέλεσμα του μηχανισμού αυτού καθορίζει, στη καλύτερη περίπτωση, τη μη εισβολή στο δίκτυο ή τον εντοπισμό εισβολής μέσω ανταλλαγής μηνυμάτων γειτονικών κόμβων.

Αντιμετώπιση επιθέσεων - αντίμετρα

Το μεγαλύτερο ποσοστό μηχανισμών ασφαλείας που χρησιμοποιούνται για την αντιμετώπιση των παθητικών επιθέσεων δεν θεωρούνται ανίχνευσης αλλά περισσότερο προληπτικοί - αυτό προκύπτει επειδή οι παθητικές επιθέσεις θέτουν δύσκολο τον εντοπισμό τους, καθώς ο εισβολέας δεν κάνει καμία τροποποίηση στα πακέτα που μεταδίδονται. Όπως θα αναφερθεί στη συνέχεια, η αντιμετώπιση επιθέσεων παθητικής μορφής γίνεται κυρίως με κρυπτογραφημένους αλγόριθμους. Αντίθετα, οι επιθέσεις ενεργής μορφής περιλαμβάνουν την απόκριση σε μια επίθεση προκειμένου να ανακτηθεί το δίκτυο από τις δυσκολίες που προκαλούνται από αυτήν. Ωστόσο, η πρόληψη μιας ενεργητικής επίθεσης καθίσταται πιο δύσκολη καθώς η επίτευξή της απαιτεί συνεχή φυσική προστασία όλων των δομών και καναλιών επικοινωνίας.

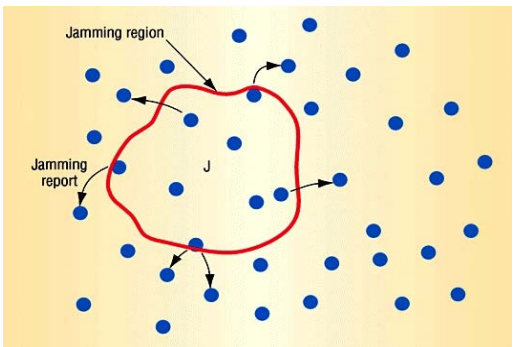
5.1.1 Αντιμετώπιση επιθέσεων DoS

Στην υποενότητα αυτή παρουσιάζονται μέθοδοι αντιμετώπισης επιθέσεων DoS οι οποίες βασίζονται στην πολυεπίπεδη αρχιτεκτονική του δικτύου WSN.

5.1.1.1 Φυσικό επίπεδο

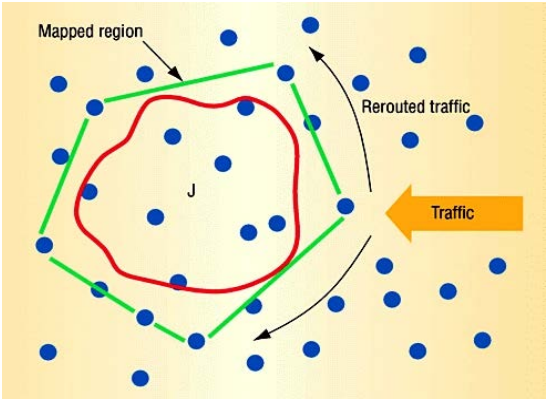
Οι τεχνικές όπως μεταπήδηση συχνότητας εξάπλωσης φάσματος FHSS (Frequency – hopping spread spectrum) και διαμόρφωσης φάσματος (Code spreading) συμβάλουν στην αντιμετώπιση επιθέσεων παρεμβολής. Η τεχνική διαμόρφωσης φάσματος, δεν θεωρείται δημοφιλής στα WSN, διότι είναι πιο περίπλοκη με συνέπεια την αύξηση κατανάλωσης ενέργειας και υπολογιστικών πόρων των κόμβων. Επιπλέον, οι Perrig A. ,Stankovic J. και Wagner D. (2004) [67] αναφέρουν μια πρόσθετη τεχνική για την αντιμετώπιση των παρεμβολών. Αυτή η τεχνική λειτουργεί με τη λογική εξαίρεσης της περιοχής, που έχει επηρεαστεί από την επίθεση παρεμβολής, από το σχέδιο δρομολόγησης. Η συνεισφορά των επηρεαζόμενων κόμβων, αλλά και των γειτονικών τους, είναι ζωτικής σημασίας για τον εντοπισμό επιθέσεων και την ενημέρωση των σταθμών βάσης.

Η τεχνική αναπήδησης συχνότητας χρησιμοποιεί ένα σήμα φορέα με στενό φάσμα, το οποίο αλλάζει συνεχώς, σύμφωνα με μια ψευδο-τυχαία ακολουθία, την κεντρική του συχνότητα. Το σήμα εκπέμπεται, για μικρό χρονικό διάστημα, σε μια συχνότητα και στη συνέχεια μεταπηδά σε μια άλλη. Ο αλγόριθμος αναπήδησης συχνότητας γνωστοποιείται, τόσο στον πομπό όσο και στον δέκτη, εκ των προτέρων. Σε περίπτωση που ληφθεί σήμα από δέκτη μη εξουσιοδοτημένο, ερμηνεύεται ως μικρής διάρκειας θόρυβος και αγνοείται. Ο εισβολέας δεν δύναται να προβλέψει την επακριβή ακολουθία αναπήδησης και επομένως δεν μπορεί να δημιουργήσει συνοδευτικές παρεμβολές. Ωστόσο, δεδομένου ότι το διαθέσιμο φάσμα διαθέτει περιορισμούς, ένας εισβολέας θα επιτύχει τον στόχο του εάν πραγματοποιήσει παρεμβολή σε ολόκληρο το φάσμα των διαθέσιμων συχνοτήτων.



Εικόνα 5.1. Οι προσβεβλημένοι κόμβοι καθώς και οι γειτονικοί τους επιχειρούν ενημέρωση της κατάστασής τους (jamming report)

Πηγή: https://doi.ieeecomputersociety.org/10.1109/MC.2002.1039518



Εικόνα 5.2. Αποκλεισμός προσβεβλημένης περιοχής σύμφωνα με την τεχνική αντιμετώπισης επίθεσης παρεμβολής [68]

Πηγή: https://doi.ieeecomputersociety.org/10.1109/MC.2002.1039518

Ο μηχανισμός προστασίας από παραβίαση των συσκευών που απαρτίζουν το δίκτυο μπορεί να αντισταθεί σε επιθέσεις παραβίασης ή υποκλοπής. Η επιτυχία εξαρτάται από διάφορους παράγοντες όπως, την πληρότητα και ακρίβεια με την οποία εξετάστηκαν οι πιθανές απειλές, τους διαθέσιμους πόρους, καθώς και από την αποτελεσματικότητα και την ευφυία των επιτιθέμενων. Η φυσική απόκρυψη των συσκευών στο περιβάλλον εφαρμογής τους, καθώς και οι μηχανισμοί αυτόματης απενεργοποίησης της συσκευής σε περίπτωση παραβίασης (self-termination) παρέχουν πρόσθετη προστασία από τέτοιες επιθέσεις.

5.1.1.2 Επίπεδο Ζεύξης Δεδομένων

Η εν μέρει αντιμετώπιση της επίθεσης σύγκρουσης δεδομένων επιτυγχάνεται χρησιμοποιώντας κώδικες διόρθωσης σφαλμάτων (error-correcting codes). Αυτοί οι κώδικες λειτουργούν ορθά για μικρές διενέξεις, αλλά προσθέτουν πολυπλοκότητα. Σε μια μεγαλύτερη επίθεση στο δίκτυο, αυτοί οι κώδικες ενδέχεται να μην λειτουργούν αποδοτικά, δημιουργώντας έτσι κενά ασφαλείας σε ένα δίκτυο WSN. Αποτελεσματική ορίζεται η αποφυγή χρήσης πρωτοκόλλων MAC που χρησιμοποιούν το σχήμα RTS/CTS.

Η επίθεση εξάντλησης ενεργειακών πόρων μπορεί να αντιμετωπιστεί χρησιμοποιώντας πολλαπλή πρόσβαση διαίρεσης χρόνου (TDMA). Έτσι, επιτρέπει τη χρονική διαχώριση των κόμβων με την ανάθεσή τους σε καθεμία από αυτές τις χρονοθυρίδες (timeslots). Είναι σημαντικό να επιτευχθεί ο συγχρονισμός των κόμβων, διαφορετικά προκύπτουν ζητήματα παρεμβολής μεταξύ αυτών. Συμπληρωματικά, για την αντιμετώπιση αυτής της επίθεσης, τα πακέτα μπορούν να δρομολογηθούν μόνο μετά τον

έλεγχο ταυτότητας του αποστολέα και τα πακέτα που είναι μεγαλύτερα από το μέγεθος του πακέτου εφαρμογής μπορούν να αποκλειστούν.

Όσον αφορά την καταπολέμηση των επιθέσεων μεροληψίας, χρησιμοποιούνται πλαίσια δεδομένων μικρού μεγέθους, έτσι ώστε το χρονικό διάστημα πρόσβασης κάθε κόμβου στο κανάλι να είναι σύντομο. Αντίθετα, τα μικρότερα σε μέγεθος πλαίσια είναι συχνά λιγότερο αποτελεσματικά και οι εισβολείς μπορεί να προσπαθήσουν να αναμεταδώσουν γρήγορα αντί να περιμένουν ένα τυχαίο χρονικό διάστημα, καθιστώντας τους ευάλωτους σε πρόσθετες επιθέσεις.

5.1.1.3 Επίπεδο Δικτύου

Ο πιο αποτελεσματικός τρόπος αντιμετώπισης επιθέσεις επιπέδου δικτύου είναι η χρήση ενός πρωτοκόλλου δρομολόγησης για την παρακολούθηση του δικτύου και τον εντοπισμό μη φυσιολογικής συμπεριφοράς. Αυτή η ανώμαλη συμπεριφορά στη συνέχεια απομονώνεται δημιουργώντας εναλλακτικές διαδρομές δρομολόγησης. Μόνο με τη συμμετοχή εξουσιοδοτημένων κόμβων στη δρομολόγηση προσφέρεται πρόσθετη ασφάλεια. Τέλος, ο πλεονασμός μεταδιδόμενης κυκλοφορίας (redundancy) βοηθά στην προστασία από κακόβουλες ενέργειες.

5.1.1.4 Επίπεδο Μεταφοράς

Η τεχνική client puzzles [67] συμβάλει στην αντιμετώπιση επιθέσεων πλημμύρας (flooding). Τα client puzzles μοιράζονται στους κόμβους από τους σταθμούς βάσης του δικτύου και κάθε κόμβος που τα λύνει επιβεβαιώνει την έγκυρη σύνδεσή του. Ένας εισβολέας αναγκάζεται να τα επιλύσει προκειμένου να εκτελέσει κακόβουλες λειτουργίες στο δίκτυο. Άλλα αντίμετρα παρέχουν μέτρα περιορισμού σύνδεσης και μηχανισμούς ελέγχου ταυτότητας.

Ένα αντίμετρο κατά των επιθέσεων αποσυγχρονισμού είναι ο έλεγχος ταυτότητας (αυθεντικοποίηση) όλων των συναλλασσόμενων πακέτων, όπως επίσης και των πεδίων ελέγχου που περιέχονται στις κεφαλίδες του πρωτοκόλλου μεταφοράς. Οι συμμετέχοντες κόμβοι θα έχουν τη δυνατότητα ανίχνευσης και αγνόησης κακόβουλων πακέτων, με την υπόθεση πως ο επιτιθέμενος δεν θα έχει την ικανότητα παράκαμψης του μηχανισμού ελέγχου.

5.1.2 Αντίμετρα – Επίθεση καταβόθρας

Ανθεκτικότητα στα WSN έναντι επιθέσεων καταβόθρας, παρέχουν τα κρυπτογραφικά πρωτόκολλα δρομολόγησης RESIST-0 και RESIST-1 (RESIlient and Simple Topology-

based reconfiguration protocols) [69] αλλά με κόστος αυξημένης πολυπλοκότητας. Επιπλέον, το πρωτόκολλο δρομολόγησης Mint-Route [70], [71], [72] παρέχει τη δυνατότητα εντοπισμού και αντιμετώπισης της επίθεσης αυτής. Στο συγκεκριμένο πρωτόκολλο, κάθε κόμβος εφαρμόζει ένα «δέντρο δρομολόγησης» στον σταθμό βάσης σύμφωνα με υπολογισμούς ποιότητας σύνδεσης (Link Quality) με τους γείτονές του. Η ποιότητα της σύνδεσης προκείπτει από το ποσοστό των χαμένων πακέτων ή τον επιτυγχανόμενο λόγο σήματος προς θόρυβο (SNR). Για την υλοποίηση ενός δέντρου δρομολόγησης, κάθε κόμβος στέλνει περιοδικά πακέτα ενημέρωσης δρομολόγησης που περιέχουν αυτές τις πληροφορίες στον σταθμό βάσης. Για να διατηρείται ενημερωμένο το δέντρο δρομολόγησης, κάθε κόμβος στέλνει περιοδικά ενημερώσεις διαδρομής (route update packet) στον σταθμό βάσης. Κάθε κόμβος διατηρεί, στον πίνακα γειτόνων (neighbor table), τις ταυτότητες των γειτονικών κόμβων του. Ο πίνακας αυτός, ενημερώνεται συνεχώς με στόχο την εύρεση ζεύξεων υψηλότερης ποιότητας (higher interface quality) μεταξύ γειτονικών κόμβων.

5.1.3 Αντίμετρα – Σιβυλλική επίθεση

Προσεγγίσεις για την αντιμετώπιση της σιβυλλικής επίθεσης αναφέρουν Οι Douceur J., Levine N., και Shields C. [73] [74]. Ο έλεγχος ταυτότητας των κόμβων που συμμετέχουν στο δίκτυο ορίζεται ως βασικός παράγοντας στις στρατηγικές. Η πρώτη προσέγγιση είναι η χρήση συμμετρικής κρυπτογράφησης δημόσιου κλειδιού. Για την εξάλειψη της επίθεσης και τη διασφάλιση πιστοποιημένης ταυτότητας κάθε οντότητας στο δίκτυο, χρησιμοποιείται η αξιόπιστη προσέγγιση πιστοποίησης (trusted certification). Κατά τη προσέγγιση αυτή, κρίνεται αναγκαία η εύρεση των κλεμμένων από τον επιτιθέμενο ή χαμένων ταυτοτήτων και, εν συνεχεία, η ανάκληση αυτών. Η δεύτερη προσέγγιση αφορά τη δοκιμή πόρων (resource testing), προκειμένου να ανιχνευθούν κόμβοι που μπορεί να λειτουργούν με λιγότερους από τους αναμενόμενους πόρους (υπολογισμών, αποθήκευσης, εύρος ζώνης). Αυτή η προσέγγιση προσφέρει μια μερική λύση και είναι περισσότερο αποτρεπτική. Μια άλλη προσέγγιση είναι η προσέγγιση των επαναλαμβανόμενων δαπανών και τελών (recruiting costs and fees) η οποία βασίζεται στον, κατά διαστήματα, επαναπροσδιορισμό ταυτοτήτων και στη πραγματοποίηση δοκιμών επικύρωσης. Τα συστήματα φήμης (reputation systems) οι αξιόπιστες συσκευές (trusted devices) και παρατήρησης (observation) [74], θεωρούνται επιπρόσθετες προσεγγίσεις.

5.1.4 Αντίμετρα - Σκουληκότρυπα

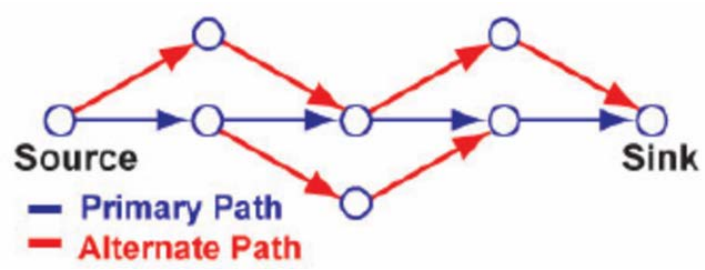
Το πρωτόκολλο δρομολόγησης DAWSSEN (Defense mechanism Against Wormhole attacks in Wireless Sensor Networks) παρουσιάζεται από τους Kaissi E. ,Dawy Z. και Kayssi A. (2005) [75]. Είναι ένα πρωτόκολλο δρομολόγησης , προληπτικό, που θεμελιώνεται σε μια ιεραρχική δομή του δικτύου WSN.

Επιπλέον, οι Perrig A. ,Stankovic J. και Wagner D. (2004) [67] παρουσιάζουν λύσεις που βασίζονται στη χρήση γεωγραφικής τοποθεσίας (geographic) ή πληροφορίας χρόνου (temporal) από τους κόμβους.

5.1.5 Αντίμετρα – Επίθεση ανάλυσης κίνησης

Για τον χειρισμό της επίθεσης ανάλυσης κίνησης τρεις μέθοδοι έχουν προταθεί σύμφωνα με τον Jing Deng M. [59]. Σκοπός των μεθόδων είναι η παραπλάνηση του εισβολέα, κατά τη πιθανή προσπάθειά του να εντοπίσει τη θέση του σταθμού βάσης, δημιουργώντας κινήσεις εντός του δικτύου προς τυχαίες κατευθύνσεις.

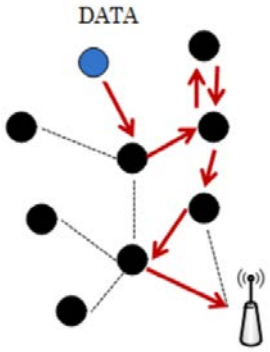
Η πρώτη τεχνική που εφαρμόζει αυτή τη λογική είναι η MPR (multiple parent routing), η οποία επιτρέπει στα πακέτα να δρομολογούνται από τον κόμβο αισθητήρα στον σταθμό βάσης μέσω εναλλακτικών διαδρομών (Εικόνα 5.3) αντί της συντομότερης διαδρομής.



Εικόνα 5.3. Τεχνική αντιμετώπισης κίνησης: Συντομότερο μονοπάτι δρομολόγησης & τεχνική MPR

https://www.researchgate.net/profile/Boleslaw_Szymanski/publication/221420430/figure/fig4/AS:305477851336707@1449843003490/Braided-Multi-path-routing-1.png

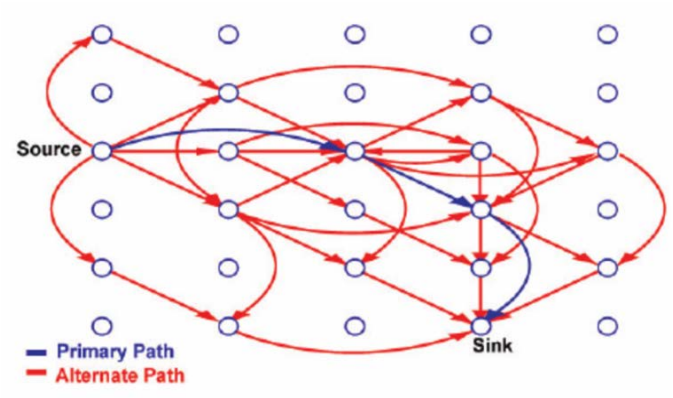
Η δεύτερη τεχνική RW (random walk, Εικόνα 5.4) χρησιμοποιεί έναν αλγόριθμο προώθησης που εισάγει την τυχαιότητα στον προσδιορισμό της διαδρομής δρομολόγησης. Οποιοσδήποτε κόμβος λάβει ένα πακέτο το αποστέλλει εξίσου σε οποιονδήποτε από τους γείτονές του, γεγονός που καθιστά πιο δύσκολο για έναν εισβολέα να καθορίσει τη διαδρομή. Ωστόσο, η τεχνική RW μπορεί να οδηγήσει σε μεγάλες διαδρομές δρομολόγησης, οι οποίες μπορούν να οδηγήσουν σε υψηλότερη μέση κατανάλωση ενέργειας των κόμβων.



Εικόνα 5.4. Τεχνική αντιμετώπισης κίνησης RW

Πηγή: https://www.researchgate.net/profile/Fabrice-Valois/publication/45908491/figure/fig10/AS:307397819158532@1450300759277/Random-Walk-Routing-Data-dissemination.png

Η τρίτη μέθοδος που αναφέρεται ως κλασματική διάδοση (fractal propagation) βασίζεται στη δημιουργία εικονικής κίνησης στο δίκτυο (Εικόνα 5.5) και στη δημιουργία πλαστών πακέτων. Κάθε κόμβος, σύμφωνα με αυτή την τεχνική, λαμβάνει ένα πακέτο και στη συνέχεια δημιουργεί με καθορισμένη πιθανότητα ένα ψεύτικο πακέτο και το προωθεί σε έναν γειτονικό κόμβο. Με βασικό, όμως, μειονέκτημα τη μεγάλη πιθανότητα δημιουργίας βαριάς κυκλοφορίας πλησίον του σταθμού βάσης, με αποτέλεσμα την αύξηση απωλειών και συγκρούσεων πακέτων.



Εικόνα 5.5. Τεχνική αντιμετώπισης κίνησης κλασματικής διάδοσης

https://www.researchgate.net/profile/Boleslaw_Szymanski/publication/221420430/figure/fig6/AS:305477851336709@1449843003571/figure-fig6.png

5.1.6 Αντίμετρα – Επιθέσεις κατά του απορρήτου

Οι Walters, Liang, Shi, & Chaudhary (2007) [76] αναφέρουν διάφορες στρατηγικές για την αντιμετώπιση των επιθέσεων απορρήτου. Οι μηχανισμοί ανωνυμίας ορίζονται ως ένα από τα βασικά αντίμετρα. Οι μηχανισμοί αυτοί βρίσκουν εφαρμογή με την τροποποίηση της κυκλοφορίας δεδομένων, την εξασφάλιση ενός ασφαλούς καναλιού επικοινωνίας και με την αποκέντρωση ευαίσθητων δεδομένων. Οι τεχνικές που

περιγράφονται στην προηγούμενη παράγραφο (MPR, RW, fractal propagation) υλοποιούν τη τροποποίηση της κυκλοφορίας δεδομένων. Τα ασφαλή πρωτόκολλα επικοινωνίας (π.χ. SPINS) υλοποιούν την εξασφάλιση ενός καναλιού επικοινωνίας. Η μεθοδολογία της αποκέντρωσης δεδομένων είναι ο διαμοιρασμός των πληροφοριών σε γειτονικούς κόμβους, έτσι ώστε οι πληροφορίες να μην είναι εξ ολοκλήρου διαθέσιμες σε έναν μόνο κόμβο [76]. Παρόμοιες στρατηγικές, όπως πλημμύρισμα φαντάσματος (phantom flooding), πλημμύρισμα με ψεύτικα μηνύματα (flooding with fake messages), πιθανολογική πλημμύρα (probabilistic flooding) και το πλημμύρισμα αρχικής τιμής (baseline flooding) έχουν στόχο τη παραπλάνηση του εισβολέα ως προς την δρομολόγηση των πακέτων στο δίκτυο [76].

5.1.7 Αντίμετρα – Φυσικές επιθέσεις, αναπαραγωγή κόμβου

Οι μηχανισμοί FHSS και διαμόρφωσης φάσματος ενεργούν κατά των παρεμβολών προσφέροντας κάποιο βαθμό προστασίας έναντι ενός εισβολέα που ανιχνεύει τη θέση των κόμβων. Πρόσθετος αμυντικός μηχανισμός, μπορεί να θεωρηθεί, ο εξοπλισμός των κόμβων με υλικό αντίστασης (hardware) που έχει ως σκοπό την αποτροπή υποκλοπής ή τροποποίησης δεδομένων από τον επιτιθέμενο. Ο αυτό-τερματισμός (self termination) της συσκευής, προσφέρει λύση αντιμετώπισης φυσικών επιθέσεων. Συγκεκριμένα, εφόσον ο κόμβος ανιχνεύσει μια πιθανή επίθεση, τερματίζει τη λειτουργία του καταστρέφοντας έτσι κρυπτογραφικά κλειδιά και δεδομένα. Σε δίκτυα με πλεονασμό πληροφοριών, αυτή η τεχνική είναι η πιο αποτελεσματική. Τέλος, σύμφωνα με τους Walters, Liang, Shi, & Chaudhary (2007) [76] η αντιμετώπιση επιθέσεων αναπαραγωγής κόμβου επιτυγχάνεται με χρήση αλγορίθμων τυχαιοποιημένης πολυεκπομπής (randomized multicast) και αλγορίθμων γραμμικής πολυεκπομπής (line-select multicast).

5.1.8 Σύνοψη

Λύσεις σε θέματα προστασίας των εφαρμοσμένων πρωτοκόλλων δρομολόγησης ενός δικτύου WSN προσφέρουν, η αυθεντικοποίηση, η κρυπτογράφηση, η επιβεβαίωση ταυτότητας, η πολυδιαδρομική δρομολόγηση, αυθεντικοποίηση εκπομπών και η αμφίδρομη επιβεβαίωση ζεύξης. Σημαντικό ρόλο έχει η σχεδίαση πρωτοκόλλων επιπέδου δικτύου ώστε να περιορίζονται οι επιπτώσεις των επιθέσεων διότι οι περισσότερες επιθέσεις στοχεύουν στη μη ορθή δρομολόγηση πακέτων στο δίκτυο. Στον Πίνακα 5.1 παραθέτονται οι μηχανισμοί ασφαλείας που χρησιμοποιούνται για την αντιμετώπιση των ζητημάτων που αναφέρονται σε αυτό το κεφάλαιο.

Πίνακας 5.1 Μηχανισμοί αντιμετώπισης επιθέσεων

Επίθεση	Μηχανισμοί αντιμετώπισης
Παρεμβολή	Τεχνική μεταπήδησης συχνότητας, Τεχνική διαμόρφωσης φάσματος
Αλλοίωση και υποκλοπή	Μηχανισμοί προστασίας παραβίασης, Φυσική απόκρυψη, Μηχανισμοί απενεργοποίησης
Φυσική επίθεση	Φυσική απόκρυψη
Αναπαραγωγή κόμβου	Φυσική απόκρυψη, Κρυπτογράφηση
Σύγκρουση δεδομένων	Κώδικας διόρθωσης σφαλμάτων, Αποφυγή χρήσης πρωτοκόλλων MAC σχήματος RTS/CTS
Σκουληκότρυπα	Πρωτόκολλο DAWWSEN [75] , Χρήση πληροφοριών θέσης και χρόνου [78]
Μεροληψία	Χρήση μικρών σε μήκος πακέτων
Καταβόθρα	Πρωτόκολλο δρομολόγησης Mint-Route [70] [71] [72], Κρυπτογραφικά πρωτόκολλα RESIST-0/RESIST-1 [77]
Πλημμύρισμα	Client puzzles, Περιορισμός συνδέσεων, Αυθεντικοποίηση
Παραπλάνηση	Τεχνικές αυθεντικοποίησης
Επιλεκτική προώθηση	Τεχνικές πλεονασμού
Μαύρη τρύπα	Τεχνικές αυθεντικοποίησης
Hello flood	Τεχνικές αυθεντικοποίησης
Σιβυλλική επίθεση	Πιστοποίηση ταυτότητας [73]
Επίθεση homing	Κρυπτογράφηση
Πλαστογράφηση αναγνώρισης	Τεχνικές αυθεντικοποίησης
Ανάλυση κίνησης	Τεχνικές MPR - RW, Κλασματικής διάδοσης
Αποσυγχρονισμός	Τεχνικές αυθεντικοποίησης
Παρακολούθηση & Υποκλοπή	Κρυπτογράφηση, Τεχνική μεταπήδησης συχνότητας
Εξάντληση ενεργειακών πόρων	Χρήση πολλαπλής προσπέλασης διαίρεσης χρόνου, Δρομολόγηση μετά από αυθεντικοποίηση αποστολέα, Φραγή πακέτων υπερμεγέθους
Παραλλαγή	Τεχνικές αυθεντικοποίησης
Επιθέσεις κατά του απορρήτου	Μηχανισμοί ανωνυμίας

5.2 Κρυπτογράφηση

Η κρυπτογράφηση (encryption) [79], [80], είναι ένας μηχανισμός για την αντιμετώπιση επιθέσεων που στοχεύουν στη διαρροή πληροφοριών δικτύου με στόχο το μετασχηματισμό του μηνύματος κόμβου αποστολέα σε κατανοητή μορφή, αποκλειστικά και μόνο από το κόμβο παραλήπτη, χρησιμοποιώντας ένα μυστικό κλειδί. Επειδή τα WSN είναι περιορισμένα όσον αφορά την επεξεργασία δεδομένων και την κατανάλωση ενέργειας, χρησιμοποιείται εξ ολοκλήρου η συμμετρική κρυπτογράφηση η οποία αναφέρεται στη βιβλιογραφία και ως κρυπτογράφηση μυστικού/ιδιωτικού κλειδιού.

Προσφέρουν αποτελεσματική προστασία, σε ένα ασύρματο δίκτυο των ροών δεδομένων (data streams), οι μηχανισμοί κρυπτογράφησης. Απαραίτητη είναι η παράθεση των βασικών ορισμών των κρυπτογραφικών συστημάτων για την επιδίωξη πληρέστερης κατανόησης των μηχανισμών αυτών.

- **Αρχικό ή απλό κείμενο (plaintext)** Στην κρυπτογραφία, το απλό κείμενο είναι συνήθως αναγνώσιμο κείμενο πριν κρυπτογραφηθεί σε κρυπτογραφημένο κείμενο ή αναγνώσιμο κείμενο αφού αποκρυπτογραφηθεί. Η είσοδος ή η έξοδος δεδομένων από αλγόριθμους κρυπτογράφησης δεν είναι πάντα απλό κείμενο. Για παράδειγμα, όταν τα δεδομένα είναι υπερκρυπτογραφημένα ή κρυπτογραφημένα περισσότερες από μία φορές χρησιμοποιώντας διαφορετικούς αλγόριθμους κρυπτογράφησης, μόνο η είσοδος στην πρώτη μέθοδο κρυπτογράφησης θεωρείται απλό κείμενο. Κρυπτογραφημένο κείμενο (ciphertext), αντίστοιχα, είναι το κείμενο που μετασχηματίζεται από απλό κείμενο χρησιμοποιώντας έναν αλγόριθμο κρυπτογράφησης. Ο κόμβος παραλήπτης, καθώς λαμβάνει το κρυπτογραφημένο κείμενο, δε μπορεί να το ερμηνεύσει και καλείται να το αποκρυπτογραφήσει με τη χρήση ενός κλειδιού. Το κρυπτογραφημένο κείμενο εξαρτάται τόσο από το κλειδί κρυπτογράφησης όσο και από το απλό κείμενο. Συμπερασματικά, μέσω του αλγόριθμου κρυπτογράφησης, για ένα δεδομένο πρωτότυπο κείμενο που χρησιμοποιεί το ίδιο κλειδί, θα ληφθούν διαφορετικά κρυπτογραφημένα κείμενα.
- **Αλγόριθμος κρυπτογράφησης (encryption algorithm)** ορίζεται η διαδικασία μετατροπής αναγνώσιμου κειμένου σε μη αναγνώσιμη μορφή. Αυτή η μέθοδος περιλαμβάνει αντικαταστάσεις και μετασχηματισμούς στο απλό κείμενο (plaintext). Αντίστροφα, ο αλγόριθμος αποκρυπτογράφησης (decryption algorithm) είναι η διαδικασία μετατροπής μη αναγνώσιμου κρυπτογραφημένου κειμένου σε απλό κείμενο (plaintext).

- **Κρυπτογράφηση (encryption)** ορίζεται η διαδικασία μέσω της οποίας το επιθυμητό κείμενο κωδικοποιείται έτσι ώστε να παραμείνει κρυφό ή απρόσιτο σε μη εξουσιοδοτημένους χρήστες ενώ αποκρυπτογράφηση (decryption) ορίζεται η μετατροπή των κρυπτογραφημένων δεδομένων στην αρχική τους μορφή. Με λίγα λόγια, είναι μια αντίστροφη διαδικασία κρυπτογράφησης. Αποκωδικοποιεί τις κρυπτογραφημένες πληροφορίες έτσι ώστε μόνο ένας εξουσιοδοτημένος χρήστης να έχει τη δυνατότητα να αποκρυπτογραφήσει τα δεδομένα καθώς η αποκρυπτογράφηση απαιτεί μυστικό κλειδί ή κωδικό πρόσβασης.
- **Κλειδί (key) κρυπτογράφησης** είναι συνήθως μια τυχαία συμβολοσειρά bits που δημιουργείται ειδικά για την κωδικοποίηση και αποκωδικοποίηση δεδομένων. Τα κλειδιά κρυπτογράφησης δημιουργούνται με αλγόριθμους σχεδιασμένους να διασφαλίζουν ότι κάθε κλειδί είναι μοναδικό και απρόβλεπτο. Όσο μεγαλύτερο είναι το κλειδί που κατασκευάζεται με αυτόν τον τρόπο, τόσο πιο δύσκολο είναι να παραβιαστεί.

5.2.1 Μέθοδοι κρυπτογράφησης

Τα διακινούμενα μηνύματα του δικτύου μπορούν να κρυπτογραφηθούν με δύο τρόπους. Σύμφωνα με το πρώτο τρόπο, γίνεται χρήση της κρυπτογράφησης ζεύξης (link encryption), η οποία σε κάθε συσκευή του δικτύου κρυπτογραφεί τα πακέτα δεδομένων, έτσι ώστε πριν τη δρομολόγηση να έχει πραγματοποιηθεί ο προσδιορισμός του παραλήπτης. Σύμφωνα με το δεύτερο τρόπο, με τη χρήση κρυπτογράφησης από άκρο σε άκρο (end-to-end encryption – E2EE), η οποία κρυπτογραφεί τα πακέτα δεδομένων από τον αποστολέα στον παραλήπτη και κρατά μυστικό το περιεχόμενο των μηνυμάτων. Κάθε συσκευή πρέπει να εφαρμόσει τους αλγόριθμους κρυπτογράφησης και αποκρυπτογράφησης έχοντας γνώση του κλειδιού κρυπτογράφησης. Η ιδιαιτερότητα της κρυπτογράφησης E2EE έγκειται στο τρόπο λειτουργίας τής, καθώς η κρυπτογράφηση και η επακόλουθη αποκρυπτογράφηση πραγματοποιείται αποκλειστικά και μόνο στον κόμβο πηγής των πληροφοριών και στον τελικό παραλήπτη. Ως αποτέλεσμα, οι ενδιάμεσοι κόμβοι που προωθούν τα πακέτα κατά τη δρομολόγηση πολλαπλών βημάτων δεν θέτουν σε λειτουργία τους αλγόριθμους κρυπτογράφησης ή αποκρυπτογράφησής τους. Αυτό σημαίνει ότι παίρνουν ένα κρυπτόγραμμα και το προωθούν ως έχει, πράγμα που αναγκάζει τον κόμβο πηγής των πακέτων να μην κρυπτογραφεί την επικεφαλίδα του πακέτου δεδομένων. Αυτό καθιστά τα δίκτυα που βασίζονται σε κρυπτογράφηση από άκρο σε άκρο επιρρεπή Οι επιθέσεις ανάλυσης κυκλοφορίας, μπορούν να

εκμεταλλευτούν το γεγονός αυτό, καθώς δεν καλύπτεται το μοτίβο της κυκλοφορίας πακέτων, αφήνοντάς το ανοιχτό σε πιθανές επιθέσεις.

5.2.2 Κρυπτογραφικοί αλγόριθμοι

Οι αλγόριθμοι κρυπτογράφησης ταξινομούνται σε ασύμμετρους, συμμετρικούς και υβριδικούς. Οι ασύμμετροι αλγόριθμοι χρησιμοποιούν, για κρυπτογράφηση, ένα δημόσιο κλειδί και για την αποκρυπτογράφηση, ένα μυστικό κλειδί για κάθε παραλήπτη. Οι συμμετρικοί αλγόριθμοι χρησιμοποιούν, τόσο για κρυπτογράφηση όσο και για αποκρυπτογράφηση, το ίδιο κλειδί. Οι υβριδικοί αλγόριθμοι είναι ένας συνδυασμός των παραπάνω, χρησιμοποιώντας αρχικά ασύμμετρους αλγόριθμους για τη διανομή κλειδιών σε όλους τους συμμετέχοντες στο δίκτυο, και όταν τα κλειδιά γίνουν γνωστά σε όλο το δίκτυο χρησιμοποιούνται συμμετρικοί αλγόριθμοι. Οι DES (Data Encryption Standard), AES (Advanced Encryption Standard), RC4, RC5, Kasumi, Camellia, Serpent, MISTY1, SHA-1, MD5, IDEA και TEA είναι μερικοί από τη πληθώρα συμμετρικών αλγορίθμων κρυπτογράφησης που έχουν προταθεί στη βιβλιογραφία. Επιπρόσθετα, οι RSA, NTRU, El-Gamal, PGP, GPG, ελλειπτικών καμπυλών (ECC) και οι SSL [60], [79] θεωρούνται από τους πιο σημαντικούς ασύμμετρους και υβριδικούς αλγόριθμους κρυπτογράφησης.

Η εφαρμογή κρυπτογράφησης πραγματοποιείται σύμφωνα με δύο τρόπους. Με τον πρώτο τρόπο, γίνεται ανάλυση του αρχικού κειμένου σε n μέρη ψηφίων (block cipher). Στη συνέχεια, κάθε μέρος υποβάλλεται σε ανεξάρτητη κρυπτογράφηση από το υπόλοιπο αρχικό κείμενο. Οι αλγόριθμοι που χρησιμοποιούν αυτή την τεχνική ονομάζονται αλγόριθμοι κατάτμησης. Η δεύτερη μέθοδος κρυπτογράφησης είναι η κρυπτογράφηση ροής (stream cipher). Αυτή η τεχνική χρησιμοποιείται για την κρυπτογράφηση κάθε ψηφίου ξεχωριστά και οι αλγόριθμοι που χρησιμοποιούνται ονομάζονται αλγόριθμοι ροής. Στους αλγόριθμους αυτούς έγκειται η δυσκολία συγχρονισμού πομπού και δέκτη, θέτοντας την εξαγωγή του αρχικού κειμένου από τον υποκλοπέα δυσμενότερη. Πιο δημοφιλής αλγόριθμος τμημάτων είναι ο AES ενώ ροής ο RC5.

Η χρήση πιο περίπλοκων ασύμμετρων και υβριδικών αλγορίθμων κρυπτογράφησης δεν προτιμάται λόγω των περιορισμών των δυνατοτήτων επεξεργασίας των κόμβων [61].

Σε εφαρμογές WSN, βέλτιστος αλγόριθμος κρυπτογράφησης είναι ο AES. Το προηγμένο πρότυπο κρυπτογράφησης AES (Advanced Encryption Standard – AES [79], [80], [56]) του ινστιτούτου NIST (National Institute of Standards and Technology) σχεδιάστηκε το 1997 ως επέκταση του προτύπου κρυπτογράφησης δεδομένων (Data Encryption Standard – DES, [79], [80], [56]) και είναι ο πλέον δημοφιλής σε δίκτυα

WSN και βρίσκει εφαρμογή στα πρότυπα ZigBee και Bluetooth LE. Ο σκοπός της επέκτασης ήταν να δημιουργηθεί ένας ισχυρότερος κρυπτογραφικός αλγόριθμος που είναι πιο δύσκολο να παραβιαστεί, καθώς τα χρησιμοποιούμενα κλειδιά κρυπτογράφησης θα γίνονταν μεγαλύτερα. Ο αλγόριθμος AES υπερέχει σε ταχύτητα είναι πιο προσιτός στην εφαρμογή του και απαιτεί χαμηλότερη χρήση μνήμης έναντι του DES. Τέλος, το μέγεθος τμήματος εισόδου καθορίζεται από τον αλγόριθμος AES και είναι 128 ψηφία όπως, επίσης, και το μήκος κλειδιού που θα πρέπει να είναι 128, 192 ή 256 ψηφία. Σε δημοφιλή πρότυπα WSN (ZigBee, Bluetooth LE) γίνεται εφαρμογή του αλγορίθμου AES-128bits όπου, με βάση αυτό το μήκος κλειδιού (μεγέθους 39 ψηφίων) υπάρχουν 2128 ≈ 3*1038 συνδιασμοί κλειδιών σε αντίθεση με τον αλγόριθμος DES ο οποίος προβλέπει 256 διατάξεις κλειδιών.

5.3 Ασφάλεια διασταυρωμένου επιπέδου (Cross Layer Security)

Προκειμένου να αντιμετωπιστούν τα προβλήματα ασφάλειας στα ασύρματα δίκτυα, συνήθως δίνεται μεγάλη προσοχή στην πολυεπίπεδη αρχιτεκτονική αυτών των δικτύων. Μια διαφορετική προσέγγιση των ζητημάτων ασφαλείας, δίνουν οι Sharma K & Ghose M.K. (2011) [81], η οποία καλύπτει τις απαιτήσεις των δικτύων με υψηλές απαιτήσεις ασφαλείας (Hard Security Requirement Applications - HSRA). Η προσέγγιση αυτή, αφορά το πρωτόκολλο CLIFFs (Cross Layer Integrated Framework for security for WSN) και βασίζεται στη ταυτόχρονη και ομαλή λειτουργία όλων των επιπέδων. Το πρωτόκολλο αυτό, με τη χρήση του συμμετρικού αλγορίθμου RC5 για εφαρμογές HSRA διαθέτει μήκος κλειδιού 80 ψηφίων (RC5/80/4). Τέλος, με χρήση της οντότητας ISA (Intelligent Security Agent), η οποία προσφέρει ευρηματικότητα στις διαδικασίες ανίχνευσης και αντιμετώπισης κακόβουλων ενεργειών, το πρωτόκολλο CLIFFs επιδρά ενεργειακά αποδοτικότερα στις λειτουργίες του δικτύου.

5.4 Ασφάλεια τεχνολογίας ZigBee και προτύπου Bluetooth

Για τη παροχή ευελιξίας στο επίπεδο ασφάλειας που εφαρμόζεται, χρησιμοποιείται το πρωτόκολλο IEEE 802.15.4. Οι αλγόριθμος συμμετρικής κρυπτογράφησης που χρησιμοποιεί το πρωτόκολλο είναι ο AES-128bits και οι MICs (Message Integrity Code) για να διασφαλίσει την εμπιστευτικότητα και τον έλεγχο ταυτότητας των δεδομένων σε κάθε ζεύξη [82]. Ωστόσο, δεν προσδιορίζει μηχανισμούς για τη διανομή κρυπτογραφικού κλειδιού και τον έλεγχο ταυτότητας αντικειμένων.

Το πρωτόκολλο ZigBee, συμπληρωματικό του IEEE 802.15.4 (Κεφάλαιο 3), προσθέτει μηχανισμούς πιστοποίησης ταυτότητας και διαχείρισης κλειδιών κρυπτογράφησης. Οι μηχανισμοί αυτοί βασίζονται στο σχήμα SKKE (Symmetric – Key Key Exchange) [82] στον ορισμό τριών κλειδιών (pairwise keys), (network keys) και (master keys) καθώς και ενός κέντρου αξιοπιστίας (Trust Center - TC). Η συσκευή TC είναι μια εύρωστη έναντι κακόβουλων ενεργειών και αξιόπιστη οντότητα η οποία υλοποιείται στο σταθμό βάσης. Επιπρόσθετα, αυτό το πρωτόκολλο προσφέρει ακεραιότητα, αυθεντικοποίηση και εμπιστευτικότητα δεδομένων, χρησιμοποιώντας τη λειτουργία CCM (Counter with CBC-MAC) του πρωτοκόλλου [82] και τον κρυπτογραφικό αλγόριθμο AES-128bits.

Η διαχείριση ασφάλειας του πρωτοκόλλου Bluetooth διαθέτει διαφορετικά στάδια κατά τα οποία χρησιμοποιεί διάφορους αλγόριθμους κλειδιών κρυπτογράφησης για την ορθή λειτουργία του. Οι πιο συνηθισμένοι αλγόριθμοι κλειδιών κρυπτογράφησης που χρησιμοποιούνται από την πιο πρόσφατη έκδοση του Bluetooth (4.0 και άνω) είναι η κρυπτογράφηση ελλειπτικής καμπύλης (ECC) και ο συμμετρικός αλγόριθμος AES 128bits.

Τέλος, για την παροχή επικοινωνίας με έλεγχο ταυτότητας, εμπιστευτικότητα και ακεραιότητα δεδομένων, το πρωτόκολλο αυτό, παρέχει κρυπτογραφικούς μηχανισμούς διαχείριση κλειδιών. Η διασφάλιση των αναγκών που προαναφέρθηκαν γίνεται εφικτή σύμφωνα με το συνδυασμό τριών τύπων κρυπτογραφικών κλειδιών (initialization keys, combination keys και master keys) [82].

Συμπεράσματα

Στην εργασία αυτή, πραγματοποιήθηκε εκτενής μελέτη ζητημάτων ασφάλειας που σχετίζονται με ασύρματα δίκτυα αισθητήρων (WSNs) αλλά και με συσκευές IoT. Τα WSN εκτίθενται σε πολυάριθμες απειλές ασφαλείας που μπορούν να θέσουν σε κίνδυνο την επιτυχία των εφαρμογών. Η υποστήριξη ασφαλείας στα WSN αποτελεί μια σύνθετη διαδικασία με πολλές προκλήσεις, λόγω των απαιτήσεων για μειωμένη κατανάλωση ενέργειας, για βέλτιστη διαχείριση του διαθέσιμου εύρους ζώνης επικοινωνίας και της περιορισμένης υπολογιστικής ισχύος. Επίσης, οι αισθητήρες συχνά αναπτύσσονται σε ανοιχτό περιβάλλον όπου δεν υπάρχει διαθέσιμη φυσική ασφάλεια. Δεδομένης της ποικιλομορφίας των εφαρμογών WSN και πιθανώς των διαφορετικών απαιτήσεων ασφαλείας, μπορεί να θεωρηθεί πως είναι απαραίτητες ειδικές ενισχυτικές προσεγγίσεις για την ασφάλεια των δικτύων WSN.

Το Διαδίκτυο των Πραγμάτων οδεύει σε έναν κόσμο απεριόριστων δυνατοτήτων για εφαρμογές σε διάφορους τομείς της κοινωνίας μας, αλλά έχει επίσης πολλές προκλήσεις. Μία από αυτές τις προκλήσεις είναι η ασφάλεια και η ιδιωτικότητα. Οι συσκευές IoT είναι πιο επιρρεπείς σε απειλές και επιθέσεις ασφαλείας, λόγω των περιορισμών τους. Έγινε παρουσίαση της τρέχουσας κατάστασης ασφάλειας στο IoT και των λύσεων που πρέπει να τεθούν σε εφαρμογή για να πειστούν οι χρήστες πως το IoT δεν αφορά μόνο την παροχή συσκευών χαμηλού κόστους. αλλά εξίσου σημαντική είναι η παροχή των βέλτιστων λύσεων ασφάλειας που αντιμετωπίζουν τις απειλές για την ασφάλεια και τις ανησυχίες όσον αφορά το απόρρητο των χρηστών.

Η εργασία αυτή προσεγγίζει κατά βάση το θεωρητικό υπόβαθρο των προκλήσεων και ζητημάτων ασφάλειας ασύρματων δικτύων αισθητήρων WSNs και των υλοποιήσεων τους στο Διαδίκτυο των πραγμάτων IoT. Μελλοντική επέκταση της εργασίας σε πειραματικό επίπεδο μπορεί να πραγματοποιηθεί με τη χρήση κατάλληλων προγραμμάτων προσομοίωσης ασύρματων δικτύων όπως: NS2, NS3, OMNET++, OPNET.

Καθώς τα ασύρματα δίκτυα αισθητήρων και το Διαδίκτυο των Πραγμάτων συνεχίζουν να αναπτύσσονται, αναμένεται η απαίτηση περαιτέρω προσδοκιών ασφάλειας από τις ήδη υπάρχουσες. Με την ελπίδα πως οι ενδελεχής έρευνες πιθανότατα θα καταστήσουν την ισχυρή ασφάλεια πιο ρεαλιστική προσδοκία στο μέλλον.

Βιβλιογραφία

[1] D. Rainham, "A wireless sensor network for urban environmental health monitoring: UrbanSense," in *IOP Conference Series Earth and Environmental Science 34(1):012028*, Canada, April 2016.

[2] S. LABS, "Silicon Laboratories, Inc," [Online]. Available: https://www.silabs.com/documents/public/white-papers/evolution-of-wireless-sensor-networks.pdf. [Accessed 18 March 2022].

[3] W. J., Sensor Technology, MA Burlington USA: Handbook Elsevier Newnes, 2005.

[4] A. S. Tanenbaum, "Δίκτυα Υπολογιστων," Εκδόσεις Κλειδάριθμος, pp. σελ. 827 - 952.

[5] J. Jeong and Cheng-Tien, "Forward Error Correction in Sensor Networks," in *EECS Department, University of California*, Berkeley, California, USA.

[6] "Sensor Network Architecture," GeeksforGeeks, 30 January 2020. [Online]. Available: https://www.geeksforgeeks.org/sensor-network-architecture/.

[7] G. Ferrari, "Device-to-device communications in wireless sensor networks," *International Journal of Distributed Sensor Networks,* August 2016.

[8] B. H, "The industrial internet of things (IIoT): an analysis framework.," pp. 1 - 12, 2018.

[9] S. A, "A sensor cloud test-bed for multi-model and multi-user sensor applications.," *IEEE wireless communications and networking conference,* pp. 1-7, 2016.

[10] A. DS, "Integrating cloud-WSN to analyze weather data and notify SAAS user alerts during weather disasters.," *IEEE international advance computing conference,* pp. 899-904, 2015.

[11] I. Zain, "Internet of Things," vol. 4, no. 3, pp. 3-5, 2016.

[12] T. Tesca, "What is Wireless Sensor Network and Types of WSN?," 2021.

[13] M. Akyilidiz, "Wireless sensor networks," *A survey Computer Networks,* 2002.

[14] B. A., "Sensor Networks: An Overview," Davis, Department of Computer Science, University of California, 2001.

[15] Y. J, "Wireless sensor network," *Computer Networks,* no. 12, p. 52, 2008.

[16] B. A., Algorithms and Protocols for Wireless, Mobile Ad Hoc Networks, John Wiley & Sons. Inc, 2009.

[17] Sohraby, K.; Minoli, D.; Znati, T., "Wireless sensor networks: technology, protocols, and applications," John Wiley and Sons, 2010, pp. 203-209.

[18] B. Chiara, C. Andrea, D. Davide, V. Roberto, D. Davide and V. Roberto, "An Overview on Wireless Sensor Networks Technology and Evolution," *Sensors,* 2009.

[19] R. Verdone, D. Dardari, G. Mazzini and A. Conti, Wireless Sensor and Actuator Networks, London, UK: Elsevier, 2008.

[20] S. Huh, S. Cho and S. Kim, "Managing IoT devices using blockchain platform.," in *Proceedings of the 19th International Conference on Advanced Communication (pp. 464-467).*, IEEE, 2017.

[21] W. Zhang, "The 10 Research Topics on the Internet of Things," in *Proceedings of the 2020 IEEE 6th International Conference on Collaboration and Internet Computing (CIC)*, 2020.

[22] I. Lee and K. Lee, in *The Internet of Things (IoT): Applications, investments, and challenges for enterprises.*, Business Horizons, 2015, pp. 431-440.

[23] M. Mohammadi, A. Al-Fuqaha, S. Sorour and M. Guizani, "Deep Learning for IoT Big Data and Streaming Analytics: A Survey," *IEEE Communication Surveys & Tutorials,* vol. 20, no. 4, pp. 2923-2960, 2018.

[24] L. S. Vailshery, "https://www.statista.com/," Statista, 06 September 2022. [Online]. Available: https://www.statista.com/statistics/1101442/iot-number-of-connected-devices-worldwide/. [Accessed 01 January 2023].

[25] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo and D. P. Agrawal, Choices for interaction with things on Internet andunderlying issues, ELSEVIER, 2015.

[26] N. Huansheng, "Unit and Ubiquitous Internet Of Things," CRC Press, 2013.

[27] A. R. Mohammed, T. Djamel and R. Imed, Architecting the Internet of Things, State of the Art, 2015.

[28] A. Botta, W. d. Donato, V. Persico and A. Pescape, "Integration of cloud computing and Internet of Things: A survey," *Future Generation Computer Systems,* 2015.

[29] L. Atzori, A. Iera and G. Morabito, The Internet of Things: A survey, ELSEVIER, 2010.

[30] K. Mekki, E. Bajic, F. Chaxel and F. Meyer, "A comparative study of LPWAN technologies for large-scale IoT deployment," *ICT Express,* vol. 5, no. 1, pp. 1-7, 2019.

[31] A. G. Sauve, B. D. Kelper and J. Voix, "Man Down Situation Detection Using an in-Ear Inertial Platform," *Sensors 2021,* no. 21(5), 3 March 2021.

[32] A. Dunkels, "Adam Dunkels," 25 November 2001. [Online]. Available: http://dunkels.com/adam/software.html. [Accessed 4 February 2023].

[33] A. Dunkels, Programming Memory-Constrained Networked Embedded Systems, PhD dissertation, Institutionen för datavetenskap och elektronik, 2007.

[34] S. Alam, M. M. R. Chowdhury and J. Noll, "Interoperability of Security-Enabled Internet of Things," *Wireless Personal Communications,* vol. 61, pp. 567-586, 2011.

[35] S. Sicari, A. Rizzardi, L. Grieco and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahaed," in *Computer Networks*, Italy, ELSEVIER, 2015, pp. 146-164.

[36] R. Roman, J. Zhou and J. Lopez, On the features and challenges of security and privacy in distributed internet of things, ELSEVIER, 2013.

[37] Q. Jing, A. Vasilakos, J. Wan and J. Lu, Security of the Internet of Things: Perspectives and challenges, New York: Springer Science+Business Media, 2014.

[38] SWEENEY and LATANYA, "A MODEL FOR PROTECTING PRIVACY," *USA : International Journal on Uncertainty, Fuzziness and Knowledge-based Systems,* 2002.

[39] guduruaishwarya, "Introduction of IEEE 802.15.4 technology," Geeks for geeks, 3 August 2022. [Online]. Available: https://www.geeksforgeeks.org/introduction-of-ieee-802-15-4-technology/. [Accessed 19 October 2022].

[40] K. Finkenzeller, "Animal Identification," in *RFID Handbook: Second Edition*, 203, p. 364.

[41] Considerations for High-Performance Toll Systems, Dallas: TransCore Marketing Communications, 2002.

[42] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler and J. Anderson, in *Workshop on Wireless Sensor Networks and Applications*, Atlanta, ACM New York, 2002, p. 88.

[43] W. Zhongmin, S. Zhen, C. Peng-Yu, A. Anisha, M. Kevin and C. YangQuan, MASmote -- A Mobility Node for MASnet (Mobile Actuator Sensor Networks), Logan: Utah State University, 2004.

[44] R. Sanda, M. Gordana, C. Mirjana and L. Tadija, "RFID and Supply Chain Management for Manufacturing Digital Enterprise," in *Supply Chain Management - New Perspectives*, Croatia, University of Zagreb, 2011.

[45] F. Alshahrany, Zedan and I. Moualek, A Conceptual Framework for Small WSN Configuration using Intelligent Decision Support Systems, London: INTECH, 2013.

[46] F. Alshahranya, M. Abboda and I. Moualek, "WSN and RFID Integration to Support Intelligent Monitoring in Smart Buildings Using Hybrid Intelligent Decision Support Systems," *Special issue of the International Conference on Computational and Experimental Science and Engineering,* vol. 128, pp. 3-5, 2015.

[47] N. Forum, "The keys to truly interoperable commmunications," NFC Forum Marketing White Paper, 2007.

[48] Opperman and G. P. C. A., "A generic nfc-enabled mearurement system for remote monitoring and control of client-side equipment," *2011 Third International Workshop on Near Field Communication,* 2011.

[49] "NFC Forum homepage," [Online]. Available: www.nfc-forum.org. [Accessed 22 October 2022].

[50] A. Belic, "About Us: Baggizmo," Baggizmo, [Online]. Available: https://getbaggizmo.com/top-10-uses-for-nfc-tags/. [Accessed 22 October 2022].

[51] E. International, Near field communication interface and protocol (nfcip- 1), E. International.

[52] NXP, Pn532 application note, NXP, December 2006.

[53] Sony Corporation, Sony Corporation, [Online]. Available: https://www.sony.net/Products/felica/business/tech-support/. [Accessed 23 October 2022].

[54] Α. Σπένδας, Ασύρματα Δίκτυα Αισθητήρων και Ζητήματα Ασφαλείας, Πανεπιστήμιο Μακεδονίας: Τμήμα Εφαρμοσμένης Πληροφορικής.

[55] O. MS and L. J-S, "Security in wireless sensor networks.," in *Security and Communication Networks.*, 2016, pp. 101-103.

[56] W. Stallings, Βασικές Αρχές Ασφαλείας Δικτύων, Εφαρμογές και Πρότυπα, Εκδόσεις Κλειδάριθμος, Δεκέμβριος 2008.

[57] Hubboub and H. Bader, Denial of Service Attack in Wireless Sensor Networks, Gaza - Islamic University: Computer Engineering Department, Faculty of Engineering, Deanery of Higher Studies.

[58] W. Anthony D and J. A. Stankovic, "Denial of Service in Sensor Networks," USA, University of Virginia, pp. 54 - 62.

[59] J. Deng, H. Richard and S. Mishra, Countermeasures Against Traffic Analysis Attacks in Wireless Sensor Networks, Boulder, Colorado, USA: Computer Science Department, University of Colorado at Boulder.

[60] W. Yong, A. Garhan and R. Byrav, A Survey of Security Issues In Wireless Sensor Networks, Lincoln: University of Nebraska.

[61] J. Sen, in *A Survey on Wireless Sensor Network Security*, Kolkata, India, Tata Consultancy Services Limited, Wireless & Multimedia Innovation Lab, Bengal Intelligent Park, Salt Lake Electronics Complex, pp. 55-78.

[62] S. Zhu, S. Setia, S. Jajodia and P. Ning, "An interleaved hop by hop authentication scheme for filtering of injected false data in sensor networks," in *In Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, May 2004.

[63] O. Camp and P. Albers, "Security in ad hoc networks: A general intrusion detection architecture enhancing trust-based approaches," in *In Proceedings of the 1st International Workshop on Wireless Information Systems*, 4th International Conference on Enterprise Information Systems, 2002.

[64] F. Ye, H. Luo, S. Lu and L. Zhang, "Statistical En-Route Filtering of Injected False Datasensor Networks," in *Proc. IEEE INFOCOM*, Hong Kong, 2004.

[65] P. Brutch and C. Ko, "Challenges in intrusion detection for wireless ad-hoc networks," in *In Proceedings of the Symposium on Applications and the Internet Workshops (SAINT'03*

Workshops), 2003.

[66] G. Wang, W. Zhang, C. Cao and T. Porta, "On supporting distributed collaboration in sensor networks," in *In Proceedings of MILCOM*, 2003.

[67] A. Perrig, J. Stankovic and D. Wagner, "Security in Wireless Sensor Networks," *Communications of the ACM,* vol. 47, no. 6, pp. 53-57, June 2004.

[68] A. Wood and J. Stankovic, "Denial of Service in Sensor Networks" in Computer," vol. 35, no. 10, pp. 54-62, 2002.

[69] A. Papadimitriou, F. L. Fessant, A. C. Viana and C. Sengul, Cryptographic Protocols to Fight Sinkhole Attacks on Tree-based Routing in Wireless Sensor Networks.

[70] M. J. Baek, K.-I. Kim and S. Cho, "A Revised Mint-Route Protocol in Wireless Sensor Networks," Jinju, Korea, Department of Informatics Gyeongsang National University, pp. 258-259.

[71] I. Hegazy, R. Safavi-Naini and C. Williamson, Towards Securing MintRoute in Wireless Sensor Networks, Calgary, AB, Canada: Department of Computer Science, University of Calgary.

[72] I. Krontiris, T. Dimitriou, T. Giannetsos and M. Mpasoukos, "Intrusion Detection of Sinkhole Attacks in Wireless Sensor Networks," Athens Information Technology, pp. 150-161.

[73] Douceur and J. R., "The Sybil Attack," Microsoft Research.

[74] B. N. Levine, C. Shields and N. B. Margolin, "A Survey of Solutions to the Sybil Attack".

[75] R. E. Kaissi, Z. Dawy and A. Kayssi, "DAWWSEN: A Defense Mechanism against Wormhole attack in Wireless Sensor Network," in *Proceedings of the Second International Conference on Innovations in Information Technology, Department of Electrical and Computer Engineering*, American University of Beirut, Beirut, Lebanon, 2005.

[76] J. P. Walters, W. Shi, Z. Liang and V. Chaudhary, "Wireless Sensor Network Security: A Survey," in *Security in Distributed, Grid, Mobile, and Pervasive Computing*, April 2007, pp. 367-409.

[77] A. Papadimitriou, F. Le Fessant, A. Carneiro Viana and C. Sengul, Cryptographic Protocols to Fight Sinkhole Attacks on Tree-based Routing in Wireless Sensor Network.

[78] Y.-C. Hu, A. Perrig and D. B. Johnson, Packet Leashes: A Defense against Wormhole Attacks in Wireless Networks, Carnegie Mellon University.

[79] Ν. Αλεξανδρής, Β. Χρυσικόπουλος and Κ. Πατσάκης, Εισαγωγή στη θεωρία πληροφοριών, κωδίκων και κρυπτογραφίας, Εκδόσεις Βαρβαρίγου.

[80] Β. Κάτος and Γ. Στεφανίδης, Τεχνικές κρυπτογραφίας και κρυπτανάλυσης, Εκδόσεις Ζυγός.

[81] K. Sharma and M. Ghose, "Cross Layer Security Framework for Wireless Sensor Networks," *International Journal of Security and Its Applications,* vol. 5, no. No. 1, January, 2011.

[82] M. Kuorilehto, M. Kohvakka, J. Suhonen, P. Haemaelaeinen, M. Haemaelaeinen and T. D. Haemaelaeinen, in *Ultra – Low Energy Wireless Sensor Networks in Practice, Theory, Realization and Deployment*, Finland, Tampere University of Technology, pp. 125-142.

[83] Elprocus, "Wireless Sensor Network Architecture and Its Applications," [Online]. Available: https://www.elprocus.com/architecture-of-wireless-sensor-network-and-applications/.

[84] K. Herbert, "Networking and communications," TechTarget, [Online]. Available: https://www.techtarget.com/whatis/glossary/Networking-and-Communications.

[85] A. Cole, "Wireless Networking," *Network Virtualization: The Future of the OSI Model,* June 12, 2020.

[86] K. Sohraby, D. Minoli and T. Znati, Wireless Sensor Networks: Technology, Protocols and Applications, Hoboken, NJ, USA: John Wiley & Sons, Inc., 2007.

[87] G. Kapatos and V. Paramythellis, 10 12 2021. [Online]. Available: https://polynoe.lib.uniwa.gr/xmlui/handle/11400/1630. [Accessed 4 February 2023].

[88] Ν. Δ. Χαρίτος, "https://pergamos.lib.uoa.gr," Νοέμβριος 2016. [Online]. Available: https://pergamos.lib.uoa.gr/uoa/dl/frontend/file/lib/default/data/1324973/theFile. [Accessed 3 Φεβρουάριος 2023].

[89] Α. Βούρος, "https://dspace.lib.ntua.gr," Μάρτιος 2015. [Online]. Available: shorturl.at/hsWY6. [Accessed 3 Φεβρουάριος 2023].

[90] Δ. Κυριακάκης, "Ιδρυματικό Αποθετήριο Πολυνόη," 17 Μάρτιος 2021. [Online]. Available: https://polynoe.lib.uniwa.gr/xmlui/handle/11400/513. [Accessed 3 Φεβρουάριος 2023].

[91] W. Dargie and C. Poellabauer, "Fundamentals of wireless sensor networks: theory and practice," John Wiley and Sons, 2010, pp. 168-183, 191-192.

[92] E. Ngai, L. J and L. M, "On the intruder detection for sinkhole attack in wireless sensor networks," in *In Proceedings of the 2006 IEEE International Conference on Communications*, Istanbul, Turkey, 2006.

[93] Wehrle and P. D. Klaus, "Wireless Sensor Networks Lab," COMSYS, [Online]. Available: https://www.comsys.rwth-aachen.de/teaching/ss-13/wireless-sensor-networks-lab.

[94] Rashmi, S. Begum and P. B. Kishore, "A Review Paper based on Various Mac Protocols for Wireless Sensor Networks," 13 June 2019.

[95] Ergen and S. Coleri, "http://pages.cs.wisc.edu," 10 September 2004. [Online]. Available: https://scholar.google.gr/scholar_url?url=http://pages.cs.wisc.edu/~suman/courses/707/papers/zigbee.pdf&hl=el&sa=X&ei=YZ9OY8GEA9qTy9YPuZmDwAY&scisig=AAGBfm3ZR3bqRJ1XxClhNSlvbXWR0_Qx2Q&oi=scholarr. [Accessed 19 October 2022].