ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

Διπλωματική Εργασία

Ανάπτυξη συστήματος ανίχνευσης ανωμαλιών στο IEC 60870-5-104 με τη χρήση τεχνικών μηχανικής μάθησης

Ονοματεπώνυμο: Κωνσταντίνος Ρόμπολος

ΑΜ: 1063

Επιβλέπων καθηγητής: Επίκουρος Καθηγητής, Παναγιώτης Σαρηγιαννίδης

Κοζάνη 2020

Περίληψη

Η ασφάλεια από κυβερνοεπιθέσεις αποτελεί ερευνητική περιοχή αυξημένου ενδιαφέροντος. Ιδιαίτερα η ανάγκη προστασίας κρίσιμων υποδομών, όπως: συστήματα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων (SCADA), Συστήματα Βιομηχανικού Ελέγχου (ICS), από κακόβουλες επιθέσεις αποτελεί επιτακτική ανάγκη. Η αύξηση της πολυπλοκότητας και της διασυνδεσιμότητας στα συστήματα κρίσιμων υποδομών τα καθιστά ευάλωτα σε εξωτερικές κυβερνοεπιθέσεις. Τα βιομηχανικά πρωτόκολλα επικοινωνίας, που χρησιμοποιούνται στις εγκαταστάσεις αυτές, συχνά εκθέτουν την υποδομή σε κινδύνους.

Η παρούσα διπλωματική εργασία αποσκοπεί στη δημιουργία συστήματος ανίχνευσης ανωμαλιών σε δεδομένα δικτυακών καταγραφών του βιομηχανικού πρωτοκόλλου IEC 60870-5-104 με χρήση τεχνικών μηχανικής μάθησης. Τα δεδομένα, με τα οποία έγινε η αξιολόγηση του συστήματος αυτού, παράχθηκαν στα πλαίσια της διπλωματικής εργασίας με την προσομοίωση ενός συστήματος SCADA και την εκτέλεση επιθέσεων εναντίον του.

Σε πρώτο επίπεδο γίνεται μελέτη του βιομηχανικού πρωτοκόλλου επικοινωνίας IEC 60870-5-104 αναφορικά με τη δομή των μηνυμάτων και των κινδύνων που εισάγει η χρήση του σε κρίσιμες υποδομές.

Στη συνέχεια, παρατίθενται λεπτομέρειες σχετικά με την τοπολογία του συστήματος SCADA, το οποίο προσομοιώνεται. Πρωτόκολλο επικοινωνίας του σύστηματος είναι το πρωτόκολλο IEC 60870-5-104. Ακολούθως παρουσιάζονται λεπτομερώς οι τεχνικές που χρησιμοποιήθηκαν με στόχο την διατάραξη της ομαλής λειτουργίας του.

Στο επόμενο στάδιο της διπλωματικής εργασίας αναλύεται η καταγεγραμμένη δικτυακή κίνηση στο εικονικό σύστημα SCADA με χρήση προγράμματος ανάλυσης δικτυακών καταγραφών και εξαγωγής στοιχείων σε επίπεδο δικτυακών ροών, που αναπτύχθηκε στα πλαίσια της εργασίας.

Τέλος γίνεται ανίχνευση και κατηγοριοποίηση διαφορετικών τύπων ανωμαλιών στα στοιχεία δικτυακών ροών με τη χρήση τεχνικών μηχανικής μάθησης, τα είδη των οποίων παρουσιάζονται εκτενώς, καθώς και τα αποτελέσματα που προκύπτουν από την ανίχνευση ανωμαλιών. Επιπροσθέτως, γίνεται σύγκριση των αποτελεσμάτων της ανίχνευσης ανωμαλιών με χρήση των δεδομένων, που υπέστησαν επεξεργασία με το προαναφερθέν πρόγραμμα ανάλυσης δεδομένων δικτυακών καταγραφών, με τα αντίστοιχα αποτελέσματα της ανίχνευσης ανωμαλιών, που προέκυψαν με τη χρήση των δεδομένων, που εξήχθησαν μετά από επεξεργασία του λογισμικού ανάλυσης δικτυακής κίνησης CICFlowMeter.

Λέξεις κλειδιά: Συστήματα Ανίχνευσης Εισβολών, δικτυακές ροές, κατηγοριοποίηση, ανίχνευση ανωμαλιών, βιομηχανικά πρωτόκολλα επικοινωνίας, IEC 60870-5-104, Μηχανική μάθηση, Συστήματα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων.

Abstract

Cybersecurity is a research area of paramount importance, specifically regarding Critical Infrastructures, such as Supervisory Control and Data Acquisition (SCADA) systems or Industrial Control Systems (ICS), where the need for security from malicious cyber-attacks is critical. The increase in complexity and interconnectivity of Critical Infrastructures deems them vulnerable to cyber-attacks. The industrial communication protocols which are used in these infrastructures often expose them to such threats.

The goal of this thesis is the development of a system which detects anomalies in network data of the industrial communication protocol IEC 60870-5-104, utilizing machine learning techniques. The data used for the evaluation of the developed system were generated, in the scope of this thesis, with the simulation of a SCADA system and the execution of cyber-attacks against it.

At first, the industrial protocol IEC 60870-5-104 is studied regarding the structure of its messages and the risks of its utilization in Critical Infrastructures.

Next, details are provided regarding the simulated SCADA system, which utilizes the IEC 60870-5-104 industrial protocol, for the purposes of this thesis. Moreover, the techniques aiming to disrupt the normal operation of the system are described.

Consequently, the captured network traffic of the SCADA system is analyzed with a custom program, which exports network flow level parameters.

Finally, anomaly detection is attempted on the processed data, along with the classification of the different types of detected anomalies. The machine learning techniques which are used for the anomaly detection and the evaluation results are presented as well. There is also a comparison between the anomaly detection results from the collected data, processed with the aforementioned script, with the anomaly detection results from the collected data, processed with the CICFlowMeter network traffic analysis tool.

Keywords: Intrusion Detection Systems, network flows, Classification, anomaly detection, industrial communication protocols, IEC 60870-5-104, Machine Learning, Supervisory Control and Data Acquisition Systems.

Ευχαριστίες

Η παρούσα διπλωματική εργασία αποτελεί το τελευταίο κεφάλαιο της φοίτησης μου στο Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών της Πολυτεχνικής Σχολής του Πανεπιστημίου Δυτικής Μακεδονίας. Μετά από μία συναρπαστική διαδρομή κατά τη διάρκεια της οποίας βρέθηκα αντιμέτωπος με πληθώρα προκλήσεων, μέσα από τις οποίες απέκτησα γνώσεις, εμπειρίες, δεξιότητες και εφόδια, άλλαξε ο τρόπος σκέψης μου και η οπτική μου για τα πράγματα.

Θα ήθελα να ευχαριστήσω όλους τους καθηγητές μου, που συνέβαλαν στην ολοκλήρωση των σπουδών μου, αλλά ιδιαίτερα αισθάνομαι την ανάγκη να ευχαριστήσω θερμά τον επιβλέποντα καθηγητή της διπλωματικής μου εργασίας ,Επίκουρο Καθηγητή, Παναγιώτη Σαρηγιαννίδη για την εμπιστοσύνη που μου έδειξε, για τις ευκαιρίες και την καθοδήγηση που μου έδωσε για την ολοκλήρωση αυτής της εργασίας.

Επίσης, θα ήθελα να ευχαριστήσω τον διδακτορικό φοιτητή Παναγιώτη Ράδογλου Γραμματίκη για την υποστήριξη και βοήθεια που μου προσέφερε κατά τη διάρκεια της διπλωματικής αυτής εργασίας.

Στη συνέχεια, θα ήθελα να εκφράσω την ευγνωμοσύνη προς την οικογένειά μου για την συνεχή στήριξη, το ενδιαφέρον και την κατανόησή τους σε όλη τη διάρκεια των σπουδών μου.

Τέλος θα ήθελα, να ευχαριστήσω του φίλους και συμφοιτητές μου, με τους οποίους μοιράστηκα τα φοιτητικά μου χρόνια, για τις αξέχαστες εμπειρίες και στιγμές που μοιραστήκαμε.

Περιεχόμενα

Συντομογραφίες

Εποπτικός Έλεγχος και Απόκτηση Πληροφοριών (Supervisory Control And Data Acquisition - **SCADA**)

Σύστημα Βιομηχανικού Ελέγχου (Industrial Control System - **ICS**)

Master Terminal Unit - **MTU**

Master Station Unit - **MSU**

Substitute Master Station Unit - **Sub-MTU**

Σύστημα Ανίχνευσης Εισβολών (Intrusion Detection System - **IDS**)

Σύστημα Ανίχνεθσης και Αποτροπής Εισβολών (Intrusion Detection and Prevention System - **IDPS**)

Programmable Logical Controller - **PLC**

Remote Terminal Unit - **RTU**

Intelligent Electronic Device - **IED**

Διεπαφή Ανθρώπου-Μηχανής (Human Machine Interface - **HMI**)

Application Data Unit - **ADU**

Modbus Application Protocol - **MBAP**

Protocol Data Unit - **PDU**

Distributed Network Protocol 3 - **DNP3**

Application Protocol Data Unit - **APDU**

Application Protocol Control Information - **APCI**

Application Service Data Unit - **ASDU**

Αίτιο Μετάδοσης (Cause Of Transmission - **COT**)

Structure Qualifier - **SQ**

Information Object Address - **IOA**

Άνθρωπος στη Μέση (Man-In-The-Middle - **MITM**)

Time To Live - **TTL**

Άρνηση Εξυπηρέτησης (Denial-of-Service - **DoS**)

Κατανεμημένη Άρνηση Εξυπηρέτησης (Distributed Denial-of-Service - **DDoS**)

Πλατφόρμα Διαχείρισης Ασφάλειας (Security Management Platform - **SMP**)

Internet Traffic and Content Analysis - **ITACA**

Inter-Arrival Time - **IAT**

Κατανεμημενο Σύστημα Ανίχνευσης Εισβολών (Distributed Intrusion Detection System - **DIDS**)

Σύστημα Ανίχνευσης Δικτυακών Εισβολών (Network Intrusion Detection System - **NIDS**)

Host-based Intrusion Detection System - **HIDS**

Μηχανές Δεδομένων Υποστήριξης (Support Vector Machine - **SVM**)

Πρωτόκολλο Ελέγχου Μετάδοσης/Πρωτόκολλο Διαδικτύου (Transmission Control Protocol/Internet Protocol - **TCP/IP**)

Frame Relay – **FR**

Asynchronous Transfer Mode – **ATM**

Ψηφιακό Δίκτυο Ενοποιημένων Υπηρεσιών (Integrated Services Digital Network – **ISDN**)

Πεδίο Ελέγχου (Control Field - **CF**)

Κεντρική Μονάδα Επεξεργασίας (Command Processing Unit – **CPU**)

Multilayer Perceptron Classifier - **MLPC**

Πίνακας Σχημάτων και Πινάκων

1. Εισαγωγή

Η ασφάλεια από κυβερνοεπιθέσεις αποτελεί ερευνητική περιοχή αυξημένου ενδιαφέροντος. Ιδιαίτερα η ανάγκη προστασίας κρίσιμων υποδομών, όπως: Συστήματα SCADA ή ICS, από κακόβουλες επιθέσεις είναι πολλαπλάσια. Η αύξηση της πολυπλοκότητας και της διασυνδεσιμότητας στα συστήματα κρίσιμων υποδομών, τα καθιστά ευάλωτα σε εξωτερικές κυβερνοεπιθέσεις. Τα βιομηχανικά πρωτόκολλα επικοινωνίας που χρησιμοποιούνται στις εγκαταστάσεις αυτές, συχνά εκθέτουν τις υποδομές σε κινδύνους. Η εμφάνιση τέτοιων αδυναμιών αποτελεί πόλο έλξης για πολλούς επιτιθέμενους, οι οποίοι επιχειρούν την εκμετάλλευση των αδυναμιών αυτών για την πρόκληση διαταραχής της φυσιολογικής λειτουργίας των υποδομών αυτών. Τέτοια περιστατικά παρατηρείται ότι αυξάνονται τα τελευταία χρόνια καθιστώντας την εύρεση τρόπων προστασίας των υποδομών επιτακτική ανάγκη.

Η συνειδητοποίηση της σημασίας διασφάλισης της κανονικής λειτουργίας των συστημάτων SCADA ξεκίνησε με την αύξηση των περιστατικών κυβερνοεπιθέσεων οι οποίες είχαν συνέπειες οικονομικές, περιβαλλοντικές αλλά και στη δημόσια ασφάλεια. Ένα από αυτά τα περιστατικά αποτελεί η επίθεση σε ένα σύστημα επεξεργασίας λυμάτων στην Αυστραλία το 2000, κατά την οποία ένας επιτιθέμενος απέκτησε πρόσβαση σε συσκευές ελέγχου του SCADA συστήματος προβαίνοντας σε ενέργειες που έπληττων τη φυσιολογική λειτουργία του συστήματος. Σημαντικό ορόσημο αποτέλεσε η ανίχνευση του Stuxnet worm [1], το οποίο δημιουργήθηκε με το σκοπό να επιφέρει καταστροφές σε πυρηνικά εργοστάσια του Ιράκ. Από τα πιο πρόσφατα περιστατικά επιθέσεων εναντίων κρίσιμων υποδομών αποτελεί η επίθεση στο δίκτυο ηλεκτρικής ενέργειας της Ουκρανίας το 2015 με χρήση του BlackEnergy trojan, η οποία οδήγησε σε γενική διακοπή ρεύματος [2] [3].

1.1 Κίνητρο και Στόχοι Διπλωματικής Εργασίας

Η εύρεση αποτελεσματικών λύσεων για την οικουμενική προστασία των κρίσιμων υποδομών αποτελεί μέχρι σήμερα πρόκληση στον τομέα της ασφάλειας. Αρκετά μέτρα πρόληψης έχουν αναπτυχθεί για την ανίχνευση εισβολών, όπως είναι τα IDS, και για την αντιμετώπισή τους, όπως είναι τα IDPS και τα Honeypots**.** Τα παραπάνω εργαλεία χρησιμοποιούνται για την προστασία των κρίσιμων υποδομών από κινδύνους του δικτύου του συστήματος, τόσο εξωτερικούς όσο και εσωτερικούς. Τέτοια μέτρα, όμως, ενδέχεται να μη μπορούν να εφαρμοστούν σε οποιοδήποτε σύστημα SCADA, καθώς θα πρέπει να ληφθούν υπόψη τα ιδιαίτερα χαρακτηριστικά των διαφορετικών ειδών των συστημάτων αυτών. Άλλο

ένα εμπόδιο για την αποτελεσματική προστασία των υποδομών αυτών αποτελεί η χρήση πρωτοκόλλων επικοινωνίας, τα οποία δεν έχουν υλοποιημένους μηχανισμούς προστασίας από εισβολές, όπως μηχανισμούς αυθεντικοποίησης.

Βασικός στόχος αυτής της διπλωματικής εργασίας αποτελεί η ανίχνευση ανωμαλιών με χρήση τεχνικών Μηχανικής Μάθησης σε χαρακτηριστικά δεδομένων δικτυακών ροών του βιομηχανικού πρωτοκόλλου IEC 60870-5-104, τα οποία συγκεντρώθηκαν από επιθέσεις που εκτελέστηκαν εναντίον ενός συστήματος SCADA, το οποίο προσομοιώθηκε για το σκοπό αυτό.

1.2 Δομή Διπλωματικής Εργασίας

Η εν λόγω διπλωματική εργασία απαρτίζεται από έξι ενότητες οι οποίες παρουσιάζουν το θεωρητικό και πρακτικό υπόβαθρο που απαιτήθηκε για την ολοκλήρωσή της.

Στην τρέχουσα ενότητα γίνεται παρουσίαση του κινήτρου και των κύριων σκοπών αυτής της εργασίας παράλληλα με την δομή της.

Στη δεύτερη ενότητα ακολουθεί ανάλυση των συστημάτων SCADA σχετικά με την αρχιτεκτονική τους και τα βιομηχανικά πρωτόκολλα επικοινωνίας που χρησιμοποιούν. Στην ίδια ενότητα γίνεται αναφορά στη δομή των μηνυμάτων και στις αδυναμίες του βιομηχανικού πρωτοκόλλου επικοινωνίας IEC 60870-5-104, στο οποίο επικεντρώνεται το ενδιαφέρον της παρούσας διπλωματικής εργασίας.

Στην τρίτη ενότητα παρουσιάζονται συνοπτικά οι στόχοι, η αρχιτεκτονική και οι παραλλαγές των IDS τα οποία χρησιμοποιούνται σε συστήματα SCADA.

Στην τέταρτη ενότητα γίνεται παρουσίαση των διαφορετικών τύπων μηχανικής μάθησης, αλγορίθμων κατηγοριοποίησης αλλά και μετρικών αξιολόγησης μοντέλων μηχανικής μάθησης, τα οποία χρησιμοποιήθηκαν για τους σκοπούς αυτής της διπλωματικής εργασίας. Επιπλέον στο κεφάλαιο αυτό παρατίθενται τεχνητά σύνολα δεδομένων που χρησιμοποιούνται για την αξιολόγηση συστημάτων ανίχνευσης ανωμαλιών.

Στην πέμπτη ενότητα παρουσιάζεται αναλυτικά το σύστημα ανίχνευσης ανωμαλιών που αναπτύχθηκε και η διαδικασία αξιολόγησής του. Συγκεκριμένα παρουσιάζονται η δομή του προγράμματος εξαγωγής χαρακτηριστικών επιπέδου δικτυακών ροών, η δομή του συστήματος SCADA, το οποίο προσομοιώθηκε, η διαδικασία εκτέλεσης των επιθέσεων εναντίον του συστήματος και τέλος οι μέθοδοι ανίχνευσης των διαφορετικών τύπων επιθέσεων στα δεδομένα που συγκεντρώθηκαν, καθώς και τα αποτελέσματα.

Στην έκτη και τελευταία ενότητα, παρουσιάζονται τα συμπεράσματα των αποτελεσμάτων της διπλωματικής εργασίας και αναφέρονται πιθανές μελλοντικές επεκτάσεις της.

2. Συστήματα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων

Τα συστήματα SCADA χρησιμοποιούνται σε εγκαταστάσεις, οι οποίες είναι κεντρικοποιημένες ή μη κεντρικοποιημένες για τον έλεγχο, τη διαχείριση και την παρακολούθηση συστημάτων και συσκευών. Μερικά παραδείγματα τέτοιων υποδομών αποτελούν τα διυλιστήρια πετρελαίου, εργοστάσια παραγωγής ενέργειας, υποδομές ύδρευσης, γεννήτριες πυρηνικής ενέργειας, εγκαταστάσεις λυμάτων και αεροδρόμια.

2.1 Αρχιτεκτονική συστημάτων Εποπτικού Ελέγχου και Απόκτησης Δεδομένων

Ένα τυπικό σύστημα SCADA [4] [5] αποτελείται από PLC, αισθητήρες, RTU, IED, MTU. Οι διαχειριστές του συστήματος καλούνται να παρακολουθούν και να διασφαλίζουν την ομαλή διεξαγωγή των επιμέρους εργασιών των συσκευών του συστήματος. Οι διαχειριστές χρησιμοποιούν σταθμούς εργασίας ως HMI για αποστολή εντολών ελέγχου στις παραπάνω συσκευές, κάνοντας έτσι δυνατό τον έλεγχο του συστήματος, είτε με φυσική πρόσβαση σε αυτό, είτε απομακρυσμένα.

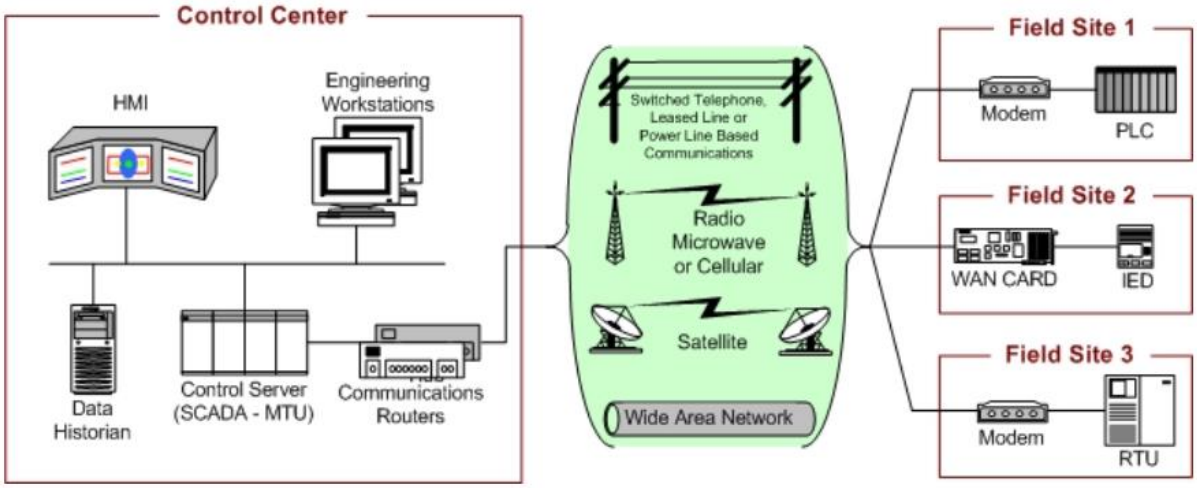
Το HMI απεικονίζει τις λαμβανόμενες πληροφορίες από το MTU για την κατάσταση του συστήματος και χρησιμοποιείται από τον διαχειριστή για την αποστολή εντολών στα αντίστοιχα MTU για αποφυγή διατάραξης της ομαλής λειτουργίας της υποδομής.

Το MTU, γνωστό και ως MSU, αποτελεί το κέντρο ελέγχου του συστήματος SCADA, καθώς είναι υπεύθυνο για τη συλλογή δεδομένων, αποστολή τους στο HMI, αλλά και για την αποστολή εντολών ελέγχου στους αισθητήρες. Αξίζει να σημειωθεί ότι υπάρχουν περιπτώσεις στις οποίες απαιτείται η χρήση και Sub-MTU που διαδραματίζει το ρόλο δευτερεύοντος κέντρου ελέγχου για το συστήμα SCADA.

Τα RTU χρησιμοποιούνται για τη μετάδοση εντολών ελέγχου στους αισθητήρες αλλά και για συγκέντρωση δεδομένων από τους αισθητήρες και μεταβίβασή τους στο MTU.

Παραδείγματα βιομηχανικών αισθητήρων συλλογής μετρήσεων και παρακολούθησης αποτελούν οι έξυπνες ηλεκτρικές συσκευές IED και τα PLC. Ένα IED χρησιμοποιείται σε βιομηχανίες παραγωγής ηλεκτρικής ενέργειας και είναι υπεύθυνο για τον έλεγχο-ρύθμιση ισχύος. Μερικά παραδείγματα IED αποτελούν οι μετασχηματιστές, οι ασφάλειες (circuit breaker) και συστοιχίες πυκνωτών. Τα PLC είναι συνδεδεμένα στους αισθητήρες και μετατρέπουν τα σήματα εξόδου των αισθητήρων σε ψηφιακά.

Το MTU μπορεί να διασυνδεθεί με RTU, PLC και IED με χρήση ποικίλων τρόπων, όπως Ethernet, WiFi ή χρήση οπτικών ίνων. Στην παρακάτω εικόνα παρουσιάζεται η δομή ενός συστήματος SCADA.



Εικόνα 1. Αρχιτεκτονική δικτύου SCADA [6]

Οι αρχιτεκτονικές των SCADA συστημάτων διακρίνονται σε [7] [8]:

- Μονολιθική αρχιτεκτονική, σύμφωνα με την οποία το MTU συνδέεται με όλα τα RTU. Τα συστήματα αυτά δεν επικοινωνούν με άλλα δίκτυα.
- Κατανεμημένη αρχιτεκτονική, σύμφωνα με την οποία η επεξεργασία των πληροφοριών και τον εντολών ελέγχου γίνεται σε πολλούς σταθμούς, οι οποίοι ήταν συνδεδεμένοι σε τοπικό δίκτυο. Η επικοινωνία MTU και RTU γίνεται με τη χρήση βιομηχανικών πρωτοκόλλων επικοινωνίας.
- Δικτυωμένη αρχιτεκτονική, σύμφωνα με την οποία οι σταθμοί είναι διασυνδεδεμένοι μέσω πολλών τοπικών δικτύων, αντίθετα με την κατανεμημένη αρχιτεκτονική.
- Web-Based αρχιτεκτονική, σύμφωνα με την οποία οι εξουσιοδοτημένοι χρήστες έχουν πρόσβαση με χρήση προγραμμάτων περιήγησης ιστού και κινητών συσκευών στις συσκευές ελέγχου του συστήματος.

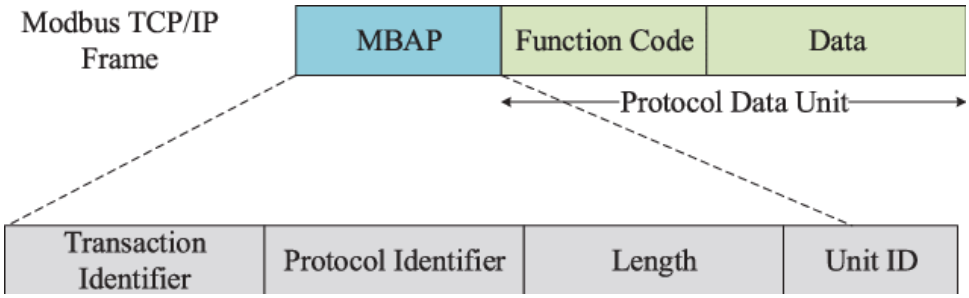
2.2 Επικοινωνίες σε συστήματα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων

Στη συντριπτική πλειοψηφία των σύγχρονων συστημάτων SCADA η ανταλλαγή δεδομένων και εντολών μεταξύ MTU και RTU, PLC, IED γίνεται κατά κύριο λόγο με χρήση ειδικών βιομηχανικών πρωτοκόλλων επικοινωνίας [9]. Μερικά από τα γνωστότερα και πιο ευρέως χρησιμοποιούμενα είναι το IEC 60870-5-104, το DNP3 και το Modbus. Τα πρωτόκολλα Modbus και DNP3 περιγράφονται σύντομα στις επόμενες ενότητες, ενώ το

πρωτόκολλο IEC 60870-5-104, του οποίου η μελέτη αποτελεί αντικείμενο της παρούσας ερευνητικής εργασίας, θα περιγραφεί αναλυτικά σε ακόλουθες ενότητες.

2.2.1 Βιομηχανικό πρωτόκολλο επικοινωνίας Modbus

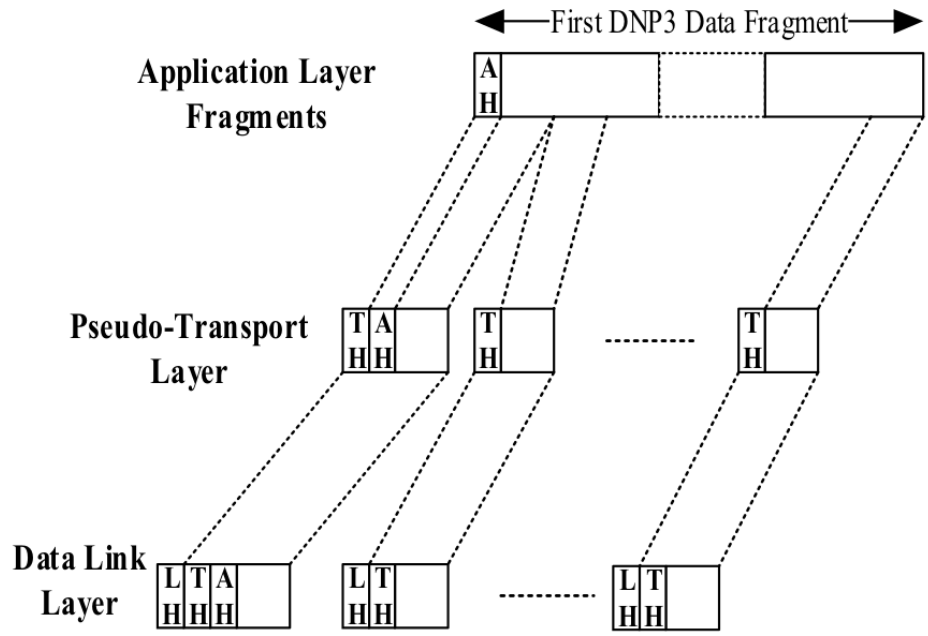
Το βιομηχανικό πρωτόκολλο επικοινωνίας Modbus [10] [11] [12] δημιουργήθηκε το 1979 και αποτελεί, ίσως, το πιο διαδεδομένο πρωτόκολλο επικοινωνίας, λόγω της δυνατότητας χρησιμοποίησής του σε ποικίλες συσκευές SCADA (RTU, PLC, HMI), καθώς υπάρχουν αρκετοί διαφορετικοί τύποι του πρωτοκόλλου MODBUS, όπως το Modbus TCP/IP και Modbus Serial. Στα πακέτα του πρωτοκόλλου Modbus TCP/IP, το ADU αποτελείται από την κεφαλίδα MBAP και το PDU. Τα πεδία που περιλαμβάνονται στο MBAP είναι: το Transaction Identifier, για προσδιορισμό ζευγών εναλλασσόμενων μηνυμάτων σε κάθε TCP ροή, το Protocol Identifier, το οποίο αρχικοποιείται στο 0, το Length, στο οποίο προσδιορίζεται το μέγεθος των υπόλοιπων πεδίων και το Unit ID, το οποίο χρησιμοποιείται για να προσδιορίσει τον υπολογιστή που είναι διασυνδεδεμένος στο δίκτυο. Η δομή των πακέτων Modbus παρουσιάζεται στην παρακάτω εικόνα:



Εικόνα 2. Δομή Modbus-TCP Frame [11]

2.2.2 Βιομηχανικό πρωτόκολλο επικοινωνίας DNP3

Το πρωτόκολλο DNP3 [13] [14] αναπτύχθηκε το 1993 βασιζόμενο σε μια πρώιμη έκδοση του αναπτυσσόμενου τότε πρωτοκόλλου IEC 60870-5-104. Το πρωτόκολλο αυτό χρησιμοποιείται στη βιομηχανία ηλεκτρισμού και σε βιομηχανίες παροχής νερού στη Βόρεια Αμερική. Σε σύγκριση με άλλα πρωτόκολλα, όπως το Modbus, το DNP3 έχει χαρακτηριστικά που του προσδίδουν καλύτερη απόδοση και διαλειτουργικότητα μεταξύ πολλαπλών SCADA συσκευών. Το αντίκτυπο, όμως, για αυτές τις επιπλέον παροχές αποτελεί η αύξηση στην πολυπλοκότητα. Τα πακέτα DNP3 απαρτίζονται από το επίπεδο χρήστη (user layer), το επίπεδο δεσμού (link layer), το επίπεδο μεταφοράς (transportation layer), το επίπεδο εφαρμογής (application layer) και το φυσικό επίπεδο (physical layer). Η δομή των DNP3 πακέτων εικονίζεται παρακάτω:



Εικόνα 3.Δομή DNP3 Frame [15]

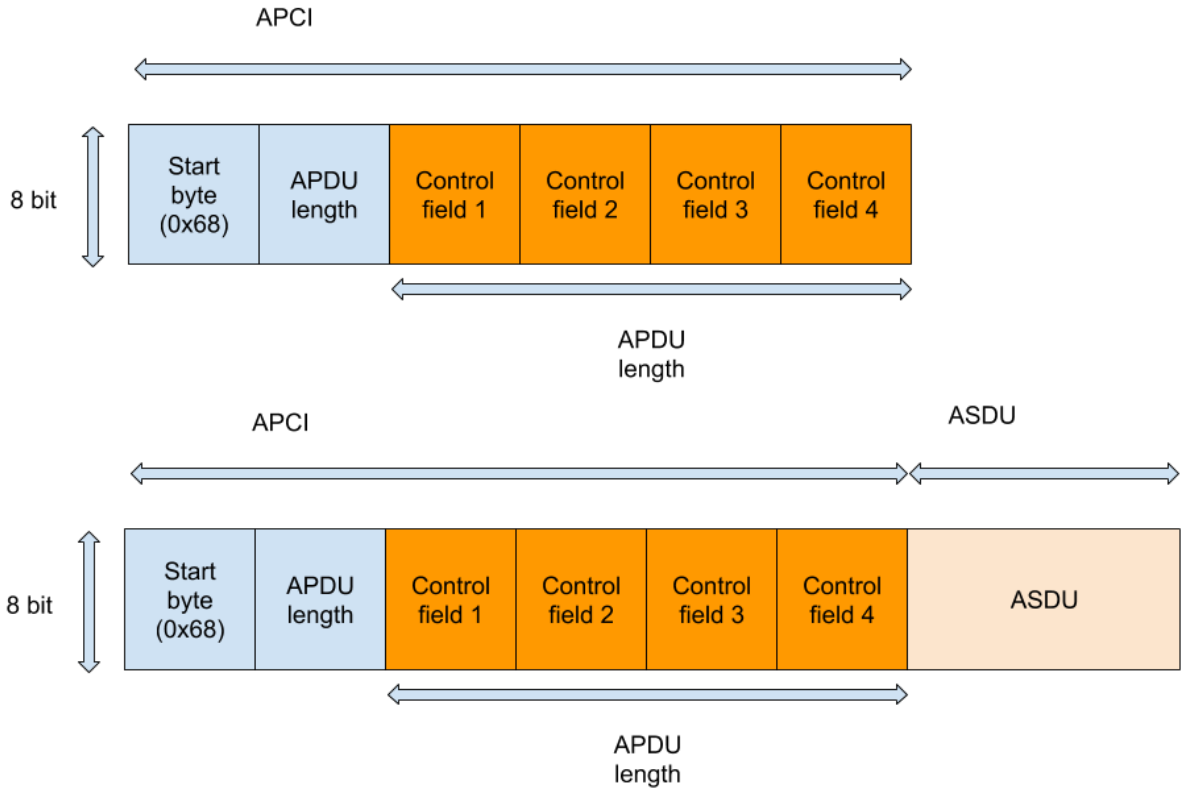
2.3 Βιομηχανικό πρωτόκολλο επικοινωνίας IEC 60870-5-104

Το βιομηχανικό πρωτόκολλο επικοινωνίας IEC 60870-5-104, γνωστό και ως IEC 104, ανήκει στην οικογένεια προτύπων IEC 60870 και δημιουργήθηκε για την απομακρυσμένη παρακολούθηση, έλεγχο και διαχείριση αυτοματισμού συστημάτων ισχύος και εγκαταστάσεων ηλεκτρισμού. Το IEC 60870-5-104 είναι υλοποιημένο, βασισμένο στη στοίβα του πρωτοκόλλου TCP/IP. Το IEC 60870-5-104 χρησιμοποιεί μια TCP/IP διεπαφή, ώστε να εξασφαλίσει πρόσβαση στο τοπικό δίκτυο, αλλά και σε άλλους τύπους δικτύων όπως X.25 και FR, ATM, ISDN, Ethernet και X.21.

Υπάρχουν τρεις τύποι έγκυρων IEC 60870-5-104 πλαισίων. Τα πλαίσια αυτά αποστέλλονται ως ένα APDU, το οποίο αποτελείται από ένα APCI και, ανάλογα με τον τύπο του πλαισίου, ίσως και ένα ASDU. Η δομή των APCI και ASDU αναλύεται στη συνέχεια.

2.3.1 IEC 60870-5-104 Application Protocol Control Information

Το APCI [16] [17] ξεκινά πάντα με ένα byte έναρξης με τιμή 0x68, το οποίο ακολουθείται από ένα πεδίο 8 bit, τα οποία παρουσιάζουν το μήκος του APDU και μετά από αυτό ακολουθούν 4 πεδία ελέγχου των 8 bit το καθένα. Με τον όρο μήκος του APDU εννοείται το συνολικό μήκος του APCI και του ASDU. Οι διαφορετικοί τύποι IEC 60870-5-104 APDU εικονίζονται παρακάτω.



Εικόνα 4. Διαφορετικοί τύποι APDU. APDU σταθερού μήκους (πάνω εικόνα) και APDU μεταβλητού μήκους (κάτω εικόνα)

Ο τύπος IEC 60870-5-104 πλαισίου καθορίζεται από τα 2 τελευταία bit του CF 1. Σε περίπτωση που το τελευταίο bit του CF 1 έχει τιμή 1, το πλαίσιο ανήκει στην κατηγορία των I-format (information transfer format) και έχει τα παρακάτω χαρακτηριστικά:

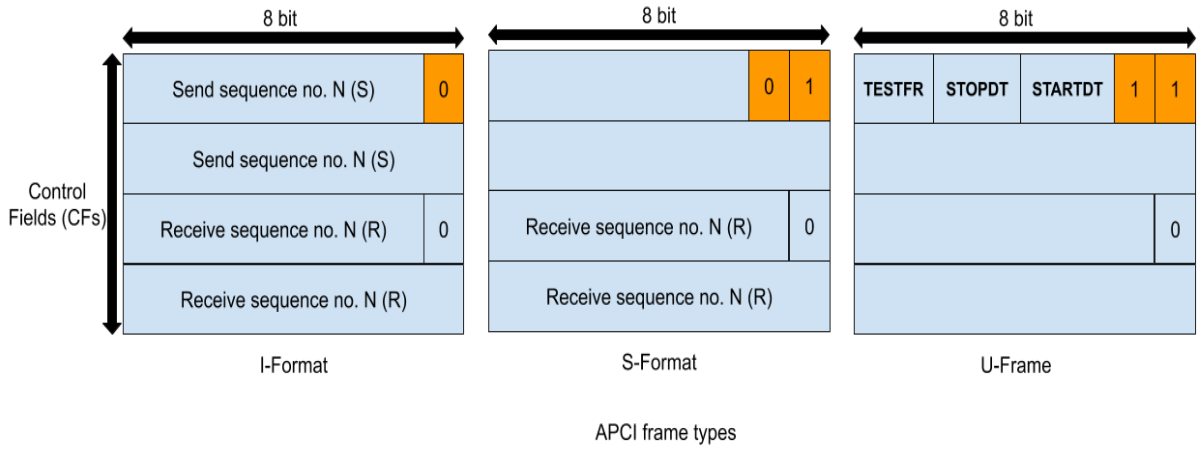
- Χρησιμοποιείται για την αριθμημένη μεταφορά πληροφοριών μεταξύ του σταθμού ελέγχου και των υπόλοιπων σταθμών. Το μήκος των πλαισίων αυτών δεν είναι σταθερό.
- Το APDU αυτών των πλαισίων περιλαμβάνει πάντα και ένα ASDU.

Σε περίπτωση που τα τελευταία bit του CF 1 είναι 01, το πλαίσιο ανήκει στην κατηγορία των πλαισίων S-format (numbered supervisory functions). Κάποια από τα χαρακτηριστικά αυτών των πλαισίων αναφέρονται παρακάτω:

- Τα πλαίσια αυτά χρησιμοποιούνται για την εκτέλεση εποπτικών συναρτήσεων και έχουν σταθερό μήκος.
- Το APDU αποτελείται αποκλειστικά από ένα APCI.
- Τα δεδομένα μεταφέρονται προς μία μόνο κατεύθυνση.

Ο τελευταίος τύπος πλαισίου είναι το U-format (unnumbered control functions). Τα πλαίσια αυτού του τύπου παρατηρούνται όταν τα τελευταία bit του CF 1 είναι 11. Μερικά από τα στοιχεία αυτού του τύπου πλαισίου παρατίθενται παρακάτω:

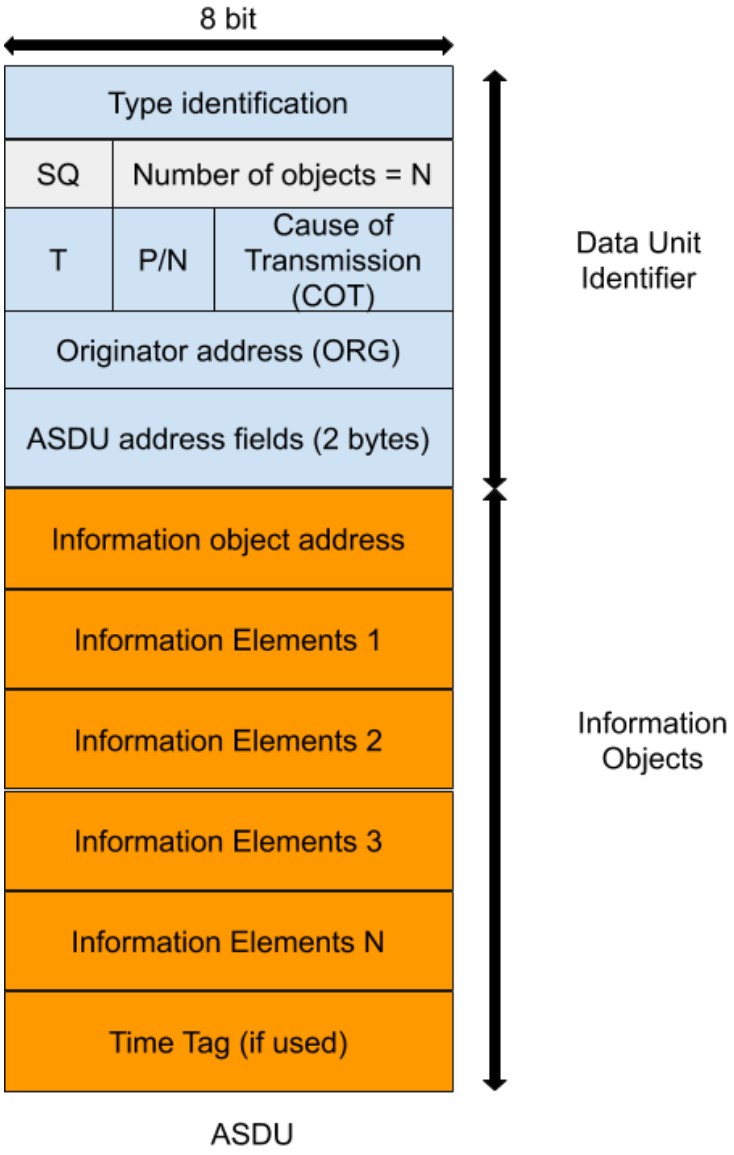
- Τα πλαίσια αυτά χρησιμοποιούνται για την εκτέλεση μη αριθμημένων συναρτήσεων ελέγχου και, όπως και τα S-format πλαίσια, έχουν σταθερό μήκος.
- Τα APDU αποτελούνται αποκλειστικά από ένα APCI.
- Αυτός ο τύπος IEC 60870-5-104 πλαισίων χρησιμοποιείται ως μηχανισμός ενεργοποίησης και επιβεβαίωσης των λειτουργιών STARTDT, STOPDT και TESTFR.
- Οι λειτουργίες STARTDT και STOPDT χρησιμοποιούνται από τον σταθμό ελέγχου για τη διαχείριση της μεταφοράς πληροφοριών από έναν από τους σταθμούς που ελέγχονται. Η λειτουργία TESTFR χρησιμοποιείται για περιοδικό έλεγχο της κατάστασης επικοινωνίας των συνδέσεων για όσο το δυνατόν πιο άμεση ανίχνευση προβλημάτων.



Εικόνα 5. Δομές διαφορετικών τύπων IEC 60870-5-104 Frames

2.3.2 IEC 60870-5-104 Application Service Data Unit

Το IEC 60870-5-104 ASDU [16] [17] περιλαμβάνει δύο βασικά πεδία: το Data Unit Identifier, το οποίο έχει σταθερό μήκος 6 bytes, και ένα πεδίο που περιλαμβάνει τα μεταδιδόμενα δεδομένα. Το πεδίο δεδομένων περιλαμβάνει από 1 έως και 127 Information Objects. Πιο συγκεκριμένα στο Data Unit Identifier ορίζονται οι προκαθορισμένοι τύποι δεδομένων, παρέχεται η διευθυνσιοδότηση για την ταυτοποίηση των δεδομένων και περιλαμβάνονται επιπλέον πληροφορίες, όπως το COT. Η δομή του IEC 60870-5-104 ASDU παρουσιάζεται στο παρακάτω σχήμα.



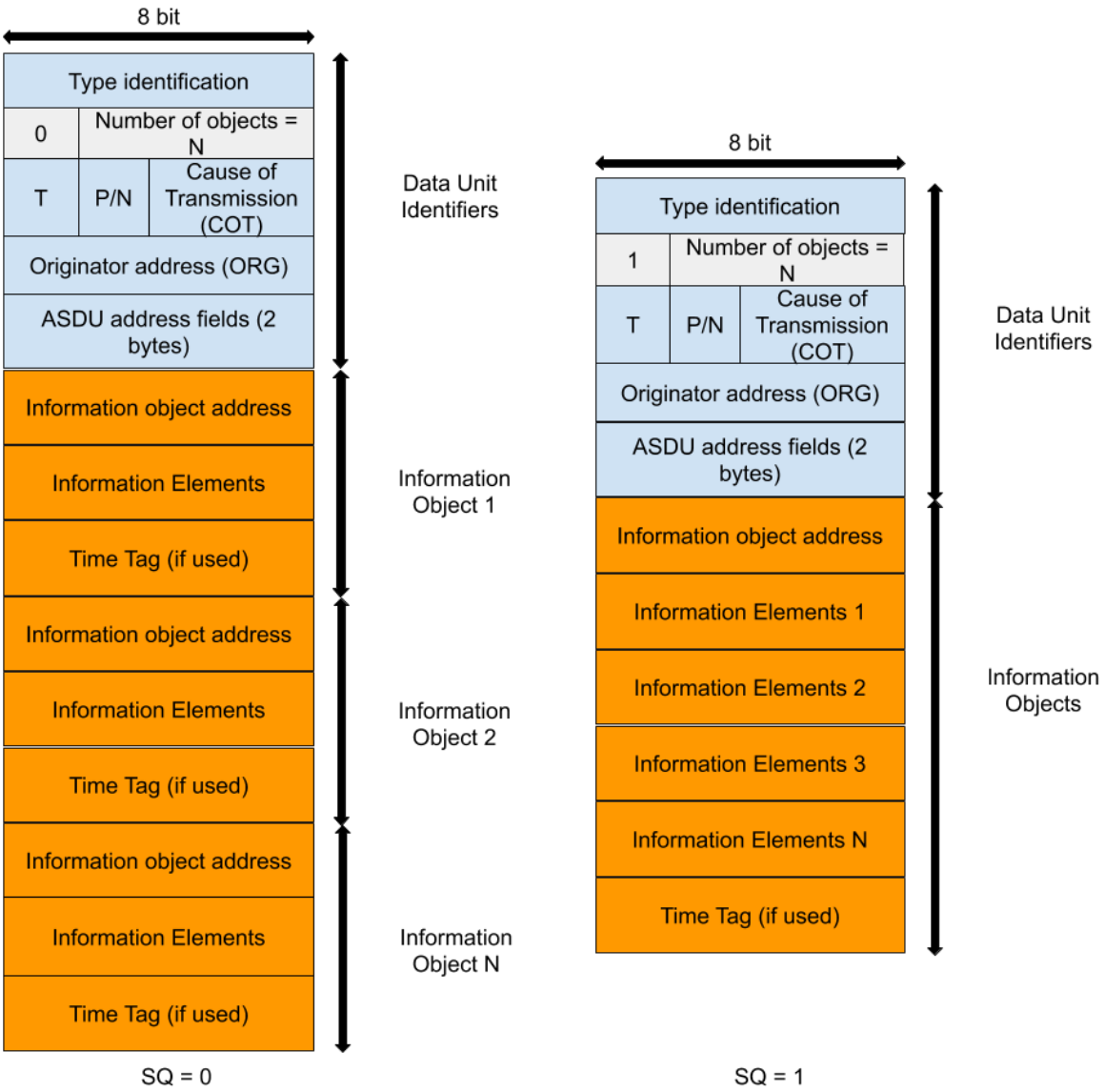
Εικόνα 6. Δομή IEC 60870-5-104 ASDU

Ένα από τα πεδία που περιλαμβάνει το Data Unit Identifier, είναι το TypeID, μεγέθους 1 bit, από την τιμή του οποίου εξαρτάται η δομή ολόκληρου του ASDU. Οι έγκυρες τιμές του πεδίου TypeID ανήκουν στο διάστημα 1-127 και παρουσιάζονται στον παρακάτω πίνακα:

Type ID	Group
1-40	Πληροφορίες Διεργασιών στην κατεύθυνση παρακολούθησης
45-51	Πληροφορίες Διεργασιών στην κατεύθυνση ελέγχου
70	Πληροφορίες Συστήματος στην κατεύθυνση παρακολούθησης
100-106	Πληροφορίες Συστήματος στην κατεύθυνση παρακολούθησης
110-113	Παράμετροι στην κατεύθυνση ελέγχου
120-126	Μεταφορά αρχείων

Εικόνα 7. Πεδία τιμών των IEC 60870-5-104 ASDU TypeID

Το πεδίο SQ έχει μέγεθος 1 bit και είναι μέρος του Data Unit Identifier. Το πεδίο αυτό καθορίζει τον τρόπο με τον οποίο θα γίνει η διευθυνσιοδότηση των Information Objects. Όταν η τιμή του πεδίου είναι 0, τότε το ASDU αποτελείται από ένα ή περισσότερα Information Objects, τα οποία διευθυνσιοδοτούνται ξεχωριστά, ενώ στην περίπτωση που έχει τιμή 1, όλα τα Information Objects του ASDU διευθυνσιοδοτούνται ως ένα μόνο αντικείμενο. Οι δύο προαναφερθείσες μορφές του ASDU εικονίζονται παρακάτω.



Εικόνα 8. Δομή IEC 60870-5-104 ASDU στις περιπτώσεις που SQ=1 ή SQ=0

Ο ρόλος του πεδίου COT είναι εμφανής από την ονομασία του πεδίου. Το μέγεθος του πεδίου είναι 6 bit και οι έγκυρες τιμές του πεδίου αυτού ανήκουν στο διάστημα 1-47.

Το ASDU Address Field (Common Address of ASDU) έχει μέγεθος 2 byte και χρησιμοποιείται για τη διευθυνσιοδότηση είτε ενός μόνο σταθμού είτε όλων των σταθμών μαζί ή ακόμα και υποσταθμών.

Τα Information Objects αποτελούν τη μονάδα μεταφοράς δεδομένων του ASDU. Η διεύθυνση του κάθε Information Object δίνεται από το IOA, το μήκος του οποίου είναι 3 byte. Ανάλογα με τον τύπο του ASDU, σε ένα Information Object μπορεί να περιλαμβάνονται δεδομένα (όπως δεκαδικές τιμές).

2.4 Δικτυακές επιθέσεις κατά του πρωτοκόλλου IEC 60870-5-104

Η ευρεία χρήση του πρωτοκόλλου IEC 60870-5-104 στα συστήματα SCADA δεν εξασφαλίζει δυστυχώς και την ασφάλεια από κυβερνοεπιθέσεις [16] [18] [19] [20] [21]. Για τον περιορισμό των αδυναμιών του πρωτοκόλλου έχει δημοσιευθεί το IEC 62351, το οποίο, όμως εισάγει αυξημένη πολυπλοκότητα και καθυστέρηση, πράγμα που αποτρέπει τους παρόχους να χρησιμοποιήσουν τη λύση αυτή, καθώς στα συστήματα SCADA δεν υπάρχει περιθώριο για αύξηση της καθυστέρησης ή του υπάρχοντος φόρτου. Τα κύρια κενά ασφαλείας του IEC 60870-5-104 και οι πιθανές επιπτώσεις τους συνοψίζονται παρακάτω:

- Κοινά προβλήματα ασφάλειας με το πρωτόκολλο TCP/IP, καθώς, όπως έχει αναφερθεί, το IEC 60870-5-104 είναι βασισμένο στη στοίβα του πρωτοκόλλου TCP/IP.
- Η μετάδοση δεδομένων μεταξύ του MTU και των υποσταθμών (RTU, PLC, IED) γίνεται σε μορφή απλού κειμένου, χωρίς την ύπαρξη κάποιου μηχανισμού κρυπτογράφησης. Δίνεται με αυτό τον τρόπο η δυνατότητα, σε κακόβουλους τρίτους να παρακολουθούν, να αναλύουν ακόμα και να μεταβάλλουν τα δεδομένα και να τα αποστέλλουν στον αρχικό τους προορισμό μέσω επίθεσης MITM. Οι παραπάνω κακόβουλες ενέργειες μπορεί να οδηγήσουν σε διατάραξη της σταθερότητας, να θέσουν σε κίνδυνο την ασφάλεια του συστήματος ή και να βοηθήσουν σε μελλοντικές προσπάθειες εισβολής στο σύστημα.
- Η απουσία μηχανισμών αυθεντικοποίησης σε interrogation commands, remote control commnads και remote adjustment commands μπορεί να οδηγήσει στην εκμετάλλευση από κακόβουλους χρήστες της κατάστασης αυτής, δίνοντάς τους έτσι τη δυνατότητα μη εξουσιοδοτημένης πρόσβασης σε διάφορες συσκευές ελέγχου των συστημάτων SCADA. Η κατάσταση αυτή μπορεί να οδηγήσει από απλή διαταραχή της ομαλής λειτουργίας του συστήματος έως και σε ανεπανόρθωτη ζημιά του συστήματος. Χαρακτηριστικό παράδειγμα αποτελεί η πρόκληση διακοπών ρεύματος ή η πρόκληση αυξημένου φόρτου στο σύστημα, λόγω αποστολής μη έγκυρων εντολών ελέγχου.

3. Συστήματα Ανίχνευσης Εισβολών

Όπως έχει αναφερθεί στις παραπάνω ενότητες, λόγω της σημασίας των συστημάτων SCADA, είναι αναγκαία η έγκαιρη ενημέρωση των διαχειριστών για πιθανές προσπάθειες εισβολής στο σύστημα, ώστε να υπάρχει περιθώριο αντίδρασης για την διατήρηση της ομαλής λειτουργίας του συστήματος, στην καλύτερη περίπτωση, ή για τον περιορισμό της ζημιάς, στο χειρότερο σενάριο. Στις προσπάθειες εισβολής συμπεριλαμβάνονται: οι αποκλίσεις από την κανονική λειτουργία, η εκτέλεση λειτουργιών, οι οποίες οδηγούν σε εισβολές, δηλαδή ανίχνευση κακόβουλης συμπεριφοράς, και τέλος η ανίχνευση εισβολών με βάση κάποιες προδιαγραφές, οι οποίες χρησιμοποιούνται για κατηγοριοποίηση της κίνησης με βάση κάποια σημεία αναφοράς, που προσδιορίζουν τη ‘φυσιολογική κίνηση’. Τα συστήματα που πραγματοποιούν αυτή την αυτοματοποιημένη ανίχνευση εισβολών, ονομάζονται IDS. Στη συνέχεια του κεφαλαίου θα αναλυθούν οι στόχοι, η αρχιτεκτονική των συστημάτων αυτών, υπάρχοντα μοντέλα ανίχνευσης εισβολών και θα παρουσιαστούν υπάρχοντα συστήματα ανίχνευσης εισβολών στοχευμένα σε συστήματα SCADA.

3.1 Δικτυακές ροές

Μία δικτυακή ροή [22] αποτελεί ένα σύνολο πακέτων, τα οποία διέρχονται από ένα σημείο παρατήρησης για ένα συγκεκριμένο χρονικό διάστημα και χαρακτηρίζονται από κοινά στοιχεία. Τα πακέτα μίας δικτυακής ροής χαρακτηρίζονται από ίδιες διευθύνσεις IP της πηγής και του προορισμού, ίδιες δικτυακές θύρες πηγής και προορισμού και ίδιο πρωτόκολλο πακέτου. Οι δικτυακές ροές μπορούν να ταξινομηθούν σε μονής ή αμφίδρομης κατεύθυνσης. Οι δικτυακές ροές μονής κατεύθυνσης αφορούν τη δικτυακή κίνηση, η οποία προέρχεται από την πηγή και κατευθύνεται προς τον προορισμό, ενώ οι αμφίδρομες ροές αφορούν τη συνολική δικτυακή κίνηση που ανταλλάσσεται μεταξύ της πηγής και του προορισμού. Στην συγκεκριμένη εργασία έχει γίνει χρήση των δικτυακών ροών αμφίδρομης κατεύθυνσης.

3.2 Στόχοι Συστημάτων Ανίχνευσης εισβολών

Ένα από τα απαιτούμενα χαρακτηριστικά ενός Συστήματος Ανίχνευσης Εισβολών είναι η δυνατότητά του να ανιχνεύει πολλούς διαφορετικούς τύπους εισβολών. Θα πρέπει, δηλαδή, να είναι δυνατή η ανίχνευση επιθέσεων που προέρχονται είτε από το εσωτερικό είτε από το εξωτερικό του δικτύου, οι οποίες συγκαταλέγονται σε υπάρχουσες επιθέσεις ή είναι νέοι τύποι επιθέσεων.

Μια ακόμα αναγκαία ιδιότητα των IDS αποτελεί η έγκαιρη ανίχνευση εισβολών, δηλαδή η ανίχνευση μίας εισβολής σε αρκετά μικρό χρονικό διάστημα, ώστε να υπάρχει κάποιο περιθώριο για αντίδραση, για τον περιορισμό των επιπτώσεων της επίθεσης. Όπως είναι κατανοητό, σε περίπτωση που η ανίχνευση της επίθεσης απαιτήσει μεγάλο χρονικό διάστημα, η ζημιά, που έχει προκληθεί, μπορεί να είναι μη αναστρέψιμη, άρα και η πληροφορία ότι έχει γίνει κάποια προσπάθεια εισβολής δεν είναι πλέον χρήσιμη.

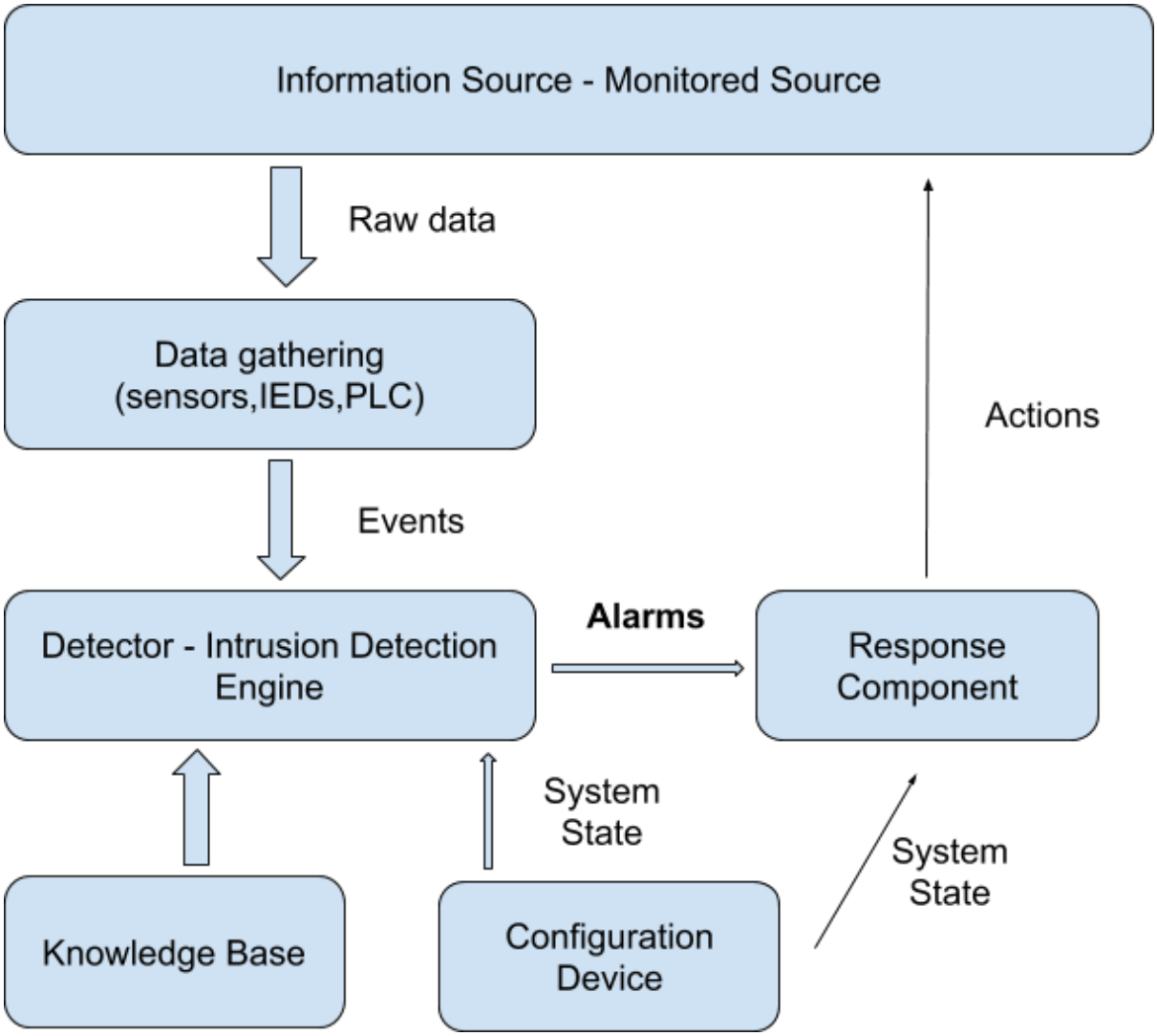
Επιπλέον, τα δεδομένα ανίχνευσης μίας εισβολής θα πρέπει να παρουσιάζονται σε εύκολη και κατανοητή μορφή στον υπεύθυνο ασφαλείας του συστήματος. Επειδή, όμως, οι μηχανισμοί ανίχνευσης εισβολών είναι δυνατό να παρακολουθούν περισσότερα από ένα συστήματα, κρίσιμο ζήτημα αποτελεί ο σχεδιασμός της διεπαφής τους με τον χρήστη.

Τέλος ένα IDS θα πρέπει να επιστρέφει ακριβή δεδομένα. Ένα από τα αίτια μείωσης της αξιοπιστίας του συστήματος είναι η εμφάνιση ψευδών θετικών σημάτων (false positives), δηλαδή αναφορά μίας επίθεσης, ενώ, στην πραγματικότητα, δεν υπάρχει κάποια επίθεση σε εξέλιξη [23]. Άλλος ένας παράγοντας μείωσης της αξιοπιστίας των συστημάτων ανίχνευσης εισβολών αποτελούν τα ψευδώς αρνητικά (false negatives) σήματα, τα οποία παράγονται, όταν το σύστημα, ενώ κάποια επίθεση βρίσκεται σε εξέλιξη, δεν αναφέρει το γεγονός αυτό.

3.3 Αρχιτεκτονική Συστημάτων Ανίχνευσης Εισβολών

Παρά το γεγονός ότι τα συστήματα ανίχνευσης εισβολών χρησιμοποιούν μεγάλη ποικιλία τεχνικών για συλλογή και ανάλυση δεδομένων, τα περισσότερα έχουν κοινή δομή [24]. Τα δομικά στοιχεία των συστημάτων ανίχνευσης εισβολών είναι:

- Μία συσκευή συλλογής δεδομένων του συστήματος που παρακολουθείται.
- Μία συσκευή ανίχνευσης εισβολών, η οποία αναλύει τα συλλεγόμενα δεδομένα, για να αναγνωρίσει προσπάθειες εισβολών.
- Μία βάση γνώσης, η οποία περιέχει πληροφορίες, που έχουν συλλεχθεί σε προ επεξεργασμένη μορφή.
- Μία συσκευή, που παρέχει πληροφορίες σχετικά με την τρέχουσα κατάσταση του IDS.
- Και τέλος ένα στοιχείο υπεύθυνο για την απόκριση του συστήματος, το οποίο, σε περίπτωση ανίχνευσης κάποιας προσπάθειας εισβολής, εκκινεί τις κατάλληλες διαδικασίες για διατήρηση της ομαλής λειτουργίας του παρακολουθούμενου συστήματος.



Εικόνα 9. Γενική Αρχιτεκτονική IDS

3.4 Μοντέλα Ανίχνευσης Εισβολών

Για την αξιολόγηση των συλλεγόμενων δεδομένων και την αναγνώρισή τους ως φυσιολογική κίνηση ή ως μη φυσιολογική κίνηση χρησιμοποιούνται από την αντίστοιχη μονάδα του IDS ένα ή και περισσότερα μοντέλα ανίχνευσης εισβολών. Τα μοντέλα διακρίνονται σε προσαρμοστικά, που έχουν δυνατότητα να μεταβάλλουν τη συμπεριφορά τους ανάλογα με τις ενέργειες των συστημάτων, και σε στατιστικά, με τη λειτουργία των τελευταίων να βασίζεται σε ένα προκαθορισμένο και στατικό σύνολο δεδομένων.

3.4.1 Μοντέλο Κακόβουλης Συμπεριφοράς

Το συγκεκριμένο μοντέλο χρησιμοποιείται συχνά σε εμπορικά IDS. Για την ανίχνευση μη ομαλής κίνησης γίνεται χρήση κάποιων προκαθορισμένων προτύπων εισβολών, τα οποία ονομάζονται υπογραφές. Γίνεται σύγκριση των παρατηρούμενων ενεργειών του

παρακολουθούμενου συστήματος με τις υπογραφές αυτές και σε περίπτωση που βρεθούν κοινά χαρακτηριστικά προκύπτει ότι υπάρχει μια εισβολή σε εξέλιξη.

Όπως είναι κατανοητό, το μοντέλο αυτό ανιχνεύει με μεγάλη αξιοπιστία καταγεγραμμένους τύπους εισβολών, δεν του είναι όμως δυνατό να αναγνωρίσει νέους τύπους εισβολών, για τους οποίους δεν έχουν δημιουργηθεί οι αντίστοιχες υπογραφές. Για τη βέλτιστη απόδοση του μοντέλου αυτού είναι αναγκαία η συχνή ανανέωση των υπογραφών νέων επιθέσεων, ώστε να είναι γνωστή η συντριπτική πλειοψηφία των αδυναμιών των συστημάτων, τις οποίες μπορούν να εκμεταλλευτούν οι επιτιθέμενοι.

3.4.2 Μοντέλα Ανίχνευσης Εισβολών

Αυτός ο τύπος μοντέλων ανιχνεύει εισβολές στο σύστημα με βάση την απόκλιση των παρατηρούμενων δραστηριοτήτων του συστήματος από αυτό που θεωρείται ‘φυσιολογικό’ για το σύστημα. Πιο αναλυτικά, μετά τη συγκέντρωση δεδομένων και στατιστικών, τα οποία θα ορίζουν τη ‘φυσιολογική δραστηριότητα’ του παρακολουθούμενου συστήματος, κάθε παρατηρούμενη ενέργεια, η οποία δεν συμπίπτει με τα πλαίσια λογικής συμπεριφοράς του συστήματος, θα αναγνωρίζεται από το σύστημα ως πιθανή περίπτωση εισβολής. Η πρόκληση στη δημιουργία τέτοιων μοντέλων βρίσκεται στον καλό ορισμό της ‘φυσιολογικής συμπεριφοράς’ του συστήματος, καθώς η δραστηριότητα των συστημάτων εμφανίζει διακυμάνσεις.

3.4.2.1 Μοντέλο Στατιστικών Ροπών

Οι στατιστικές ροπές είναι σύνολο στατιστικών μετρικών γνωστού συνόλου δεδομένων φυσιολογικής δραστηριότητας ενός συστήματος, μερικά από τα οποία είναι η τυπική απόκλιση, η διακύμανση, η μέση τιμή και η επικρατούσα τιμή. Τα παρατηρούμενα δεδομένα, τα οποία βρίσκονται εκτός των αναμενόμενων ορίων της αντίστοιχης στατιστικής ροπής, αναγνωρίζονται ως πιθανές εισβολές.

Η πολυπλοκότητα για την κατασκευή του εν λόγω μοντέλου είναι ιδιαίτερα μεγάλη, καθώς θα πρέπει να μοντελοποιηθεί τόσο η συμπεριφορά των χρηστών του συστήματος, η οποία παρουσιάζει σημαντικές διακυμάνσεις, αλλά και οι διεργασίες του συστήματος.

3.4.2.2 Μοντέλο Τιμών Κατωφλίου

Προϋπόθεση για τη δημιουργία του μοντέλου αποτελεί η καταμέτρηση ορισμένων χαρακτηριστικών των δραστηριοτήτων των χρηστών και του συστήματος, όπως είναι ο συνολικός αριθμών αρχείων, ο αριθμός αποτυχημένων προσπαθειών εισόδου ενός χρήστη στο σύστημα σε ορισμένο χρονικό διάστημα ή ακόμα και το ποσοστό χρήσης CPU, και ο ορισμός ενός ανώτατου επιτρεπτού ορίου, το οποίο μπορεί να είναι στατικό ή να μεταβάλλεται

δυναμικά για καθένα από αυτά τα χαρακτηριστικά. Εάν γίνει η υπόθεση ότι μία συγκεκριμένη ενέργεια μπορεί να εμφανιστεί κατά ελάχιστο x φορές και κατά μέγιστο y φορές, τότε, σε περίπτωση που σε ορισμένο χρονικό διάστημα η ενέργεια αυτή παρατηρηθεί λιγότερες φορές από τον αριθμό ελάχιστων επιτρεπόμενων φορών ή περισσότερες φορές από τον μέγιστο επιτρεπόμενο αριθμό φορών, παρατηρούμε μη φυσιολογική συμπεριφορά του συστήματος.

Συγκριτικά με το μοντέλο στατιστικών ροπών, η πολυπλοκότητα για τη δημιουργία ενός μοντέλου κατωφλίου είναι μικρότερη, με την ευελιξία, όμως, να είναι περιορισμένη.

3.5 Συστήματα Ανίχνευσης Εισβολών για συστήματα Εποπτικού Ελέγχου και Απόκτησης Δεδομένων

Στη συγκεκριμένη ενότητα γίνεται αναφορά προσεγγίσεων IDS, τα οποία είναι επικεντρωμένα σε ανίχνευση εισβολών σε συστήματα SCADA.

Πρόσφατες προτάσεις μέτρων ασφαλείας των συστημάτων SCADA στρέφονται σε συστήματα ανίχνευσης εισβολών πολλαπλών επιπέδων, όπως το [25], όπου το πρώτο επίπεδο ανιχνεύει την εισβολή, το δεύτερο ελέγχει τις μεταδιδόμενες εντολές σχετικά με το κατά πόσο είναι γνήσιες και τέλος, το τρίτο επίπεδο είναι υπεύθυνο για την αναφορά της εισβολής στους διαχειριστές του συστήματος. Έγινε δοκιμή του συστήματος σε δεδομένα του συνόλου τεχνητών δεδοδομένων KDD99 με χρήση του εργαλείου εξόρυξης δεδομένων WEKA, η οποία έδωσε αποτελέσματα που κατηγοριοποιούσαν σωστά πάνω από 94% των συνολικών δειγμάτων.

Στο [26] οι Maglaras L. A. και Jiang J. προτείνουν μια μονάδα ανίχνευσης εισβολών, η οποία βασίζεται στον αλγόριθμο μηχανικής μάθησης One-Class SVM, η οποία, αρχικά, εξάγει χαρακτηριστικά σε επίπεδο πακέτων από δικτυακές καταγραφές και τα χρησιμοποιεί για να κάνει την εκπαίδευση του αλγορίθμου. Πιο συγκεκριμένα τα βασικά στοιχεία, με βάση τα οποία γίνεται η εκπαίδευση, σχετίζονται με το ρυθμό μετάδοσης και το μέγεθος πακέτου. Στη συνέχεια, η μονάδα ανίχνευσης εισβολών ενημερώνει το σύστημα σχετικά με την προέλευση, τη στιγμή και τη σοβαρότητα της εισβολής. Τα αποτελέσματα από τη δοκιμή με δύο σύνολα δεδομένων έδειξαν ακρίβεια κατά μέσο όρο 98%.

Το έργο [27] αφορά τη χρήση αλγορίθμων μηχανικής μάθησης, όπως οι: J48, KNN, Naive Bayes και Random Forest, του εργαλείου εξόρυξης δεδομένων WEKA για κατηγοριοποίηση δεδομένων IEC 60870-5-104 σε επίπεδο πακέτου που έχουν συλλεχθεί από ένα σύστημα. Πιο αναλυτικά, μετά από καταγραφή κίνησης IEC 60870-5-104, τα δεδομένα δικτυακών καταγραφών αναλύονται, αφού πρώτα απομακρυνθούν τα πακέτα διαφορετικών

πρωτοκόλλων. Από την ανάλυση εξάγονται στοιχεία σε επίπεδο πακέτου, τα οποία σχετίζονται με το μήκος του πλαισίου, τον χρόνο που μεσολαβεί μεταξύ διαδοχικών πακέτων και το ρυθμό μετάδοσης πακέτων, σύμφωνα με τα οποία γίνεται κατηγοριοποίηση των πακέτων είτε ως φυσιολογικά είτε ως μη φυσιολογικά. Γίνεται στη συνέχεια χρήση των αλγορίθμων κατηγοριοποίησης του εργαλείου εξόρυξης δεδομένων Weka, όπως J48, KNN, Naive Bayes, Random Forest, με καλύτερα αποτελέσματα να προκύπτουν από τη χρήση του Decision Tree που επιτυγχάνει ακρίβεια πάνω από 91%.

Στο συγκεκριμένο έργο [28] γίνεται προσπάθεια ανίχνευσης σε promiscuous mode του δικτύου και χρήση του αλγορίθμου κρυπτογράφησης MD5, με στόχο την ανίχνευση προσπαθειών παρακολούθησης της κίνησης του δικτύου, βάσει των τιμών TTL των πακέτων, αναγνωρίζοντας και απομονώνοντας με αυτό τον τρόπο επιθέσεις DDoS. Η συγκεκριμένη τεχνική αξίζει να σημειωθεί ότι απαιτεί περιορισμένη χρήση εύρους ζώνης σε σχέση με υπάρχοντα IDS.

Σε αυτό το έργο [29], στο προτεινόμενο IDS που είναι προσαρμοσμένο σε σενάρια επιθέσεων σε SCADA συστήματα, αρχικά προσδιορίζονται οι φυσιολογικές και μη φυσιολογικές καταστάσεις του συστήματος και δημιουργούνται κανόνες ανίχνευσης εισβολών με βάση τις καταστάσεις του συστήματος που έχουν προσδιοριστεί. Στις καταστάσεις του συστήματος ορίζεται μια κλίμακα επικινδυνότητας, και όσο πιο επικίνδυνη είναι η κατάσταση στη οποία βρίσκεται το παρατηρούμενο σύστημα, τόσο περισσότερα προειδοποιητικά μηνύματα παραβίασης επιστρέφει.

Στο έργο [30] προτείνεται μια αρχιτεκτονική για ένα DIDS, το οποίο συνδυάζει πράκτορες ανίχνευσης πληροφοριών (NIDS, Honeypots, HIDS, συσκευές παρατήρησης-μέτρησης), σχετικών με τους ρόλους, τις θέσεις και τη συμπεριφορά των συσκευών του συστήματος SCADA και μια δομή πολλαπλών επιπέδων, στην οποία γίνεται επεξεργασία των παραπάνω δεδομένων που έχουν συλλεγεί από το σύστημα και στη συνέχεια ανίχνευση ανωμαλιών με χρήση αλγορίθμου μηχανικής μάθησης One-Class SVM. Η διαχείριση του συστήματος γίνεται με τη χρήση μίας SMP.

Η προτεινόμενη αρχιτεκτονική στο έργο [31] συγκρίνει προκαθορισμένες περιπτώσεις φυσιολογικής συμπεριφοράς του συστήματος για συγκεκριμένες καταστάσεις του πρωτοκόλλου IEC 60870-5-104, και παρατηρούμενη δραστηριότητα, ώστε να ανιχνεύσει αποκλίσεις και μη φυσιολογική συμπεριφορά. Έγινε, στη συνέχεια, υλοποίηση προτεινόμενου εργαλείου με χρήση του εργαλείου ITACA. Σε ένα σύνολο 1116497 πακέτων με 28 μη φυσιολογικά έγινε επιτυχής ανίχνευση όλων των μη φυσιολογικών πακέτων.

Σύμφωνα με την προτεινόμενη αρχιτεκτονική ανίχνευσης εισβολών στο έργο [32] υπάρχει μια μονάδα εξαγωγής κανόνων, που είναι υπεύθυνη για την εξαγωγή ενός συνόλου κανόνων για τη φυσιολογική κίνηση πρωτοκόλλου Modbus-TCP και ενός συνόλου κανόνων για τη μη φυσιολογική κίνηση πρωτοκόλλου Modbus-TCP, η οποία γίνεται με χρήση χαρακτηριστικών σε επίπεδο πακέτου, τα οποία έχουν εξαχθεί από δεδομένα δικτυακής κίνησης. Τα σύνολα κανόνων, που έχουν παραχθεί, χρησιμοποιούνται από τη μονάδα βαθιάς επιθεώρησης, η οποία κάνει την ανίχνευση ανωμαλιών σε πραγματικό χρόνο. Το σύστημα έχει δοκιμαστεί με δεδομένα, που παρήγαγαν οι συγγραφείς, τα οποία περιλαμβάνουν 40 κακόβουλα πακέτα Modbus-TCP, τα οποία ανιχνεύθηκαν με False Negative rate μικρότερο του 0.045% .

Στο έργο [33] προτείνεται μια τακτική μη επιβλεπόμενης μάθησης, σύμφωνα με την οποία γίνεται αναγνώριση φυσιολογικών και μη φυσιολογικών καταστάσεων σε δεδομένα, τα οποία δεν είναι κατηγοριοποιημένα. Σε κάθε παρατήρηση υπολογίζεται ένας βαθμός συνέπειας με χρήση της υλοποίησης του αλγορίθμου KNN στο λογισμικό εξόρυξης δεδομένων WEKA, καταλήγοντας στην εξαγωγή κανόνων με βάση την εγγύτητα των δεδομένων. Τα δεδομένα που χρησιμοποιήθηκαν για την αξιολόγηση του συστήματος αποτελούνται τόσο από διαθέσιμα σύνολα δεδομένων όσο και δεδομένα που παρήγαγαν οι συγγραφείς με χρήση ενός περιβάλλοντος, το οποίο προσομοίωσαν. Με τη χρήση του προτεινόμενου συστήματος επιτεύχθηκε F1-score και ρυθμός ανίχνευσης, που ξεπερνούσε, σε κάποιες περιπτώσεις, το 98%.

Τέλος στο έργο [16], μετά τη αναζήτηση των προβλημάτων ασφαλείας του πρωτοκόλλου IEC 60870-5-104, δημιουργήθηκαν κανόνες IEC 60870-5-104 για το SNORT IDS, για κοινούς τύπους επιθέσεων, όπως unauthorized read commands, unauthorized reset commands, unauthorized remote control and adjustment commands, spontaneous packets storm, unauthorized interrogation commands, buffer overflows, unauthorized broadcast requests και IEC-104 port communication. Η αρχιτεκτονική εφαρμόστηκε σε αρχείο δικτυακής κίνησης, που παράχθηκε από τους συγγραφείς, το οποίο περιελάβανε 41 μη φυσιολογικά πακέτα IEC 60870-5-104, ανιχνεύοντας επιτυχώς το σύνολο των μη φυσιολογικών πακέτων.

4. Μηχανική Μάθηση, ένα μέσο αυτοματοποιημένης βελτίωσης της απόδοσης συστημάτων

Η Μηχανική μάθηση [34] αποτελεί εφαρμογή της Τεχνητής Νοημοσύνης (Artificial Intelligence), η οποία παρέχει τη δυνατότητα σε συστήματα, να βελτιώνουν την απόδοσή τους στα αντικείμενά τους χωρίς επιπλέον προγραμματισμό, μόνο με τη χρήση των πληροφοριών που έχουν συλλεχθεί μέχρι στιγμής.

Με τον όρο μάθηση εννοείται η παρατήρηση δεδομένων, τα οποία αποτελούν παραδείγματα ή οδηγίες, με στόχο την εξαγωγή μοτίβων, τα οποία θα χρησιμοποιηθούν για την βελτίωση των αποφάσεων που θα λαμβάνει το σύστημα μετά την έκθεσή του στα δεδομένα που του παρασχέθηκαν. Απώτερος σκοπός της μηχανικής μάθησης είναι η αυτοματοποίηση της διαδικασίας της μάθησης των συστημάτων, χωρίς ανθρώπινη παρέμβαση, και, στη συνέχεια, αντίστοιχη ενημέρωση της υπάρχουσας βάσης γνώσης του συστήματος.

4.1 Κατηγορίες Μηχανικής Μάθησης

Η μηχανική μάθηση, γενικά διακρίνεται σε τρεις κατηγορίες οι οποίες, όμως, εάν κριθεί αναγκαίο, μπορούν να συνδυαστούν για επίτευξη των επιθυμητών αποτελεσμάτων. Οι κατηγορίες αυτές είναι [35]:

- Η Επιτηρούμενη μάθηση (Supervised Learning), σύμφωνα με την οποία ένας αλγόριθμος μηχανικής μάθησης μπορεί να εφαρμόσει την εμπειρία, που έχει αποκτήσει από παλαιότερα δεδομένα, για πρόβλεψη μελλοντικών γεγονότων. Πιο συγκεκριμένα, μετά την ανάλυση ενός γνωστού, κατηγοριοποιημένου συνόλου δεδομένων, ο αλγόριθμος μάθησης δημιουργεί μια συνάρτηση, ώστε να μπορεί να κάνει ακριβείς προβλέψεις.
- Η Μη Επιτηρούμενη μάθηση (Unsupervised Learning), στην οποία, σε αντίθεση με την Επιτηρούμενη μάθηση, τα δεδομένα, που χρησιμοποιούνται για την εκπαίδευση, δεν είναι ούτε κατηγοριοποιημένα, ούτε έχουν κάποια ετικέτα για τον τύπο ή την κατηγορία τους. Το δημιουργούμενο μοντέλο αναζητά από μόνο του χρήσιμες πληροφορίες, όπως διάφορα μοτίβα, τα οποία θα βοηθήσουν στην ομαδοποίηση των δεδομένων.
- Η Ενισχυτική μάθηση (Reinforcement Learning) έχει ως αντικείμενο την εκπαίδευση ενός μοντέλου μηχανικής μάθησης με στόχο την λήψη μίας ακολουθίας αποφάσεων. Ένας πράκτορας Ενισχυτικής μάθησης κάνει κάποιες ενέργειες σε ένα περιβάλλον, το

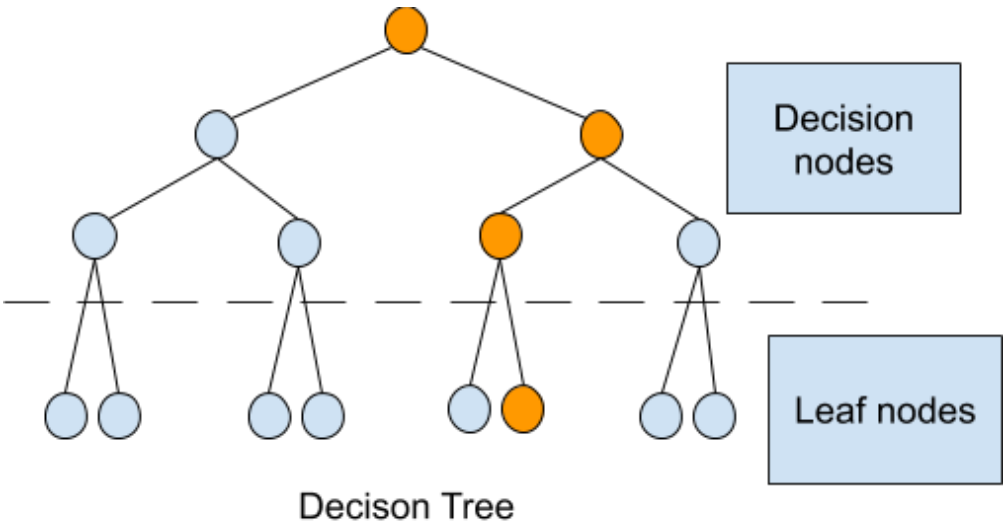
οποίο μπορεί να είναι άγνωστο σε αυτόν, και ανακαλύπτει, με βάση τα αποτελέσματα των ενεργειών του, ανταμοιβές, αλλά και σφάλματα.

4.2 Κατηγοριοποίηση

Η κατηγοριοποίηση αποτελεί μια κατηγορία Επιτηρούμενης μάθησης και στόχος της είναι η κατάταξη μίας παρατήρησης σε προκαθορισμένες κατηγορίες, με βάση ένα σύνολο δεδομένων, το οποίο περιλαμβάνει παρατηρήσεις, των οποίων η κατηγορία, στη οποία κατατάσσονται, είναι γνωστή. Μερικοί από τους γνωστότερους αλγόριθμους μηχανικής μάθησης και νευρωνικών δικτύων που χρησιμοποιούνται για κατηγοριοποίηση παρουσιάζονται στις παρακάτω ενότητες.

4.2.1 Decision Tree classifier

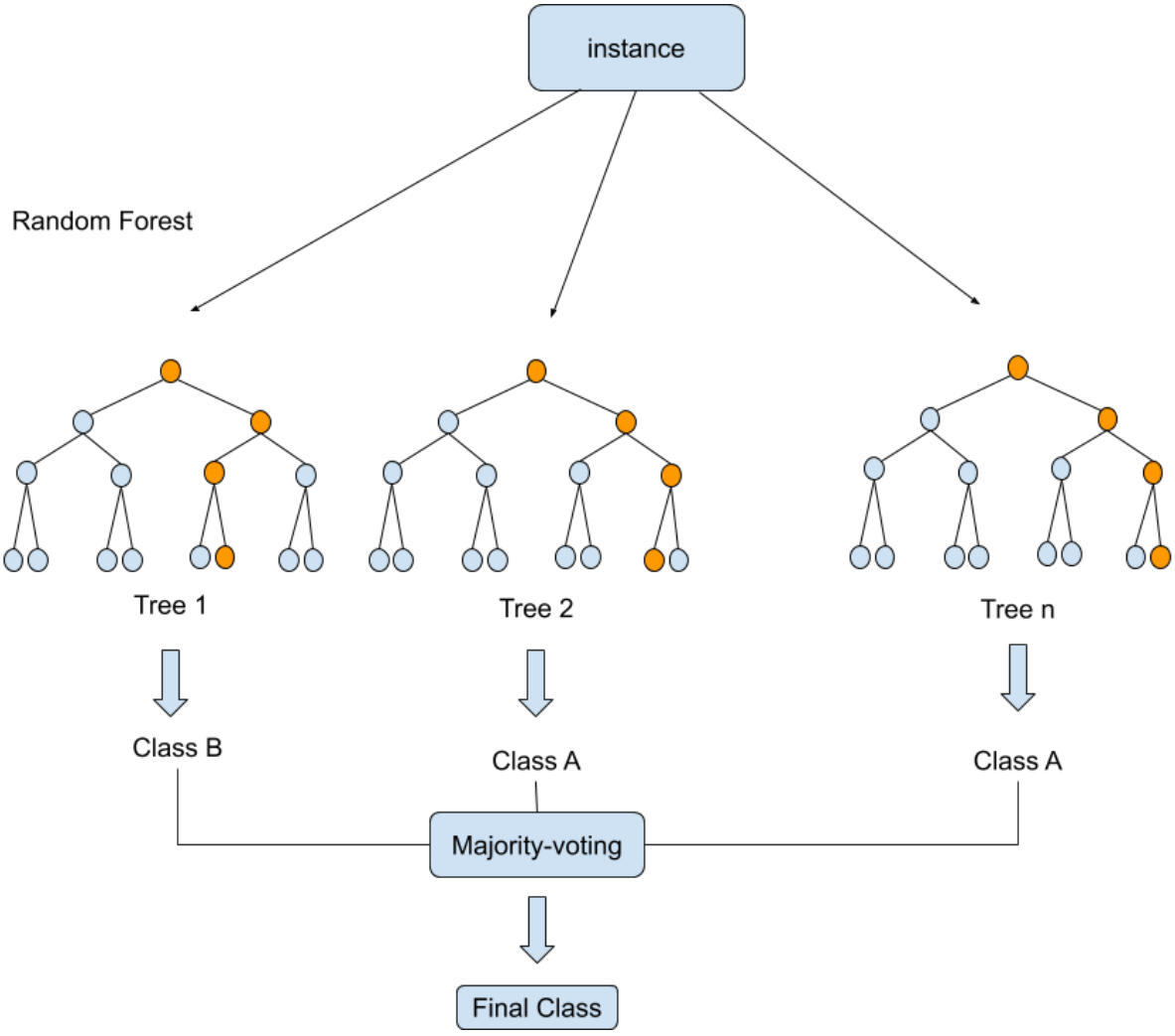
Τα δέντρα απόφασης (Decision Trees) [36] [37] αποτελούν μία από τις γνωστότερες μεθόδους κατηγοριοποίησης με χρήση επιβλεπόμενης μάθησης. Τα δέντρα απόφασης έχουν ιεραρχική δομή δέντρου, η οποία αποτελείται από κόμβους απόφασης (decision nodes) και κόμβους φύλλα (leaf nodes). Κάθε κόμβος απόφασης αντιστοιχεί σε μια συνθήκη σχετικά με κάποιο χαρακτηριστικό μίας συγκεκριμένης μεταβλητής. Η συνθήκη έχει διακλαδώσεις, καθεμιά από τις οποίες διαχειρίζεται ένα από τα πιθανά αποτελέσματα της συνθήκης. Οι κόμβοι φύλλα, παρουσιάζουν μια από τις κλάσεις στις οποίες πρέπει να κατηγοριοποιηθούν τα δείγματα, η οποία είναι το αποτέλεσμα της απόφασης σε κάποια συγκεκριμένη περίπτωση. Ο κατηγοριοποιητής αυτός αποσκοπεί στη δημιουργία αρκετών συνθηκών, ώστε να μην υπάρχουν άλλα χαρακτηριστικά των δεδομένων προς διάσπαση. Μία δομή δέντρων απόφασης φαίνεται στην παρακάτω εικόνα.



Εικόνα 10. Δομή Decision Tree

4.2.2 Random Forest classifier

Ο αλγόριθμος Random Forest είναι ένας συνδυαστικός αλγόριθμος, βασισμένος στον αλγόριθμο μηχανικής μάθησης δέντρων απόφασης. Ο αλγόριθμος κατηγοριοποίησης Random Forest αποτελεί ένα σύνολο δέντρων απόφασης από ένα τυχαίο υποσύνολο των δεδομένων εκπαίδευσης. Ο αλγόριθμος προσθέτει τις αποφάσεις από όλα τα δέντρα που έχουν δημιουργηθεί, και με τον τρόπο αυτό, ορίζεται η κλάση, στην οποία θα κατηγοριοποιηθεί η κάθε παρατήρηση του συνόλου δεδομένων αξιολόγησης. Η αρχιτεκτονική του αλγορίθμου παρουσιάζεται παρακάτω.



Εικόνα 11. Δομή Random Forest

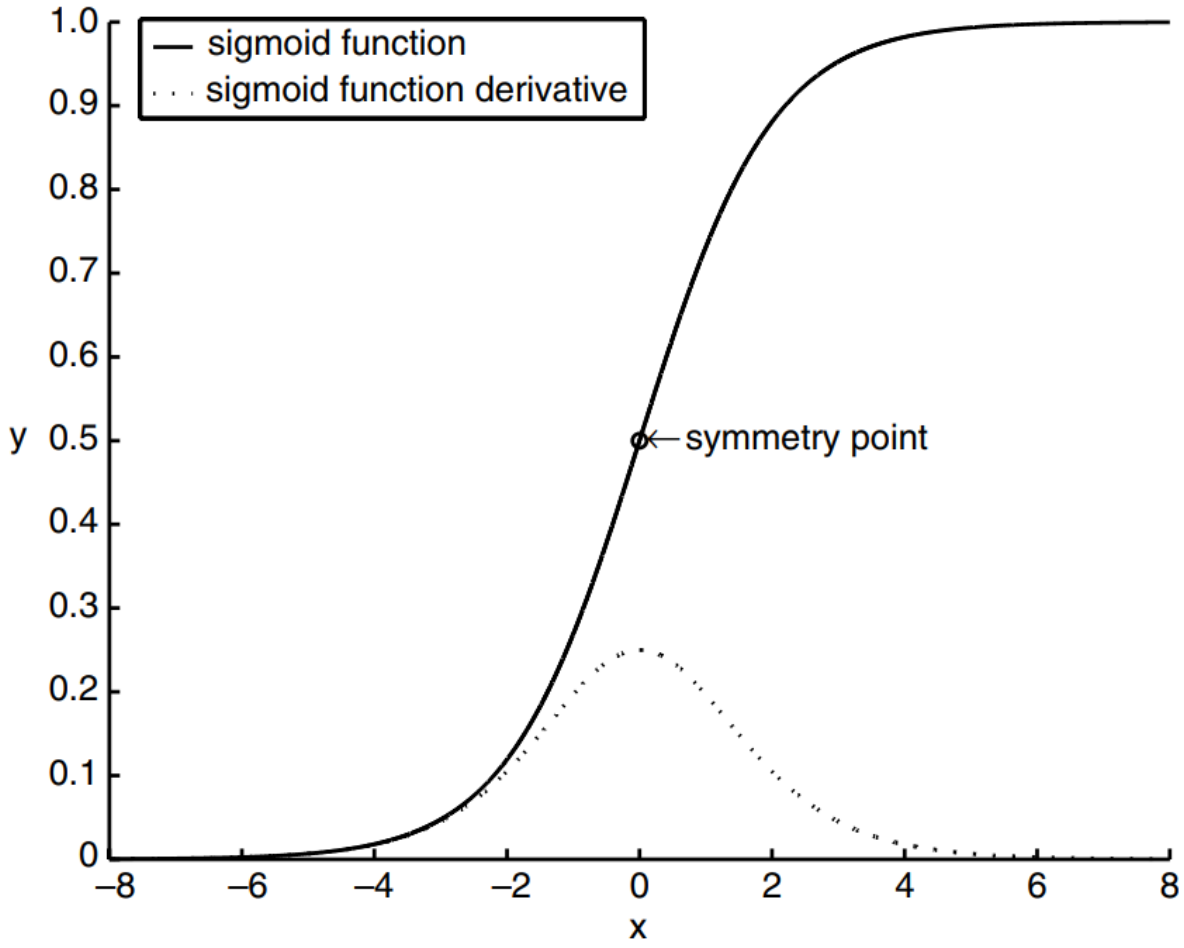
4.2.3 K-Nearest Neighbour classifier

Η λειτουργία του αλγορίθμου KNN βασίζεται στην κατηγοριοποίηση δεδομένων βάσει ενός μέτρου ομοιότητας. Αρχικά, γίνεται αποθήκευση όλων των δεδομένων. Τα χαρακτηριστικά των εγγραφών θα πρέπει να έχουν αριθμητικές τιμές, έτσι ώστε, για την κατηγοριοποίηση των εγγραφών, να μπορεί να υπολογιστεί η εγγύτητα μίας εγγραφής ως προς

τις υπόλοιπες. Για τον προσδιορισμό της εγγύτητας υπάρχουν αρκετές προτεινόμενες μετρικές, όπως είναι η Ευκλείδεια απόσταση και η απόσταση Manhattan. Μια εγγραφή κατηγοριοποιείται με βάση την κατηγορία των γειτόνων της. Η τελική κλάση, στην οποία κατατάσσεται η εγγραφή, είναι η πιο συχνά εμφανιζόμενη από τις κλάσεις των K κοντινότερων γειτονικών εγγραφών.

4.2.4 Logistic Regression classifier

Η μέθοδος Logistic Regression είναι ένας τύπος Στατιστικής μάθησης (Statistical Learning), η οποία εντάσσεται στην Μη Επιβλεπόμενη Μάθηση, μπορεί, όμως, με κάποιες τροποποιήσεις να χρησιμοποιηθεί και σαν τεχνική επιβλεπόμενης μάθησης. Η τεχνική αυτή χρησιμοποιείται για την κατηγοριοποίηση γεγονότων, τα οποία μπορεί να ανήκουν σε 2 κλάσεις και στην περίπτωση αυτή αναφερόμαστε σε Binomial Logistic Regression Classification, ή μπορεί να ανήκουν και σε περισσότερες κλάσεις και στην περίπτωση αυτή αναφερόμαστε σε Multinomial Logistic Regression Classification. Ο κατηγοριοποιητής Logistic Regression μετασχηματίζει την έξοδό του χρησιμοποιώντας τη συνάρτηση sigmoid ή logistic function, η οποία εικονίζεται στο παρακάτω σχήμα.



Εικόνα 12. Λογιστική Συνάρτηση / συνάρτηση Sigmoid [38]

4.2.5 Κατηγοριοποίηση με χρήση νευρωνικών δικτύων

Μία μέθοδος νευρωνικών δικτύων που χρησιμοποιείται για κατηγοριοποίηση δεδομένων, αποτελεί ο Perceptron, ο οποίος είναι ένας γραμμικός κατηγοριοποιητής, που παράγει μια συγκεκριμένη έξοδο βασισμένη σε πολλαπλές εισόδους, δημιουργώντας έναν γραμμικό συνδυασμό με χρήση βαρών, που δέχεται ως είσοδο.

Μια άλλη μέθοδος είναι η MLPC [37], που αποτελεί ένα τεχνητό νευρωνικό δίκτυο βαθιάς μάθησης, το οποίο απαρτίζεται από περισσότερους από έναν Perceptron. Η δομή αυτού του νευρωνικού δικτύου είναι η εξής:

- Ένα επίπεδο εισόδου, που λαμβάνει το σήμα.
- Ένα επίπεδο εξόδου, που κάνει την πρόβλεψη.
- Και, μεταξύ των επιπέδων εισόδου και εξόδου, ένα ή περισσότερα επίπεδα, τα οποία αποτελούν τον υπολογιστικό πυρήνα του νευρωνικού δικτύου.

4.2.6 Naive Bayes classifier

Ο αλγόριθμος Naive Bayes [39] [40] [41] αποτελεί μια πιθανοτική μέθοδο κατηγοριοποίησης, βασισμένη στο θεώρημα του Bayes. Ο αλγόριθμος υπολογίζει μια όμαδα πιθανοτήτων από την καταμέτρηση της συχνότητας και των συνδυασμών των τιμών ενός συνόλου δεδομένων. Παρά το γεγονός ότι η παραπάνω υπόθεση σπάνια είναι ορθή σε πραγματικά προβλήματα, ο αλγορίθμος χαρακτηρίζεται από ταχύτατο ρυθμό μαθησης σε ποικίλα επιτηρούμενα προβλήματα κατηγοριοποίησης. Ένα Naive Bayes μοντέλο είναι εύκολο να δημιουργηθεί, άρα είναι ιδιαίτερα χρήσιμο για μεγάλα σύνολα δεδομένων. Παρά την απλότητα του μοντέλου Naive Bayes, η απόδοσή του ξεπερνά αρκετές πιο πολύπλοκες τεχνικές κατηγοριοποίησης.

4.2.7 Support Vector Machine classifier

Γενικά οι κατηγοριοποιητές SVM [37] προσπαθούν να διακρίνουν το χώρο των δεδομένων με χρήση γραμμικών ή μη γραμμικών μεθόδων για διάκριση των ορίων μεταξύ διαφορετικών κλάσεων. Στην αρχική του μορφή ο αλγόριθμος SVM χρησιμοποιείται για τη δυαδική κατηγοριοποίηση, με παραλλαγές του να χρησιμοποιούνται και σε κατηγοριοποίηση δεδομένων πολλαπλών κλάσεων. Στόχος των αλγορίθμων αυτών είναι η εύρεση των βέλτιστων ορίων μεταξύ των διαφορετικών κλάσεων για χρησιμοποίησή τους με σκοπό την κατηγοριοποίηση.

4.3 Σύνολα Δεδομένων Ανίχνευσης Εισβολών

Όπως έχει αναφερθεί, τα συστήματα κρίσιμων υποδομών, λόγω της σημασίας των υπηρεσιών τους, δεν παρέχουν πρόσβαση σε λεπτομέρειες σχετικά με τη λειτουργία τους στο κοινό. Συνεπώς, τα σύνολα δεδομένων συστημάτων SCADA ή ICS είναι λιγοστά και δεν περιλαμβάνουν πραγματικά δεδομένα από πραγματικά συστήματα, αλλά δεδομένα από προσομοιώσεις, οι οποίες έχουν γίνει με βάση τις λιγοστές πληροφορίες που παρέχονται στο κοινό σχετικά με την ανταλλαγή δεδομένων σε τέτοια συστήματα. Ένα τέτοιο σύνολο δεδομένων για ανίχνευση εισβολών στο βιομηχανικό πρωτόκολλο IEC 60870-5-104 έχει δημιουργηθεί και παρέχεται στο κοινό στο έργο [42], και περιλαμβάνει επιθέσεις MITM. Υπάρχουν κάποια αξιόπιστα τεχνητά σύνολα δεδομένων για αξιολόγηση IDS, όπως το KDD99 [43], το NSLKDD και το UNSW [44], τα οποία, όμως, δεν είναι δεδομένα από προσομοιώσεις βιομηχανικών συστημάτων.

4.4 Μέτρα Αξιολόγησης Μοντέλου Μηχανικής Μάθησης

Μετά την εκπαίδευση και τη δημιουργία του μοντέλου μηχανικής μάθησης είναι απαραίτητη η αξιολόγησή του πριν τη χρήση του σε άγνωστα δεδομένα, ώστε να φανεί κατά πόσο οι προβλέψεις του μοντέλου είναι έμπιστες. Σε αρκετές περιπτώσεις, με τη διαδικασία της αξιολόγησης είναι δυνατή η βελτίωση του μοντέλου [35].

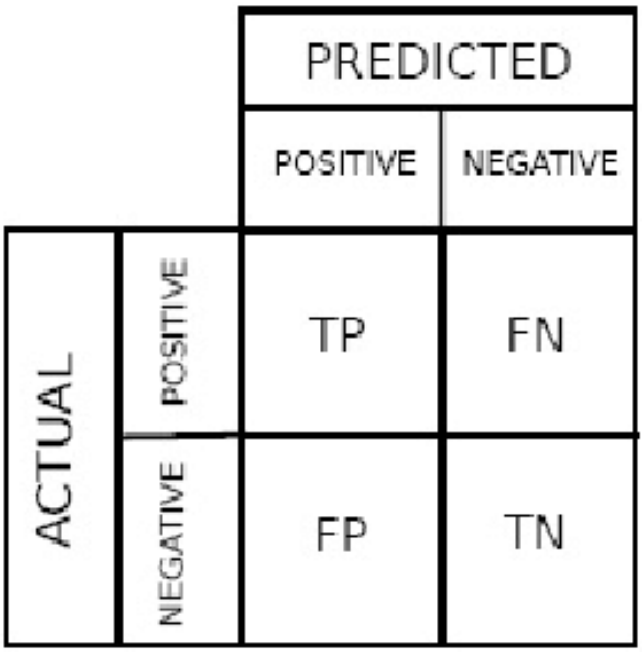
Η συχνότερη πρακτική αξιολόγησης ενός μοντέλου, ως προς την αξιοπιστία των προβλέψεων του, γίνεται με την κατηγοριοποίηση δεδομένων ενός Test set και ενός Training set. Τα δύο σύνολα δεδομένων θα πρέπει να έχουν την ίδια μορφή. Τα δεδομένα για την σωστή αξιολόγηση του μοντέλου θα πρέπει να μην είναι ίδια στο Training και στο Test set, καθώς, σε αντίθετη περίπτωση, θα παρατηρείται υπερπροσαρμογή (overfitting) του μοντέλου, το οποίο, αντί να βρίσκει σχέσεις μεταξύ των δεδομένων, απομνημονεύει τα δεδομένα στην είσοδο που του δίνεται. Η συγκεκριμένη μέθοδος υιοθετείται από την διπλωματική αυτή για την αξιολόγηση των πειραματικών δεδομένων.

Κατά τη δημιουργία του Test set είναι σημαντικό να εξασφαλίζεται ισορροπία μεταξύ του πλήθους δεδομένων του Test και του Training set. Πέρα από την ισορροπία ως προς το πλήθος των δεδομένων, θα πρέπει να λαμβάνεται υπόψη και ο βαθμός ομοιότητας του Test set με του Training set. Γενικά, όσο μεγαλύτερη είναι η ομοιότητα, τόσο μειώνεται η αξιοπιστία των αποτελεσμάτων, καθώς δεν είναι δυνατή η γενίκευση των αποτελεσμάτων σε διαφορετικά σύνολα δεδομένων.

Για την αποφυγή της υπερπροσαρμογής (overfitting) ενός μοντέλου μηχανικής μάθησης, πέρα από τη λύση της χρήσης δύο διαφορετικών συνόλων δεδομένων, δηλαδή ενός Training set και ενός Test set, μια εξίσου διαδεδομένη λύση αποτελεί η διαίρεση του Training set σε δύο τμήματα, ένα για την εκπαίδευση του μοντέλου, της τάξης του 60-70% των αρχικών δεδομένων και ένα για την αξιολόγησή του, της τάξης του 40-30% αντίστοιχα. Το αρχικό σύνολο δεδομένων είναι σημαντικό να έχει δημιουργηθεί προσεκτικά, καθώς, σε αντίθετη περίπτωση, τα δεδομένα μπορεί να παρουσιάζουν ομοιότητες, οδηγώντας και πάλι σε υπερπροσαρμογή του μοντέλου. Η μέθοδος αυτή χρησιμοποιείται αρκετά συχνά και, παρά τους κινδύνους, επιστρέφει ρεαλιστικά αποτελέσματα.

Ένας άλλος τρόπος μείωσης της πιθανότητας υπερπροσαρμογής κατά τη δημιουργία ενός μοντέλου μηχανικής μάθησης είναι η χρήση της μεθόδου του Cross-Validation, στην οποία γίνεται χρήση μόνο ενός Training set, με το οποίο γίνεται η εκπαίδευση και η αξιολόγηση του μοντέλου. Υποκατηγορία της μεθόδου αυτής αποτελεί το k-fold Cross-Validation, σύμφωνα με την οποία το Training set χωρίζεται σε ισομεγέθη υποσύνολα δεδομένων, με ένα από αυτά να χρησιμοποιείται ως σύνολο αξιολόγησης του μοντέλου και τα υπόλοιπα k-1 σύνολα, να ενώνονται σε ένα, το οποίο χρησιμοποιείται για την εκπαίδευση του μοντέλου μηχανικής μάθησης και όλη αυτή η διαδικασία επαναλαμβάνεται k φορές. Κάθε επανάληψη της διαδικασίας αυτής εξάγει ένα σφάλμα του μοντέλου και ο μέσος όρος των σχετικών σφαλμάτων από τις k επαναλήψεις ορίζει το τελικό σφάλμα το μοντέλου.

Αναφορικά με την έκβαση της προσπάθειας δυαδικής κατηγοριοποίησης ενός περιστατικού με βάση ένα μοντέλο μηχανικής μάθησης, τέσσερις είναι οι πιθανές εκβάσεις της προσπάθειας αυτής. Τα δεδομένα που προκύπτουν χρησιμοποιούνται για τον υπολογισμό μετρικών, όπως είναι η ακρίβεια (precision), η ανάκληση (recall) και το F-1 score. Για να γίνει πιο κατανοητή η επεξήγηση των καταστάσεων αυτών θα χρησιμοποιήσουμε το παράδειγμα ανίχνευσης μη φυσιολογικής κίνησης σε ένα σύστημα SCADA. Στην παρακάτω εικόνα εικονίζεται ένας confusion matrix, ο οποίος εμφανίζει αρκετές από τις πληροφορίες, που θα χρησιμοποιηθούν για την αξιολόγηση ενός μοντέλου.



Εικόνα 13. Confusion Matrix [45]

- TP (True Positive). Το οποίο υποδηλώνει τις περιπτώσεις, οι οποίες χαρακτηρίστηκαν ως μη φυσιολογική κίνηση από τον κατηγοριοποιητή και είναι πράγματι περιπτώσεις μη φυσιολογικής κίνησης .
- TN (True Negative). Το οποίο υποδηλώνει τις περιπτώσεις, οι οποίες χαρακτηρίστηκαν ως φυσιολογική κίνηση από τον κατηγοριοποιητή και είναι πράγματι περιπτώσεις φυσιολογικής κίνησης .
- FP (False Positive). Το οποίο υποδηλώνει τις περιπτώσεις, οι οποίες χαρακτηρίστηκαν ως μη φυσιολογική κίνηση από τον κατηγοριοποιητή, οι οποίες στην πραγματικότητα αποτελούν περιπτώσεις φυσιολογικής κίνησης .
- FN (False Negative). Το οποίο υποδηλώνει τις περιπτώσεις, οι οποίες χαρακτηρίστηκαν ως φυσιολογική κίνηση από τον κατηγοριοποιητή, οι οποίες στην πραγματικότητα αποτελούν περιπτώσεις μη φυσιολογικής κίνησης .

Η ακρίβεια (precision) δίνεται από τους παρακάτω τύπους για δυαδική κατηγοριοποίηση και για κατηγοριοποίηση με περισσότερες από δύο κλάσεις .

$$\text{Ακρίβεια} = \frac{\text{TP}}{\text{άθροισμα TP και FP}}$$

τύπος υπολογισμού της ακρίβειας στη δυαδική κατηγοριοποίηση

$$\text{Ακρίβεια} = \frac{\text{άθροισμα TP όλων των κλάσεων}}{\text{άθροισμα TP και FP όλων των κλάσεων}}$$

τύπος υπολογισμού της ακρίβειας στην κατηγοριοποίηση περισσότερων από 2 κλάσεων

Εικόνα 14. Τύποι υπολογισμού της μετρικής της ακρίβειας στην κατηγοριοποίηση

Η ανάκληση (recall) είναι μια ακόμα μετρική για την αξιολόγηση ενός μοντέλου μηχανικής μάθησης και υπολογίζεται με τους παρακάτω τύπους για την κατηγοριοποίηση με δύο ή περισσότερες κλάσεις.

$$\text{Ανάκληση} = \frac{\text{TP}}{\text{άθροισμα TP και FN}}$$

τύπος υπολογισμού της ανάκλησης στη δυαδική κατηγοριοποίηση

$$\text{Ανάκληση} = \frac{\text{άθροισμα TP όλων των κλάσεων}}{\text{άθροισμα TP και FN όλων των κλάσεων}}$$

τύπος υπολογισμού της ανάκλησης στην κατηγοριοποίηση περισσότερων από 2 κλάσεων

Εικόνα 15. Τύποι υπολογισμού της μετρικής της ανάκλησης στην κατηγοριοποίηση

Η ακρίβεια και η ανάκληση δεν αποτελούν, όμως, από μόνες τους μετρικές που προσφέρουν αξιόπιστα συμπεράσματα για την αξιολόγηση του μοντέλου. Για το σκοπό αυτό χρησιμοποιείται το F-1 score ή F-score, το οποίο αποτελεί συνδυασμό των μετρικών της ακρίβειας και της ανάκλησης σύμφωνα με τον παρακάτω τύπο.

$$\text{F1-score} = \frac{2 * \text{Ακρίβεια} * \text{Ανάκληση}}{\text{άθροισμα Ακρίβειας και Ανάκλησης}}$$

τύπος υπολογισμού της f1-score

Εικόνα 16. Τύπος υπολογισμού μετρικής F1-score στην κατηγοριοποίηση

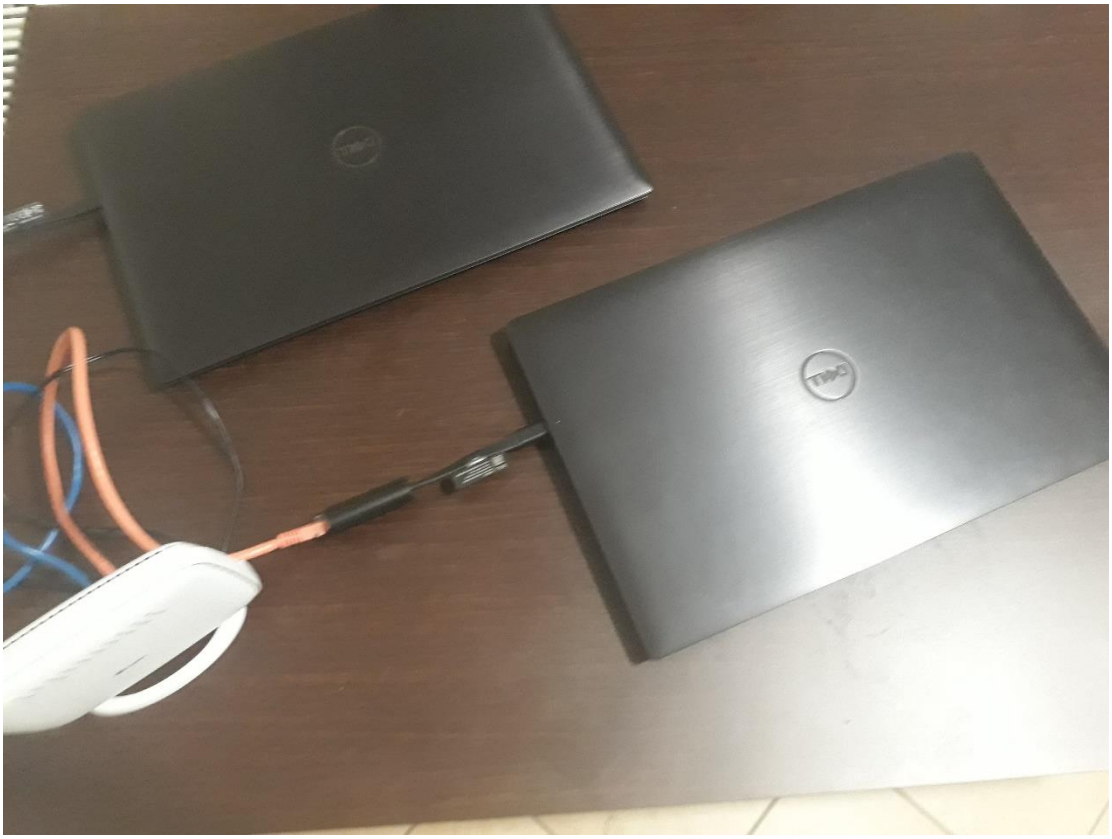
5. Σύστημα Ανίχνευσης Εισβολών του πρωτοκόλλου IEC 60870-5-104

Το προτεινόμενο σύστημα ανίχνευσης εισβολών του βιομηχανικού πρωτοκόλλου επικοινωνίας IEC 60870-5-104, που αναπτύχθηκε στα πλαίσια αυτής της διπλωματικής εργασίας, κάνει ανάλυση αρχείων δικτυακών καταγραφών, τα οποία περιέχουν φυσιολογική και μη φυσιολογική κίνηση IEC 60870-5-104, και εξάγει χαρακτηριστικά σε επίπεδο δικτυακών ροών, τα οποία χρησιμοποιούνται στη συνέχεια για τη δημιουργία μοντέλου μηχανικής μάθησης για τη σωστή κατηγοριοποίηση διαφόρων τύπων επιθέσεων με χρήση αλγορίθμων επιβλεπόμενης μάθησης, όπως είναι Decision Trees, Random Forest, KNN, Logistic Regression Classifier, Multilayer Perceptron Classifier, Perceptron, Support Vector Machines.

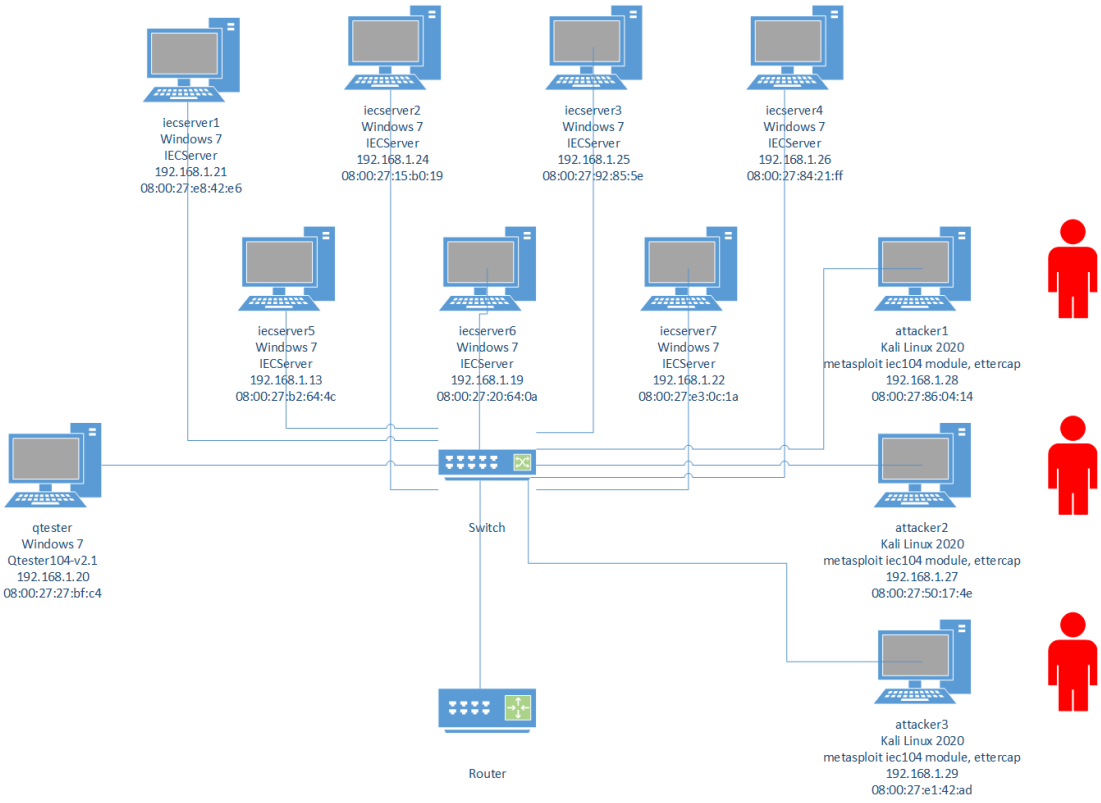
5.1 Καταγραφή και Ανάλυση Δικτυακής κίνησης του πρωτοκόλλου IEC 60870-5-104

Στα πλαίσια της εργασίας αυτής προσομοιώθηκε ένα σύστημα SCADA, στο οποίο πραγματοποιήθηκαν διάφοροι τύποι επιθέσεων και καταγράφηκαν τα απαραίτητα δεδομένα δικτυακής κίνησης.

Η προσομοίωση του συστήματος γίνεται με χρήση δύο υπολογιστών με ίδιες προδιαγραφές: επεξεργαστή Intel i7 8850H, 16GB RAM, 512 GB SSD, οι οποίοι είναι συνδεδεμένοι γεφυρωμένα με χρήση ενός Router. Το σύνολο των συσκευών του συστήματος προσομοιώνεται με χρήση του λογισμικού εικονοποίησης Oracle VirtualBox. Πιο συγκεκριμένα το σύστημα, που προσομοιώνεται, αποτελείται από τρεις εικονικές μηχανές με λειτουργικό σύστημα Kali Linux 2020, από τις οποίες γίνονται οι περισσότερες επιθέσεις με χρήση των λογισμικών εύρεσης αδυναμιών συστημάτων Ettercap και Metasploit, επτά εικονικές μηχανές με λειτουργικό σύστημα Windows 7, οι οποίες δρουν ως PLC με χρήση του λογισμικού IEC TestServer και μία εικονική μηχανή, η οποία διαδραματίζει, με χρήση του λογισμικού Qtester104, το ρόλο του MTU, που επικοινωνεί με τα PLC. Τόσο το φυσικό testbed όσο και η γενική τοπολογία του συστήματος φαίνονται στις παρακάτω εικόνες.



Εικόνα 17. Φυσικό Testbed



Εικόνα 18. Γενική τοπολογία του SCADA συστήματος που προσομοιώνεται

Για την καταγραφή την δικτυακής κίνησης χρησιμοποιήθηκε το tshark και έγινε καταγραφή σε αρχεία καταγραφής δικτυακής κίνησης τύπου .pcap, ξεχωριστά σε καθεμία από τις προσομοιούμενες συσκευές του δικτύου για κάθε επίθεση, που εκτελείται στο σύστημα. Στη συνέχεια από όλες τις δικτυακές καταγραφές έγινε απομόνωση μόνο των πακέτων IEC 60870-5-104, καθώς η ανάλυση αφορά μόνο τα πακέτα αυτού του πρωτοκόλλου.

Μετά τη συγκέντρωση των δικτυακών καταγραφών IEC 60870-5-104, για την ανάλυσή τους και την εξαγωγή χαρακτηριστικών σε επίπεδο δικτυακών ροών του πρωτοκόλλου, χρησιμοποιήθηκε πρόγραμμα ανάλυσης γραμμένο σε γλώσσα προγραμματισμού python3, το οποίο αναπτύχθηκε στα πλαίσια της διπλωματικής. Το εν λόγω πρόγραμμα κάνει χρήση της python3 βιβλιοθήκης scapy 2.4.3 για την ανίχνευση των διαφορετικών τύπων μηνυμάτων IEC 60870-5-104 (i-frame, u-frame, s-frame) και των πεδίων τους. Αντίστοιχη διαδικασία ανάλυσης της δικτυακής κίνησης και εξαγωγής χαρακτηριστικών επιπέδου δικτυακών ροών πραγματοποιήθηκε και με το λογισμικό CICFlowMeter.

5.1.1 Επεξήγηση κώδικα ανάλυσης αρχείων δικτυακών καταγραφών

Πιο αναλυτικά, το πρόγραμμα ανάλυσης που αναπτύχθηκε λαμβάνει ως είσοδο από το χρήστη ένα αρχείο δικτυακής καταγραφής (.pcap), μία παράμετρο threshold, σύμφωνα με την οποία υπολογίζεται ο χρόνος κατά τον οποίο μια δικτυακή ροή είναι ενεργή ή ανενεργή, μία παράμετρο flow_timeout, η οποία ορίζει τη μέγιστη δυνατή διάρκεια μίας ροής και τέλος μία παράμετρο attack_label στην οποία για στις ετικέτες των δικτυακών ροών ορίζεται η τιμή 'NoLabel'.

Κατά την εκτέλεση του προγράμματος γίνεται διάκριση των δικτυακών ροών, σύμφωνα με τον ορισμό των δικτυακών ροών που έχει δοθεί παραπάνω. Οι δικτυακές ροές, που θα βρεθούν, συγκεντρώνονται σε μία λίστα.

Μετά τη διάκριση των δικτυακών ροών ακολουθεί ο υπολογισμός των χαρακτηριστικών των δικτυακών ροών, τα οποία σχετίζονται με :

- Το IAT, δηλαδή το χρόνο που μεσολαβεί μεταξύ δύο διαδοχικών πακέτων που ανήκουν στην ίδια δικτυακή ροή IEC 60870-5-104.
- Τους active και idle χρόνους μίας δικτυακής ροής, δηλαδή τον έλεγχο των IAT κάθε δικτυακής ροής με βάση την τιμή threshold, που έχει δοθεί από τον χρήστη. Σε περίπτωση που το IAT δύο διαδοχικών πακέτων μίας δικτυακής ροής υπερβαίνει την τιμή threshold, η ροή είναι αδρανής για τον χρόνο αυτό.
- Τα χαρακτηριστικά επιπέδου TCP των πακέτων μίας δικτυακής ροής, δηλαδή τα στοιχεία σχετικά με τις σημαίες TCP και το μέγεθος του παραθύρου TCP.

- Τα χαρακτηριστικά επιπέδου IEC 60870-5-104 των πακέτων μίας δικτυακής ροής σχετικά με το COT και στοιχεία σχετικά με πεδία των διαφορετικών τύπων IEC 60870-5-104 πλαισίων.

Το σύνολο των στοιχείων για όλες τις δικτυακές ροές που έχουν ανιχνευθεί αποθηκεύεται σε ένα αρχείο .csv. Τα εξαγόμενα στοιχεία παρουσιάζονται σε σχετικό πίνακα στο Παράρτημα.

5.2 Σύνολο Δεδομένων Εισβολών στο πρωτόκολλο IEC 60870-5-104

Το σύνολο δεδομένων που συγκεντρώθηκε περιλαμβάνει δεδομένα δικτυακής κίνησης κατά τη διάρκεια επιθέσεων MITM και επιθέσεων τύπου Command Injecton. Στις παρακάτω ενότητες αναλύονται τόσο η φυσιολογική επικοινωνία μεταξύ του MTU και των PLC αλλά και οι επιθέσεις που εκτελέστηκαν. Τα ονόματα και τα χαρακτηριστικά των επιθέσεων εμφανίζονται στον παρακάτω πίνακα.

Attack label	Iec 104 message intervals (seconds)	Attack dutation	Attack topology
m_sp_na_1_DoS	0	3h	1 HMI 7 Field Devices
c_ci_na_1	[20,60]	3.5h	1 HMI 7 Field Devices 3 Attackers
c_ci_na_1_DoS	0	3.5h	1 HMI 7 Field Devices 3 Attackers
c_se_na_1	[20,60]	4h	1 HMI 7 Field Devices 3 Attackers
c_se_na_1_DoS	0	4h	1 HMI 7 Field Devices 3 Attackers

c_sc_na_1	[20,60]	4h	1 HMI 7 Field Devices 3 Attackers
c_sc_na_1_DoS	0	4h	1 HMI 7 Field Devices 3 Attackers
c_rd_na_1	[20,60]	5h	1 HMI 7 Field Devices 3 Attackers
c_rd_na_1_DoS	0	5h	1 HMI 7 Field Devices 3 Attackers
c_rp_na_1	[20,60]	5h	1 HMI 7 Field Devices 3 Attackers
c_rp_na_1_DoS	0	5h	1 HMI 7 Field Devices 3 Attackers
mitm_drop	0	5h	1 HMI 7 Field Devices 3 Attackers

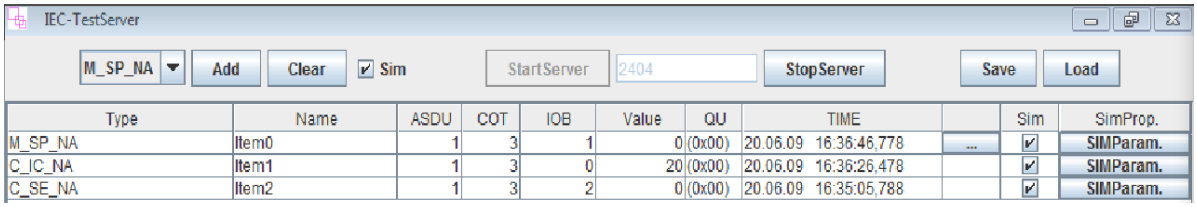
Εικόνα 19. Ετικέτες και χαρακτηριστικά επιθέσεων που εκτελέστηκαν

5.2.1 Φυσιολογική Επικοινωνία πρωτοκόλλου IEC 60870-5-104

Προτεραιότητα για τη ρεαλιστική προσομοίωση ενός συστήματος SCADA, το οποίο πλήττεται από επιθέσεις, αποτελεί ο ορισμός της φυσιολογικής επικοινωνίας μεταξύ ενός υποσταθμού και ενός IEC 60870-5-104 Client.

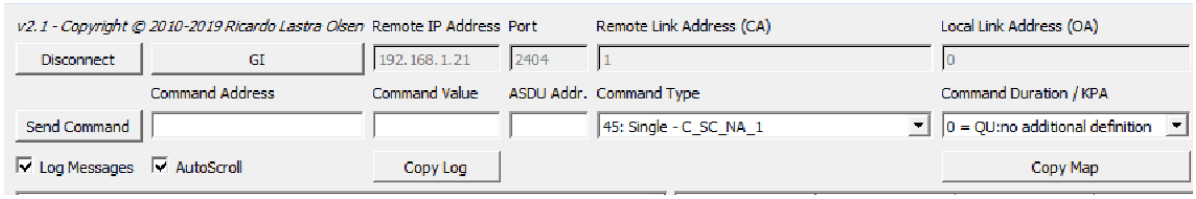
Στην περίπτωση του συστήματος, το οποίο προσομοιώνεται στα πλαίσια αυτής της διπλωματικής εργασίας, ως υποσταθμοί εννοούνται οι εικονικές μηχανές με εγκατεστημένο το λογισμικό IECServer. Σε αυτές τις εικονικές μηχανές εκκινείται ένας server IEC 60870-5-104 στη θύρα 2404 και για την συνεχή ροή δεδομένων στο εσωτερικό δίκτυο γίνεται ενεργοποίηση της επιλογής λειτουργίας προσομοίωσης του λογισμικού και προσθέτονται δύο IEC 60870-5-104 πεδία, ένα για τον ASDU TypeID M_SP_NA_1, στο οποίο στις παραμέτρους προσομοίωσης, το διάστημα στο οποίο αλλάζει η τιμή ορίζεται σε 50 δευτερόλεπτα, και ένα

για τον ASDU TypeID C_IC_NA_1. Για τις επιθέσεις γίνεται επιπλέον προσθήκη ενός ή τριών IEC 60870-5-104 πεδίων, αναλογα με την επίθεση, έτσι ώστε το λογισμικό IECServer να μπορεί να επιστρέψει απαντήσεις για τους διαφορετικούς τύπους μηνυμάτων που αποστέλλονται. Στην παρακάτω εικόνα φαίνεται η παραμετροποίηση του IECServer για την επίθεση τύπου C_SE_NA_1, η οποία παρουσιαζεται αναλυτικά παρακάτω.



Εικόνα 20. Παράμετροι που ορίζονται στο λογισμικό IECServer για τη φυσιολογική επικοινωνία

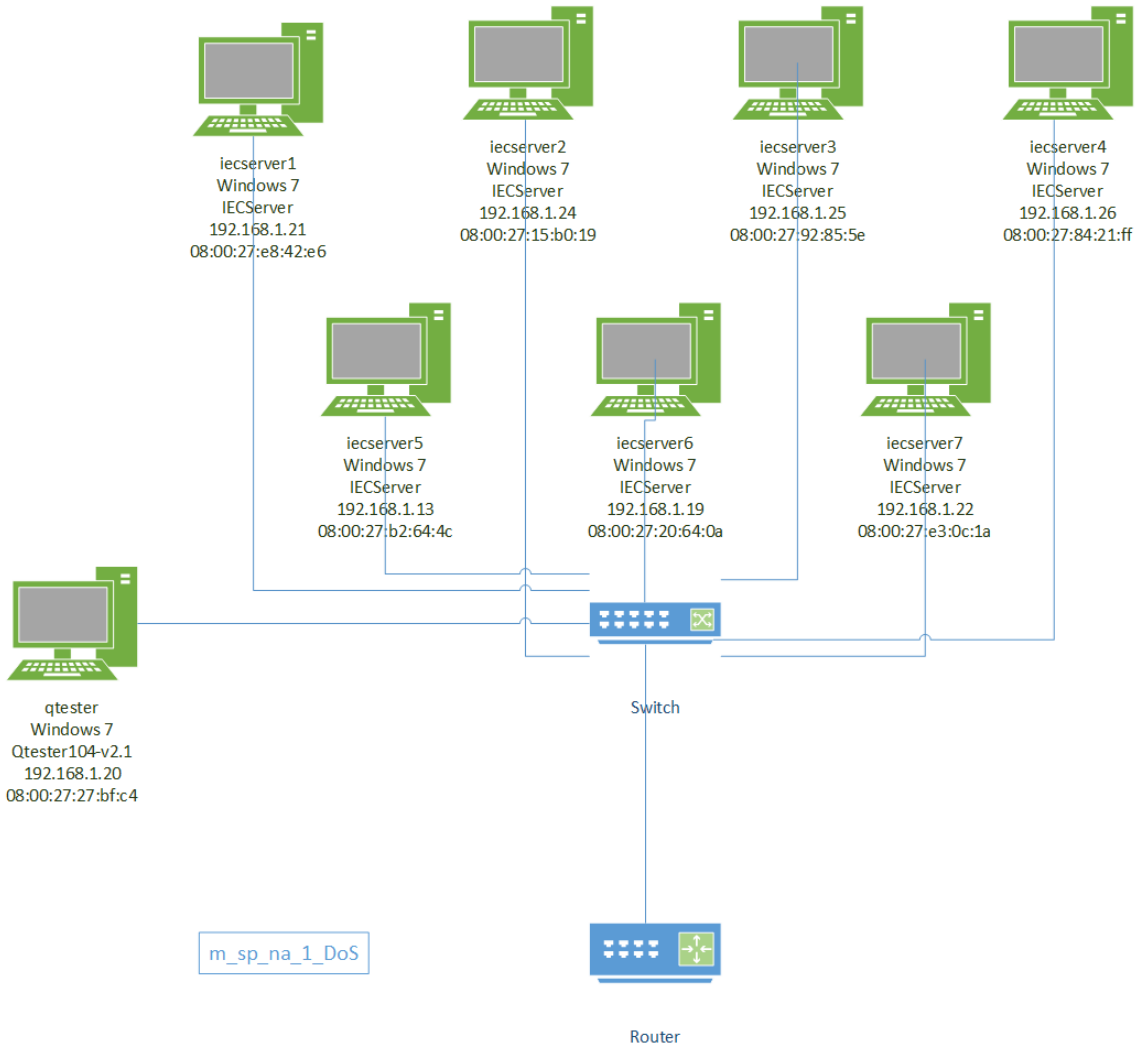
Το ρόλο του IEC 60870-5-104 Client διαδραματίζει η εικονική μηχανή, στην οποία είναι εγκατεστημένο το λογισμικό Qtester104. Για την εγκαθίδρυση επικοινωνίας με τον υποσταθμό απαιτείται η αλλαγή των ρυθμίσεων σύμφωνα με τις ρυθμίσεις του υποσταθμού. Με την εγκαθίδρυση της επικοινωνίας γίνεται αποστολή IEC 60870-5-104 C_IC_NA_1 μηνύματος κάθε 330 δευτερόλεπτα, χρόνος προκαθορισμένος από το χρησιμοποιούμενο λογισμικό. Μετά την επιτυχή σύνδεση με τον υποσταθμό στο πλαίσιο του Qtester104 που φαίνεται στην παρακάτω εικόνα παρουσιάζονται τα δεδομένα επικοινωνίας μεταξύ των συσκευών.



Εικόνα 21. Παράμετροι που ορίζονται στο λογισμικό QTester104 για τη φυσιολογική επικοινωνία

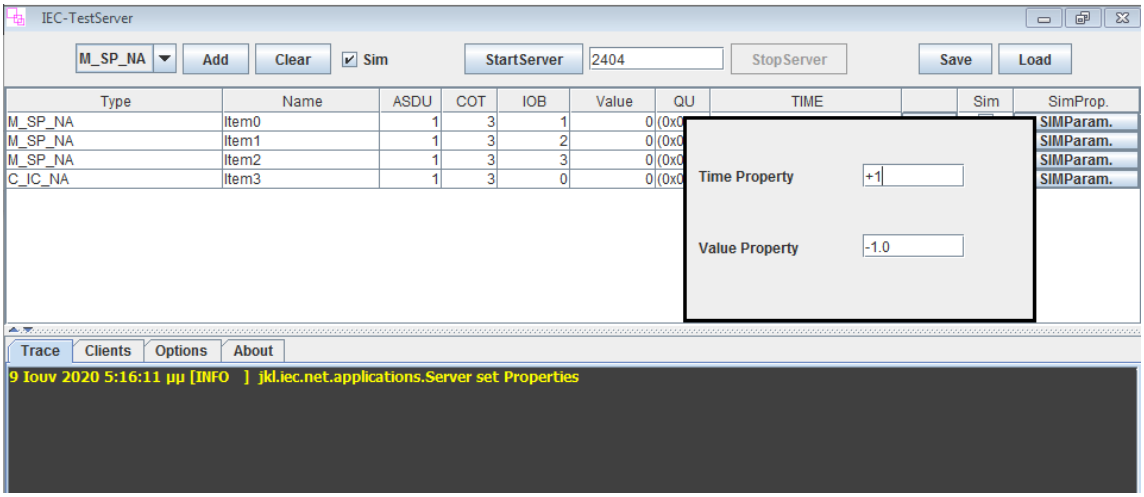
5.2.2 Επίθεση κορεσμού μηνυμάτων IEC 60870-5-104

Στην επίθεση αυτή γίνεται η υπόθεση ότι οι επιτιθέμενοι έχουν αποκτήσει τον έλεγχο των υποσταθμών του συστήματος, άρα δεν υπάρχει φυσιολογική κίνηση. Η τοπολογία που χρησιμοποιήθηκε για την επίθεση αυτή παρουσιάζεται στο παρακάτω σχήμα.



Εικόνα 22. Τοπολογία επίθεσης κορεσμού μηνυμάτων IEC 60870-5-104

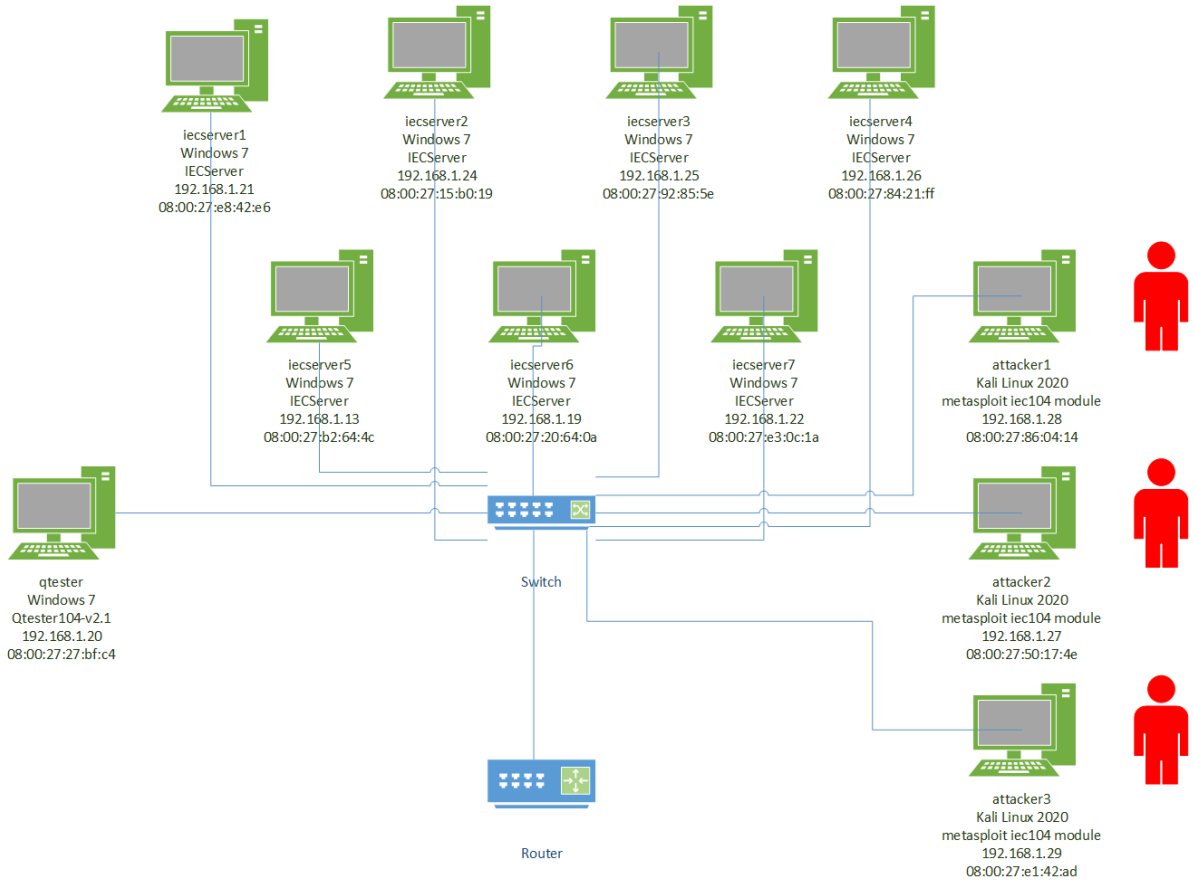
Το σύνολο των υποσταθμών του συστήματος έχουν ρυθμιστεί ώστε να αποστέλλουν μηνύματα M_SP_NA_1 κάθε δευτερόλεπτο, με στόχο οι συσκευές να μην μπορούν να διαχειριστούν τον αυξημένο ρυθμό μεταδιδόμενων μηνυμάτων, όπως περιγράφεται στο [16]. Στην παρακάτω εικόνα εμφανίζεται ο προσδιορισμός των παραμέτρων προσομοίωσης στο λογισμικό IECServer.



Εικόνα 23. Ρυθμίσεις παραμέτρων προσομοίωσης στο IECServer λογισμικό, για την επίθεση κορεσμού μηνυμάτων IEC 60870-5-104

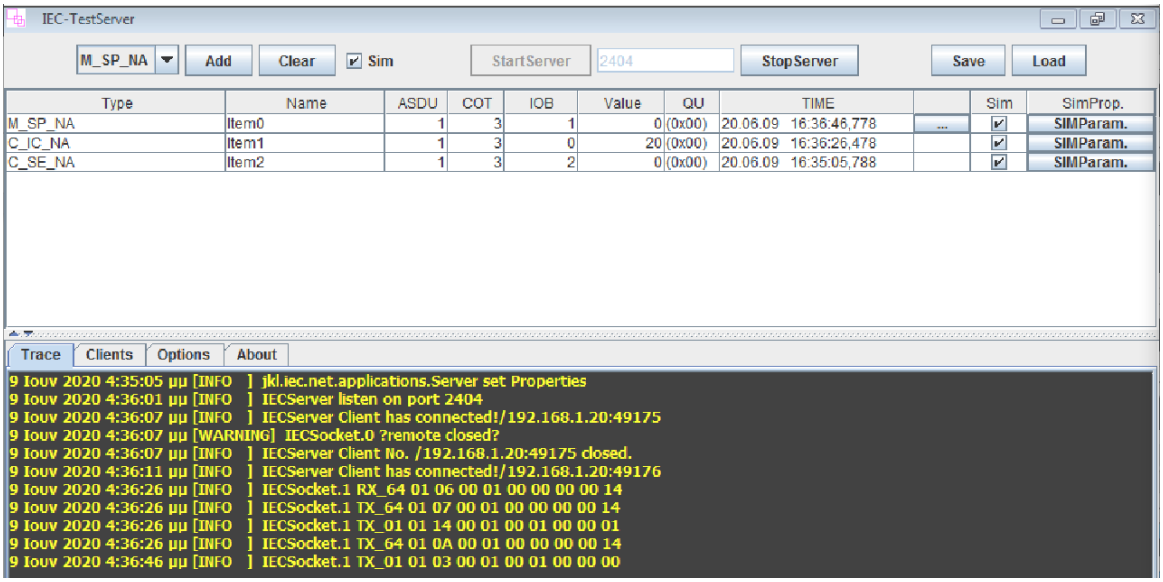
5.2.3 Αποστολή εντολών πρωτοκόλλου IEC 60870-5-104 από μη εξουσιοδοτημένους χρήστες

Οι αδυναμίες του πρωτοκόλλου, που έχουν αναλυθεί σε προηγούμενες ενότητες κάνουν δυνατή μια τέτοια επίθεση. Με χρήση κάποιων bash script, που χρησιμοποιούν τη μονάδα αποστολής μηνυμάτων IEC 60870-5-104 του λογισμικού Metsploit, τα οποία γράφηκαν ειδικά για την υπάρχουσα τοπολογία, γίνεται περιοδική αποστολή εντολών ελέγχου (Counter interrogation command (C_CI_NA_1), Read command (C_RD_NA_1), Reset process command (C_RP_NA_1)), set-point command (Set-point command, normalized value without time tag (C_SE_NA_1)) και Single Command (Single command without time tag (C_SC_NA_1)). Για όλες τις παραπάνω επιθέσεις χρησιμοποιείται η ίδια τοπολογία, η οποία φαίνεται στο επόμενο σχήμα.

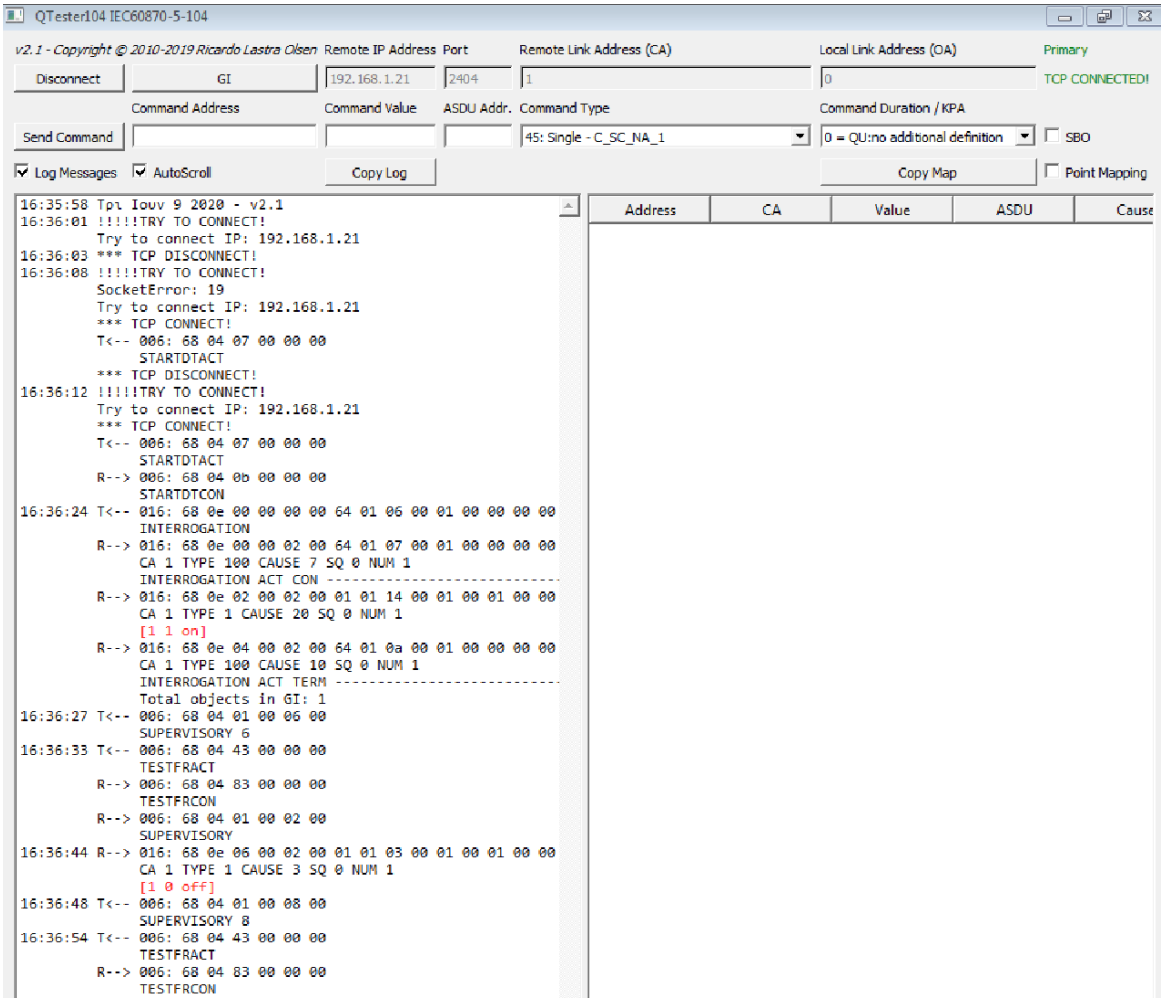


Εικόνα 24. Τοπολογία του συστήματος για τις command injection επιθέσεις

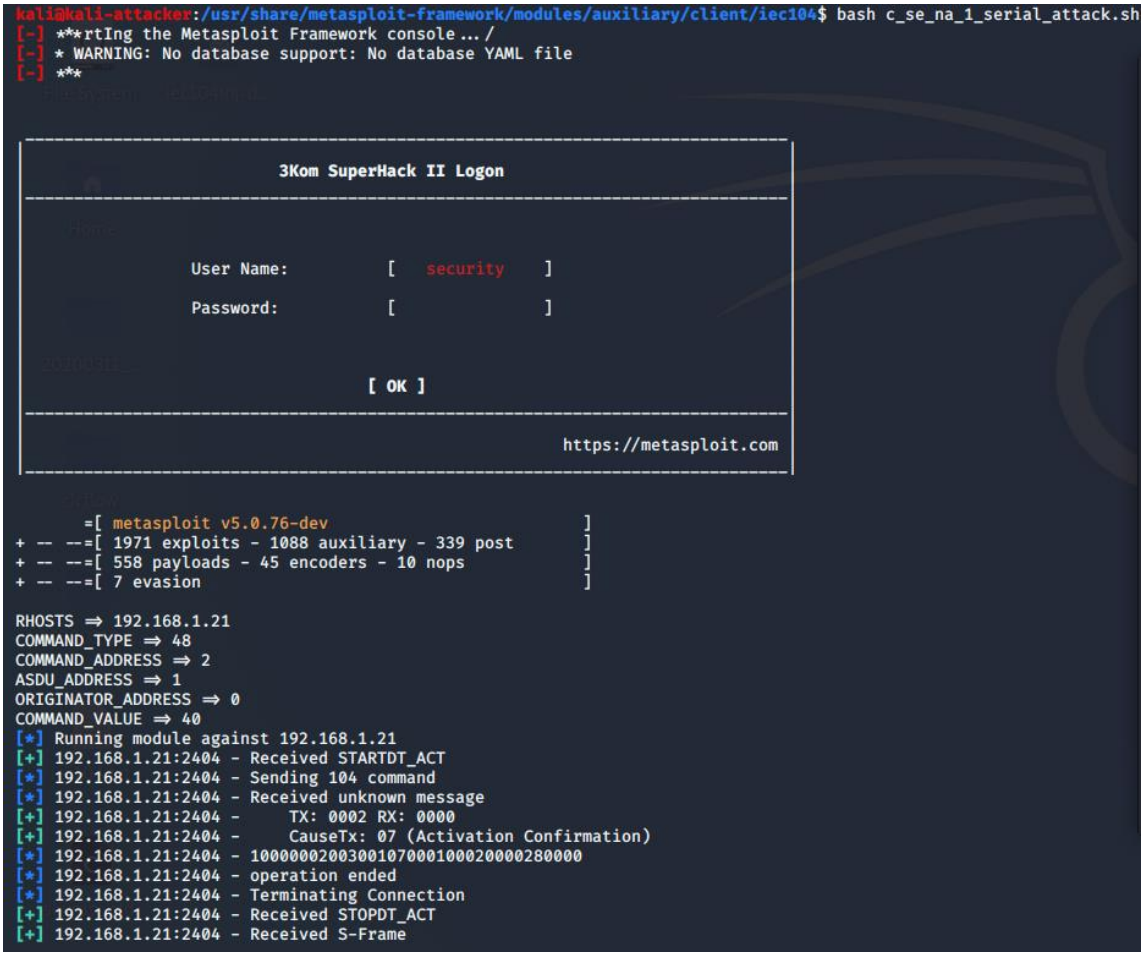
Για κάθε ένα διαφορετικό TypeID γίνονται δύο παραλλαγές της επίθεσης, μία κατά την οποία οι επιτιθέμενοι στέλνουν IEC 60870-5-104 μηνύματα κάθε 20 με 60 δευτερόλεπτα μετά το προηγούμενο απεσταλμένο IEC 60870-5-104 πακέτο, και μία, στην οποία γίνεται αποστολή μηνυμάτων συνεχόμενα. Για τις επιθέσεις αυτές η ρύθμιση των επιθέσεων είναι ίδια με την μόνη αλλαγή να είναι το TypeID και το διάστημα μεταξύ της αποστολής διαδοχικών πακέτων. Στις παρακάτω εικόνες παρουσιάζεται η διαδικασία εκτέλεσης της επίθεσης (C_SE_NA).



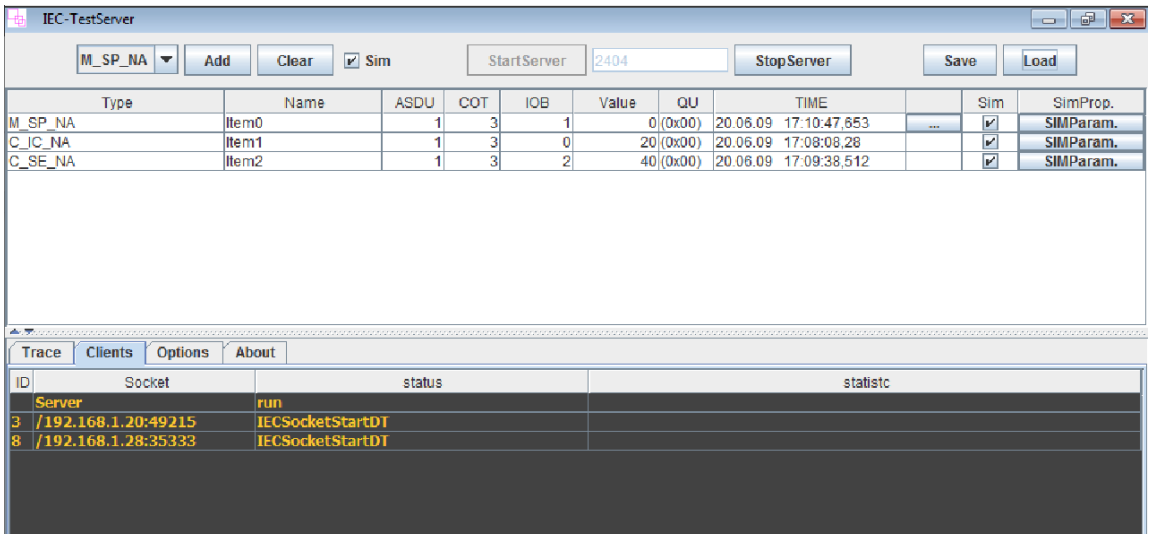
Εικόνα 25. Καταγραφόμενα δεδομένα επικοινωνίας από το λογισμικό IECServer κατά τη διάρκεια φυσιολογικής επικοινωνίας



Εικόνα 26. Καταγραφόμενα δεδομένα στο λογισμικό QTester104 κατά τη διάρκεια φυσιολογικής κίνησης



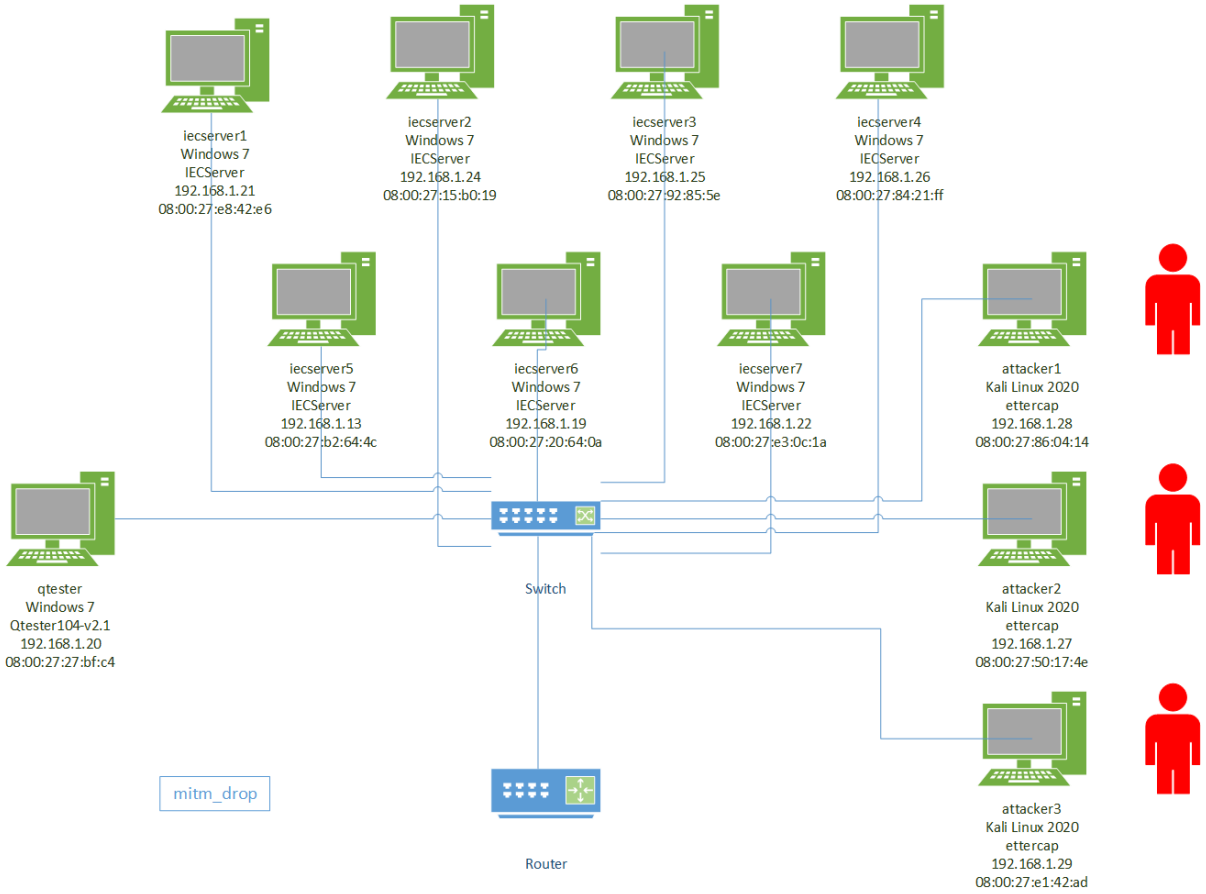
Εικόνα 27. Έκκίνηση ενός bash script από τη συσκευή του επιτιθέμενου, το οποίο κάνει χρήση του Metasploit IEC 104 module για τις επιθέσεις command injection



Εικόνα 28. Στις συνδεδεμένες συσκευές στο λογισμικό IECServer είναι ορατή η IP μίας εικονικής συσκευής επιτιθέμενου κατά τη διάρκεια των επιθέσεων command injection

5.2.4 Επίθεση Ανθρώπου Στη Μέση

Οι επιθέσεις MITM είναι ένας κοινός, αλλά αποτελεσματικός τύπος επίθεσης με πολλές παραλλαγές. Η MITM επίθεση, που εκτελέστηκε στην παρούσα διπλωματική, είχε ως στόχο την απομόνωση της IEC 60870-5-104 κίνησης των IECServer. Για την επίθεση αυτή χρησιμοποιήθηκε το λογισμικό Ettercap και δημιουργήθηκε ένα φίλτρο για το σκοπό αυτό. Η τοπολογία της επίθεσης, αλλά και τα βήματα που ακολουθήθηκαν για την εκτέλεσή της παρουσιάζονται στις παρακάτω εικόνες.



Εικόνα 29. Τοπολογία της επίθεσης MITM DROP

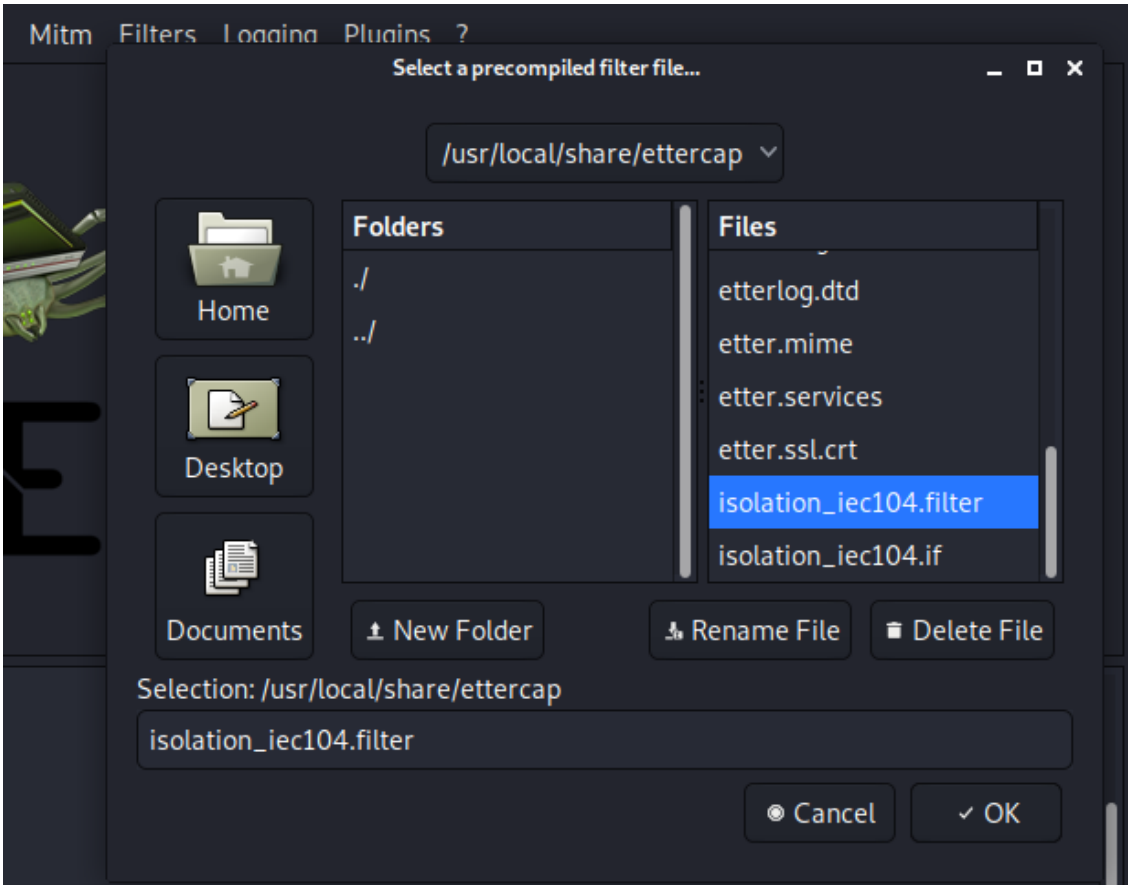
```
if ( ip.src == "192.168.1.21" || ip.src == "192.168.1.24" ) {
        if ( tcp.src == 2404 ) {
                drop()
        }
}
```

```
if ( ip.src == "192.168.1.25" || ip.src == "192.168.1.26" ) {
        if ( tcp.src == 2404 ) {
                drop()
        }
}
```

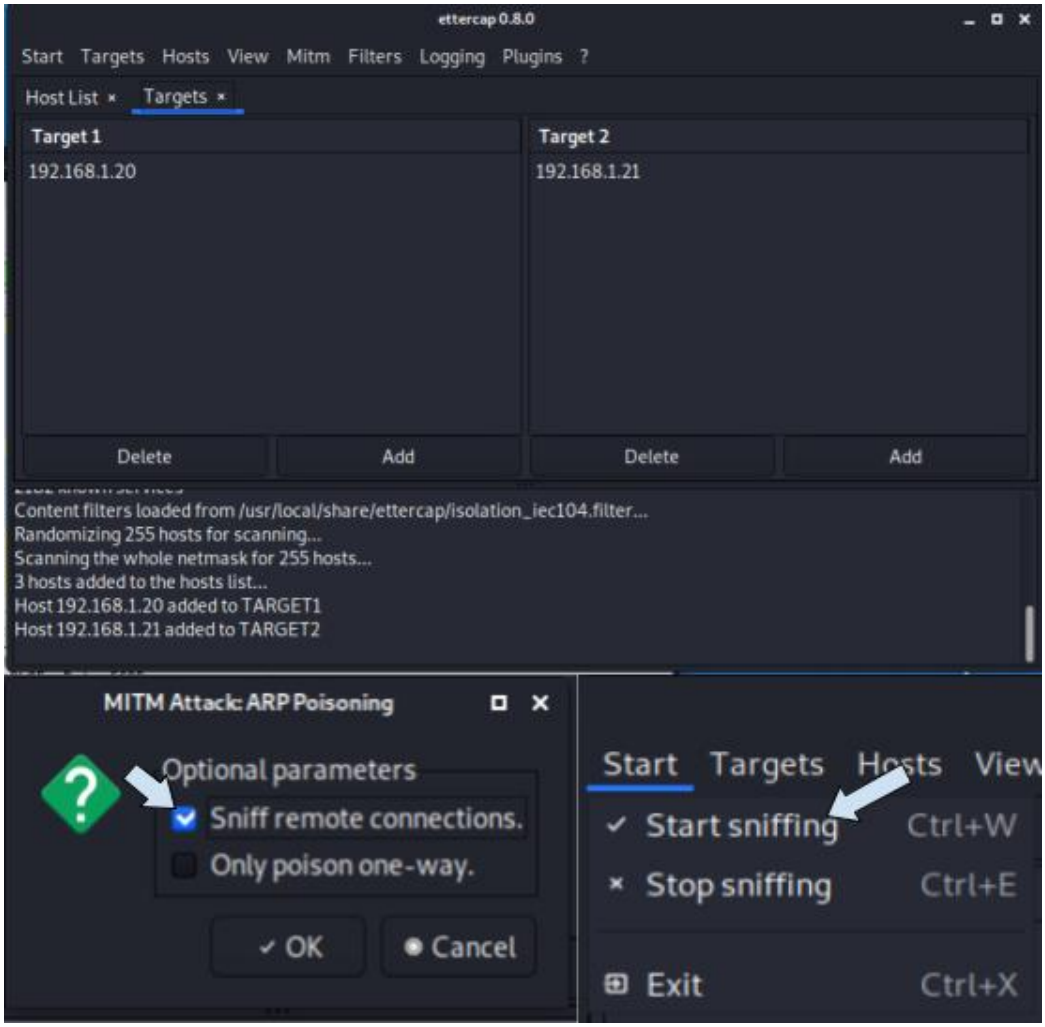
```
if ( ip.src == "192.168.1.19" || ip.src == "192.168.1.13" || ip.src == "192.168.1.22" ) {
       if ( tcp.src == 2404 ) {
               drop()
       }
}
```

Εικόνα 30. Ειδικά Ettercap script για την απομόνωση της δικτυακής κίνησης IEC 60870-5-104 από τις συσκευές IECServer

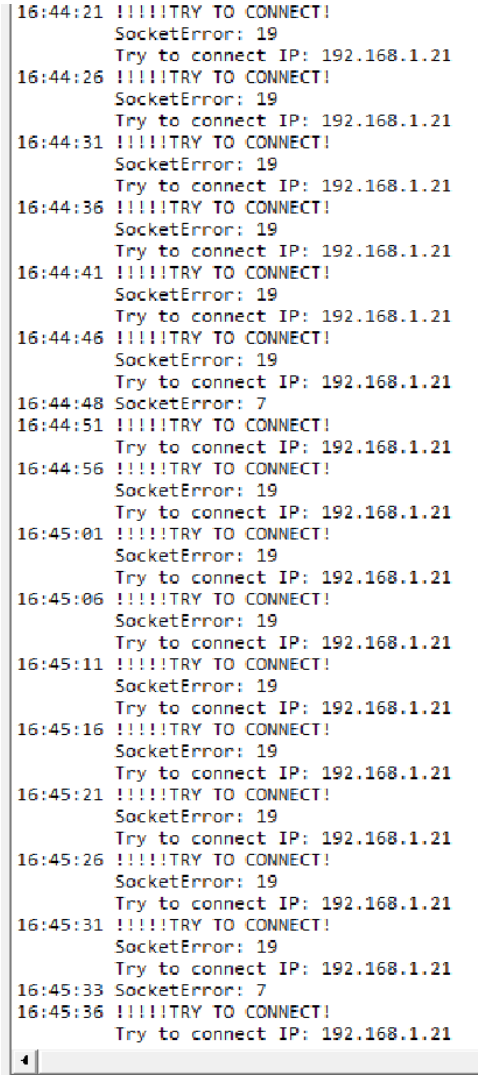
Εικόνα 31. Παραμετροποίηση του unified sniffing module του Ettercap



Εικόνα 32. Επιλογή του ειδικού Ettercap φίλτρου για την επίθεση MITM DROP



Εικόνα 33. Ανίχνευση IEC 60870-5-104 hosts και εκκίνηση της επίθεσης MITM DROP



Εικόνα 34. Εικόνα των καταγραφών του λογισμικού Qtester104 και εμφάνιση σφάλματος σύνδεσης λόγω της επίθεσης MITM DROP

5.2.5 Προεπεξεργασία συνόλου δεδομένων

Τα τελικά δεδομένα, τα οποία συγκεντρώθηκαν, περιλαμβάνουν δικτυακή κίνηση IEC 60870-5-104 από όλες τις συσκευές, ανάλογα με τις συσκευές που χρησιμοποιούνταν σε κάθε επίθεση. Στη συνέχεια, τα αρχεία δικτυακής κίνησης αναλύθηκαν με χρήση του προγράμματος εξαγωγής χαρακτηριστικών σε επίπεδο δικτυακών ροών σε μορφή .csv, το οποίο παρουσιάστηκε σε προηγούμενη ενότητα, αλλά και με το λογισμικό ανάλυσης σε επίπεδο δικτυακών ροών CICFlowMeter, το οποίο χρησιμοποιείται για ανίχνευση ανωμαλιών. Τέλος ορίστηκαν οι κατάλληλες ετικέτες για τις δικτυακές ροές των .csv αρχείων. Μια δικτυακή ροή ορίζεται ως φυσιολογική, με αντίστοιχη ετικέτα ‘NORMAL’, στην περίπτωση που δεν περιλαμβάνει ως source IP ή destination IP κάποια από τις IP των συσκευών, που επιτελούσαν το ρόλο του επιτιθέμενου στη συγκεκριμένη επίθεση.

5.3 Ανίχνευση εισβολών στο πρωτόκολλο IEC 60870-5-104

Τελικό αντικείμενο, με το οποίο ασχολείται η συγκεκριμένη διπλωματική, αποτελεί η χρήση των προαναφερθέντων δεδομένων, για την εκπαίδευση αλγορίθμων μηχανικής μάθησης με στόχο την κατηγοριοποίηση όλων των διαφορετικών κατηγοριών κίνησης που συλλέχθηκαν κατά τη διάρκεια των επιθέσεων που εκτελέστηκαν. Παρουσιάζεται ακόμα σύγκριση των αποτελεσμάτων δύο ομάδων μοντέλων μηχανικής μάθησης, εκ των οποίων η μία έχει εκπαιδευτεί με τα δεδομένα που εξήχθησαν από το πρόγραμμα ανάλυσης και εξαγωγής χαρακτηριστικών σε επίπεδο δικτυακών ροών που αναπτύχθηκε, και η άλλη με χρήση δεδομένων δικτυακών ροών, που εξήχθησαν με το λογισμικό CICFlowMeter.

Πιο συγκεκριμένα, για καθένα από τα σύνολα δεδομένων, που προέκυψαν με χρήση των παραπάνω λογισμικών, έχουν δημιουργηθεί δύο αρχεία για την εκπαίδευση των αλγορίθμων και την αξιολόγηση των προβλέψεών τους. Το πρώτο είναι το Training Set .csv αρχείο, το οποίο περιλαμβάνει 400 δικτυακές ροές κακόβουλης κίνησης και 400 δικτυακές ροές φυσιολογικής κίνησης για καθεμία από τις επιθέσεις αποστολής IEC 60870-5-104 εντολών από μη εξουσιοδοτημένους χρήστες, εκτός από την επίθεση M_SP_NA_1 κορεσμού μηνυμάτων, στην οποία, λόγω της απουσίας φυσιολογικής κίνησης, που έχει επεξηγηθεί παραπάνω, περιλαμβάνονται 400 δικτυακές ροές κακόβουλης κίνησης. Το δεύτερο αποτελεί ένα Testing Set .csv αρχείο, το οποίο περιλαμβάνει 169 δικτυακές ροές κακόβουλης κίνησης και 169 δικτυακές ροές φυσιολογικής κίνησης για καθεμία από τις επιθέσεις αποστολής IEC 60870-5-104 εντολών από μη εξουσιοδοτημένους χρήστες, εκτός από την επίθεση M_SP_NA_1 κορεσμού μηνυμάτων, στην οποία, λόγω της απουσίας φυσιολογικής κίνησης, που έχει επεξηγηθεί παραπάνω, περιλαμβάνονται 169 δικτυακές ροές κακόβουλης κίνησης.

Οι αλγόριθμοι μηχανικής μάθησης, που χρησιμοποιήθηκαν, έχουν επεξηγηθεί σε προηγούμενο κεφάλαιο και οι μετρικές, που χρησιμοποιήθηκαν για την αξιολόγηση των μοντέλων, είναι οι μετρικές precision, recall, F1-score και accuracy, που έχουν, επίσης, παρουσιαστεί σε προηγούμενη ενότητα. Έγινε χρήση των υλοποιήσεων των αλγορίθμων μηχανικής μάθησης που παρέχει η python3 βιβλιοθήκη scikit-learn 0.21 [46]. Η σύγκριση των αποτελεσμάτων για τα δύο σύνολα δεδομένων παρουσιάζεται στους παρακάτω πίνακες.

Classification Algorithms	Weighted average precision	Weighted average recall	Weighted average F1-score	accuracy
Random Forest	0,77	0,78	0,77	0,78
Decision Tree	0,75	0,76	0,75	0,76
KNN	0,66	0,66	0,66	0,66
Logistic Regression	0,66	0,68	0,66	0,68
MLPC	0,31	0,53	0,38	0,53
Naïve Bayes	0,57	0,6	0,53	0,6
Perceptron	0,54	0,57	0,53	0,57
SVM RBF	0,55	0,57	0,54	0,57

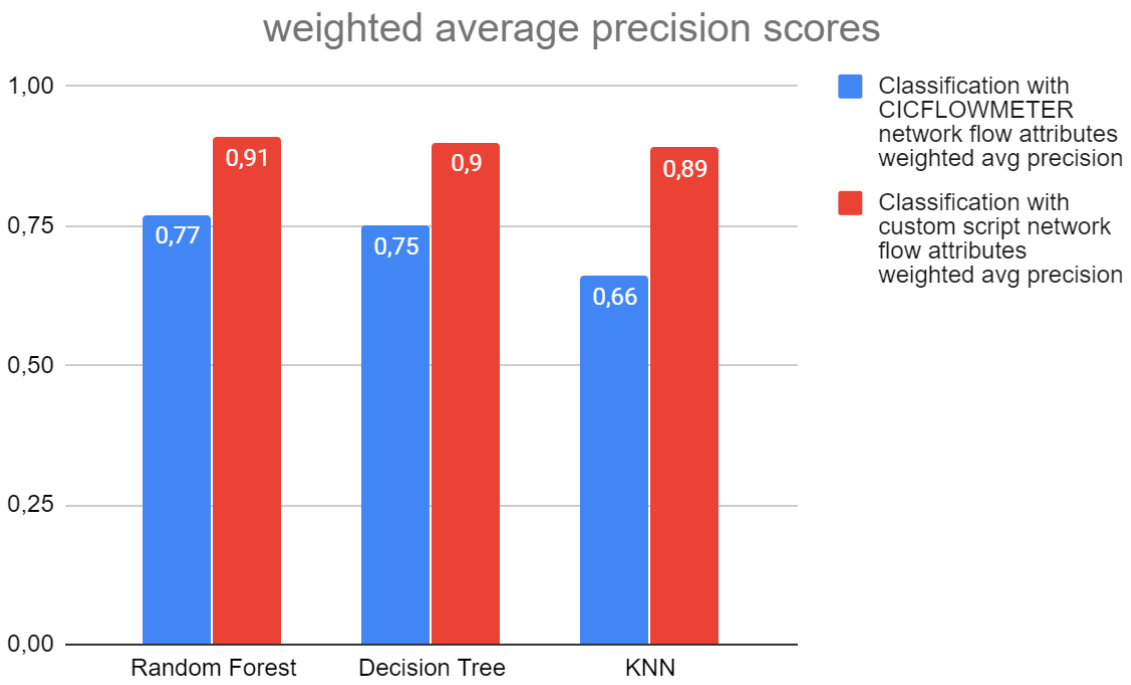
Εικόνα 35. Αποτελέσματα κατηγοριοποίησης με χρήση των δεδομένων δικτυακών ροών που εξήχθησαν με χρήση του CICFlowMeter

Classification Algorithms	Weighted average precision	Weighted average recall	Weighted average F1-score	Accuracy
Random Forest	0,91	0,92	0,91	0,92
Decision Tree	0,9	0,91	0,9	0,91
KNN	0,89	0,89	0,89	0,89
Logistic Regression	0,81	0,8	0,79	0,8
MLPC	0,79	0,78	0,77	0,78
Naïve Bayes	0,73	0,74	0,69	0,74
Perceptron	0,6	0,66	0,6	0,66
SVM RBF	0,64	0,6	0,57	0,6

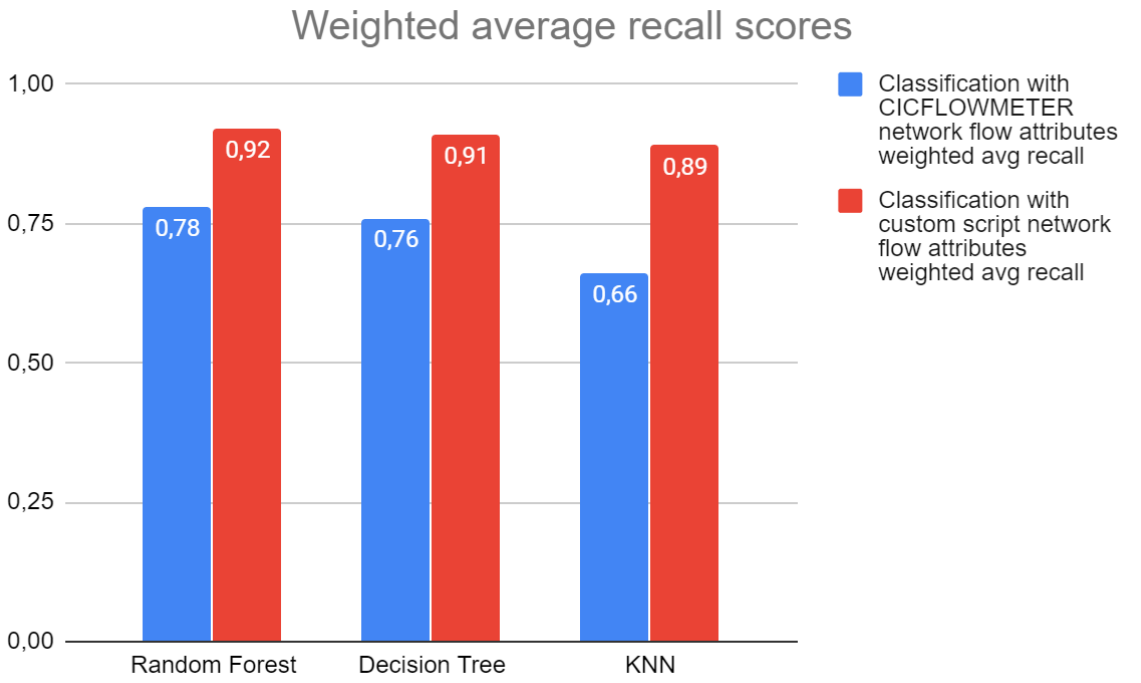
Εικόνα 36. Αποτελέσματα κατηγοριοποίησης με χρήση των δεδομένων δικτυακών ροών που εξήχθησαν με χρήση του προγράμματος ανάλυσης δικτυακής κίνησης που δημιουργήθηκε στα πλαίσια της διπλωματικής εργασίας

Με βάση τα αποτελέσματα που εικονίζονται στους παραπάνω πίνακες παρατηρούμε αυξημένη αξιοπιστία στις προβλέψεις σε όλους τους αλγορίθμους που εξετάστηκαν. Βασική μετρική αξιολόγησης των προβλέψεων των αλγορίθμων αποτελεί το F1-score, η τιμή του οποίου παρουσιάζεται κατά μέσο όρο μεγαλύτερη κατά 0,1575 στις προβλέψεις με τα

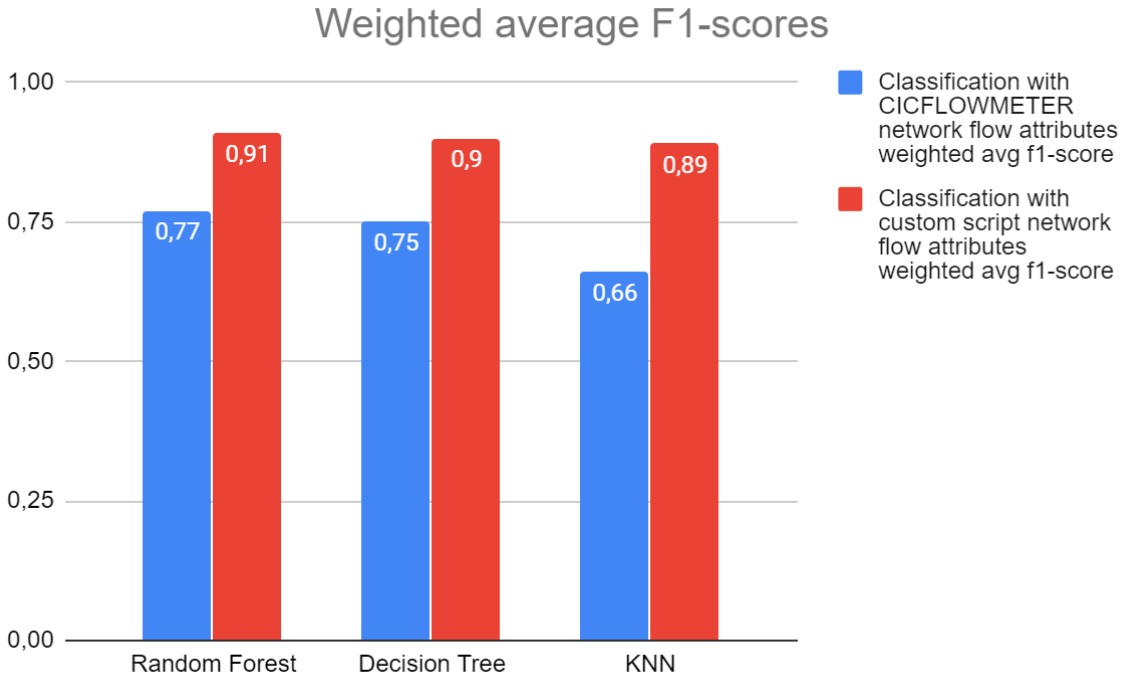
δεδομένα από το πρόγραμμα ανάλυσης που αναπτύχθηκε στην εργασία αυτή σε σχέση με τις προβλέψεις με τα δεδομένα από το λογισμικό CICFlowMeter. Καλύτερα αποτελέσματα παρουσιάζουν οι αλγόριθμοι Random Forest, Decision Tree, KNN με τις τιμές του F1-score στα δεδομένα του CICFlowMeter να είναι 77%, 75%, 66% αντίστοιχα και με βάση τα δεδομένα του προγράμματος που αναπτύχθηκε στα πλαίσια της εργασίας να είναι 91%, 90%, 89% αντίστοιχα. Τα αποτελέσματα αυτά εμφανίζονται στα παρακάτω γραφήματα.



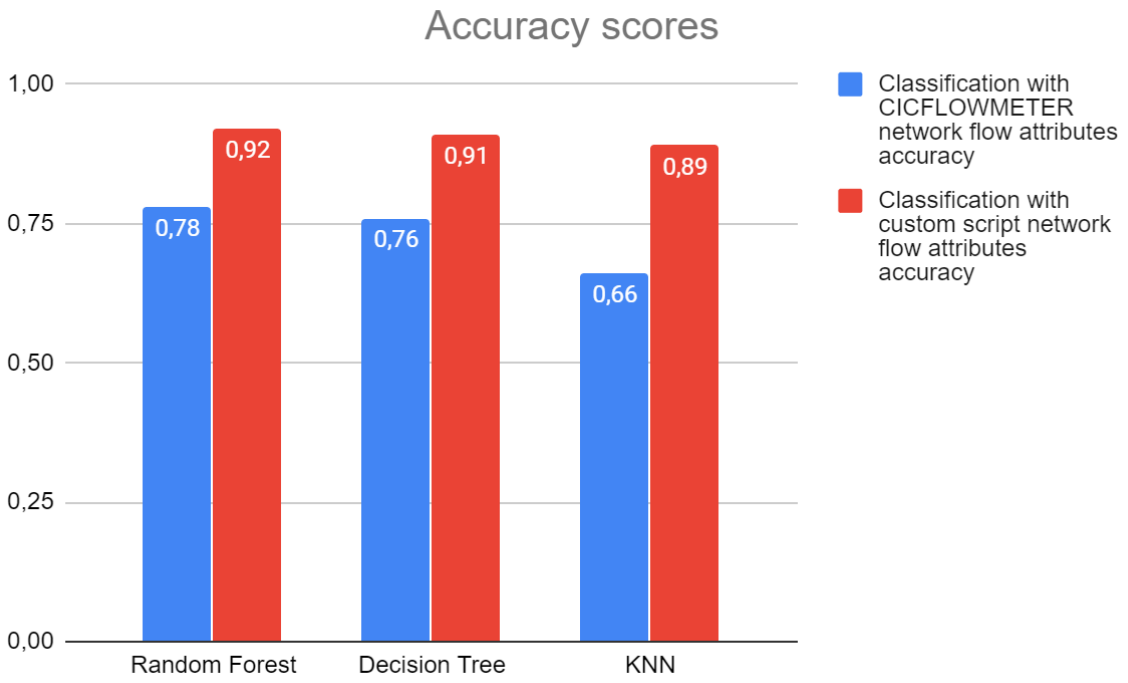
Εικόνα 37. Σύγκριση των τριών καλύτερων αποτελεσμάτων κατηγοριοποίησης με στοιχεία δικτυακών ροών που εξήχθησαν από το CICFlowMeter και το πρόγραμμα που αναπτύχθηκε στα πλαίσια της διπλωματικής εργασίας, με βάση τη μετρική Weighted average precision



Εικόνα 38. Σύγκριση των τριών καλύτερων αποτελεσμάτων κατηγοριοποίησης με στοιχεία δικτυακών ροών που εξήχθησαν από το CICFlowMeter και το πρόγραμμα που αναπτύχθηκε στα πλαίσια της διπλωματικής εργασίας, με βάση τη μετρική Weighted average recall



Εικόνα 39. Σύγκριση των τριών καλύτερων αποτελεσμάτων κατηγοριοποίησης με στοιχεία δικτυακών ροών που εξήχθησαν από το CICFlowMeter και το πρόγραμμα που αναπτύχθηκε στα πλαίσια της διπλωματικής εργασίας, με βάση τη μετρική Weighted average F1-score



Εικόνα 40. Σύγκριση των τριών καλύτερων αποτελεσμάτων κατηγοριοποίησης με στοιχεία δικτυακών ροών που εξήχθησαν από το CICFlowMeter και το πρόγραμμα που αναπτύχθηκε στα πλαίσια της διπλωματικής εργασίας, με βάση τη μετρική accuracy

6. Συμπεράσματα και Μελλοντικές Επεκτάσεις

Η αύξηση των περιστατικών διατάραξης της φυσιολογικής λειτουργίας κρίσιμων υποδομών από κυβερνοεπιθέσεις τα τελευταία χρόνια έχει φέρει το θέμα της προστασίας των βιομηχανικών δικτύων από εσωτερικές και εξωτερικές απειλές στο ερευνητικό προσκήνιο. Η αναγκαιότητα εύρεσης λύσεων για την προστασία βιομηχανικών συστημάτων, όπως είναι τα συστήματα SCADA και τα ICS, γίνεται κατανοητή, εάν αναλογιστεί κανείς ότι αρκετές πτυχές της καθημερινής ζωής επηρεάζονται σε περίπτωση δυσλειτουργίας τους. Έχουν προταθεί ποικίλες λύσεις για την ανίχνευση κυβερνοεπιθέσεων σε τέτοιες εγκαταστάσεις, οι οποίες στην πλειοψηφία τους χρησιμοποιούν στοιχεία σε επίπεδο πακέτων για την ανίχνευση των εισβολών. Τα τελευταία χρόνια έχει παρατηρηθεί αύξηση της χρήσης στοιχείων επιπέδου δικτυακών ροών σε IDS.

Στα πλαίσια της διπλωματικής εργασίας έγινε μελέτη της δομής και λειτουργίας των συστημάτων SCADA, του βιομηχανικού πρωτοκόλλου επικοινωνίας IEC 60870-5-104, διαφόρων τύπων και μοντέλων ανίχνευσης εισβολών και διαφόρων αλγορίθμων μηχανικής μάθησης με στόχο την δημιουργία ενός IDS με εφαρμογή αλγορίθμων μηχανικής μάθησης σε χαρακτηριστικά δικτυακών ροών και αξιολόγηση της εμπιστοσύνης των προβλέψεών του με χρήση δεδομένων, τα οποία παράχθηκαν για το σκοπό αυτό από μία προσομοίωση ενός συστήματος SCADA, εναντίον του οποίου εκτελέστηκαν διαφορετικοί τύποι επιθέσεων. Τα δεδομένα που καταγράφηκαν υπέστησαν επεξεργασία με δύο διαφορετικούς τρόπους, με χρήση του λογισμικού CICFlowMeter αλλά και ενός προγράμματος ανάλυσης δικτυακής κίνησης και εξαγωγής χαρακτηριστικών δικτυακών ροών, που κατασκευάστηκε στα πλαίσια της εργασίας και, χρησιμοποιήθηκαν για την εκπαίδευση και αξιολόγηση αλγορίθμων μηχανικής μάθησης για την κατηγοριοποίηση των διαφορετικών τύπων επιθέσεων. Τα σημαντικά καλύτερα αποτελέσματα με χρήση δεδομένων επεξεργασμένων από το πρόγραμμα ανάλυσης δικτυακής κίνησης που αναπτύχθηκε στα πλαίσια της εργασίας είναι πολλά υποσχόμενα. Καλύτερα αποτελέσματα παρουσιάζουν οι αλγόριθμοι Random Forest, Decision Tree, KNN με αποτελέσματα F1-score στα δεδομένα του CICFlowMeter να είναι 77%, 75%, 66% αντίστοιχα, και με βάση τα δεδομένα του προγράμματος που αναπτύχθηκε στα πλαίσια της εργασίας να είναι 91%, 90%, 89% αντίστοιχα. Η διαφορά αυτή στα αποτελέσματα μπορεί να αποδοθεί στο γεγονός ότι τα χαρακτηριστικά δικτυακών ροών που εξάγονται με το πρόγραμμα που αναπτύχθηκε περιλαμβάνουν χαρακτηριστικά σε επίπεδο του πρωτοκόλλου IEC 60870-5-104, οδηγώντας σε καλύτερη κατηγοριοποίηση επιθέσεων που στοχεύονται στα κενά ασφαλείας του πρωτοκόλλου αυτού.

Το σύστημα ανίχνευσης εισβολών που αναπτύχθηκε αποτελεί μια καλή βάση για μελλοντική εξέλιξη. Πιθανή επέκταση της εφαρμογής θα μπορούσε να αποτελέσει η αναζήτηση και δοκιμή άλλων αλγορίθμων μηχανικής μάθησης ή και αλγορίθμων νευρωνικών δικτύων για βελτίωση της ακρίβειας της κατηγοριοποίησης διαφορετικών τύπων επιθέσεων. Θα μπορούσε επίσης να γίνει επέκταση του υπάρχοντος συστήματος για την ανίχνευση ανωμαλιών σε περισσότερα βιομηχανικά πρωτόκολλα, όπως Modbus ή DNP3, με χρήση στοιχείων δικτυακών ροών των πρωτοκόλλων αυτών. Άλλη μια πιθανή βελτίωση του υπάρχοντος συστήματος, σχετικά, με την εξαγωγή των στοιχείων δικτυακών ροών, αποτελεί και η επέκταση των εξαγόμενων στοιχείων, ώστε να μπορούν να βρεθούν περισσότερες συσχετίσεις στα δεδομένα δικτυακών καταγραφών που αναλύονται. Θα μπορούσε, ακόμα, να αναπτυχθεί ένα δεύτερο επίπεδο ανάλυσης δεδομένων με χρήση βαθιάς ανίχνευσης πακέτων, το οποίο να ενσωματωθεί στο υπάρχον σύστημα, για καλύτερη ανίχνευση εισβολών. Τέλος θα μπορούσε να ενσωματωθεί το υπάρχον σύστημα σε έναν Honeypot Manager και με κριτήριο τις προβλέψεις σχετικά με τις εισερχόμενες ροές να παρατάσσει Παγίδες Εισβολών (Honeypots) σε σωστές μορφολογικά σωστές.

Βιβλιογραφία

[1] "IEEE Spectrum: Technology, Engineering, and Science News," [Online]. Available: https://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet. [Accessed 25 June 2020].

[2] D. E. Whitehead, K. Owens, D. Gammel and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in *2017 70th Annual Conference for Protective Relay Engineers (CPRE)*, 2017, pp. 1-8.

[3] S. N. Shirazi, A. Gouglidis, K. N. Syeda, S. Simpson, A. Mauthe, I. M. Stephanakis and D. Hutchison, "Evaluation of anomaly detection techniques for scada communication resilience," in *2016 Resilience Week (RWS)*, 2016, pp. 140-145.

[4] S. Ghosh and S. Sampalli, "A survey of security in SCADA networks: Current issues and future challenges," *IEEE Access,* vol. 7, pp. 135812-135831, 2019.

[5] S. Samtani, S. Yu, H. Zhu, M. Patton and H. Chen, "Identifying SCADA vulnerabilities using passive and active vulnerability assessment techniques," in *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 2016, pp. 25-30.

[6] W. Clinton, "Executive order 13010, establishing the president's commission on critical infrastructure protection (PCCIP)," *US Government Printing Office, Washington, DC,* 1996.

[7] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, E. G. Im, Z. Yao, B. Pranggono and H. Wang, "Man-in-the-middle attack test-bed investigating cyber-security vulnerabilities in smart grid SCADA systems," IET, 2012.

[8] H. A. Abbas, "Future SCADA challenges and the promising solution: the agent-based SCADA," *International journal of critical infrastructures,* vol. 10, pp. 307-333, 2014.

[9] D. Pliatsios, P. Sarigiannidis, T. Lagkas and A. G. Sarigiannidis, "A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics," *IEEE Communications Surveys & Tutorials,* 2020.

[10] S. Tamboli, M. Rawale, R. Thoraiet and S. Agashe, "Implementation of Modbus RTU and Modbus TCP communication using Siemens S7-1200 PLC for batch process," in *2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)*, 2015, pp. 258-263.

[11] D. Pliatsios, P. Sarigiannidis, T. Liatifis, K. Rompolos and I. Siniosoglou, “A Novel and Interactive Industrial Control System Honeypot for Critical Smart Grid Infrastructure,” in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1-6.

[12] I. N. Fovino, Carcano, rea, M. Masera and A. Trombetta, “Design and implementation of a secure modbus protocol,” in *International conference on critical infrastructure protection*, 2009, pp. 83-96.

[13] A. Richard and P. Appiah-Kubi, “Design and performance of a split protocol architecture on Distributed Network Protocol 3 (DNP3),” in *2017 IEEE International Conference on Electro Information Technology (EIT)*, 2017, pp. 249-253.

[14] G. Clarke, D. Reynders and E. Wright, Practical modern SCADA protocols: DNP3, 60870.5 and related systems, Newnes, 2004, pp. 249-253.

[15] I. Darwish, O. Igbe, O. Celebi, T. Saadawi and J. Soryal, “Smart grid DNP3 vulnerability analysis and experimentation,” in *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing*, 2015, pp. 141-147.

[16] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, B. Pranggono and H. Wang, “Intrusion detection system for IEC 60870-5-104 based SCADA networks,” in *2013 IEEE power \& energy society general meeting*, 2013, pp. 1-5.

[17] T. Teodorowicz, “Comparison of SCADA protocols and implementation of IEC 104 and MQTT in MOSAIK,” *University of Muenster, Muenster*, 2017.

[18] P. Radoglou-Grammatikis, P. Sarigiannidis, I. Giannoulakis, E. Kafetzakis and E. Panaousis, “Attacking IEC-60870-5-104 SCADA Systems,” in *2019 IEEE World Congress on Services (SERVICES)*, 2019, pp. 41-46.

[19] Y. Xu, Y. Yang, T. Li, J. Ju and Q. Wang, “Review on cyber vulnerabilities of communication protocols in industrial control systems,” in *2017 IEEE Conference on Energy Internet and Energy System Integration (EI2)*, 2017, pp. 1-6.

[20] Q. S. Qassim, N. Jamil, M. Daud, N. Ja’affar, S. Yussof, R. Ismail and W. A. W. Kamarulzaman, “Simulating command injection attacks on iec 60870-5-104 protocol in scada system,” *International Journal of Engineering & Technology*, vol. 7, pp. 153-159, 2018.

[21] P. Maynard, K. McLaughlin and B. Haberler, "Towards understanding man-in-the-middle attacks on iec 60870-5-104 scada networks," in *2nd International Symposium for ICS & SCADA Cyber Security Research 2014 (ICS-CSR 2014) 2*, 2014, pp. 30-42.

[22] T. Fioreze, M. O. Wolbers, R. van de Meent and A. Pras, "Finding elephant flows for optical networks," in *2007 10th IFIP/IEEE International Symposium on Integrated Network Management*, 2007, pp. 627-640.

[23] D. Joo, T. Hong and I. Han, "The neural network models for IDS based on the asymmetric costs of false negative errors and false positive errors," *Expert Systems with Applications*, vol. 25, pp. 69-75, 2003.

[24] A. Lazarevic, V. Kumar and J. Srivastava, "Intrusion detection: A survey," in *Managing Cyber Threats*, 2005, pp. 19-78.

[25] R. Samdarshi, N. Sinha and P. Tripathi, "A triple layer intrusion detection system for SCADA security of electric utility," in *2015 Annual IEEE India Conference (INDICON)*, 2015, pp. 1-5.

[26] L. A. Maglaras and J. Jiang, "Intrusion detection in SCADA systems using machine learning techniques," in *2014 Science and Information Conference*, 2014, pp. 626-631.

[27] E. Hodo, S. Grebeniuk, H. Ruotsalainen and P. Tavolato, "Anomaly detection for simulated iec-60870-5-104 trafiic," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1-7.

[28] S. Shitharth and D. P. Winston, "A novel IDS technique to detect DDoS and sniffers in smart grid," in *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, 2016, pp. 1-6.

[29] A. Almalawi, A. Fahad, Z. Tari, A. Alamri, R. AlGhamdi and A. Y. Zomaya, "An efficient data-driven clustering technique to detect attacks in SCADA systems," *IEEE Transactions on Information Forensics and Security*, vol. 11, pp. 893-906, 2015.

[30] T. Cruz, L. Rosa, J. Proenca, L. Maglaras, M. Aubigny, L. Lev, J. Jiang and P. Simoes, "A cybersecurity detection framework for supervisory control and data acquisition systems," *IEEE Transactions on Industrial Informatics*, vol. 12, pp. 2236-2246, 2016.

[31] Y. Yang, K. McLaughlin, S. Sezer, Y. Yuan and W. Huang, "Stateful intrusion detection for IEC 60870-5-104 SCADA security," in *2014 IEEE PES General Meeting| Conference \& Exposition*, 2014, pp. 1-5.

[32] W. Yusheng, F. Kefeng, L. Yingxu, L. Zenghui, Z. Ruikang, Y. Xiangzhen and L. Lin, "Intrusion detection of industrial control system based on Modbus TCP protocol," in *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*, 2017, pp. 156-162.

[33] A. Almalawi, X. Yu, Z. Tari, A. Fahad and I. Khalil, "An unsupervised anomaly-based detection approach for integrity attacks on SCADA systems," *Computers \& Security*, vol. 46, pp. 94-110, 2014.

[34] I. Portugal, P. Alencar and D. Cowan, "The use of machine learning algorithms in recommender systems: A systematic review," *Expert Systems with Applications*, vol. 97, pp. 205-227, 2018.

[35] T. Pang-Ning, Introduction to data mining, Dorling Kindersley: Pearson, 2015.

[36] G. Stein, B. Chen, A. S. Wu and K. A. Hua, "Decision tree classifier for network intrusion detection with GA-based feature selection," in *Proceedings of the 43rd annual Southeast regional conference-Volume 2*, 2005, pp. 136-141.

[37] C. C. Aggarwal and C. Zhai, "A survey of text classification algorithms," in *Mining text data*, Springer, 2012, pp. 163-222.

[38] M. Tommiska, "Efficient digital implementation of the sigmoid function for reprogrammable logic," *IEE Proceedings-Computers and Digital Techniques*, vol. 150, pp. 403-411, 2003.

[39] I. Rish, "IJCAI 2001 workshop on empirical methods in artificial intelligence," *New York: IBM*, pp. 41-46, 2001.

[40] M. M. Saritas and A. Yasar, "Performance analysis of ANN and Naive Bayes classification algorithm for data classification," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 7, pp. 88-91, 2019.

[41] G. Dimitoglou, J. A. Adams and C. M. Jim, "Comparison of the C4. 5 and a Naive Bayes classifier for the prediction of lung cancer survivability," *arXiv preprint arXiv:1206.1121*, 2012.

[42] P. Maynard, K. McLaughlin and S. Sezer, "An Open Framework for Deploying Experimental SCADA Testbed Networks," in *5th International Symposium for ICS \& SCADA Cyber Security Research 2018 5*, 2018, pp. 92-101.

[43] G. Meena and R. R. Choudhary, “A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA,” in *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, 2017, pp. 553-558.

[44] T. Salman, D. Bhamare, A. Erbad, R. Jain and M. Samaka, “Machine learning for anomaly detection and categorization in multi-cloud environments,” in *2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud)*, 2017, pp. 97-103.

[45] S. Nalband, R. Sreekrishna and A. A. Prince, “Analysis of knee joint vibration signals using ensemble empirical mode decomposition,” *Procedia Computer Science*, vol. 89, pp. 820-827, 2016.

[46] A. Géron, Hands-on machine learning with Scikit-Learn, Keras, and TensorFlow: Concepts, tools, and techniques to build intelligent systems, O'Reilly Media, 2019.

Παράρτημα

Εξαγόμενα χαρακτηριστικά επιπέδου δικτυακών ροών που προκύπτουν από ανάλυση αρχείων δικτυακών καταγραφών με χρήση του προγράμματος στα πλαίσια της διπλωματικής εργασίας.

Ονόματα χαρακτηριστικών	Περιγραφή χαρακτηριστικών
flow id	'src ip_dst ip_src port_dst_port_IEC60870-5-104'
src ip	src ip των πακέτων της δικτυακής ροής
src port	src port των πακέτων της δικτυακής ροής
dst ip	dst ip των πακέτων της δικτυακής ροής
dst port	dst port των πακέτων της δικτυακής ροής
Protocol	'IEC 60870-5-104'
flow start timestamp	timestamp του χρόνου άφιξης του πρώτου IEC 104 πακέτου μίας δικτυακής ροής
flow duration	διάρκεια σε δευτερόλεπτα μίας δικτυακής ροής, από το πρώτο IEC 104 πακέτο μέχρι το τελευταίο
total flow packets	συνολικά IEC 104 πακέτα μίας δικτυακής ροής
total fw packets	συνολικά forward direction IEC 104 πακέτα μίας δικτυακής ροής
total bw packets	συνολικά backward direction IEC 104 πακέτα μίας δικτυακής ροής
flow IAT tot	άθροισμα όλων των interarrival times μίας δικτυακής ροής
flow IAT mean	μέση τιμή των interarrival times μίας δικτυακής ροής
flow IAT std	τυπική απόκλιση των interarrival times μίας δικτυακής ροής
flow IAT max	μέγιστη τιμή των interarrival times μίας δικτυακής ροής
flow IAT min	ελάχιστη τιμή των interarrival times μίας δικτυακής ροής

fw IAT tot	άθροισμα όλων των interarrival times των fw direction IEC 104 πακέτων μίας δικτυακής ροής
fw IAT mean	μέση τιμή των interarrival times των fw direction IEC 104 πακέτων μίας δικτυακής ροής
fw IAT std	τυπική απόκλιση των interarrival times των fw direction IEC 104 πακέτων μίας δικτυακής ροής
fw IAT max	μέγιστη τιμή των interarrival times των fw direction IEC 104 πακέτων μίας δικτυακής ροής
fw IAT min	ελάχιστη των interarrival times των fw direction IEC 104 πακέτων σε ένα flow
bw IAT tot	άθροισμα όλων των interarrival times των bw direction IEC 104 πακέτων μίας δικτυακής ροής
bw IAT mean	μέση τιμή των interarrival times των bw direction IEC 104 πακέτων μίας δικτυακής ροής
bw IAT std	τυπική απόκλιση των interarrival times των bw direction IEC 104 πακέτων μίας δικτυακής ροής
bw IAT max	μέγιστη τιμή των interarrival times των bw direction IEC 104 πακέτων μίας δικτυακής ροής
bw IAT min	ελάχιστη τιμή των interarrival times των bw direction IEC 104 πακέτων μίας δικτυακής ροής
fw PSH flag amount	σύνολο fw direction IEC 104 πακέτων που έχουν ορισμένο το TCP flag PSH
bw PSH flag amount	σύνολο bw direction IEC 104 πακέτων που έχουν ορισμένο το TCP flag PSH

fw URG flag amount	σύνολο fw direction IEC 104 πακέτων που έχουν ορισμένο το TCP flag URG
bw URG flag amount	σύνολο bw direction IEC 104 πακέτων που έχουν ορισμένο το TCP flag URG
fw TCP total header length	σύνολο των tcp header length των fw direction IEC 104 πακέτων μίας δικτυακής ροής
bw TCP total header length	σύνολο των tcp header length των bw direction IEC 104 πακέτων μίας δικτυακής ροής
flow FIN flag count	σύνολο IEC 104 πακέτων που έχουν ορισμένο το TCP flag FIN
flow SYN flag count	σύνολο IEC 104 πακέτων που έχουν ορισμένο το TCP flag SYN
flow RST flag count	σύνολο IEC 104 πακέτων που έχουν ορισμένο το TCP flag RST
flow PSH flag count	σύνολο IEC 104 πακέτων που έχουν ορισμένο το TCP flag PSH
flow ACK flag count	σύνολο IEC 104 πακέτων που έχουν ορισμένο το TCP flag ACK
flow URG flag count	σύνολο IEC 104 πακέτων που έχουν ορισμένο το TCP flag URG
flow CWE flag count	σύνολο IEC 104 πακέτων που έχουν ορισμένο το TCP flag CWE
flow ECE flag count	σύνολο IEC 104 πακέτων που έχουν ορισμένο το TCP flag ECE
init fw window bytes	Το window size του πρώτου fw direction IEC 104 πακέτου μίας δικτυακής ροής
init bw window bytes	Το window size του τελευταίου bw direction IEC 104 πακέτου μίας δικτυακής ροής
flow IEC 104 packts/s	αριθμός IEC 104 πακέτων της δικτυακής ροής / διάρκεια της δικτυακής ροής (seconds)

fw IEC 104 packts/s	αριθμός IEC 104 fw direction πακέτων της δικτυακής ροής / διάρκεια της δικτυακής ροής (seconds)
bw IEC 104 packts/s	αριθμός IEC 104 bw direction πακέτων της δικτυακής ροής / διάρκεια της δικτυακής ροής (seconds)
flow IEC 104 bytes/s	άθροισμα των APDU lengths των πακέτων της δικτυακής ροής σε bytes / διάρκεια της δικτυακής ροής (seconds)
fw IEC 104 bytes/s	άθροισμα των APDU lengths των fw direction IEC 104 πακέτων της δικτυακής ροής σε bytes / διάρκεια της δικτυακής ροής (seconds)
bw IEC 104 bytes/s	άθροισμα των APDU lengths των bw direction IEC 104 πακέτων της δικτυακής ροής σε bytes / διάρκεια της δικτυακής ροής (seconds)
flow down/up ratio	συνολικός αριθμός bw direction IEC 104 πακέτων της δικτυακής ροής / συνολικός αριθμός fw direction IEC 104 πακέτων της δικτυακής ροής
fw avg bytes/bulk	Άθροισμα των length των payload όλων των IEC 104 πακέτων στα forward bulks / το πλήθος των φορών που έχει εμφανιστεί ένα forward bulk
fw avg packets/bulk	Το πλήθος των IEC 104 πακέτων όλων των fwd bulks / το πλήθος των φορών που έχει εμφανιστεί σε ένα forward bulk
fw avg bulk rate	Άθροισμα των payload όλων των IEC 104 πακέτων σε fwd bulk / τη διάρκεια του bulk σε seconds
bw avg bytes/bulk	Άθροισμα του length των payload όλων των IEC 104 πακέτων στα backward bulks / το

	πλήθος των φορών που έχει εμφανιστεί ένα backward bulk
bw avg packets/bulk	Το πλήθος των πακέτων όλων των IEC 104 bwd bulks / το πλήθος των φορών που έχει εμφανιστεί σε ένα backward bulk
bw avg bulk rate	Άθροισμα των payload όλων των πακέτων σε IEC 104 bwd bulk / τη διάρκεια του bulk σε seconds
fw_subflow_packets	σύνολο fw direction IEC 104 πακέτων της δικτυακής ροής που είναι διαδοχικά μεταξύ τους (χρονικά) και το IAT του είναι > 1sec
fw_subflow_bytes	άθροισμα των payload όλων των fw direction IEC 104 πακέτων της δικτυακής ροής / προς το πλήθος των πακέτων του subflow
bw_subflow_packets	σύνολο bw direction IEC 104 πακέτων της ροής που είναι διαδοχικά μεταξύ τους (χρονικά) και το IAT του είναι > 1sec
bw_subflow_bytes	άθροισμα των payload όλων των bw direction IEC 104 πακέτων της δικτυακής ροής / προς το πλήθος των πακέτων του subflow
flow active time mean	μέση τιμή των χρόνων που η δικτυακή ροή είναι ενεργή
flow active time std	τυπική απόκλιση των χρόνων που η δικτυακή ροή είναι ενεργή
flow active time var	διακύμανση των χρόνων που η δικτυακή ροή είναι ενεργή
flow active time max	μέγιστη τιμή των χρόνων που η δικτυακή ροή είναι ενεργή
flow active time min	ελάχιστη τιμή των χρόνων που η δικτυακή ροή είναι ενεργή
flow idle time mean	μέση τιμή των χρόνων που η δικτυακή ροή είναι αδρανής

flow idle time std	τυπική απόκλιση των χρόνων που η δικτυακή ροή είναι αδρανής
flow idle time var	διακύμανση των χρόνων που η δικτυακή ροή είναι αδρανής
flow idle time max	μέγιστη τιμή των χρόνων που η δικτυακή ροή είναι αδρανής
flow idle time min	ελάχιστη τιμή των χρόνων που η δικτυακή ροή είναι αδρανής
flow packets APDU total length	άθροισμα όλων των APDU lengths όλων των IEC 104 πακέτων της δικτυακής ροής (είτε fw direction είτε bw direction)
fw packets APDU total length	άθροισμα όλων των APDU lengths όλων των fw direction IEC 104 πακέτων της δικτυακής ροής
bw packets APDU total length	άθροισμα όλων των APDU lengths όλων των bw direction IEC 104 πακέτων της δικτυακής ροής
flow packet APDU length min	ελάχιστη τιμή των APDU lengths όλων των IEC 104 πακέτων της δικτυακής ροής (είτε fw direction είτε bw direction)
flow packet APDU length max	μέγιστη τιμή των APDU lengths όλων των IEC 104 πακέτων της δικτυακής ροής (είτε fw direction είτε bw direction)
flow packet APDU length mean	μέση τιμή των APDU lengths όλων των IEC 104 πακέτων της δικτυακής ροής (είτε fw direction είτε bw direction)
flow packet APDU length std	τυπική απόκλιση των APDU lengths όλων των IEC 104 πακέτων της δικτυακής ροής (είτε fw direction είτε bw direction)
flow packet APDU length var	διακύμανση των APDU lengths όλων των IEC 104 πακέτων της δικτυακής ροής (είτε fw direction είτε bw direction)

fw packet APDU length max	μέγιστη τιμή των APDU lengths όλων των fw direction IEC 104 πακέτων της δικτυακής ροής
fw packet APDU length min	ελάχιστη τιμή των APDU lengths όλων των fw direction IEC 104 πακέτων της δικτυακής ροής
fw packet APDU length mean	μέση τιμή των APDU lengths όλων των fw direction IEC 104 πακέτων της δικτυακής ροής
fw packet APDU length std	τυπική απόκλιση των APDU lengths όλων των fw direction IEC 104 πακέτων της δικτυακής ροής
fw packet APDU length var	διακύμανση των APDU lengths όλων των fw direction IEC 104 πακέτων της δικτυακής ροής
bw packet APDU length max	μέγιστη τιμή των APDU lengths όλων των bw direction IEC 104 πακέτων της δικτυακής ροής
bw packet APDU length min	ελάχιστη τιμή των APDU lengths όλων των bw direction IEC 104 πακέτων της δικτυακής ροής
bw packet APDU length mean	μέση τιμή των APDU lengths όλων των bw direction IEC 104 πακέτων της δικτυακής ροής
bw packet APDU length std	τυπική απόκλιση των APDU lengths όλων των bw direction IEC 104 πακέτων της δικτυακής ροής
bw packet APDU length var	διακύμανση των APDU lengths όλων των bw direction IEC 104 πακέτων της δικτυακής ροής
flow total IEC104_I_Message_SeqIOA packets	συνολικός αριθμός IEC 104 I-format APCI πακέτων ,που έχουν περισσότερα από 1 information objects, της δικτυακής ροής

fw total IEC104_I_Message_SeqIOA packets	συνολικός αριθμός fw direction IEC 104 I-format APCI πακέτων ,που έχουν περισσότερα από 1 information objects, της δικτυακής ροής
bw total IEC104_I_Message_SeqIOA packets	συνολικός αριθμός bw direction IEC 104 I-format APCI πακέτων ,που έχουν περισσότερα από 1 information objects, της δικτυακής ροής
flow total IEC104_I_Message_SingleIOA packets	συνολικός αριθμός IEC 104 I-format APCI πακέτων ,που έχουν 1 information object στο ASDU, της δικτυακής ροής
fw total IEC104_I_Message_SingleIOA packets	συνολικός αριθμός fw direction IEC 104 I-format APCI πακέτων ,που έχουν 1 information object στο ASDU, της δικτυακής ροής
bw total IEC104_I_Message_SingleIOA packets	συνολικός αριθμός bw direction IEC 104 I-format APCI πακέτων ,που έχουν 1 information object στο ASDU, της δικτυακής ροής
flow total IEC104_S_Message packets	συνολικός αριθμός IEC 104 S-format APCI πακέτων , της δικτυακής ροής
fw total IEC104_S_Message packets	συνολικός αριθμός fw direction IEC 104 S-format APCI πακέτων , της δικτυακής ροής
bw total IEC104_S_Message packets	συνολικός αριθμός bw direction IEC 104 S-format APCI πακέτων , της δικτυακής ροής
flow total IEC104_U_Message packets	συνολικός αριθμός IEC 104 U-format APCI πακέτων , της δικτυακής ροής
fw total IEC104_U_Message packets	συνολικός αριθμός fw direction IEC 104 U-format APCI πακέτων , της δικτυακής ροής
bw total IEC104_U_Message packets	συνολικός αριθμός bw direction IEC 104 U-format APCI πακέτων , της δικτυακής ροής

total IEC104 packets with COT=1	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT periodic,cyclic
total IEC104 packets with COT=2	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT background interrogation
total IEC104 packets with COT=3	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT spontaneous
total IEC104 packets with COT=4	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT initialized
total IEC104 packets with COT=5	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT interrogation or interrogated
total IEC104 packets with COT=6	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT activation
total IEC104 packets with COT=7	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT confirmation activation
total IEC104 packets with COT=8	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT deactivation
total IEC104 packets with COT=9	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT confirmation deactivation
total IEC104 packets with COT=10	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT termination activation
total IEC104 packets with COT=11	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT feedback, caused by distant command

total IEC104 packets with COT=12	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT feedback, caused by local command
total IEC104 packets with COT=13	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT data transmission
total IEC104 packets with COT=20	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν COT interrogated by general interrogation
total IEC104packets with type_id_process_information_in_monitor_direction	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν TypeID στο διάστημα 1-40
total IEC104packets with type_id_process_information_in_control_direction	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν TypeID στο διάστημα 45-51
total IEC104packets with type_id_system_information_in_monitor_direction	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν TypeID στο διάστημα 70
total IEC104packets with type_id_system_information_in_control_direction	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν TypeID στο διάστημα 100-106
total IEC104packets with type_id_parameter_in_control_direction	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν TypeID στο διάστημα 110-113
total IEC104packets with type_id_file_transfer	συνολικός αριθμός IEC 104 πακέτων της δικτυακής ροής, τα οποία έχουν TypeID στο διάστημα 120-126