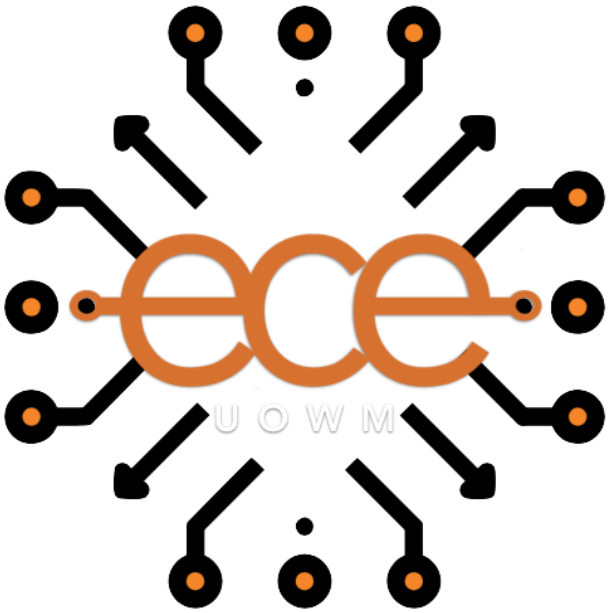
ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ



ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σύστημα Ελέγχου Εισβολών στο Διαδίκτυο των Πραγμάτων με Χρήση Τεχνικών Βαθιάς Μάθησης

Κέλλη Βασιλική

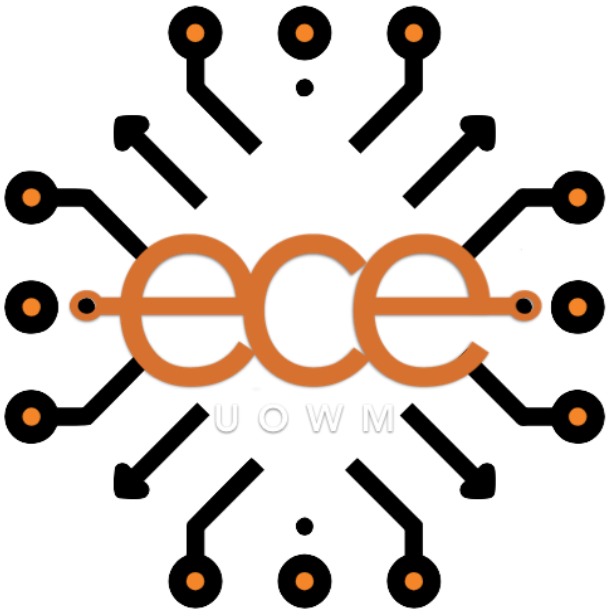
Επιβλέπων Καθηγητής : Επίκουρος Καθηγητής, Παναγιώτης Σαρηγιαννίδης

Κοζάνη, Ιούνιος 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ



ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Σύστημα Ελέγχου Εισβολών στο Διαδίκτυο των Πραγμάτων με Χρήση Τεχνικών Βαθιάς Μάθησης

Κέλλη Βασιλική

Επιβλέπων Καθηγητής : Επίκουρος Καθηγητής, Παναγιώτης Σαρηγιαννίδης

Κοζάνη, Ιούνιος 2020

Δήλωση Πνευματικών Δικαιωμάτων

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν. 1599/1986 και τα άρθρα 2,4,6 παρ. 3 του Ν. 1256/1982, η παρούσα Διπλωματική Εργασία με τίτλο

“ Σύστημα Ελέγχου Εισβολών στο Διαδίκτυο των Πραγμάτων με χρήση Τεχνικών Βαθιάς Μάθησης **”**

καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας και αναφέρονται ρητώς μέσα στο κείμενο που συνοδεύουν, και η οποία έχει εκπονηθεί στο Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών του Πανεπιστημίου Δυτικής Μακεδονίας, υπό την επίβλεψη του μέλους του Τμήματος κ. Παναγιώτη Σαρηγιαννίδη

αποτελεί αποκλειστικά προϊόν προσωπικής εργασίας και δεν προσβάλλει κάθε μορφής πνευματικά δικαιώματα τρίτων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή / και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή.

Απαγορεύεται η αντιγραφή, αποθήκευση και διανομή της παρούσας εργασίας, εξ ολοκλήρου ή τμήματος αυτής, για εμπορικό σκοπό. Επιτρέπεται η ανατύπωση, αποθήκευση και διανομή για σκοπό μη κερδοσκοπικό, εκπαιδευτικής ή ερευνητικής φύσης, υπό την προϋπόθεση να αναφέρεται η πηγή προέλευσης και να διατηρείται το παρόν μήνυμα. Ερωτήματα που αφορούν τη χρήση της εργασίας για κερδοσκοπικό σκοπό πρέπει να απευθύνονται προς τον συγγραφέα. Οι απόψεις και τα συμπεράσματα που περιέχονται σε αυτό το έγγραφο εκφράζουν τον συγγραφέα και μόνο.

Υπογραφή Φοιτητή:

Περίληψη

Στόχος της διπλωματικής εργασίας, αποτελεί η παρουσίαση ενός συστήματος ανίχνευσης εισβολών για βιομηχανικά συστήματα ελέγχου και συγκεκριμένα για το Διανεμημένο Δικτυακό Πρωτόκολλο 3 (Distributed Network Protocol 3 - DNP3), με χρήση τεχνικών βαθιάς μάθησης. Η μετάβαση στη χρήση πλήρως δικτυωμένων συσκευών σε όλους τους τομείς της ανθρώπινης ζωής έχει επιφέρει μεγάλες αλλαγές στον τρόπο και την ποιότητα ζωής, συντελώντας στην βελτίωση της καθημερινότητας. Η χρήση τους έχει επεκταθεί και στον τομέα της βιομηχανίας, με τις δικτυωμένες συσκευές να καταλαμβάνουν κυρίαρχο ρόλο στη διαδικασία παρακολούθησης και ελέγχου. Η ένταξή τους σε ευαίσθητες υποδομές, με την ταυτόχρονη αύξηση των κυβερνοεπιθέσεων που έχει επιφέρει η δικτύωση, εγείρει ερωτήματα σχετικά με την ασφάλεια των συστημάτων και διαδικασιών. Επιθέσεις ενάντια σε εξαιρετικά ευαίσθητες υποδομές, όπως έχει αποδειχθεί και στο παρελθόν, είναι ικανές να προκαλέσουν υλικές καταστροφές εξαρτημάτων, διακοπή παροχών, αλλά και προβλήματα μεγαλύτερης κλίμακας. Συνεπώς, κρίνεται απαραίτητη η διαμόρφωση συστημάτων ανίχνευσης εισβολών ικανών να αναγνωρίζουν επιθέσεις οι οποίες μπορεί να θέσουν σε κίνδυνο την ακεραιότητα, εμπιστευτικότητα και διαθεσιμότητα των βιομηχανικών συστημάτων. Η διπλωματική εργασία, επικεντρώνεται στην υλοποίηση ενός συστήματος ανίχνευσης εισβολών για βιομηχανικά συστήματα που χρησιμοποιούν DNP3. Συνεπώς, πραγματοποιείται η ανάλυση του πρωτοκόλλου DNP3 και πιθανές σχετικές επιθέσεις ενάντια σε αυτό, οι οποίες χρησιμοποιούνται για την σύνθεση και τη δημιουργία ενός συνόλου δεδομένων. Με βάση το συγκεκριμένο σύνολο δεδομένων, αναπτύχθηκε μοντέλο βαθιάς μάθησης, ικανό να αναγνωρίσει 8 επιθέσεις, συγκεκριμένα, επιθέσεις ψυχρής και θερμής επανεκκίνησης, απενεργοποίησης ανεπιθύμητων μηνυμάτων, δύο επιθέσεις αναγνώρισης, αρχικοποίησης δεδομένων, τερματισμού εφαρμογής και επανάληψης. Συγκεκριμένα, το μοντέλο βαθιάς μάθησης το οποίο δουλεύει με DNP3 δικτυακές ροές, ενσωματώνεται για τη δημιουργία του τελικού συστήματος ανίχνευσης εισβολών με το όνομα Medium. Η αποτελεσματικότητα του μοντέλου του Medium αποδεικνύεται μέσα από την ανάλυση αξιολόγησης σε σύγκριση με άλλους ταξινομητές μηχανικής μάθησης. Συγκεκριμένα, η ακρίβεια και το F1 score του προτεινόμενου μοντέλου αγγίζουν το 96.5% και 96.47% αντίστοιχα.

Λέξεις-κλειδιά: *Σύστημα ελέγχου εισβολών, βιομηχανικά πρωτόκολλα, επιθέσεις, μηχανική μάθηση, βαθιά μάθηση, IoT*

Abstract

The main purpose of this diploma thesis is the implementation of an Intrusion Detection System (IDS) for DNP3 Supervisory Control and Data Acquisition (SCADA) environments, based on deep learning techniques. The use of smart devices has improved the quality of human life in many aspects. The existence of smart interconnected devices in Critical Infrastructures (CI) is necessary to monitor and control the industrial processes. Their extended use to such delicate infrastructures, combined with the recent rise of cyberattacks, has raised a lot of questions about the security and safety of this smart equipment. Recent cyberattacks have already shown their disastrous consequences against CIs that can vary from the hardware destruction, cease of production and even to fatal accidents. Evidently, the implementation of intrusion detection systems, capable of identifying attacks compromising the confidentiality, integrity and availability of Industrial Control Systems (ICS) is crucial. This diploma thesis focuses on the implementation of an IDS which can recognize timely cyber attacks against DNP3. Therefore, the DNP3 protocol is analyzed, relevant attacks against DNP3 are investigated and performed in order to compose a DNP3 intrusion detection dataset. Next, based on this dataset, a deep neural network (DNN) was trained and deployed, thus detecting eight DNP3 cyberattacks, namely cold restart, disable unsolicited messages, warm restart, dnp3 enumerate with NSE, dnp3 info with NSE, stop application, initialize data and replay attack. In particular, the aforementioned DNN works with DNP3 network flows, and it is integrated into a complete IDS system called Medium. The efficiency of Medium and particularly, of DNN is demonstrated by the evaluation analysis with other machine learning methods. In particular, the accuracy and the F1 score of the proposed DNN reach 96.5% and 96.47% respectively.

***Key-words**: intrusion detection systems, industrial protocols, attacks, machine learning, deep learning, IoT*

Ευχαριστίες

Πρωτίστως, θα ήθελα να ευχαριστήσω τους γονείς μου όχι μόνο για την οικονομική συμπαράσταση, αλλά κυρίως για την πνευματική υποστήριξή τους και πίστη τους σε εμένα. Επίσης, θα ήθελα να ευχαριστήσω τον επίκουρο καθηγητή του Τμήματος Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών, Παναγιώτη Σαρηγιαννίδη, επιβλέποντα της διπλωματικής, για τις γνώσεις που μου μετέδωσε. Επιπλέον, θα ήθελα να ευχαριστήσω τον υποψήφιο Δρ. Παναγιώτη Ράδογλου-Γραμματίκη, για την μεγάλη υποστήριξη και καθοδήγηση, η οποία έπαιξε καθοριστικό ρόλο στην ολοκλήρωση της διπλωματική εργασίας.

Περιεχόμενα

Ευρετήριο Σχημάτων

Ευρετήριο Πινάκων

Συντομογραφίες

Συντομογραφία	**Επεξήγηση**
TCP	Πρωτόκολλο Ελέγχου Μετάδοσης (Transmission Control Protocol)
IP	Πρωτόκολλο Διαδικτύου (Internet Protocol)
DNP3	Διανεμημένο Δικτυακό Πρωτόκολλο 3 (Distributed Network Protocol 3)
SCADA	Σύστημα Ελέγχου-Εποπτείας και Μεταφοράς Δεδομένων Λειτουργίας (Supervisory Control And Data Acquisition)
PLC	Προγραμματιζόμενος Λογικός Ελεγκτής (Programmable Logic Controller)
RTU	Απομακρυσμένη Μονάδα Τερματικού (Remote Terminal Unit)
IED	Ευφυείς Ηλεκτρονική Συσκευή (Intelligent Electronic Device)
.PCAP	Καταγραφή Πακέτου (Packet Capture)
IDS	Σύστημα Ελέγχου/Ανίχνευσης Εισβολών (Intrusion Detection System)
.CSV	Τιμές Διαχωρισμένες με Κόμμα (Comma Separated Values)
TCP/IP	Πρωτόκολλο Ελέγχου Μετάδοσης/ Πρωτόκολλο Διαδικτύου (Transmission Control Protocol/Internet Protocol)
ANN	Τεχνητό Νευρωνικό Δίκτυο(Artificial Neural Network)
DNN	Βαθύ Νευρωνικό Δίκτυο (Deep Neural Network)
RFC	Request For Comments

IIN	Εσωτερικές Ενδείξεις (Internal Indications)
CRC	Κυκλικός Έλεγχος Πλεονασμού (Cyclic Redundancy Check)
ARP	Πρωτόκολλο Επίλυσης Διευθύνσεων (Address Resolution Protocol)
MITM	Man In The Middle
UI	Διεπαφή Χρήστη (User Interface)
DOS	Άρνηση Υπηρεσιών (Denial Of Service)
IEEE	Ινστιτούτο Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronics Engineers)
CI	Κρίσιμη Υποδομή (Critical Infrastructure)
NSE	Nmap Scripting Engine
OSI	Ανοιχτή Διασύνδεση Συστημάτων (Open Systems Interconnection)

1. Εισαγωγή

Είναι αδιαμφισβήτητο πως την τελευταία δεκαετία έχει παρατηρηθεί αλματώδη εξέλιξη στον τομέα της πληροφορικής και των δικτύων. Η ανθρώπινη επικοινωνία, ψυχαγωγία, υγεία, ποιότητα ζωής, καθώς και πολλοί ακόμα τομείς της ανθρώπινης καθημερινότητας έχουν γνωρίσει βελτίωση μέσα από αυτή την εξέλιξη. Πλέον, η χρήση δικτυωμένων συσκευών είναι αναπόσπαστο κομμάτι της κοινωνίας.

Τα πρόσφατα χρόνια, η αξιοποίηση έξυπνων, δικτυωμένων συσκευών έχει αρχίσει να εισέρχεται και στον τομέα της βιομηχανίας, και συγκεκριμένα στις βιομηχανίες παραγωγής ενέργειας. Τα πλεονεκτήματα που προσφέρουν είναι άπλετα, ενώ με την πάροδο του χρόνου συστήνονται ολοένα και πιο σύγχρονες, καινοτόμες και αποτελεσματικές λύσεις αυτοματοποίησης της διαδικασίας ελέγχου παραγωγής ενέργειας.

Η δικτύωση τόσο ευαίσθητων διαδικασιών απαιτεί μέγιστη ακρίβεια και προσοχή στην διασφάλιση της ακεραιότητας, εμπιστευτικότητας και διαθεσιμότητας των δεδομένων και συσκευών που απαρτίζουν ένα έξυπνο δίκτυο. Ωστόσο, πολλά πρωτόκολλα επικοινωνίας δεν έχουν κατασκευαστεί προκειμένου να παρέχουν την αναγκαία και απαιτούμενη ασφάλεια. Ταυτόχρονα, και λόγω της μεγάλης ένταξης των δικτύων στην ανθρώπινη ζωή, η εύρεση ευπαθειών σε πρωτόκολλα επικοινωνίας, και η κακόβουλη εκμετάλλευσή τους, αποτελεί συχνό φαινόμενο [1] το οποίο απειλεί με έως και καταστροφικές συνέπειες την αρμονικότητα που απαιτούν διαδικασίες τόσο λεπτές όσο και αυτές του ενεργειακού τομέα.

Για τον παραπάνω σκοπό, αναπτύσσονται λύσεις με εφαρμογή καινοτόμων μεθόδων, όπως αυτή της μηχανικής μάθησης, προκειμένου να βρεθούν κατάλληλες ενέργειες έγκυρης και έγκαιρης ανίχνευσης εισβολών.

1.1 Κίνητρο και Στόχοι Διπλωματικής Εργασίας

Οι επιθέσεις ενάντια σε βιομηχανικά συστήματα ελέγχου είναι ένα νέο φαινόμενο που έπεται την πρόσφατη ανάπτυξη του συγκεκριμένου τομέα. Ίσως η πλέον γνωστότερη κακόβουλη ενέργεια, αποτελεί το Stuxnet Worm, η δράση του οποίου αποκαλύφθηκε το 2010, ενώ εικάζεται πως στόχος του αποτελούσε το πυρηνικό πρόγραμμα του Ιράν. Κατασκευασμένο να στοχοποιεί συστήματα Windows τα οποία χρησιμοποιούσαν λογισμικό Συστημάτων Ελέγχου-Εποπτείας και Μεταφοράς Δεδομένων Λειτουργίας (Supervisory Control And Data Acquisition – SCADA) της

Siemens, αποκτά τον έλεγχο της επικοινωνίας μεταξύ του SCADA και των Προγραμματιζόμενων Λογικών Ελεγκτών (Programmable Logic Controller – PLC) [2] τα οποία είναι υπεύθυνα για την επίβλεψη φυγόκεντρων διαχωρισμού πυρηνικού υλικού για την παραγωγή εμπλουτισμένου ουράνιου [3] , και δρα προκαλώντας την υλική καταστροφή των φυγόκεντρων.

Η επιτυχία του Stuxnet ενάντια σε υποδομές πυρηνικού ενδιαφέροντος, εγείρει ερωτήματα σχετικά με την ασφάλεια και την ετοιμότητα του τομέα της βιομηχανίας ενέργειας. Ο εκτενής έλεγχος προκειμένου να αποφευχθεί η εύρεση zero-day ευπαθειών από κακόβουλα άτομα, καθώς και η ανάπτυξη κατάλληλων συστημάτων ελέγχου εισβολών, και η τοποθέτησή τους σε κομβικά σημεία του έξυπνου δικτύου μπορεί να αποτρέψουν την εκτέλεση τέτοιων ενεργειών.

Στόχος της παρούσας διπλωματικής εργασίας, είναι να παρουσιάσει ένα σύστημα ελέγχου εισβολών για το Διανεμημένο Δικτυακό Πρωτόκολλο 3 (Distributed Network Protocol 3 - DNP3), το οποίο παρακολουθώντας τις δικτυακές ροές και εξάγοντας ιδιότητες χαρακτηρισμού της κάθε ροής, με την ταυτόχρονη εφαρμογή μοντέλου βαθιάς μάθησης, είναι σε θέση να αναγνωρίσει επιθέσεις.

1.2 Δομή Διπλωματικής Εργασίας

Η παρούσα διπλωματική εργασία αποτελείται από έξι κεφάλαια. Το πρώτο κεφάλαιο, αποτελεί αναφορά της ανάπτυξης της ζήτησης έξυπνων συσκευών αυτοματισμού στον βιομηχανικό τομέα καθώς και τους κινδύνους που ελλοχεύουν από την ένταξή τους.

Στο δεύτερο κεφάλαιο, αναλύονται τα συστήματα ανίχνευσης εισβολών, τόσο σε στόχους, όσο και σε αρχιτεκτονική, ενώ συγκρίνονται τα μοντέλα ανίχνευσης εισβολών, και τέλος πραγματοποιείται βιβλιογραφική ανασκόπηση των Συστημάτων Ανίχνευσης Εισβολών (Intrusion Detection Systems – IDS) στα βιομηχανικά συστήματα.

Στο τρίτο κεφάλαιο, περιγράφεται το θεωρητικό υπόβαθρο του DNP3 και στη συνέχεια πραγματοποιείται ανάλυση των επιθέσεων που υλοποιήθηκαν στα πλαίσια αυτής της διπλωματικής εργασίας, ενάντια στο συγκεκριμένο πρωτόκολλο.

Στο τέταρτο κεφάλαιο παρουσιάζεται μια θεωρητική εισαγωγή στη μηχανική μάθηση, και κατόπιν αναλύονται οι τεχνικές Τυχαίου Δάσους, Naïve Bayes, Τεχνητού Νευρωνικού Δικτύου (Artificial Neural Network – ANN), Δένδρου Απόφασης, ενώ υποδεικνύονται τρόποι αξιολόγησης μοντέλων μηχανικής μάθησης.

Στο πέμπτο κεφάλαιο, πραγματοποιείται η παρουσίαση του συστήματος ανίχνευσης εισβολών που υλοποιήθηκε στα πλαίσια της διπλωματικής εργασίας. Αναλυτικότερα, παρουσιάζεται ο τρόπος καταγραφής και ανάλυσης δικτυακής κίνησης σε DNP3 ροές, και στη συνέχεια περιγράφεται ο τρόπος εκπαίδευσης και εξαγωγής του μοντέλου βαθιάς μάθησης ενώ συγκρίνεται η αξιολόγησή του με αυτήν των υπόλοιπων τεχνικών μηχανικής μάθησης. Τέλος, παρουσιάζεται η ολοκληρωμένη λειτουργία του IDS.

Στο έκτο και τελευταίο κεφάλαιο, αναλύονται τα συμπεράσματα καθώς και οι μελλοντικές επεκτάσεις.

2. Συστήματα Ανίχνευσης Εισβολών

Τα τελευταία χρόνια, είναι αναμφίβολο πως υπάρχει μια αλματώδη αύξηση των λειτουργιών που παρέχονται με χρήση δικτύου, σε όλους τους τομείς της καθημερινότητας. Η συγκεκριμένη αύξηση στη χρήση δικτύων, οδήγησε και σε αύξηση κυβερνοεπιθέσεων σε πλήθος και πολυπλοκότητα. Συνεπώς, είναι απαραίτητη η ενσωμάτωση ενός αποτελεσματικού συστήματος ανίχνευσης εισβολών, κυρίως σε συστήματα με ευαίσθητες πληροφορίες και λειτουργίες. Σαν σύστημα ανίχνευσης εισβολών, σύμφωνα με το [4], ορίζεται ένα λογισμικό ή υλικό το οποίο είναι υπεύθυνο για την αυτοματοποίηση της διαδικασίας παρακολούθησης των συσκευών ενός δικτύου και την ανάλυση της κίνησης για εύρεση πιθανών επιθέσεων.

Στο συγκεκριμένο κεφάλαιο πρόκειται να αναλυθούν εκτενέστερα τα συστήματα ελέγχου εισβολών, οι στόχοι τους, η αρχιτεκτονική τους, και τα μοντέλα ενώ τέλος πραγματοποιείται βιβλιογραφική ανασκόπηση συστημάτων ελέγχου εισβολών σε βιομηχανικά συστήματα.

2.1 Στόχοι Συστημάτων Ανίχνευσης Εισβολών

Στόχος ενός συστήματος ελέγχου εισβολών αποτελεί η έγκυρη και έγκαιρη αναγνώριση πληθώρας επιθέσεων. Η έγκυρη αναγνώριση επιθέσεων αναφέρεται στη σωστή ταυτοποίηση της κίνησης, ή με άλλα λόγια, το σύστημα ελέγχου εισβολών θα πρέπει να είναι σε θέση να καθορίσει με ακρίβεια για το αν η κίνηση είναι φυσιολογική ή όχι. Σε περίπτωση που δεν είναι ικανό να αναγνωρίσει σωστά επιθέσεις, όπως για παράδειγμα αν αναγνωρίσει εσφαλμένα φυσιολογική κίνηση ως επίθεση ή το αντίστροφο, τότε το σύστημα δεν είναι άξιο εμπιστοσύνης.

Σε ότι αφορά την έγκαιρη ταυτοποίηση, το σύστημα ελέγχου εισβολών οφείλει να αναγνωρίζει επιθέσεις αν όχι σε πραγματικό χρόνο, τότε το συντομότερο δυνατό προκειμένου να μπορέσουν να αποτραπούν επιτυχώς οι κακόβουλες ενέργειες.

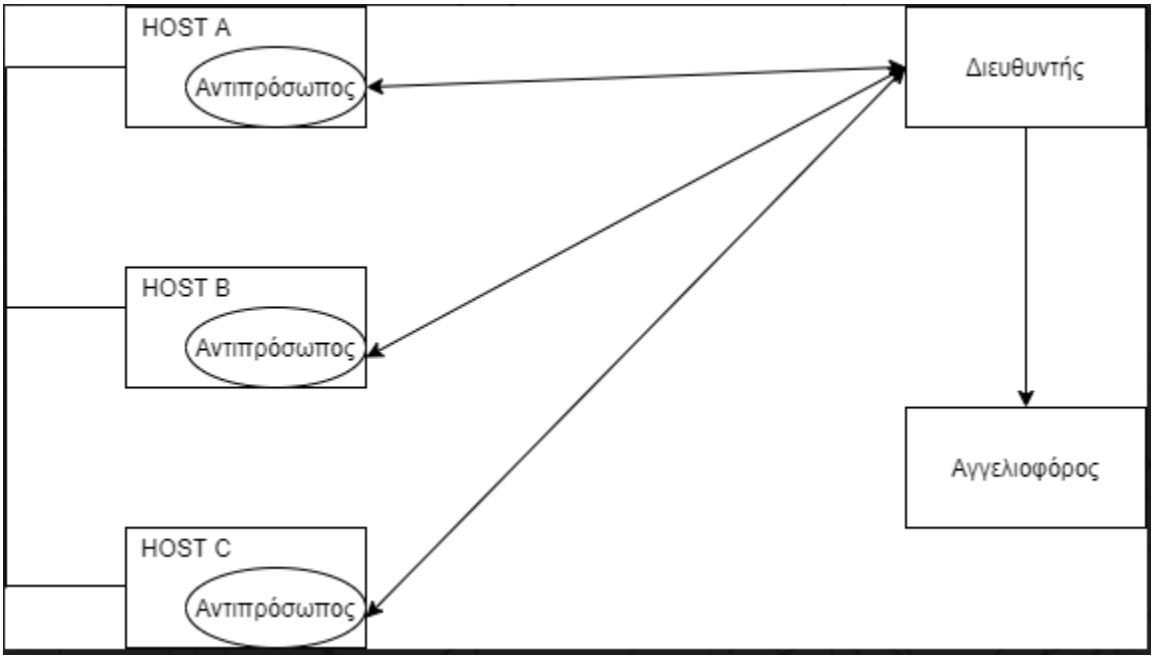
Ο τομέας της κυβερνοασφάλειας είναι ένα αντικείμενο συνεχώς εξελισσόμενο. Μαζί με αυτήν όμως εξελίσσονται και οι τεχνικές επιθέσεων. Συνεπώς, ένα IDS οφείλει να είναι ενημερωμένο σχετικά με πληθώρα επιθέσεων, προκειμένου να μπορεί να τις αναγνωρίσει. Ακόμα και αν μια επίθεση δεν είναι γνωστή, το IDS, ιδανικά, θα μπορεί να χαρακτηρίσει τη κίνηση σαν κακόβουλη.

2.2 Αρχιτεκτονική Συστήματος Ανίχνευσης Εισβολών

Η αρχιτεκτονική ενός συστήματος ελέγχου εισβολών αποτελείται από τρία επιμέρους στοιχεία:

- **Αντιπρόσωπος:** Ένα σύστημα ελέγχου εισβολών μπορεί να αποτελείται από έναν ή και παραπάνω αντιπροσώπους (agent). Οι αντιπρόσωποι είναι κατανεμημένοι στα συστήματα του δικτύου και αναλαμβάνουν τη συλλογή πληροφοριών, όπως για παράδειγμα δικτυακής κίνησης, και την αναμετάδοσή τους στον Διευθυντή σε συγκεκριμένη μορφή.
- **Διευθυντής:** Στόχος του διευθυντή (director) είναι η αναγνώριση μιας επίθεσης με βάση τα δεδομένα που λαμβάνει από τον/τους αντιπροσώπους. Αρχικά, απορρίπτει τις περιττές πληροφορίες και στη συνέχεια, αναλύει τα δεδομένα για να καθορίσει εάν συμβαίνει ή αν πρόκειται να συμβεί μια επίθεση.
- **Αγγελιοφόρος:** Ο αγγελιοφόρος (notifier) λαμβάνει δεδομένα από τον διευθυντή, και στη συνέχεια ενεργεί είτε ενημερώνοντας τον υπεύθυνο ασφαλείας για τα αποτελέσματα που προέκυψαν από την ανάλυση του διευθυντή και άρα για την πιθανή επίθεση, είτε ενεργεί αντεπιτιθέμενος.

Στο παρακάτω σχήμα, απεικονίζεται μια τυπική αρχιτεκτονική συστήματος ελέγχου εισβολών.



Σχήμα 1: Σχηματικά μια τυπική αρχιτεκτονική IDS [5]

2.3 Μοντέλα Ανίχνευσης Εισβολών

Τα μοντέλα ανίχνευσης εισβολών καθορίζουν τον τρόπο με τον οποίο ένα IDS αναγνωρίζει τις επιθέσεις. Συγκεκριμένα, υπάρχουν τρείς μεθοδολογίες ανίχνευσης εισβολών, η ανίχνευση ανωμαλιών, η ανίχνευση κακής χρήσης και η ανίχνευση βασισμένη σε προδιαγραφές.

Η ανίχνευση ανωμαλιών, θεωρεί επίθεση οτιδήποτε δεν είναι φυσιολογικό. Αναλυτικότερα, παρατηρούνται οι ενέργειες του συστήματος σε φυσιολογική κατάσταση, χωρίς τη παρέμβαση επιθέσεων και στη συνέχεια, με τεχνικές μηχανικής μάθησης γίνεται εκπαίδευση ενός μοντέλου στη συγκεκριμένη φυσιολογική κατάσταση. Οτιδήποτε αποτελεί απόκλιση αυτής της συμπεριφοράς, θεωρείται κακόβουλη συμπεριφορά. Μειονέκτημα του συγκεκριμένου μοντέλου αποτελεί η λανθασμένη ενημέρωση για πιθανή επίθεση, το οποίο μπορεί να συμβεί από ελλιπή ενημέρωση του IDS για όλες τις ενέργειες φυσιολογικής συμπεριφοράς. Συνεπώς, μη-κακόβουλη συμπεριφορά χαρακτηρίζεται ως κακόβουλη [6].

Σε αντίθεση με την ανίχνευση ανωμαλιών, η ανίχνευση κακής χρήσης καθορίζει αρχικά μια κακόβουλη συμπεριφορά, με τη μορφή υπογραφών, διαθέτει δηλαδή στη βάση γνώσης του χαρακτηριστικά αναγνωρισμένων επιθέσεων. Οτιδήποτε δεν αντιστοιχίζεται σε μια ήδη γνωστή επίθεση, θεωρείται φυσιολογικό και αντίστοιχα, αν υπάρχει ταυτοποίηση χαρακτηριστικών με κάποια υπογραφή, τότε θα θεωρηθεί ως επίθεση. Μειονέκτημα της συγκεκριμένης μεθόδου αποτελεί το γεγονός ότι δεν είναι εφικτό να αναγνωρίσει επιθέσεις των οποίων η υπογραφή δεν υπάρχει καταχωρημένη στη βάση γνώσης του IDS.

Τέλος, η ανίχνευση βασισμένη σε προδιαγραφές, συνδυάζει τα οφέλη της ανίχνευσης ανωμαλιών και της ανίχνευσης κακής χρήσης. Συγκεκριμένα, συμπεριφορές συστήματος χαρακτηρίζονται με χειροκίνητο τρόπο ως φυσιολογικές και όχι με μηχανική μάθηση όπως στην ανίχνευση ανωμαλιών, οπότε η παραγωγή εσφαλμένων ειδοποιήσεων, χαρακτηρίζοντας μη-κακόβουλη συμπεριφορά ως κακόβουλη, βρίσκεται σε χαμηλότερο επίπεδο από αυτή της ανίχνευσης ανωμαλιών [7]. Σε ότι αφορά την αναγνώριση επιθέσεων, ισχύει ότι και στην ανίχνευση ανωμαλιών, δηλαδή οτιδήποτε δεν ανήκει στη προκαθορισμένη φυσιολογική συμπεριφορά, θεωρείται κακόβουλη πράξη. Μειονέκτημα της συγκεκριμένης μεθόδου αποτελεί το γεγονός ότι η διαδικασία του χειροκίνητου καθορισμού πληθώρας φυσιολογικών συμπεριφορών, όπως απαιτείται για την σωστή λειτουργία του IDS, είναι αρκετά χρονοβόρα.

2.4 Συστήματα Ανίχνευσης Εισβολών σε Βιομηχανικά Συστήματα

Στον τομέα της βιομηχανίας, υπάρχει μια τάση αντικατάστασης χειροκίνητων εργασιών με τη χρήση αυτοματοποιημένων συστημάτων. Για παράδειγμα, ο έλεγχος των μετρήσεων και η απόφαση για την επόμενη ενέργεια, δεν πραγματοποιούνται πλέον με την ανθρώπινη παρέμβαση παρά μόνο αν αυτό κριθεί απαραίτητο. Ο αυτοματισμός των συσκευών πραγματοποιείται με την υλοποίηση εφαρμογών που δίνουν την δυνατότητα σε έξυπνες συσκευές να επικοινωνούν μεταξύ τους, οπότε, δημιουργείται πλέον ένα δίκτυο από συσκευές ελέγχου και συσκευές που εκτελούν εργασίες. Συνεπώς, η δικτύωση και η μετατροπή της διαδικασίας ελέγχου και εργασίας από εκτός σύνδεσης σε συνδεδεμένη [8], ελλοχεύει κινδύνους για την ασφάλεια της εξαιρετικά ευαίσθητης υποδομής [9]. Συμπερασματικά, είναι απαραίτητη η υλοποίηση συστημάτων ελέγχου εισβολών που να μπορούν να καλύπτουν τις ανάγκες των βιομηχανικών υποδομών. Για τον παραπάνω σκοπό έχουν δημοσιευθεί διάφορες έρευνες προκειμένου να προταθούν λύσεις για τη δημιουργία συστημάτων ελέγχου εισβολών στα βιομηχανικά συστήματα.

Οι Igbe κ.ά. [10], πρότειναν την τεχνική ανίχνευσης εισβολών ενάντια στο DNP3 με χρήση ντετερμινιστικού αλγόριθμου δεντρικού κυττάρου (deterministic Dentric Cell Algorithm), η οποία λαμβάνει έμπνευση από τα κύτταρα του ανθρώπινου ανοσοποιητικού συστήματος, τα οποία δρουν σαν σύστημα ελέγχου εισβολών για αυτό, ελέγχοντας τα όργανα και τους ιστούς για εισβολείς με τη μορφή παθογόνων. Ο παραπάνω αλγόριθμος εφαρμόστηκε για την ανίχνευση επιθέσεων οι οποίες υλοποιήθηκαν ενάντια στο DNP3. Οι επιθέσεις αφορούσαν Άρνηση Υπηρεσιών (Denial Of Service – DoS), έγχυση και τροποποίηση πακέτων κατόπιν Man In The Middle (MiTM), με χρήση διάφορων εργαλείων.

Οι Rodofile κ.ά. [11] παρουσίασαν μια δομή επιθέσεων για παραγωγή κακόβουλης κίνησης στα δίκτυα SCADA, με σκοπό τη δημιουργία συνόλου δεδομένων και την εφαρμογή τους για την εκπαίδευση μοντέλου για παραγωγή συστήματος ελέγχου εισβολών. Συγκεκριμένα, η δομή εφαρμόστηκε ενάντια στο DNP3, και οι επιθέσεις περιλαμβάνουν DNP3 αναγνώριση, επιθέσεις έγχυσης πακέτων, μεταμφίεσης, επανάληψης, πλημμύρας, και MiTM.

Οι Yang κ.ά. [12] επικεντρώθηκαν στη δημιουργία πολυδιαστασιακού συστήματος ελέγχου εισβολών, για το πρωτόκολλο IEC61850. Οι διαστάσεις του, αφορούν ανίχνευση ελέγχου πρόσβασης, ανίχνευση επιτρεπόμενων πρωτοκόλλων με τη μορφή λίστας, ανίχνευση βάση μοντέλου ανίχνευσης μη φυσιολογικής συμπεριφοράς, δεδομένου ότι έχει καθοριστεί φυσιολογική κίνηση, και τέλος ανίχνευση πολλαπλών παραμέτρων, αναγνωρίζοντας πιθανές

επιθέσεις λόγω εσωτερικής κακής χρήσης ή εξωτερικής επίθεσης με παρακολούθηση λειτουργικά ευαίσθητων παραμέτρων.

Οι Kwon κ.ά. [13] προτείνουν ένα σύστημα ελέγχου εισβολών βασισμένο στο πρωτόκολλο Ινστιτούτου Ηλεκτρολόγων και Ηλεκτρονικών Μηχανικών (Institute of Electrical and Electronics Engineers – IEEE) 1815.1, το οποίο πραγματοποιεί ελέγχους κεφαλίδας και φορτίου για ανίχνευση μη φυσιολογικής συμπεριφοράς. Η επαλήθευση της παραπάνω τεχνικής, ελέγχθηκε με βάση πραγματικά δεδομένα που συλλέχθηκαν στην Κορέα, με βάση το πρωτόκολλο IEEE 1815.1, και με βάση συμπεριφορές κακόβουλου λογισμικού, ψευδή έγχυση δεδομένων και αποτροπής απόκτησης δεδομένων. Το προτεινόμενο σύστημα ελέγχου εισβολών, αναγνώρισε επιτυχώς πέντε τύπους επιθέσεων συμπεριφοράς κακόβουλου λογισμικού, τρείς τύπους εσφαλμένης έγχυσης πακέτων, και τρείς τύπους αποτροπής απόκτησης δεδομένων.

Οι Yin κ.ά. [14] αναφέρονται σε μια λύση για SCADA/DNP3 που αποτελείται από τρία σημεία, τα δεδομένα εισόδου, την ανάλυση των δεδομένων και την ταξινόμηση των δεδομένων. Τα δεδομένα εισόδου, αποτελούνται κατά 55% από δεδομένα επίθεσης και κατά 45% από δεδομένα φυσιολογικής κίνησης, τα οποία συγκεντρώθηκαν από διάφορες πηγές. Στα πλαίσια της δημοσίευσης, και κατόπιν ανάλυσης ευπαθειών του DNP3, μοντελοποιήθηκαν οι επιθέσεις ενάντια στο συγκεκριμένο πρωτόκολλο, οι οποίες αφορούσαν και τα τρία επίπεδα του DNP3. Αναλυτικότερα, οι επιθέσεις στο επίπεδο συνδέσμου αφορούσαν κωδικό λειτουργίας επαναφοράς, σημαία του συγκεκριμένου επιπέδου, καθώς και επίθεση υπερχείλισης μήκους. Για το δεύτερο επίπεδο, αυτό της μεταφοράς, οι επιθέσεις αφορούν αλλαγή σειράς και διακοπή κατακερματισμένου μηνύματος ενώ για το τρίτο επίπεδο, οι επιθέσεις ήταν τύπου μετατροπής κωδικού λειτουργίας καθώς και ειδικές με το πεδίο Εσωτερικών Ενδείξεων (Internal Indications – IIN). Στη συνέχεια, τα δεδομένα προεπεξεργάστηκαν, ενώ πραγματοποιήθηκε εξαγωγή ιδιοτήτων και τέλος εφαρμόσθηκαν διάφοροι αλγόριθμοι μηχανικής μάθησης. Τα αποτελέσματα δείχνουν ότι η προτεινόμενη μέθοδος κατάφερε να αναγνωρίσει και να ταξινομήσει τις επιθέσεις του συνόλου δεδομένων, καθώς και να παρέχει αναλυτικές πληροφορίες σχετικά με τα μέρη του DNP3 πακέτου τα οποία έχουν εκτεθεί.

Τέλος, οι Irvene κ.ά. [15] διαφωνούν με το γεγονός ότι οι λύσεις μηχανικής μάθησης είναι οι μοναδικές αποδεκτές μέθοδοι για την παραγωγή συστήματος ελέγχου εισβολών. Προτείνουν έναν ελαφρύ μηχανισμό αύξησης της ασφάλειας για υποσταθμούς που χρησιμοποιούν το DNP3. Συγκεκριμένα, συλλέχθηκαν και αναλύθηκαν δεδομένα από τέσσερις πραγματικούς

υποσταθμούς ενέργειας στην πάροδο 2.5 ετών. Από την ανάλυση των παραπάνω δεδομένων, προέκυψε ότι σε αντίθεση με πολλές υποθέσεις, η επικοινωνία των master και slave δεν είναι πολυποίκιλη σε ότι αφορά τους κωδικούς λειτουργίας του επιπέδου εφαρμογής. Λαμβάνοντας υπόψιν το παραπάνω γεγονός, χαρτογραφήθηκαν τα βασικά χαρακτηριστικά της φυσιολογικής κίνησης, τα οποία μπορούν να χρησιμοποιηθούν σαν κανόνας για σύστημα ελέγχου εισβολών. Τα χαρακτηριστικά αυτά αφορούν τον ενδιάμεσο χρόνο άφιξης πακέτων με τον ίδιο κωδικό λειτουργίας, πόσες φορές εμφανίζεται ένας συγκεκριμένος κωδικός λειτουργίας και τέλος πόσο εύκολα θα παράγει ειδοποιήσεις το σύστημα ελέγχου εισβολών, αν ανιχνευθεί κάποια απόκλιση.

3. Διαδικτυακές Επιθέσεις Ενάντια του Διανεμημένου Δικτυακού Πρωτοκόλλου 3

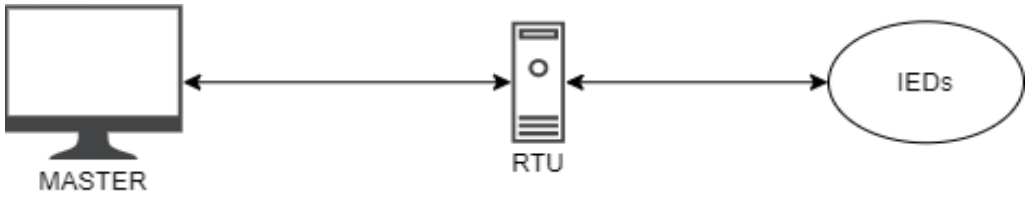
Σκοπός αυτό του κεφαλαίου είναι να παρουσιάσει μια εισαγωγή στο πρωτόκολλο DNP3 και στις εφαρμογές του, και κατόπιν να γίνει μια ανάλυση των επιθέσεων ενάντια στο DNP3.

3.1 Ανάλυση του Πρωτοκόλλου

Το DNP3, πρόκειται για ένα βιομηχανικό πρωτόκολλο SCADA το οποίο χρησιμοποιείται κυρίως σε εργοστάσια παραγωγής ηλεκτρικής ενέργειας [16], αλλά και στις βιομηχανίες νερού και πετρελαίου. Σύμφωνα με το [17], πάνω από το 75% των εργοστασίων ηλεκτρικής ενέργειας στη Βόρεια Αμερική χρησιμοποιεί το DNP3.

Το DNP3, εφαρμόζεται για την επικοινωνία μεταξύ των συσκευών που απαρτίζουν ένα έξυπνο ηλεκτρικό δίκτυο, όπως οι Απομακρυσμένες Μονάδες Τερματικού (Remote Terminal Units – RTUs), οι Master Stations και οι Ευφυείς Ηλεκτρονικές Συσκευές (Intelligent Electronic Devices – IEDs). Συγκεκριμένα, το πρωτόκολλο λειτουργεί ακολουθώντας λογική παρόμοια με αυτή του πελάτη-εξυπηρετητή, όπου ο πελάτης είναι ο Master Station και ο εξυπηρετητής είναι ο Outstation ή αλλιώς Slave. Σαν Slaves, θεωρούνται οι συσκευές που βρίσκονται στο πεδίο, ενώ σαν Masters θεωρούνται οι συσκευές ελέγχου των Slaves. Ο Master στέλνει αιτήματα στον Slave, ο οποίος με τη σειρά του απαντάει κατάλληλα σε αυτά τα αιτήματα. Ένας Master μπορεί να στέλνει αιτήματα σε πολλούς Slaves, και αντίστοιχα ένας Slave μπορεί να λαμβάνει αιτήματα από πάνω από έναν Master. Ένα κοινό αίτημα που πραγματοποιεί ένας Master, είναι αυτό του Polling, όπου απαιτεί από τον Slave να του στείλει τις τιμές των δεδομένων που έχει στη βάση δεδομένων του. Οι τιμές αυτές μπορεί να αναπαριστούν την κατάσταση μιας συσκευής, μετρήσεις κτλ.

Παρακάτω, παρουσιάζεται ένα παράδειγμα επικοινωνίας, στο οποίο το RTU συμπεριφέρεται σαν slave για τον master, και σαν master για τα IEDs.



Σχήμα 2: Παράδειγμα επικοινωνίας DNP3, με το RTU να συμπεριφέρεται σαν slave για τον master, και σαν master για τα IEDs

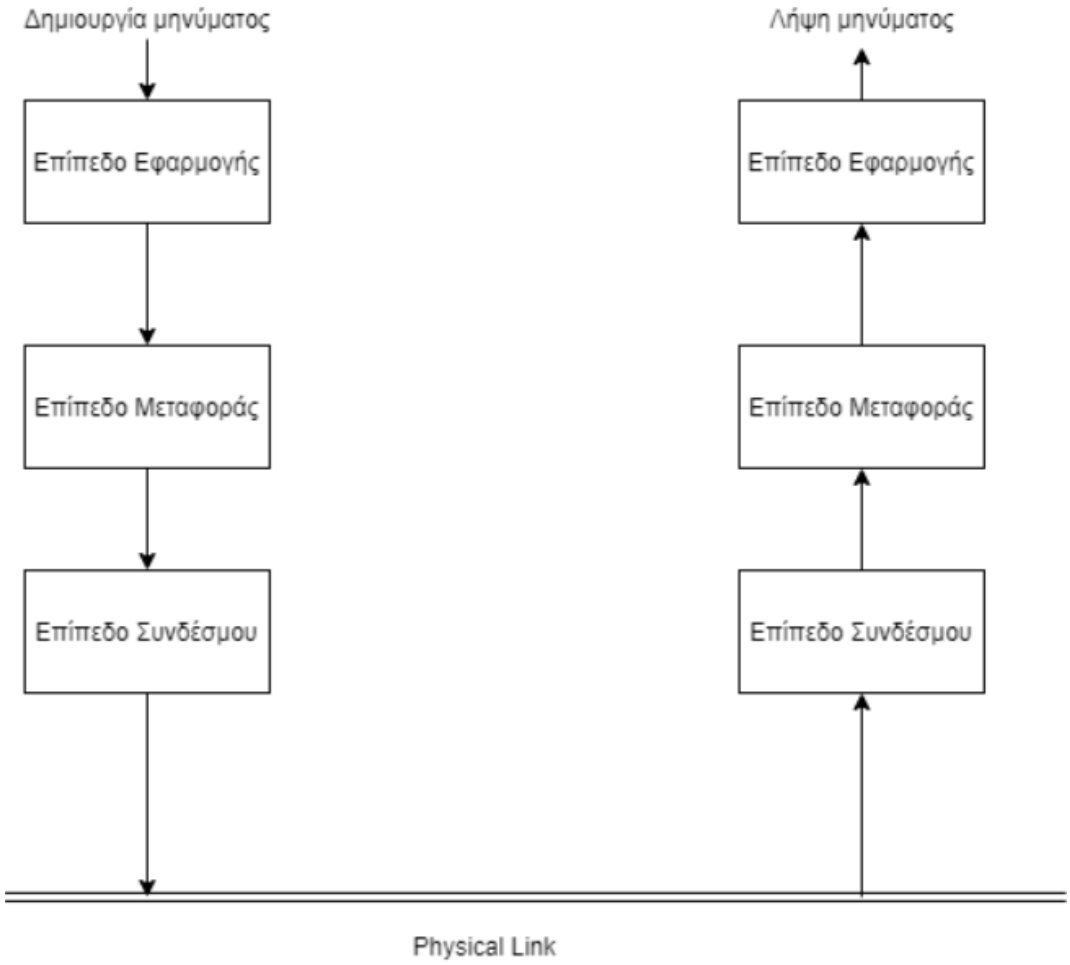
Το DNP3 δύναται να δουλεύει πάνω στο Πρωτόκολλο Ελέγχου Μετάδοσης/Πρωτόκολλο Διαδικτύου (Transmission Control Protocol/Internet Protocol - TCP/IP), ενώ συνήθως καταλαμβάνει τη θύρα 20000 του Πρωτοκόλλου Ελέγχου Μετάδοσης (Transmission Control Protocol – TCP). Σε ότι αφορά την αρχιτεκτονική του, χωρίζεται σε 3 επίπεδα, κάθε ένα από τα οποία εκτελεί ξεχωριστή λειτουργία.

- **Επίπεδο Συνδέσμου:** Σκοπός του επίπεδου συνδέσμου ή link layer, είναι η αποστολή και λήψη πακέτων, τα οποία αποκαλούνται «πλαίσια», καθώς το συγκεκριμένο επίπεδο λειτουργεί με παρόμοιο τρόπο με το Ethernet, ανιχνεύοντας πιθανά σφάλματα με υπολογισμό Κυκλικού Ελέγχου Πλεονασμού (Cyclic Redundancy Check – CRC). Πληροφορίες σχετικά με το πλαίσιο υπάρχουν στην κεφαλίδα συμπεριλαμβανομένου του πεδίου κωδικού λειτουργίας, που χρησιμοποιείται κυρίως για τον έλεγχο της κατάστασης του συνδέσμου (link), ενώ το φορτίο είναι τα δεδομένα που περνούν από τα ανώτερα επίπεδα του DNP3. Το επίπεδο συνδέσμου μπορεί να διαχειριστεί μέχρι και 250 bytes δεδομένων.
- **Επίπεδο Ψευδο-Μεταφοράς:** Το συγκεκριμένο επίπεδο δεν επιτελεί εργασίες μεταφοράς, αλλά διάσπασης πολύ μεγάλων πακέτων, τα οποία λαμβάνει από το επίπεδο εφαρμογής, σε μικρότερα κομμάτια, ή αλλιώς θραύσματα, με σκοπό να μπορέσει το επίπεδο συνδέσμου να τα μεταδώσει. Η κεφαλίδα του αποτελείται από στοιχεία σχετικά με τα θραύσματα, προκειμένου να επανασυναρμολογηθούν σωστά όταν φτάσουν στον προορισμό, όπως η σειρά του εκάστοτε θραύσματος και αν είναι το πρώτο ή το τελευταίο θραύσμα σε μια ακολουθία.
- **Επίπεδο εφαρμογής:** Το επίπεδο εφαρμογής ή αλλιώς application layer, είναι υπεύθυνο για τη δημιουργία των μηνυμάτων που θέλει να μεταδώσει ο Master ή ο Slave. Συγκεκριμένα, η κεφαλίδα του πακέτου θα διαφοροποιείται ανάλογα με την πηγή του

μηνύματος, καθώς η κάθε συσκευή έχει διαφορετικές απαιτήσεις. Το πεδίο των εσωτερικών ενδείξεων, βρίσκεται μόνο στα μηνύματα από τον Slave, και υπάρχει για να χαρακτηρίσει την κατάσταση του Slave.

Κάθε μήνυμα χαρακτηρίζεται και από κάποιον κωδικό λειτουργίας (function code), ενώ οι Masters και οι Slaves έχουν διαφορετικούς κωδικούς λειτουργίας. Ο συγκεκριμένος κωδικός, ορίζει τον τρόπο με τον οποίο η λαμβάνουσα συσκευή οφείλει να διαχειριστεί το μήνυμα. Για παράδειγμα, ο κωδικός εντολής 0x01 (READ), προέρχεται αποκλειστικά από τον Master, και απαιτεί από τον Slave να του επιστρέψει τα δεδομένα για τα αντικείμενα τα οποία αναφέρονται στο φορτίο του μηνύματος. Το επίπεδο εφαρμογής μπορεί να περιέχει δεδομένα, τα οποία ταξινομούνται σε ομάδες, και κάθε ομάδα αντιπροσωπεύει ένα είδος αντικειμένων. Τα κάθε είδος αντικειμένου, δηλαδή η κάθε ομάδα, διαχωρίζεται ανάλογα με τους τρόπους αναπαράστασης των δεδομένων της.

Στο παρακάτω σχήμα, απεικονίζεται η διαδικασία διαχειρισμού των DNP3 μηνυμάτων από όλα τα εμπλεκόμενα επίπεδα του DNP3, κατά τη διαδικασία αποστολής και λήψης του μηνύματος.



Σχήμα 3: Σχηματικά η διαδικασία αποστολής και λήψης μηνυμάτων από τα επίπεδα του DNP3

3.2 Επιθέσεις Ενάντια στο Διανεμημένο Δικτυακό Πρωτόκολλο 3

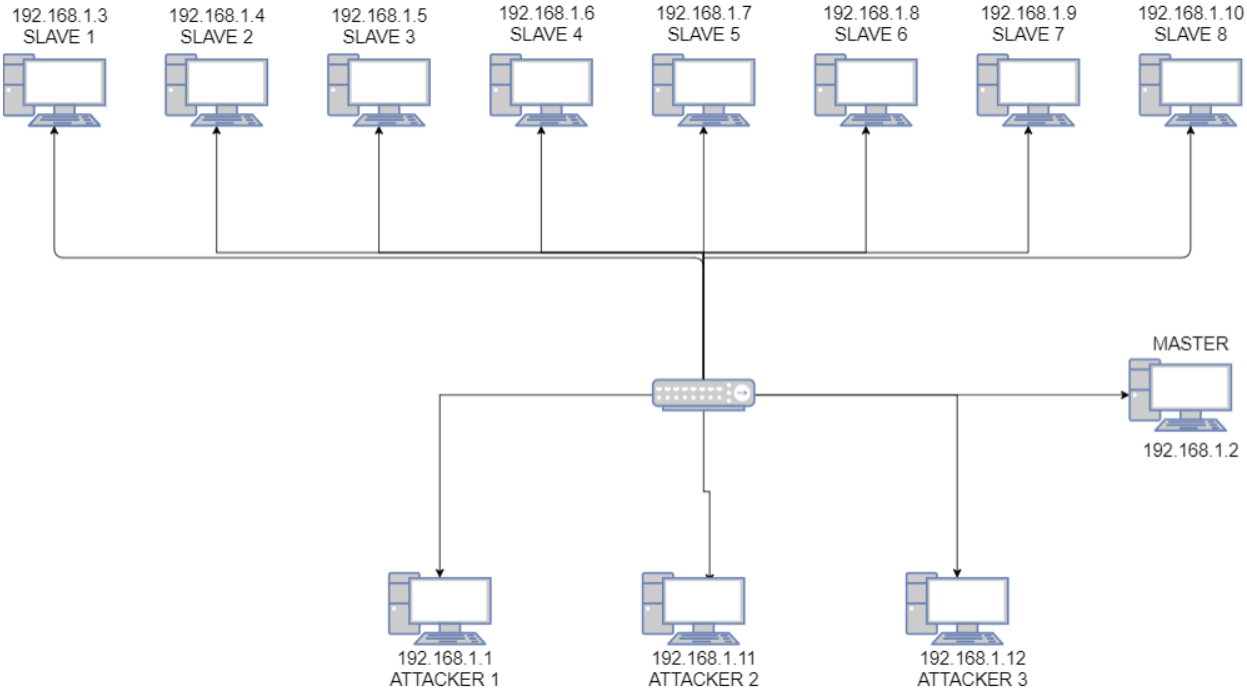
Σκοπός αυτού του κεφαλαίου είναι να παρουσιάσει επιθέσεις ενάντια στο DNP3. Οι επιθέσεις ενάντια σε συστήματα SCADA είναι ικανές να επιφέρουν σοβαρές επιπτώσεις, ως και καταστροφή, ακόμα και στο φυσικό επίπεδο των συσκευών [17]. Το DNP3, δεν έχει κατασκευαστεί λαμβάνοντας υπόψιν την ασφάλεια [18] συνεπώς υπάρχουν αρκετά κενά ασφαλείας τα οποία μπορεί να εκμεταλλευτεί κάποιος ο οποίος κατέχει γνώσεις σχετικά με τη λειτουργία του πρωτοκόλλου.

Οι επιθέσεις που αναλύονται παρακάτω, υλοποιήθηκαν στο πλαίσιο της συγκεκριμένης διπλωματικής εργασίας με σκοπό την δημιουργία ενός συνόλου δεδομένων εκπαίδευσης του νευρωνικού βαθιάς μάθησης, προκειμένου να συγκροτηθεί το τελικό σύστημα ανίχνευσης εισβολών. Για την προσομοίωση της επικοινωνίας ανάμεσα σε Master και Slave,

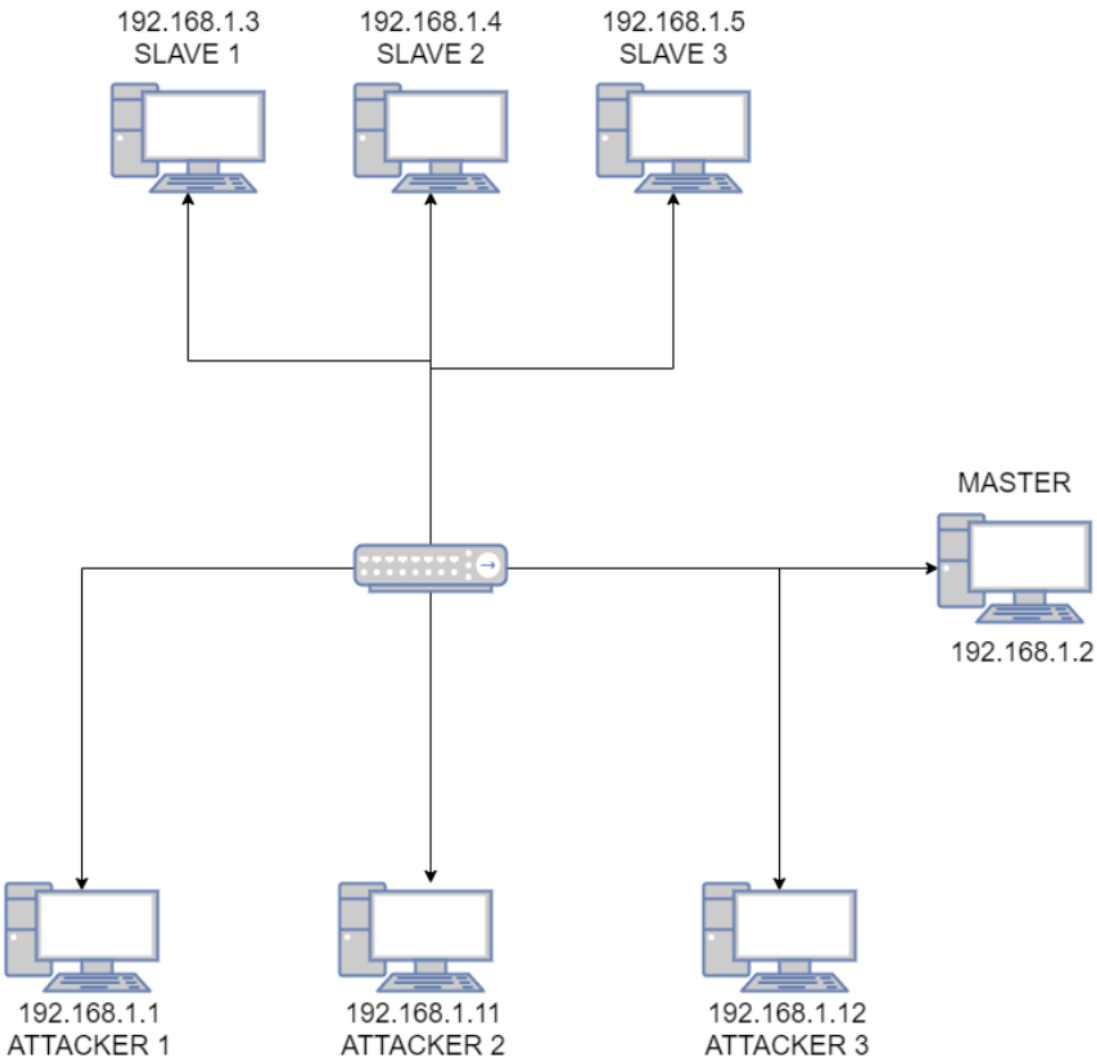
χρησιμοποιήθηκε το opendnp3 που πρόκειται για μια ανοιχτού κώδικα εφαρμογή του πρωτοκόλλου DNP3 γραμμένη σε C++, και συγκεκριμένα τα Master και Outstation Demos που παρέχει [19].

Για τον σκοπό του πειράματος, θεωρείται ότι οι επιτιθέμενοι έχουν αποκτήσει πρόσβαση στο δίκτυο των Slaves και Master.

Οι τοπολογίες που υλοποιήθηκαν για την εκτέλεση των επιθέσεων φαίνονται σχηματικά παρακάτω.



Σχήμα 4: Τοπολογία 01



Σχήμα 5: Τοπολογία 02

3.2.1 Επίθεση Απενεργοποίησης Μη Επιθυμητών Μηνυμάτων

Παραπάνω έγινε ανάλυση της σημασίας του κωδικού λειτουργίας στο επίπεδο εφαρμογής του DNP3. Έγινε αναφορά επίσης στο γεγονός ότι ο Slave στέλνει απαντήσεις, κατόπιν αιτήματος του Master. Σε περίπτωση που ο Slave ανιχνεύσει μια αντικανονικότητα, μπορεί να αποστείλει ένα μήνυμα για να ειδοποιήσει τον Master για αυτήν την αλλαγή, τα οποία μηνύματα λέγονται μη-επιθυμητές απαντήσεις (unsolicited responses) καθώς εστάλησαν χωρίς την πρωτοβουλία του Master.

Ο Master μπορεί να απενεργοποιήσει αυτή τη δυνατότητα του Slave, στέλνοντας σε αυτόν μήνυμα με κωδικό λειτουργίας επιπέδου εφαρμογής 21. Η συγκεκριμένη επίθεση

εκμεταλλεύεται το γεγονός ότι δεν υπάρχει πιστοποίηση κατά την αποστολή αιτήματος στον Slave από έναν μη εξουσιοδοτημένο πελάτη, το οποίο αίτημα ο Slave θα εκτελέσει και θα απαντήσει σε αυτό φυσιολογικά.

Για την επίθεση, χρησιμοποιήθηκε η τοπολογία 01, στο οποίο οι επιτιθέμενοι, συνδέονται σε κάθε Slave και στέλνουν αιτήματα απενεργοποίησης μη-επιθυμητών μηνυμάτων, τα οποία ο Slave δέχεται. Για τους σκοπούς δημιουργίας συνόλου δεδομένων με μεγάλο πλήθος κακόβουλων πακέτων, γίνεται αποστολή ενός αιτήματος απενεργοποίησης μη-επιθυμητών μηνυμάτων από όλους τους επιτιθέμενους, σε τυχαίο χρόνο ανά [20s,30s].

Παρακάτω, απεικονίζεται στιγμιότυπο οθόνης που προέκυψε από την καταγραφή ενός πακέτου επίθεσης, και της αντίστοιχης απάντησης.

```
192.168.1.11        192.168.1.10        DNP 3.0    90 Disable Spontaneous Messages
192.168.1.4         192.168.1.11        DNP 3.0    83 Response
```

Σχήμα 6: Παράδειγμα πακέτου απενεργοποίησης μη-επιθυμητών μηνυμάτων και απάντησης

3.2.2 Επίθεση Ψυχρής Επανεκκίνησης

Η διαδικασία της ψυχρής επανεκκίνησης, συμβαίνει όταν ο Master στείλει το κατάλληλο αίτημα με κωδικό λειτουργίας επιπέδου εφαρμογής 13 στο Slave, ο οποίος με τη σειρά του απαντά στο αίτημα και επανεκκινείται πλήρως ενώ κατόπιν εκτελεί διαδικασία αυτοελέγχων. Η επανεκκίνηση μπορεί να κρατήσει τον Slave σε μη ανταποκρίσιμη κατάσταση για κάποιο χρονικό διάστημα, το οποίο ίσως είναι ο απώτερος σκοπός ενός κακόβουλου χρήστη.

Η υλοποίηση της επίθεσης, ομοίως με παραπάνω, πραγματοποιήθηκε με χρήση της τοπολογίας 01 και του opendnp3, ενώ αποστέλλεται ένα πακέτο από κάθε επιτιθέμενο προς κάθε Slave, σε τυχαίο χρόνο, ανάμεσα στα [20s,30s].

Παρακάτω, απεικονίζεται στιγμιότυπο οθόνης που προέκυψε από την καταγραφή ενός πακέτου επίθεσης, και της αντίστοιχης απάντησης.

```
192.168.1.11        192.168.1.5         DNP 3.0    81 Cold Restart
192.168.1.6         192.168.1.11        DNP 3.0    83 Response
```

Σχήμα 7: Παράδειγμα πακέτου ψυχρής επανεκκίνησης και απάντησης

3.2.3 Επίθεση Θερμής Επανεκκίνησης

Η συγκεκριμένη επίθεση ακολουθεί την λογική της ψυχρής επανεκκίνησης, με την διαφορά ότι σε αυτή την περίπτωση ο Slave δεν πραγματοποιεί πλήρη επανεκκίνηση, αλλά επαναφέρει μόνο την εφαρμογή του DNP3 αφού απαντήσει στο αίτημα. Και σε αυτή την επίθεση ο Slave παραμένει μη ανταποκρίσιμος για κάποιο χρονικό διάστημα, ώσπου να πραγματοποιηθεί η διαδικασία.

Η υλοποίηση της επίθεσης, ομοίως και με τις παραπάνω, πραγματοποιήθηκε με χρήση της τοπολογίας 01 και του opendnp3, ενώ αποστέλλεται ένα πακέτο με κωδικό λειτουργίας επιπέδου εφαρμογής 14 από κάθε επιτιθέμενο προς κάθε Slave, σε τυχαίο χρόνο, ανάμεσα στα [20s,30s].

Παρακάτω, απεικονίζεται στιγμιότυπο οθόνης που προέκυψε από την καταγραφή ενός πακέτου επίθεσης, και της αντίστοιχης απάντησης.

```
192.168.1.11        192.168.1.4         DNP 3.0    81 Warm Restart
192.168.1.8         192.168.1.11        DNP 3.0    83 Response
```

Σχήμα 8: Παράδειγμα αιτήματος θερμής επανεκκίνησης και απάντησης

3.2.4 Απαρίθμηση Διευθύνσεων

Η συγκεκριμένη επίθεση πρόκειται για το DNP3 Enumerate Nmap Scripting Engine - NSE, στόχος του οποίου είναι να καθοριστεί εάν σε έναν host υπάρχει λειτουργία DNP3, ή αλλιώς αν η συγκεκριμένη διεύθυνση Πρωτοκόλλου Διαδικτύου (Internet Protocol – IP) και θύρα 20000 του TCP ανήκει σε κάποιον DNP3 Slave. Αυτό το πραγματοποιεί στέλνοντας στην IP του στόχου ένα DNP3 αίτημα με κωδικό λειτουργίας επιπέδου συνδέσμου 9 ή αλλιώς αίτημα κατάστασης συνδέσμου. Για να καθορίσει σε ποια διεύθυνση επιπέδου συνδέσμου λειτουργεί ο Slave, στέλνει το παραπάνω αίτημα σε 100 διευθύνσεις επιπέδου συνδέσμου για να ελέγξει από ποια θα λάβει απάντηση.

Η παραπάνω διαδικασία αναγνώρισης πραγματοποιείται στη τοπολογία 02, σε τυχαίο χρόνο στα [20s,30s].

Παρακάτω, απεικονίζεται στιγμιότυπο οθόνης που προέκυψε από την καταγραφή ενός πακέτου επίθεσης, και της αντίστοιχης απάντησης.

```
192.168.1.11        192.168.1.4         DNP 3.0  1076 from 0 to 100, len=5, Request Link Status
192.168.1.4         192.168.1.11        DNP 3.0    83 Unsolicited Response
```

Σχήμα 9: Παράδειγμα υλοποίησης NSE και απάντηση

3.2.5 Επίθεση Αναγνώρισης

Πρόκειται για επίθεση αναγνώρισης DNP3 Slaves στη θύρα 20000 σε μια IP, με χρήση του DNP3 info NSE. Ομοίως με παραπάνω, στέλνει αιτήματα στις 100 πρώτες διευθύνσεις επιπέδου συνδέσμου για να ελέγξει από ποια θα λάβει απάντηση.

Η διαδικασία αυτή επαναλαμβάνεται σε τυχαίο χρόνο στα [20s,30s] στη τοπολογία 02.

Παρακάτω, απεικονίζεται στιγμιότυπο οθόνης που προέκυψε από την καταγραφή ενός πακέτου επίθεσης, και της αντίστοιχης απάντησης.

```
192.168.1.11        192.168.1.4         DNP 3.0  1076 from 0 to 32916, len=64, Unknown function (0x0c)
192.168.1.4         192.168.1.11        DNP 3.0    83 Unsolicited Response
```

Σχήμα 10: Παράδειγμα υλοποίησης NSE και απάντηση

3.2.6 Επίθεση Αρχικοποίησης Δεδομένων

Ακολουθώντας ίδια λογική με τις επιθέσεις που αφορούν διάφορους κώδικες λειτουργίας, η συγκεκριμένη επίθεση αφορά τον κωδικό λειτουργίας επιπέδου εφαρμογής 15. Με την λήψη αιτήματος με τον συγκεκριμένο κωδικό και τα αντικείμενα προς αρχικοποίηση στο φορτίο, ο Slave επαναφέρει τα δεδομένα των συγκεκριμένων αντικειμένων στις προκαθορισμένες τιμές τους. Συνεπώς οι νέες τιμές δεν αντιπροσωπεύουν την πραγματική κατάσταση του συστήματος.

Στη συγκεκριμένη περίπτωση υλοποιήθηκε πρόγραμμα σε python με τη χρήση του NetfilterQueue, του scapy και της βιβλιοθήκης για DNP3 όπου τροποποιεί και επανεισάγει στην κίνηση ένα πακέτο με τον συγκεκριμένο κωδικό λειτουργίας στον Slave [20]. Η επίθεση αφορά τροποποίηση της φυσιολογικής κίνησης σε κίνηση επίθεσης, ανά [20s,30s]. Για την επίθεση, χρησιμοποιήθηκε το σχήμα τοπολογίας 02.

Παρακάτω, απεικονίζεται στιγμιότυπο οθόνης που προέκυψε από την καταγραφή ενός πακέτου επίθεσης, και της αντίστοιχης απάντησης.

```
192.168.1.11        192.168.1.4         DNP 3.0    84 Initialize Data
192.168.1.4         192.168.1.11        DNP 3.0    83 Response
```

Σχήμα 11: Παράδειγμα αιτήματος αρχικοποίησης δεδομένων και απάντησης

3.2.7 Επίθεση Τερματισμού Εφαρμογής

Η συγκεκριμένη επίθεση αφορά τον κωδικό λειτουργίας επιπέδου εφαρμογής 18, ο οποίος απαιτεί από τον Slave να τερματίσει την λειτουργία της εφαρμογής και συνεπώς να μην ανταποκρίνεται πλέον σε αιτήματα από τον Master. Σαν αποτέλεσμα, προκαλείται DoS.

Για την υλοποίηση της επίθεσης, χρησιμοποιήθηκε πρόγραμμα σε python, που με χρήση του NetfilterQueue, του scapy και της βιβλιοθήκης scapy για DNP3, τροποποιεί ένα πακέτο φυσιολογικής κίνησης, σε πακέτο με το συγκεκριμένο κωδικό λειτουργίας, και το εισάγει πάλι στην κίνηση. Η επίθεση αφορά τροποποίηση της φυσιολογικής κίνησης σε κίνηση επίθεσης, ανά [20s,30s]. Για την επίθεση, χρησιμοποιήθηκε η τοπολογία του σχήματος 02.

Παρακάτω, απεικονίζεται στιγμιότυπο οθόνης που προέκυψε από την καταγραφή ενός πακέτου επίθεσης, και της αντίστοιχης απάντησης.

```
192.168.1.11        192.168.1.4         DNP 3.0    93 Stop Application
192.168.1.4         192.168.1.11        DNP 3.0    83 Response
```

Σχήμα 12: Παράδειγμα αιτήματος τερματισμού εφαρμογής και απάντησης

3.2.8 Επίθεση Επανάληψης

Σκοπός της συγκεκριμένης επίθεσης είναι η επανάληψη ή η καθυστέρηση της μετάδοσης ενός μη κακόβουλου πακέτου, το οποίο προέρχεται από νόμιμη πηγή. Προκειμένου να επιτευχθεί η επίθεση, απαιτείται πρωτίστως να βρεθεί κάποια μέθοδος MiTM προκειμένου ο επιτιθέμενος να μπορέσει να «κρυφακούσει» την κίνηση, την οποία θα αποθηκεύει και στη συνέχεια θα επαναλαμβάνει ή θα καθυστερεί τη μετάδοσή της.

Για την εκτέλεση της επίθεσης, χρησιμοποιήθηκε η τοπολογία 02. Αρχικά, πραγματοποιήθηκε MiTM επίθεση με δηλητηρίαση Πρωτοκόλλου Επίλυσης Διευθύνσεων (Address Resolution Protocol – ARP) προκειμένου ο επιτιθέμενος να έχει πρόσβαση στην επικοινωνία μεταξύ του Master και του εκάστοτε Slave. Αν και υπάρχουν αρκετά διαθέσιμα εργαλεία που εκτελούν επίθεση επανάληψης, υλοποιήθηκε πρόγραμμα σε python που αναλαμβάνει να καθυστερήσει την μετάδοση ενός πακέτου που προέρχεται από τον Master κατά τυχαία επιλεγμένο χρόνο που κυμαίνεται στα [5s,10s].

4. Μηχανική Μάθηση για τη Διάκριση Ανωμαλιών

Η μηχανική μάθηση αφορά την ανάπτυξη προγραμμάτων ικανών να βελτιώνονται αυτόματα, με βάση τα δεδομένα εκπαίδευσης. Τα δεδομένα εκπαίδευσης είναι αναλυτικές πληροφορίες χαρακτηριστικών ή αλλιώς, ιδιότητες (features) σχετικά με μια κατάσταση που οφείλει να μάθει το πρόγραμμα. Κατά τη διάρκεια της εκπαίδευσης γίνεται αναζήτηση για μοτίβα μέσα στα δεδομένα εκπαίδευσης προκειμένου να λαμβάνονται καλύτερες αποφάσεις χωρίς να απαιτείται ανθρώπινη παρέμβαση. Το αποτέλεσμα της μηχανικής μάθησης, είναι το μοντέλο. Με την ολοκλήρωση της διαδικασίας εκπαίδευσης, πραγματοποιείται έκθεση του μοντέλου σε δεδομένα τα οποία δεν έχει ξαναδεί, τα δεδομένα επιβεβαίωσης [21], προκειμένου να αξιολογηθεί η απόδοσή του, ή με άλλα λόγια γίνεται έλεγχος του πόσο καλά έμαθε να αξιολογεί τα μοτίβα που αναγνώρισε. Μόλις εξαχθεί το επιθυμητό μοντέλο, μπορεί να δεχθεί και να αναγνωρίσει πραγματικά δεδομένα, με βάση την εκπαίδευσή του.

4.1 Κατηγορίες Μηχανικής Μάθησης

Η μηχανική μάθηση μπορεί να διακριθεί σε τρείς κατηγορίες. Η επιλογή κατηγορίας προκύπτει ανάλογα με τη φύση του προβλήματος και τα δεδομένα εκπαίδευσης.

- **Επιβλεπόμενη μάθηση:** Σε αυτήν την κατηγορία, τα δεδομένα εκπαίδευσης είναι χωρισμένα σε δεδομένα εισόδου (input data) και στα αντίστοιχα δεδομένα εξόδου (output data). Η έξοδος είναι το επιθυμητό αποτέλεσμα που αναμένεται από το μοντέλο στη συγκεκριμένη είσοδο. Ένα σωστά εκπαιδευμένο μοντέλο συσχετίζει με μεγάλη ακρίβεια τις μη-ταυτοποιημένες εισόδους πραγματικών δεδομένων, με τις συγκεκριμένες εξόδους που προσδιορίστηκαν στη διαδικασία εκμάθησης από τα δεδομένα επιθυμητής εξόδου [22]. Για την υλοποίηση του προγράμματος αυτής της διπλωματικής εργασίας, θα χρησιμοποιηθεί επιβλεπόμενη μάθηση.
- **Μη επιβλεπόμενη μάθηση:** Σε αντίθεση με την επιβλεπόμενη μάθηση, σε αυτήν την κατηγορία δεν ορίζονται οι επιθυμητές έξοδοι κατά τη διαδικασία την εκπαίδευσης. Ο αλγόριθμος επικεντρώνεται στην αναζήτηση μοτίβων και χαρακτηριστικών μέσα στα δεδομένα εκπαίδευσης, τα οποία είναι χρήσιμα για την μετέπειτα κατηγοριοποίησή τους. Ένα παράδειγμα μη επιβλεπόμενης μάθησης αποτελεί αυτό της ομαδοποίησης, όπου αναζητούνται κοινά σημεία μέσα στα δεδομένα,

προκειμένου τα παρόμοια μεταξύ τους δεδομένα να ομαδοποιηθούν σε μια ομάδα [23].

- **Ενισχυτική μάθηση:** Σε αυτή την κατηγορία, η εκμάθηση πραγματοποιείται από την αλληλεπίδραση με το περιβάλλον, και από την βαθμολόγηση της κάθε πράξης. Κάθε κίνηση, επιφέρει αλλαγή του περιβάλλοντος και της αποδίδεται μια ανταμοιβή ανάλογα με την ποιότητα της παραγόμενης κατάστασης [24].

4.2 Ταξινόμηση

Οι πιο κοινές κατηγορίες επιβλεπόμενης μάθησης, είναι η ταξινόμηση (classification) και η οπισθοδρόμηση (regression). Ανάλογα με τις απαιτήσεις του κάθε προβλήματος επιβλεπόμενης μάθησης, επιλέγεται η κατάλληλη προσέγγιση. Σε αυτή τη διπλωματική εργασία, εφαρμόστηκε επιβλεπόμενη μάθηση με ταξινόμηση.

Το πρόβλημα της ταξινόμησης στη μηχανική μάθηση, αφορά την εύρεση τρόπου κατηγοριοποίησης δεδομένων σε διάφορες κλάσεις οι οποίες έχουν οριστεί κατά την εκπαίδευση. Παραδείγματα ταξινόμησης αποτελούν η εύρεση τρόπου αναγνώρισης είδους ζώων, ή η κατάταξη γνωστών αντικειμένων σε μια φωτογραφία.

Η ταξινόμηση χωρίζεται σε δυαδική, πολυ-ταξική και πολλών ετικετών.

- **Δυαδική ταξινόμηση:** Σε αυτήν την κατηγορία, κατατάσσονται τα προβλήματα που ξεχωρίζουν δύο επιθυμητές κλάσεις για τα δεδομένα εισόδου. Για παράδειγμα, η κατηγοριοποίηση δικτυακής κίνησης σε φυσιολογική ή μη φυσιολογική.
- **Πολυ-ταξική ταξινόμηση:** Στη συγκεκριμένη κατηγορία, οι ανάγκες του προβλήματος απαιτούν μη δυαδικό χαρακτηρισμό για τα δεδομένα εισόδου. Συνεπώς σε αυτήν την κατηγορία κατατάσσονται τα προβλήματα που χαρακτηρίζονται από πάνω από δύο κλάσεις. Στο παράδειγμα της κατηγοριοποίησης δικτυακής κίνησης, οι κλάσεις θα μπορούσαν να είναι όσες και οι επιθέσεις που υλοποιήθηκαν, συν η κλάση της φυσιολογικής κίνησης (εάν υφίσταται). Σε αυτή τη διπλωματική εργασία, χρησιμοποιήθηκε πολυ-ταξική ταξινόμηση.
- **Ταξινόμηση πολλών ετικετών:** Η συγκεκριμένη κατηγορία χρησιμοποιείται όταν τα δεδομένα πρέπει να χαρακτηριστούν από πάνω από μια κλάση.

4.2.1 Ταξινομητές

Σαν ταξινομητής, ορίζεται οποιοσδήποτε αλγόριθμος μηχανικής μάθησης που μπορεί να κατανέμει τα δεδομένα στις κατάλληλες κλάσεις.

4.2.1.1 Ταξινομητής Naïve Bayes

Ο ταξινομητής Naïve bayes, είναι βασισμένος στο θεώρημα του Bayes, το οποίο υποστηρίζει ότι είναι εφικτός ο υπολογισμός της πιθανότητας πραγματοποίησης ενός γεγονότος Α, αν συνέβη το γεγονός Β. Το θεώρημα αυτό εκφράζεται μέσα από τον εξής τύπο, ο οποίος απεικονίζεται παρακάτω :

$$P(A|B) = \frac{\mathrm{P(B|A)P(A)}}{P(B)} \qquad (4.1)$$

Όπου το P(A|B) είναι η πιθανότητα το Α να είναι αληθές, αν το Β είναι αληθές και αντίστοιχα P(B|A) είναι η πιθανότητα το Β να είναι αληθές, αν το Α είναι αληθές. P(A) είναι η πιθανότητα το Α να είναι αληθές, και P(B) είναι η πιθανότητα το Β να είναι αληθές.

Στη μηχανική μάθηση, σαν Α θα θεωρηθεί η κλάση, ή αλλιώς η έξοδος που αναμένεται αν ο αλγόριθμος δεχτεί σαν είσοδο τα δεδομένα Β.

4.2.1.2 Ταξινομητής Δένδρου Απόφασης

Ο ταξινομητής δένδρου απόφασης, ή αλλιώς Decision Tree Classifier, μπορεί να απεικονισθεί σαν ένα δένδρο, στο οποίο κάθε τελικός κόμβος (κόμβος χωρίς "παιδιά" ή αλλιώς φύλλο του δένδρου) αναπαριστά τις κλάσεις στις πρόκειται να ταξινομηθούν τα δεδομένα. Ο τρόπος με τον οποίο καταλήγει ο αλγόριθμος στα τελικά φύλλα είναι ο εξής : Κάθε εσωτερικός κόμβος, αποτελεί μια συνθήκη, η οποία προκύπτει από τις ιδιότητες (features) των δεδομένων εισόδου. Ο κάθε κόμβος μπορεί να έχει μέχρι και 2 παιδιά (binary tree), ενώ η επιλογή παιδιού γίνεται ανάλογα με το αν η συνθήκη είναι True (αληθείς) ή False (ψευδής) [25].

Τα δένδρα απόφασης είναι από τους πιο διαδεδομένους ταξινομητές λόγω της υψηλής ακρίβειας (accuracy) που μπορούν να δώσουν, και της απλότητας τους, ενώ είναι εύκολο να γίνει ορατό το παραγόμενο δένδρο.

4.2.1.3 Ταξινομητής Τυχαίου Δάσους

Ο ταξινομητής τυχαίου δάσους, ή Random Forest classifier μπορεί να θεωρηθεί επέκταση του δένδρου απόφασης. Αντί να λαμβάνονται υπόψιν τα αποτελέσματα από μόνο ένα δένδρο, ο ταξινομητής τυχαίου δάσους υλοποιεί πολλά δένδρα, όπου παίρνει από το κάθε ένα τα τελικά αποτελέσματα, τα οποία συμψηφίζει προκειμένου να καταλήξει στην τελική ταξινόμηση. Ο τρόπος συμψηφισμού είναι αυτός της πλειοψηφίας στα προβλήματα ταξινόμησης [26]. Η μέθοδος με την οποία διαφοροποιούνται τα δένδρα μεταξύ τους στις εσωτερικές συνθήκες και αποφάσεις, είναι η εισαγωγή διαφορετικών, τυχαία επιλεγμένων δειγμάτων δεδομένων εκπαίδευσης.

4.2.1.4 Τεχνητά Νευρωνικά Δίκτυα

Τα ANN αποτελούν μια μέθοδο μηχανικής μάθησης εμπνευσμένη από τη διαδικασία μάθησης που ακολουθεί ο άνθρωπος. Όταν ένας άνθρωπος πραγματοποιεί μια εργασία, πυροδοτούνται νευρώνες στον εγκέφαλο του, ενώ με την επανάληψη της διαδικασίας, οι “δεσμοί” των νευρώνων γίνονται πιο ισχυροί με αποτέλεσμα να έχει καλύτερη απόδοση. Με τον ίδιο τρόπο πραγματοποιείται η εκπαίδευση ενός μοντέλου με χρήση νευρωνικού δικτύου. Συγκεκριμένα, τα νευρωνικά δίκτυα αποτελούνται από στοιβάδες (layers) νευρώνων. Δεν υπάρχει περιορισμός στον αριθμό των νευρώνων που μπορεί να περιέχει ένα επίπεδο. Είναι σύνηθες οι νευρώνες του κάθε επιπέδου να είναι πλήρως συνδεδεμένοι με όλους τους νευρώνες του επόμενου επιπέδου. Η αρχιτεκτονική ενός νευρωνικού αποτελείται από τα εξής επιμέρους στοιχεία:

1. **Είσοδος (input) :** Σε αυτό το σημείο εισάγουμε τα δεδομένα εκπαίδευσης στο νευρωνικό. Οι είσοδοι θα είναι τόσοι σε πλήθος, όσες και οι ιδιότητες (features) των δεδομένων εκπαίδευσης.
2. **Κρυφά επίπεδα (hidden layers) :** Εδώ βρίσκεται η ουσία των νευρωνικών δικτύων. Ένας νευρώνας χαρακτηρίζει τα δεδομένα ανάλογα με το βάρος και το bias. Τα βάρη θεωρούνται η ισχύς της σύνδεσης μεταξύ των κόμβων και είναι αυτά που καθορίζουν το αποτέλεσμα του νευρωνικού. Το bias, είναι η δεύτερη είσοδος που λαμβάνει ο νευρώνας, και αντιστοιχεί συνήθως στην τιμή 1 ενώ πολλαπλασιάζεται με το βάρος του [27].

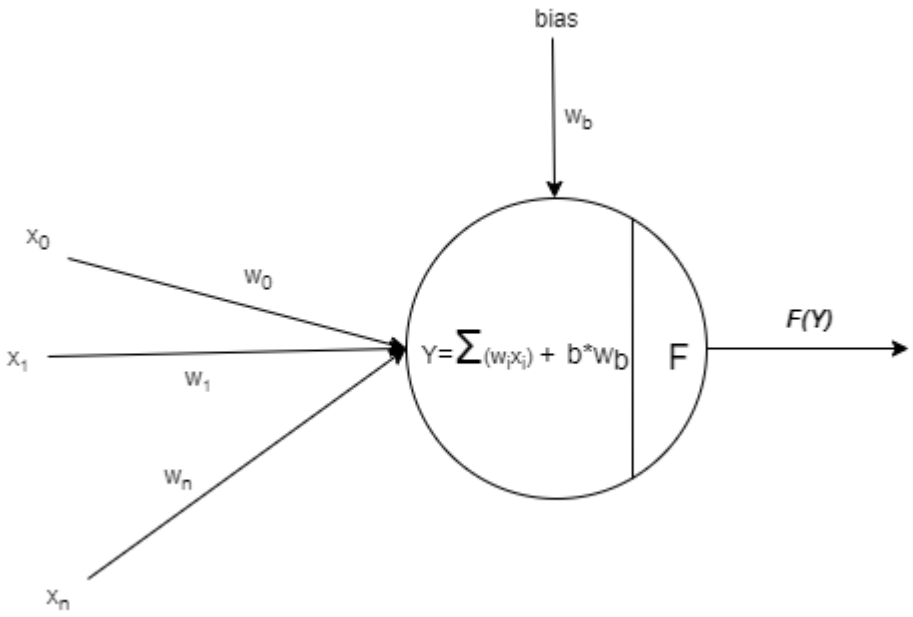
   Ο κάθε νευρώνας αναλύει τα δεδομένα με τον εξής τρόπο: Δέχεται σαν είσοδο σήματα από τη προηγούμενη στοιβάδα, και για κάθε είσοδο που λαμβάνει, την πολλαπλασιάζει

με το αντίστοιχο βάρος της. Στη συνέχεια, προσθέτει στο παραπάνω άθροισμα την τιμή του bias επί το βάρος του. Η συνάρτηση αυτή αποκαλείται net input. Κατόπιν, τροφοδοτείται το αποτέλεσμα σε μια συνάρτηση ενεργοποίησης (activation function) , εργασία της οποίας είναι να καθορίσει αν ο νευρώνας μπορεί να ενεργοποιηθεί η όχι, ανάλογα με το αν το αποτέλεσμά της ξεπερνά ένα κατώφλι.

Παρακάτω απεικονίζονται οι συναρτήσεις του net input καθώς και της εξόδου του νευρώνα, ενώ το σχεδιάγραμμα περιγράφει σχηματικά τη διαδικασία που ακολουθείται στο εσωτερικό του νευρώνα.

$$Y_i = \sum_i w_i x_i + b \times w_b \qquad (4.2)$$

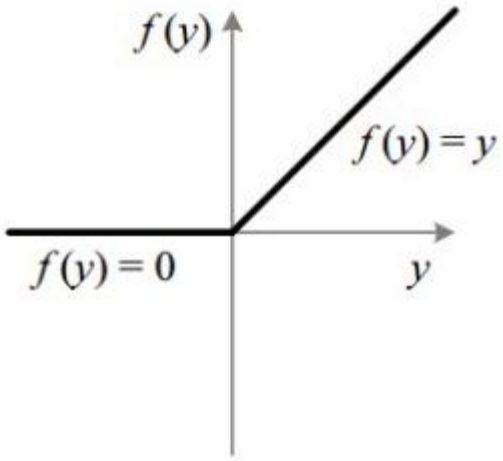
$$output = f(Y_i) \qquad (4.3)$$



Σχήμα 13: Παράδειγμα επεξεργασίας δεδομένων από έναν νευρώνα κρυφού επιπέδου

Η πιο συχνή συνάρτηση ενεργοποίησης είναι η ReLU,η οποία αναπαρίσταται από τον εξής τύπο:

$$f(y) = \begin{cases} 0, & y \leq 0 \\ y, & y > 0 \end{cases} \qquad (4.4)$$



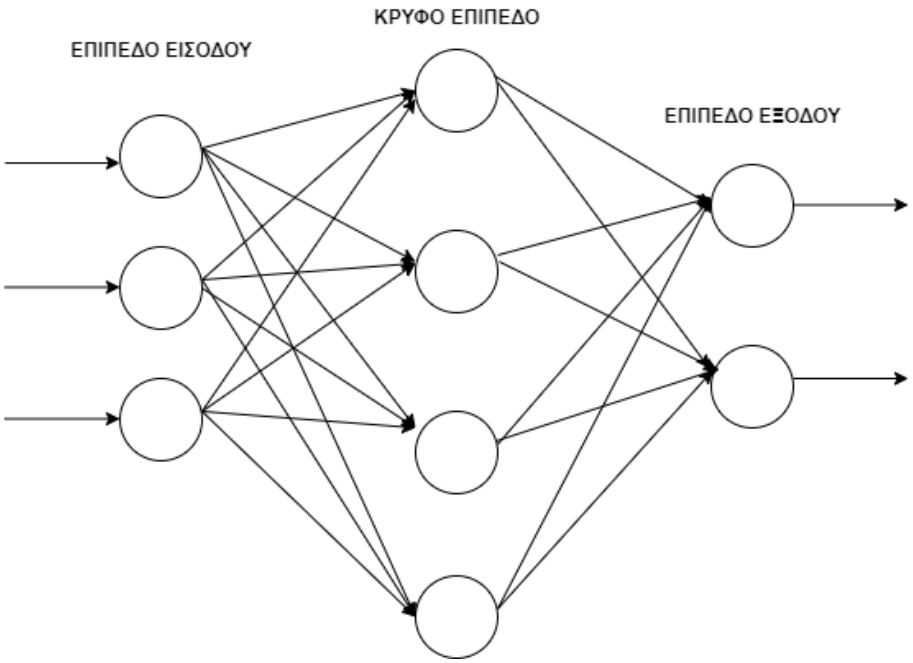
Σχήμα 14: Γραφική αναπαράσταση συνάρτησης ReLU [19]

Η έξοδος του νευρώνα θα είναι το αποτέλεσμα της συνάρτησης ενεργοποίησης, το οποίο μεταβιβάζει σε όλους τους νευρώνες της επόμενης στοιβάδας με τους οποίους είναι συνδεδεμένος.

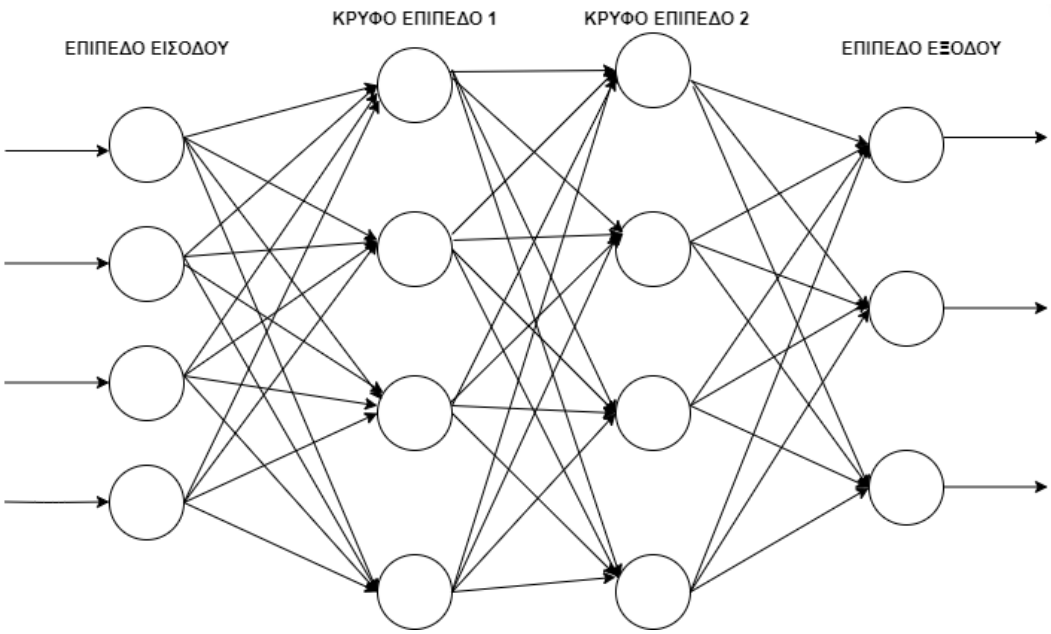
3. **Έξοδος(output) :** Το επίπεδο εξόδου, είναι η τελική στοιβάδα ενός νευρωνικού δικτύου. Συγκροτείται από έναν νευρώνα ή πλήθος νευρώνων που ισούνται με τον αριθμό των κλάσεων ταξινόμησης δεδομένων, ανάλογα με τη συνάρτηση ενεργοποίησης που θα χρησιμοποιηθεί και με τις ανάγκες του προβλήματος.

Τα ANNs διακρίνονται σε ρηχά (shallow) και βαθιά (deep). Ρηχά θεωρούνται όταν υπάρχει μόνο ένα κρυφό επίπεδο, ενώ ως Βαθιά Νευρωνικά Δίκτυα (Deep Neural Network - DNN) χαρακτηρίζονται όσα διαθέτουν πάνω από ένα κρυφό επίπεδο. Το μεγαλύτερο πλήθος των κρυφών επιπέδων δίνει τη δυνατότητα στο μοντέλο να ανακαλύπτει και να αφομοιώνει πιο περίπλοκα μοτίβα στις ιδιότητες (features) των δεδομένων εισόδου [28].

Στα παρακάτω σχήματα, απεικονίζεται ένα ρηχό ANN και ένα DNN με 2 κρυφά επίπεδα.



Σχήμα 15: Παράδειγμα ρηχού ANN με 1 κρυφό επίπεδο



Σχήμα 16: Παράδειγμα από βαθύ ANN (DNN) με 2 κρυφά επίπεδα

4.2.1.5 Ταξινομητής K-Nearest Neighbor

Ο K-Nearest Neighbor ακολουθεί την ιδεολογία πως πανομοιότυπα αντικείμενα, δηλαδή αντικείμενα που ανήκουν στην ίδια κλάση, βρίσκονται σε κοντινή απόσταση μεταξύ τους. Ο υπολογισμός της απόστασης μπορεί να πραγματοποιηθεί με την ευκλείδεια απόσταση, της οποίας ο τύπος αναγράφεται παρακάτω.

$$E(x, y) = \sqrt{\sum_{i=0}^{n}(x_i - y_i)^2} \qquad (4.5)$$

4.3 Μέτρα Αξιολόγησης

Μετά το πέρας της εκπαίδευσης ενός αλγορίθμου μηχανικής μάθησης, σειρά έχουν οι προβλέψεις. Αναλυτικότερα, γίνεται εισαγωγή δεδομένων στο μοντέλο, δεδομένα τα οποία δεν έχει ξαναδεί, τα δεδομένα αξιολόγησης, τα οποία υπόκεινται την ίδια προεπεξεργασία με τα δεδομένα εκπαίδευσης. Στόχος είναι, να προβλεφθεί η σωστή ταξινόμηση για τα δεδομένα αυτά. Η αξιολόγηση για το αν το μοντέλο προέβλεψε σωστά τις κλάσεις των δεδομένων αξιολόγησης, μπορεί να πραγματοποιηθεί με τις παρακάτω μετρήσεις.

4.3.1 Ακρίβεια

Η πιο εύκολα κατανοητή μέθοδος αξιολόγησης, προκύπτει από τη διαίρεση του συνόλου των δεδομένων για τα οποία το μοντέλο προέβλεψε σωστά την κλάση, προς τον συνολικό αριθμό των προβλέψεων.

Ο τύπος της ακρίβειας αναγράφεται παρακάτω.

$$Ακρίβεια = \frac{σωστές\ προβλέψεις}{συνολικός\ αριθμός\ προβλέψεων} \qquad (4.6)$$

4.3.2 Ορθότητα

Η ορθότητα, υπολογίζει την ορθότητα πρόβλεψης μιας κλάσης, προς το σύνολο προβλέψεων που ταξινόμησαν δεδομένα σε αυτή την κλάση. Με άλλα λόγια, το σύνολο των σωστών προβλέψεων για μια κλάση K, προς το σύνολο των προβλέψεων για αυτήν την κλάση K.

Ο τύπος της ορθότητας αναγράφεται παρακάτω.

$$Ορθότητα = \frac{σωστές\ προβλέψεις\ K}{σύνολο\ προβλέψεων\ K} \quad (4.7)$$

4.3.3 Ανάκληση

Η ανάκληση, υπολογίζει πόσα από τα δεδομένα που ταξινομήθηκαν σε μια κλάση, ανήκουν όντως σε αυτή την κλάση. Η αλλιώς, μετράει το σύνολο των προβλέψεων για μια κλάση K, προς το σύνολο των δεδομένων που ανήκουν στην κλάση K.

Ο τύπος της ανάκλησης αναγράφεται παρακάτω.

$$Ανάκληση = \frac{σύνολο\ προβλέψεων\ K}{σύνολο\ δεδομένων\ που\ πραγματικά\ ανήκουν\ στην\ K} \quad (4.8)$$

4.3.4 F1 Score

Το F1 score είναι χρήσιμο καθώς συνδυάζει και την ορθότητα και την ανάκληση. Ο τύπος που τον εκφράζει αναγράφεται παρακάτω.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recal} \quad (4.9)$$

5. Ανάλυση Συστήματος Ανίχνευσης Εισβολών Medium

Στο συγκεκριμένο κεφάλαιο, παρουσιάζονται αναλυτικά τα επιμέρους στοιχεία που συνέθεσαν στο τελικό σύστημα ανίχνευσης εισβολών ενάντια στο DNP3, με όνομα Medium, ενώ περιγράφεται η λειτουργία του από άποψη αρχιτεκτονικής, καταγραφής κίνησης και εξαγωγής αποτελεσμάτων. Επιπροσθέτως, πραγματοποιείται συγκριτική ανάλυση μοντέλων που προέκυψαν με χρήση διάφορων ταξινομητών μηχανικής μάθησης.

5.1 Ανάλυση Κίνησης σε Ροές

Σύμφωνα με το Request For Comments (RFC) 2722 [29], η λειτουργία της δικτυακής ροής, μπορεί να παρομοιαστεί με την λογική μιας τηλεφωνικής κλήσης. Υπάρχει μια πηγή, ένας προορισμός, έναρξη και λήξη της κλήσης, και δεδομένα που ανταλλάσσονται κατά τη διάρκειά της. Παρακάτω, παρουσιάζεται το πρόγραμμα που υλοποιήθηκε για τον σκοπό ανάλυσης της κίνησης σε DNP3 ροές, αλλά και το πρόγραμμα ανάλυσης κίνησης σε TCP/IP ροές, CICFlowMeter, για σκοπούς σύγκρισης μοντέλων.

5.1.1 Ανάλυση Κίνησης σε Ροές Διανεμημένου Δικτυακού Πρωτοκόλλου 3

Πρωταρχικό μέλημα για την υλοποίηση του συστήματος ελέγχου εισβολών που χρησιμοποιεί ως βάση τον έλεγχο δικτυακών ροών, αποτελεί η δημιουργία ενός python3 προγράμματος που όχι μόνο θα καταχωρεί τα πακέτα της δικτυακής κίνησης σε DNP3 ροές, αλλά και θα εξάγει για κάθε μια στατιστικές ιδιότητες που την εκφράζουν, με χρήση του εργαλείου scapy για τον διαμελισμό των πακέτων, και συγκεκριμένα τη βιβλιοθήκη DNP3 για scapy [30] [31].

Στόχος του προγράμματος ανάλυσης κίνησης σε ροές, είναι η καταχώρηση πακέτων πρωτοκόλλου DNP3 σε αμφίδρομες ροές, δηλαδή σε ροές όπου υπάρχει επικοινωνία με τη μορφή αποστολής ερωτήματος και απάντησης.

Θεωρώντας ότι υπάρχει διαθέσιμο αρχείο Καταγραφής Πακέτου (Packet Capture - .pcap), η ανάλυση της κίνησης ξεκινά παίρνοντας το πρώτο DNP3 πακέτο της λίστας πακέτων. Πραγματοποιείται στη συνέχεια αναζήτηση στην υπόλοιπη λίστα για DNP3 πακέτα με τα ίδια χαρακτηριστικά IP πηγής και προορισμού, και θύρας πηγής και προορισμού με αυτά του πρώτου πακέτου ή και με αντεστραμμένα χαρακτηριστικά, όπως αναμένεται να υπάρχουν σε μια αμφίδρομη επικοινωνία. Σε περίπτωση που βρεθούν αντιστοιχήσεις στα κριτήρια αναζήτησης,

εξάγονται για κάθε πακέτο συγκεκριμένες ιδιότητες χρόνου, μεγέθους, ιδιοτήτων πρωτοκόλλου και προστίθενται σε κατάλληλες λίστες.

Ο επιτρεπτός χρόνος διάρκειας μιας ροής ορίζεται στα δύο λεπτά. Σε περίπτωση που μια ροή διακοπεί λόγω του παραπάνω κατωφλιού ενώ υπάρχουν περεταίρω πακέτα στη λίστα που να αντιστοιχίζονται από άποψη χαρακτηριστικών με το πρώτο πακέτο, θα καταχωρηθούν σε διαφορετική ροή.

Μόλις ολοκληρωθεί η διαδικασία κατάταξης πακέτων εντός του επιτρεπόμενου χρόνου σε μια ροή, εξάγονται στατιστικά στοιχεία με βάση τις ιδιότητες που συλλέχθηκαν από κάθε πακέτο της ροής. Τα αποτελέσματα της παραπάνω διαδικασίας καταγράφονται σε αρχείο Τιμών Διαχωρισμένων με Κόμμα (Comma Separated Values - .csv).

Στο Παράρτημα Ι, παρουσιάζεται ο πίνακας των στατιστικών με μια συνοπτική περιγραφή του κάθε ενός.

5.1.2 Ανάλυση Κίνησης σε Ροές Πρωτοκόλλου Ελέγχου Μετάδοσης/Πρωτόκολλο Διαδικτύου με το Εργαλείο CICFlowMeter

Ακολουθώντας την παραπάνω λογική κατάταξης πακέτων σε ροές, εξαγωγής στατιστικών και αποθήκευσή τους σε ένα .csv, το CICFlowMeter αποτελεί από τα πλέον γνωστότερα προγράμματα παραγωγής TCP/IP δικτυακών ροών [32]. Σε αντίθεση με το πρόγραμμα ανάλυσης του πρωτοκόλλου DNP3, που κατατάσσεται στο επίπεδο εφαρμογής του μοντέλου αναφοράς Ανοιχτής Διασύνδεσης Συστημάτων (Open Systems Interconnection – OSI), το οποίο υλοποιήθηκε στα πλαίσια της διπλωματικής εργασίας, το CICFlowMeter αφορά πρωτόκολλα του επιπέδου 4 του OSI, δηλαδή του επιπέδου μεταφοράς. Συνεπώς η χρήση του σε βιομηχανικά συστήματα μπορεί να δικαιολογηθεί μόνο αν αυτά χρησιμοποιούν το Internet για την μεταξύ τους επικοινωνία, χωρίς όμως να παρέχει εξατομικευμένα στοιχεία για κάθε βιομηχανικό πρωτόκολλο.

Στο Παράρτημα ΙΙ, παρουσιάζεται ο πίνακας στατιστικών του CICFlowMeter και η συνοπτική περιγραφή του κάθε ενός.

5.2 Μηχανική Μάθηση για Εξαγωγή Μοντέλου του Συστήματος Ανίχνευσης Εισβολών

Στόχος του κεφαλαίου είναι να επεξηγηθεί η μέθοδος εξαγωγής δεδομένων εκπαίδευσης, και κατόπιν να αναλυθεί η αρχιτεκτονική του αλγορίθμου βαθιάς μάθησης που υλοποιήθηκε για την εκπαίδευση του μοντέλου. Στη συνέχεια, παρουσιάζεται συγκριτικός πίνακας με τις αποδόσεις των υπόλοιπων ταξινομητών στα συγκεκριμένα δεδομένα εκπαίδευσης.

5.2.1 Εξαγωγή Δεδομένων Εκπαίδευσης με Χρήση Διαφορετικών Εργαλείων Κατανομής Πακέτων σε Ροές

Για τον σκοπό της εξαγωγής των δεδομένων εκπαίδευσης, υλοποιήθηκαν οι επιθέσεις του Κεφαλαίου 3.2. Κατά τη διάρκεια των επιθέσεων, πραγματοποιήθηκε καταγραφή της κίνησης από όλα τα συστήματα της εκάστοτε τοπολογίας.

Στη συνέχεια, τα παραγόμενα .pcap αρχεία εισάγονται στο πρόγραμμα καταχώρησης DNP3 πακέτων σε ροές που παρουσιάστηκε στο 5.1.1, αλλά και στο πρόγραμμα παραγωγής TCP/IP ροών, CICFlowMeter του 5.1.2 για σκοπούς σύγκρισης απόδοσης μοντέλων.

Κατόπιν, υλοποιήθηκε πρόγραμμα σε python, το οποίο δέχεται σαν είσοδο τα .csv αρχεία ροών και στη συνέχεια κατηγοριοποιεί τις ροές σε κλάσεις. Η κάθε κλάση φέρει τον τίτλο της επίθεσης, ή τον τίτλο της φυσιολογικής κίνησης. Για παράδειγμα, στην επίθεση ψυχρής επανεκκίνησης, αν η IP πηγής η προορισμού ροής ανήκει στον επιτιθέμενο, τότε θα είναι σίγουρο ότι η ροή ανήκει στην COLD_RESTART κλάση. Με αυτόν τον τρόπο δημιουργήθηκαν τα ταυτοποιημένα .csv.

Κατόπιν, τα ταυτοποιημένα .csv ενώθηκαν μεταξύ τους, ενώ επιλέχθηκε με τυχαίο τρόπο συγκεκριμένος αριθμός ροών οι οποίες ανήκουν στην ίδια κλάση, με σκοπό η κάθε κλάση να αντιπροσωπεύεται από το ίδιο πλήθος ροών. Με τον τρόπο αυτό, συγκροτήθηκε το σύνολο δεδομένων. Στη συνέχεια, πραγματοποιήθηκε διαχωρισμός του συνόλου δεδομένων σε δεδομένα εκπαίδευσης και επιβεβαίωσης. Τα δεδομένα εκπαίδευσης αντιπροσωπεύονται από ποσοστό 70%, ενώ τα δεδομένα επιβεβαίωσης από ποσοστό 30% ενώ η παρουσία των κλάσεων και στα δύο σύνολα είναι ισάριθμη.

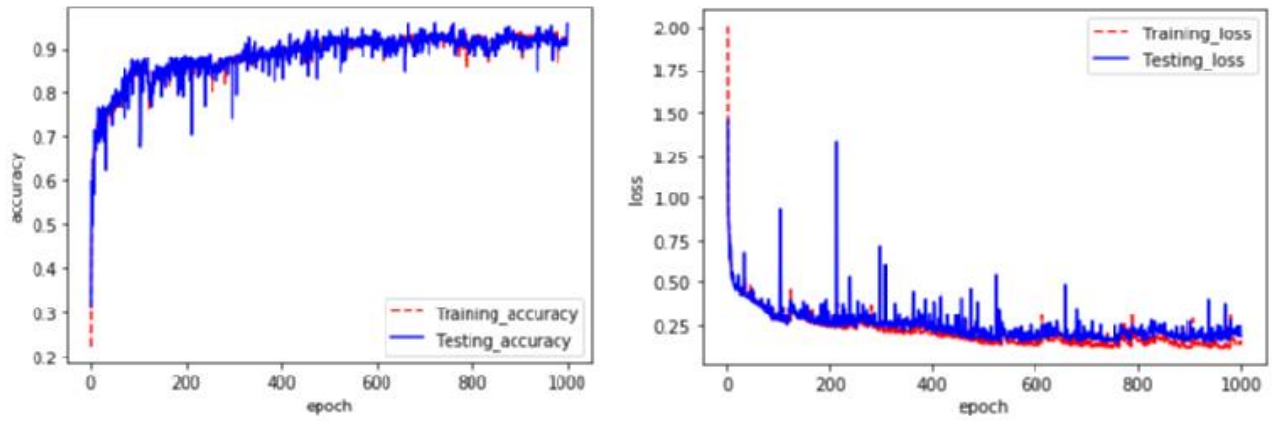
5.2.2 Εκπαίδευση Μοντέλου Αναγνώρισης Επιθέσεων με Χρήση Τεχνικών Βαθιάς Μάθησης

Για τον σκοπό της εκπαίδευσης του μοντέλου για την ταξινόμηση των εισβολών, υλοποιήθηκε αλγόριθμος νευρωνικού βαθιάς μάθησης. Συγκεκριμένα, ο αλγόριθμος δέχεται σαν είσοδο τα .csv εκπαίδευσης και επιβεβαίωσης, από τα οποία απορρίπτει τις ιδιότητες που δεν είναι τύπου float, όπως για παράδειγμα οι IP διευθύνσεις, η ημερομηνία και ο χρόνος έναρξης της ροής, το flowID. Στη συνέχεια, διαχωρίζονται τα δεδομένα εισόδου από τα δεδομένα εξόδου. Στην προκειμένη περίπτωση, δεδομένα εισόδου είναι όλες οι ιδιότητες, εκτός από το Label, ενώ δεδομένα εξόδου, δηλαδή η επιθυμητή απόκριση του συστήματος στην συγκεκριμένη είσοδο, είναι το πεδίο Label. Κατόπιν, πραγματοποιείται προεπεξεργασία των δεδομένων και στη συνέχεια ορίζεται η αρχιτεκτονική του νευρωνικού.

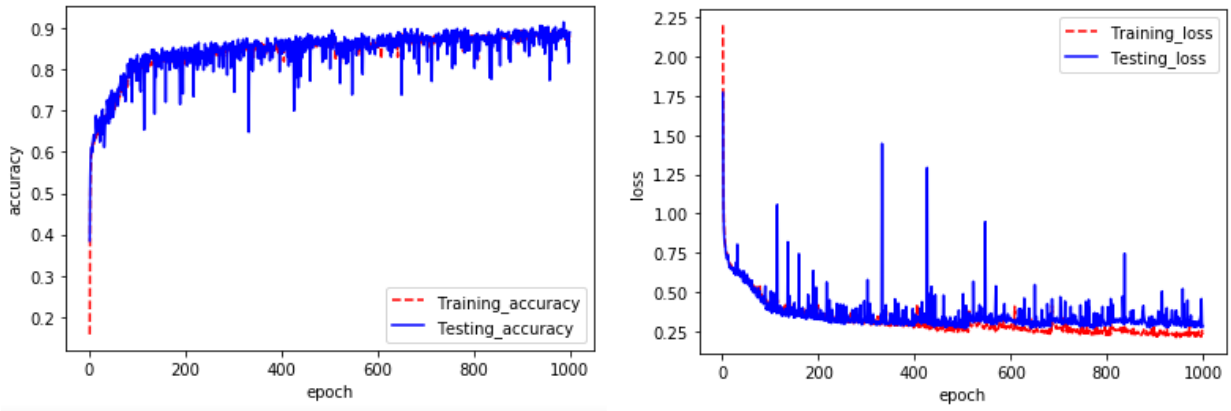
Συγκεκριμένα, αποτελείται από το επίπεδο εισόδου με τόσους νευρώνες εισόδου όσους και το πλήθος των ιδιοτήτων που δεν απορρίφθηκαν, και στη συνέχεια ορίζονται 10 πλήρως συνδεδεμένα κρυφά επίπεδα, 90 νευρώνων το κάθε ένα. Τέλος, το επίπεδο εξόδου καθορίζεται από τόσους νευρώνες, όσες και οι κλάσεις που ορίστηκαν. Το μοντέλο εκπαιδεύεται συνολικά για 1000 επαναλήψεις.

Σαν είσοδοι, χρησιμοποιήθηκαν τα .csv ροών και από το πρόγραμμα παραγωγής DNP3 ροών, και από το CICFlowMeter. Έτσι, έχουν εξαχθεί δύο διαφορετικά μοντέλα, με χρήση δύο διαφορετικών προγραμμάτων κατάταξης πακέτων σε ροές. Η σύγκριση απόδοσης των δύο μοντέλων βαθιάς μάθησης, αναλύεται εκτενώς στο παρακάτω κεφάλαιο.

Παρακάτω, φαίνονται οι γραφικές παραστάσεις οι οποίες προέκυψαν με το πέρας της διαδικασίας εκπαίδευσης, και αφορούν την ακρίβεια προβλέψεων καθώς και τις απώλειες σε κάθε επανάληψη, και για τα δύο μοντέλα.



Σχήμα 17: Σχεδιάγραμμα ακρίβειας (αριστερά) και απωλειών (δεξιά) εκπαίδευσης με δεδομένα DNP3 ροών.



Σχήμα 18: Σχεδιάγραμμα ακρίβειας (αριστερά) και απωλειών (δεξιά) εκπαίδευσης με δεδομένα TCP/IP ροών του εργαλείου CICFlowMeter.

Από την ανάλυση των σχεδιαγραμμάτων, προκύπτει ότι η ανταπόκριση του αλγορίθμου βαθιάς μάθησης ήταν αποδοτικότερη από άποψη ακρίβειας, στα δεδομένα εκπαίδευσης και επιβεβαίωσης DNP3 ροών, καθώς το σχεδιάγραμμα ακολουθεί ανοδική πορεία και έχει ελάχιστες διακυμάνσεις. Αν και το διάγραμμα ακρίβειας του αλγορίθμου βαθιάς μάθησης στα δεδομένα εκπαίδευσης και επιβεβαίωσης TCP/IP ροών ακολουθεί επίσης ανοδική πορεία, η έλλειψη σταθερότητας είναι πιο διακριτή, καθώς οι καθοδικές διακυμάνσεις είναι πιο έντονες. Συμπληρωματικά, η ανάλυση του διαγράμματος απωλειών στα δεδομένα εκπαίδευσης και επιβεβαίωσης DNP3 ροών, ακολουθεί καθοδική πορεία, με το αποτέλεσμα μετά τις 1000 επαναλήψεις να βρίσκεται στο 0.25, κάτι που αποδεικνύει ότι το μοντέλο είναι ικανό να αναγνωρίσει, με μικρές απώλειες, την κλάση της κάθε ροής. Αντίθετα, το διάγραμμα απωλειών στα δεδομένα εκπαίδευσης και επιβεβαίωσης TCP/IP ροών, κυμαίνεται ανάμεσα στο 0.25 και

0.5, διαφορά που αν και φαίνεται αμελητέα, είναι κρίσιμη στην διαφοροποίηση των δύο μοντέλων.

Στο παρακάτω κεφάλαιο, παρουσιάζεται αναλυτικά η σύγκριση απόδοσης των μοντέλων για κάθε πρόγραμμα παραγωγής ροών, με χρήση όλων των ταξινομητών.

5.2.3 Συγκριτική Αξιολόγηση Μοντέλων

Προκειμένου να αξιολογηθεί η απόδοση των διαφορετικών εργαλείων παραγωγής ροών, δηλαδή του παραγωγέα DNP3 ροών ο οποίος υλοποιήθηκε στα πλαίσια της διπλωματικής εργασίας, και του παραγωγέα TCP/IP ροών CICFlowMeter, εφαρμόσθηκαν οι ταξινομητές επιβλεπόμενης μηχανικής μάθησης Δένδρο Απόφασης, DNN, Naïve Bayes, K-Nearest Neighbor και Τυχαίου Δάσους.

Ο πίνακας συγκριτικών αποτελεσμάτων με χρήση των μέτρων αξιολόγησης που προτάθηκαν στο Κεφάλαιο 4, τόσο για τα μοντέλα που παρήχθησαν με χρήση δεδομένων εκπαίδευσης του προγράμματος κατάταξης DNP3 κίνησης σε ροές, όσο και του προγράμματος κατάταξης TCP/IP κίνησης σε ροές, CICFlowMeter, παρατίθεται αναλυτικά παρακάτω.

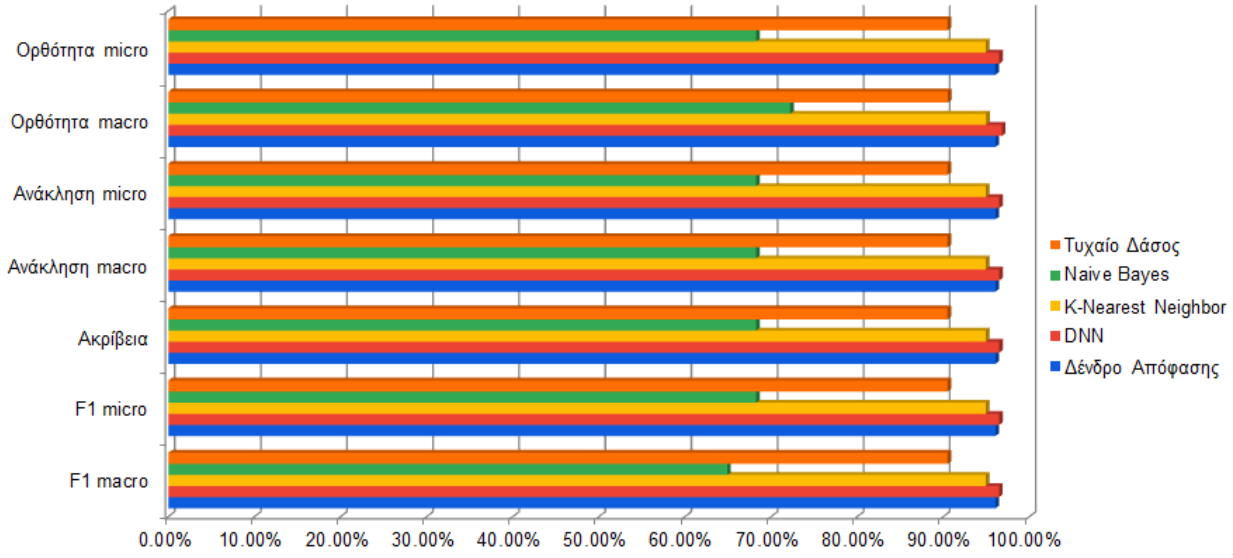
Πίνακας 1: Πίνακας σύγκρισης μοντέλων με δεδομένα εκπαίδευσης DNP3 ροών.

	Δένδρο Απόφασης	**DNN**	K-Nearest Neighbor	Naïve Bayes	Τυχαίο Δάσος
F1 macro	0.96055	**0.9647**	0.9494	0.6490	0.9049
F1 micro	0.96055	**0.965**	0.9494	0.6827	0.905
Ακρίβεια	0.96055	**0.965**	0.9494	0.6827	0.905
Ανάκληση macro	0.96055	**0.9649**	0.9494	0.6827	0.9049
Ανάκληση micro	0.96055	**0.965**	0.9494	0.6827	0.905
Ορθότητα macro	0.9606	**0.9680**	0.9497	0.7222	0.9053
Ορθότητα micro	0.9605	**0.965**	0.9494	0.6827	0.905

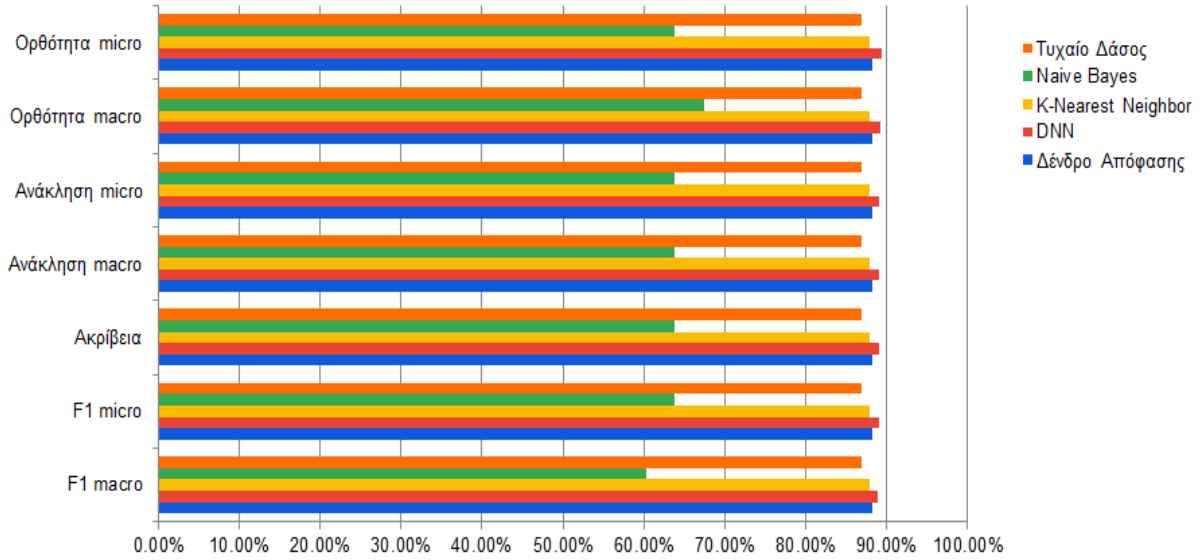
Πίνακας 2: Πίνακας σύγκρισης μοντέλων με δεδομένα εκπαίδευσης CICFlowMeter ροών.

	Δένδρο Απόφασης	**DNN**	K-Nearest Neighbor	Naïve Bayes	Τυχαίο Δάσος
F1 macro	0.88180	**0.8895**	0.8794	0.6022	0.8690
F1 micro	0.88181	**0.8904**	0.8794	0.6377	0.8690
Ακρίβεια	0.88181	**0.8904**	0.8794	0.6377	0.8690
Ανάκληση macro	0.88181	**0.8904**	0.8794	0.6377	0.8690
Ανάκληση micro	0.88181	**0.8904**	0.8794	0.6377	0.8690
Ορθότητα macro	0.88181	**0.8928**	0.8797	0.6746	0.8694
Ορθότητα micro	0.88181	**0.8945**	0.8794	0.6377	0.8690

Από την παραπάνω σύγκριση, είναι προφανές ότι τα μοντέλα που προέκυψαν από DNN αποδίδουν καλύτερα σε όλα τα πεδία σε σύγκριση με τους υπόλοιπους αλγορίθμους μηχανικής μάθησης. Παρακάτω, παρατίθενται τα αντίστοιχα bar διαγράμματα συγκρίσεων απόδοσης μοντέλων, σε ποσοστό επί τοις εκατό.



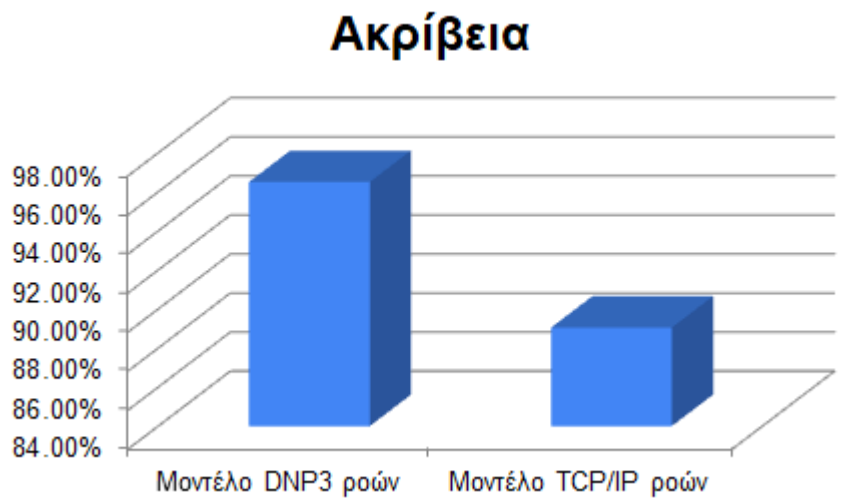
Σχήμα 19: Σχεδιάγραμμα αξιολόγησης μοντέλων ταξινομητών με βαση DNP3 ροές



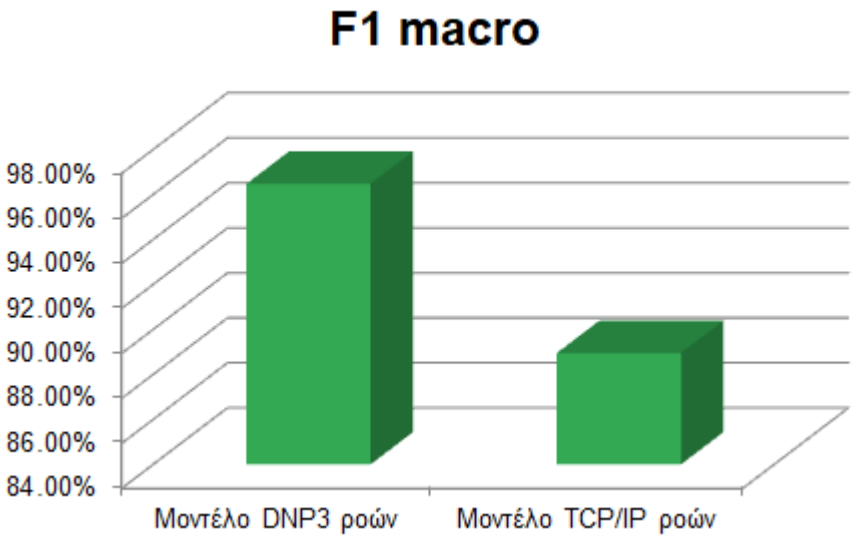
Σχήμα 20: Σχεδιάγραμμα αξιολόγησης μοντέλων ταξινομητών με βαση TCP/IP ροές με χρήση του εργαλείου CICFlowMeter

Από τα αποτελέσματα, παρατηρείται πως ο αλγόριθμος βαθιάς μάθησης είναι ικανός να αποφέρει καλύτερα αποτελέσματα σε σύγκριση με τους υπόλοιπους ταξινομητές μηχανικής μάθησης, οδηγώντας σε μεγαλύτερη αξιοπιστία στην ταξινόμηση ροών στις αντίστοιχες κλάσεις, και στις δύο κατηγορίες δεδομένων εκπαίδευσης.

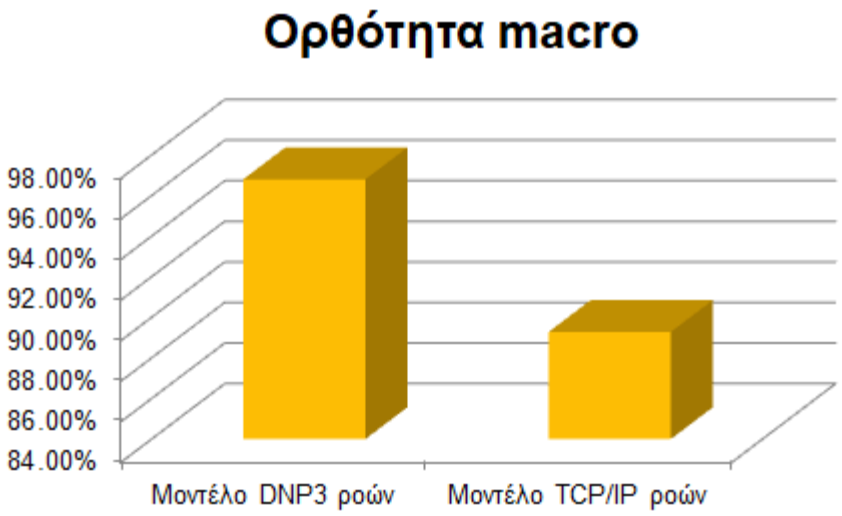
Σχετικά με την σύγκριση των δύο μοντέλων DNN που προέκυψαν με χρήση δεδομένων εκπαίδευσης DNP3 ροών και TCP/IP ροών, παρατίθεται ανάλυση των αποτελεσμάτων σχετικά με τις μετρικές ακρίβειας και F1, macro ορθότητας και ανάκλησης, οι οποίες αναλύονται παρακάτω. Ο λόγος για τον οποίο επιλέχθηκαν οι macro μετρικές, είναι ότι υπολογίζουν τον μέσο όρο για κάθε κλάση, χωρίς να λαμβάνεται υπόψιν οποιαδήποτε ανισορροπία τους, προσδίδοντας έτσι την ίδια βαρύτητα σε κάθε μια, εφόσον έχουν ήδη ισορροπηθεί όλες οι κλάσεις στα δεδομένα εκπαίδευσης και επιβεβαίωσης σε προηγούμενο βήμα [33]. Παρακάτω, εμφανίζονται διαγραμματικά τα αποτελέσματα.



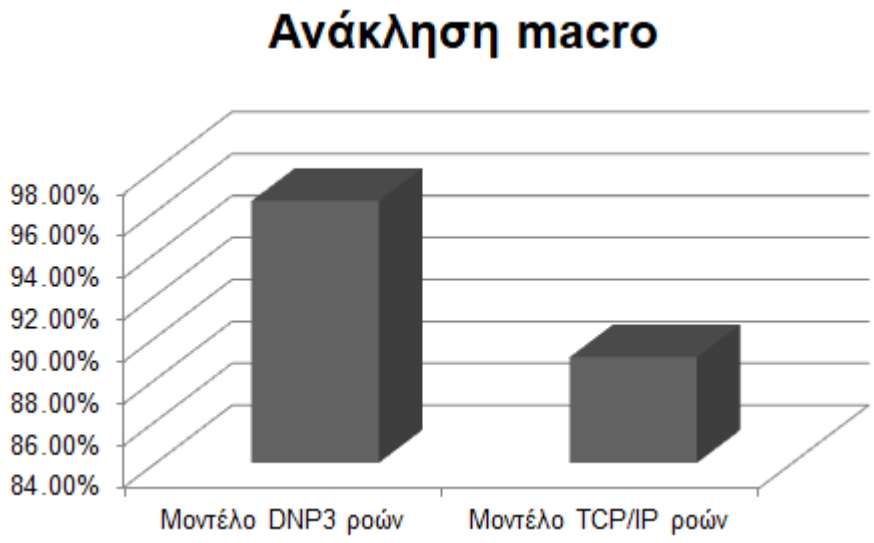
Σχήμα 21: Ακρίβεια μοντέλου DNP3 ροών και μοντέλου TCP/IP ροών



Σχήμα 22: F1-score μοντέλου DNP3 ροών και μοντέλου TCP/IP ροών



Σχήμα 23: Ορθότητα μοντέλου DNP3 ροών και μοντέλου TCP/IP ροών



Σχήμα 24: Ανάκληση μοντέλου DNP3 ροών και μοντέλου TCP/IP ροών

Είναι πλέον εύκολα ορατή η διαφορά στην απόδοση των δύο μοντέλων. Το μοντέλο το οποίο προέκυψε από δεδομένα εκπαίδευσης με τη μορφή DNP3 ροών, είναι σαφές ότι υπερτερεί σε όλους τους τομείς, συνεπώς, είναι σε θέση να αναγνωρίσει με μεγαλύτερη ακρίβεια τις επιθέσεις ενάντια στο DNP3. Αντίθετα, το μοντέλο το οποίο προέκυψε με δεδομένα εισόδου καταχωρημένα σε TCP/IP ροές εμφανίζει αρκετά χαμηλότερα αποτελέσματα στις μετρικές, επομένως, δεν προσφέρει την απαιτούμενη εγκυρότητα στην αναγνώριση των κλάσεων.

Συμπερασματικά, το μοντέλο το οποίο θα χρησιμοποιηθεί στα πλαίσια της διπλωματικής εργασίας για την υλοποίηση του συστήματος ανίχνευσης εισβολών ενάντια στο βιομηχανικό πρωτόκολλο DNP3, θα είναι αυτό το οποίο εκπαιδεύτηκε με βαθιά μάθηση, στα δεδομένα που προέκυψαν από ροές DNP3.

5.3 Παρουσίαση Medium

Το Medium IDS πρόκειται για πρόγραμμα γραμμής εντολών γραμμένο σε python, το οποίο συνδυάζει τα παραπάνω στοιχεία προκειμένου να μπορέσει να αναγνωρίσει επιτυχώς τις προκαθορισμένες επιθέσεις. Παρακάτω, αναλύεται η αρχιτεκτονική του, ο τρόπος με τον οποίο καταγράφεται η κίνηση, ο τρόπος εξαγωγής αποτελεσμάτων, καθώς και παραδείγματα εκτέλεσης.

5.3.1 Αρχιτεκτονική και Λειτουργία

Το πρόγραμμα αποτελείται από πέντε δομικά στοιχεία, τα οποία αναλύονται εκτενώς παρακάτω:

1. **Μοντέλο:** Το βασικότερο στοιχείο για την αναγνώριση και ταξινόμηση επιθέσεων, αποτελεί το μοντέλο. Πρόκειται για το μοντέλο που προέκυψε από τη διαδικασία βαθιάς μάθησης, με δεδομένα εισόδου τα .csv του προγράμματος κατάταξης DNP3 πακέτων σε ροές. Από το συγκεκριμένο μοντέλο, πρόκειται να πραγματοποιηθεί η εισαγωγή των νέων δεδομένων, προκειμένου να κατηγοριοποιηθούν στις προκαθορισμένες κλάσεις.
2. **Προεπεξεργαστής δεδομένων εισόδου:** Προκειμένου να υπάρχει έγκυρη πρόβλεψη των κλάσεων, είναι απαραίτητο τα νέα δεδομένα να υπόκεινται στην ίδια προεπεξεργασία με τα δεδομένα εκπαίδευσης. Για το σκοπό αυτό, δεν αρκεί να γίνει απλά η χρήση της ίδιας συνάρτησης προεπεξεργασίας, αλλά να χρησιμοποιηθεί ακριβώς η ίδια μέθοδος επεξεργασίας που προέκυψε από τα δεδομένα εκπαίδευσης. Συγκεκριμένα, τα δεδομένα εκπαίδευσης επεξεργάστηκαν κατάλληλα έτσι ώστε οι τιμές τους να κυμαίνονται από το 0 για την μικρότερη τιμή μιας στήλης, έως το 1 για την μεγαλύτερη τιμή της ίδιας στήλης. Οι τιμές των στηλών δεν είναι οι ίδιες και για τα δεδομένα εκπαίδευσης και για τα δεδομένα επιβεβαίωσης ή τα πραγματικά δεδομένα. Συνεπώς, πρέπει για λόγους ομοιομορφίας στην μετατροπή, να χρησιμοποιηθεί στα πραγματικά δεδομένα το ίδιο «πατρόν» που προέκυψε

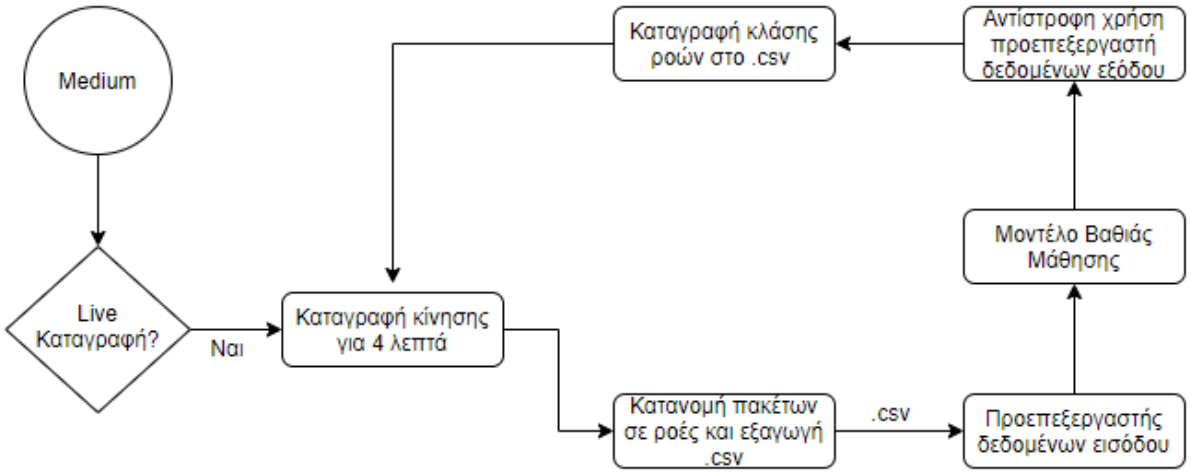
από τα δεδομένα εκπαίδευσης. Ο προεπεξεργαστής δεδομένων εισόδου είναι το «πατρόν» για τη μετατροπή αυτή.

3. **Προεπεξεργαστής δεδομένων εξόδου:** Ομοίως με παραπάνω, τα δεδομένα εξόδου δηλαδή οι κλάσεις, προεπεξεργάζονται έτσι ώστε να αναπαριστώνται με δυαδικό τρόπο. Συνεπώς, το «πατρόν» προεπεξεργασίας των δεδομένων εκπαίδευσης, εφαρμόζεται και στα πραγματικά δεδομένα.
4. **Πρόγραμμα καταγραφής κίνησης και παραγωγής DNP3 δικτυακών ροών:** Το συγκεκριμένο πρόγραμμα, αποτελεί εφαρμογή του προγράμματος παραγωγής DNP3 ροών στο τελικό IDS. Συγκεκριμένα, αναλαμβάνει, ανάλογα με την επιλογή του χρήστη που λαμβάνει από τη Διεπαφή Χρήστη (User Interface – UI) για καταγραφή ζωντανής κίνησης ή επεξεργασίας .pcap, να εκτελέσει τις εξής λειτουργίες:
   4.1. Αν ζητήθηκε καταγραφή κίνησης, πραγματοποιείται ζωντανή καταγραφή πακέτων για συγκεκριμένο χρονικό διάστημα. Με την λήξη του χρόνου, το .pcap αρχείο ονομάζεται ανάλογα με το timestamp του πρώτου πακέτου και στη συνέχεια πραγματοποιείται η ανάλυση των πακέτων, η ταξινόμησή τους σε DNP3 ροές και η εξαγωγή των στατιστικών σε .csv.
   4.2. Αν ζητήθηκε επεξεργασία .pcap, τότε ο χρήστης παροτρύνεται να εισάγει το όνομα του .pcap από το οποίο πραγματοποιεί την κατάταξη των DNP3 πακέτων στις κατάλληλες ροές και την εξαγωγή των στατιστικών που προέκυψαν σε .csv με την ίδια ονομασία με το .pcap.
5. **Πρόγραμμα Medium:** Το συγκεκριμένο πρόγραμμα, αναλαμβάνει να εμφανίζει στον χρήστη τις παροτρύνσεις για τις διαθέσιμες επιλογές και στη συνέχεια να καλεί τις κατάλληλες διαδικασίες, καθώς και να εφαρμόζει τους προεπεξεργαστές στα δεδομένα, και να τα εισάγει στο μοντέλο. Συγκεκριμένα, :
   5.1. Αν ο χρήστης επιλέξει να πραγματοποιήσει επεξεργασία ήδη καταγεγραμμένων αρχείων τοτε:
      5.1.1. Αν επιλέξει καταγεγραμμένο αρχείο .pcap, τότε το Medium προωθεί την επιλογή του χρήστη στο πρόγραμμα παραγωγής DNP3 ροών προκειμένου να εισάγει ο χρήστης το .pcap που επιθυμεί και στη συνέχεια να πραγματοποιηθεί η ανάλυσή του σε DNP3 ροές. Το παραγόμενο .csv εισέρχεται στο μοντέλο, όπου κι γίνεται η ταυτοποίηση των ροών.

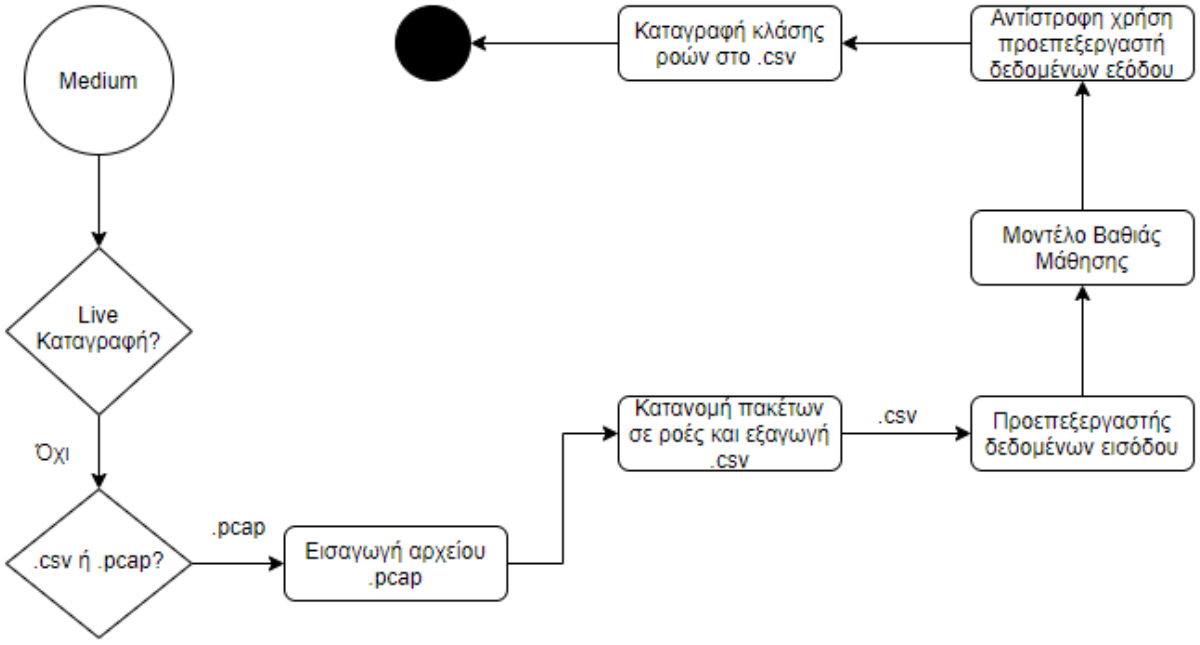
5.1.2. Αν επιλέξει καταγεγραμμένο αρχείο .csv, με την προϋπόθεση ότι το .csv προέκυψε από το πρόγραμμα ανάλυσης σε DNP3 ροές, τότε περνάει άμεσα το .csv από τον προεπεξεργαστή δεδομένων εισόδου και το μοντέλο, προκειμένου να πραγματοποιηθεί η ταξινόμηση.

5.2. Αν ο χρήστης επιλέξει να πραγματοποιήσει ζωντανή καταγραφή κίνησης, τότε περνάει το αίτημα του χρήστη στο πρόγραμμα καταγραφής κίνησης και ανάλυσης της σε DNP3 ροές. Αφού λάβει το εξαγόμενο .csv ροών, περνάει τα δεδομένα εισόδου τον προεπεξεργαστή, και στη συνέχεια τα εισάγει στο μοντέλο για την ταξινόμηση.

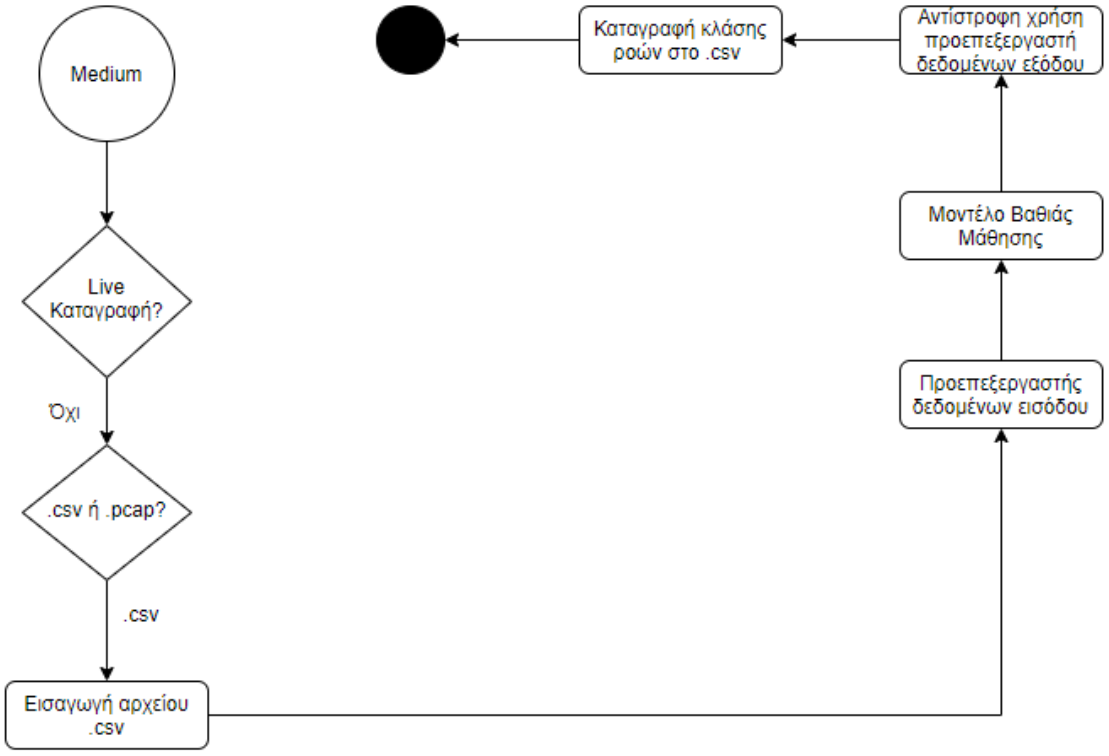
Παρακάτω, περιγράφεται σχηματικά η αλληλεπίδραση όλων των δομικών στοιχείων του Medium IDS μέσω διαγραμμάτων ροής για κάθε επιλογή του χρήστη.



Σχήμα 25: Σχεδιάγραμμα ροής του Medium IDS για καταγραφή ζωντανής κίνησης



Σχήμα 26: Σχεδιάγραμμα ροής του Medium IDS για επεξεργασία .pcap αρχείου εκτός σύνδεσης



Σχήμα 27: Σχεδιάγραμμα ροής του Medium IDS για επεξεργασία .csv αρχείου εκτός σύνδεσης

5.3.2 Καταγραφή Κίνησης

Η ζωντανή καταγραφή κίνησης πραγματοποιείται από το πρόγραμμα καταγραφής κίνησης και ανάλυσής της σε DNP3 ροές. Συγκεκριμένα, η καταγραφή πραγματοποιείται από τη συνάρτηση sniff του scapy. Σαν χρονικό όριο, ορίζονται τα τέσσερα λεπτά, στη διάρκεια των οποίων καταγράφει την δικτυακή κίνηση όλων των πρωτοκόλλων και αποθηκεύει τα πακέτα σε μια λίστα προκειμένου να αναλυθούν αργότερα. Η επιθυμητή χρονική διάρκεια μπορεί να μεταβληθεί με αλλαγή των παραμέτρων στον κώδικα. Με το πέρας της διαδικασίας ζωντανής καταγραφής πακέτων, αποθηκεύει τη λίστα σε ένα .pcap το οποίο σαν όνομα φέρει τη χρονική διάκριση, ή αλλιώς timestamp του πρώτου πακέτου της λίστας.

5.3.3 Εξαγωγή Αποτελεσμάτων

Παραπάνω, περιγράφηκαν εκτενώς τα δομικά στοιχεία του συστήματος ανίχνευσης εισβολών. Στο συγκεκριμένο κεφάλαιο, πρόκειται να αναλυθεί η ακριβής μεθοδολογία λειτουργίας του προγράμματος, καθώς και να δοθούν παραδείγματα εκτέλεσης.

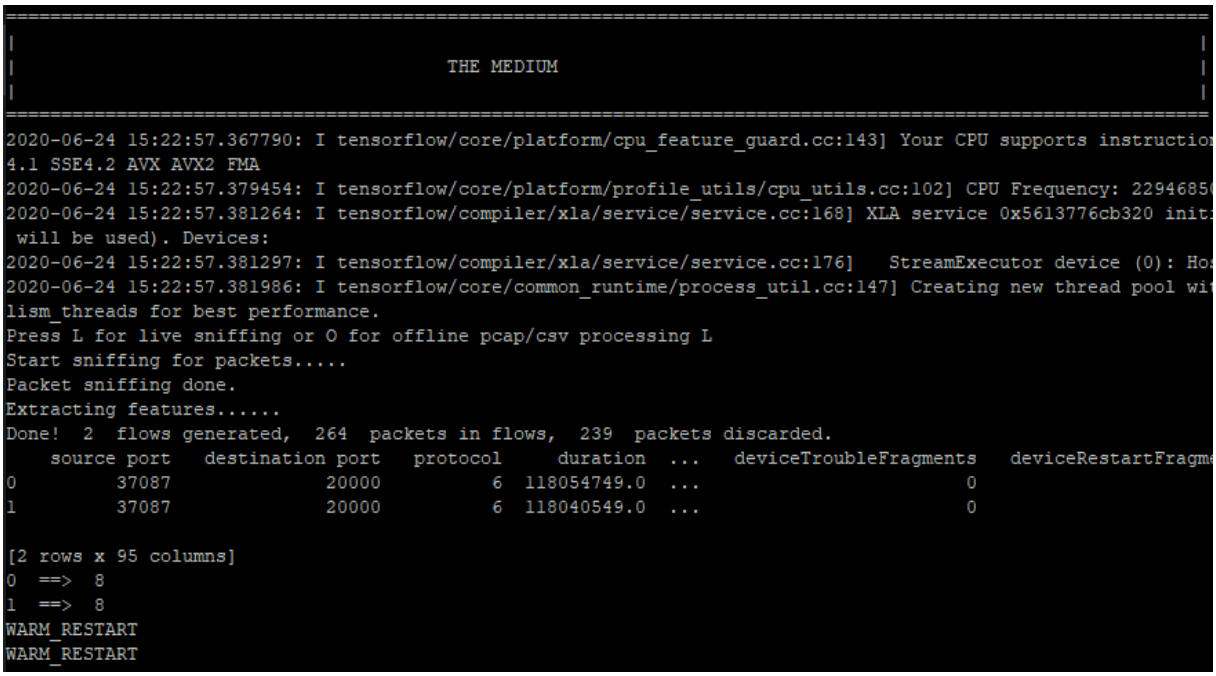
Αφού το πρόγραμμα λάβει τις απαραίτητες εντολές από τον χρήστη, και δεδομένου ότι έχει ήδη παραχθεί ένα .csv αρχείο, τότε από αυτό απορρίπτονται οι στήλες οι οποίες απορρίφθηκαν κατά την εκπαίδευση και στη συνέχεια εφαρμόζεται το «πατρόν» προεπεξεργασίας που προέκυψε από τα δεδομένα εκπαίδευσης, εξάγοντας έτσι τα νέα δεδομένα εισόδου. Στη συνέχεια, τα νέα δεδομένα εισόδου εισέρχονται στο μοντέλο βαθιάς μάθησης, όπου πραγματοποιείται η ταξινόμησή τους σύμφωνα με τις κλάσεις που ορίστηκαν κατά την εκπαίδευση.

Μόλις προβλεφθούν οι κλάσεις για κάθε ροή, μετατρέπονται τα αποτελέσματα από τη δυαδική μορφή τους, στη φυσική μορφή λέξεων προκειμένου να είναι κατανοητό από τον χρήστη. Η διαδικασία αυτή πραγματοποιείται από την αντίστροφη χρήση του προεπεξεργαστή δεδομένων εξόδου.

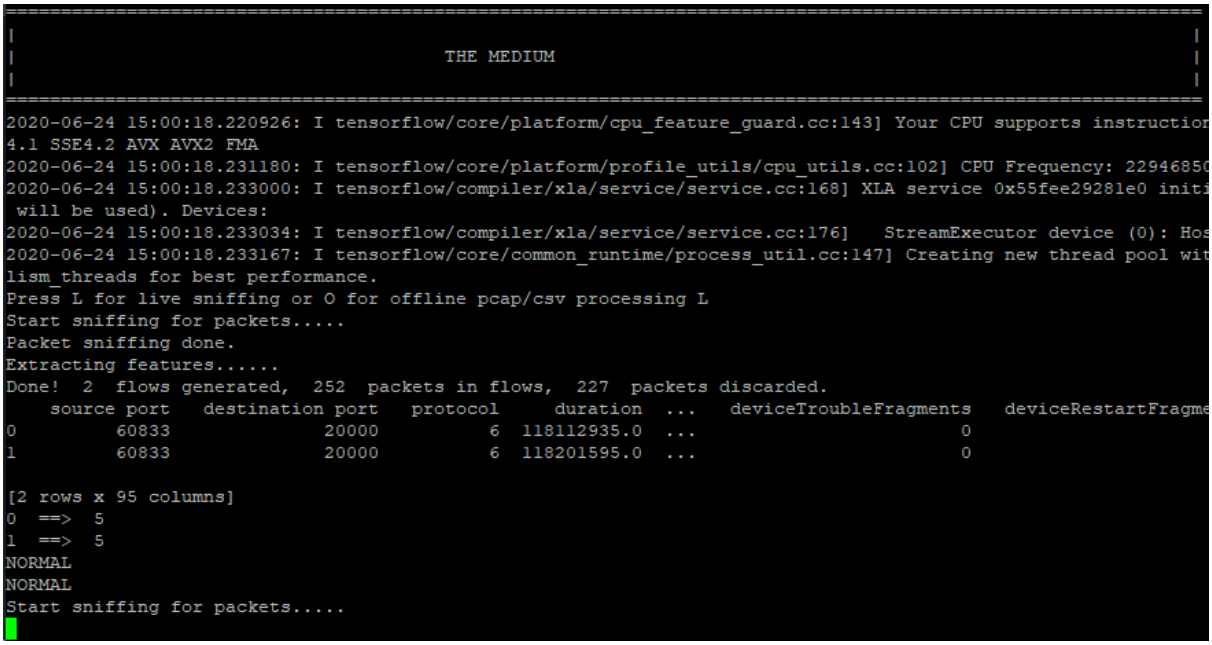
Τέλος, τα παραγόμενα αποτελέσματα, προστίθενται στην τελευταία στήλη του αρχικού .csv, τη στήλη «Label». Το συνολικό, ταξινομημένο .csv, αποθηκεύεται με νέα ονομασία, η οποία υποδεικνύει την ολοκλήρωση της διαδικασίας ταυτοποίησης των ροών.

Η παραπάνω διαδικασία, η οποία αποτελεί την λειτουργία του τελικού IDS, εκτελείται επ’αορίστον αν ο χρήστης επιλέξει ζωντανή καταγραφή κίνησης, και μια φορά αν επιλέξει μεμονωμένη επεξεργασία αρχείων.

Παρακάτω, εμφανίζονται παραδείγματα εκτέλεσης του προγράμματος, τόσο για ζωντανή λειτουργία όσο και για offline επεξεργασία αρχείων, για τις επιθέσεις θερμής επανεκκίνησης, απαρίθμησης διευθύνσεων με το DNP3 Enumerate NSE, τερματισμού εφαρμογής, καθώς και για φυσιολογική κίνηση.

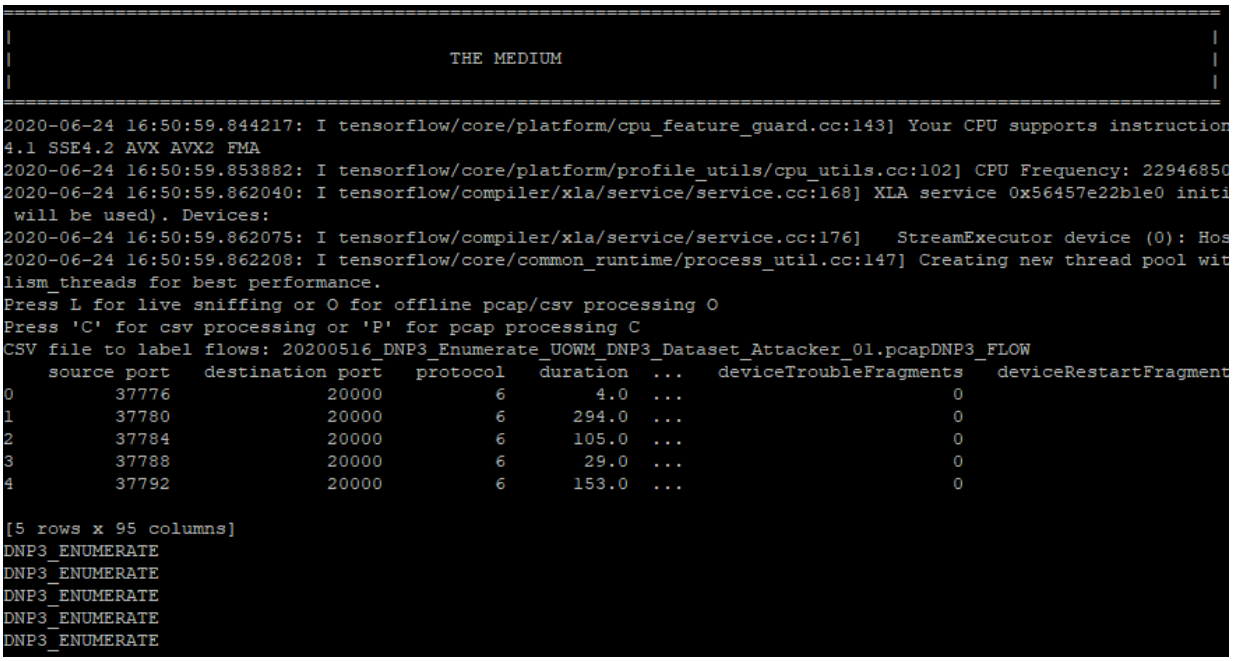


Σχήμα 28: Παράδειγμα ζωντανής λειτουργίας, σε επίθεση τύπου θερμής επανεκκίνησης (WARM RESTART)

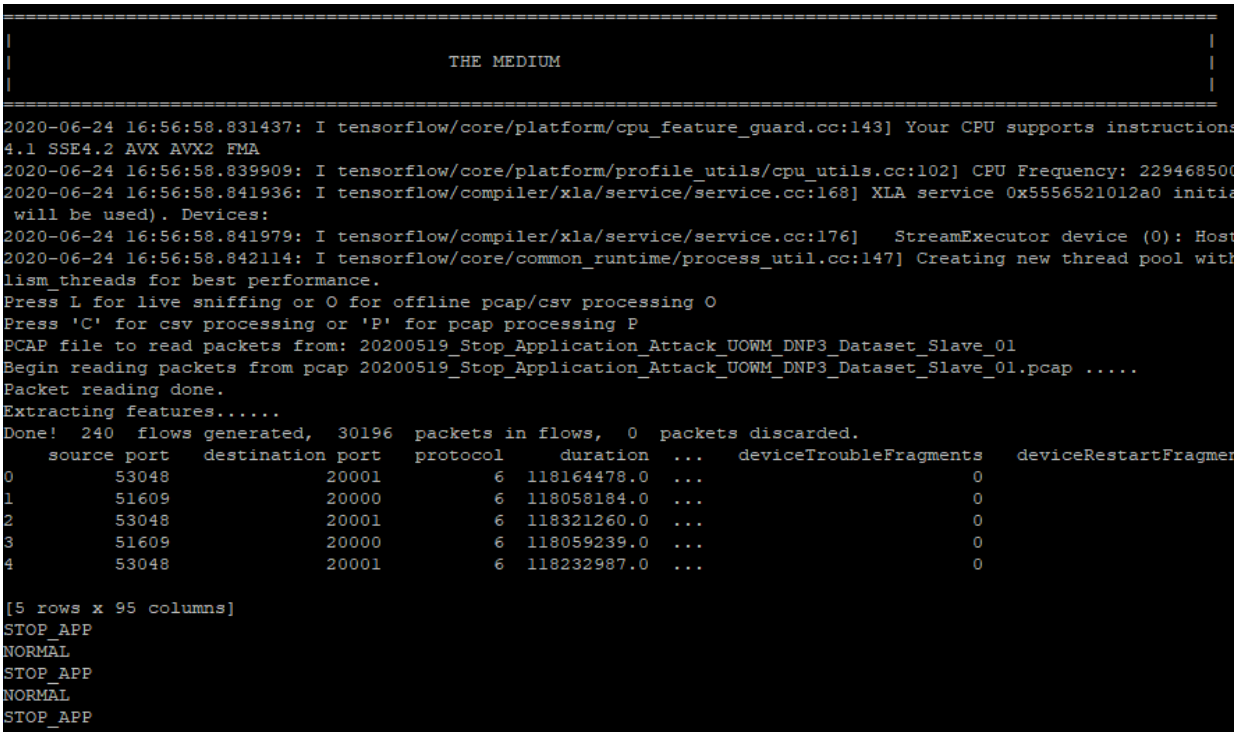


Σχήμα 29: Παράδειγμα ζωντανής λειτουργίας, με φυσιολογική κίνηση

.



Σχήμα 30: Παράδειγμα offline λειτουργίας με επεξεργασία .csv για την επίθεση NSE DNP3_ENUMERATE



Σχήμα 31: Παράδειγμα offline λειτουργίας με επεξεργασία .pcap που περιέχει και επίθεση και φυσιολογική κίνηση, για την επίθεση τερματισμού εφαρμογής (STOP_APPLICATION)

6. Συμπεράσματα και Μελλοντικές Επεκτάσεις

Η μελέτη και η υλοποίηση συστημάτων ανίχνευσης εισβολών για ICS, αποτελεί το επίκεντρο πολλών ερευνών τα τελευταία χρόνια, λόγω της αύξησης της χρήσης δικτυωμένων συσκευών στις βιομηχανίες. Η εφαρμογή μηχανικής μάθησης για εξαγωγή μοντέλων ανίχνευσης εισβολών έχει συμβάλλει σημαντικά στην βελτίωση της διαδικασίας υλοποίησης IDS. Ταυτόχρονα, λόγω του ολοένα αυξανόμενου ρυθμού και επικινδυνότητας των κυβερνοεπιθέσεων ενάντια σε βιομηχανικά συστήματα, κρίνεται ακόμα πιο αναγκαία η δημιουργία συστημάτων ανίχνευσης εισβολών, τα οποία θα είναι ικανά να αναγνωρίζουν πληθώρα επιθέσεων ενάντια σε συγκεκριμένα πρωτόκολλα, προκειμένου να διασφαλιστεί η αρμονικότητα των λειτουργιών των ευαίσθητων υποδομών. Συνεπώς, είναι απαραίτητη η εύρεση κατάλληλων λύσεων ικανών να καλύψουν τις βιομηχανικές ανάγκες στον τομέα της ασφάλειας των συστημάτων αυτοματισμού.

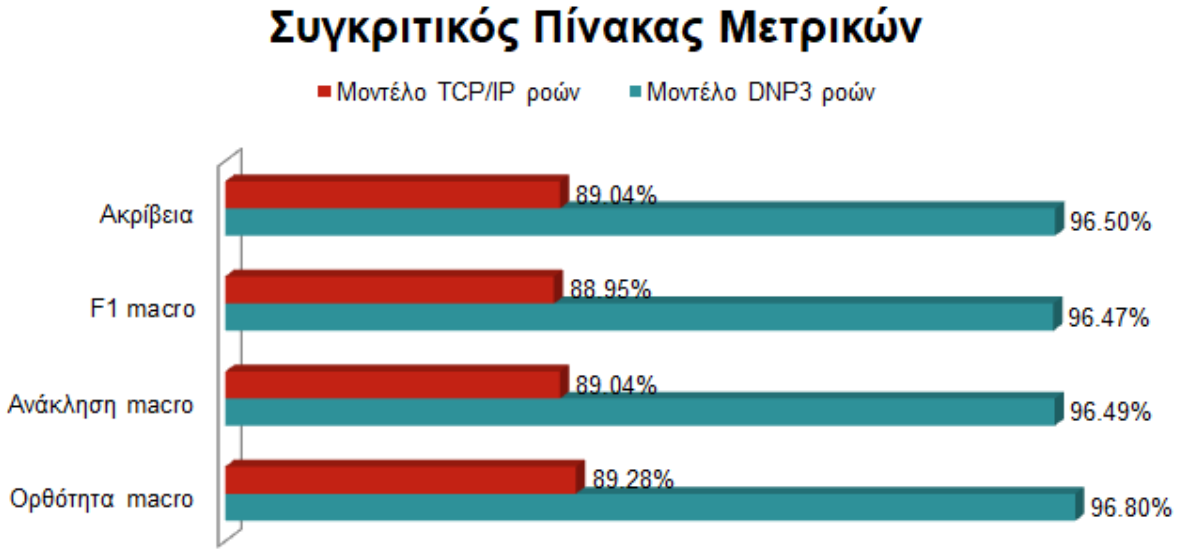
Στις παραπάνω ενότητες, προτάθηκε μια λύση ασφάλειας για το πρωτόκολλο DNP3. Αρχικά, ορίστηκαν θεωρητικά οι έννοιες των συστημάτων ελέγχου εισβολών, μηχανικής μάθησης, και πραγματοποιήθηκε επεξήγηση δομικών στοιχείων του πρωτοκόλλου DNP3.

Στο πρακτικό σκέλος της διπλωματικής εργασίας, έγινε ανάλυση των επιθέσεων που μπορεί να εκτελεστούν ενάντια στο πρωτόκολλο DNP3, αλλά και των επιπτώσεων που αποφέρει η κάθε μια, ενώ στη συνέχεια υλοποιήθηκαν οι αναφερόμενες επιθέσεις, με σκοπό τη δημιουργία συνόλου δεδομένων. Η ομαδοποίηση των πακέτων των επιθέσεων βασίστηκε στη λογική των δικτυακών ροών. Συγκεκριμένα, χρησιμοποιήθηκαν δύο ξεχωριστά προγράμματα παραγωγής δικτυακών ροών, προκειμένου να βρεθεί η βέλτιστη λύση η οποία μπορεί να χαρακτηρίσει καλύτερα μια επίθεση ενάντια στο DNP3. Το ένα πρόγραμμα, το οποίο αναπτύχθηκε στα πλαίσια της διπλωματικής εργασίας, αφορά την κατανομή δικτυακής κίνησης σε DNP3 ροές, οι οποίες χαρακτηρίζονται από ιδιότητες επικεντρωμένες πάνω στο συγκεκριμένο βιομηχανικό πρωτόκολλο. Το άλλο πρόγραμμα, αφορά την κατανομή πακέτων σε TCP/IP δικτυακές ροές, οι ιδιότητες των οποίων αφορούν και περιγράφουν λειτουργίες του TCP/IP.

Κατόπιν, εφαρμόσθηκαν τεχνικές νευρωνικού βαθιάς μάθησης για την εκπαίδευση ενός μοντέλου προκειμένου να είναι σε θέση να αναγνωρίζει με μεγάλη ακρίβεια τις παραπάνω επιθέσεις. Για το σκοπό της εκπαίδευσης του νευρωνικού, εφαρμόσθηκαν και τα δεδομένα που προέκυψαν από την κατανομή πακέτων σε DNP3 ροές, και τα δεδομένα που προέκυψαν από την κατανομή πακέτων σε TCP/IP ροές, συντελώντας στη δημιουργία δύο ξεχωριστών μοντέλων,

προκειμένου να αξιολογηθούν με τις κατάλληλες μετρικές και συνεπώς να βρεθεί η αποτελεσματικότερη λύση.

Τα αποτελέσματα της απόδοσης των δύο μοντέλων, έδειξαν πως το μοντέλο το οποίο εκπαιδεύτηκε στην αναγνώριση επιθέσεων, μέσα από DNP3 ροές, είναι σε θέση να αναγνωρίσει με μεγαλύτερη ορθότητα και ακρίβεια τις επιθέσεις ενάντια στο συγκεκριμένο πρωτόκολλο. Αντίθετα, το μοντέλο που εκπαιδεύτηκε με TCP/IP ροές, δεν επέφερε τα επιθυμητά αποτελέσματα, με τις μετρικές του να καταγράφουν διαφορά έως και 7.52 ποσοστιαίες μονάδες χαμηλότερα από τις αντίστοιχες μετρικές του μοντέλου που βασίστηκε σε DNP3 ροές. Συγκεκριμένα, η ακρίβεια του επικρατέστερου μοντέλου, ανέρχεται στο 96.5%, ενώ η ακρίβεια του επόμενου μοντέλου στο 89.04%, διαφορά η οποία είναι κρίσιμη για την επιλογή εφαρμογής του μοντέλου στο σύστημα ανίχνευσης εισβολών. Παρακάτω, αναφέρεται και γραφικά η σύγκριση απόδοσης των παραγόμενων μοντέλων, με γνώμονα τις μετρικές ακρίβειας, F1, ανάκλησης και ορθότητας.



Σχήμα 32: Συγκριτικός Πίνακας Μετρικών μοντέλων TCP/IP ροών και DNP3 ροών

Λόγω της ξεκάθαρα βέλτιστης απόδοσης του μοντέλου το οποίο βασίστηκε σε DNP3 ροές, προκύπτει το συμπέρασμα, ότι για την παραγωγή επιεικούς συστήματος ανίχνευσης εισβολών με τη μορφή ανωμαλιών για ένα συγκεκριμένο πρωτόκολλο, με βάση τις δικτυακές ροές, είναι απαραίτητη προϋπόθεση η επαρκής περιγραφή του πρωτοκόλλου για το οποίο διαμορφώνεται το IDS. Δηλαδή, οι στατιστικές ιδιότητες που περιγράφουν τις ροές, οφείλουν να είναι

εφαρμοσμένες πάνω σε αυτό, να περιγράφουν πλήρως και με σωστό τρόπο όλα τα πεδία του. Ταυτόχρονα, κατόπιν αναζήτησης ευπαθειών πάνω στο συγκεκριμένο πρωτόκολλο, η ανάλυση δικτυακών ροών θα πρέπει να συμπεριλαμβάνει κρίσιμα πεδία του πρωτοκόλλου τα οποία θεωρούνται επιρρεπή σε διάφορες επιθέσεις.

Συμπερασματικά, αναγκαία συνθήκη για την παραγωγή αξιόπιστου συστήματος ανίχνευσης εισβολών, το οποίο βασίζεται στην παραγωγή δικτυακών ροών, είναι η πλήρης περιγραφή των λειτουργιών και ευπαθειών του εκάστοτε πρωτοκόλλου για το οποίο υλοποιείται το IDS. Η περιγραφή αυτή, πραγματοποιείται μέσα από στατιστικές ιδιότητες ροών, ικανές να υποβοηθήσουν έναν αλγόριθμο μηχανικής μάθησης να αφομοιώσει τα κατάλληλα μοτίβα προκειμένου να είναι σε θέση να αναγνωρίσει έγκυρα αν η κίνηση είναι φυσιολογική ή κακόβουλη. Επομένως, η βέλτιστη λύση η οποία μπορεί να ταξινομήσει με μεγαλύτερη ακρίβεια τις ροές δικτυακής κίνησης, προκύπτει από το συνδυασμό της μηχανικής μάθησης με την εξατομικευμένη ανάλυση του ίδιου του πρωτοκόλλου που χρησιμοποιείται για την επικοινωνία.

Το τελικό σύστημα ανίχνευσης εισβολών για το πρωτόκολλο DNP3, το οποίο βασίζεται στην κατανομή δικτυακής κίνησης σε ροές, αξιοποιεί πρόγραμμα παραγωγής DNP3 ροών το οποίο περιγράφει εκτενώς τα πεδία του πρωτοκόλλου, ενώ έχει δοθεί έμφαση στον κατάλληλο χαρακτηρισμό μέσω στατιστικών, των επιρρεπών σε επιθέσεις σημείων του DNP3. Συνεπώς, το Medium είναι ικανό να προβλέψει με μεγάλη ακρίβεια την κλάση των DNP3 ροών, καθώς το μοντέλο του έχει εκπαιδευτεί με στατιστικά στοιχεία τα οποία καλύπτουν τις ανάγκες του συγκεκριμένου πρωτοκόλλου. Συνεπώς, το Medium προτείνεται ως μια ικανή λύση στις μεγάλες απαιτήσεις ασφάλειας των βιομηχανιών, οι οποίες αξιοποιούν το DNP3 για την επικοινωνία των επιμέρους συστημάτων τους για την επίβλεψη των διαδικασιών.

Το Medium, προς το παρόν, είναι ικανό να αναγνωρίζει επιθέσεις που αφορούν κυρίως το επίπεδο εφαρμογής. Μελλοντικά, πρόκειται να πραγματοποιηθεί επέκταση του εύρους των κακόβουλων ενεργειών που μπορεί να αναγνωρίσει το Medium, με την υλοποίηση επιθέσεων και σε άλλα πεδία του DNP3. Παραδειγματικά, πρόκειται να συμπεριληφθούν επιθέσεις που στοχεύουν και τα υπόλοιπα επίπεδα του DNP3, δηλαδή αυτά του επιπέδου μεταφοράς και επιπέδου συνδέσμου. Επιπροσθέτως, αναμένεται η προσθήκη επιπλέον στατιστικών ιδιοτήτων στο πρόγραμμα κατάταξης πακέτων σε DNP3 ροές, προκειμένου να περιγράφονται με το σωστό τρόπο οι νέες επιθέσεις που θα υλοποιηθούν και άρα να υπάρχει εξίσου μεγάλη ακρίβεια των προβλέψεων του Medium. Επίσης, πρόκειται να υλοποιηθεί η κατάλληλη διεπαφή χρήστη, έτσι

ώστε η χρήση αλλά και η εξαγωγή αποτελεσμάτων του Medium να πραγματοποιείται με τρόπο φιλικό και εύκολα κατανοητό από τον χρήστη.

Παράρτημα Ι

Πίνακας 3: Πίνακας ιδιοτήτων για DNP3

Όνομα Ιδιότητας	Επεξήγηση
Flow ID	Η ταυτότητα της ροής, όπως ορίστηκε από το πρώτο πακέτο.
Source IP	Η IP πηγής ροής, όπως ορίστηκε από το πρώτο πακέτο.
Destination IP	Η IP προορισμού ροής, όπως ορίστηκε από το πρώτο πακέτο.
Source Port	Η θύρα πηγής ροής, όπως ορίστηκε από το πρώτο πακέτο.
Destination Port	Η θύρα προορισμού ροής, όπως ορίστηκε από το πρώτο πακέτο.
Protocol	Το πρωτόκολλο της ροής.
Date	Η ημερομηνία και ώρα έναρξης της ροής.
Duration	Η διάρκεια της ροής σε μsec.
TotalFwdPkts	Συνολικός αριθμός πακέτων της ροής σε forward κατεύθυνση.
TotalBwdPkts	Συνολικός αριθμός πακέτων της ροής σε backward κατεύθυνση.
TotLenfwdDL	Συνολικό μέγεθος του payload του επιπέδου συνδέσμου του DNP3, στην forward κατεύθυνση.
TotLenfwdTR	Συνολικό μέγεθος του payload του επιπέδου μεταφοράς του DNP3, στην forward κατεύθυνση.
TotLenfwdAPP	Συνολικό μέγεθος του payload του επιπέδου εφαρμογής του DNP3, στην forward κατεύθυνση.

TotLenbwdDL	Συνολικό μέγεθος του payload του επιπέδου συνδέσμου του DNP3, στην backward κατεύθυνση.
TotLenbwdTR	Συνολικό μέγεθος του payload του επιπέδου μεταφοράς του DNP3, στην backward κατεύθυνση.
TotLenbwdAPP	Συνολικό μέγεθος του payload του επιπέδου εφαρμογής του DNP3, στην backward κατεύθυνση.
DLfwdPktLenMAX	Το μέγιστο μήκος payload του επιπέδου συνδέσμου, στη forward κατεύθυνση.
DLfwdPktLenMIN	Το ελάχιστο μήκος payload του επιπέδου συνδέσμου, στη forward κατεύθυνση.
DLfwdPktLenMEAN	Η μέση τιμή του μήκους payload του επιπέδου συνδέσμου, στη forward κατεύθυνση.
DLfwdPktLenSTD	Η τυπική απόκλιση του μήκους payload του επιπέδου συνδέσμου, στη forward κατεύθυνση.
TRfwdPktLenMAX	Το μέγιστο μήκος payload του επιπέδου μεταφοράς, στη forward κατεύθυνση.
TRfwdPktLenMIN	Το ελάχιστο μήκος payload του επιπέδου μεταφοράς, στη forward κατεύθυνση.
TRfwdPktLenMEAN	Η μέση τιμή του μήκους payload του επιπέδου μεταφοράς, στη forward κατεύθυνση.
TRfwdPktLenSTD	Η τυπική απόκλιση του μήκους payload του επιπέδου μεταφοράς, στη forward κατεύθυνση.
APPfwdPktLenMAX	Το μέγιστο μήκος payload του επιπέδου

	εφαρμογής, στη forward κατεύθυνση.
APPfwdPktLenMIN	Το ελάχιστο μήκος payload του επιπέδου εφαρμογής, στη forward κατεύθυνση.
APPfwdPktLenMEAN	Η μέση τιμή του μήκους payload του επιπέδου εφαρμογής, στη forward κατεύθυνση.
APPfwdPktLenSTD	Η τυπική απόκλιση του μήκους payload του επιπέδου εφαρμογής, στη forward κατεύθυνση.
DLbwdPktLenMAX	Το μέγιστο μήκος payload του επιπέδου συνδέσμου, στη backward κατεύθυνση.
DLbwdPktLenMIN	Το ελάχιστο μήκος payload του επιπέδου συνδέσμου, στη backward κατεύθυνση.
DLbwdPktLenMEAN	Η μέση τιμή του μήκους payload του επιπέδου συνδέσμου, στη backward κατεύθυνση.
DLbwdPktLenSTD	Η τυπική απόκλιση του μήκους payload του επιπέδου συνδέσμου, στη backward κατεύθυνση.
TRbwdPktLenMAX	Το μέγιστο μήκος payload του επιπέδου μεταφοράς, στη backward κατεύθυνση.
TRbwdPktLenMIN	Το ελάχιστο μήκος payload του επιπέδου μεταφοράς, στη backward κατεύθυνση.
TRbwdPktLenMEAN	Η μέση τιμή του μήκους payload του επιπέδου μεταφοράς, στη backward κατεύθυνση.
TRbwdPktLenSTD	Η τυπική απόκλιση του μήκους payload του επιπέδου μεταφοράς, στη backward κατεύθυνση.
APPbwdPktLenMAX	Το μέγιστο μήκος payload του επιπέδου

	εφαρμογής, στη backward κατεύθυνση.
APPbwdPktLenMIN	Το ελάχιστο μήκος payload του επιπέδου εφαρμογής, στη backward κατεύθυνση.
APPbwdPktLenMEAN	Η μέση τιμή του μήκους payload του επιπέδου εφαρμογής, στη backward κατεύθυνση.
APPbwdPktLenSTD	Η τυπική απόκλιση του μήκους payload του επιπέδου εφαρμογής, στη backward κατεύθυνση.
DLflowBytes/sec	Πόσα bytes του payload του επιπέδου συνδέσμου ανταλλάχθηκαν ανά sec.
TRflowBytes/sec	Πόσα bytes του payload του επιπέδου μεταφοράς ανταλλάχθηκαν ανά sec.
APPflowBytes/sec	Πόσα bytes του payload του επιπέδου εφαρμογής ανταλλάχθηκαν ανά sec.
FlowPkts/sec	Πόσα πακέτα ανταλλάχθηκαν ανά sec.
FlowIAT_MEAN	Η μέση τιμή του ενδιάμεσου χρόνου άφιξης πακέτων της ροής.
FlowIAT_STD	Η τυπική απόκλιση του ενδιάμεσου χρόνου άφιξης πακέτων της ροής.
FlowIAT_MAX	Η μέγιστη τιμή του ενδιάμεσου χρόνου άφιξης πακέτων της ροής.
FlowIAT_MIN	Η ελάχιστη τιμή του ενδιάμεσου χρόνου άφιξης πακέτων της ροής.
TotalFwdIAT	Το άθροισμα των ενδιάμεσων χρόνων άφιξης πακέτων της forward κατεύθυνσης.
FwdIAT_MEAN	Η μέση τιμή των ενδιάμεσων χρόνων άφιξης πακέτων της forward κατεύθυνσης.
FwdIAT_STD	Η τυπική απόκλιση των ενδιάμεσων χρόνων άφιξης πακέτων της forward κατεύθυνσης.

FwdIAT_MAX	Η μέγιστη τιμή των ενδιάμεσων χρόνων άφιξης πακέτων της forward κατεύθυνσης.
FwdIAT_MIN	Η ελάχιστη τιμή των ενδιάμεσων χρόνων άφιξης πακέτων της forward κατεύθυνσης.
TotalBwdIAT	Το άθροισμα των ενδιάμεσων χρόνων άφιξης πακέτων της forward κατεύθυνσης.
bwdIAT_MEAN	Η μέση τιμή των ενδιάμεσων χρόνων άφιξης πακέτων της backward κατεύθυνσης.
bwdIAT_STD	Η τυπική απόκλιση των ενδιάμεσων χρόνων άφιξης πακέτων της backward κατεύθυνσης.
bwdIAT_MAX	Η μέγιστη τιμή των ενδιάμεσων χρόνων άφιξης πακέτων της backward κατεύθυνσης.
bwdIAT_MIN	Η ελάχιστη τιμή των ενδιάμεσων χρόνων άφιξης πακέτων της backward κατεύθυνσης.
DLfwdHdrLen	Το άθροισμα των κεφαλίδων του επιπέδου συνδέσμου για τα forward πακέτα.
TRfwdHdrLen	Το άθροισμα των κεφαλίδων του επιπέδου μεταφοράς για τα forward πακέτα.
APPfwdHdrLen	Το άθροισμα των κεφαλίδων του επιπέδου μεταφοράς για τα forward πακέτα.
DLbwdHdrLen	Το άθροισμα των κεφαλίδων του επιπέδου συνδέσμου για τα backward πακέτα.
TRbwdHdrLen	Το άθροισμα των κεφαλίδων του επιπέδου μεταφοράς για τα backward πακέτα.
APPbwdHdrLen	Το άθροισμα των κεφαλίδων του επιπέδου μεταφοράς για τα backward πακέτα.
FwdPkts/sec	Το πλήθος των forward πακέτων ανά sec.
BwdPkts/sec	Το πλήθος των backward πακέτων ανά sec.
DLpktLenMEAN	Η μέση τιμή των bytes στο payload του επιπέδου συνδέσμου.

DLpktLenMIN	Τα λιγότερα bytes στο payload του επιπέδου συνδέσμου.
DLpktLenMAX	Τα περισσότερα bytes στο payload του επιπέδου συνδέσμου.
DLpktLenSTD	Η τυπική απόκλιση των bytes στο payload του επιπέδου συνδέσμου.
DLpktLenVAR	Η διαφορά των bytes στο payload του επιπέδου συνδέσμου.
TRpktLenMEAN	Η μέση τιμή των bytes στο payload του επιπέδου μεταφοράς.
TRpktLenMIN	Τα λιγότερα bytes στο payload του επιπέδου μεταφοράς.
TRpktLenMAX	Τα περισσότερα bytes στο payload του επιπέδου μεταφοράς.
TRpktLenSTD	Η τυπική απόκλιση των bytes στο payload του επιπέδου μεταφοράς.
TRpktLenVAR	Η διαφορά των bytes στο payload του επιπέδου μεταφοράς.
APPpktLenMEAN	Η μέση τιμή των bytes στο payload του επιπέδου εφαρμογής.
APPpktLenMIN	Τα λιγότερα bytes στο payload του επιπέδου εφαρμογής.
APPpktLenMAX	Τα περισσότερα bytes στο payload του επιπέδου εφαρμογής.
APPpktLenSTD	Η τυπική απόκλιση των bytes στο payload του επιπέδου εφαρμογής.
APPpktLenVAR	Η διαφορά των bytes στο payload του επιπέδου εφαρμογής.
ActiveMEAN	Η μέση τιμή του χρόνου κατά τον οποίο η ροή ήταν ενεργή.

ActiveSTD	Η τυπική απόκλιση του χρόνου κατά τον οποίο η ροή ήταν ενεργή.
ActiveMAX	Η μέγιστη τιμή του χρόνου κατά τον οποίο η ροή ήταν ενεργή.
ActiveMIN	Η ελάχιστη τιμή του χρόνου κατά τον οποίο η ροή ήταν ενεργή.
IdleMEAN	Η μέση τιμή του χρόνου κατά τον οποίο η ροή ήταν αδρανής πριν γίνει ενεργή.
IdleSTD	Η τυπική απόκλιση του χρόνου κατά τον οποίο η ροή ήταν αδρανής πριν γίνει ενεργή.
IdleMAX	Η μέγιστη τιμή του χρόνου κατά τον οποίο η ροή ήταν αδρανής πριν γίνει ενεργή.
IdleMIN	Η ελάχιστη τιμή του χρόνου κατά τον οποίο η ροή ήταν αδρανής πριν γίνει ενεργή.
FrameSrc	Η διεύθυνση επιπέδου συνδέσμου της πηγής της ροής.
FrameDst	Η διεύθυνση επιπέδου συνδέσμου του προορισμού της ροής.
TotPktsinFlow	Ο συνολικός αριθμός πακέτων της ροής.
FirstPacketDIR	Πηγή του πρώτου πακέτου της ροής, αν δηλαδή είναι MASTER ή OUTSTATION.
MostCommonREQ_FUNC_CODE	Ο πιο συχνά εμφανιζόμενος κωδικός λειτουργίας αιτημάτων επιπέδου εφαρμογής στη ροή.
MostCommonRESP_FUNC_CODE	Ο πιο συχνά εμφανιζόμενος κωδικός λειτουργίας αποκρίσεων επιπέδου εφαρμογής στη ροή.
CorruptConfigFragment	Πλήθος αποκρίσεων από τον slave, με set το corruptConfig bit του IIN.
DeviceTroubleFragment	Πλήθος αποκρίσεων από τον slave, με set το

	deviceTrouble bit του IIN.
DeviceRestartFragment	Πλήθος αποκρίσεων από τον slave, με set το deviceRestart bit του IIN.
PktsFromMaster	Το πλήθος των πακέτων με πηγή τον master.
pktsFromSlave	Το πλήθος των πακέτων με πηγή τον slave.
Label	Η κατηγορία ταξινόμησης της ροής, δηλαδή, η κλάση στην οποία ανήκει.

Παράρτημα ΙΙ

Πίνακας 4: Πίνακας ιδιοτήτων CICFlowMeter

Όνομα Ιδιότητας	Επεξήγηση
Flow ID	Η ταυτότητα της ροής, όπως προκύπτει από το πρώτο πακέτο
Src IP	Η IP πηγής της ροής, όπως καθορίστηκε από το πρώτο πακέτο.
Src Port	Η θύρα πηγής της ροής, όπως καθορίστηκε από το πρώτο πακέτο.
Dst IP	Η IP προορισμού της ροής, όπως καθορίστηκε από το πρώτο πακέτο.
Dst Port	Η θύρα προορισμού της ροής, όπως καθορίστηκε από το πρώτο πακέτο.
Protocol	Το πρωτόκολλο της ροής.
Timestamp	Το timestamp της ροής.
Flow Duration	Η διάρκεια της ροής σε microsec
Tot Fwd Pkts	Το πλήθος πακέτων στην forward κατεύθυνση.
Tot Bwd Pkts	Το πλήθος πακέτων στην backward κατεύθυνση.
TotLen Fwd Pkts	Το συνολικό μήκος πακέτου στην forward κατεύθυνση.
TotLen Bwd Pkts	Το συνολικό μήκος πακέτου στην backward κατεύθυνση.
Fwd Pkt Len Max	Η μέγιστη τιμή του μέγεθος του πακέτου στην forward κατεύθυνση.
Fwd Pkt Len Min	Η ελάχιστη τιμή του μέγεθος του πακέτου στην forward κατεύθυνση.
Fwd Pkt Len Mean	Η μέση τιμή του μέγεθος του πακέτου στην

	forward κατεύθυνση.
Fwd Pkt Len Std	Η τυπική απόκλιση του μέγεθος του πακέτου στην forward κατεύθυνση.
Bwd Pkt Len Max	Η μέγιστη τιμή του μέγεθος του πακέτου στην backward κατεύθυνση.
Bwd Pkt Len Min	Η ελάχιστη τιμή του μέγεθος του πακέτου στην backward κατεύθυνση.
Bwd Pkt Len Mean	Η μέση τιμή του μέγεθος του πακέτου στην backward κατεύθυνση.
Bwd Pkt Len Std	Η τυπική απόκλιση του μέγεθος του πακέτου στην backward κατεύθυνση.
Flow byts/sec	Το πλήθος των bytes ανά sec.
Flow Pkts/sec	Το πλήθος των πακέτων ανά sec.
Flow IAT Mean	Η μέση τιμή του χρόνου ανάμεσα σε δύο πακέτα της ροής.
Flow IAT Std	Η τυπική απόκλιση του χρόνου ανάμεσα σε δύο πακέτα της ροής.
Flow IAT Max	Ο μέγιστος χρόνος ανάμεσα σε δύο πακέτα της ροής.
Flow IAT Min	Ο ελάχιστος χρόνος ανάμεσα σε δύο πακέτα της ροής.
Fwd IAT Tot	Ο συνολικός χρόνος ανάμεσα στην αποστολή δύο διαδοχικών πακέτων με forward κατεύθυνση.
Fwd IAT Mean	Η μέση τιμή του χρόνου ανάμεσα στην αποστολή δύο διαδοχικών πακέτων με forward κατεύθυνση.
Fwd IAT Std	Η τυπική απόκλιση του χρόνου ανάμεσα στην αποστολή δύο διαδοχικών πακέτων με forward κατεύθυνση.

Fwd IAT Max	Ο μέγιστος χρόνος ανάμεσα στην αποστολή δύο διαδοχικών πακέτων με forward κατεύθυνση.
Fwd IAT Min	Ο ελάχιστος χρόνος ανάμεσα στην αποστολή δύο διαδοχικών πακέτων με forward κατεύθυνση.
Bwd IAT Tot	Ο συνολικός χρόνος ανάμεσα στην άφιξη δύο διαδοχικών πακέτων με backward κατεύθυνση.
Bwd IAT Mean	Η μέση τιμή του χρόνου ανάμεσα στην άφιξη δύο διαδοχικών πακέτων με backward κατεύθυνση.
Bwd IAT Std	Η τυπική απόκλιση του χρόνου ανάμεσα στην άφιξη δύο διαδοχικών πακέτων με backward κατεύθυνση.
Bwd IAT Max	Ο μέγιστος χρόνος ανάμεσα στην άφιξη δύο διαδοχικών πακέτων με backward κατεύθυνση.
Bwd IAT Min	Ο ελάχιστος χρόνος ανάμεσα στην άφιξη δύο διαδοχικών πακέτων με backward κατεύθυνση.
Fwd PSH Flags	Πλήθος forward πακέτων με PSH σημαία.
Bwd PSH Flags	Πλήθος backward πακέτων με PSH σημαία.
Fwd URG Flags	Πλήθος forward πακέτων με URG σημαία.
Bwd URG Flags	Πλήθος backward πακέτων με URG σημαία.
Fwd Header Len	Συνολικό μήκος κεφαλίδας στα πακέτα με forward κατεύθυνση.
Bwd Header Len	Συνολικό μήκος κεφαλίδας στα πακέτα με backward κατεύθυνση.
Fwd pkts/s	Πλήθος των πακέτων με forward κατεύθυνση

	ανά sec.
Bwd pkts/s	Πλήθος των πακέτων με backward κατεύθυνση ανά sec.
Pkt Len Min	Η ελάχιστη τιμή μήκους πακέτου.
Pkt Len Max	Η μέγιστη τιμή μήκους πακέτου.
Pkt Len Mean	Η μέση τιμή του μήκους πακέτων.
Pkt Len Std	Η τυπική απόκλιση του μήκους πακέτων.
Pkt Len Var	Η διαφορά του μήκους πακέτων.
FIN Flag Cnt	Πλήθος πακέτων με τη σημαία FIN.
SYN Flag Cnt	Πλήθος πακέτων με τη σημαία SYN.
RST Flag Cnt	Πλήθος πακέτων με τη σημαία RST.
PSH Flag Cnt	Πλήθος πακέτων με τη σημαία PSH.
ACK Flag Cnt	Πλήθος πακέτων με τη σημαία ACK.
URG Flag Cnt	Πλήθος πακέτων με τη σημαία URG.
CWR Flag Cnt	Πλήθος πακέτων με τη σημαία CWR.
ECE Flag Cnt	Πλήθος πακέτων με τη σημαία ECE.
Down/Up Ratio	Η αναλογία download/upload.
Pkt Size Avg	Το μέσο μέγεθος ενός πακέτου της ροής.
Fwd Seg Size Avg	Η μέση τιμή του μεγέθους που παρατηρήθηκε στην forward κατεύθυνση.
Bwd Seg Size Avg	Η μέση τιμή του μεγέθους που παρατηρήθηκε στην backward κατεύθυνση.
Fwd Byts/b Avg	Η μέση τιμή των bytes ανά bulk στην forward κατεύθυνση.
Fwd Pkts/b Avg	Η μέση τιμή των πακέτων ανά bulk στην forward κατεύθυνση
Fwd Bulk Rate Avg	Η μέση τιμή του ρυθμού του bulk στην forward κατεύθυνση.
Bwd Byts/b Avg	Η μέση τιμή των bytes ανά bulk στην backward κατεύθυνση.

Bwd Pkts/b Avg	Η μέση τιμή των πακέτων ανά bulk στην backward κατεύθυνση.
Bwd Bulk Rate Avg	Η μέση τιμή του ρυθμού του bulk στην backward κατεύθυνση.
Subflow Fwd Pkts	Η μέση τιμή των forward πακέτων σε μια υπορροή.
Subflow Fwd Byts	Η μέση τιμή των bytes forward πακέτων σε μια υπορροή.
Subflow Bwd Pkts	Η μέση τιμή των backward πακέτων σε μια υπορροή.
Subflow Bwd Byts	Η μέση τιμή των backward bytes πακέτων σε μια υπορροή.
Init Fwd Win Byts	Το σύνολο των bytes στο initial window, στην forward κατεύθυνση.
Init Bwd Win Byts	Το σύνολο των bytes στο initial window, στην backward κατεύθυνση.
Fwd Act Data Pkts	Το πλήθος των πακέτων με τουλάχιστον 1 byte TCP payload, στην forward κατεύθυνση.
Fwd Seg Size Min	Το ελάχιστο μέγεθος segment που παρατηρήθηκε σε forward κατεύθυνση.
Active Mean	Μέση τιμή του χρόνου κατά τον οποίο μια ροή ήταν ενεργή πριν γίνει αδρανής.
Active Std	Τυπική απόκλιση του χρόνου κατά τον οποίο μια ροή ήταν ενεργή πριν γίνει αδρανής.
Active Max	Μέγιστος χρόνος κατά τον οποίο μια ροή ήταν ενεργή πριν γίνει αδρανής.
Active Min	Ελάχιστος χρόνος κατά τον οποίο μια ροή ήταν ενεργή πριν γίνει αδρανής.
Idle Mean	Η μέση τιμή του χρόνου κατά τον οποίο μια ροή παρέμεινε αδρανής.

Idle Std	Η τυπική απόκλιση του χρόνου κατά τον οποίο μια ροή παρέμεινε αδρανής.
Idle Max	Μέγιστος χρόνος κατά τον οποίο μια ροή παρέμεινε αδρανής.
Idle Min	Ελάχιστος χρόνος κατά τον οποίο μια ροή παρέμεινε αδρανής.

Βιβλιογραφία

[1] D. Lee, H. Kim, K. Kim και P. D. Yoo, «Simulated Attack on DNP3 Protocol in SCADA System,» 2014.

[2] O. Koucham, «Intrusion detection for industrial control systems».

[3] M. Holloway, «Stuxnet Worm Attack on Iranian Nuclear Facilities,» 2015.

[4] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin και K.-Y. Tung, «Intrusion detection system: A comprehensive review,» *Journal of Network and Computer Applications,* 2012.

[5] «www.cs.clemson.edu,» [Ηλεκτρονικό]. Available: https://www.cs.clemson.edu/course/cpsc420/material/Security%20Practice/Intrusion%20Detection/Architecture.pdf.

[6] P. Uppuluri και R. Sekar, «Experiences with Specification-Based Intrusion».

[7] R. Sekar, A. Gupta, J. Frullo, T. Shanbhag, A. Tiwari, H. Yang και S. Zhou, «Specification-based Anomaly Detection:A New Approach for Detecting Network Intrusions,» 2002.

[8] I. N. Fovino, A. Carcano, T. D. L. Murel και A. Trombetta, «Modbus/DNP3 State-based Intrusion Detection,» 2010.

[9] T. Mander, F. Nabhani, L. Wang και R. Cheung, «Data Object Based Security for DNP3 Over TCP/IP for Increased Utility Commercial Aspects Security».

[10] O. Igbe, I. Darwish και T. Saadawi, «Deterministic Dendritic Cell Algorithm Application to Smart Grid Cyber-Attack Detection,» 2017.

[11] N. R. Rodofile, K. Radke και E. Foo, «Framework for SCADA Cyber-attack Dataset Creation,» 2017.

[12] Y. Yang, L. Gao, Y.-B. Yuan, K. McLaughlin, S. Sezer και Y.-F. Gong, «Multidimensional Intrusion Detection System for IEC 61850 based SCADA Networks,» 2016.

[13] S. KWON, H. YOO και T. SHON, «IEEE 1815.1-Based Power System Security With Bidirectional RNN-Based Network Anomalous Attack Detection for Cyber-Physical System,» 2020.

[14] X. C. Yin, Z. G. Liu, L. Nkenyereye και B. Ndibanje, «Toward an Applied Cyber Security Solution in IoT-Based Smart Grids: An Intrusion Detection System Approach,» 2019.

[15] C. Irvene, T. Shekari, D. Formby και R. Beyah, «If I Knew Then What I Know Now: On Reevaluating DNP3 Security using Power Substation Traffic,» 2019.

[16] D. Jin, D. M. Nicol και G. Yan, «AN EVENT BUFFER FLOODING ATTACK IN DNP3 CONTROLLED SCADA SYSTEMS».

[17] S. East, J. Butts, M. Papa και S. Shenoi, «A Taxonomy of Attacks on the DNP3 Protocol».

[18] R. Amoah, S. Camtepe και E. Foo, «Securing DNP3 Broadcast Communications in SCADA Systems».

[19] Automatak, «https://dnp3.github.io/,» [Ηλεκτρονικό].

[20] «NetfilterQueue,» [Ηλεκτρονικό]. Available: https://pypi.org/project/NetfilterQueue/.

[21] R. Bost, R. A. Popa, S. Tu και S. Goldwasser, «Machine Learning Classification over Encrypted Data».

[22] A. Singh , N. Thakur και A. Sharma, «A review of supervised machine learning algorithms».

[23] M. T. Law, R. Urtasun και R. S. Zemel, «Deep spectral clustering learning,» 2017.

[24] L. Buşoniu, R. Babuška και B. De Schutter, Multi-agent Reinforcement Learning: An Overview.

[25] S. R. Safavian και D. Landgrebe, «A Survey of Decision Wee Classifier Methodology».

[26] A. Liaw και M. Wiener, «Classification and Regression by randomForest,» 2002.

[27] A. Jain, J. Mao και K. Mohiuddin, «Artificial neural networks: a tutorial,» 1996.

[28] K. Pasupa και W. Sunhem, «A Comparison between Shallow and Deep Architecture Classifiers on Small Dataset,» 2016.

[29] «https://tools.ietf.org/html/rfc2722,» [Ηλεκτρονικό].

[30] «scapy,» [Ηλεκτρονικό]. Available: https://scapy.net/.

[31] «ScapyDNP3_lib,» [Ηλεκτρονικό]. Available: https://github.com/nrodofile/ScapyDNP3_lib.

[32] «cicflowmeter,» [Ηλεκτρονικό]. Available: https://github.com/ahlashkari/CICFlowMeter.

[33] V. V. Asch, «Macro- and micro-averaged evaluation measures [[BASIC DRAFT]],» 2013.

[34] «towardsdatascience,» [Ηλεκτρονικό]. Available: https://towardsdatascience.com/activation-functions-neural-networks-1cbd9f8d91d6.