ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΙΚΗΣ ΙΣΧΥΟΣ

Ανάλυση Δεδομένων Έξυπνων Μετρητών για Ανίχνευση Απάτης

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Ελιάνα, Η. Ντεζατζιάκομο

Υπεύθυνος καθηγητής: Χατζηαργυρίου Νικόλαος
Καθηγητής Τομέα Ηλεκτρικής Ισχύος

Αθήνα, Ιούλιος 2016

ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ
ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ
ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ
ΤΟΜΕΑΣ ΗΛΕΚΤΙΚΗΣ ΙΣΧΥΟΣ

Ανάλυση Δεδομένων Έξυπνων Μετρητών για Ανίχνευση Απάτης

Διπλωματική εργασία

Ελιάνα, Η. Ντεζατζιάκομο

Υπεύθυνος καθηγητής: Χατζηαργυρίου Νικόλαος
Καθηγητής Τομέα Ηλεκτρικής Ισχύος

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 13η Ιουλίου 2016

(Υπογραφή)	*(Υπογραφή)*	*(Υπογραφή)*
.....	.....	.....
Ν. Χατζηαργύριου	Σ. Παπαθανασίου	Π. Γεωργιλάκης
Καθηγητής Ε.Μ.Π	Αν. Καθηγητής Ε.Μ.Π.	Επ. Καθηγητής Ε.Μ.Π.

Αθήνα, Ιούλιος 2016

(Υπογραφή)

.....
Ελιάνα, Η. Ντεζατζιάκομο
Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών Ε.Μ.Π.

Copyright © Ελιάνα, Η. Ντεζατζιάκομο , 2016

Με επιφύλαξη παντός δικαιώματος. All rights reserved.

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 δεν πρέπει να ερμηνευθεί ότι αντιπροσωπεύουν τις επίσημες θέσεις του Εθνικού Μετσόβιου Πολυτεχνείου.

Περίληψη

Σκοπός της παρούσας διπλωματικής εργασίας είναι η ανάλυση δεδομένων έξυπνων μετρητών για ανίχνευση απάτης. Τα δεδομένα, τα οποία είναι διαθέσιμα, αφορούν μετρήσεις για πάνω από 5000 καταναλωτές για ενάμιση χρόνο. Ο μεγάλος αριθμός και η ποικιλία καταναλωτών, οι μεγάλων περιόδων μετρήσεις και η διαθεσιμότητά τους δημόσια καθιστά αυτά τα δεδομένα μία εξαιρετική πηγή για ανάλυση δεδομένων έξυπνων μετρητών.

Γίνεται μια εισαγωγή στους έξυπνους μετρητές και τα πλεονεκτήματά τους έναντι των συμβατικών, αναλογικών μετρητών, καθώς επίσης και της σημασίας του έξυπνου δικτύου και της υποδομής προηγμένων μετρήσεων (Advanced Metering Infrastructure,AMI). Στα συστήματα μεταφοράς και διανομής ηλεκτρικής ενέργειας κατέχει σημαντικό ρόλο η παρουσία των τεχνικών και των μη τεχνικών απωλειών. Οι τεχνικές απώλειες αναφέρονται στις φυσικές απώλειες, όπως στις απώλειες των αντιστάσεων γραμμών μεταφοράς και μετασχηματιστών διανομής. Οι μη τεχνικές απώλειες από την άλλη, όταν παρουσιάζονται, προέρχονται συνηθέστερα από ενέργειες δόλιων επεμβάσεων στα συστήματα. Για αυτό το λόγο, καθίσταται επιτακτική ανάγκη εύρεσης αποδοτικών λύσεων για την ανίχνευση τους. Οι εταιρείες παροχής ηλεκτρισμού παγκοσμίως χάνουν τεράστια ποσά χρημάτων λόγω κλοπών στην ενέργεια. Το γεγονός αυτό, έχει αντίκτυπο τόσο στην εκάστοτε εταιρεία όσο και στην ποιότητα της ενέργειας που διοχετεύεται στους καταναλωτές.

Παρουσιάζεται βιβλιογραφική έρευνα για τις τεχνικές εντοπισμού απάτης. Οι τεχνικές αυτές, βασίζονται στην ταξινόμηση, στην εκτίμηση κατάστασης και τελευταία, στην θεωρία παιγνίων. Στην παρούσα διπλωματική εργασία χρησιμοποιείται η τεχνική βάσει ταξινόμησης και συγκεκριμένα των Μηχανών Διανυσμάτων Υποστήριξης (Support Vector Machines, SVM). Σε αυτήν την τεχνική, εκπαιδεύεται το μοντέλο ταξινόμησης σε γνωστά δεδομένα και δοκιμάζεται σε νέα δεδομένα, αφού γίνει πρώτα βελτιστοποίηση των παραμέτρων του. Τα δεδομένα στην είσοδο του μοντέλου είναι στη μορφή ετήσιων πινάκων για κάθε καταναλωτή. Σκοπός του ταξινομητή είναι να διαχωρίσει τα ημερήσια διανύσματα των καταναλωτών με παρουσία κάποιας απάτης και εκείνων χωρίς απάτη. Λόγω του ότι τα αρχικά δεδομένα είναι άρτια, χωρίς κάποια παραβίαση, γίνεται προσομοίωση απάτης, δοκιμάζοντας και αναλύοντας κάθε φορά τον βαθμό αλλοίωσης των δεδομένων. Στην συνέχεια εξάγονται τα αποτελέσματα της ταξινόμησης για τα συμπεράσματα σχετικά με την απόδοσή της. Για την υλοποίηση του αλγόριθμου χρησιμοποιήθηκε το προγραμματιστικό περιβάλλον MATLAB.

Λέξεις Κλειδιά : ανάλυση δεδομένων, έξυπνοι μετρητές, έξυπνο δίκτυο, υποδομή προηγμένων μετρήσεων (AMI), μη τεχνικές απώλειες, προσομοίωση απάτης, ανίχνευση απάτης, ταξινόμηση, μηχανές διανυσμάτων υποστήριξης (SVM)

Abstract

The subject of this thesis is the smart meter data analysis for fraud detection. The available dataset consists of half hourly energy readings for 5000 consumers. The large number and variety of customers, long period of measurements and availability to the public make this dataset an excellent source for research in the area of smart meter data analysis.

An introduction is made to smart meters and their advantages over conventional, analog meters, as well as the importance of smart grid and advanced metering infrastructure (AMI). Technical and non-technical losses play a significant role electricity transmission and distribution systems. Technical losses refer to physical losses, such as losses in transmission lines and distribution transformers. Non-technical losses, on the other hand, usually originate from tampering systems. Therefore, it becomes imperative to find efficient solutions for their detection. The electricity supply companies worldwide lose huge amounts of money due electricity theft. This has an impact on both the company and the quality of the power supply.

A literature review is presented for fraud detection techniques. These techniques are: classification-based, state-based and game theory-based. In the present thesis a classification-based technique is used, namely Support Vector Machines (SVM). In this technique, the classification model is trained on labeled data and tested on unlabeled data, after optimizing the SVM's parameters.. The input data of the model is in the form of annual tables for each consumer. The purpose of the classifier is to divide the daily consumer vectors with the presence of a fraud action and those without fraud. Since the original data is sound, frauds are simulated, testing each time the degree of data corruption. Then, the classification results are obtained to extract conclusions on its performance. The algorithm was developed using the MATLAB programming system.

Keywords: data analytics, smart meters, smart grid, advanced metering infrastructure (AMI), non-technical losses, fraud simulation, fraud detection, classification, support vector machines (SVM)

Ευχαριστίες

Η παρούσα διπλωματική εργασία εκπονήθηκε το ακαδημαϊκό έτος 2015-2016, στον τομέα Ηλεκτρικής Ισχύος της σχολής Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Ε.Μ.Π.

Αρχικά, θα ήθελα να απευθύνω τις θερμές μου ευχαριστίες στον υπεύθυνο καθηγητή της εργασίας κ. Χατζηαργυρίου Νικόλαο, για την ανάθεσή της σε εμένα και την ευκαιρία που μου δόθηκε να ανακαλύψω και να μάθω τόσα ενδιαφέροντα θέματα.

Παράλληλα, θα ήθελα ειλικρινά να ευχαριστήσω τον κ. Μεσσήνη Γεώργιο, διδάκτορα της σχολής Η.Μ.Μ.Υ του Ε.Μ.Π, για την πολύτιμη βοήθεια, καθοδήγησή του και τον χρόνο που αφιέρωσε σε εμένα κατά την εκπόνηση της εργασίας.

Ένα μεγάλο ευχαριστώ οφείλω στην οικογένειά μου και τους ανθρώπους δίπλα μου για την στήριξη και την συμπαράστασή τους καθ' όλη τη διάρκεια των φοιτητικών μου χρόνων.

Στον Πατέρα μου

ΠΕΡΙΕΧΟΜΕΝΑ

1. Εισαγωγή 1
1.1 Έξυπνοι Μετρητές 1
1.2 Έξυπνοι Δίκτυο και τεχνολογία AMI 2
1.3 Τεχνικές και Μη τεχνικές Απώλειες στα συστήματα Μεταφοράς και Διανομής Ηλεκτρικής Ενέργειας (T&D) 6
1.4 Η κλοπή ενέργειας παγκοσμίως 7
1.5 Θέματα Απάτης 10
1.5.1 Επιπτώσεις απάτης στην ενέργεια 10
1.5.2 Λόγοι κλοπής στην ενέργεια 10
1.5.3 Μέθοδοι απάτης 11
1.5.4 Το δέντρο επίθεσης 12
1.5.5 Απαιτήσεις ασφάλειας του συστήματος 15

2. Εντοπισμός Κλοπών Ενέργειας 17
2.1 Εισαγωγή 17
2.2 Τεχνική Ανίχνευσης με αλγόριθμους ταξινόμησης 17
2.3 Τεχνική ανίχνευσης με βάση την εκτίμηση κατάστασης 21
2.4 Τεχνική ανίχνευσης με βάση τη Θεωρία Παιγνίων 24
2.5 Σύγκριση των μεθόδων 25
2.6 Τεχνική ανίχνευσης κλοπής με συνδυασμό SVM και δέντρων απόφασης 26
2.7 Οι αλγόριθμοι ταξινόμησης με Μηχανές Διανυσμάτων Υποστήριξης (Support Vector Machines) 29
2.7.1 Εισαγωγή-Ιστορική Ανασκόπηση 29
2.7.2 Μαθηματικό μοντέλο 30
2.8 Μεγέθη αξιολόγησης 35
2.8.1 Confusion Matrix 35
2.8.2 Βασικοί δείκτες 36
2.8.3 Καμπύλη ROC 38

3. Μεθοδολογία εντοπισμού απάτης 41
3.1 Εισαγωγή 41
3.2 Εξόρυξη γνώσης και κατηγοριοποίηση δεδομένων 41
3.2.1 Εξόρυξη δεδομένων 41
3.2.2 Προεπεξεργασία δεδομένων 43

3.2.3 Εξαγωγή χαρακτηριστικών 44
3.2.4 Βελτιστοποίηση παραμέτρων αλγόριθμου ταξινόμηση-Cross Validation 44
3.2.5 Ταξινόμηση 48
3.3 Διαδικασία ανάλυσης δεδομένων 50
3.3.1 Περιγραφή ιστορικών δεδομένων κατανάλωσης προς ανάλυση 50
3.3.2 Προσομοίωση απάτης 52
3.3.3 Διαμόρφωση εισόδου SVM 58
3.3.4 Διαμόρφωση εισόδου SVM με εξαγωγή χαρακτηριστικών 60
3.3.5 Εξαγωγή αποτελεσμάτων 63

4. Αποτελέσματα εφαρμογής αλγόριθμου Μηχανών Διανυσμάτων Υποστήριξης(SVM) για ανίχνευση απάτης 65
4.1 Εισαγωγή 65
4.2 Μελέτη μεταβλητότητας της έντασης της επίθεσης 66
4.2.1 Περίπτωση έντονης επίθεσης, της τάξης του 90% των δεδομένων 66
4.2.2 Περίπτωση μέτριας επίθεσης, της τάξης του 50% των δεδομένων 67
4.2.3 Περίπτωση ήπιας επίθεσης, της τάξης του 20 % των δεδομένων 68
4.2.4 Περίπτωση επίθεσης από μια κατανομή 74
4.2.4.1 Κατανομή beta 74
4.2.4.2 Κανονική Κατανομή 76
4.2.4.3 Τυχαία κατανομή 78
4.2.5 Σχόλια και συμπεράσματα από τη μελέτη για μεταβλητή ένταση της επίθεσης 81
4.3 Μελέτη ως προς το χρόνο επίθεσης 81
4.3.1 Περιπτώσεις 81
4.3.2 Σχόλια και συμπεράσματα της μελέτης ως προς το χρόνο επίθεσης 82
4.4 Μελέτη συνδυασμού επιθέσεων 84
4.4.1 Περίπτωση συνδυασμού επιθέσεων του 90% και 50% των δεδομένων 84
4.4.2 Περίπτωση συνδυασμού επιθέσεων του 50% και 20% των δεδομένων 84
4.4.3 Σχόλια και συμπεράσματα της μελέτης συνδυασμού επιθέσεων 84
4.5 Μελέτη με διαφορετική επίθεση σε Training και Test Set 85
4.5.1 Περίπτωση επίθεσης του 90% και 50% των δεδομένων στο Training Set και 20% στο Test Set 85
4.5.2 Περίπτωση επίθεσης του 20% και 50% στο Training Set Και 90% στο Test Set 85
4.5.3 Σχόλια και συμπεράσματα για τη μελέτη διαφορετικής επίθεσης στο Training και Test Set 85
4.6 Μελέτη ως προς την ωριαία διάρκεια των μετρήσεων 86

4.6.1 Ώρες μετρήσεων....86
4.6.2 Σχόλια και συμπεράσματα από τη μελέτη ως προς τη χρονική διάρκεια των μετρήσεων....87
4.7 Μελέτη με βάση εξαγωγή χαρακτηριστικών....88
4.7.1 Περίπτωση έντονης επίθεσης, της τάξης του 90% των δεδομένων....88
4.7.2 Περίπτωση μέτριας επίθεσης, της τάξης του 50% των δεδομένων....88
4.7.3 Περίπτωση ήπιας επίθεσης, της τάξης του 20 %....88
4.7.4 Κατανομή Βήτα....94
4.7.5 Κανονική Κατανομή....94
4.7.6 Τυχαία κατανομή....95
4.7.7 Μελέτη ως προς το χρόνο επίθεσης....97
4.7.8 Σχόλια και Συμπεράσματα από την μελέτη με εξαγωγή χαρακτηριστικών....98
4.8 Συγκριτική μελέτη των δοκιμών χωρίς εξαγωγή χαρακτηριστικών και με εξαγωγή χαρακτηριστικών....99
4.9 Μελέτη σε 5000 καταναλωτές....106
4.9.1 Περίπτωση επίθεσης....106
4.9.2 Σχόλια και συμπεράσματα από την μελέτη 5000 καταναλωτών....108

5. Συμπεράσματα και Βελτιωτικές Προτάσεις....109
5.1 Συμπεράσματα....109
5.2 Βελτιωτικές Προτάσεις....109

Βιβλιογραφία....113

Ευρετήριο Σχημάτων

Σχήμα 1.1 : Αρχιτεκτονική της τεχνολογίας AMI 5

Σχήμα 1.2 : Ένα δέντρο επίθεσης με τα φύλλα να αναγράφουν τις απαραίτητες επιθέσεις που χρειάζονται για μια επίθεση στην ενέργεια 13

Σχήμα 1.3 : Το δέντρο επίθεσης στην κλοπή ενέργειας 15

Σχήμα 2.1 : Η βασική διαδικασία στην ταξινόμηση για την ανίχνευση κλοπών στην ενέργεια..... 18

Σχήμα 2.2 : Βασικό διάγραμμα ροής της μεθόδου ανίχνευσης μη τεχνικών απωλειών με βάση την εκτίμηση κατάστασης και την ανάλυση της διακύμανσης 24

Σχήμα 2.3 : Ο συνδυασμός δέντρου απόφασης και SVM..... 28

Σχήμα 2.4: Σχηματική αναπαράσταση ενός βέλτιστου υπερεπιπέδου δύο γραμμικών διαχωρίσιμων τάξεων 34

Σχήμα 2.5: Confusion Matrix 36

Σχήμα 2.6 : Παράδειγμα καμπυλών ROC 39

Σχήμα 3.1 : 10-fold Cross Validation..... 45

Σχήμα 3.2: Διάγραμμα ροής της προτεινόμενης μεθόδου εκπαίδευσης του αλγόριθμου C-SVM με βελτιστοποίηση παραμέτρων 47

Σχήμα 3.3 : Η ροή του προτεινόμενου τρόπου ανίχνευσης απάτης σε καταναλωτές με ασυνήθιστες και κακόβουλες δραστηριότητες 49

Σχήμα 3.4 : Παραδείγματα διαφόρων περιπτώσεων κατανομής Βήτα 54

Σχήμα 3.5 : Παραδείγματα διαφόρων περιπτώσεων κανονικής κατανομής 55

Σχήμα 3.6: Προσομοίωση απάτης της τάξης του 90% στα δεδομένα (το μπλε γράφημα είναι η αρχική και το κόκκινο είναι η τελική με εφαρμογή απάτης) 56

Σχήμα 3.7 : Προσομοίωση απάτης της τάξης του 50% στα δεδομένα (το μπλε γράφημα είναι η αρχική και το κόκκινο είναι η τελική με εφαρμογή απάτης) 56

Σχήμα 3.8: Προσομοίωση απάτης της τάξης του 20% στα δεδομένα (το μπλε γράφημα είναι η αρχική και το κόκκινο είναι η τελική με εφαρμογή απάτης) 57

Σχήμα 3.9: Προσομοίωση απάτης της τάξης του 90% στα δεδομένα για 10 ώρες (το μπλε γράφημα είναι η αρχική και το κόκκινο είναι η τελική με εφαρμογή απάτης).. 57

Σχήμα 3.10: Προσομοίωση απάτης της τάξης του 20% στα δεδομένα για 10 ώρες (το μπλε γράφημα είναι η αρχική και το κόκκινο είναι η τελική με εφαρμογή απάτης).. 58

Σχήμα 3.11 : Απεικόνιση διαχωρισμού και στάδια δειγματοληπτικής επιλογής ημερών 60

Σχήμα 3.12 : Διάγραμμα ροής της πειραματικής διαδικασίας 64

Σχήμα 4.1 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 24 ωρών..... 69

Σχήμα 4.2: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια 24 ωρών..... 70

Σχήμα 4.3 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 24 ωρών 70

Σχήμα 4.4 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια από 10 έως 24 ώρες..... 71

Σχήμα 4.5: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια από 10 έως 24 ώρες..... 71

Σχήμα 4.6 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια από 10 έως 24 ώρες..... 72

Σχήμα 4.7 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 10 ωρών..... 73

Σχήμα 4.8: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια 10 ωρών..... 73

Σχήμα 4.9 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 10 ωρών 74

Σχήμα 4.10 : Κατανομή Βήτα(beta) με παράγοντες α=1,b=3 75

Σχήμα 4.11 : Κατανομή Beta με παράγοντες α=7,b=3 75

Σχήμα 4.12 : Κατανομή Normal με μέση τιμή=0.25,τυπική απόκλιση σ=0.1 76

Σχήμα 4.13 : Κατανομή Normal με μέση τιμή=0.5,τυπική απόκλιση σ=0.1 77

Σχήμα 4.14 : Κατανομή Normal με μέση τιμή=0.8,τυπική απόκλιση σ=0.07 77

Σχήμα 4.15 : Κατανομή Random στο διάστημα [0.1,0.9]..... 79

Σχήμα 4.16 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 24 ωρών με παράγοντες αλλοίωσης από κατανομές 80

Σχήμα 4.17 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 24 ωρών με παράγοντας αλλοίωσης από κατανομές..... 80

Σχήμα 4.18 : Διάγραμμα Χρόνου Επίθεσης-FPR 82

Σχήμα 4.19 : Διάγραμμα Χρόνου Επίθεσης-TPR..... 83

Σχήμα 4.20 : Γραφική παράσταση Highest Difference -Hours of Measurements..... 87

Σχήμα 4.21 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 24 ωρών με εξαγωγή χαρακτηριστικών... 89

Σχήμα 4.22: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια 24 ωρών με εξαγωγή χαρακτηριστικών 90

Σχήμα 4.23 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 24 ωρών με εξαγωγή χαρακτηριστικών..... 90

Σχήμα 4.24 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια από 10 έως 24 ώρες με εξαγωγή χαρακτηριστικών..... 91

Σχήμα 4.25: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια από 10 έως 24 ώρες με εξαγωγή χαρακτηριστικών 91

Σχήμα 4.26 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια από 10 έως 24 ώρες με εξαγωγή χαρακτηριστικών 92

Σχήμα 4.27 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 10 ωρών με εξαγωγή χαρακτηριστικών ... 93

Σχήμα 4.28: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια 10 ωρών με εξαγωγή χαρακτηριστικών 93

Σχήμα 4.29 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 10 ωρών με εξαγωγή χαρακτηριστικών 94

Σχήμα 4.30 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 24 ωρών με παράγοντες αλλοίωσης από κατανομές από εξαγωγή χαρακτηριστικών 96

Σχήμα 4.31 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 24 ωρών με παράγοντας αλλοίωσης από κατανομές από εξαγωγή χαρακτηριστικών..... 96

Σχήμα 4.32 : Διάγραμμα Χρόνου Επίθεσης-FPR με εξαγωγή χαρακτηριστικών 97

Σχήμα 4.33 : Διάγραμμα Χρόνου Επίθεσης-TPR με εξαγωγή χαρακτηριστικών 98

Σχήμα 4.34 : Γραφική Παράσταση TPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και TPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για 24 ώρες..... 99

Σχήμα 4.35 : Γραφική Παράσταση FPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και FPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για 24 ώρες..... 100

Σχήμα 4.36 : Γραφική Παράσταση Highest Difference-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και Highest Difference-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για 24 ώρες..... 100

Σχήμα 4.37 : Γραφική Παράσταση TPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και TPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για διάστημα 10-24 ωρών 101

Σχήμα 4.38 : Γραφική Παράσταση FPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και FPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για διάστημα 10-24 ωρών 101

Σχήμα 4.39 : Γραφική Παράσταση Highest Difference-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και Highest Difference-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για διάστημα 10-24 ωρών..... 102

Σχήμα 4.40 : Γραφική Παράσταση TPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και TPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για σταθερό διάστημα 10 ωρών 102

Σχήμα 4.41 : Γραφική Παράσταση FPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και FPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για σταθερό διάστημα 10 ωρών 103

Σχήμα 4.42 : Γραφική Παράσταση Highest Difference-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και Highest Difference-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για σταθερό διάστημα 10 ωρών 103

Σχήμα 4.43 : Γραφική Παράσταση TPR-Time of attack each day χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και TPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε) 104

Σχήμα 4.44 : Γραφική Παράσταση FPR-Time of attack each day χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και FPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε) 104

Σχήμα 4.45 : Γραφική Παράσταση Highest Difference -Time of attack each day χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και Highest Difference -Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε) 105

Ευρετήριο Πινάκων

Πίνακας 3.1 : Δείγμα αρχικών ιστορικών δεδομένων κατανάλωσης 51
Πίνακας 4.1 : Αποτελέσματα ταξινόμησης απάτης του 90% των δεδομένων 66
Πίνακας 4.2 : Confusion Matrix για απάτη 10 ωρών στο 90% 66
Πίνακας 4.3 : Confusion Matrix για απάτη 10-24 ωρών στο 90% 66
Πίνακας 4.4 : Confusion Matrix για απάτη 24 ωρών στο 90% 67
Πίνακας 4.5 : Αποτελέσματα ταξινόμησης απάτης του 50% των δεδομένων 67
Πίνακας 4.6 : Confusion Matrix για απάτη 10 ωρών στο 50% 67
Πίνακας 4.7 : Confusion Matrix για απάτη 10-24 ωρών στο 50% 67
Πίνακας 4.8 : Confusion Matrix για απάτη 24 ωρών στο 50% 68
Πίνακας 4.9 : Αποτελέσματα ταξινόμησης απάτης του 50% των δεδομένων 68
Πίνακας 4.10 : Confusion Matrix για απάτη 10 ωρών στο 20% 68
Πίνακας 4.11 : Confusion Matrix για απάτη 10-24 ωρών στο 20% 68
Πίνακας 4.12 : Confusion Matrix για απάτη 24 ωρών στο 20% 69
Πίνακας 4.13 : Αποτελέσματα ταξινόμησης για επίθεση από κατανομή beta 75
Πίνακας 4.14 : Confusion Matrix για απάτη από κατανομή beta (α=1,b=3) 75
Πίνακας 4.15 : Confusion Matrix για απάτη από κατανομή beta (α=7,b=3) 76
Πίνακας 4.16 : Αποτελέσματα ταξινόμησης για επίθεση από κανονική Normal..... 77
Πίνακας 4.17 : Confusion Matrix για απάτη από κατανομή Normal (μ=0.25,σ=0.1) 78
Πίνακας 4.18 : Confusion Matrix για απάτη από κατανομή Normal (μ=0.5,σ=0.1) .. 78
Πίνακας 4.19 : Confusion Matrix για απάτη από κατανομή Normal (μ=0.8,σ=0.07) 78
Πίνακας 4.20 : Αποτελέσματα ταξινόμησης για επίθεση από κανονική Random 79
Πίνακας 4.21 : Confusion Matrix για απάτη από κατανομή Random ([0.1,0.9])..... 79
Πίνακας 4.22 : Αποτελέσματα ταξινόμησης διαφόρων δοκιμών ως προς την ώρα επίθεσης 82
Πίνακας 4.23 : Αποτελέσματα ταξινόμησης συνδυασμού επιθέσεων (80%&50%)... 84
Πίνακας 4.24 : Αποτελέσματα ταξινόμησης συνδυασμού επιθέσεων (50%&20%)... 84
Πίνακας 4.25 : Αποτελέσματα ταξινόμησης 1η περίπτωση διαφορετικού Training-Test Set 85
Πίνακας 4.26 : Αποτελέσματα ταξινόμησης 2η περίπτωση διαφορετικού Training-Test Set 85
Πίνακας 4.27 : Αποτελέσματα ταξινόμησης μελέτης διάρκειας των μετρήσεων..... 86
Πίνακας 4.28 : Αποτελέσματα ταξινόμησης απάτης του 90% των δεδομένων με εξαγωγή χαρακτηριστικών..... 88

Πίνακας 4.29 : Αποτελέσματα ταξινόμησης απάτης του 50% των δεδομένων με εξαγωγή χαρακτηριστικών..... 88

Πίνακας 4.30 : Αποτελέσματα ταξινόμησης απάτης του 20% των δεδομένων με εξαγωγή χαρακτηριστικών..... 89

Πίνακας 4.31 : Αποτελέσματα ταξινόμησης για επίθεση από κατανομή βήτα (beta) με εξαγωγή χαρακτηριστικών..... 94

Πίνακας 4.32 : Αποτελέσματα ταξινόμησης για επίθεση από κανονική κατανομή (Normal) με εξαγωγή χαρακτηριστικών..... 95

Πίνακας 4.33 : Αποτελέσματα ταξινόμησης για επίθεση από τυχαία κατανομή (random) με εξαγωγή χαρακτηριστικών..... 95

Πίνακας 4.34 : Αποτελέσματα ταξινόμησης διαφόρων δοκιμών ως προς την ώρα επίθεσης με εξαγωγή χαρακτηριστικών 97

Πίνακας 4.35 : Περίπτωση έντονης επίθεσης, της τάξης του 90% των δεδομένων για 5000 καταναλωτές..... 106

Πίνακας 4.36 : Confusion Matrix για απάτη 24 ωρών στο 90% για 5000 καταναλωτές 107

Πίνακας 4.37 : Περίπτωση επίθεσης από κατανομή βήτα για 5000 καταναλωτές.. 107

Πίνακας 4.38 : Confusion matrix επίθεσης από κατανομή βήτα για 5000 καταναλωτές 107

Πίνακας 4.39 : Περίπτωση επίθεσης από κατανομή βήτα για 5000 καταναλωτές με εξαγωγή χαρακτηριστικών..... 107

Κεφάλαιο 1
Εισαγωγή

Η παγκόσμια παραγωγή ηλεκτρικής ενέργειας και τα συστήματα μετάδοσής της μετατρέπονται σε ένα νέο σύστημα, το «έξυπνο δίκτυο». Ένα από τα κύρια χαρακτηριστικά του έξυπνου δικτύου είναι η υποδομή προηγμένων μετρήσεων, με την οποία οι αναλογικοί μετρητές ρεύματος αντικαθίστανται από τους ψηφιακούς έξυπνους μετρητές. Η αρχιτεκτονική αυτή συνεπάγεται έναν καινούργιο κίνδυνο, ο οποίος αφορά την απάτη στο δίκτυο ηλεκτρικής ενέργειας[5]. Ως εκ τούτου, καθίσταται επιτακτική η ανάγκη εύρεσης αποδοτικών λύσεων για την ανίχνευση της. Το γεγονός αυτό έχει αντίκτυπο όχι μόνο στην εταιρεία ηλεκτρικής ενέργειας, που χάνει μεγάλα ποσά χρημάτων, αλλά και στους ίδιους τους καταναλωτές. Στην συνέχεια του κεφαλαίου, περιγράφονται οι έξυπνοι μετρητές, η αρχιτεκτονική του έξυπνου δικτύου, η κλοπή ενέργειας σε παγκόσμιο επίπεδο, οι λόγοι και οι τρόποι πιθανής διάπραξης απάτης καθώς και οι σχετικές απαιτήσεις ασφαλείας του συστήματος.

1.1 Έξυπνοι Μετρητές

Οι έξυπνοι μετρητές είναι προηγμένοι μετρητές ενέργειας, μέσω των οποίων μετριέται η κατανάλωση ενέργειας των καταναλωτών και παρέχονται πρόσθετες πληροφορίες στην εταιρεία ηλεκτρισμού, σε σύγκριση με τους συμβατικούς μετρητές ενέργειας. Δύνανται να «διαβάσουν» πληροφορίες για την κατανάλωση σε πραγματικό χρόνο, συμπεριλαμβανομένων των τιμών της τάσης και της συχνότητας, και με ασφάλεια να μεταφέρουν τα δεδομένα αυτά. Η ικανότητα των έξυπνων μετρητών για αμφίδρομη επικοινωνία δεδομένων επιτρέπει την συλλογή πληροφοριών σχετικά με την ηλεκτρική ενέργεια, πέρα από την αποστολή των δεδομένων. Το σύστημα του έξυπνου μετρητή περιλαμβάνει τον έξυπνο μετρητή, τις υποδομές επικοινωνίας και πιθανόν τον έλεγχο των συσκευών. Επιπλέον, μέσω αυτού συλλέγονται διαγνωστικές πληροφορίες σχετικά με το δίκτυο διανομής, το σπίτι και τις συσκευές και καθίσταται εύκολη η επικοινωνία μεταξύ των μετρητών[1].

Η συλλογή των στοιχείων κατανάλωσης από όλους τους πελάτες σε τακτική βάση, επιτρέπει στις επιχειρήσεις ηλεκτρισμού την αποτελεσματική διαχείριση της ηλεκτρικής ενέργειας. Οι πελάτες θα ενημερώνονται για το κόστος, έτσι ώστε με αποτελεσματικό τρόπο να χρησιμοποιούν τις συσκευές τους. Για παράδειγμα, ο

καταναλωτής θα γνωρίζει ανά πάσα στιγμή την κατανάλωσή του και θα είναι σε θέση να λαμβάνει τα απαραίτητα μέτρα, όπως την μείωση χρήσης συγκεκριμένων συσκευών. Επίσης, η χρέωση θα μπορεί να γίνεται ανά ώρα. Με αυτό τον τρόπο, το μεσημέρι που η ζήτηση είναι πολύ μεγάλη, ο ηλεκτρισμός θα χρεώνεται παραπάνω, ενώ το βράδυ λιγότερο. Έτσι, εκείνες τις ώρες θα τίθενται σε λειτουργία συσκευές πιο ενεργοβόρες. Η ενσωμάτωση των έξυπνων μετρητών βοηθάει τις εταιρείες ηλεκτρισμού στην ανίχνευση μη εξουσιοδοτημένης κατανάλωσης και κλοπής ηλεκτρικής ενέργειας, με στόχο την βελτίωση της διανομής και ποιότητάς της.

1.2 Έξυπνο δίκτυο και τεχνολογία AMI

Μία από τις κύριες συνιστώσες του έξυπνου δικτύου είναι η υποδομή προηγμένης μέτρησης (Advanced Metering Infrastructure, AMI). Η τεχνολογία AMI αντικαθιστά τους αναλογικούς μετρητές με ηλεκτρονικά συστήματα, τα οποία αναφέρουν την μέτρηση ενέργειας με ψηφιακές διεπαφές επικοινωνίας, όπως οι τηλεφωνικές γραμμές. Η τεχνολογία AMI αναφέρεται στο σύστημα εκείνο, το οποίο μετράει, ελέγχει και αναλύει την κατανάλωση ενέργειας σε ένα δίκτυο, ενώ ταυτόχρονα επιτρέπει την σύνδεση των έξυπνων μετρητών με τους πάροχους ηλεκτρικής ενέργειας μέσω ενός εξελιγμένου δικτύου επικοινωνίας [2].

Η υποδομή AMI προσφέρει αποτελεσματικότερη διαχείριση της ενέργειας, με χαμηλότερο κόστος και περιβαλλοντικά ορθότερη και είναι ένα πολύ σημαντικό κομμάτι της νέας υποδομής έξυπνου δικτύου. Παρέχεται ένα σύστημα αισθητήρων, το οποίο εκτείνεται από καταναλωτές ηλεκτρικής ενέργειας στις εταιρείες διαχείρισής της. Από άποψη τεχνολογίας προσφέρει την απαραίτητη επικοινωνία και τις λειτουργίες ελέγχου, που απαιτούνται για την υλοποίηση κρίσιμων υπηρεσιών διαχείρισης ενέργειας, όπως τα συστήματα τιμολόγησης, την αυτόματη ανάγνωση μετρητών, την ανταπόκριση της ζήτησης και την διαχείριση της ποιότητας ισχύος. Το έξυπνο δίκτυο έχει ευρέως εφαρμοστεί στην Ευρώπη, την Ασία και ιδιαίτερα στην Αμερική, και σταδιακά υιοθετείται από άλλες χώρες του κόσμου [5].

Νέες προκλήσεις για την ασφάλεια εισάγονται με το έξυπνο δίκτυο, συγκεκριμένα με την τεχνολογία AMI[3]. Το AMI θα αποτελείται από δισεκατομμύρια συσκευές σχετικά χαμηλού κόστους, που θα τοποθετούνται σε μη ελέγξιμες περιοχές. Ο εξοπλισμός θα είναι υπό τον έλεγχο συχνά ανιδιοτελών, απλών ή ορισμένες φορές κακόβουλων χρηστών. Από τις πιο σημαντικές απειλές κατά του νέου έξυπνου δικτύου είναι η κλοπή ενέργειας. Το φαινόμενο αυτό συμβαίνει, όταν ένας πελάτης μεταβάλει τα στατιστικά της ενεργειακής χρήσης του, τα οποία παρέχονται στην εταιρεία. Για την κατανόηση της απειλής μπορεί να χρησιμοποιηθεί ένα δέντρο επίθεσης, το οποίο συστηματικά αρθρώνει τους τρόπους, με τους οποίους χειραγωγούνται τα δεδομένα που συλλέγονται, αποθηκεύονται ή μεταδίδονται. Η παραδοσιακή κλοπή απαιτούσε τη χειροκίνητη παρέμβαση στους αναλογικούς

μετρητές. Αντίθετα, στην περίπτωση του AMI, τα δεδομένα χρήσης μπορούν να αλλοιώνονται μετά την εγγραφή ή την μετάδοσή τους στις εταιρείες[5].

Το AMI αποτελείται από αισθητήρες του έξυπνου δικτύου. Παρέχει πληροφορίες σχετικά με την χρήση της ενέργειας(ζήτησης)στις εταιρείες ηλεκτρισμού, στους καταναλωτές αλλά και στο ίδιο το έξυπνο δίκτυο. Δίνει τη δυνατότητα να λαμβάνονται καλύτερες αποφάσεις σχετικά με τη μείωση του κόστους και την υπερφόρτωση του δικτύου κατά τις περιόδους αιχμής ζήτησης. Η ανάγκη πληροφόρησης για την ζήτηση, συνδέεται με την διανομή ηλεκτρικής ενέργειας. Η πληροφορία αυτή μετριέται και συγκεντρώνεται από τους έξυπνους μετρητές που περιέχουν στοιχεία, όπως επεξεργαστές(CPUs), αποθήκευση και διεπαφές επικοινωνίας. Σε γενικές γραμμές, από τους έξυπνους μετρητές εκτελούνται τέσσερις βασικές λειτουργίες σε σχέση με την διαχείριση ενέργειας : α) η παρακολούθηση και καταγραφή της κατανάλωσης, β) η καταγραφή των συναφών πράξεων με την ενέργεια, όπως διακοπές ηλεκτρικού ρεύματος, γ) η παράδοση της ενέργειας και η καταγραφή πληροφοριών στην επιχείρηση, δ) η παροχή και λήψη των μηνυμάτων ελέγχου, όπως ο έλεγχος των έξυπνων συσκευών, η αυτόματη αποσύνδεση, κτλ[5].

Η τεχνολογία AMI επιτρέπει μια σειρά από υπηρεσίες, που σχετίζονται με την μέτρηση της ζήτησης και την χρέωση. Οι μετρητές, που υποστηρίζουν την αυτοματοποιημένη διαδικασία μέτρησης της ενέργειας (AMR), αναφέρουν την ζήτηση στις εταιρείες αυτόματα, μέσω δικτύων επικοινωνίας. Ένα τοπικό δίκτυο καταρτίζεται από επαναλαμβανόμενους μετρητές (repeaters) για την συγκέντρωση των πληροφοριών της χρήσης ενέργειας σε ένα συλλέκτη μετρητή (collector). Ύστερα, ένα ενδιάμεσο δίκτυο χρησιμοποιείται για την μεταφορά των συνολικών δεδομένων από τον συλλέκτη στο βοηθητικό πρόγραμμα. Τα τοπικά δίκτυα, τυπικά βασίζονται, είτε στην ασύρματη τοπολογία δικτύου, είτε στις επικοινωνίες μέσω γραμμών ισχύος (PLC). Συχνά, η ενδιάμεση σύνδεση χρησιμοποιεί δημόσιο δίκτυο, όπως το Internet ή το δημόσιο τηλεφωνικό δίκτυο (PSTN). Μαζί με το σύστημα AMR για την μέτρηση, το σύστημα AMI παρέχει πρόσθετες δυνατότητες για δυναμικά συστήματα τιμολόγησης[5].

Η τιμολόγηση βάσει της ώρας χρήσης (Time-Of-Use, TOU) αναφέρεται σε ένα σύστημα τιμολόγησης, με το οποίο το κόστος ενέργειας ανάγεται στη διάρκεια των ωρών αιχμής. Τα συστήματα αυτά διαιρούν τη μέρα σε επιμέρους τμήματα (τιμολόγια αιχμής και εκτός αιχμής). Στην ιδανική περίπτωση, το κόστος μπορεί να μειωθεί μεταφέροντας ενεργοβόρες εργασίες σε ώρες εκτός αιχμής[5][6].

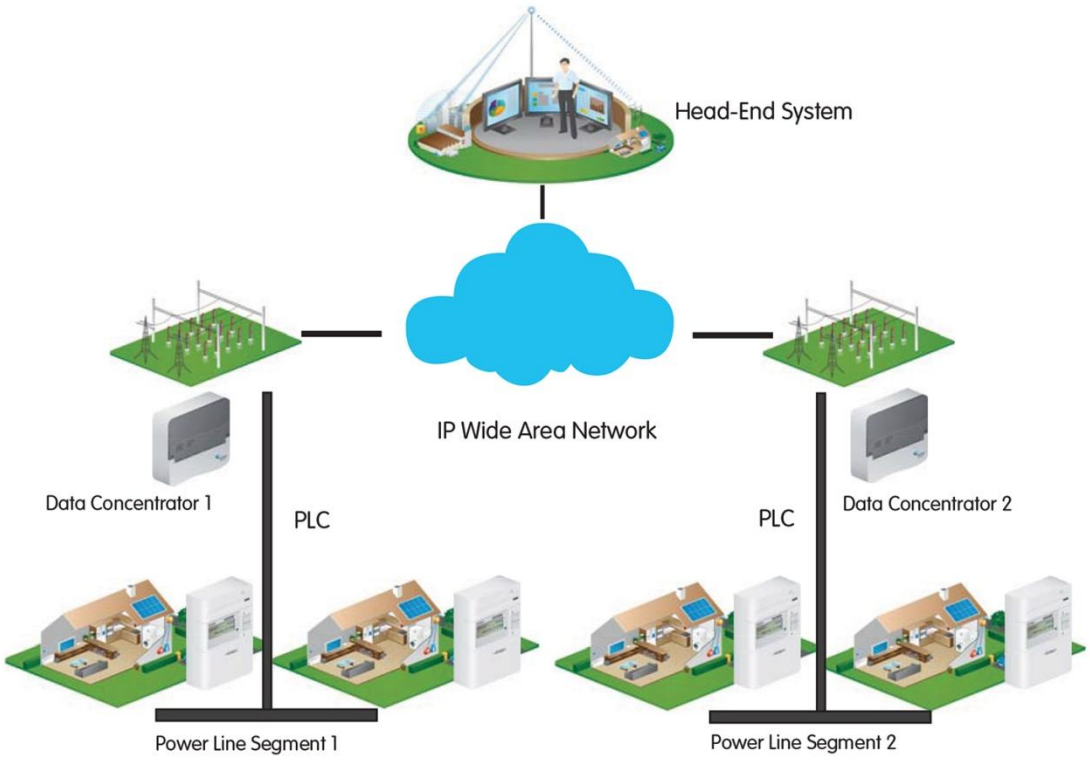
Η τεχνολογία AMI αποτελείται από διαφορετικά δίκτυα επικοινωνίας, τα οποία είναι:

- Home Area Network (HAN): Το οικιακό δίκτυο είναι ένα είδος τοπικού δικτύου με έξυπνους μετρητές στον πυρήνα του. Οι οικιακές συσκευές συνδέονται με τον έξυπνο μετρητή μέσω ασύρματου καναλιού (π.χ. ZigBee),

το οποίο βοηθάει στην παρακολούθηση και τον έλεγχο χρήσης των οικιακών τους συσκευών, για οικονομικότερη διαχείριση.

- Neighborhood Area Network (NAN): Το γειτονικό δίκτυο είναι ένα δίκτυο το οποίο αποτελείται από «γειτονικούς» μετρητές. Ένας συλλέκτης στο δίκτυο αυτό λαμβάνει τη συνολική μετρούμενη ενέργεια από όλους τους έξυπνους μετρητές της περιοχής. Σε αυτό το δίκτυο προτείνεται τεχνολογία WiFi.
- Wide Area Network (WAN): Το δίκτυο ευρείας περιοχής χρησιμεύει για την σύνδεση των συλλεκτών του NAN και των κέντρων ελέγχου της εταιρείας. Σε αυτό το δίκτυο μεταφέρονται εκατομμύρια δεδομένα μετρήσεων και απαιτείται ικανοποιητικό εύρος ζώνης και αξιοπιστία. Ως εκ τούτου, η κύρια προτεινόμενη τεχνολογία επικοινωνίας είναι οι οπτικές ίνες [4].

Βασικό χαρακτηριστικό της τεχνολογίας AMI, είναι η ικανότητα του έξυπνου μετρητή να συλλέγει δεδομένα ανά τακτά χρονικά διαστήματα για την κατανάλωση ισχύος κάθε συσκευής ενός οικιακού δικτύου. Τα δεδομένα αυτά, αποστέλλονται και είναι άμεσα διαθέσιμα στον πάροχο ηλεκτρικής ενέργειας, καθώς οι μετρήσεις αναφέρονται σε πραγματικό χρόνο (ή στη χειρότερη περίπτωση τα δεδομένα είναι διαθέσιμα την επόμενη μέρα). Επομένως, υπάρχει μια σαφής εικόνα για τη ζήτηση ηλεκτρικής ενέργειας κάθε χρονική στιγμή. Οι μετρήσεις αυτές μπορούν να προωθηθούν στο σύστημα SCADA, με σκοπό την εξισορρόπηση παροχής και ζήτησης και την παραγωγή κατάλληλων σημάτων τιμολόγησης. Στο Σχήμα 1.1, φαίνεται η αρχιτεκτονική αναπαράσταση του AMI.



Σχήμα 1.1 : Αρχιτεκτονική της τεχνολογίας AMI [11]

Πέρα από νέες αλληλεπιδράσεις των πελατών και του δικτύου, οι έξυπνοι μετρητές προϋποθέτουν νέα μέτρα ασφάλειας. Οι προηγούμενοι μηχανισμοί ανίχνευσης παραβίασης μετρητών περιορίζονταν σε κλειδαριές ασφαλείας. Παρ' όλο που οι παλαιότερες μέθοδοι ήταν επαρκείς ώστε να διαφυλάξουν την εντιμότητα, δεν ενδείκνυνται για την αποτροπή κακόβουλης αλλοίωσης, με αποτέλεσμα στη σημερινή εποχή να κατατροπώνονται. Οι έξυπνοι μετρητές ρυθμίζονται, ώστε να συνδέουν γεγονότα, που αφορούν το ιστορικό ζήτησης και τις συνθήκες του περιβάλλοντος των μετρητών. Αυτό περιλαμβάνει την ανίχνευση γεγονότων, που υποδεικνύουν κάποια φυσική παραβίαση. Ένας τέτοιος μηχανισμός, είναι η διακοπή καταγραφών σε περιόδους κατά τις οποίες η τάση πέφτει ή αφαιρείται από τους αισθητήρες του μετρητή. Η αντίστροφη ροή ενέργειας, η οποία συνδέεται με την αναστροφή της υποδοχής του μετρητή, μπορεί επίσης να ανιχνευθεί μέσω του λογισμικού του μετρητή. Εάν όμως, οι πελάτες διαθέτουν διεσπαρμένη παραγωγή, η αντίστροφη ροή ενέργειας δεν είναι πλέον ενδεικτική της αναστροφής του μετρητή. Σε αυτήν την περίπτωση είναι απαραίτητες πρόσθετες ανιχνεύσεις παραβίασης, για να γίνει σωστή διάκριση της αλλοιωμένης καταγραφής του μετρητή και εκείνης που πραγματικά λαμβάνεται από το δίκτυο[5].

Οι τεχνολογίες AMI έχουν ταχέως ξεπεράσει τις παραδοσιακές τεχνολογίες μέτρησης ενέργειας και εκατομμύρια έξυπνων μετρητών έχουν εξοπλίσει τις κατοικίες σε όλο τον κόσμο. Για παράδειγμα, υπάρχουν ήδη πάνω από 4,7 εκατομμύρια έξυπνοι μετρητές, που χρησιμοποιούνται για πληρωμές και άλλους σκοπούς, στο Οντάριο του Καναδά. Σύμφωνα με το Αμερικάνικο Ινστιτούτο

Ηλεκτρικής Αποδοτικότητας (IEE), περίπου 36 εκατομμύρια έξυπνοι μετρητές εγκαταστάθηκαν στις Ηνωμένες πολιτείες μέχρι τον Μάιο του 2012, και επιπλέον 30 εκατομμύρια αναμένεται να αναπτυχθούν τα επόμενα χρόνια.[4][7].

1.3 Τεχνικές και Μη τεχνικές Απώλειες στα συστήματα Μεταφοράς και Διανομής Ηλεκτρικής Ενέργειας

Η οικονομία του συστήματος ηλεκτρικής ενέργειας επηρεάζεται από ορισμένες απώλειες. Είναι ευρέως γνωστό το γεγονός ότι δεν φθάνει στον τελικό καταναλωτή όλη η ενέργεια, που παρέχεται από το βοηθητικό σύστημα διανομής. Μια σημαντική ποσότητα χάνεται στα συστήματα διανομής μέσω των τεχνικών και μη τεχνικών απωλειών, οι οποίες αναλύονται ακολούθως.

Α) Τεχνικές Απώλειες (Technical Losses, TLs)

Οι τεχνικές απώλειες στα συστήματα ισχύος προκαλούνται από τις φυσικές ιδιότητες των συστατικών του συστήματος ισχύος. Το πιο προφανές παράδειγμα είναι η ισχύς, που χάνεται, λόγω της εσωτερικής ηλεκτρικής αντίστασης των γραμμών μεταφοράς και μετασχηματιστών. Υπολογίζονται και ελέγχονται, εφόσον το σύστημα ενέργειας αποτελείται από γνωστές ποσότητες φορτίων. Σχετίζονται με τις απώλειες της γραμμής, δηλαδή την αντίσταση απωλειών των πρωτογενών τροφοδοτών, τις απώλειες του μετασχηματιστή διανομής(αντίσταση απωλειών στις περιελίξεις και στις απώλειες πυρήνα), την αντίσταση απωλειών στο δευτερεύον του δικτύου, την αντίσταση απωλειών στις εναέριες συνδέσεις, και τις απώλειες μετρητών kWh. Επομένως, οι απώλειες αυτές είναι σύμφυτες με την διανομή της ηλεκτρικής ενέργειας και δεν εξαλείφονται[8].

Β) Μη-τεχνικές απώλειες (Non technical Losses, NTLs)

Οι μη τεχνικές απώλειες προκαλούνται από δράσεις εκτός του συστήματος τροφοδοσίας ή προκαλούνται από τα φορτία υπό τον όρο ότι ο υπολογισμός των τεχνικών απωλειών δεν λαμβάνεται υπόψη. Είναι δυσκολότερο να μετρηθούν, λόγω του ότι οι συχνά αγνοούνται από τους διαχειριστές του συστήματος και ως εκ τούτου δεν φέρουν καταγεγραμμένες πληροφορίες. Προκύπτουν ως αποτέλεσμα κλοπής, ανακριβειών μέτρησης και μη μετρήσιμης ενέργειας. Έτσι, θεωρείται ότι αφορούν κυρίως την κλοπή ρεύματος οποιασδήποτε μορφής. Η δράση της κλοπής στην ηλεκτρική ενέργεια αποδίδεται στους πελάτες. Αυτό μπορεί να συμβεί ως αποτέλεσμα αλλοίωσης του μετρητή ή παράκαμψής του. Οι απώλειες, λόγω ανακρίβειας στις μετρήσεις, ορίζονται ως η διαφορά μεταξύ του ποσού ενέργειας, που πράγματι παραδίδεται μέσω των μετρητών, και του ποσού που καταχωρείται από τους μετρητές. Οι πιο πιθανές αιτίες μη τεχνικών απωλειών είναι [8]:

1) Αλλοίωση δια χειρός των μετρητών, ώστε να καταγράφονται μετρήσεις χαμηλότερης κατανάλωσης
2) Λάθη στον υπολογισμό των τεχνικών απωλειών
3) Αλλοίωση (σύνδεση) σε γραμμές χαμηλής τάσης
4) Διευθέτηση ψευδών αναγνώσεων δωροδοκώντας τους υπεύθυνους ανάγνωσης των μετρήσεων
5) Κλοπή παρακάμπτοντας τον μετρητή ή με άλλο παράνομο τρόπο σύνδεσης
6) Λανθασμένη μέτρηση ενέργειας ή μη μετρούμενη παροχή
7) Λάθη και καθυστερήσεις στην ανάγνωση του μετρητή και στη πληρωμή

Η έλλειψη εμπιστοσύνης στους πελάτες ηλεκτρισμού είναι ένα πρόβλημα που χρήζει αντιμετώπισης από της εταιρείες ενέργειας. Η εύρεση αποδοτικών μέτρων για την ανίχνευση δόλιων καταναλώσεων ενέργειας αποτελεί μία ενεργή περιοχή έρευνας τα τελευταία χρόνια. Οι μη τεχνικές απώλειες συνδέονται άμεσα με ρευματοκλοπές σε μια περιοχή. Ως αποτέλεσμα, κατά την διανομή της ηλεκτρικής ενέργειας, δημιουργούν σοβαρό πρόβλημα στις αναπτυσσόμενες χώρες και οι εταιρείες δυσκολεύονται να τις ανιχνεύσουν και να τις καταπολεμήσουν. Αυτές οι απώλειες επιδρούν στην ποιότητα του αποθέματος, αυξάνουν το φορτίο στο σταθμό παραγωγής, και επηρεάζουν την διατίμηση, που επιβάλλεται στο σύνολο των πελατών. Σε πολλές αναπτυσσόμενες χώρες, το ποσό των μη τεχνικών απωλειών υπολογίζεται σε περίπου 10-40% της συνολικής ικανότητας παραγωγής[10].

1.4 Η κλοπή ενέργειας παγκοσμίως

Παγκοσμίως, οι μη τεχνικές απώλειες στα συστήματα μεταφοράς και διανομής (T&D) αντιπροσωπεύουν ποσότητα ενέργειας μεγαλύτερη και από την συνολική εγκατεστημένη ικανότητα παραγωγής στη Γερμανία, στο Ηνωμένο Βασίλειο και στη Γαλλία. Εκτιμάται ότι, χάνονται από τις επιχειρήσεις ηλεκτρισμού σε όλο τον κόσμο πάνω από 25 δισεκατομμύρια δολάρια κάθε χρόνο, λόγω κλοπής στην ενέργεια,. Στην Ινδία χάνονται περίπου 4,5 δις. δολάρια κάθε χρόνο[10]. Η ανάκτηση του 10% των οποίων θα μπορούσε να διατηρήσει περίπου 83.000 GWh ηλεκτρικής ενέργειας και να μειώσει την εκπομπή διοξειδίου του άνθρακα κατά 9,2 εκατομμύρια τόνους ετησίως[12]. Η απώλεια, περίπου 4,5 δις δολαρίων ετησίως, που θα μπορούσε να θεωρηθεί ίση ή μεγαλύτερη από το συνολικό κέρδος, σημαίνει ότι αυτές οι εταιρείες κοινής ωφέλειας προμηθεύουν ενέργεια χωρίς κέρδος, ή ακόμα και με οικονομικές απώλειες. Επομένως είναι αναπόφευκτη, η σχεδίαση ενός μηχανισμού από τις εταιρείες ηλεκτρισμού, ο οποίος θα μειώνει τις μη τεχνικές απώλειες και θα ελέγχει τις πράξεις κλοπής [10].

Στην Ινδία, η υιοθέτηση πολλών προγραμμάτων ευαισθητοποίησης και πρωτοβουλιών από την κυβέρνηση έχουν ρίξει τις συνολικές απώλειες T&D από το

38,86% το 2001-2002 στο 34,54% το 2005-2006. Όπως διαπιστώνεται, παρόλο που υπάρχει κάποια μείωση στις απώλειες, χρειάζεται ακόμα βελτίωση του συστήματος διανομής ηλεκτρισμού για σωστή εκτίμηση και μείωση της ενεργειακής κλοπής. Υπό το πρίσμα αυτής της κατάστασης, θα ήταν απαραίτητη η εύρεση μιας αποδοτικής λύσης για τον εντοπισμό παρατυπιών. Το πρώτο βήμα σε αυτή την υπόθεση θα ήταν η αντικατάσταση των συμβατικών μετρητών ενέργειας με τους απαραβίαστους έξυπνους μετρητές[10].

Ανάμεσα σε όλες τις επιθέσεις στην τεχνολογία AMI, η κλοπή ενέργειας στις αναδυόμενες οικονομίες υπήρξε πολύ διαδεδομένη πράξη. Μια έκθεση της Παγκόσμιας Τράπεζας βρίσκει ότι έως και το 50% της ηλεκτρικής ενέργειας στις αναπτυσσόμενες χώρες αποκτάται μέσω κλοπής. Αναφέρεται, πως κάθε χρόνο μόνο στις Η.Π.Α χάνονται πάνω από 6 δις. δολάρια λόγω της κλοπής ενέργειας. Το 2009, το FBI ανέφερε μία μεγάλη και οργανωμένη προσπάθεια κλοπής ενέργειας, η οποία μπορεί να κόστισε μέχρι και 400 εκατ. δολάρια ετησία σε μια εταιρεία ακολουθούμενη την ανάπτυξη της τεχνολογίας AMI. Στον Καναδά, αναφέρονται 100 εκατ. δολάρια σε απώλειες κάθε χρόνο. Οι εταιρείες ηλεκτρισμού στην Βραζιλία υφίστανται απώλειες της τάξης των 5 δις. δολαρίων, λόγω της κλοπής ηλεκτρισμού. Υπάρχουν επίσης βίντεο στο διαδίκτυο, τα οποία υποδεικνύουν τον τρόπο αλλοίωσης ενός μετρητή. Σαν αποτέλεσμα, το θέμα της ενεργειακής κλοπής γίνεται μία από τις πιο σημαντικές ανησυχίες, που υπαγορεύουν την ανάπτυξη του AMI [4].

Σημαντικές πόλεις, όπως η Βομβάη και το Δελχί, υπολογίζουν έναν πολύ μεγάλο αριθμό μη τεχνικών απωλειών, περίπου το 30%. Αυτό συμβαίνει διότι μερικές συνεταιρικές επιχειρήσεις εκκρεμούν τις πληρωμές προς τις εταιρείες παροχής ενέργειας. Για παράδειγμα, στην Βομβάη ένα σοβαρό θέμα είναι η δράση του οργανωμένου εγκλήματος. Μέρος της δράσης αυτής είναι η κατάχρηση ηλεκτρισμού από τους μετασχηματιστές διανομής της περιοχής, χρησιμοποιώντας παράλληλο τοπικό δίκτυο. Ο εξοπλισμός φυλάσσεται κρυφά, προκειμένου να μην εντοπιστεί από την εταιρεία. Επιτρέπεται απεριόριστη χρήση ηλεκτρισμού με χρέωση περίπου 5 δολαρίων τον μήνα, συγκρίνοντας με ένα μέσο λογαριασμό των 15 δολαρίων για μια τετραμελή οικογένεια. Οι καταναλωτές σε δυσμενή οικονομική κατάσταση, με χαμηλό μηνιαίο εισόδημα, προτιμούν τέτοιες ηλεκτρικές συνδέσεις. Υπόψη αυτών των συμπεριφορών, οι εταιρείες παροχής ηλεκτρισμού χρειάζονται να συλλέξουν περίπου 2 δις. δολάρια από εκκρεμείς λογαριασμούς [10].

Στον Καναδά επίσης, το κίνητρο για την κλοπή ηλεκτρισμού είναι η αποφυγή πληρωμής για την θεωρημένη ηλεκτρική ενέργεια. Είναι μια προφανής κατάσταση για τους ανθρώπους που προωθούν μεγάλες ποσότητες μαριχουάνας και έτσι υποκλέπτουν ηλεκτρισμό, καθώς η κατανάλωση είναι πολύ υψηλή. Αυτό συμβαίνει και στις Ηνωμένες Πολιτείες, όπου οι άνθρωποι που καλλιεργούν παράνομα μαριχουάνα, διαπράττουν κλοπές ηλεκτρισμού, για να κρύψουν την συνολική τους κατανάλωση σε ηλεκτρισμό και να αποφύγουν τον έλεγχο και την δίωξη της

αστυνομίας. Η ηλεκτρική κλοπή έχει γίνει κυρίαρχη κατά την διάρκεια της οικονομικής ύφεσης και καταστολής του 2008-2009. Στο Πακιστάν, η κλοπή ηλεκτρικής ενέργειας είναι ένα κοινό φαινόμενο στις φτωχικές κατοικημένες περιοχές στις οποίες η παρουσία ενός τροφοδότη διανομής είναι ανέφικτη. Αυτό ονομάζεται σύστημα Kunda, το οποίο είναι αποδεκτό από τους εργαζόμενους της εταιρείας ως τρόπος ζωής σε περιοχές δυσμενούς οικονομικής κατάστασης και χωρίς επαρκή υποδομή. Έχει ανακαλυφθεί ότι ορισμένες κυβερνητικές υπηρεσίες, συμπεριλαμβανομένου του στρατού, οφείλουν μεγάλα ποσά χρημάτων στις εταιρείες ηλεκτρισμού. Το 2000 η εταιρεία παροχής ηλεκτρισμού στο Καράτσι (Karachi electric supply corporation, KESC) ανέφερε ότι μόνο το 52% των 1,67 εκατομμυρίων πελατών της πλήρωναν τους λογαριασμούς ηλεκτρισμού [10].

Κάποιες επιπλέον αναφορές για την κλοπή ενέργειας παγκοσμίως είναι [10]:

- Στην Μαλαισία, οι ομάδες ελέγχου αποκάλυψαν ότι 587 από 684 ύποπτες περιπτώσεις προέρχονται επιβεβαιωμένα από πράξεις κλοπής.
- Στο Μεξικό, υπολογίζεται ότι οι εταιρείες χάνουν περίπου 475 εκατομμύρια δολάρια έσοδα ετησίως.
- Στην Αρμενία, της Νοτίου Αφρικής, περίπου το 80-90% των κατοίκων απέφυγαν την πληρωμή ηλεκτρισμού. Στο Σοβέτο, περίπου 6 τόνοι καλωδίων, που χρησιμοποιούνται για παράνομη αλλοίωση, κατασχέθηκαν μέσα σε έξι μήνες.
- Στην Ινδονησία, η τοπική εταιρεία ηλεκτρισμού, ισχυρίστηκε ότι, περίπου 16,85 εκατομμύρια δολάρια πρέπει να συλλεχθούν από απλήρωτες υποθέσεις, εκ των οποίων ο στρατός οφείλει τα 3,1 εκατομμύρια δολάρια.
- Στην Τζαμάικα, η κλοπή ηλεκτρικού ρεύματος και η παραποίηση του μετρητή είναι κοινή σε πλούσιες περιοχές και εμπορικούς τομείς.
- Στην Βραζιλία, έγινε μια ανάλυση για την σχέση μεταξύ των μη τεχνικών απωλειών και των κοινωνικο-οικονομικών συνθηκών, η οποία έδειξε ότι οι περιοχές με υψηλό δείκτη εγκληματικότητας και χαμηλό εισόδημα είχαν μεγαλύτερες πιθανότητες να προβούν σε πράξεις αλλοίωσης της κατανάλωσής τους.

Το ηλεκτρικό δίκτυο αποτελεί μια αναγκαιότητα στη σύγχρονη κοινωνία. Χωρίς ένα σταθερό και αξιόπιστο δίκτυο ηλεκτρικής ενέργειας, δεκάδες των εκατομμυρίων καθημερινές ζωές των ανθρώπων θα είχαν υποβαθμιστεί δραματικά. Για παράδειγμα, η συσκότιση στην Ινδία τον Ιούλιο του 2012 επηρέασε πάνω από 60 εκατομμύρια ανθρώπους (περίπου το 9% του παγκόσμιου πληθυσμού) και βύθισε 20 από τις 28 πολιτείες της Ινδίας στο σκοτάδι. Πράγματι, το παραδοσιακό δίκτυο ενέργειας, το οποίο παραμένει ακόμα σταθερό στο σχεδιασμό για πάνω από 100 χρόνια, δεν υφίσταται πλέον κατάλληλο για την σημερινή κοινωνία. Με την ανάπτυξη του συστήματος τεχνολογίας πληροφοριών και επικοινωνιών, πολλές χώρες έχουν εκσυγχρονίσει τη γήρανση του συστήματος ρεύματος με το έξυπνο δίκτυο, το οποίο

χαρακτηρίζεται από μια αμφίδρομη μετάδοση, υψηλή αξιοπιστία, ανταπόκριση της ζήτησης σε πραγματικό χρόνο, αυτοίαση και ασφάλεια [4][14].

1.5 Θέματα Απάτης

1.5.1 Επιπτώσεις απάτης στην ενέργεια

Οι επιπτώσεις από απάτη στην ηλεκτρική ενέργεια είναι σοβαρές και επικίνδυνες και επηρεάζουν τόσο την εταιρεία παροχής ηλεκτρισμού όσο και τους καταναλωτές. Από μια τέτοιου είδους δράση επιβαρύνεται η μονάδα παραγωγής και επηρεάζεται η ποιότητα της παροχής ηλεκτρισμού. Αυτό συμβαίνει διότι, η εκάστοτε εταιρεία δεν μπορεί να εκτιμήσει σωστά την ποσότητα του ηλεκτρισμού, που χρειάζεται να δοθεί σε όλους τους καταναλωτές, είτε είναι τίμιοι είτε παράνομοι. Αυτή η υπερφόρτωση οδηγεί σε υπέρταση, επηρεάζει την απόδοση και προκαλεί βλάβες στις συσκευές των καταναλωτών. Το μεγάλο ποσό μη τεχνικών απωλειών είναι ικανό να καθυστερήσει την μονάδα παραγωγής και με επακόλουθα την διακοπή παροχής ρεύματος σε όλους τους πελάτες, περιόδους χαμηλής τάσης και διακοπές ρεύματος κατά τη διάρκεια των περιόδων αιχμής φορτίου. Προκειμένου να διατηρηθούν σε καλά επίπεδα ο συντελεστής ισχύος και το επίπεδο τάσης κατά μήκος των τροφοδοτών, πρέπει να παρέχεται επαρκής άεργος ισχύς μαζί με το παρεχόμενο ηλεκτρικό ρεύμα, κάτι το οποίο δεν είναι εφικτό χωρίς πλήρεις πληροφορίες σχετικά με την συνολική ροή φορτίου. Αποτελεί, έτσι, μία αρνητική συνέπεια η απώλεια φορτίου για την αντιστάθμιση της κατάρρευσης της τάσης κατά τη διάρκεια αιχμής φορτίου[10][15].

Το σημαντικό ποσό εσόδων, που χάνουν οι εταιρείες παροχής ηλεκτρισμού από μη τεχνικές απώλειες στις αναπτυσσόμενες χώρες, καθιστά αναγκαία την ανάπτυξη συστημάτων ελέγχου τους. Επιπλέον, οι εταιρείες αναγκάζονται να επιβάλουν υψηλότερη τιμολόγηση σε όλους τους πελάτες, ώστε να αντέξουν οικονομικά, κάτι το οποίο δεν θεωρείται ηθικό απέναντι σε τίμιους πελάτες. Ακόμα, η κλοπή ηλεκτρικού ρεύματος εγείρει ανησυχίες για την ασφάλεια, όπως ατυχημάτων ηλεκτροσόκ από ακατάλληλο χειρισμό του τροφοδότη διανομής και των καλωδίων με εμφάνιση σπινθήρων και επιπτώσεις, όπως πυρκαγιά κατά τη διάρκεια ακραίων καιρικών συνθηκών [10].

1.5.2 Λόγοι που οδηγούν σε κλοπή ρεύματος

Υπάρχουν μερικοί παράγοντες που ενθαρρύνουν τους ανθρώπους να υποκύψουν στην απάτη ηλεκτρισμού, από τους οποίους οι περισσότεροι είναι κυρίως κοινωνικο-οικονομικοί. Μερικοί από αυτούς είναι [10]:

- Η κοινή αντίληψη των παράνομων καταναλωτών ότι δεν θεωρούν ανέντιμη μια δράση απάτης απέναντι στο κράτος ή στη δημόσια επιχείρηση κοινής ωφέλειας.
- Ο αυξανόμενος δείκτης ανεργίας και η δυσμενής οικονομική κατάσταση
- Η έλλειψη ενημέρωσης σχετικά με θέματα που αφορούν τους νόμους και τα αδικήματα, που σχετίζονται με κλοπή
- Η υπερτιμολόγηση της ηλεκτρικής ενέργειας στην εν λόγω περιοχή
- Οι χώρες με αδύναμη επιβολή του νόμου κατά της κλοπής ηλεκτρικού ρεύματος παρουσιάζουν ρεκόρ υψηλού ποσοστού κλοπών

1.5.3 Μέθοδοι απάτης

Ο κύριος λόγος για τον οποίο προβαίνει κάποιος σε απάτη, είναι η μείωση του λογαριασμού της πραγματικής τιμής καταναλισκόμενης ενέργειας. Οι τεχνικές απάτης διακρίνονται σε τρεις κατηγορίες [17]:

1) <u>Επιθέσεις που γίνονται απευθείας από τον άνθρωπο</u>

Αυτού του τύπου οι επιθέσεις συμβαίνουν κυρίως, είτε παραβιάζοντας μία εξωτερική πηγή, όπως είναι ο τροφοδότης διανομής, είτε παραβιάζοντας τον μετρητή, ώστε να δίνεται η επιθυμητή μέτρηση κατανάλωσης. Το τελευταίο μπορεί να γίνει με εισαγωγή μαγνητών στο εσωτερικό του μετρητή, οι οποίοι παρεμβαίνουν μέσω ηλεκτρομαγνητικών κινητήρων ή μετασχηματιστών ρεύματος. Ακόμη μπορεί να γίνει αντιστρέφοντας ή αποσυνδέοντας τον μετρητή. Σε επίπεδο δικτύου, οι εισβολείς συνήθως προσπερνούν τον μετρητή και συνδέουν συσκευές υψηλής κατανάλωσης άμεσα με το δίκτυο, ή συνδέουν ολόκληρο το ηλεκτρικό σύστημα σε έναν εξωτερικό τροφοδότη με ένα πειρατικό μετασχηματιστή.

2) <u>Η επίθεση μέσω κυβερνοχώρου</u>

Η δικτυακή επικοινωνία και οι έξυπνες συσκευές στο δίκτυο έχουν φέρει νέες πτυχές απάτης. Οι επιθέσεις στον κυβερνοχώρο έχουν πρόσφατα αναλυθεί και περιλαμβάνουν διακοπή των μετρήσεων, κερδίζοντας προνομιούχα πρόσβαση στο λογισμικό του μετρητή ή παραποιώντας την αποθήκευση του μετρητή και παρακολουθώντας τις επικοινωνίες του, με σκοπό να διακόπτονται ή να μεταβάλλονται οι τιμές κατανάλωσης, που καταγράφηκαν.

3) <u>Επιθέσεις στα δεδομένα</u>

Οι επιθέσεις αυτού του τύπου έχουν στόχο τις καταγραφείσες τιμές του μετρητή και γίνονται μέσω της πρώτης και δεύτερης κατηγορίας, που προαναφέρθηκαν.

Συνοψίζοντας, επιγραμματικά οι επιμέρους τύποι επιθέσεων σύμφωνα με την κάθε κατηγορία είναι[17]:

- Μέσω Κυβερνοχώρου
    - Έλεγχος μετρητών μέσω εκμετάλλευσης απομακρυσμένου δικτύου
    - Τροποποίηση του λογισμικού/αποθήκης του μετρητή
    - Κλοπή διαπιστευτηρίων (username,password) για σύνδεση σε μετρητές
    - Εξάντληση της CPU/μνήμης
    - Διακοπή/Αλλαγή επικοινωνίας
    - Κατακλυσμός του εύρους ζώνης NAN (Neighborhood Area Network)

- Μέσω άμεσης φυσικής επαφής
    - Αλλοίωση του μετρητή
    - Αντιστροφή του μετρητή
    - Αποσύνδεση του μετρητή
    - Εξαγωγή του κωδικού πρόσβασης
    - Κατάχρηση της οπτικής θύρας για απόκτηση πρόσβασης στον μετρητή
    - Παράκαμψη του μετρητή για την αφαίρεση φορτίων από τις μετρήσεις

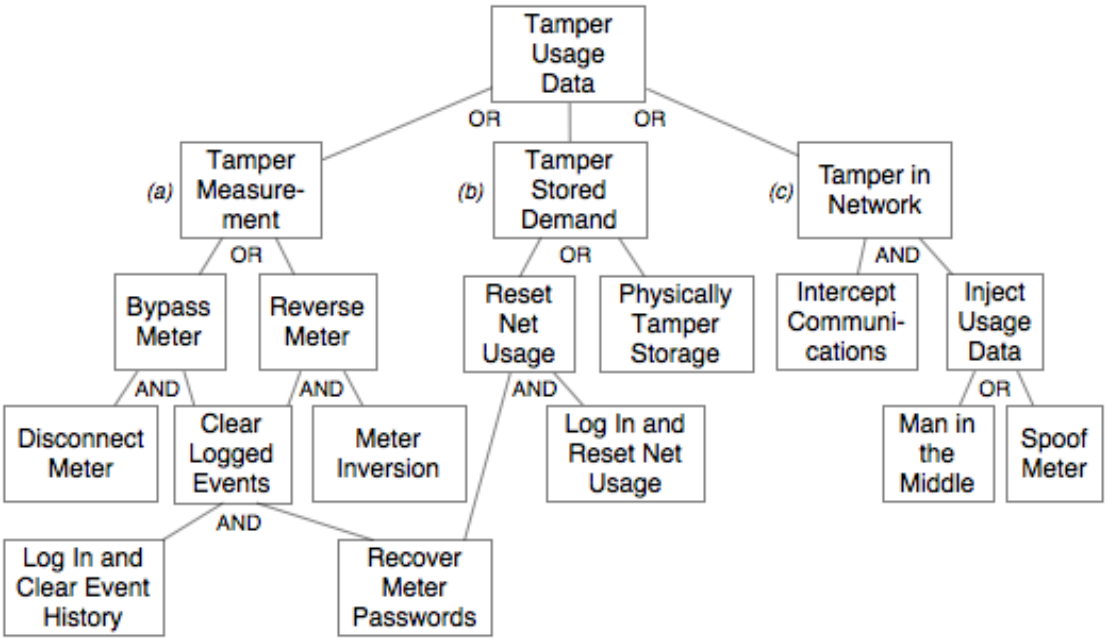
- Μέσω Δεδομένων
    - Διακοπή της αναφοράς ολόκληρης της κατανάλωσης
    - Αφαίρεση μεγάλων συσκευών από την μέτρηση
    - Αποκοπή της έκθεσης ορισμένου ποσού
    - Αλλαγή της συσκευής προφίλ φορτίου για την απόκρυψη μεγάλων φορτίων
    - Αναφορά μηδενικής κατανάλωσης
    - Αναφορά αρνητικής κατανάλωσης (δρα ως γεννήτρια)

1.5.4 Το δέντρο επίθεσης

Οι τεχνικές απάτης διακρίνονται, ακόμα καλύτερα, μέσα από το δέντρο επίθεσης. Το δέντρο επίθεσης κατακερματίζει έναν κύριο στόχο σε υπο-στόχους, έως ότου επιτευχθεί ένας ικανοποιητικός αριθμός στρατηγικών επίθεσης. Σε αυτή την περίπτωση, κύριος στόχος είναι η παραποίηση/πλαστογράφηση της ζήτησης. Το δέντρο επίθεσης απαριθμεί όλες τις δυναμικές δράσεις, τις οποίες ένας πιθανός εισβολέας θα μπορούσε να χρησιμοποιήσει για την απόκτηση πρόσβασης στο σύστημα-στόχο. Κάθε κλαδί του δέντρου αντιπροσωπεύει μια σειρά από ενδιάμεσα βήματα, τα οποία λαμβάνονται για την απόκτηση πρόσβασης στο σύστημα- στόχο, ο οποίος αποτελεί τη ρίζα του δέντρου. Τα παιδιά-κόμβοι αντιπροσωπεύουν τις συγκεκριμένες επιθέσεις, που πρέπει να γίνουν για την επίτευξη του. Ύστερα, κάθε παιδί-κόμβος, που δεν διαιρείται παραπάνω, γίνεται φύλλο-κόμβος. Διαφορετικά, οι εν λόγω κόμβοι αντιμετωπίζονται ως υπο-στόχοι, με σκοπό να αποσυντεθούν μέχρι όλα τα γεγονότα να γίνουν φύλλα-κόμβοι[4].

Τα μονοπάτια/κόμβοι προς τον τελικό στόχο συνδέονται με τις λογικές πύλες ΚΑΙ (AND) και Η΄ (OR). Οι πύλες καθορίζουν, εάν πρέπει να ολοκληρωθούν ένα ή όλα τα παιδιά σε έναν εσωτερικό κόμβο, προκειμένου να επιτευχθεί ο τελικός στόχος. Στην ουσία, η OR-πύλη αντιπροσωπεύει εναλλακτικές μεθόδους επίθεσης, ενώ η AND-πύλη αντιπροσωπεύει διαφορετικά βήματα, τα οποία πρέπει να γίνουν για την επίτευξη του[4].

Ένα παράδειγμα δέντρου επίθεσης φαίνεται παρακάτω:



Σχήμα 1.2 : Ένα δέντρο επίθεσης με τα φύλλα να αναγράφουν τις απαραίτητες επιθέσεις που χρειάζονται για μια επίθεση στην ενέργεια[16]

Η «Κλοπή Ενέργειας» ορίζεται ως τελικός στόχος του εισβολέα. Η διαδικασία της κατασκευής του δέντρου επίθεσης για την κλοπή στο AMI περιγράφεται ως εξής[4]:

- Ορισμός του γενικού στόχου του εισβολέα «G- Κλοπή Ενέργειας» στην τεχνολογία AMI.
- Αποσύνθεση του στόχου G σε υπό-στόχους: διακοπή μέτρησης, παραβίαση αποθηκευμένης ζήτησης, τροποποίηση δικτύου. Ο σκοπός του εισβολέα μπορεί να επιτευχθεί, εάν πραγματοποιηθεί ένα από τα τρία συστατικά. Αυτή η λίστα μπορεί να είναι εκτεταμένη και να προστεθούν περισσότεροι υπό-στόχοι.
- Συνέχιση της σταδιακής αποσύνθεσης, έως ότου η εργασία να μην διαιρείται σε επιμέρους.

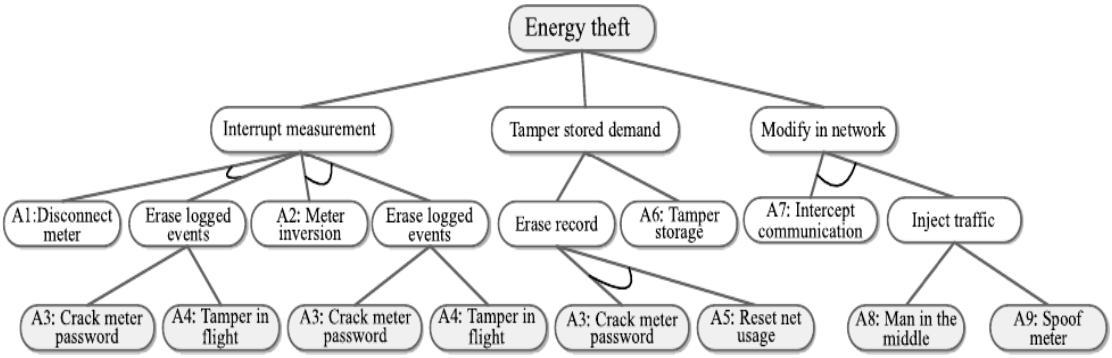
Τρεις τρόποι για την επίτευξη του στόχου «Κλοπή Ενέργειας», είναι :

- **Διακοπή Μέτρησης** (Interrupt Measurement): Αυτή η επίθεση λαμβάνει χώρα πριν ο έξυπνος μετρητής καταγράψει μια μέτρηση της ζήτησης. Έχει στόχο να αποτρέψει τον έξυπνο μετρητή από την μέτρηση της κατανάλωσης ηλεκτρικής ενέργειας. Υπάρχουν δύο τρόποι για την διάπραξη της συγκεκριμένης επίθεσης· Ο πρώτος είναι η αποσύνδεση του μετρητή. Ο δεύτερος είναι η αντιστροφή του μετρητή. Τα καταγεγραμμένα συμβάντα, που δείχνουν την διακοπή ή την αντιστροφή της ροής της, διαγράφονται, ώστε να μην είναι ανιχνεύσιμα από την εταιρεία ηλεκτρισμού [4].

- **Αλλοίωση της αποθηκευμένης ζήτησης** (Tamper stored demand): Ο εισβολέας παρεμβαίνει στα δεδομένα, που είναι αποθηκευμένα στον έξυπνο μετρητή, για την επίτευξη κλοπής. Αυτό συμβαίνει δεδομένου ότι, η συμπεριφορά του έξυπνου μετρητή είναι ελεγχόμενη από αυτά τα δεδομένα (όπως τα τιμολόγια για TOU τιμολόγηση, τα αρχεία καταγραφής και των δύο φυσικών γεγονότων και εκτελούμενων εντολών, η καταγεγραμμένη εντολή δικτύου). Άλλος τρόπος για την αλλοίωση της αποθηκευμένης ζήτησης είναι η διαγραφή των σχετικών αρχείων, τα οποία είναι αρχεία ελέγχου καταγραφής της συνολικής κατανάλωσης. Αυτά τα αρχεία μπορεί να προσπελαστούν από διοικητικές διασυνδέσεις, που χρειάζονται κωδικούς πρόσβασης [4].

- **Τροποποίηση του δικτύου** (Modify in network): Η επίθεση αυτή διοχετεύει άμεσα τα ψευδή στοιχεία στο δίκτυο επικοινωνίας μεταξύ των έξυπνων μετρητών και της εταιρείας κοινής ωφέλειας. Ο εισβολέας υλοποιεί δύο βήματα για την επίτευξη αυτού του υπό-στόχου : την υποκλοπή επικοινωνίας και της έκχυση της κυκλοφορίας. Μετά από επιτυχή παρεμπόδιση των δεσμών μεταξύ των έξυπνων μετρητών και του συλλέκτη, ένας «άνθρωπος στη μέση της επίθεσης» ή ένας «μετρητής πλαστής επίθεσης» χρησιμοποιείται για την αποστολή πλαστών αρχείων καταγραφής δεδομένων και συμβάντων [4].

Στο Σχήμα 1.3 επίσης απεικονίζεται ένα δέντρο επίθεσης με τα παραπάνω στάδια.



Σχήμα 1.3 : Το δέντρο επίθεσης στην κλοπή ενέργειας [4]

1.5.5 Απαιτήσεις ασφάλειας του συστήματος

Κάθε τμήμα της τεχνολογίας AMI έχει τις δικές του απαιτήσεις ασφαλείας. Για παράδειγμα, οι πελάτες ενδιαφέρονται για την προστασία των πληροφοριών/μετρήσεων τους και την τακτική χρήση της ηλεκτρικής ενέργειας. Από την άλλη, οι εταιρείες ηλεκτρισμού στοχεύουν στην παροχή σταθερού ενεργειακού εφοδιασμού και στην πρόληψη κλοπών. Σε γενικές γραμμές, τα ευαίσθητα σημεία, που πρέπει να προστατευθούν στο δίκτυο AMI, ταξινομούνται ως εξής [4] :

- Δεδομένα έξυπνων μετρητών (Smart meter data): Τα δεδομένα, τα οποία συλλέγονται από τους έξυπνους μετρητές, δεν πρέπει να προσεγγίζονται από οποιαδήποτε μη εξουσιοδοτημένη οντότητα.
- Έλεγχος δεδομένων (Control data): Η εντολή ελέγχου λαμβάνεται και υλοποιείται ορθά και πλήρως από τους έξυπνους μετρητές.
- Πληροφορίες λογαριασμού (Bill Information): Η τιμή της ηλεκτρικής ενέργειας και ο λογαριασμός, που καταβάλλεται στην εταιρεία κοινής ωφέλειας, δεν πρέπει να χειραγωγείται από μη εξουσιοδοτημένες οντότητες.
- Προσωπικές πληροφορίες καταναλωτών (Customer’s personal information): Αυτές οι πληροφορίες περιλαμβάνονται στα στοιχεία μιας πιστωτικής κάρτας, στην ημερήσια χρήση ηλεκτρισμού, και ούτω καθεξής.

Με βάση τους παραπάνω ευαίσθητους στόχους, οι απαιτήσεις ασφάλειας του AMI ταξινομούνται ως εξής[4]:

- *Εμπιστευτικότητα:* Οι ευαίσθητες πληροφορίες θα πρέπει να είναι προσπελάσιμες μόνο από εξουσιοδοτημένους φορείς
- *Ακεραιότητα:* Τα δεδομένα που διαβιβάζονται στο AMI, πρέπει να είναι αυθεντικά και να αντανακλούν σωστά τα δεδομένα προέλευσης, χωρίς οποιαδήποτε μη εξουσιοδοτημένη χειραγώγηση

- *Διαθεσιμότητα:* Τα δεδομένα στο AMI πρέπει να είναι προσβάσιμα από εξουσιοδοτημένους φορείς, όποτε χρειάζεται.
- *Μη αποκήρυξη:* Οποιαδήποτε παραλαβή, όπως αναθεωρημένη τιμή της ηλεκτρικής ενέργειας, δεν πρέπει να αποκηρύσσεται από την στιγμή που έχει ληφθεί. Επίσης, τα δεδομένα δεν μπορούν να αποκρύπτονται, για παράδειγμα η ποσότητα ηλεκτρικής ενέργειας, που έχει καταναλωθεί και δεν έχει αποσταλεί.
- *Προστασία Προσωπικών Δεδομένων:* Οποιαδήποτε ιδιωτική πληροφορία, από τα δημοσιευμένα στοιχεία μέτρησης, δεν μπορεί να μεταφέρεται .

Με σκοπό την ασφάλεια του συστήματος, είναι απαραίτητοι οι μηχανισμοί ασφαλείας στο υλικό του συστήματος AMI, καθώς δεν είναι επαρκής η προστασία του λογισμικού σε ανοιχτά δίκτυα επικοινωνίας.

Κεφάλαιο
2
Τεχνικές ανίχνευσης απάτης

2.1 Εισαγωγή

Ο εντοπισμός των κλοπών ενέργειας αποτελεί ένα από τα πιο δισεπίλυτα αλλά και σημαντικά θέματα, που πρέπει να αντιμετωπίσει ο διαχειριστής του δικτύου διανομής (ΔΔ). Η προσπάθεια του αυτή μπορεί πλέον να ενισχυθεί και από την εγκατάσταση έξυπνων μετρητών. Οι οικονομικοί λόγοι και η ανθρώπινη φύση που περιλαμβάνουν οι δράσεις κλοπής δεν μπορούν να παρατηρηθούν και να ελεγχθούν ακόμα και από το πιο προηγμένο εξοπλισμό μέτρησης. Γι' αυτό το λόγο, η ανίχνευση και ο εντοπισμός της κάθε απάτης στα συστήματα ηλεκτρικής ενέργειας συχνά αντιμετωπίζονται με στατιστικές τεχνικές. Σε αυτό το κεφάλαιο, παρουσιάζεται μια ταξινόμηση των τεχνικών ανίχνευσης για ρευματοκλοπές σε συστήματα έξυπνων μετρητών. Από αυτές τις τεχνικές διακρίνονται τρεις, οι οποίες αναλύονται, εξάγοντας κάποια συμπεράσματα για την κάθε τεχνική, ενώ στην παρούσα διπλωματική εργασία προτείνεται μία από αυτές για ανάλυση. Οι τρεις τεχνικές που θα αναλυθούν είναι: α) τεχνικές ταξινόμησης(classification), β) εκτίμηση κατάστασης (state estimation) και γ) θεωρία παιγνίων(game theory)[4].

2.2 Τεχνική Ανίχνευσης με αλγόριθμους ταξινόμησης

Από τις ευρέως χρησιμοποιούμενες τεχνικές ανίχνευσης κλοπής ενέργειας είναι η τεχνική της ταξινόμησης. Η τεχνική αυτή ταξινομεί τους καταναλωτές με βάση το προφίλ του φορτίου τους κατά τη διάρκεια μιας χρονικής περιόδου. Η βασική διαδικασία της ανίχνευσης αυτής αποτελείται από εφτά μέρη [4]:

α) Απόκτηση των δεδομένων

β) Προεπεξεργασία των δεδομένων

γ) Εξαγωγή χαρακτηριστικών

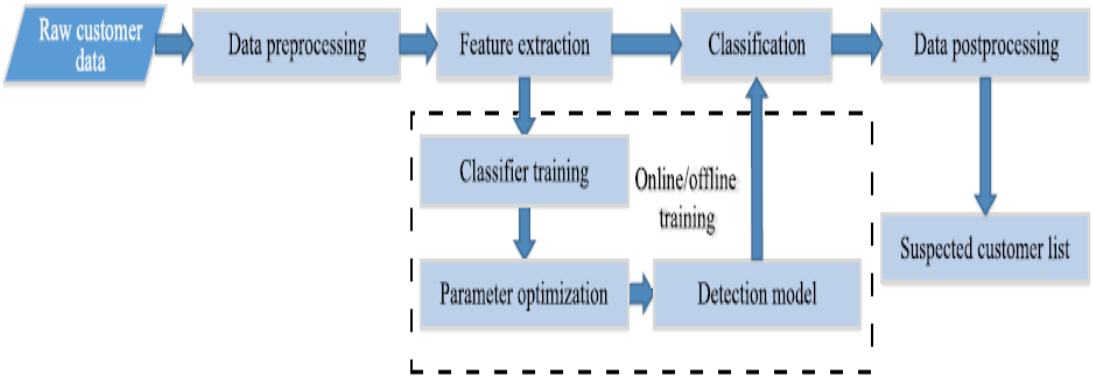
δ) Κατάρτιση του ταξινομητή

ε) Βελτιστοποίηση των παραμέτρων του ταξινομητή

στ) Ταξινόμηση

ζ) Επεξεργασία των αποτελεσμάτων και παραγωγή της λίστας με τους ύποπτους καταναλωτές

Οι τεχνικές της ταξινόμησης έχουν σαν στόχο να κατατάξουν τα πρότυπα ενός συνόλου δεδομένων καταναλωτών σε δύο τάξεις· την γνήσια τάξη και την τάξη επίθεσης (τάξη ρευματοκλοπών). Στο παρακάτω σχήμα φαίνεται ένα διάγραμμα, που περιγράφει την γενικευμένη ροή της διαδικασίας κατά την ταξινόμηση στα εφτά σημεία της.



Σχήμα 2.1 : Η βασική διαδικασία στην ταξινόμηση για την ανίχνευση κλοπών στην ενέργεια[4]

Οι μηχανές διανυσμάτων υποστήριξης (Support Vector Machines, SVM) είναι από τις πιο δημοφιλείς τεχνικές ταξινόμησης του φορτίου κάθε καταναλωτή και ανήκουν στις μεθόδους μηχανικής μάθησης. Οι μέθοδοι αυτές, δίνουν την ικανότητα σε μια μηχανή να αξιοποιεί προγενέστερη γνώση και εμπειρία, προκειμένου να βελτιώνεται η απόδοσή της σε μια συγκεκριμένη εργασία. Τα SVM εισήχθησαν από τον Vapnik[19] στα τέλη της δεκαετίας του 1960, θέτοντας τα θεμέλια της στατιστικής ανάλυσης. Ο αλγόριθμος με SVM μετασχηματίζει τα αρχικά δεδομένα προς ταξινόμηση, έτσι ώστε να είναι γραμμικά διαχωρίσιμα, και στη συνέχεια υπολογίζει το γραμμικό τους διαχωριστή. Ο μετασχηματισμός επιβάλλει τη «μεταφορά» των δεδομένων σε ένα νέο χώρο, όπου θα είναι δυνατός ο γραμμικός διαχωρισμός τους. Ο διαχωρισμός επιτυγχάνεται μέσω μιας συνάρτησης απεικόνισης φ.

$$\varphi : x \rightarrow \varphi(x)$$

Ουσιαστικά οι συναρτήσεις απεικόνισης μεταφέρουν τα δεδομένα σε ένα χώρο μετασχηματίζοντας τις συνιστώσες τους, από τη στιγμή που αναφέρονται σε δεδομένα-ανύσματα [4]. Το μαθηματικό μοντέλο στο οποίο στηρίζεται η ταξινόμηση με SVM αναλύεται παρακάτω.

Κατά την διαδικασία ανίχνευσης μιας απάτης, γίνεται συσχετισμός των μετρήσεων κατανάλωσης με τις μη τεχνικές απώλειες του δικτύου. Οι μη τεχνικές απώλειες αφορούν τις απώλειες, οι οποίες ανιχνεύονται σε σχέση με τη συνολική

παροχή του μετασχηματιστή μιας περιοχής και δεν οφείλονται σε απώλειες τεχνικές, όπως στις αντιστάσεις και στις γραμμές μεταφοράς. Έτσι, όταν υπάρχουν μη τεχνικές απώλειες, υπάρχουν και πολλές πιθανότητες να έχει διαπραχθεί κάποιου είδους απάτης στην περιοχή. Τα SVM έχουν συχνά συνδυαστεί με τη μέτρηση μη τεχνικών απωλειών στο μετασχηματιστή προκειμένου να ανιχνευθούν οι περιπτώσεις απάτης.

Μία προτεινόμενη μέθοδος εντοπισμού απάτης είναι ο συνδυασμός των αλγορίθμων SVM με τον Γενετικό Αλγόριθμο (Genetic Algorithm,GA)[20].Οι γενετικοί αλγόριθμοι ανήκουν στον κλάδο της επιστήμης των υπολογιστών και αποτελούν μια μέθοδο αναζήτησης βέλτιστων λύσεων σε συστήματα που μπορούν να περιγραφούν ως μαθηματικό πρόβλημα. Είναι χρήσιμοι σε προβλήματα που περιέχουν πολλές παραμέτρους/διαστάσεις και δεν υπάρχει αναλυτική μέθοδος εύρεσης του βέλτιστου συνδυασμού τιμών για τις μεταβλητές, ώστε το υπό εξέταση σύστημα να αποδίδει με τον επιθυμητό τρόπο. Ο τρόπος λειτουργίας των Γενετικών Αλγορίθμων είναι εμπνευσμένος από την βιολογία. Χρησιμοποιεί τις ιδέες της εξέλιξης μέσω γενετικής μετάλλαξης, φυσικής επιλογής και διασταύρωσης. Στην υλοποίηση τους, οι γενετικοί αλγόριθμοι είναι αρκετά απλοί. Οι τιμές για τις παραμέτρους του συστήματος πρέπει να κωδικοποιούνται με τέτοιο τρόπο, ώστε να αναπαριστώνται από μια μεταβλητή που περιέχει σειρά χαρακτήρων ή δυαδικών ψηφίων (0/1). Αρχικά, ο Γενετικός Αλγόριθμος παράγει πολλαπλά αντίγραφα της μεταβλητής, συνήθως με τυχαίες τιμές, δημιουργώντας έναν πληθυσμό λύσεων. Κάθε λύση (τιμές για τις παραμέτρους του συστήματος)ελέγχεται για το πόσο κοντά φέρνει την επιθυμητή αντίδραση στο σύστημα, μέσω μιας συνάρτησης που δίνει το μέτρο ικανότητας της λύσης και η οποία ονομάζεται Συνάρτηση Ικανότητας (Σ.Ι). Οι λύσεις που βρίσκονται πιο κοντά στην θεμιτή σύμφωνα τη Συνάρτηση Ικανότητας, αναπαράγονται στην επόμενη γενιά λύσεων και λαμβάνουν μια τυχαία μετάλλαξη. Επαναλαμβάνοντας αυτή τη διαδικασία για αρκετές γενιές, οι τυχαίες μεταλλάξεις, σε συνδυασμό με την επιβίωση και αναπαραγωγή των λύσεων που πλησιάζουν καλύτερα το επιθυμητό αποτέλεσμα, θα παράγουν μία λύση που θα περιέχει τις τιμές για τις παραμέτρους που ικανοποιούν όσο καλύτερα γίνεται την Σ.Ι. [21].

Στον συνδυασμό των SVM και Γενετικού Αλγόριθμου, πρώτα γίνεται η εκπαίδευση του μοντέλου ταξινόμησης με SVM και ύστερα η εφαρμογή του Γ.Α., για την βελτιστοποίηση των παραμέτρων του SVM, επιστρέφοντας τις βέλτιστες, ώστε να προχωρήσει η δοκιμή του ταξινομητή σε νέα δεδομένα[4].

Άλλες τεχνικές ταξινόμησης που χρησιμοποιούνται είναι η ασαφής ταξινόμηση (fuzzy classification) και τα νευρωνικά δίκτυα (neural networks) [4]. Στην ασαφή ταξινόμηση διακρίνουμε δύο στάδια· Στο πρώτο εκτελείται μια ασαφής ομαδοποίηση (fuzzy clustering) για να βρεθούν παρόμοια προφίλ κατανάλωσης. Μια τέτοια τεχνική είναι η Fuzzy C-means (FCM), τεχνική ομαδοποίησης δεδομένων, στην οποία ένα σύνολο δεδομένων ομαδοποιείται σε n συστάδες (clusters) με κάθε σημείο δεδομένων του συνόλου να ανήκει σε συστάδα με έναν ορισμένο βαθμό συμμετοχής. Ο αλγόριθμος, δηλαδή, δεν αντιστοιχίζει το κάθε αντικείμενο σε μια

μόνο ομάδα, αλλά υλοποιεί ασαφείς διαμερίσεις. Έτσι, κάθε αντικείμενο ανήκει σε όλες τις ομάδες με διαφορετικό βαθμό συμμετοχής για την καθεμία. Ο βαθμός κυμαίνεται ανάμεσα σε 0 και 1. Αυτού του είδους η τεχνική είναι ιδιαίτερα χρήσιμη σε περιπτώσεις που τα όρια μεταξύ των ομάδων δεν είναι ξεκάθαρα και καλά διαχωρισμένα [4].

Ο Fuzzy C-means είναι ένας επαναληπτικός αλγόριθμος καθώς και ένας από τους πιο δημοφιλείς fuzzy αλγορίθμους. Η βασική του ιδέα είναι να βρεθεί μία ομάδα (C fuzzy cluster) στην οποία ένα ορισμένο σημείο δεδομένων, που βρίσκεται κοντά στο κέντρο της, να έχει υψηλό βαθμό συμμετοχής σε αυτήν και ένα άλλο σημείο δεδομένων, που βρίσκεται μακριά από το κέντρο της, να έχει ένα χαμηλό βαθμό συμμετοχής στην ομάδα. Δύο τέτοιες ομάδες θα μπορούσαν να είναι των τίμιων και κακόβουλων καταναλωτών, κατηγοριοποιώντας με αυτό τον τρόπο τους καταναλωτές στις δύο ομάδες ανάλογα με τα χαρακτηριστικά των μετρήσεων τους[4].

Μια άλλη μεθοδολογία που προτείνεται και προαναφέρθηκε είναι τα νευρωνικά δίκτυα. Σε αυτή την περίπτωση υπάρχουν δύο βασικές ενότητες· μια για το φιλτράρισμα της βάσης δεδομένων και μία άλλη για την πραγματική κατάταξη των πελατών. Κάθε ενότητα αποτελείται από πέντε νευρωνικά δίκτυα. Κάθε δίκτυο έχει μια έξοδο που ταξινομεί τους πελάτες σε δύο κατηγορίες: τους παράνομους και τους νόμιμους. Το μοντέλο αυτό αξιολόγησης παρέχει μια πολύ καλή απόδοση στη χαμηλή τάση, βελτιώνοντας σε μεγάλο βαθμό τον τρέχοντα ρυθμό ανίχνευσης απάτης [22].

Η δοκιμή με τον Γενικευμένο Λόγο Πιθανοφάνειας (Generalized Likelihood Ratio, GLR) είναι ένας ακόμη τρόπος ανίχνευσης επίθεσης στην ενέργεια. Στηρίζεται στην μοντελοποίηση της κατανομής πιθανότητας των τίμιων και κακόβουλων προτύπων κατανάλωσης [23].Σε αυτή την περίπτωση, χρησιμοποιείται το μοντέλο ARMA (Auto Regressive Moving Average), με σκοπό την εξαγωγή μοντέλων κατανομής κατανάλωσης τίμιων και κακόβουλων πελατών. Υποθέτεται ότι ένας εισβολέας θα προτιμήσει την κατανομή πιθανότητας, η οποία ελαχιστοποιεί την μέση τιμή της πραγματικής κατανάλωσης. Ένα σοβαρό πρόβλημα με το μοντέλο ανίχνευσης ARMA-GLR είναι το γεγονός ότι αποδίδει, εάν τα πρότυπα επίθεσης δύνανται να μοντελοποιηθούν με ακριβή τρόπο από το μοντέλο ARMA[24].

Σε όλες τις παραπάνω τεχνικές υπάρχει πάντα το πρόβλημα της παραβίασης του ιδιωτικού απόρρητου στα προσωπικά δεδομένα, όπως τα χαρακτηριστικά φορτίου ή οι ενδείξεις του μετρητή σε ορισμένες χρονικές περιόδους. Γι αυτό προτείνονται τρεις αλγόριθμοι peer-to-peer (P2P)[9], οι οποίοι μπορούν να προσδιορίσουν τους πελάτες που έχουν διαπράξει απάτη, χωρίς να παραβιαστεί η ιδιωτική τους ζωή. Σε αυτή τη μέθοδο, ένας κεντρικός μετρητής τοποθετείται σε μια περιοχή για τη μέτρηση της συνολικής κατανάλωσης ηλεκτρικής ενέργειας κάθε χρονική στιγμή, η οποία θεωρείται ότι είναι ένας γραμμικός συνδυασμός της κατανάλωσης όλων των πελατών στην περιοχή. Παρ’ όλα αυτά, η μέθοδος αυτή είναι ευάλωτη σε ανακρίβειες κατά

την παρουσία «τεχνικών απωλειών» του δικτύου. Επιπλέον, είναι αποτελεσματική κυρίως όταν οι καταναλωτές διαπράττουν απάτη, μειώνοντας σταθερά τις μετρήσεις τους για πολλές διαδοχικές ημέρες, δηλαδή καταχρώνται ενέργεια με ένα σταθερό ποσοστό, το οποίο δεν αλλάζει ποτέ. Το ποσοστό αυτό ονομάζεται σταθερός συντελεστής ειλικρίνειας. Έτσι, η μέθοδος γίνεται ευάλωτη σε περιπτώσεις απάτης με τυχαίο τρόπο, δηλαδή επιλέγεται το ποσοστό κλοπής(συντελεστής ειλικρίνειας) να είναι πιο ομοιόμορφος και τυχαίος[24].

2.3 Τεχνική ανίχνευσης με βάση την εκτίμηση κατάστασης

Η ανάγκη για έλεγχο και ρύθμιση του συστήματος ηλεκτρικής ενέργειας και της βέλτιστης και οικονομικής λειτουργίας του, έχει οδηγήσει τις εταιρείες ηλεκτρισμού στην συγκέντρωση πληροφοριών σε πραγματικό χρόνο[55]. Η εκτίμηση κατάστασης είναι ένας αλγόριθμος επεξεργασίας πληροφοριών, που υπολογίζει την καλύτερη δυνατή εκτίμηση κατάστασης (μέτρα και γωνίες τάσεων των ζυγών) του συστήματος χρησιμοποιώντας:

- Μετρήσεις σε πραγματικό χρόνο
- Μαθηματικό μοντέλο του συστήματος
- Ψευδομετρήσεις

Προκειμένου να αναγνωρισθεί η τρέχουσα λειτουργική κατάσταση του συστήματος, οι εκτιμητές κατάστασης διευκολύνουν στην ακριβή και αποδοτική παρακολούθηση των λειτουργικών περιορισμών ορισμένων ποσοτήτων, όπως η φόρτιση των γραμμών μεταφοράς ή τα μέτρα τάσεων των ζυγών. Επίσης, παρέχουν μια βάση δεδομένων του συστήματος, πραγματικού χρόνου, περιλαμβανομένης της τρέχουσας κατάστασης, πάνω στην οποία μπορούν να εφαρμοστούν λειτουργίες ελέγχου της ασφάλειάς του. Η εκτίμηση κατάστασης, επομένως, χρησιμοποιεί ένα σύστημα παρακολούθησης το οποίο βοηθάει το ποσοστό ανίχνευσης. Η παρακολούθηση μπορεί να προέρχεται από ασύρματα δίκτυα αισθητήρων, ταυτοποίηση μέσω ραδιοσυχνοτήτων (Radio Frequency Identification, RFID), αμοιβαία επιθεώρηση, τεχνολογία AMI , κτλ.[4].

Τα ασύρματα δίκτυα αισθητήρων είναι φθηνά και εύκολα στην εφαρμογή, εισάγοντας μία νέα επιχειρηματική δραστηριότητα, στην οποία η πληροφορική και οι επικοινωνίες συνδέονται με τον κόσμο των ασύρματων αισθητήρων και τον διαδικτυακό προγραμματισμό. Το σύστημα ανίχνευσης εισβολέων (AMI Intrusion Detection System,AMIDS), για παράδειγμα, χρησιμοποιεί σύντηξη πληροφοριών(information fusion) για να συνδυάσει τους αισθητήρες και τα στοιχεία κατανάλωσης από έναν έξυπνο μετρητή με περισσότερη ακρίβεια στον εντοπισμό κλοπής. Το AMIDS συνδυάζει τα αρχεία καταγραφής ελέγχου φυσικών γεγονότων

και γεγονότων κυβερνοχώρου με δεδομένα κατανάλωσης σε ένα πιο ακριβές μοντέλο και εντοπίζει τις συμπεριφορές που σχετίζονται με απάτη[4].

Η τεχνολογία RFID βοηθάει την εταιρεία παροχής ηλεκτρισμού να χειριστεί την απογραφή του αμπερομέτρου της και την πρόληψη κλοπής ενέργειας [25]. Είναι η τεχνολογία εκείνη, η οποία έχει την δυνατότητα να επιτρέψει σε μηχανήματα να προσδιορίσουν αντικείμενα, να κατανοήσουν τις καταστάσεις τους, να επικοινωνήσουν και να δράσουν, εάν είναι απαραίτητο, ώστε να δημιουργηθεί μία «γνώση σε πραγματικό χρόνο». Όμως, για την εγκατάσταση του συστήματος γίνεται μία εκτίμηση του κόστους-οφέλους της εταιρείας μέσα από ένα δείκτη που καλείται Return on Investment (ROI). Ο δείκτης αυτός πρέπει να είναι μεγαλύτερος της μονάδας, ώστε να θεωρείται κερδοφόρο ένα εγχείρημα. Όταν είναι μεγαλύτερος της μονάδας σημαίνει ότι το κόστος είναι χαμηλότερο από το όφελος. Για να γίνει η εκτίμηση του δείκτη ROI, χρειάζεται μια ανάλυση των επιμέρους μερών του συστήματος RFID, τα οποία είναι: η διαχείριση της απογραφής του αμπερομέτρου και ο έλεγχος της επαλήθευσης του αμπερομέτρου[4].

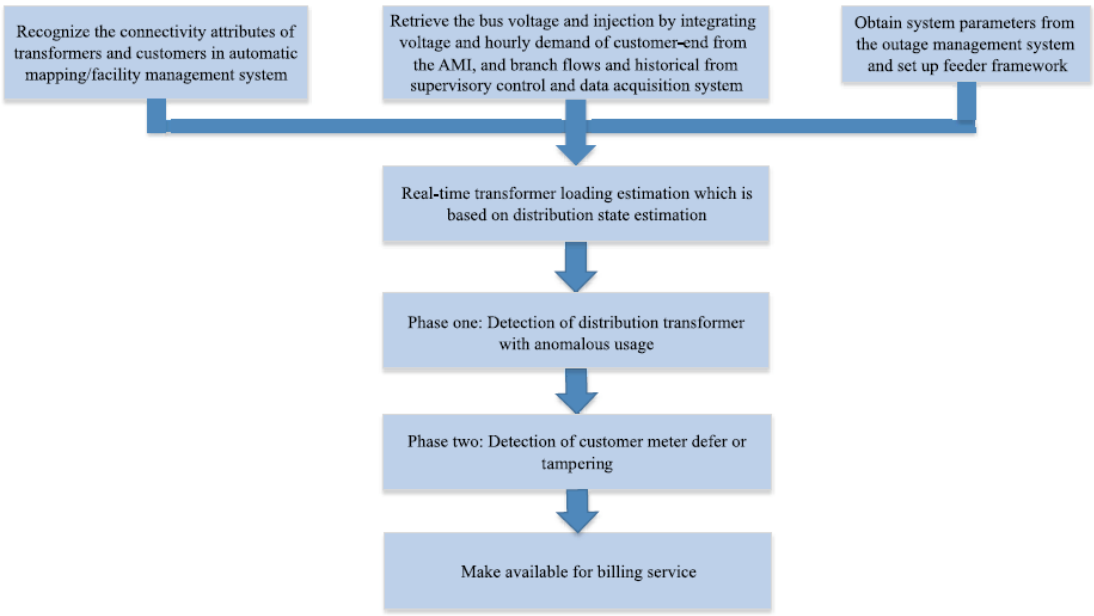
Η διαχείριση απογραφής του αμπερομέτρου αποτελείται από μια RFID ετικέτα, RFID συσκευές ανάγνωσης, το λογισμικό και το δίκτυο με το σύστημα προγραμματισμού των επιχειρησιακών πόρων (Enterprise Resource Planning-ERP) της εταιρείας ηλεκτρισμού. Οι εγκατεστημένες συσκευές ανάγνωσης μπορούν συλλάβουν την πληροφορία κάθε αμπερομέτρου στις ετικέτες RFID, και στην συνέχεια να την διαβιβάσουν στο λογισμικό. Ύστερα, από το λογισμικό μεταδίδονται τα δεδομένα στο σύστημα ERP της εταιρείας μέσω του δικτύου. Με τον τρόπο αυτό, η εταιρεία μπορεί να παρακολουθεί τα αμπερόμετρα και την διαχείρισή τους σε πραγματικό χρόνο. Όταν γίνεται η επιθεώρηση για κλοπή ενέργειας, το πρώτο που πρέπει να ελεγχθεί είναι εάν η ετικέτα του αμπερομέτρου είναι άθικτη. Η παραβίαση ή αφαίρεση της ετικέτας είναι δείγμα πιθανής κλοπής. Έτσι, η φορητή συσκευή ανάγνωσης RFID αποκτά την πληροφορία που μεταφέρεται από την ετικέτα και την στέλνει στο σύστημα ERP της εταιρείας μέσω του δικτύου, για να προσδιοριστεί εάν εγκρίνεται η ετικέτα, ή κάποια άλλη έχει τοποθετηθεί από πιθανούς εισβολείς. Στη συνέχεια, με την τεχνολογία ελέγχου επαλήθευσης του αμπερομέτρου, ελέγχεται εάν η πληροφορία που έχει μεταδοθεί από την ετικέτα επαληθεύεται με εκείνη του αμπερομέτρου, το οποίο σημαίνει ότι το αμπερόμετρο δεν έχει παραποιηθεί παράνομα [4].

Πολλές φορές, οι ενδείξεις του μετρητή μπορεί να μην είναι αξιόπιστες λόγω των κακόβουλων συμπεριφορών ή εξωτερικών επιθέσεων [26]. Αυτό αποτελεί ένα πρόβλημα για τους παρόχους ηλεκτρικής ενέργειας, οι οποίοι δεν έχουν τα μέσα για να αποκτήσουν τις μετρήσεις, πέρα από το να τις παραλάβουν απευθείας από τους καταναλωτές. Για να λυθεί αυτό το ζήτημα, παρουσιάστηκε μια αμοιβαία στρατηγική επιθεώρησης, η οποία επιτρέπει την αποδοχή των ενδείξεων του μετρητή από τον διαχειριστή του έξυπνου δικτύου. Ο στόχος του προτεινόμενου συστήματος είναι να ανακαλυφθούν προβληματικοί μετρητές που αναφέρουν εσφαλμένες τιμές μετρήσεων. Υπάρχουν μόνο δύο μέρη σε αυτό το σύστημα: ο έξυπνος μετρητής που

αντιπροσωπεύει την μέτρηση του προμηθευτή και ο έξυπνος μετρητής που αντιπροσωπεύει την μέτρηση του καταναλωτή. Ο προμηθευτής ενέργειας και ο καταναλωτής δεν εμπιστεύονται ο ένας τον άλλο επειδή οι έξυπνοι μετρητές μπορεί να τεθούν σε κίνδυνο ή να δεχθούν επίθεση. Σε αυτήν την περίπτωση σχεδιάστηκε ένα πρωτόκολλο για να βεβαιώσει ότι, εάν ο πραγματικός λογαριασμός διαφέρει μεταξύ των δύο έξυπνων μετρητών και υπερβαίνει το κατώτατο όριο, η σχέση εμπιστοσύνης θα διακοπεί, και η υπηρεσία θα τερματιστεί αμέσως[4].

Προκειμένου να εντοπιστεί η εισαγωγή περισσότερων κακών δεδομένων (bad data injection) και κακών στοιχείων σε μια μικρότερη περιοχή, προτείνεται μια Εκτίμηση Κατάστασης Προσαρμοστικής Στεγανοποίησης (Adaptive Partitioning State Estimation,APSE)[27]. Σε αυτή τη μέθοδο, το σύστημα ενέργειας μετατρέπεται σε ένα σταθμισμένο μη κατευθυνόμενο γράφημα και χωρίζεται σε διάφορους υπογράφους. Για παράδειγμα, η δοκιμή χ^2 χρησιμοποιείται στην ανίχνευση κακών δεδομένων σε κάθε υπογράφο. Από τη στιγμή που το όριο του υπογράφου αναμένεται να είναι χαμηλότερο από εκείνο του όλου συστήματος, είναι πιο ευαίσθητο για την ανίχνευση κακών δεδομένων. Η μέθοδος APSE βασίζεται στα σωστά στεγανοποιημένα γραφήματα και μπορεί να ανιχνεύσει μόνο τα κακά δεδομένα(παραποιημένα) στη γραμμή μεταφοράς[4].

Η εισαγωγή κακών δεδομένων (bad data injection) είναι από τις πιο επικίνδυνες επιθέσεις στο έξυπνο δίκτυο. Η προσέγγιση με βάση την εκτίμηση κατάστασης για την εκτίμηση φορτίου στο Μ/Σ διανομής αξιοποιείται για την ανίχνευση της δυσλειτουργίας/παραποίησης του μετρητή και παρέχει ποσοτικά στοιχεία των μη τεχνικών απωλειών. Το βασικό διάγραμμα ροής της προτεινόμενης μεθόδου φαίνεται στο παρακάτω σχήμα. Ακολουθώντας τα αποτελέσματα εκτίμησης της κατάστασης, αξιοποιείται μια ανάλυση της διακύμανσης, για να δημιουργήσει μια λίστα ύποπτων πελατών με προβληματικές μετρήσεις και να εκτιμηθεί η πραγματική χρησιμοποιούμενη ενέργεια [4].



Σχήμα 2.2 : Βασικό διάγραμμα ροής της μεθόδου ανίχνευσης μη τεχνικών απωλειών με βάση την εκτίμηση κατάστασης και την ανάλυση της διακύμανσης [27]

2.4 Τεχνική ανίχνευσης με βάση τη Θεωρία Παιγνίων

Τα συστήματα ανίχνευσης με βάση τη θεωρία παιγνίων προσφέρουν μια νέα προοπτική για την λύση του προβλήματος της κλοπής ενέργειας[4].

Διατυπώνεται το πρόβλημα της ανίχνευσης κλοπής ενέργειας ως ένα παιχνίδι μεταξύ του διανομέα ηλεκτρισμού και του καταναλωτή που διαπράττει απάτη, ο οποίος θέλει να ελαχιστοποιήσει την πιθανότητα εντοπισμού[29]. Συγκεκριμένα, μοντελοποιείται η απάτη ενέργειας και καταπολεμούνται οι απώλειες, σαν ένα παιχνίδι, στο οποίο ο διανομέας λειτουργεί σαν αρχηγός και οι καταναλωτές σαν ακόλουθοι (leader-follower). Η παρακολούθηση και η αποδοτικότητα της χρέωσης βελτιώνονται από τον διανομέα μειώνοντας την συνολική ποσότητα μη τεχνικών απωλειών λόγω κλοπής. Η αποδοτικότητα της ανίχνευσης αυξάνεται με επενδύσεις της τεχνολογίας AMI. Επιπλέον, ο ηλεκτρισμός προσφέρει ένα μη γραμμικό τιμολογιακό πρόγραμμα και επιλέγει ένα επίπεδο εξόδου. Οι πελάτες, δοθέντος μιας στρατηγικής του διανεμητή και του προγράμματος προστίμου για την ανίχνευση μη πληρωτέου ηλεκτρισμού, επιλέγουν τα επίπεδα κατανάλωσης των πληρωμένων και μη ποσοτήτων, ώστε να μεγιστοποιείται η ατομικής τους χρησιμότητα. Ο διανεμητής, ανάλογα με τη στρατηγική των πελατών, πρέπει να επιλέξει τις βέλτιστες ποσότητες των επενδύσεων, τιμολογιακού προγράμματος και επιπέδου εξόδου, ώστε να μεγιστοποιηθεί το κέρδος του. Με βάση αυτό, ορίζεται μια ρύθμιση ανώτατων τιμών με την οποία ο διανεμητής αντιμετωπίζει ένα μέσο περιορισμό εσόδων. Αυτός ο κανονισμός διεγείρει το συνολικό επίπεδο εξόδου και το επίπεδο επένδυσης της AMI, ενώ το οριακό δελτίο τιμών ανταποκρινόμενο στην βέλτιστη τιμολόγηση παραμένει ίδιο. Παρόλο που η βέλτιστη ποσότητα κλεμμένης ηλεκτρικής ενέργειας εκτιμάται

από τον διανεμητή, ορισμένοι έξυπνοι πελάτες είναι πιθανό να αποφύγουν την ανίχνευση, χρησιμοποιώντας πιο εξελιγμένες τεχνικές [4].

2.5 Σύγκριση των μεθόδων

Σε αυτήν την ενότητα, παρουσιάζεται μια σύγκριση των μεθόδων ανίχνευσης απάτης που αναφέρθηκαν παραπάνω. Κάθε τεχνική έχει τα δικά της χαρακτηριστικά, όπως φαίνεται παρακάτω[4]:

- Η τεχνική βάσει ταξινόμησης χρησιμοποιεί τις συλλεγόμενες καταναλώσεις από τους μετρητές. Η μηχανική μάθηση (machine learning) και οι τεχνολογίες εξόρυξης δεδομένων (data mining) χρησιμοποιούνται για τη σχεδίαση ενός καλού ταξινομητή, ο οποίος βασίζεται σε δείγματα δεδομένων. Εάν τα δείγματα δεδομένων συλλέγονται κατάλληλα, οι περισσότερες συμπεριφορές κλοπής ενέργειας ανιχνεύονται με ένα μέτριο κόστος από τον ταξινομητή. Ωστόσο, λόγω της παρουσίας ημερών χωρίς επίθεση υπάρχουν ορισμένα πρακτικά προβλήματα, από τα οποία δεν είναι εύκολο να αποκτηθεί καλή εικόνα της τάξης επίθεσης εκ των προτέρων. Επιπλέον, στα περισσότερα συστήματα υπάρχει η υπόθεση ότι, οι εισβολείς δεν είναι προσαρμοστικοί και δεν προσπαθούν να αποφύγουν τον μηχανισμό ανίχνευσης. Αυτό όταν συμβαίνει έχει ως αποτέλεσμα την δραματική μείωση του δείκτη ανίχνευσης. Για την αντιμετώπιση του ζητήματος αυτού, απαιτούνται αυτοματοποιημένες τεχνικές, με σκοπό να εξασφαλίσουν ότι τα γνωστά προφίλ αντανακλούν την πραγματικότητα με ακρίβεια.

- Με τη βοήθεια ειδικών συσκευών τα συστήματα ανίχνευσης που χρησιμοποιούν τεχνικές εκτίμησης κατάστασης μπορούν να βελτιώσουν το ποσοστό ανίχνευσης και να μειώσουν τον δείκτη λανθασμένης ανίχνευσης απάτης. Το τίμημα το οποίο αυτά τα συστήματα πληρώνουν, είναι ότι οι συσκευές παρακολούθησης χρειάζονται επιπλέον επενδύσεις από τις εταιρείες κοινής ωφέλειας. Το μεγαλύτερο κόστος της εφαρμογής των συσκευών παρακολούθησης περιλαμβάνει το κόστος της συσκευής, το κόστος του λογισμικού, το κόστος εγκατάστασης συστήματος και το αυξημένο κόστος λειτουργίας/κατάρτισης. Επιπλέον, η ακριβής ανίχνευση των προσπαθειών κλοπής ενέργειας απαιτεί ακριβή σχεδιασμό του συστήματος. Η επιλογή των παραμέτρων μπορεί να γίνει είτε από εμπειρογνώμονα ή αυτόματα από τις λύσεις της μηχανικής μάθησης.

- Τα συστήματα ανίχνευσης, που βασίζονται στη θεωρία παιγνίων, παρέχουν μια νέα προοπτική για την επίλυση της κλοπής ενέργειας. Το πρόβλημα της ανίχνευσης κλοπής ενέργειας διατυπώνεται σαν ένα παιχνίδι ανάμεσα στην εταιρεία ηλεκτρισμού και τον καταναλωτή της ηλεκτρικής ενέργειας. Στο

παιχνίδι, ο στόχος του καταναλωτή είναι η κλοπή ενός προκαθορισμένου ποσού ηλεκτρικής ενέργειας, ενώ ελαχιστοποιείται η πιθανότητα να εντοπιστεί. Από την άλλη πλευρά, οι εταιρείες θέλουν να μεγιστοποιήσουν την πιθανότητα ανίχνευσης και το βαθμό του λειτουργικού κόστους, το οποίο θα προκύψει από τη διαχείριση αυτού του μηχανισμού ανίχνευσης ανωμαλιών. Τα συστήματα ανίχνευσης, που βασίζονται στη θεωρία παιγνίων παρουσιάζουν μια σταθερή και λογική (αν και όχι βέλτιστη) λύση στη μείωση των απωλειών ηλεκτρικής ενέργειας, ως αποτέλεσμα της κλοπής ενέργειας. Ωστόσο, εξακολουθεί να είναι ένα δύσκολο έργο το πώς θα διαμορφωθούν η συνάρτηση χρησιμότητας όλων των παικτών (ρυθμιστής, διανομέας, και εισβολείς) και οι πιθανές στρατηγικές.

2.6 Τεχνική ανίχνευσης κλοπής με συνδυασμό SVM και δέντρων απόφασης

Οι μη τεχνικές απώλειες αποτελούν μια μεγάλη ανησυχία τελευταία για τις εταιρείες ενεργειακών συστημάτων και καθίσταται αναγκαίο να αναπτυχθεί ένα σύστημα, το οποίο θα ανιχνεύει με ακρίβεια τις κλοπές. Ακολουθεί μια περιγραφή ενός τέτοιου συστήματος, το οποίο βασίζεται στις μηχανές διανυσμάτων υποστήριξης και στα δέντρα απόφασης. Σε αντίθεση με άλλες μεθόδους, η συγκεκριμένη είναι αρκετά ικανή στην ανίχνευση απάτης σε κάθε επίπεδο της μεταφοράς και διανομής ηλεκτρικής ενέργειας. Με λίγα λόγια, το προτεινόμενο σύστημα μπορεί να θεωρηθεί ως δύο επιπέδων ανάλυση δεδομένων. Τα δεδομένα τροφοδοτούνται από δέντρα απόφασης σαν είσοδο στον ταξινομητή SVM. Τα αποτελέσματα εφαρμογής της μεθόδου δείχνουν μειωμένο δείκτη λανθασμένων ταξινομήσεων σε μεγάλη έκταση [30].

Αρχικά, τα δέντρα απόφασης χρησιμοποιούνται, για να ταξινομήσουν τα πρότυπα σε διάφορες ομάδες, με βάση τις αντίστοιχες ιδιότητές τους. Παρ' όλα αυτά, μέχρι τώρα, με αυτό τον τρόπο δεν μπορεί να γίνει ανίχνευση κλοπής, γι' αυτό έχει επιλεχθεί το SVM σαν ένας των ταξινομητών στο προτεινόμενο σύστημα, λόγω των πλεονεκτημάτων του σε σχέση με άλλους ταξινομητές. Επίσης, το SVM έχει εκτενώς χρησιμοποιηθεί σε εφαρμογές ανάλυσης δεδομένων. Πρώτον, το SVM έχει δοκιμαστεί στο παρελθόν παρέχοντας μεγάλη ακρίβεια. Δεύτερον, είναι ικανό στο χειρισμό του προβλήματος της υπερεκπαίδευσης (over-fitting), το οποίο σχετίζεται με κατάλληλο χειρισμό άγνωστων δεδομένων για την παραγωγή των σχετικών εξόδων/αποτελεσμάτων. Έτσι, με το SVM γίνεται καλή ταξινόμηση των πελατών ως κακόβουλων ή γνήσιων, ανάλογα με την κατανάλωσή τους. Επίσης, το SVM βοηθάει στον διαχωρισμό δεδομένων, τα οποία δεν είναι γραμμικώς διαχωρίσιμα [30].

Ένα έξυπνο δίκτυο αποτελείται από πολυάριθμα διασυνδεδεμένα μέρη. Τέτοια είναι η παραγωγή της ενέργειας, οι γραμμές μεταφοράς, οι σταθμοί διανομής και οι τελικοί χρήστες/καταναλωτές. Αρχικά, η ενέργεια παράγεται στη μονάδα παραγωγής ηλεκτρικής ενέργειας και μεταφέρεται στους διάφορους σταθμούς διανομής μέσω των γραμμών μεταφοράς υψηλής τάσης. Ύστερα, αναδιανέμεται σε διάφορους κλάδους και τομείς. Συνήθως, αυτός που διαπράττει κλοπή ενέργειας μπορεί να εμφανιστεί σε κάθε επίπεδο της μεταφοράς ενέργειας, όπως προαναφέρθηκε. Για τον εντοπισμό των εισβολέων, το προτεινόμενο σύστημα χρησιμοποιεί αναλυτές δεδομένων πάνω σε δεδομένα, τα οποία συγκεντρώνονται σε διάφορα μέρη. Έξυπνοι μετρητές και αισθητήρες εγκαθίστανται σε όλα τα επίπεδα για την συλλογή των σχετικών δεδομένων κατανάλωσης ηλεκτρικής ενέργειας σε πραγματικό χρόνο. Οι έξυπνοι μετρητές χρησιμοποιούν ασύρματο μέσον για να στείλουν τις μετρήσεις τους στην εταιρεία. Από τη στιγμή που συλλεχθούν τα δεδομένα, αναμεταδίδονται σε έναν κεντρικό διακομιστή της εταιρείας για περαιτέρω επεξεργασία[30].

Αρχικά η συνολική ενέργεια, που μεταφέρεται, και η συνολική ενέργεια που λαμβάνεται στα διάφορα επίπεδα μεταφοράς και διανομής, συγκρίνεται από την εταιρεία. Οι υπολογισμοί γίνονται σε πραγματικό χρόνο και με ομοιογενή τρόπο από τον διακομιστή/εξυπηρετητή (sever), ο οποίος αποφασίζει, εάν έχει γίνει απάτη σε ένα συγκεκριμένο επίπεδο ή όχι. Εάν η συνολική μεταφερόμενη ενέργεια υπερβαίνει την ενέργεια που λαμβάνεται (συμπεριλαμβανομένων των απωλειών, στο στάδιο μεταφοράς και διανομής), τότε ο διακομιστής της εταιρείας το εκλαμβάνει ως κλοπή στο αντίστοιχο επίπεδο, το οποίο έχει ως επακόλουθο την επιθεώρηση. Διαφορετικά, δεν θεωρείται κλοπή στο αντίστοιχο επίπεδο και η ίδια διαδικασία συνεχίζει στο επόμενο επίπεδο. Οι απώλειες μεταφοράς και διανομής υπολογίζονται ως εξής:

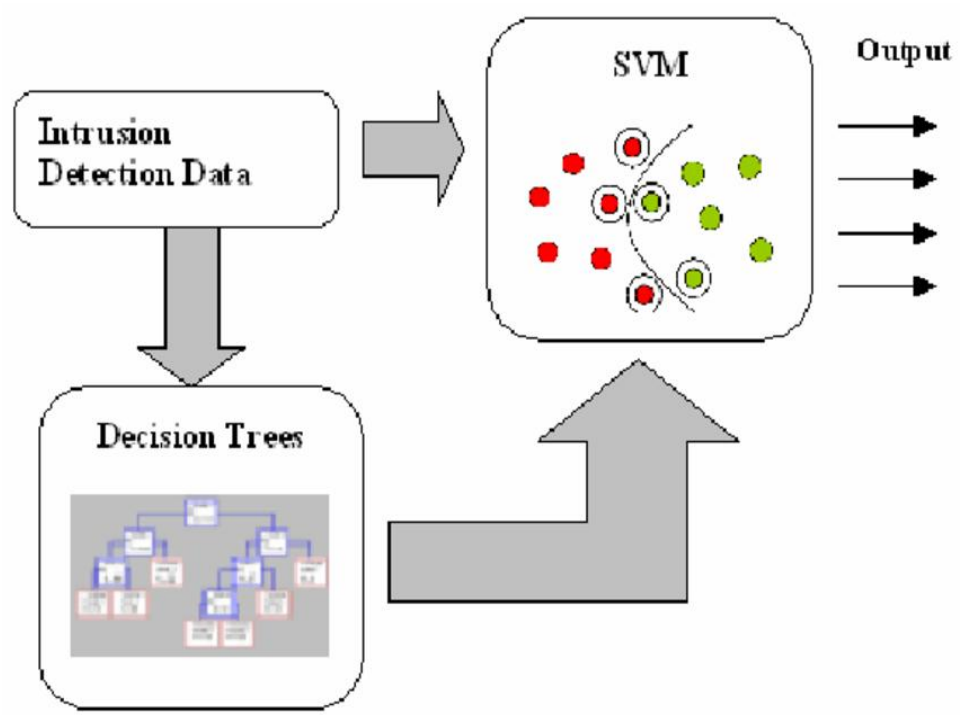
$$L_2=(1-\alpha)L_1,$$

όπου L_1, είναι το επίπεδο από το οποίο μεταφέρεται η ενέργεια, L_2 είναι το επίπεδο, στο οποίο φτάνει ενέργεια, και α είναι ο παράγοντας απώλειας, ο οποίος εξαρτάται από το φορτίο[30].

Εκτός από τον εντοπισμό κλοπής στα επίπεδα, είναι σημαντικός ο προσδιορισμός των εισβολέων στο επίπεδο των τελικών καταναλωτών. Η κλοπή σε αυτό το επίπεδο μπορεί να γίνει με δύο τρόπους· με φυσική αλλοίωση, όπου ο καταναλωτής κάνει μια μη εξουσιοδοτημένη σύνδεση στο δίκτυο για να κλέψει ενέργεια και με ηλεκτρονική αλλοίωση των μετρούμενων δεδομένων με σκοπό τη μείωση της τιμής της κατανάλωσης της ενέργειας. Οι δύο αυτοί, τύποι κλοπής, μειώνουν το προφίλ κατανάλωσης των τελικών χρηστών και οι χρήστες, που συμμετέχουν σε οποιοδήποτε από αυτά, θεωρούνται ύποπτοι. Για την αντιμετώπιση αυτών των προβλημάτων, προτείνεται η μέθοδος του συνδυασμού δέντρων απόφασης και SVM. Οι είσοδοι στο δέντρο απόφασης είναι χαρακτηριστικά όπως οι συσκευές, τα άτομα, η θερμοκρασία, η εποχή, ο χρόνος, τα οποία είναι είσοδοι και στο SVM. Επιπλέον, στο SVM είναι είσοδος η πραγματική κατανάλωση ενέργειας και η έξοδος

του δέντρου απόφασης, η οποία είναι η αναμενόμενη κατανάλωση ενέργειας. Τέλος, η έξοδος του SVM είναι η ταξινόμηση των καταναλωτών σε καλούς και κακόβουλους. Όλα αυτά τα χαρακτηριστικά, που δίνονται ως είσοδοι στο δέντρο απόφασης και στο SVM, ταξινομούνται ένα προς ένα. Η όλη διαδικασία αυτού του συστήματος ταξινόμησης ερμηνεύεται με δύο βήματα. Στο πρώτο βήμα, ο ταξινομητής του δέντρου απόφασης λειτουργεί επί των εν λόγω παραμέτρων και υπολογίζει την αναμενόμενη κατανάλωση ενέργειας των πελατών. Στη συνέχεια, λειτουργεί ο ταξινομητής SVM με βάση προηγούμενων καθορισμένων παραμέτρων κατά μήκος των πρόσφατων υπολογισμένων παραμέτρων. Ως αποτέλεσμα αυτών των υπολογισμών είναι ότι, το SVM τελικά ανιχνεύει τους κακόβουλους καταναλωτές, που εμπλέκονται σε κλοπή ενέργειας. Έτσι, το σύστημα αυτό επιτυγχάνει καλύτερη απόδοση, λόγω του συνδυασμού των δύο ταξινομητών [30].

Μια σχηματική αναπαράσταση του συνδυασμού δέντρων απόφασης και SVM παρατίθεται στο Σχήμα 2.3.



Σχήμα 2.3 : Ο συνδυασμός δέντρου απόφασης και SVM [31]

- **<u>Προτεινόμενη μέθοδος</u>**

Στην παρούσα διπλωματική εργασία χρησιμοποιείται η τεχνική ταξινόμησης και συγκεκριμένα αυτή των μηχανών διανυσμάτων υποστήριξης (SVM). Η επιλογή αυτή έγινε λόγω των ανώτερων επιδόσεων των SVM σε πολλές εφαρμογές σε σύγκριση με τις παραδοσιακές μεθόδους, όπως ο έλεγχος λόγου πιθανοφάνειας και τα νευρωνικά δίκτυα. Στην επόμενη ενότητα αναλύεται το μαθηματικό μοντέλο των μηχανών διανυσμάτων υποστήριξη.

2.7 *Οι αλγόριθμοι ταξινόμησης με Μηχανές Διανυσμάτων Υποστήριξης*

2.7.1 Εισαγωγή-Ιστορική Ανασκόπηση

Πρωτοπόρος στον τομέα των μηχανών διανυσμάτων υποστήριξης υπήρξε ο Vapnik. Η πρώτη περιγραφή μιας μηχανής διανυσμάτων υποστήριξης παρουσιάστηκε από τους Boser, Guyon και Vapnik το 1992, αν και η εισαγωγή τους έγινε από τον Vapnik στα τέλη της δεκαετίας του 1960. Η πιο περιεκτική και λεπτομερής περιγραφή αυτής της νέας κατηγορίας μηχανών μάθησης περιλαμβάνεται στο βιβλίο του Vapnik με τίτλο «Statistical Learning Theory»[19], το οποίο είναι ήδη «κλασικό» στον τομέα του. Ο αλγόριθμος ταξινόμησης με μηχανές διανυσμάτων υποστήριξης, που βασίζεται στα θεμέλια της θεωρίας της στατιστικής ανάλυσης, είναι μια γενική μέθοδος κατηγοριοποίησης. Έχουν πρόσφατα εφαρμοσθεί σε διάφορες εφαρμογές που κυμαίνονται από την αναγνώριση προσώπου και κατηγοριοποίηση κειμένου στην βιοπληροφορική και την εξόρυξη δεδομένων[32].

Οι μηχανές διανυσμάτων υποστήριξης (Support Vector Machines, SVM) είναι ένας είδος αλγορίθμων μηχανικής μάθησης, οι οποίοι θα μπορούσαν να χαρακτηριστούν ως η πιο κομψή απ' όλες τις μεθόδους μάθησης. Είναι ευκολότερο να γίνει κατανοητό το πώς δουλεύει μια τέτοια μηχανή μέσα από την περίπτωση των διαχωρίσιμων προτύπων, στο πλαίσιο ταξινόμησης προτύπων. Η κεντρική ιδέα πίσω από τη μηχανή μπορεί να συνοψιστεί ως εξής:

«Δοθέντος ενός δείγματος εκπαίδευσης, η μηχανή διανυσμάτων υποστήριξης κατασκευάζει ένα υπερεπίπεδο ως επιφάνεια απόφασης με τέτοιο τρόπο ώστε το περιθώριο διαχωρισμού μεταξύ θετικών και αρνητικών παραδειγμάτων να μεγιστοποιείται.»[32].

Αυτή η βασική ιδέα επεκτείνεται θεωρητικά, ώστε να καλύπτει και την πιο δύσκολη περίπτωση των μη γραμμικά διαχωρίσιμων προτύπων[32].

Μια ιδέα η οποία είναι θεμελιακή για την ανάπτυξη του αλγόριθμου μάθησης της μηχανής διανυσμάτων υποστήριξης είναι ο πυρήνας εσωτερικού γινομένου (inner product kernel) μεταξύ του «διανύσματος υποστήριξης» x_i, και ενός διανύσματος x, το οποίο αντλείται από το χώρο δεδομένων εισόδου. Το σημαντικότερο όλων είναι ότι τα διανύσματα υποστήριξης αποτελούνται από ένα μικρό υποσύνολο σημείων δεδομένων, τα οποία εξάγει ένας αλγόριθμος μάθησης από το ίδιο δείγμα εκπαίδευσης. Στην πραγματικότητα, λόγω αυτής της σημαντικής ιδιότητας, ο αλγόριθμος μάθησης που εμπλέκεται στην κατασκευή μηχανής διανυσμάτων υποστήριξης αναφέρεται επίσης ως μέθοδος πυρήνα (kernel method). Η μέθοδος πυρήνα βελτιστοποιεί την σχεδίαση της μηχανής διανυσμάτων υποστήριξης. Ωστόσο, αυτό το εξαιρετικά επιθυμητό χαρακτηριστικό της μηχανής επιτυγχάνεται με αντίτιμο

την αυξημένη υπολογιστική πολυπλοκότητα. Καταλήγοντας, η μηχανή διανυσμάτων υποστήριξης μπορεί να χρησιμοποιηθεί για την επίλυση δύο τύπων προβλημάτων: της ταξινόμησης μοτίβων και της μη γραμμικής παλινδρόμησης[32].

2.7.2 Μαθηματικό μοντέλο

Ο κύριος σκοπός του (δυαδικού) SVM, το οποίο χρησιμοποιείται για ταξινόμηση, είναι να κατασκευάσει μία βέλτιστη συνάρτηση απόφασης f(x)[33]. Η συνάρτηση f(x) διαχωρίζει με ακρίβεια δεδομένα σε δύο ομάδες και ελαχιστοποιεί το σφάλμα ταξινόμησης:

$$\boldsymbol{f(x)} = \mathbf{sgn(g(x))} \tag{1}$$

όπου η g(x) είναι το όριο απόφασης μεταξύ των δύο κατηγοριών. Αυτό επιτυγχάνεται με την ακόλουθη μέθοδο της αρχής ελαχιστοποίησης, η οποία δίδεται μέσα από τον τύπο:

$$\boldsymbol{R} < \frac{\boldsymbol{t}}{\boldsymbol{n}} + \sqrt{\frac{\boldsymbol{h}\left(\ln\left(\frac{2N}{h}\right)+1\right)-\ln\left(\frac{n}{4}\right)}{\boldsymbol{n}}} \tag{2}$$

όπου R: το προσδοκώμενο σφάλμα ταξινόμησης,

t : ο αριθμός των σφαλμάτων εκπαίδευσης,

n: ο αριθμός των δειγμάτων εκπαίδευσης, και

h: το μέτρο εμπιστοσύνης.

Στην περίπτωση διαχωρίσιμων δεδομένων, ο πρώτος όρος της παραπάνω εξίσωσης είναι μηδέν και ο δεύτερος όρος ελαχιστοποιείται, με αποτέλεσμα μια καλή γενική απόδοση του SVM. Η συνάρτηση g(x) είναι το όριο απόφασης, το οποίο προέρχεται από ένα σύνολο δειγμάτων εκπαίδευσης:

$$\mathbf{X}=\{\boldsymbol{x_1}, \boldsymbol{x_2}, \dots, \boldsymbol{x_n}\},\ \boldsymbol{x_i} \in \boldsymbol{R^M},\ \mathbf{i=1,2,..,\ n} \tag{3}$$

όπου το κάθε δείγμα εκπαίδευσης x_i έχει M χαρακτηριστικά, τα οποία περιγράφουν μια συγκεκριμένη ιδιότητα και ανήκει σε μια από τις δύο κατηγορίες:

$$\mathbf{Y}=\{\boldsymbol{y_1}, \boldsymbol{y}, \dots, \boldsymbol{y_n}\},\ \boldsymbol{y_i} \in \{-\mathbf{1}, +\mathbf{1}\},\ \mathbf{i=1,2,..,\ n} \tag{4}$$

Το όριο απόφασης μεταξύ των δύο κατηγοριών είναι ένα υπέρ επίπεδο, που περιγράφεται από την εξίσωση:

$$\mathbf{g(x)=\langle \boldsymbol{w}, \boldsymbol{x}\rangle+b} \tag{5}$$

όπου το w και b προέρχονται από τέτοιο τρόπο, ώστε τα δεδομένα να ταξινομούνται σωστά. Αυτό επιτυγχάνεται μεγιστοποιώντας το περιθώριο διαχωρισμού μεταξύ των δύο κατηγοριών. Μπορεί να εφαρμοστεί σαν έναν τετραγωνικού προγραμματισμού (Quadratic Programming,QP) πρόβλημα βελτιστοποίησης[34].

$$\mathbf{\Phi(w,\zeta_i)= min}\left\{\frac{1}{2}\|\boldsymbol{w}\|^2+\mathbf{C}\sum_{i=1}^{n}\boldsymbol{\zeta_i}\right\} \tag{6}$$

υπό τον περιορισμό, ότι όλα τα δείγματα εκπαίδευσης είναι σωστά ταξινομημένα πχ. όλα τα δείγματα εκπαίδευσης είναι τοποθετημένα στο περιθώριο ή έξω από το περιθώριο, το οποίο είναι :

$$\boldsymbol{y_i}(\langle \boldsymbol{w}, \boldsymbol{x}\rangle+\mathbf{b}) \geq \mathbf{1-}\ \boldsymbol{\zeta_i},\ \mathbf{i=1,2\ldots,n} \tag{7}$$

όπου τα ζ_i για i=1,2..,n είναι μη αρνητικές μεταβλητές χαλαρότητας.

Με την ελαχιστοποίηση του πρώτου όρου της εξίσωσης Φ, η περιπλοκότητα του SVM μειώνεται, και ελαχιστοποιώντας τον δεύτερο όρο της Φ, ο αριθμός των σφαλμάτων εκπαίδευσης μειώνεται. Η παράμετρος C είναι μια παράμετρος νομιμοποίησης και έχει προεπιλεγεί ως η ανταλλαγή μεταξύ των δύο όρων. Το σταθερό πρόβλημα QP, το οποίο ορίζεται παραπάνω, λύνεται με την εισαγωγή των συντελεστών Lagrange, $\alpha_i \geq 0$ *και* $\beta_i \geq 0$, η οποία συνάρτηση Lagrange είναι[33]:

$$\begin{aligned}\mathbf{L(w,b,\zeta,\alpha,\beta)=}\ & \frac{1}{2}\|\boldsymbol{w}\|^2+\ \mathbf{C}\sum_{i=1}^{n}\boldsymbol{\zeta_i}\\ & -\ \sum_{i=1}^{n}\boldsymbol{a_\iota}\{\boldsymbol{y_i}[\langle \boldsymbol{w}, \boldsymbol{x_i}\rangle+\boldsymbol{b}]-\mathbf{1}+\boldsymbol{\zeta_i}\}\\ & -\ \sum_{i=1}^{n}\boldsymbol{\beta_\iota}\,\boldsymbol{\zeta_i}\end{aligned} \tag{8}$$

Σύμφωνα με την θεωρία της βελτιστοποίησης QP, είναι καλύτερα να λυθεί η εξίσωση (8) με την εισαγωγή της δυαδικής διατύπωσης του προβλήματος:

$$\max_{\boldsymbol{\alpha},\boldsymbol{\beta}} \boldsymbol{W}(\boldsymbol{\alpha},\boldsymbol{\beta}) = \max_{\boldsymbol{\alpha},\boldsymbol{\beta}}\{\min_{\boldsymbol{w},\boldsymbol{\beta},\boldsymbol{\zeta}}(\boldsymbol{w},\boldsymbol{b},\boldsymbol{\zeta},\boldsymbol{\alpha},\boldsymbol{\beta})\} \tag{9}$$

όπου τα a_ι και β_ι είναι οι συντελεστές Lagrange.
Έτσι, η βέλτιστη λύση δίνεται, πρωτίστως ελαχιστοποιώντας τα w,b και ζ και δευτερευόντως μεγιστοποιώντας τα, υπό την προϋπόθεση ότι $a_\iota \geq 0$ και $\beta_\iota \geq 0$.
Υπό τον περιορισμό της (8) στην (9) το πρόβλημα μετατρέπεται στην δυαδική του μορφή, που δίνεται από:

$$\max_{\alpha}\{\sum_{i=1}^{n} a_\iota - \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} a_\iota \alpha_j y_i y_j \langle x_i, x_j\rangle\} \tag{10}$$

και μεγιστοποιείται υπό των περιορισμών

$$\sum_{i=1}^{n} a_i y_i = 0 \text{ και } 0 \leq a_\iota \leq C \text{ για i=1,2,…,n} \tag{11}$$

Επιπλέον, το διάνυσμα w έχει μια επέκταση στους όρους ενός υποσυνόλου δειγμάτων εκπαίδευσης, όπου οι συντελεστές Lagrange a_ι είναι μη μηδενικοί. Αυτά τα δείγματα εκπαίδευσης συναντούν την κατάσταση Karush-Kuhn-Tucker (KKT) :

$$a_i\{y_i[\langle w, x_i\rangle + b] - 1 + \zeta_i\} = 0_i, \text{ i=1,2,…,n} \tag{12}$$

Η εξίσωση (12) αναφέρει ότι, μόνο οι φορείς κατάρτισης, δηλαδή τα διανύσματα υποστήριξης (SVs), τα οποία αντιστοιχούν σε μη μηδενικούς συντελεστές Lagrange, χρειάζονται για να περιγράψουν το υπερ-επίπεδο. Σε αυτή την περίπτωση, των γραμμικά διαχωριζόμενων δεδομένων, όλα τα διανύσματα υποστήριξης κείτονται στο περιθώριο και ως εκ τούτου ο αριθμός τους είναι λιγότερος. Ακολούθως, το όριο απόφασης g(x) προσδιορίζεται, χρησιμοποιώντας μόνο ένα υποσύνολο των δειγμάτων εκπαίδευσης :

$$g(x)=\sum_{i=1}^{N_s} a_i y_i \langle x, x_i\rangle + b \tag{13}$$

όπου x : το διάνυσμα εισόδου δοκιμής,
$\langle x, x_i\rangle$: το εσωτερικό γινόμενο,
N_s : ο αριθμός των διανυσμάτων υποστήριξης, και
b: ο όρος προκατάληψης.

Σε περιπτώσεις όπου το γραμμικό όριο απόφασης δεν είναι σωστό, το SVM αντιστοιχεί το διάνυσμα εισόδου x σε ένα υψηλότερων διαστάσεων χώρο χαρακτηριστικών. Αυτό επιτυγχάνεται με την εισαγωγή της συνάρτησης πυρήνα (kernel) K(·,·) [19][34] για να ληφθεί η παρακάτω κατάσταση στην (10).

$$\langle x_i, x_j\rangle \rightarrow K(x_i, x_j) \tag{14}$$

Αυτό αποδίδεται ως :

$$\max_{\alpha}\{\sum_{i=1}^{n} a_\iota - \frac{1}{2}\sum_{i=1}^{n}\sum_{j=1}^{n} a_\iota \alpha_j y_i y_j K(x_i, x_j)\} \tag{15}$$

και η (15) μεγιστοποιείται υπό τους περιορισμούς (7), όπου η λύση παρέχεται χρησιμοποιώντας ένα πακέτο λογισμικού για την επίλυση προβλημάτων

βελτιστοποίησης. Το όριο απόφασης g(x) στη (13) τροποποιείται με την αλλαγή του $\langle x_i, x_j \rangle$ με $K(x_i, x_j)$

$$\mathbf{g(x)}=\sum_{i=1}^{N_s} \boldsymbol{a_i y_i K(x_i, x_j) + b} \tag{16}$$

Γενικά, είναι δύσκολο να οριστεί το είδος του λειτουργικού πυρήνα (ο τύπος της συνάρτησης kernel), για να χρησιμοποιηθεί σε συγκεκριμένα πρότυπα δεδομένων. Παρ' όλα αυτά, οποιαδήποτε συνάρτηση, που ικανοποιεί την συνθήκη του Mercer από τον Vapnik, μπορεί να χρησιμοποιηθεί σαν συνάρτηση kernel [35]. Η συμβατικά χρησιμοποιούμενη συνάρτηση kernel στα SVM χωρίζεται σε δύο κατηγορίες: οι kernel που βασίζονται στην Ευκλείδεια απόσταση και οι kernels που βασίζονται στα Ευκλείδεια εσωτερικά γινόμενα. Οι συναρτήσεις kernel συλλέγονται με βάση την δομή δεδομένων και τον τύπο των ορίων μεταξύ των δύο κατηγοριών. Σε αυτή την εργασία, η συνάρτηση kernel βασίζεται στην Ευκλείδεια απόσταση, η συνάρτηση ακτινικής βάσης (Radial Basis Function,RBF) kernel δίδεται[33]:

$$\boldsymbol{K(x_i, x_j) = \exp\left(-\gamma \|x_i - x_j\|^2\right)} \tag{17}$$

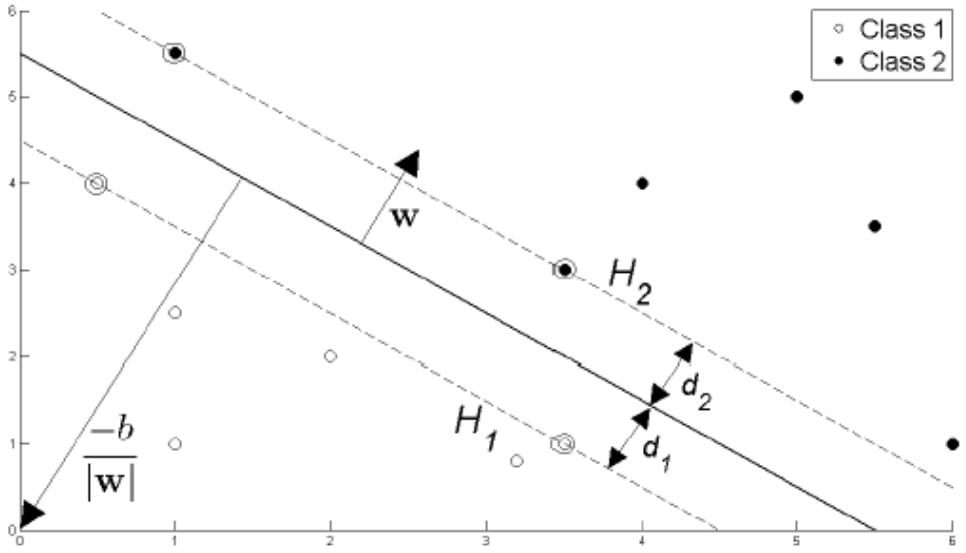
όπου η παράμετρος γ ελέγχει το πλάτος της συνάρτησης RBF Kernel.
Η RBF kernel προκαλεί έναν άπειρων διαστάσεων χώρο kernel, στο οποίο όλα τα εικονικά διανύσματα έχουν την ίδια μορφή-νόρμα. Γενικότερα, η RBF kernel προτείνεται για άγνωστες εφαρμογές.

Η επιλογή των δύο παραμέτρων του μοντέλου SVM (C,γ) είναι σημαντική για την ακρίβεια της ταξινόμησης. Για παράδειγμα, εάν το C είναι πολύ μεγάλο (περίπου στο άπειρο), τότε ο στόχος είναι η ελαχιστοποίηση του εμπειρικού κινδύνου, χωρίς την ομαλότητα του μοντέλου στην εφαρμογή βελτιστοποίησης. Η παράμετρος γ ελέγχει το πλάτος της Γκαουσιανής συνάρτησης (RBF kernel), το οποίο αντικατοπτρίζει το εύρος κατανομής των τιμών x των δεδομένων εκπαίδευσης. Έτσι, οι δύο παράμετροι επηρεάζουν την κατασκευή του μοντέλου με διαφορετικούς τρόπους. Υπάρχουν πολλές υπάρχουσες πρακτικές προσέγγισης για την επιλογή των παραμέτρων (C,γ) όπως: να οριστεί από τον χρήστη με βάση προηγούμενη γνώση και εμπειρία, η ασυμπτωτική βελτιστοποίηση, η τεχνική με cross-validation (CV) , και grid search[33].Οι τεχνικές grid search και cross validation χρησιμοποιούνται και αναλύονται στο επόμενο κεφάλαιο.

Εκτός από την διενέργεια ταξινομήσεων, τα SVMs επίσης υπολογίζουν τις πιθανότητες για κάθε ομάδα[33]. Αυτό υποστηρίζει την αναλυτική έννοια της γενίκευσης και της βεβαιότητας. Δίνεται ότι το r_{ij} είναι μια εκτίμηση για την πιθανότητα της εξόδου ενός ζεύγους ταξινομητών μεταξύ της ομάδας i και της ομάδας j (π.χ. $r_{ij} \approx P(y = \{i, j\}, x)$, $r_{ij}+r_{ji}=1$), και το p_i είναι η πιθανότητα της i-οστής ομάδας, η πιθανότητα p= $(p_1, \dots, p_k)$ μιας ομάδας μπορεί να χωριστεί μέσω του QP προβλήματος [33][36]

$$\min_{\boldsymbol{p}} \frac{1}{2}\sum_{i=1}^{k}\sum_{j:j\neq 1}(r_{ij}p_j - r_{ji}p_i)^2 \text{ , } \sum_{i=1}^{k} p_i = 1, \quad p_i \geq 0, \text{ για κάθε i} \tag{18}$$

Η γεωμετρική κατασκευή ενός βέλτιστου υπερεπιπέδου για ένα δισδιάστατο χώρο εισόδου απεικονίζεται στο Σχήμα 2.4.



Σχήμα 2.4: Σχηματική αναπαράσταση ενός βέλτιστου υπερεπιπέδου δύο γραμμικών διαχωρίσιμων τάξεων [37]

Μέχρι τώρα, έγινε μια αναφορά στο μαθηματικό μοντέλο της εφαρμογής των μηχανών διανυσμάτων υποστήριξης. Ωστόσο, στην παρούσα διπλωματική και κατά την πειραματική διαδικασία και υλοποίηση του κώδικα, που χρησιμοποιήθηκε, έγινε χρήση της βιβλιοθήκης LIBSVM του Matlab. Στην βιβλιοθήκη LIBSVM[38] υπάρχουν έτοιμες συναρτήσεις και εντολές για την εκπαίδευση και δοκιμή του αλγόριθμου SVM. Έτσι, η είσοδος ήταν τα διαθέσιμα ιστορικά δεδομένα και έξοδος ήταν τα αποτελέσματα της ταξινόμησης, σε απάτες και μη. Επομένως, αυτό που εξετάζεται και αναλύεται είναι οι μετρήσεις από τον πίνακα σύγχυσης(confusion matrix) και τις καμπύλες ROC, τα οποία αναλύονται παρακάτω.

2.8 *Μεγέθη αξιολόγησης*

Κατά την διαδικασία οικοδόμησης του μοντέλου ταξινόμησης χρειάζονται κάποιοι τρόποι, για την μέτρηση της αποτελεσματικότητας του κάθε μοντέλου, που χτίζεται. Αυτή η αξιολόγηση γίνεται κατά την διάρκεια της διαδικασίας, που κατασκευάζεται το μοντέλο. Συνήθως, η διαδικασία αυτή αποτελείται από δύο μέρη:

- Την κατασκευή του μοντέλου: Σε αυτό το βήμα χρειάζεται η τροφοδότηση των δεδομένων από τον αλγόριθμο εξόρυξης δεδομένων. Τυπικά, αυτά τα δεδομένα είναι ένα υποσύνολο των συνολικών και περιέχουν το 60% με 70 % των αρχικών δεδομένων.

- Δοκιμή του μοντέλου: Αφού εκπαιδευτεί το μοντέλο, χρειάζεται μια δοκιμή, για να φανεί πόσο αποτελεσματικά έγιναν οι προβλέψεις του. Γι' αυτό το λόγο, χρησιμοποιούνται τα δεδομένα που αφαιρέθηκαν κατά την εκπαίδευση του, δηλαδή το 40% με 30% του συνολικού. Για αυτά τα δεδομένα, υπάρχει γνώση του αποτελέσματος. Έτσι, αφού γίνει δοκιμή του μοντέλου με το υποσύνολο των δεδομένων, είναι δυνατό να μετρηθούν οι προβλεπόμενες τιμές έναντι των αληθινών τιμών

Ο πιο κοινός τρόπος για την εξαγωγή των αποτελεσμάτων είναι ο πίνακας σύγχυσης (confusion matrix). Ο πίνακας αυτός εμφανίζει τις σωστές προβλέψεις, τις λανθασμένες προβλέψεις και την εκτέλεση ενός αριθμού στατιστικών μετρήσεων.

2.8.1 Confusion Matrix

Στον τομέα της μηχανικής μάθησης και συγκεκριμένα της στατιστικής ταξινόμησης, ένας πίνακας σύγχυσης (confusion matrix), επίσης γνωστός ως πίνακας σφάλματος, επιτρέπει την απεικόνιση της απόδοσης ενός αλγορίθμου, συνήθως μιας επιβλεπόμενης εκμάθησης (supervised learning). Κάθε στήλη του πίνακα αντιπροσωπεύει τις περιπτώσεις των προβλεπόμενων τάξεων και κάθε σειρά αντιπροσωπεύει τις περιπτώσεις πραγματικών τάξεων (ή το αντίστροφο). Το όνομα προέρχεται από το γεγονός ότι υποδεικνύει, αν το σύστημα είναι συγκεχυμένο σε δύο κατηγορίες[39][43].

Ο πίνακας σύγχυσης είναι ένας πίνακας με δύο σειρές και δύο στήλες. Αναφέρει τον αριθμό των ψευδώς θετικών, ψευδώς αρνητικών, αληθώς θετικών και αληθώς αρνητικών προβλέψεων. Αυτό επιτρέπει πιο λεπτομερή ανάλυση, σε σχέση με την απλή αναλογία των σωστών προβλέψεων (ακρίβεια). Επομένως, ο πίνακας σύγχυσης περιέχει πληροφορίες σχετικά με τις πραγματικές και τις προβλεπόμενες ταξινομήσεις από ένα σύστημα ταξινόμησης. Παρακάτω απεικονίζεται ένας πίνακας σύγχυσης:

		Prediction	
		0	1
Actual	0	TN	FP
	1	FN	TP

Σχήμα 2.5: Confusion Matrix[40]

2.8.2 Βασικοί δείκτες

Ο Confusion Matrix δίνει τα εξής χαρακτηριστικά:

TP: Αληθώς θετικές προβλέψεις
FP: Ψευδώς θετικές προβλέψεις
FN: Ψευδώς αρνητικές προβλέψεις
TN: Αληθώς αρνητικές προβλέψεις
P: Θετικές προβλέψεις
N: Αρνητικές προβλέψεις

Από αυτά τα χαρακτηριστικά του Confusion matrix προκύπτουν οι ακόλουθοι δείκτες[39]:

<u>Sensitivity, recall, true positive rate (TPR)</u>
Η ευαισθησία, ή αλλιώς το ποσοστό των αληθώς θετικών, μετρά το ποσοστό των θετικών περιπτώσεων, που έχουν ταξινομηθεί σωστά[39].Για παράδειγμα, αν η κλοπή θεωρείται η θετική τάξη, τότε ο δείκτης αυτός αναφέρει τις περιπτώσεις απάτης που σωστά ταξινομήθηκαν ως απάτες.

$$\text{Sens=TPR=}\frac{TP}{P} = \frac{TP}{TP+FN}$$

<u>Specificity, true negative rate (TNR)</u>
Η ειδικότητα, ή αλλιώς το ποσοστό των αληθώς αρνητικών, μετρά το ποσοστό των αρνητικών περιπτώσεων, που έχουν ταξινομηθεί σωστά. Για παράδειγμα, αν η κλοπή θεωρείται η θετική τάξη, τότε ο δείκτης αυτός αναφέρει τις περιπτώσεις χωρίς απάτη που σωστά ταξινομήθηκαν χωρίς απάτη.

SPC=TNR==$\frac{TN}{N} = \frac{TN}{TN+FP}$

Accuracy (ACC)

Η ακρίβεια δείχνει το ποσοστό των αληθών (θετικών και αρνητικών) αποτελεσμάτων :

ACC=$\frac{TP+TN}{P+N}$

Positive predictive value,precision (PPV)

Η θετική προβλεπόμενη τιμή ορίζεται ως το ποσοστό των αληθώς θετικών προβλέψεων έναντι των θετικών:

PPV=$\frac{TP}{TP+FP}$

Negative predictive value (NPV)

Η αρνητική προβλεπόμενη τιμή είναι το ποσοστό των αληθώς αρνητικών αποτελεσμάτων έναντι των αρνητικών:

NPV=$\frac{TN}{TN+FN}$

False positive rate (FPR)

Το ποσοστό των ψευδώς θετικών αποτελεσμάτων είναι το ποσοστό των αρνητικών αποτελεσμάτων, που έχουν ταξινομηθεί ως θετικά αποτελέσματα. Για παράδειγμα, αν η κλοπή θεωρείται η θετική τάξη, τότε ο δείκτης αυτός αναφέρει τις περιπτώσεις χωρίς απάτη που λανθασμένα ταξινομήθηκαν με απάτη.

FPR=$\frac{FP}{N} = \frac{FP}{FP+TN}$ =1- SPC

False Negative rate (FNR)

Το ποσοστό των ψευδώς αρνητικών αποτελεσμάτων είναι το ποσοστό των θετικών αποτελεσμάτων, που λανθασμένα ταξινομήθηκαν ως αρνητικά, δηλαδή περιπτώσει με απάτη που λανθασμένα ταξινομήθηκαν να είναι χωρίς απάτη.

FNR=$\frac{FN}{P} = \frac{FN}{FN+TP}$

F1 Score

Το F1-Score είναι ένα μέτρο της ακρίβειας της δοκιμής, όταν ο δείκτης ακρίβειας δεν είναι επαρκές μέτρο απόδοσης. Αυτό συμβαίνει κυρίως, όταν ο αριθμός των αρνητικών περιπτώσεων (χωρίς απάτη) είναι πολύ μεγαλύτερος από τον αριθμό των θετικών περιπτώσεων (με απάτη). Το F1 Score ερμηνεύεται ως ο σταθμισμένος μέσος όρος της ακρίβειας (precision) και της ανάκλησης (recall), όπου η καλύτερη αξία του είναι το 1 και η χειρότερη το 0.

$$F1=\frac{2TP}{2TP+FP+FN}$$

Highest Difference (HD)

Το Highest Difference(HD) είναι η διαφορά του TPR με το FPR, για το οποίο η καλύτερη περίπτωση είναι κοντά στο 1, ενώ η χειρότερη είναι στο 0.

2.8.3 Καμπύλη ROC

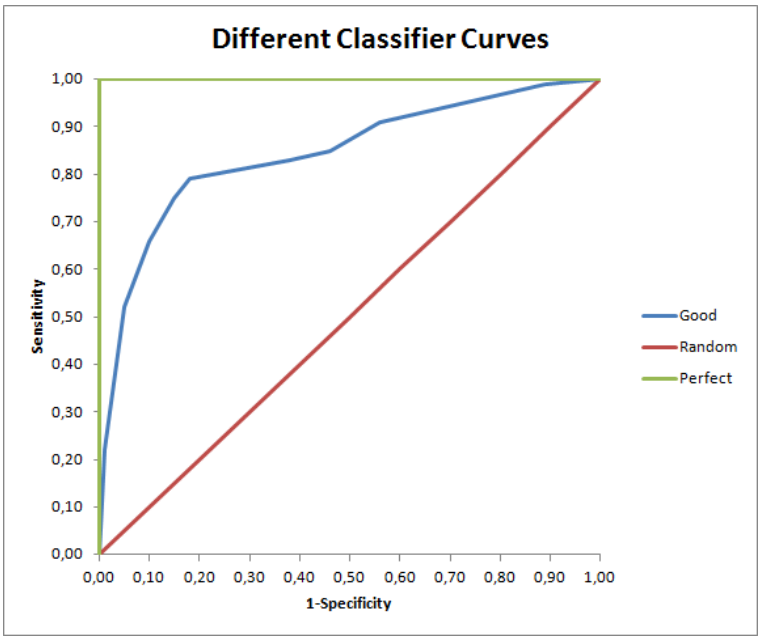
Το ROC (Receiver Operating Characteristic) γράφημα είναι ένας άλλος τρόπος, εκτός από τις μήτρες σύγχυσης, για την εξέταση της απόδοσης των ταξινομητών[41]. Η ROC ανάλυση διερευνά την σχέση, που συνδέει την ευαισθησία (sensitivity) και την ειδικότητα (specificity) ενός δυαδικού ταξινομητή. Μία καμπύλη Roc είναι μια γραφική παράσταση, με τον δείκτη των ψευδώς θετικών ενδείξεων της ταξινόμησης (FPR) στον άξονα των x και τον δείκτη των αληθώς θετικών ταξινομήσεων (TPR) στον άξονα των y. Σε πολλές περιπτώσεις, ένας ταξινομητής έχει μια παράμετρο, που ρυθμίζεται, για να αυξήσει τα αληθώς θετικά (True Positives) αποτελέσματα με κόστος αυξημένων ψευδώς θετικών (False Positives), αλλιώς μειώνοντας τα ψευδώς θετικά (FP) με κόστος τη μείωση των αληθώς θετικών (TP). Κάθε ρύθμιση παραμέτρων παρέχει ένα ζευγάρι (FP, TP) και μια σειρά από τέτοια ζεύγη χρησιμοποιούνται για να σχεδιαστεί μια καμπύλη ROC. Ένας μη παραμετρικός ταξινομητής αντιπροσωπεύεται από ένα μόνο σημείο ROC, που αντιστοιχεί στο (FP, TP) ζεύγος [43][44].

Η ερμηνεία των σημείων (FP,TP) της ROC καμπύλης είναι [43][44]:

- το σημείο (0,1) είναι για έναν τέλειο ταξινομητή επειδή ο δείκτης των ψευδώς θετικών είναι 0 και ο δείκτης των αληθώς θετικών είναι 1.
- το σημείο (0,0) αντιπροσωπεύει έναν ταξινομητή που προβλέπει όλες τις περιπτώσεις να είναι αρνητικές, ενώ

- το σημείο (1,1) απαντά σε έναν ταξινομητή που προβλέπει κάθε περίπτωση να είναι θετική και
- το σημείο (1,0) είναι ο ταξινομητής που είναι λάθος για όλες τις ταξινομήσεις.

Στο Σχήμα 2.6 φαίνονται τρεις περιπτώσεις διαφορετικής ταξινόμησης, δηλαδή ενός τέλειου, ενός μέτριου και ενός κακού μοντέλου ταξινόμησης.



Σχήμα 2.6 : Παράδειγμα καμπυλών ROC[42]

Ένα μέτρο της διαχωριστικής ικανότητας χαρακτηριστικών μεταξύ κλάσεων απεικονίζεται από μια καμπύλη ROC. Μετριέται η επικάλυψη των συναρτήσεων πυκνότητας πιθανότητας, οι οποίες περιγράφουν σε κάθε μία από τις δύο κλάσεις την κατανομή τιμών ενός χαρακτηριστικού. Η επικάλυψη ποσοτικοποιείται μέσω μιας περιοχής που ορίζουν δύο καμπύλες. Η περιοχή αυτή είναι γνωστή και ως AUC (Area Under the Receiver Operating Curve-Περιοχή κάτω από την καμπύλη ROC). Όταν υπάρχει επικάλυψη, η τιμή της AUC είναι κοντά στο μηδέν, ενώ όταν οι κλάσεις διαχωρίζονται πλήρως, ισούται με 1. Επιπλέον, το AUC αντιπροσωπεύει την πιθανότητα ένας ταξινομητής να κατατάξει ψηλότερα ένα τυχαία επιλεγμένο θετικό δείγμα από ένα τυχαίο αρνητικό, θεωρώντας πάντα ότι τα θετικά κατατάσσονται ψηλότερα από τα αρνητικά[41].Μεταφράζοντας τα παραπάνω σε περιπτώσεις κλοπών, το AUC δίνει την πιθανότητα η τιμή της δοκιμής για μία περίπτωση με κλοπή να είναι μεγαλύτερη από την τιμή της δοκιμής μιας περιτπώσεως χωρίς κλοπή. Οι τιμές του AUC είναι μεταξύ 1 και 0. Εάν ο ταξινομητής είναι πολύ καλός, ο δείκτης των αληθώς θετικών θα αυξάνει γρήγορα και η περιοχή κάτω από την

καμπύλη (AUC) θα είναι κοντά στη μονάδα (1) σε αντίθετη περίπτωση θα είναι μηδέν (0). Εάν ο ταξινομητής δεν είναι καλύτερος από την «τυχαία επιλογή», ο δείκτης των αληθώς θετικών προβλέψεων θα αυξάνει γραμμικά με τον δείκτη των ψευδώς θετικών προβλέψεων και το εμβαδόν κάτω από την καμπύλη ROC (AUC) θα είναι ίσο με 0.5.

Κεφάλαιο 3

Μεθοδολογία εντοπισμού απάτης

3.1 Εισαγωγή

Στο παρόν κεφάλαιο αναλύεται η διαδικασία της ανίχνευσης απάτης με χρήση ιστορικών δεδομένων. Αρχικά, γίνεται μια περιγραφή των εννοιών «εξόρυξη δεδομένων», «προεπεξεργασία δεδομένων», «εξαγωγή χαρακτηριστικών» και ύστερα η προετοιμασία των δεδομένων για είσοδο στον αλγόριθμο ταξινόμησης SVM, καθώς επίσης και της βελτιστοποίησης των παραμέτρων του, καταλήγοντας στο κατά πόσο τα αποτελέσματα της ταξινόμησης βοηθάνε στην εξαγωγή συμπερασμάτων σχετικά με την ανίχνευση απάτης.

Τα διαθέσιμα δεδομένα είναι άρτια, δηλαδή θεωρείται γνωστό, ότι δεν έχει διαπραχθεί κάποιου είδους απάτης. Για αυτό το λόγο, γίνεται προσομοίωση βάσει συναρτήσεων, με σκοπό να δημιουργηθεί απάτη και να μπορέσει ο αλγόριθμος να εξάγει αποτελέσματα και περαιτέρω συμπεράσματα για την απόδοσή του.

3.2 Εξόρυξη γνώσης και κατηγοριοποίηση δεδομένων

3.2.1 Εξόρυξη δεδομένων

Η εξόρυξη δεδομένων, γνωστή και ως «ανακάλυψη γνώσης» σε βάσεις δεδομένων, στην επιστήμη των υπολογιστών είναι η διαδικασία ανακάλυψης ενδιαφερόντων και χρήσιμων προτύπων και σχέσεων μεγάλων όγκων δεδομένων. Η συγκεκριμένη διαδικασία συνδυάζει εργαλεία στατιστικής ανάλυσης και τεχνητής νοημοσύνης (όπως τα νευρωνικά δίκτυα και η μηχανική μάθηση), με την διαχείριση βάσεων δεδομένων για ανάλυση ψηφιακών συλλογών, ή αλλιώς σύνολα δεδομένων. Η εξόρυξη δεδομένων χρησιμοποιείται σε επιχειρήσεις (ασφαλιστικές, τραπεζικές, λιανικού εμπορίου), σε έρευνες επιστήμης (αστρονομία, ιατρική) και στην ασφάλεια ενός κράτους [45].

Ο πολλαπλασιασμός πολλών μεγάλων, και κάποιες φορές συνδεόμενων, κυβερνητικών ή ιδιωτικών βάσεων δεδομένων έχει οδηγήσει σε ρυθμίσεις για την διασφάλιση της ακρίβειας και ασφάλειας μεμονωμένων αρχείων, για μη εξουσιοδοτημένη προβολή ή αλλοίωση. Τα περισσότερα είδη εξόρυξης δεδομένων

στοχεύουν στη διαπίστωση της γενικής γνώσης για μια ομάδα, παρά για συγκεκριμένα άτομα. Για παράδειγμα, ένα σουπερ μάρκετ ανησυχεί λιγότερο για την πώληση ενός προϊόντος σε ένα άτομο, από την πώληση πολλών σε πολλούς. Επίσης, μέσα από την εξόρυξη δεδομένων διακρίνεται μια ανώμαλη συμπεριφορά ατόμου, όπως απάτη ή άλλη εγκληματική δραστηριότητα[45].

Η πλήρης διαδικασία εξόρυξης δεδομένων περιλαμβάνει πολλά βήματα για την κατανόηση των στόχων του έργου και την εύρεση των διαθέσιμων στοιχείων σε περιπτώσεις αλλαγών στη διαδικασία με βάση την τελική ανάλυση τους. Τα τρία βασικά υπολογιστικά βήματα είναι η διαδικασία μάθησης του μοντέλου, η αξιολόγησή του, και η χρήση του. Η διαίρεση αυτή γίνεται σαφέστερη ταξινομώντας τα δεδομένα. Η εκπαίδευση του μοντέλου συμβαίνει, όταν υπάρχουν δεδομένα για τα οποία η ομάδα (ή η κατηγορία) χαρακτηριστικών τους είναι γνωστή για την παραγωγή ενός ταξινομητή ή ενός αλγόριθμου που εκπαιδεύεται από αυτά. Ο ταξινομητής στη συνέχεια δοκιμάζεται με ένα ανεξάρτητο σύνολο αξιολόγησης, το οποίο περιέχει δεδομένα με γνωστές ιδιότητες. Ο βαθμός, στον οποίο οι ταξινομήσεις του μοντέλου συμφωνούν με τη γνωστή κατηγορία αναφέρεται στον προσδιορισμό της αναμενόμενης ακρίβειας του μοντέλου. Εάν το μοντέλο είναι αρκετά ακριβές, τότε χρησιμοποιείται για την ταξινόμηση δεδομένων, των οποίων τα χαρακτηριστικά είναι άγνωστα[45].

Οι τεχνικές εξόρυξης δεδομένων διακρίνονται ως εξής[45]:

- <u>Προγνωστική Μοντελοποίηση</u>

  Η προγνωστική μοντελοποίηση χρησιμοποιείται, όταν ο σκοπός είναι η εκτίμηση της αξίας ενός συγκεκριμένου χαρακτηριστικού-στόχου και υπάρχουν δεδομένα εκπαίδευσης του δείγματος, των οποίων οι τιμές του εν λόγω χαρακτηριστικού είναι γνωστές. Ένα παράδειγμα είναι η ταξινόμηση. Από αυτή λαμβάνεται ένα σύνολο δεδομένων, που έχουν ήδη χωριστεί σε προκαθορισμένες ομάδες, και αναζητούνται μοτίβα στα δεδομένα που διαφοροποιούν αυτές τις ομάδες.

- <u>Περιγραφική Μοντελοποίηση</u>

  Η περιγραφική μοντελοποίηση, ή ομαδοποίηση, χωρίζει επίσης τα στοιχεία σε ομάδες. Με την ομαδοποίηση, ωστόσο, οι κατάλληλες ομάδες δεν είναι γνωστές εκ των προτέρων. Τα πρότυπα αναδύονται από την ανάλυση των δεδομένων που χρησιμοποιούνται για τον προσδιορισμό των ομάδων.

- Εξόρυξη Προτύπων

  Το μοτίβο προτύπων επικεντρώνεται στον προσδιορισμό κανόνων που περιγράφουν συγκεκριμένα μοτίβα μέσα στα δεδομένα. Μια σημαντική χρήση της «εξόρυξης προτύπων» είναι η ανακάλυψη διαδοχικών μοντέλων. Για παράδειγμα, ακολουθίες σφαλμάτων ή προειδοποιήσεις που προηγούνται πριν από κάποια αστοχία σε έναν εξοπλισμό, χρησιμοποιούνται για να προγραμματιστεί προληπτική συντήρηση, ειδάλλως για να παρασχεθεί μια διορατικότητα σε ένα ελάττωμα σχεδιασμού.

- Ανίχνευση ανωμαλιών

  Η ανίχνευση ανωμαλιών θεωρείται η άλλη όψη της ομαδοποίησης. Βρίσκει περιπτώσεις δεδομένων που είναι ασυνήθιστες και δεν ταιριάζουν σε οποιοδήποτε καθιερωμένο πρότυπο. Η ανίχνευση της απάτης είναι ένα παράδειγμα της ανίχνευσης ανωμαλίας. Παρ' όλο που η ανίχνευση της απάτης θεωρείται πρόβλημα για την προγνωστική μοντελοποίηση, η σχετική σπανιότητα των παράνομων συναλλαγών και η ταχύτητα με την οποία οι εγκληματίες αναπτύσσουν νέες μορφές απάτης σημαίνουν, ότι κάθε προγνωστικό μοντέλο είναι πιθανό να είναι χαμηλής ακρίβειας και να ξεπεραστεί γρήγορα. Έτσι, η ανίχνευση ανωμαλιών επικεντρώνεται στη μοντελοποίηση του «τι είναι φυσιολογική συμπεριφορά» για τον εντοπισμό ασυνήθιστων συναλλαγών. Επίσης, η ανίχνευση ανωμαλιών χρησιμοποιείται με διάφορα συστήματα παρακολούθησης, όπως στην περίπτωση ανίχνευσης εισβολών.

3.2.2 Προεπεξεργασία δεδομένων

Οι σημερινές βάσεις δεδομένων είναι αρκετά ευαίσθητες σε θορυβώδη, εκλειπόμενα και ασυνεπή δεδομένα, λόγω του μεγάλου μεγέθους τους (πολλά gigabytes) και της προέλευσης τους, από πολλαπλές και ετερογενείς πηγές. Τα χαμηλής ποιότητας δεδομένα οδηγούν σε χαμηλής ποιότητας αποτελέσματα εξόρυξης[48]. Το πρώτο μέρος της τεχνικής ανίχνευσης με βάση την ταξινόμηση είναι η προ επεξεργασία των δεδομένων. Τα δεδομένα, πριν την μελέτη τους δεν πρέπει να περιέχουν λάθη, όπως θόρυβο, έλλειψη μετρήσεων κλπ.

Υπάρχουν αρκετές τεχνικές προεπεξεργασίας δεδομένων. Ο «καθαρισμός» των δεδομένων εφαρμόζεται, ώστε να αφαιρέσει τον θόρυβο και να διορθώσει τις ασυνέπειες των δεδομένων. Η «ενοποίηση» των δεδομένων συγχωνεύει δεδομένα από πολλαπλές πηγές σε ένα συνεκτικό χώρο αποθήκευσής τους, όπως η αποθήκη δεδομένων (data warehouse). Η «μείωση» των δεδομένων μειώνει το μέγεθός τους αθροίζοντας ή εξαλείφοντας περιττά χαρακτηριστικά (features) ή με την ομαδοποίηση (clustering). Ο «μετασχηματισμός» των δεδομένων, όπως ένα

παράδειγμα είναι η κανονικοποίηση, εφαρμόζεται ώστε τα δεδομένα να κλιμακώνονται σε ένα μικρότερο εύρος τιμών, για παράδειγμα από 0 έως 1. Αυτό μπορεί να βελτιώσει την ακρίβεια και την αποδοτικότητα αλγορίθμων εξόρυξης[48].

3.2.3 Εξαγωγή χαρακτηριστικών

Στη μηχανική μάθηση, στην αναγνώριση προτύπων και την επεξεργασία εικόνας, η εξαγωγή χαρακτηριστικών ξεκινάει από ένα αρχικό δείγμα δεδομένων, αποτέλεσμα μετρήσεων, και κατόπιν χτίζονται διακριτές τιμές (χαρακτηριστικά), με σκοπό την πληροφόρηση, διευκολύνοντας τα επόμενα βήματα μάθησης και γενίκευσης. Η εξαγωγή χαρακτηριστικών σχετίζεται με τη μείωση της διάστασης του μεγάλου όγκου δεδομένων και σε ορισμένες περιπτώσεις οδηγεί σε καλύτερες ερμηνείες.

Όταν τα δεδομένα εισόδου σε ένα αλγόριθμό είναι σημαντικά μεγάλα για να υποβληθούν σε επεξεργασία, τότε μπορούν να μετατραπούν σε ένα μειωμένο σύνολο χαρακτηριστικών. Τα επιλεγμένα χαρακτηριστικά αναμένονται να περιέχουν σχετικές πληροφορίες από τα δεδομένα εισόδου, έτσι ώστε η επιθυμητή εργασία να χρησιμοποιείται με τη αξιοποίηση μειωμένης αναπαράστασης των αρχικών στοιχείων[49].

3.2.4 Βελτιστοποίηση παραμέτρων αλγόριθμου ταξινόμησης-Cross Validation

Αφού ληφθεί ο απαιτούμενος όγκος δεδομένων και προεπεξεργαστεί και στη συνέχεια, αν χρειάζεται, εξαχθούν τα κατάλληλα χαρακτηριστικά, γίνεται η πρώτη διαδικασία στην ταξινόμηση· η βελτιστοποίηση των παραμέτρων.

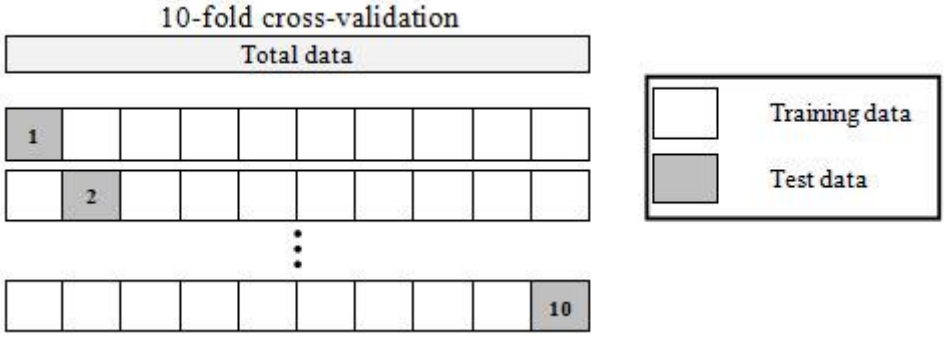
Για την εκπαίδευση του μοντέλου SVM πρέπει να προσδιοριστούν οι παράμετροι C και γ, για τις οποίες αναλύθηκε η χρησιμότητά τους στο Κεφάλαιο 2. Ο προσδιορισμός αυτών γίνεται με την βοήθεια της ακρίβειας του μοντέλου Cross-Validation. Επιστρέφονται οι παράμετροι εκείνες, που δίνουν την μεγαλύτερη ακρίβεια Cross-Validation. Το εργαλείο επιλογής των παραμέτρων θεωρείται πως είναι η RBF (Γκαουσιανή) συνάρτηση πυρήνα και χρησιμοποιείται κατ' επέκταση άλλων συναρτήσεων πυρήνα. Ο τύπος της RBF (Radial Basis Function) ορίζεται ως:

$$K(x_i, x_j) = e^{-\gamma\|x_i - x_j\|^2}$$

Στην μέθοδο Cross Validation (CV), ή αλλιώς Rotation Estimation, η οποία είναι μια τεχνική επικύρωσης δεδομένων, αξιολογούνται αποτελέσματα μιας στατιστικής ανάλυσης για το κατά πόσο γενικεύονται σε ένα ανεξάρτητο σύνολο δεδομένων. Χρησιμοποιείται κυρίως όταν στόχος είναι μια πρόβλεψη, και πρέπει να

εκτιμηθεί η ακρίβεια του μοντέλου πρόβλεψης. Στην τεχνική k-fold Cross Validation, το αρχικό δείγμα δεδομένων κατανέμεται τυχαία σε k υποσύνολα ίσου μεγέθους Από τα k υποσύνολα, ένα συγκρατείται για την δοκιμή του μοντέλου και τα υπόλοιπα k-1 υποσύνολα χρησιμοποιούνται για την εκπαίδευση του μοντέλου. Γίνονται, επομένως, k επαναλήψεις εκπαίδευσης και αξιολόγησης, ώστε σε κάθε επανάληψη ένα διαφορετικό υποσύνολο δεδομένων να χρησιμοποιείται προς αξιολόγηση και έλεγχο. Από τα k αποτελέσματα των δοκιμών υπολογίζεται ο μέσος όρος και παράγεται μία μοναδική εκτίμηση. Με τη διαδικασία αυτή, σε ένα μεγάλο k είναι δύσκολο να εμφανιστεί υποσύνολο, στο οποίο έχει γίνει «υπερεκπαίδευση»[50].

Στο παρακάτω σχήμα απεικονίζεται η διαδικασία που στηρίζεται ο αλγόριθμος του 10-fold Cross Validation.



Σχήμα 3.1 : 10-fold Cross Validation [46]

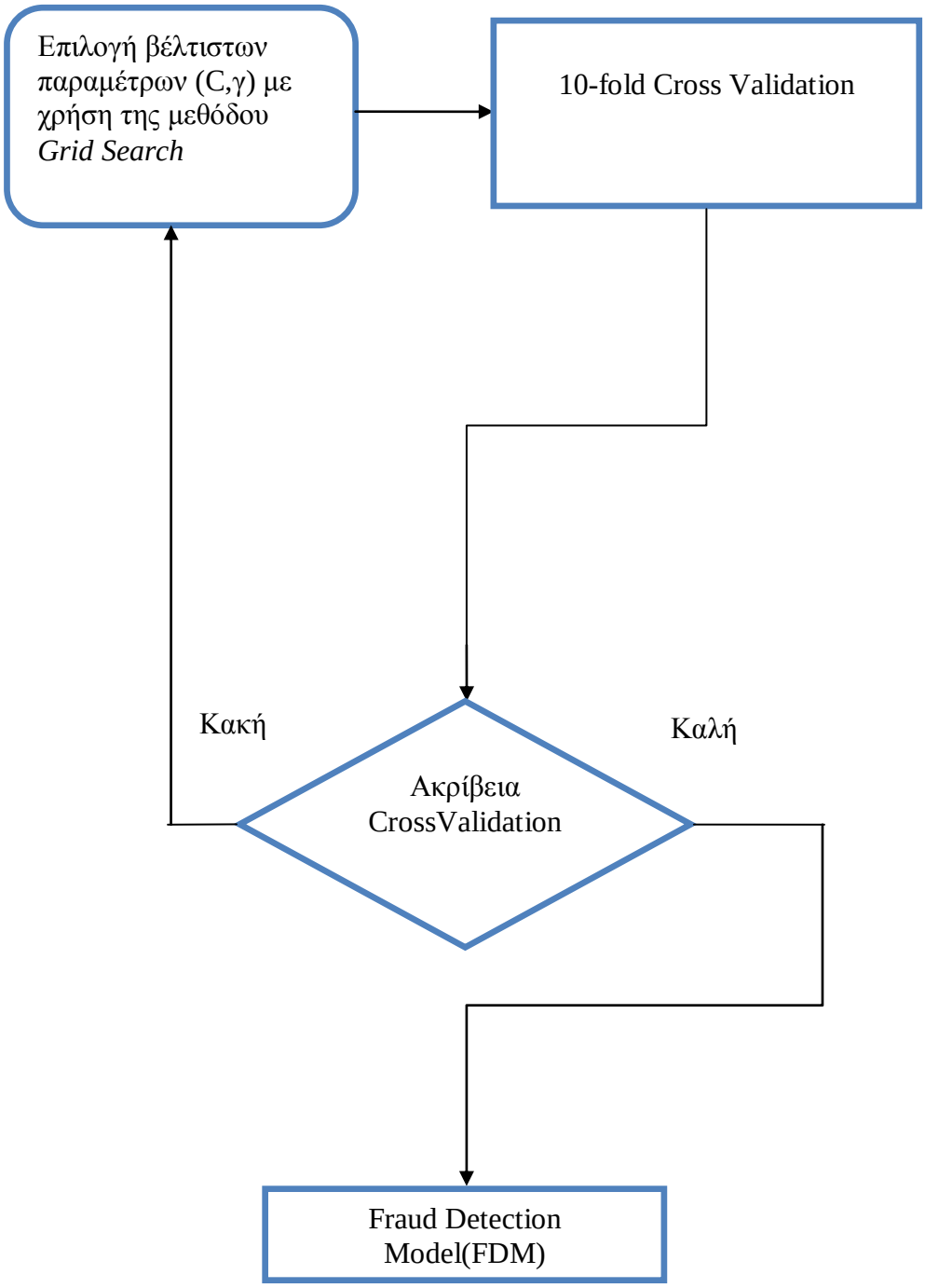
Φαίνεται, ότι κάθε φορά χρησιμοποιείται ένα υποσύνολο για να αξιολογηθεί σε σχέση με τα υπόλοιπα υποσύνολα, τα οποία είναι για την εκπαίδευση του μοντέλου.

Έτσι, οι C,γ παράμετροι υπολογίζονται, ώστε για κάθε πιθανό συνδυασμό των τιμών τους να ελέγχεται η ακρίβεια του Cross Validation. Η μέθοδος αυτή λέγεται grid searching. Σε αυτή, εκθετικά αυξανόμενες ακολουθίες των παραμέτρων C,γ χρησιμοποιούνται για τον προσδιορισμό των παραμέτρων, αποκτώντας την καλύτερη ακρίβεια του CV. Στην εργασία χρησιμοποιείται 10-fold cross-validation για την αναζήτηση των βέλτιστων παραμέτρων της συνάρτησης πυρήνα, C και γ. Όλα τα ζεύγη (C,γ) της RBF συνάρτησης πυρήνα δοκιμάστηκαν και επιλέχθηκε αυτό με την καλύτερη ακρίβεια. Οι ακολουθίες παραμέτρων ήταν, C=$[2^{-5}, 2^{-3}\ldots, 2^{15}]$ και γ=$[2^{-15}, 2^{-13}, \ldots, 2^{3}]$, και C=$[2^{0}, 2^{1}\ldots, 2^{7}]$ και γ=$[2^{-3}, 2^{-2}, \ldots, 2^{3}]$[33].

Για κάθε ζευγάρι (C,γ) η απόδοση του cross-validation μετρήθηκε με την εκπαίδευση του 70% των δεδομένων και δοκιμάστηκε στο υπόλοιπο 30%. Ο λόγος που χρησιμοποιείται 10-fold CV είναι η επιβεβαίωση, ότι δεν θα υπάρξει πρόβλημα υπερ-κάλυψης των δεδομένων κατάρτισης.

Το επόμενο διάγραμμα ροής δείχνει τη διαδικασία με την οποία κάθε φορά εξετάζεται η ακρίβεια του CV με το αντίστοιχο ζεύγος (C,γ). Όταν εξαντλούνται οι

συνδυασμοί, τότε το ζευγάρι που δίνει την μέγιστη ακρίβεια κρατιέται, με σκοπό να τροφοδοτηθεί από την αρχή το μοντέλο ταξινόμησης, αυτή τη φορά με τον διαχωρισμό των δεδομένων εκπαίδευσης και δοκιμής, όπως αναφέρθηκε στην προηγούμενη παράγραφο, και γίνεται η ταξινόμηση για απάτη.



Σχήμα 3.2: Διάγραμμα ροής της προτεινόμενης μεθόδου εκπαίδευσης του αλγόριθμου C-SVM με βελτιστοποίηση παραμέτρων

3.2.5 Ταξινόμηση

Η εξόρυξη των δεδομένων, η προεπεξεργασία τους σε ένα επιθυμητό τύπο και όγκο, και η εξαγωγή χαρακτηριστικών, εάν είναι απαραίτητο, εφαρμόζονται ώστε σε κατάλληλη μορφή, να κατηγοριοποιηθούν τα δεδομένα με τα ίδια χαρακτηριστικά. Αυτή είναι η ταξινόμηση, και συγκεκριμένα η ταξινόμηση με βάση τις μηχανές διανυσμάτων υποστήριξης, όπως έχουν αναλυθεί μέχρι τώρα. Στη προηγούμενη ενότητα έγινε αναφορά των παραμέτρων που χρειάζεται να βελτιστοποιηθούν, για να διαμορφωθούν επιθυμητά αποτελέσματα. Προς εξέταση μένει η είσοδος του αλγόριθμου ταξινόμησης με SVM και η έξοδος.

Για την είσοδο του SVM τα δεδομένα διαχωρίζονται σε δύο υποσύνολα: σε ένα σύνολο εκπαίδευσης (training set) και σε ένα σύνολο απόδοσης των αποτελεσμάτων του αλγόριθμου, ή αλλιώς αξιολόγησης του αλγορίθμου, γνωστό ως σύνολο δοκιμών (test set). Από τα δεδομένα εκπαίδευσης ο αλγόριθμος μαθαίνει την διασύνδεση των δειγμάτων, που προκύπτουν από μια πηγή. Στη συνέχεια, τα μελλοντικά δείγματα φιλτράρονται από τη συνάρτηση απόφασης φ(x), η οποία παίρνει τιμές -1,1 και στο τέλος του αλγόριθμου ανιχνεύονται ποια από τα δείγματα είναι ανώμαλα, δηλαδή έχουν παραχθεί από διαφορετική κατανομή, όπως στην περίπτωση δημιουργίας απάτης.

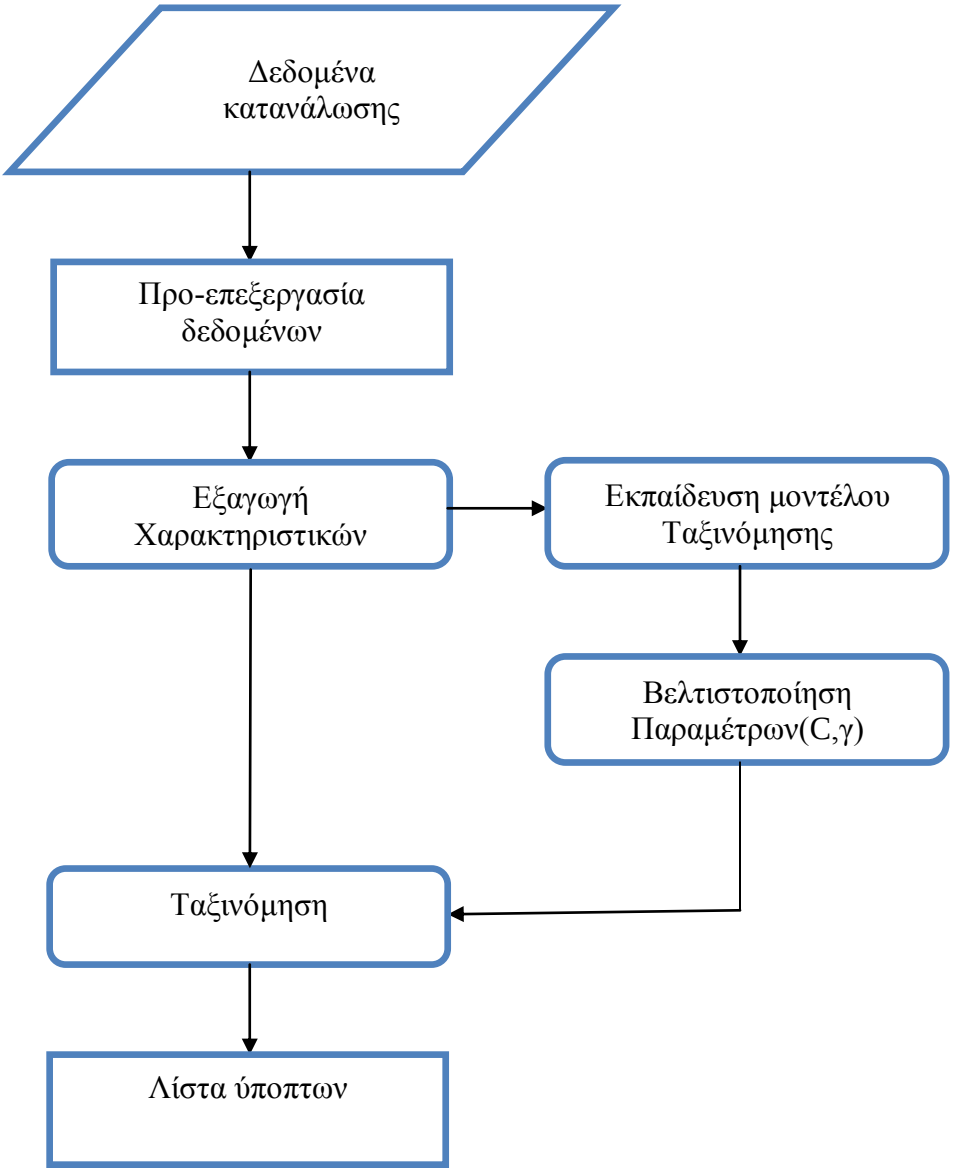
Σύμφωνα με τα παραπάνω, στον δυαδικό ταξινομητή SVM η είσοδος για την εκπαίδευση είναι τα διανύσματα $\overrightarrow{x_i}$ του συνόλου. Αυτά είναι διανύσματα με χαρακτηριστικά στην ουσία. Τα διανύσματα αυτά μπορεί να είναι πολλά, επομένως η είσοδος είναι ένας πίνακας N×M, όπου N είναι ο αριθμός των στοιχείων προς ταξινόμηση και M είναι ο αριθμός των χαρακτηριστικών του καθενός. Η τελευταία στήλη του πίνακα είναι το διάνυσμα $\vec{y}$, το οποίο παίρνει τιμές [-1,1] ή [0,1] και είναι ο στόχος της εκπαίδευσης, δηλαδή η επιθυμητή έξοδος της μηχανής. Η μηχανή καλείται να μάθει την ανωτέρω αντιστοιχία εισόδων-εξόδων, ώστε να εφαρμοστεί η γνώση αυτή σε νέες άγνωστες εισόδους που θα της παρουσιαστούν. Κατά αυτόν τον τρόπο, όταν της παρουσιαστεί μια νέα είσοδος $\vec{x}^*$, θα μπορεί να παρέχει μια αντίστοιχη τιμή της εξόδου $\vec{y}^*$. Η μηχανή εκμάθησης καλείται να μάθει την αντιστοίχηση :

$$\overrightarrow{x_i} \rightarrow \overrightarrow{y_i}$$

Όπου $y_i \epsilon$ {-1,1}

Ζητούμενο είναι το SVM να εκπαιδευτεί στην αντιστοίχιση κάθε προτύπου με την κλάση του και να μάθει να ταξινομεί σωστά.

Στο παρακάτω διάγραμμα φαίνονται όσα αναφέρθηκαν παραπάνω και ειδικότερα για την περίπτωση ανίχνευσης απάτης.



Σχήμα 3.3 : Η ροή του προτεινόμενου τρόπου ανίχνευσης απάτης σε καταναλωτές με ασυνήθιστες και κακόβουλες δραστηριότητες

3.3 *Διαδικασία ανάλυσης δεδομένων*

Σε αυτή την ενότητα γίνεται περιγραφή της διαδικασίας ανάλυσης των δεδομένων. Συγκεκριμένα, περιγράφονται τα ιστορικά δεδομένα που ήταν διαθέσιμα, η προσομοίωση απάτης, ο μετασχηματισμός των πινάκων στην κατάλληλη μορφή για είσοδο στον αλγόριθμο ταξινόμησης. Επίσης, περιγράφεται η ανάλυση με εξαγωγή χαρακτηριστικών και το τελικό στάδιο, δηλαδή εκείνο των αποτελεσμάτων και των δεικτών που θα βοηθήσουν στην εξαγωγή συμπερασμάτων.

3.3.1 *Περιγραφή ιστορικών δεδομένων κατανάλωσης προς ανάλυση*

Στην παρούσα διπλωματική εργασία χρησιμοποιήθηκαν για την εφαρμογή του μοντέλου ταξινόμησης και την εξαγωγή συμπερασμάτων ιστορικά δεδομένα κατανάλωσης. Τα δεδομένα ήταν διαθέσιμα δημόσια από το κέντρο ISSDA (Irish Social Science Data Archive). Το ISSDA αποτελεί ένα κορυφαίο κέντρο στην Ιρλανδία για ποσοτική απόκτηση, διατήρηση και διάδοση δεδομένων. Κατέχει μια σειρά βασικών Ιρλανδικών και διεθνών συνόλων δεδομένων, καθιστώντας αυτά τα δεδομένα διαθέσιμα για δευτερογενή ανάλυση από φοιτητές, ακαδημαϊκούς και ερευνητές στο δημόσιο και εμπορικό τομέα. Όλα τα δεδομένα έχουν υποβληθεί σε αυστηρούς ελέγχους για την εξασφάλιση της πλήρης ανωνυμίας, προστατεύοντας το ιδιωτικό απόρρητο[47]. Τα δεδομένα της εργασίας ήταν από την έρευνα για έξυπνους μετρητές στην Ιρλανδία (Irish smart meter trial) και περιλάμβαναν ημίωρες μετρήσεις κατανάλωσης, για πάνω από 5000 καταναλωτές, για ενάμιση χρόνο. Η πρώτη μέτρηση ξεκινάει από τα μεσάνυχτα της 14^{ης} Ιουλίου του 2009 και σταματάει την 31^{η} Δεκεμβρίου του 2010. Έτσι, κάθε καταναλωτής, ο οποίος δέχθηκε να πάρει μέρος στην έρευνα, είχε εγκατεστημένο έναν έξυπνο μετρητή στο σπίτι του ή στην επιχείρησή του. Ωστόσο, είναι λογική η υπόθεση ότι οι καταναλωτές που δέχτηκαν, να είναι τίμιοι και χωρίς απάτες. Ο μεγάλος αριθμός και η ποικιλία καταναλωτών, οι μεγάλων περιόδων μετρήσεις και η διαθεσιμότητά τους δημόσια καθιστά αυτά τα δεδομένα μία εξαιρετική πηγή για ανάλυση δεδομένων έξυπνων μετρητών[24].

Ένα μικρό δείγμα της μορφής που ήταν αρχικά τα δεδομένα φαίνεται στον παρακάτω πίνακα:

Πίνακα 3.1 : Δείγμα αρχικών ιστορικών δεδομένων κατανάλωσης

1392	19503	0,14
1392	19504	0,138
1392	19505	0,14
1392	19506	0,145
1392	19507	0,145
1392	19501	0,157
1392	19502	0,144
1392	19724	0,128
1392	19725	0,142
1392	19726	0,145
1392	19727	0,149
1392	19728	0,131
1392	19729	0,13
1392	19730	0,13
1392	19731	0,152
1392	19732	0,143
1392	19733	0,13
1392	19734	0,132
1392	19735	0,169
1392	19736	0,254
1392	19737	0,231
1392	19738	0,371
1392	19739	0,266
1392	19740	0,253

Στη πρώτη στήλη απεικονίζεται ο κωδικός του κάθε μετρητή. Στη δεύτερη στήλη αναγράφεται η ημερομηνία. Για παράδειγμα, “19503” είναι η 195^{η} μέρα του χρόνου, δηλαδή η 14^{η} Ιουλίου. “03” είναι το τρίτο ημίωρο εκείνης της ημέρας, με πρώτο να μετράται από τα μεσάνυχτα. Η τρίτη στήλη αποτελείται από τις μετρήσεις σε kWh. Τα δεδομένα αρχικά είχαν κάποιες ανομοιομορφίες, όπως ανακατεμένα ημίωρα, και έπρεπε να γίνει μια ταξινόμηση ως προς τις μέρες και τις ώρες. Επιπλέον, για μείωση του δειγματοληπτικού όγκου χρησιμοποιήθηκαν ωριαίες μετρήσεις με άθροισμα των ημιώρων, επομένως μειώθηκε ο όγκος στο μισό.

Ακόμη, σαν προεπεξεργασία έγινε ο διαχωρισμός του κάθε καταναλωτή σε πίνακες ξεχωριστούς. Εν ολίγοις, κάθε καταναλωτής αντιπροσωπεύτηκε από έναν πίνακα διαστάσεων ημέρες επί ωριαίες μετρήσεις κάθε μέρας, δηλαδή πίνακα ημερήσιων διανυσμάτων. Προς ανάλυση, κρατήθηκαν όσοι καταναλωτές είχαν τουλάχιστον μετρήσεις ενάμιση χρόνου, επομένως οι διαστάσεις των πινάκων ήταν 535×24. Τέλος, προστέθηκε σε κάθε τέτοιον πίνακα μια στήλη, η οποία έπαιρνε τιμές 0,1, διαχωρίζοντας τις μέρες με απάτη και τις άρτιες μέρες. Έτσι, ο πίνακας αυτός έγινε η είσοδος στον ταξινομητή SVM.

Αρχικά, οι μετρήσεις είναι από καταναλωτές γνήσιους, χωρίς απάτες. Για την ταξινόμηση, αλλοιώνονται τα δεδομένα σε επιλεγμένες μέρες, ώστε να υπάρχει προσομοίωση απάτης. Επιλέγονται οι μισές μέρες για κάθε καταναλωτή, με τυχαίο δειγματοληπτικό τρόπο, ώστε να γίνει καλύτερη εκπαίδευση του αλγόριθμου ταξινόμησης. Στην επόμενη ενότητα, αναφέρονται οι τρόποι αλλοίωσης των μετρήσεων και οι αντίστοιχες συναρτήσεις που κατασκευάστηκαν.

3.3.2 Προσομοίωση απάτης

Προκειμένου να εξεταστεί η απόδοση του αλγόριθμου ταξινόμησης, δημιουργήθηκαν βάσει γνήσιων δειγμάτων, ημέρες απάτης. Έτσι, ο δυαδικός ταξινομητής διαχωρίζει δύο κλάσεις [0,1], «0» για ημέρες χωρίς απάτη και «1» για ημέρες με απάτη. Ο παράγοντας αλλοίωσης άλλαζε σε κάθε δοκιμή ως προς την ένταση κλοπής, την χρονική διάρκεια της απάτης μέσα στην μέρα και τον συνδυασμό διαφορετικών βαθμών αλλοίωσης/απάτης. Για κάθε δείγμα **x**=$\{x_1, \dots, x_{24}\}$, δηλαδή δείγματα ημερών σε κάθε καταναλωτή παρήχθησαν δείγματα κακόβουλα με διάφορες συναρτήσεις, όπως φαίνονται παρακάτω.

Για κάθε t=1,…24.

1) $h_1(x_t) = ax_t,$

Όπου α είναι ο παράγοντας αλλοίωσης των δεδομένων και μπορούσε να είναι ένας σταθερός αριθμός, να προέρχεται από μια κατανομή βήτα (beta), κανονική (normal), τυχαία (random) στο διάστημα [0.1-0.9] με 0.1 να αναφέρεται σε έντονη απάτη, δηλαδή κλοπή της τάξεως του 90% των δεδομένων, ενώ με 0.9 μια ήπια απάτη, δηλαδή κλοπή της τάξεως του 10% των δεδομένων. Στην παραπάνω συνάρτηση η απάτη γίνεται και για τις 24 ώρες της ημέρας.

2) $h_2(x_t) = \beta_t x_t,$

όπου

$$\beta_t = \begin{cases} 0 & \text{start_time} < t < \text{end_time} \\ 1 & \text{else} \end{cases}$$

start_time= random(0, 23-minOfftime)
duration=random(minOfftime,24)
end_time=start_time+duration
minOfftime=[1,24]

Στην παραπάνω συνάρτηση γίνεται απάτη για τυχαία διάρκεια μέσα στη μέρα που ορίζεται από το minOfftime, duration, start_time, δηλαδή ορίζοντας την ελάχιστη ώρα όπου θα ξεκινήσει να γίνεται η απάτη. Η διάρκεια είναι τυχαία ανάμεσα στην

ελάχιστη ώρα και την τελευταία μέτρηση. Για τις ώρες που γίνεται απάτη, ο παράγοντας αλλοίωσης ήταν 0, άρα μηδενίζεται η μέτρηση, ενώ για το υπόλοιπο διάστημα ο παράγοντας αλλοίωσης είναι 1, άρα οι μετρήσεις παραμένουν αναλλοίωτες. Βέβαια, και εδώ δοκιμάστηκαν πολλές περιπτώσεις απάτης, όπως συγκεκριμένης διάρκειας ή παράγοντας αλλοίωσης, που ακολουθεί κάποια κατανομή και είναι σταθερός για κάθε ώρα.

Ακολουθούν κάποιες συναρτήσεις προσομοίωσης απάτης, όπως κατασκευάστηκαν για την εργασία από το πρόγραμμα MATLAB.

```
function [fraud]=typeofattack(x,process,b,d)

minOffTime=d;
if process == '1'
    duration=d;
else
   duration=minOffTime+23*rand(1);
end

start_time=(23-minOffTime)*rand(1);
end_time=start_time+duration;

l=length(x);
k=1;
for i=1:l
    if i>=start_time && i<=end_time
       fraud(k,1)=b*x(i);
       k=k+1;
    else
       fraud(k,1)=x(i);
       k=k+1;
    end
end
```

Σαν είσοδος της συνάρτησης είναι το διάνυσμα x μια ημέρας και η τιμή της διαδικασίας process, για τον αν η διάρκεια επίθεσης είναι καθορισμένη ή τυχαία στο διάστημα που ορίζει η μεταβλητή minOffTime. Το b συμβολίζει τον παράγοντα αλλοίωσης και το d μια καθορισμένη χρονική διάρκεια επίθεσης. Η έξοδος είναι το αλλοιωμένο διάνυσμα ημέρας, fraud.

Άλλη συνάρτηση ήταν η παρακάτω:

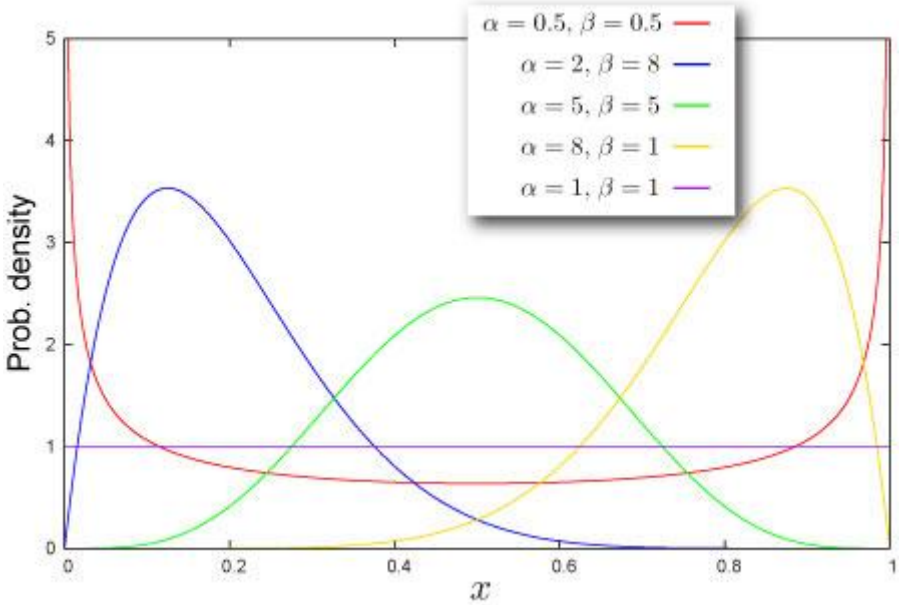
```
function [fraud]=attack(x)

pd = makedist('Beta','a',1,'b',3);
b=random(pd,1,1);

fraud=b.*x;
end
```

Στην παραπάνω συνάρτηση ο παράγοντας αλλοίωσης κάθε ωριαίας μέτρησης ακολουθεί μια κατανομή βήτα με παραμέτρους a=1 και b=3. Θα μπορούσε να προέρχεται από μια κανονική κατανομή, όπως `b=random('Normal',0.35,0.15,1,1)`.

Στο σημείο αυτό αξίζει να γίνει μια περιγραφή των κατανομών που χρησιμοποιήθηκαν:

- <u>Κατανομή Βήτα (Beta Distribution)</u>

Την κατανομή Βήτα εισήγαγε για πρώτη φορά ο Leonhard Euler. Έχει δύο θετικές παραμέτρους (α,b), και η συνάρτηση πυκνότητας πιθανότητάς της μπορεί να έχει ποικιλία μορφών ανάλογα με την επιλογή των τιμών των παραμέτρων, όπως φαίνεται στο ακόλουθο σχήμα:



Σχήμα 3.4 : Παραδείγματα διαφόρων περιπτώσεων κατανομής Βήτα[51]

Η κατανομή beta ορίζεται ως εξής:

$$B(a, b)=\int_0^1 u^{a-1}(1-u)^{b-1}du \text{ , } \alpha>0, b>0$$

Η συνάρτηση beta ορίζεται και ως $B(\alpha,b)<\infty$ για κάθε $\alpha>0$ και $b>0$.

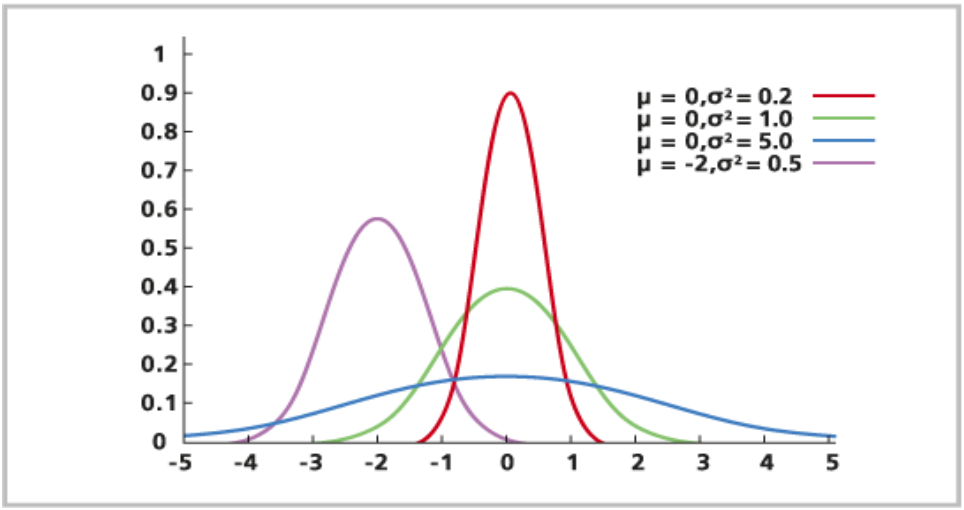
- <u>Κανονική Κατανομή (Normal Distribution)</u>

Η κανονική κατανομή (γνωστή και ως *Γκαουσιανή κατανομή*) αναφέρεται σε συνεχείς μεταβλητές αποτελώντας μία συνεχή συνάρτηση πυκνότητας πιθανότητας. Χρησιμοποιείται ως μία πρώτη προσέγγιση για να περιγραφούν τυχαίες μεταβλητές πραγματικών τιμών, οι οποίες τείνουν να συγκεντρώνονται γύρω από μια μέση τιμή. Η κανονική κατανομή αποτελεί την πιο σημαντική κατανομή της στατιστικής μεθοδολογίας.

Η γραφική παράσταση της σχετιζόμενης συνάρτησης πυκνότητας πιθανότητας έχει σχήμα "καμπάνας", και είναι γνωστή επίσης και ως κωδωνοειδής καμπύλη. Ορίζεται από τον τύπο:

$$f(x)=\frac{1}{\sqrt{2\pi\sigma^2}}e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

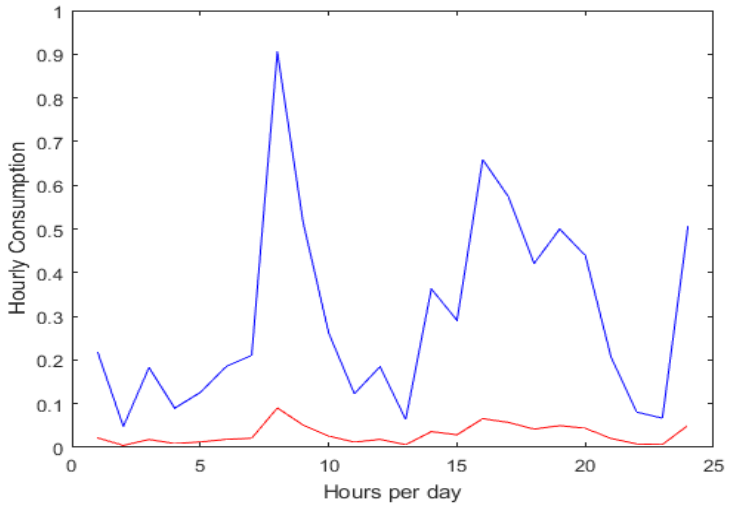
Παραδείγματα κανονικής κατανομής ανάλογα της επιλογής της μέσης τιμής και τυπικής απόκλισης απεικονίζονται στο Σχήμα 3.5 :



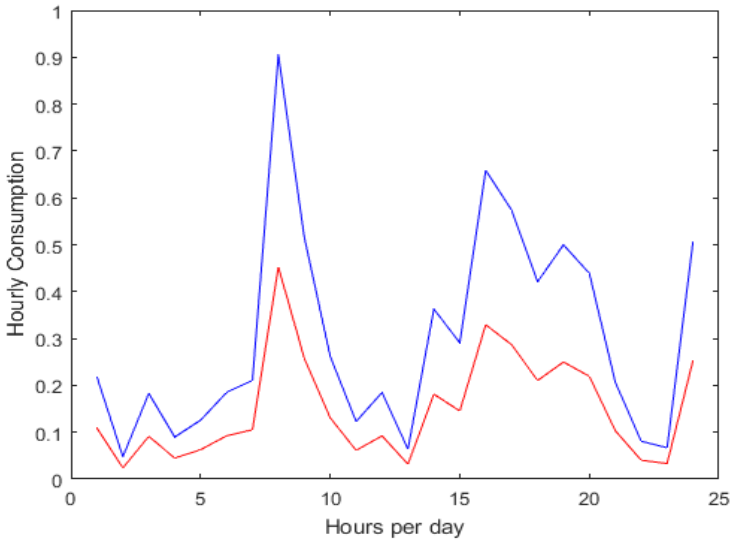
Σχήμα 3.5 : Παραδείγματα διαφόρων περιπτώσεων κανονικής κατανομής[53]

Στην εργασία, μερικές από τις περιπτώσεις απάτης, που μελετήθηκαν, αφορούσαν την εφαρμογή απάτης στις μισές μέρες του πίνακα κάθε καταναλωτή με κλοπή στο 90%

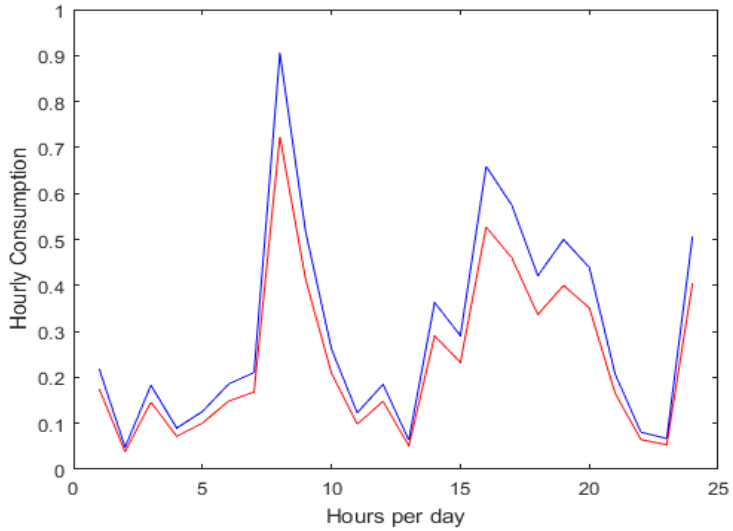
των δεδομένων (παράγοντας αλλοίωσης=0.1), με κλοπή στο 50% και 20% και χρονική διάρκεια 24 ώρες, όπως απεικονίζεται παρακάτω για μια τυπική μέρα καταναλωτή.



Σχήμα 3.6: Προσομοίωση απάτης της τάξης του 90% στα δεδομένα (το μπλε γράφημα είναι η αρχική και το κόκκινο είναι η τελική με εφαρμογή απάτης)



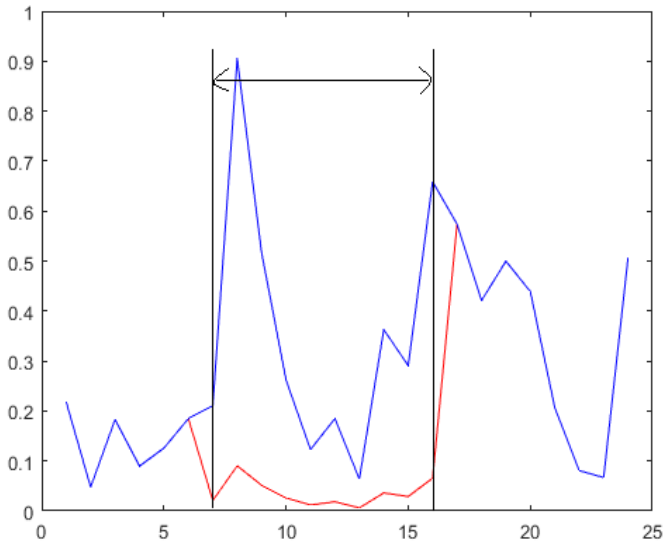
Σχήμα 3.7 : Προσομοίωση απάτης της τάξης του 50% στα δεδομένα (το μπλε γράφημα είναι η αρχική και το κόκκινο είναι η τελική με εφαρμογή απάτης)



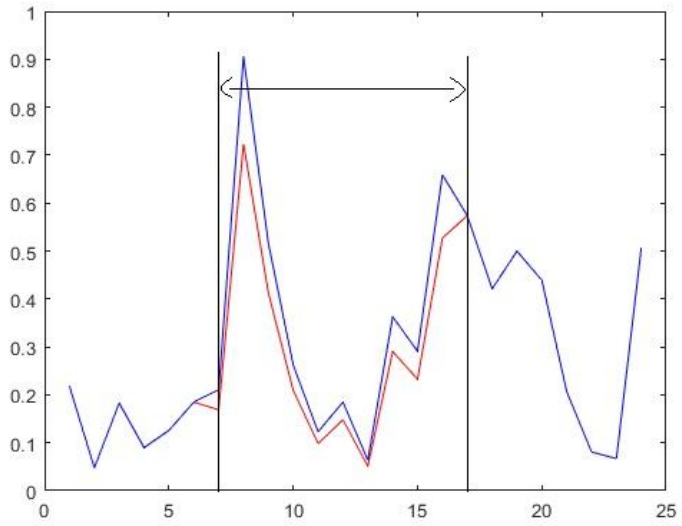
Σχήμα 3.8: Προσομοίωση απάτης της τάξης του 20% στα δεδομένα (το μπλε γράφημα είναι η αρχική και το κόκκινο είναι η τελική με εφαρμογή απάτης)

Όπως διακρίνεται και από τα παραπάνω διαγράμματα με κλοπή 20% (παράγοντας αλλοίωσης=0.8), η διαφορά με τις αρχικές μετρήσεις είναι πολύ μικρή.

Για απάτη στο 90% και 20% των δεδομένων για 10 ώρες μέσα στην ημέρα φαίνονται παρακάτω τα διαγράμματα μιας τυπικής μέρας κατανάλωσης.



Σχήμα 3.9: Προσομοίωση απάτης της τάξης του 90% στα δεδομένα για 10 ώρες (το μπλε γράφημα είναι η αρχική και το κόκκινο είναι η τελική με εφαρμογή απάτης)



Σχήμα 3.10: Προσομοίωση απάτης της τάξης του 20% στα δεδομένα για 10 ώρες (το μπλε γράφημα είναι η αρχική και το κόκκινο είναι η τελική με εφαρμογή απάτης)

3.3.3 Διαμόρφωση εισόδου SVM

Σε κάθε ημερήσιο διάνυσμα που προσομοιώνεται απάτη, η στήλη-στόχος του πίνακα εισόδου παίρνει τιμή «1». Οι υπόλοιπες, αναλλοίωτες ημέρες έχουν τιμή «0». Έτσι, η θετική τάξη προς ταξινόμηση είναι η «1» για περιπτώσεις απάτης και η αρνητική τάξη «0» για περιπτώσεις χωρίς απάτη. Ο πίνακας εισόδου στο SVM αποτελείται από μετρήσεις κάθε καταναλωτή για ενάμιση χρόνο (535 μέρες) και ανά μία ώρα. Αυτός είναι ο πίνακας εισόδου στις περισσότερες δοκιμές, και ακολούθως, εφαρμόζεται απάτη στο 50% του συνόλου των ημερών, ώστε ο ταξινομητής να εκπαιδεύεται με ισομερή σύνολα ημερών θετικής και αρνητικής τάξης. Αυτό βοηθάει στη μετέπειτα δοκιμή νέων δεδομένων προς ταξινόμηση. Η επιλογή του 50% των δεδομένων έγινε μέσω ειδικής συνάρτησης για δειγματοληπτική τυχαία επιλογή ημερών από τον πίνακα. Επίσης, η κατασκευή πινάκων σε αυτή τη μορφή χρησιμοποιείται για περιπτώσεις εφαρμογής απάτης με ένα συγκεκριμένο παράγοντα αλλοίωσης.

Στις περιπτώσεις δοκιμών με συνδυασμό επιθέσεων (παραγόντων αλλοίωσης), δηλαδή μισές μέρες με έντονη επίθεση και οι υπόλοιπες με ασθενέστερη επίθεση, η διαμόρφωση της εισόδου στο SVM για τον κάθε καταναλωτή γίνεται διαφορετικά. Για κάθε τύπο επίθεσης παράγονται 535 δείγματα, δηλαδή τα δείγματα προς ταξινόμηση του πίνακα κάθε καταναλωτή. Άρα, στην πρώτη περίπτωση, δηλαδή επίθεση στο 90% των δεδομένων, παράγεται πίνακας διαστάσεων 535 επί 24, στον οποίο έχει εφαρμοστεί απάτη στις μισές ημέρες και οι υπόλοιπες έχουν παραμείνει γνήσιες. Στην δεύτερη περίπτωση επίθεσης, δηλαδή κλοπή στο 50% των δεδομένων, παράγεται πάλι ο αρχικός πίνακας των 535 δειγμάτων, στον οποίο εφαρμόζεται η επίθεση στις μισές μέρες, όμως με επιλογή των ημερών, τέτοια ώστε η επίθεση να

εφαρμόζεται στις ημέρες που παρέμειναν γνήσιες στην πρώτη περίπτωση. Τέλος, αυτοί οι δύο πίνακες συγχωνεύτηκαν, έτσι το τελικό σύνολο δεδομένων κάθε καταναλωτή περιελάμβανε 1070 δείγματα προς ταξινόμηση. Στην ουσία, αυτά τα δείγματα περιέχουν τα ημερήσια διανύσματα κάθε καταναλωτή για έναν χρόνο απαραβίαστα, και τα ίδια με εφαρμογή απάτης και μάλιστα, μισές μέρες με έντονη επίθεση και οι υπόλοιπες με ήπια. Αυτό συμβαίνει διότι, για την καλύτερη εκπαίδευση του SVM, το δείγμα εκπαίδευσης πρέπει να περιέχει ίσα σύνολα δεδομένων από τις δύο τάξεις προς ταξινόμηση. Επομένως, στη συνέχεια, εφαρμόστηκε διαχωρισμός σε training και test δείγματα για την εκπαίδευση και δοκιμή του αλγορίθμου.

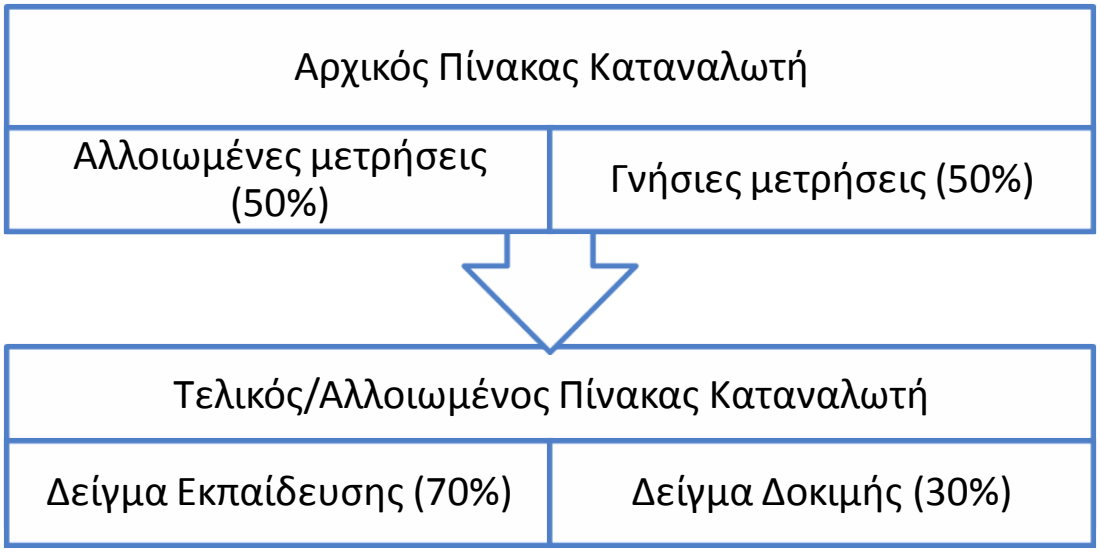
Ύστερα, αναλύθηκαν οι περιπτώσεις, όπου το δείγμα εκπαίδευσης είχε διαφορετική επίθεση από το δείγμα δοκιμής. Συγκεκριμένα, όπως συνέβη στην άνωθεν διαδικασία, έτσι και το δείγμα εκπαίδευσης αποτελούνταν από τον διπλασιασμένο πίνακα με συνδυασμό επιθέσεων ενώ το δείγμα δοκιμής είχε τον αρχικό πίνακα με εφαρμογή διαφορετικού τύπου επίθεσης. Στην ουσία, ο αλγόριθμος εκπαιδεύτηκε με διαφορετικές επιθέσεις και δοκιμάστηκε με άλλες. Αρχικά, η εκπαίδευση έγινε για επιθέσεις της τάξης του 90% και 50% των δεδομένων (1070×24), ενώ η δοκιμή έγινε για επίθεση της τάξης του 20% των δεδομένων (535×24). Ύστερα, έγινε η αντίστροφη διαδικασία, δηλαδή εκπαίδευση με ήπιες επιθέσεις της τάξης του 20% και 50%, ενώ η δοκιμή έγινε με έντονη απάτη.

Στην τελευταία δοκιμή της πειραματικής διαδικασίας, γίνεται ανάλυση με βάση ωριαίες μετρήσεις, δίωρες ή τετράωρες. Μέχρι τώρα γίνεται η ανάλυση για ωριαίες μετρήσεις μέσα στη μέρα. Έτσι, δοκιμάζεται ένα ρεαλιστικό σενάριο, με το οποίο εφαρμόζεται επίθεση σε κάθε καταναλωτή, όπου ο παράγοντα αλλοίωσης του καθενός προέρχεται από μια κατανομή beta και τιμές κοντά στο 0.2(έντονη επίθεση). Η διάρκεια επίθεσης στον κάθε καταναλωτή είναι τυχαία, αλλά σταθερή ως προς μέρες και ώρες του και ακολούθως, εξετάζεται η περίπτωση όπου οι μέρες αντιπροσωπεύονται από δίωρα άρα πίνακες 535×12, και τετράωρα 535×6. Ας σημειωθεί, ότι στους τελικούς πίνακες προστίθεται και η επιπλέον στήλη για είσοδο στο SVM, η στήλη που ορίζεται στόχος για την έξοδο.

Οι δοκιμές έγιναν με ίδια δειγματοληψία ως προς τις μέρες επίθεσης σε κάθε καταναλωτή, καθώς και ως προς τον διαχωρισμό ημερών για εκπαίδευση και δοκιμή του ταξινομητή. Το γεγονός αυτό βοήθησε, ώστε να συγκριθούν καλύτερα οι διάφορες περιπτώσεις, ιδίως όταν γίνεται ανάλυση ως προς το χρόνο επίθεσης κατά τη διάρκεια μιας μέρας. Το ίδιο ισχύει στην περίπτωση συνδυασμού επιθέσεων, στην οποία είναι αναγκαία η γνώση των ημερών με την πρώτη τάξη επίθεσης και εκείνων με τη δεύτερη.

Αφού έγινε αυτή η διαμόρφωση των πινάκων, τα δεδομένα χωρίστηκαν, έτσι ώστε το 70% να χρησιμοποιηθεί για δείγμα εκπαίδευσης και το 30% για δείγμα δοκιμής του ταξινομητή. Στο παρακάτω διάγραμμα ροής απεικονίζονται τα στάδια, κατά τα οποία έγινε η δειγματοληπτική επιλογή των ημερών για προσομοίωση

απάτης και ύστερα για διαχωρισμό των δεδομένων εκπαίδευσης και δοκιμής του αλγορίθμου ταξινόμησης.



Σχήμα 3.11 : Απεικόνιση διαχωρισμού και στάδια δειγματοληπτικής επιλογής ημερών

3.3.4 Διαμόρφωση εισόδου SVM με εξαγωγή χαρακτηριστικών

Κλασσικές τεχνικές ταξινόμησης όπως είναι τα τεχνητά νευρωνικά δίκτυα (Artificial Neural Networks, ANN) και τα Δέντρα Αποφάσεων, κάνουν ταξινόμηση με βάση δείγματα χαρακτηριστικών[54]. Αντιστοίχως, οι τεχνικές ταξινόμησης, που βασίζονται σε χρονοσειρές με βάση χαρακτηριστικά, δουλεύουν με την μετατροπή της ακολουθίας δεδομένων σε δείγμα χαρακτηριστικών, πριν την εφαρμογή του ταξινομητή. Η επιλογή των κατάλληλων χαρακτηριστικών είναι το πιο δύσκολο κομμάτι της ανάλυσης, είτε γίνεται χειροκίνητα είτε με κάποια τεχνική εξαγωγής κατάλληλων χαρακτηριστικών, όπως η ανάλυση κύριων συνιστωσών (Principal Component Analysis, PCA). Με αυτό τον τρόπο, παράγονται πληροφοριακές ομάδες για τον ταξινομητή.

Είναι γεγονός, ότι ένα πρόβλημα που εμφανίζεται σε αρκετές εφαρμογές μηχανικής μάθησης είναι ο μεγάλος αριθμός χαρακτηριστικών που θεωρούνται σχετικά με την προς προσέγγιση συνάρτηση-στόχο. Καθοριστική σημασία στην ποιότητα της εκπαίδευσης έχει η επιλογή κατάλληλων χαρακτηριστικών, τα οποία θα συστήσουν το χώρο του προβλήματος, καθώς μέσω αυτών καθίσταται δυνατή η αναπαράσταση της γνώσης που απαιτείται, για την αποδοτική λειτουργία του συστήματος. Δύο είναι οι βασικοί λόγοι για τους οποίους η μεγάλη διαστασιμότητα

αποτελεί πρόβλημα. Ο πρώτος λόγος είναι η αναπόφευκτη αύξηση της υπολογιστικής πολυπλοκότητας για την εκπαίδευση και τη λειτουργία του ταξινομητή, ακόμη και αν κάποιες φορές αυτό μπορεί να συνεπάγεται παράλληλη αύξηση της ακρίβειας του προκύπτοντος ταξινομητή. Ο δεύτερος λόγος αφορά το γεγονός ότι, όσο περισσότερα είναι τα χαρακτηριστικά, τόσο μεγαλύτερη η πιθανότητα να αναγνωριστούν λανθασμένα πολλά από αυτά ως ουσιώδη για τον προσδιορισμό της τιμής της συνάρτησης-στόχου, ενώ στην πραγματικότητα αποτελούν συμπτωματικά καλούς προσδιοριστές για το συγκεκριμένο διαθέσιμο σύνολο στιγμιότυπων εκπαίδευσης.

Είναι ενδιαφέρουσα η ανακάλυψη συστάδων που περιγράφουν διαφορετικού τύπου απαιτήσεις αιχμής ζήτησης, μεγάλης μεταβλητότητας και εποχικών διακυμάνσεων στα δεδομένα. Για να μειωθεί η διάσταση γίνεται ταξινόμηση με έναν περιορισμένο αριθμό χαρακτηριστικών. Διακρίνονται τέσσερις βασικές χρονικές περίοδοι στις οποίες θα πρέπει να αναλυθούν τα δεδομένα. Το γεγονός αυτό, επιτρέπει να γίνει μια μικρότερη χρονική ανάλυση με βάση τα δεδομένα έξυπνων μετρητών, ούτως ώστε να περιγραφεί καλύτερα η συμπεριφορά αιχμής κατανάλωσης του καταναλωτή[53].

Πρώτη σημαντική ενέργεια που πρέπει να γίνει για την εξαγωγή χαρακτηριστικών, είναι η κανονικοποίηση των δεδομένων/χαρακτηριστικών τα οποία περιγράφουν την ενδοημερήσια ζήτηση. Διαφορετικά, είναι πιθανό οι τελικές συστάδες απλώς να περιγράφουν τη μέση τιμή της ζήτησης και όχι τη διανομή της ζήτησης κατά τη διάρκεια της ημέρας. Δεύτερον, η ευρεία εξάπλωση της κανονικοποιημένης τυπικής απόκλισης, όταν περιγράφονται χαρακτηριστικά μέσων όρων, σημαίνει την εισαγωγή ενός μέτρου μεταβλητότητας, με σκοπό να γίνει πληρέστερη κατανόηση της συμπεριφοράς στη ζήτηση. Η έλλειψη ενός τέτοιου μέτρου, περιορίζει την κατανόηση μιας αντιπροσωπευτικής μέσης τιμής για την κάθε μέρα[53].

Εξαιτίας της φυσικής μεταβλητότητας των πελατών σε κάθε κατοικία, είναι σημαντικό να ερευνηθεί η μοντελοποίηση της αιχμής ζήτησης. Για πολλούς καταναλωτές (τουλάχιστον 2700), μια μεγάλη αιχμή ζήτησης είναι 5kWh κατά την διάρκεια κάθε ημιώρου, και συμβαίνει τουλάχιστον μία φορά κατά την διάρκεια του χρόνου, αλλά για λιγότερο από 5% σε όλα τα ημίωρα των δεδομένων. Επιπλέον, οι μετρήσεις κατανέμονται ανάλογα με τις εποχές(οι εποχές προσδιορίζονται από το πρότυπο ισημερίας και τις ημερομηνίες ηλιοστάσιου για την Ιρλανδία) και συμπεραίνεται ότι διαφορετικό μέγεθος αιχμών καταγράφεται σε διαφορετικές ώρες της μέρας, ανάλογα με την εποχή. Είναι πολύ σημαντικό και ενδιαφέρον θέμα η κατανόηση της ύπαρξης των συχνών, καθημερινών αιχμών ζήτησης[53].

Οι τέσσερις χρονικές περίοδοι που διακρίνονται ανάλογα των «τοπικών ελαχίστων» και των ωρών αιχμής είναι όπως ακολούθως:

1. *Χρονική Περίοδος1* :11.00 π.μ – 6.00 μ.μ—Η βραδυνή περίοδος
2. *Χρονική Περίοδος2:* 7.00 -9.00 π.μ –Η πρωινή περίοδος
3. *Χρονική Περίοδος3:* 9.00π.μ – 15.00 μ.μ – Η μεσημεριανή περίοδος
4. *Χρονική Περίοδος4:* 16.00 μ.μ – 10.00μ.μ – Η απογευματινή περίοδος

Όπως ήταν αναμενόμενο, τα επιλεγμένα χρονικά διαστήματα συμπίπτουν με τις τυπικές περιόδους δραστηριότητας ενός νοικοκυριού. Αυτές οι χρονικές περίοδοι βοηθούν στη μείωση της διάστασης των χαρακτηριστικών.

Για τον προσδιορισμό των χαρακτηριστικών εισάγονται κάποιοι συμβολισμοί. Για έναν συγκεκριμένο καταναλωτή, ορίζεται η μέση ενέργεια P_i, i=1,2,3,4 κατά τη διάρκεια όλης της ημέρας για τις τέσσερις περιόδους και με την αντίστοιχη τυπική απόκλιση σ_i. Η $\hat{P}$ είναι η μέση ημερήσια ενέργεια του καταναλωτή. Αντιστοίχως, προκύπτουν τα ακόλουθα χαρακτηριστικά για κάθε καταναλωτή:

- Η σχετική μέση ισχύς για κάθε χρονική περίοδο P_i^R=$P_i/\hat{P}$, i=1, 2, 3, 4
- Η μέση σχετική τυπική απόκλιση και δίνεται από τον τύπο $\hat{\sigma} = (1/4)\sum_{i=1}^{4}\sigma_i/P_i$

Καθώς επίσης, και τα εξής χαρακτηριστικά:

- Η αιχμή της ημέρας και το άθροισμα της ημερήσιας κατανάλωσης, καθώς και
- Οι δείκτες ασυμμετρίας (skewness) και κύρτωσης (kurtosis), οι οποίοι ορίζονται ως εξής:

$$SKEW=\frac{\sum_{t=1}^{n}(y(t)-\mu)^3}{n\sigma^3}$$

$$KURT=\frac{\sum_{t=1}^{n}(y(t)-\mu)^4}{n\sigma^4}-3$$

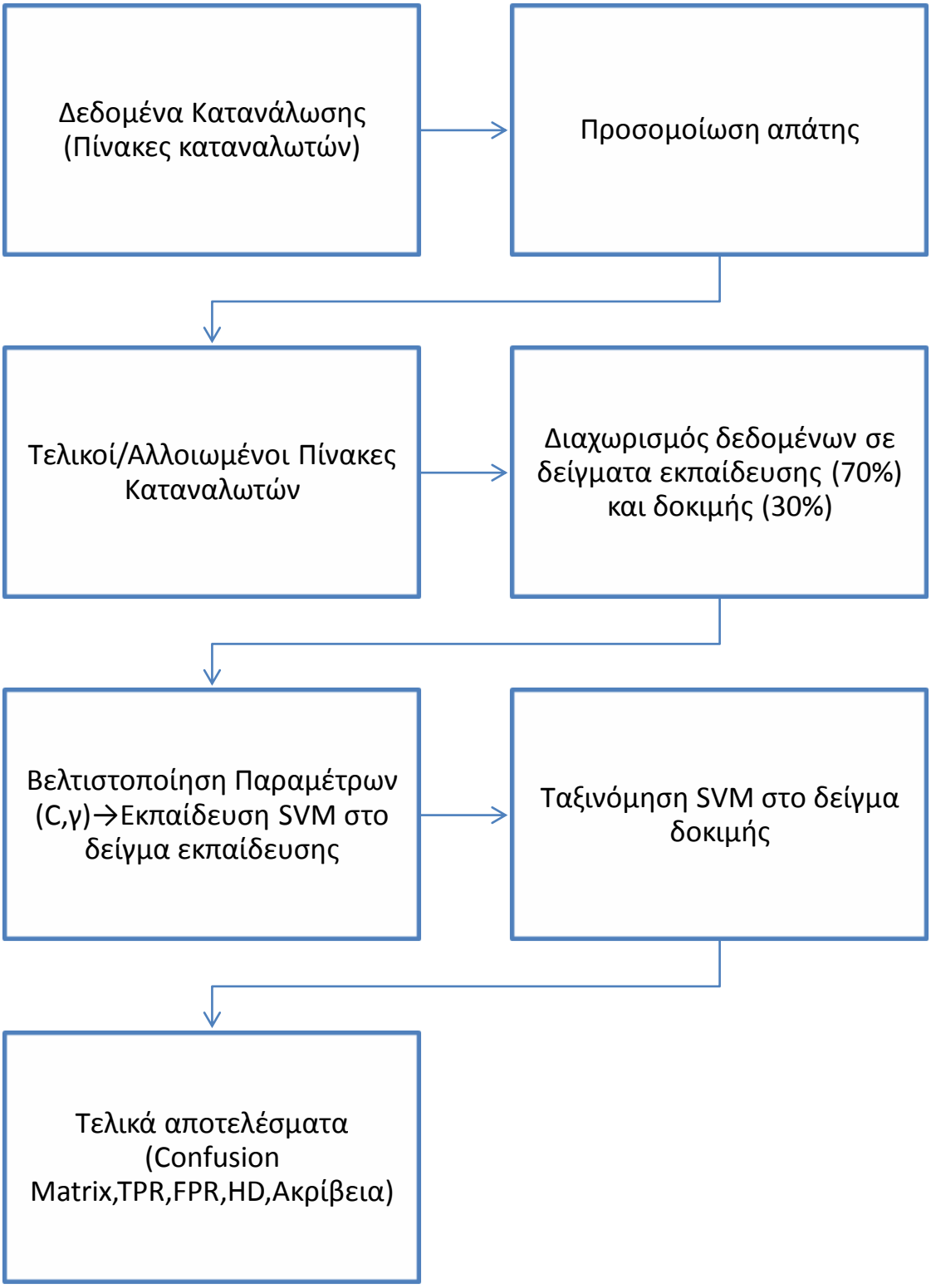
Το αποτέλεσμα όσων αναφέρθηκαν αφορούν τον σχηματισμό πινάκων για κάθε καταναλωτή, οι οποίοι βρίσκονται σε μορφή διαστάσεων μέρες επί χαρακτηριστικά και συγκεκριμένα των εννέα προαναφερθέντων χαρακτηριστικών. Αφού εξαχθούν τα χαρακτηριστικά, προστίθεται η στήλη-στόχος στον κάθε πίνακα με τιμές 1,0 και ακολουθεί ο διαχωρισμός των δειγμάτων εκπαίδευσης και δοκιμής, όπως αναλύθηκε παραπάνω, για την διαδικασία της ταξινόμησης.

3.3.5 Εξαγωγή Αποτελεσμάτων

Το τελικό στάδιο αποτελείται από την αξιολόγηση της απόδοσης του ταξινομητή με SVM. Στόχος είναι, να καταφέρει ο ταξινομητής κατάλληλο διαχωρισμό των ημερών. Σε αυτό, παίζει σημαντικό ρόλο η ένταση της επίθεσης και ο κάθε καταναλωτής. Στο μεγάλο σύνολο των καταναλωτών διακρίνονται κάποιοι καταναλωτές, οι οποίοι παρουσιάζουν διαφορετικό προφίλ φορτίου από το προσδοκώμενο. Για παράδειγμα, εμφανίζονται με μηδενικές μετρήσεις για πάνω από μισό χρόνο, το οποίο είναι αποτέλεσμα πολλών παραγόντων, όπως αλλαγή της κατοικίας, συσκευών κατανάλωσης, κ.α. Αυτού του είδους οι καταναλωτές δεν διαγράφονται από το σύνολο, αλλά κατανέμονται σε ειδική κατηγορία για περαιτέρω ανάλυση.

Εν κατακλείδι, υπολογίζονται από τους πίνακες σύγχυσης (confusion matrices) τα αποτελέσματα των δεικτών FPR (False Positive Rate),δηλαδή ο δείκτης των ημερών χωρίς απάτη που λανθασμένα χαρακτηρίστηκαν με απάτη, το TPR(True Positive Rate), δηλαδή ο δείκτης των ημερών με απάτη που σωστά ταξινομήθηκαν με απάτη, η ακρίβεια του ταξινομητή, η διαφορά TPR-FPR, δηλαδή το Highest Difference και το μέτρο ακρίβειας F1 Score. Η λεπτομερής περιγραφή των δεικτών γίνεται στο Κεφάλαιο 2.

Παρακάτω, απεικονίζεται η ροή της διαδικασίας υλοποίησης των μετρήσεων και της κατασκευής του κώδικα.



Σχήμα 3.12 : Διάγραμμα ροής της πειραματικής διαδικασίας

Κεφάλαιο
4
Αποτελέσματα εφαρμογής αλγόριθμου Μηχανών Διανυσμάτων Υποστήριξης (SVM) για ανίχνευση απάτης

4.1 Εισαγωγή

Στο παρόν κεφάλαιο γίνεται ανάλυση των αποτελεσμάτων του αλγόριθμου ανίχνευσης κλοπών ενέργειας με χρήση των μηχανών διανυσμάτων υποστήριξης. Οι περιπτώσεις αφορούν την ένταση της επίθεσης, την διάρκεια της επίθεσης και την εισαγωγή χαρακτηριστικών. Επιπλέον περίπτωση είναι η εκπαίδευση του αλγόριθμου με διαφορετικό δείγμα εκπαίδευσης ως προς την επίθεση, σε σχέση με το δείγμα δοκιμής. Τα ιστορικά δεδομένα κατανάλωσης, τα οποία ήταν διαθέσιμα, αναλύονται στο τρίτο κεφάλαιο. Πλέον, με τον κατάλληλο μετασχηματισμό τους για είσοδο του SVM θα εξεταστούν τα αντίστοιχα αποτελέσματα.

Η εκτέλεση των δοκιμών πραγματοποιήθηκε σε φορητό υπολογιστή με τα εξής χαρακτηριστικά:

- Επεξεργαστής : Intel® Core™ 2 Duo
- Μνήμη RAM : 4 GB
- Λειτουργικό Σύστημα : Windows 7 Professional, 64-bit
- Πρόγραμμα υλοποίησης δοκιμών: MATLAB έκδοση 8.6.0.267246-R2015b (win64-64bit)

Ακολουθείται η μελέτη κάθε περίπτωσης επίθεσης ξεχωριστά με την εξαγωγή των αποτελεσμάτων και την απεικόνιση της σε πίνακες. Συγκεκριμένα, οι δείκτες, που βοηθούν στην εξαγωγή συμπερασμάτων για την απόδοση του αλγορίθμου, είναι: η ακρίβεια του αλγόριθμου(accuracy), ο δείκτης των ψευδώς θετικών ενδείξεων για απάτη (FPR), ο δείκτης των αληθώς θετικών ενδείξεων απάτης (TPR), το F1-Score, και το Highest Difference (HD), δηλαδή η διαφορά TPR και FPR. Επιπλέον, παρουσιάζεται ο αθροιστικός πίνακας σύγχυσης (confusion matrix) της κάθε περίπτωσης. Τα αποτελέσματα στους πίνακες των δεικτών αφορούν τα κατά μέσο όρο από το σύνολο των 1000 καταναλωτών, για τους οποίους έγινε η ανάλυση. Από τους 1000 καταναλωτές αφαιρέθηκαν εκείνοι, οι οποίοι παρουσίαζαν μειωμένες μετρήσεις, λιγότερες του ενάμιση χρόνου Τέλος, γίνεται ανάλυση στο αρχικό σύνολο δεδομένων των 5000 καταναλωτών.

4.2 *Μελέτη μεταβλητότητας της έντασης της επίθεσης*

Σε αυτή τη παράγραφο, παρουσιάζεται η ανάλυση περιπτώσεων απάτης με διαφορετική ένταση, δηλαδή απάτη στο 90%, 50% και το 20% των δεδομένων. Επιπλέον, εξετάζονται οι ώρες επίθεσης κατά τη διάρκεια της ημέρας για κάθε περίπτωση. Τέλος, εξετάζονται περιπτώσεις στις οποίες ο βαθμός αλλοίωσης των δεδομένων ακολούθησε κατανομές, όπως βήτα (beta), κανονική (normal) και τυχαία (random).

4.2.1 Περίπτωση έντονης επίθεσης, της τάξης του 90% των δεδομένων

Σε αυτήν την περίπτωση, ο παράγοντας αλλοίωσης των δεδομένων κάθε μέρα είναι ίσος με 0.1. Αυτό αντιπροσωπεύει μια έντονη επίθεση, δηλαδή εφαρμογή κλοπής στο 90% των μετρήσεων κατανάλωσης. Επιπλέον, αναλύεται η εφαρμογή αυτού το τύπου επίθεσης σε διαφορετικές ώρες. Συγκεκριμένα, οι ώρες, που επιλέχθηκαν, ήταν: 10 ώρες της ημέρας, ένα τυχαίο διάστημα 10 έως 24 ωρών και 24 ώρες. Τα αποτελέσματα φαίνονται στον Πίνακα 4.1 :

Πίνακας 4.1 : Αποτελέσματα ταξινόμησης απάτης του 90% των δεδομένων

Ώρες/ημέρα	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
10 ώρες	87,13	15,96	90,37	87,74	74,41
10-24 ώρες	92,30	8,54	93,22	92,56	84,68
24 ώρες	97,48	4,74	99,72	97,73	94,98

Ακολούθως, φαίνονται οι αθροιστικοί πίνακες σύγχυσης και απεικονίζονται τα αθροιστικά ποσά των αληθώς αρνητικών (TN), ψευδώς θετικών (FP), ψευδώς αρνητικών (FN) και αληθώς θετικών (TP) ημερών, αντίστοιχα. Η αρνητική ένδειξη αναφέρεται σε ημέρα χωρίς απάτη και η θετική ένδειξη σε ημέρα με απάτη.

- **<u>Confusion Matrix</u>**

Πίνακας 4.2 : Confusion Matrix για απάτη 10 ωρών στο 90%

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	47972	9166
Πραγματική τάξη=1	5547	51626

Πίνακας 4.3 : Confusion Matrix για απάτη 10-24 ωρών στο 90%

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	52230	4908
Πραγματική τάξη=1	3892	53281

Πίνακας 4.4 : Confusion Matrix για απάτη 24 ωρών στο 90%

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	54415	2723
Πραγματική τάξη=1	157	57016

4.2.2 Περίπτωση μέτριας επίθεσης, της τάξης του 50% των δεδομένων

Σε αυτήν της περίπτωση επίθεσης, ο παράγοντας αλλοίωσης ήταν ίσος με 0.5, δηλαδή, οι μετρήσεις της ημέρας, που γίνεται επίθεση, μειώνονται κατά 50%. Ομοίως, μελετήθηκαν οι περιπτώσεις επίθεσης για 10 , 10-24 και 24 ώρες μέσα στην ημέρα. Οπότε, τα αποτελέσματα ήταν τα εξής:

Πίνακας 4.5 : Αποτελέσματα ταξινόμησης απάτης του 50% των δεδομένων

Ώρες/ημέρα	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
10 ώρες	69,95	34,27	74,62	71,11	40,35
10-24 ώρες	79,48	23,04	82,14	79,95	59,1
24 ώρες	88,06	16,07	92,39	88,66	76,32

Ακολούθως, φαίνονται οι αθροιστικοί πίνακες σύγχυσης και απεικονίζονται τα αθροιστικά ποσά των αληθώς αρνητικών (TN), ψευδώς θετικών (FP), ψευδώς αρνητικών (FN) και αληθώς θετικών (TP),αντίστοιχα.

- **<u>Confusion Matrix</u>**

Πίνακας 4.6 : Confusion Matrix για απάτη 10 ωρών στο 50%

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	37415	19723
Πραγματική τάξη=1	14630	42543

Πίνακας 4.7 : Confusion Matrix για απάτη 10-24 ωρών στο 50%

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	44094	13205
Πραγματική τάξη=1	10248	46764

Πίνακας 4.8 : Confusion Matrix για απάτη 24 ωρών στο 50%

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	48198	9299
Πραγματική τάξη=1	4344	52470

4.2.3 Περίπτωση ήπιας επίθεσης, της τάξης του 20 % των δεδομένων

Σε αυτήν της περίπτωση επίθεσης ο παράγοντας αλλοίωσης ήταν ίσος με 0.8, δηλαδή οι μετρήσεις μιας ημέρας μειώνονται/αλλοιώνονται στο 20%. Ομοίως, μελετήθηκαν οι περιπτώσεις επίθεσης για 10 , 10-24 και 24 ώρες μέσα στην ημέρα. Οπότε τα αποτελέσματα ήταν τα εξής:

Πίνακας 4.9 : Αποτελέσματα ταξινόμησης απάτης του 20% των δεδομένων

Ώρες/ημέρα	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
10 ώρες	55,13	49,34	60,73	56,34	11,39
10-24 ώρες	60,78	44,19	66,34	62,39	22,15
24 ώρες	65,87	39,69	71,94	67,57	32,25

Παρακάτω φαίνονται οι αθροιστικοί πίνακες σύγχυσης και απεικονίζονται τα αθροιστικά ποσά των αληθώς αρνητικών (TN), ψευδώς θετικών (FP), ψευδώς αρνητικών (FN) και αληθώς θετικών (TP),αντίστοιχα.

- **<u>Confusion Matrix</u>**

Πίνακας 4.10 : Confusion Matrix για απάτη 10 ωρών στο 20%

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	28622	28490
Πραγματική τάξη=1	22797	34402

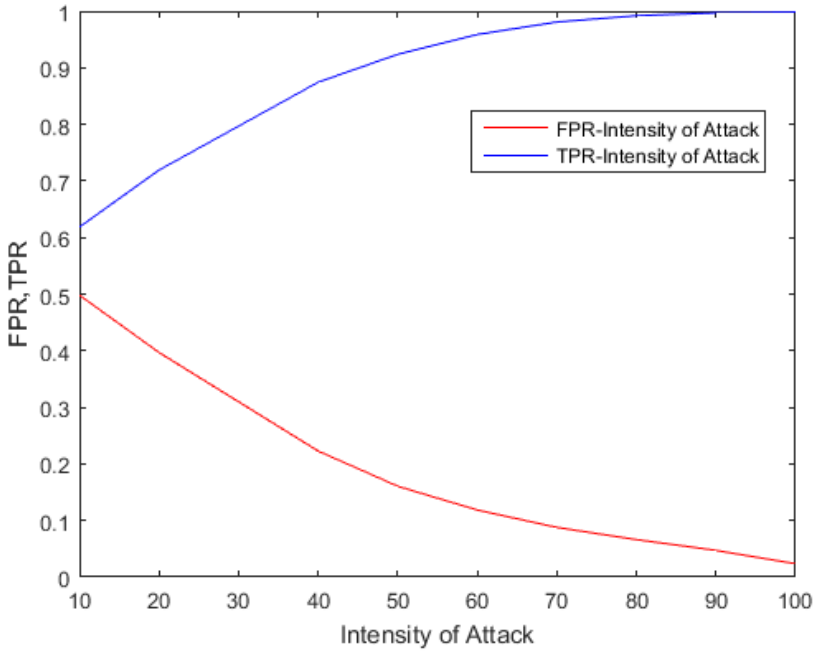
Πίνακας 4.11 : Confusion Matrix για απάτη 10-24 ωρών στο 20%

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	31641	25358
Πραγματική τάξη=1	19473	37839

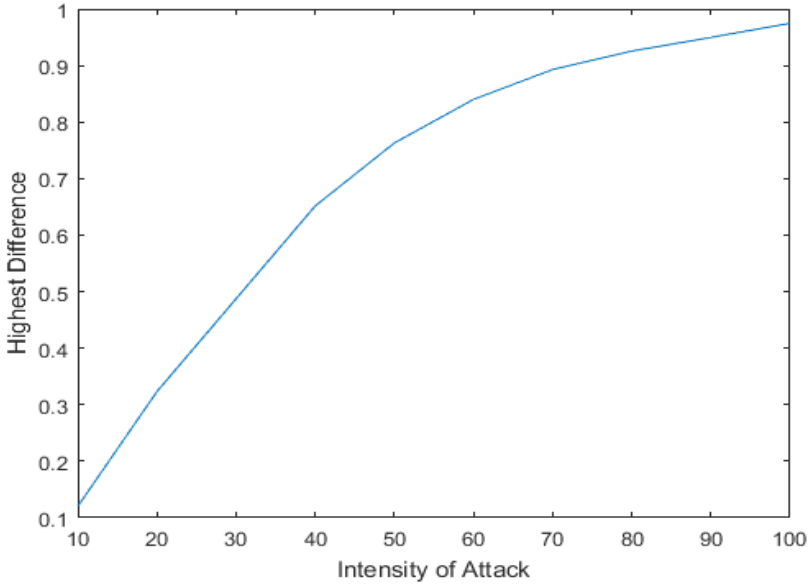
Πίνακας 4.12 : Confusion Matrix για απάτη 24 ωρών στο 20%

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	34385	22881
Πραγματική τάξη=1	16139	40906

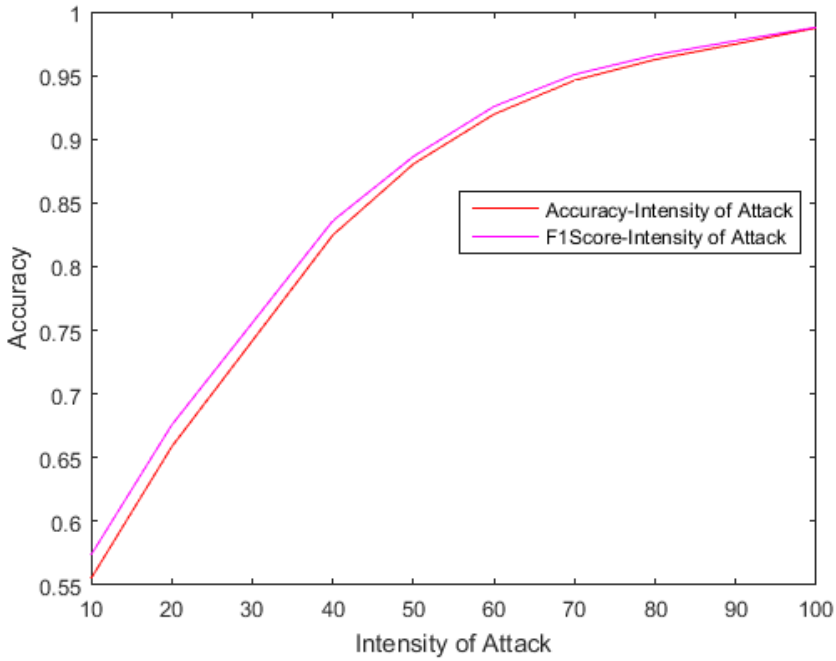
Στα παρακάτω γραφήματα απεικονίζονται οι μεταβολές του ποσοστού των ψευδώς θετικών (False Positive Rate,FPR), των αληθών θετικών (True Positive Rate,TPR), του δείκτη Highest Difference (HD) και της ακρίβειας από τον δείκτη Accuracy και F1-Score, ανάλογα με την ένταση της επίθεσης(Intensity of Attack). Η αλλοίωση των δεδομένων έγινε στο 10% έως το 100% , για όλες τις ώρες του ημερήσιου διανύσματος.



Σχήμα 4.1 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 24 ωρών



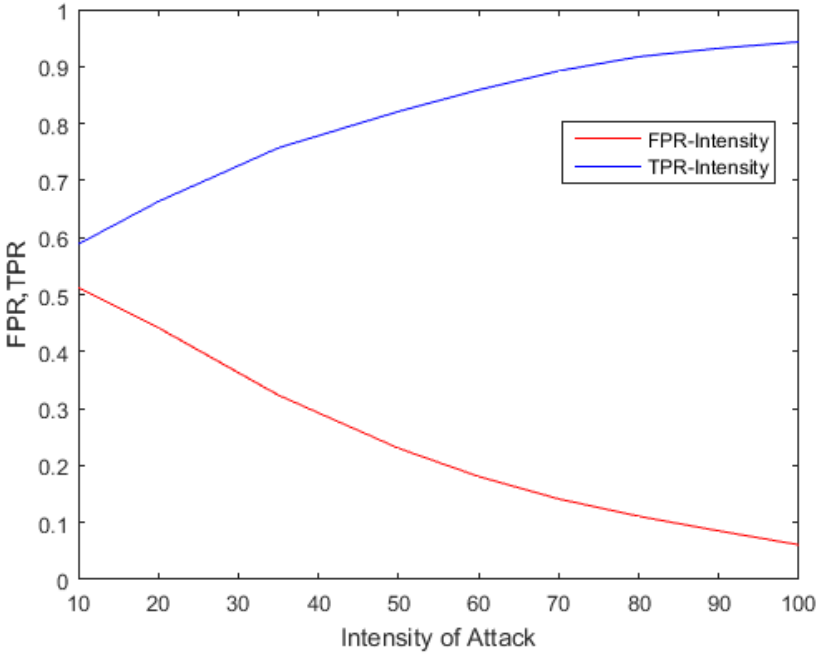
Σχήμα 4.2: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια 24 ωρών



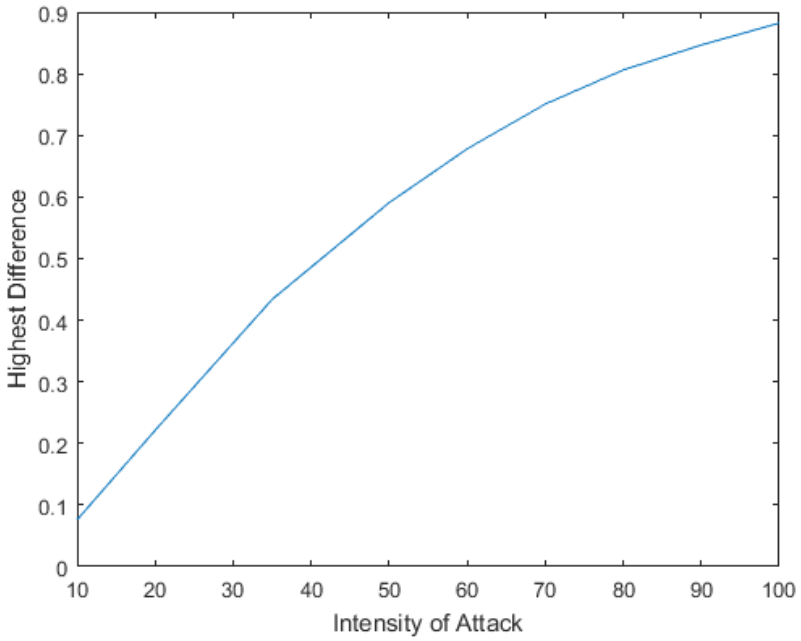
Σχήμα 4.3 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 24 ωρών

Στα παρακάτω γραφήματα απεικονίζονται οι μεταβολές του ποσοστού των ψευδώς θετικών (False Positive Rate,FPR), των αληθών θετικών (True Positive Rate,TPR), του δείκτη Highest Difference (HD) και της ακρίβειας από τον δείκτη

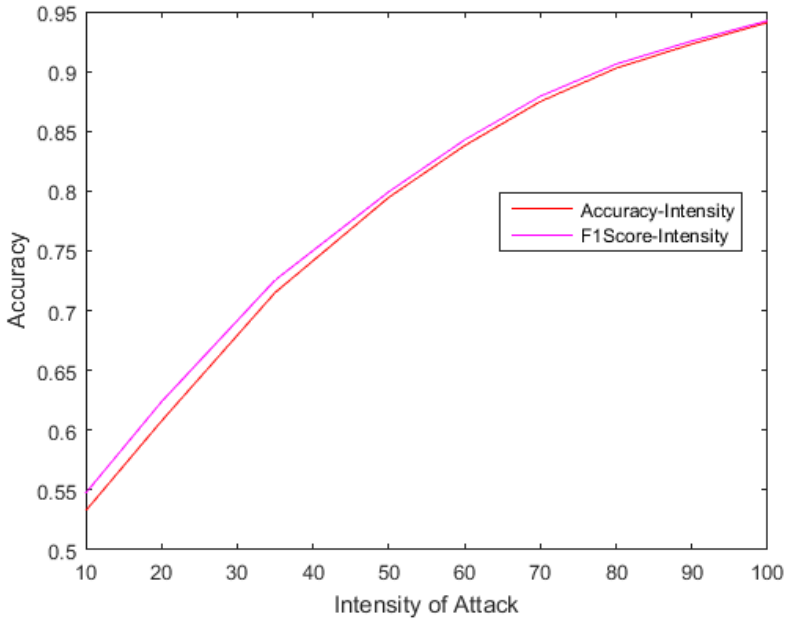
Accuracy και F1-Score, ανάλογα με την ένταση της επίθεσης (Intensity of Attack). Η αλλοίωση των δεδομένων έγινε στο 10% έως το 100% και εφαρμόστηκε σε ένα τυχαίο διάστημα ανάμεσα σε 10 και 24 ώρες.



Σχήμα 4.4 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια από 10 έως 24 ώρες

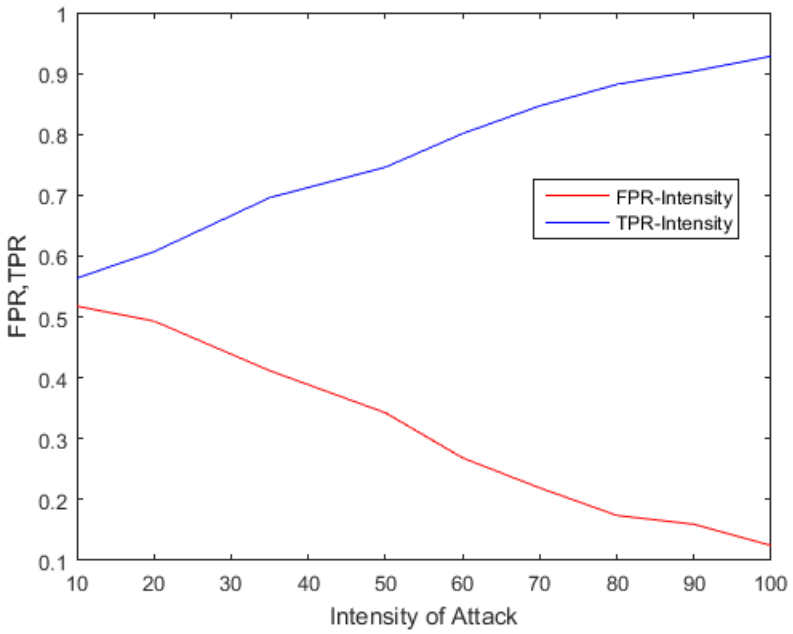


Σχήμα 4.5: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια από 10 έως 24 ώρες

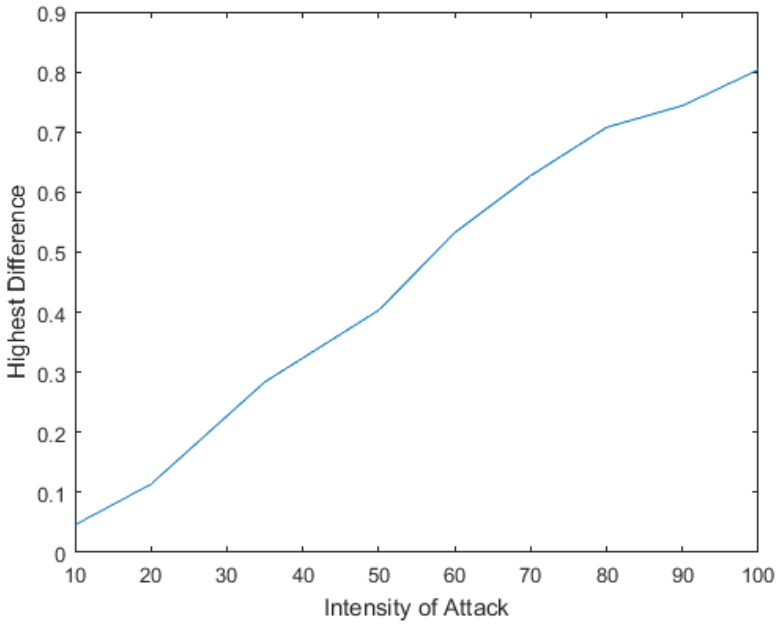


Σχήμα 4.6 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια από 10 έως 24 ώρες

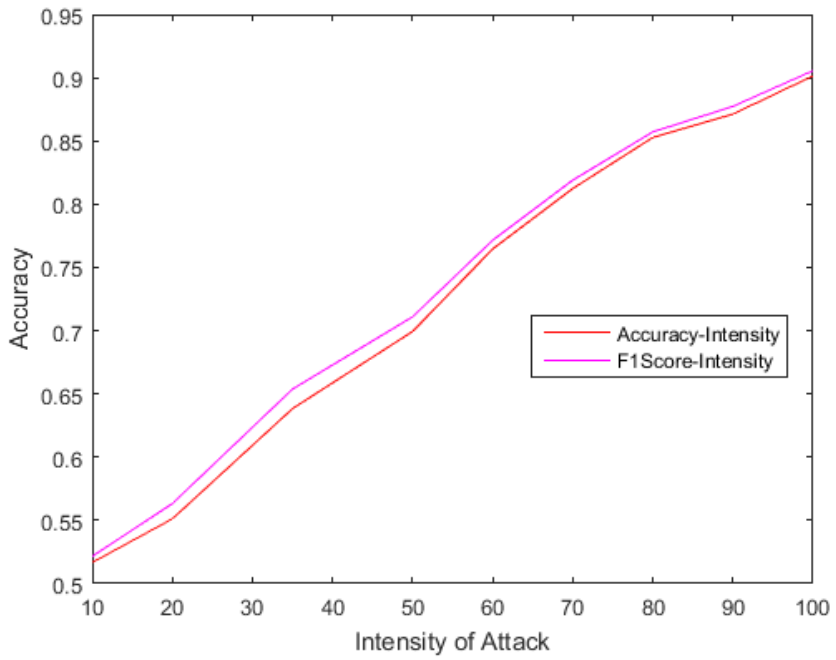
Ομοίως, ακολούθως απεικονίζονται οι μεταβολές του ποσοστού των ψευδώς θετικών (False Positive Rate,FPR), των αληθών θετικών (True Positive Rate,TPR), του δείκτη Highest Difference (HD) και της ακρίβειας από τον δείκτη Accuracy και F1-Score, ανάλογα με την ένταση της επίθεσης (Intensity of Attack). Από 10% έως 100% των καταναλώσεων ήταν οι επιλογές στην απάτη και εφαρμογή σε ένα τυχαίο διάστημα ίσο με 10 ώρες.



Σχήμα 4.7 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 10 ωρών



Σχήμα 4.8: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια 10 ωρών



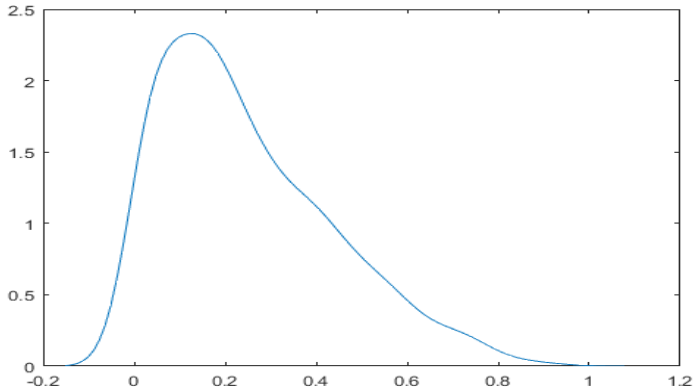
Σχήμα 4.9 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 10 ωρών

4.2.4 Περίπτωση επίθεσης από μια κατανομή

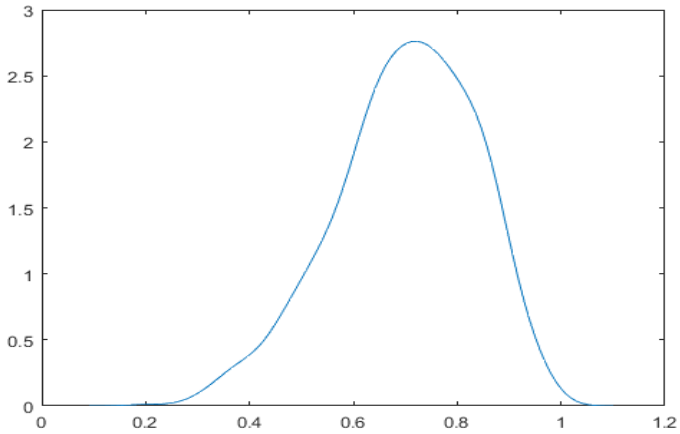
Σε αυτήν την ενότητα αναλύονται τις περιπτώσεις επίθεσης, στις οποίες ο παράγοντας αλλοίωσης των δεδομένων αλλάζει για τον κάθε καταναλωτή, ακολουθώντας κάποιες από τις γνωστές κατανομές, όπως βήτα, κανονική ή τυχαία, αλλάζοντας τις παραμέτρους τους, δηλαδή, περιπτώσεις κατανομών σε διαστήματα κοντά σε παράγοντες έντονης επίθεσης και ήπιας, αντίστοιχα. Ο παράγοντας αλλοίωσης ήταν διαφορετικός για κάθε καταναλωτή, αλλά σταθερός για τον καθένα ως προς τις μέρες και τις ώρες, στις οποίες εφαρμόστηκε.

4.2.4.1 Κατανομή beta

Σε αυτήν την εφαρμογή επίθεσης έγιναν δύο περιπτώσεις, η πρώτη με παραμέτρους α=1 και b=3 και η δεύτερη με παραμέτρους α=7 και b=3 όπως φαίνονται παρακάτω:



Σχήμα 4.10 : Κατανομή Βήτα (beta) με παράγοντες α=1,b=3



Σχήμα 4.11 : Κατανομή Beta με παράγοντες α=7,b=3

Έτσι, τα αποτελέσματα που δόθηκαν από τον αλγόριθμο ταξινόμησης ήταν:

Πίνακας 4.13 : Αποτελέσματα ταξινόμησης για επίθεση από κατανομή beta

Κατανομή	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
Beta(α=1,b=3)	94,18	8,82	97,21	94,57	88,39
Beta(α=7,b=3)	73,64	31,09	78,77	74,74	47,68

➢ Confusion Matrix

Πίνακας 4.14 : Confusion Matrix για απάτη από κατανομή beta(α=1,b=3)

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	51917	5059
Πραγματική τάξη=1	1599	55736

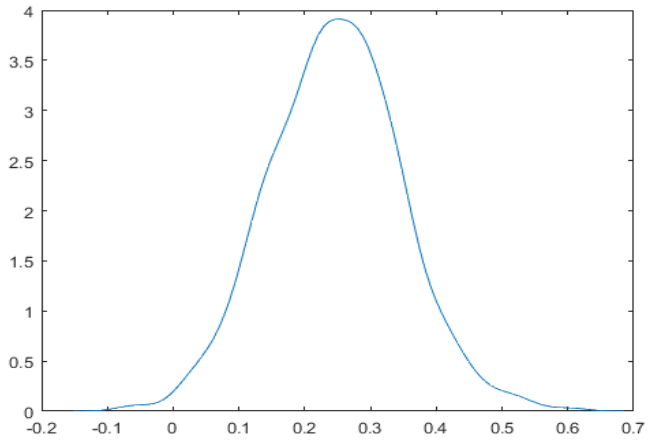
Πίνακας 4.15 : Confusion Matrix για απάτη από κατανομή beta(α=7,b=3)

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	39195	17857
Πραγματική τάξη=1	12275	44984

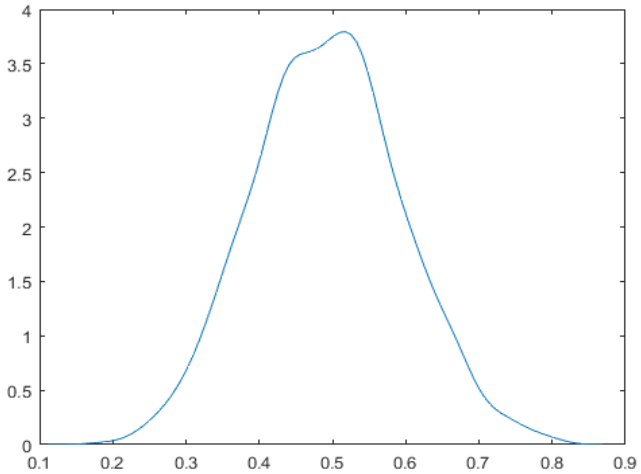
4.2.4.2 Κανονική Κατανομή

Σε αυτού του είδους την κατανομή έγινε μελέτη με τρεις τύπους δηλαδή, η πρώτη με μέση τιμή=0.25 και τυπική απόκλιση=0.1, η δεύτερη με μέση τιμή=0.5 και τυπική απόκλιση=0.1 και η τρίτη με μέση τιμή =0.8 και τυπική απόκλιση=0.07. Όπως φαίνεται από τις μέσες τιμές επιλέχθηκαν οι συγκεκριμένες για να αναλυθούν οι κατανομές κοντά σε μια μέση τιμή έντονης επίθεσης, μία μέτριας επίθεσης και μία ήπιας επίθεσης.

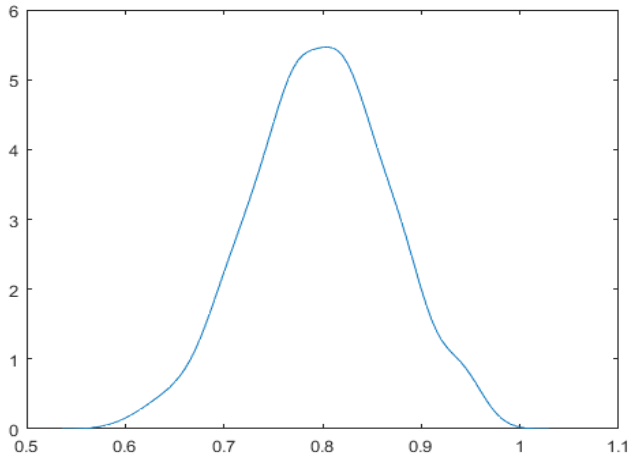
Οι γραφικές των κατανομών απεικονίζονται παρακάτω:



Σχήμα 4.12 : Κατανομή Normal με μέση τιμή=0.25,τυπική απόκλιση σ=0.1



Σχήμα 4.13 : Κατανομή Normal με μέση τιμή=0.5,τυπική απόκλιση σ=0.1



Σχήμα 4.14 : Κατανομή Normal με μέση τιμή=0.8,τυπική απόκλιση σ=0.07

Τα αποτέλεσμα της ταξινόμησης σε κάθε περίπτωση ήταν:

Πίνακας 4.16 : Αποτελέσματα ταξινόμησης για επίθεση από κανονική Normal

Κατανομή	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
Normal μ=0.25,σ=0.1	95,32	7,83	98,54	95,73	90,71
Normal μ=0.5,σ=0.1	87,57	16,86	92,04	88,47	75,18
Normal μ=0.8,σ=0.07	65,72	39,80	71,81	67,48	32,01

- **Confusion Matrix**

Πίνακας 4.17 : Confusion Matrix για απάτη από κατανομή Normal(μ=0.25,σ=0.1)

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	52621	4517
Πραγματική τάξη=1	829	56344

Πίνακας 4.18 : Confusion Matrix για απάτη από κατανομή Normal(μ=0.5,σ=0.1)

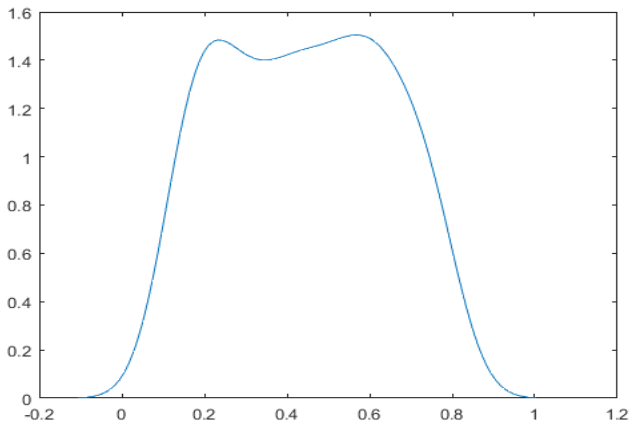
	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	47377	9619
Πραγματική τάξη=1	4591	52724

Πίνακας 4.19 : Confusion Matrix για απάτη από κατανομή Normal(μ=0.8,σ=0.07)

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	34220	22903
Πραγματική τάξη=1	16286	40902

4.2.4.3 Τυχαία κατανομή

Σε αυτήν την ανάλυση μια τυχαία κατανομή στο διάστημα [0.1,0.9] χρησιμοποιήθηκε για την εφαρμογή επίθεσης. Στην ουσία, ο παράγοντας αλλοίωσης άλλαζε για κάθε καταναλωτή τυχαία ανάμεσα σε αυτό το διάστημα. Η επιλογή ήταν ίσης πιθανότητας, όπως φαίνεται και στο παρακάτω Σχήμα.



Σχήμα 4.15 : Κατανομή Random στο διάστημα [0.1,0.9]

Τα αποτελέσματα σε αυτή την περίπτωση ήταν:

Πίνακας 4.20 : Αποτελέσματα ταξινόμησης για επίθεση από κανονική Random

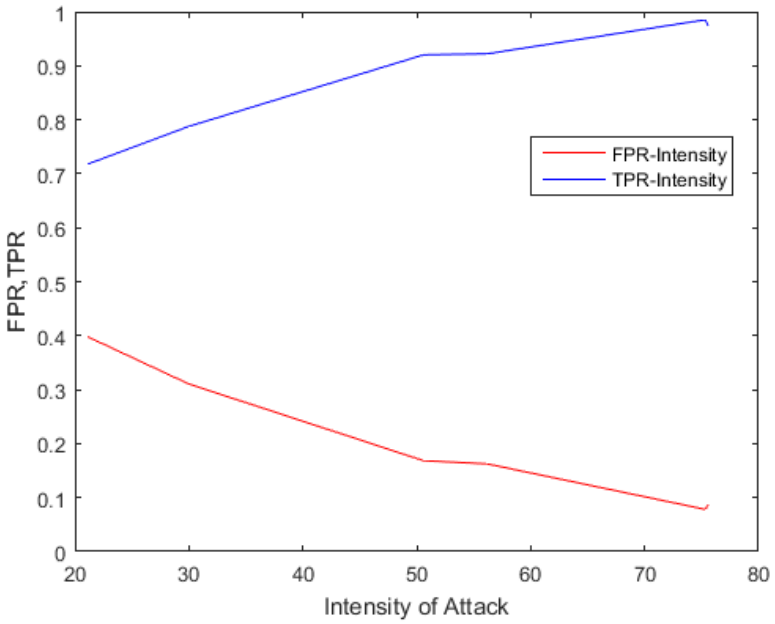
Κατανομή	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
Random [0.1-0.9]	87,90	16,27	92,23	88,69	75,96

- **<u>Confusion Matrix</u>**

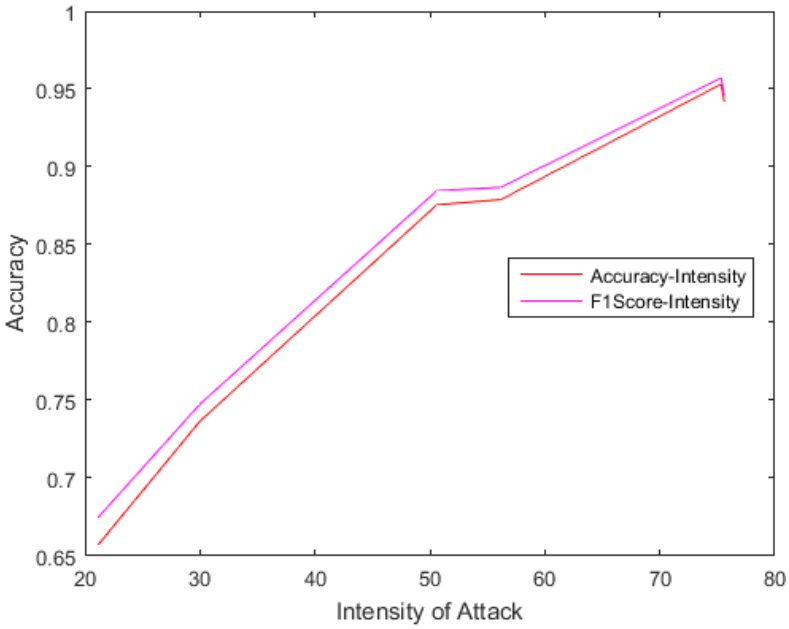
Πίνακας 4.21 : Confusion Matrix για απάτη από κατανομή Random([0.1,0.9])

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	47888	9379
Πραγματική τάξη=1	4450	52594

Στο παρακάτω σχήμα φαίνεται η μεταβολή του δείκτη FPR και TPR σε σχέση με τον μέσο παράγοντα αλλοίωσης από τις παραπάνω κατανομές που μελετήθηκαν. Επίσης, παρατίθενται οι μεταβολές της ακρίβειας (Accuracy, FI-Score) ανάλογα της έντασης προερχόμενη από κάποια κατανομή.



Σχήμα 4.16 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 24 ωρών με παράγοντες αλλοίωσης από κατανομές



Σχήμα 4.17 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 24 ωρών με παράγοντας αλλοίωσης από κατανομές.

4.2.5 Σχόλια και συμπεράσματα από τη μελέτη για μεταβλητή ένταση της επίθεσης

Στις παραγράφους 4.2.1-4.2.4 γίνεται μελέτη και εκτενής παρουσίαση των αποτελεσμάτων από τις ταξινομήσεις διαφορών δοκιμών επίθεσης. Σε κάθε ξεχωριστή δοκιμή, παρουσιάζονται οι δείκτες εκτίμησης της ταξινόμησης από τον αλγόριθμο με SVM, δηλαδή η ακρίβεια, οι δείκτες FPR,TPR,HD και οι συγκεντρωτικοί πίνακες σύγχυσης. Ακόμα, παρουσιάζονται οι γραφικές παραστάσεις των δεικτών σε σχέση με τον τύπο της επίθεσης ως προς την ένταση και την χρονική διάρκεια.

Παρατηρείται ότι οι έντονες επιθέσεις είναι εύκολα ανιχνεύσιμες από τον αλγόριθμο. Οι ημέρες με απάτη και εκείνες χωρίς απάτη, στην περίπτωση αυτή, είναι εύκολα διαχωρίσιμες. Αντίθετα, στη δοκιμή κλοπής για κάτω από 20% των δεδομένων, ο αλγόριθμος δεν είναι αποδοτικός. Συγκεκριμένα, παρατηρείται μία αύξηση της ακρίβειας και του δείκτη αληθώς θετικών ταξινομήσεων καθώς αυξάνεται η ένταση, είτε ως προς τον βαθμό αλλοίωσης είτε ως προς την χρονική διάρκεια. Παράλληλα, μειώνεται ο δείκτης των ψευδώς θετικών ταξινομήσεων. Παρ' όλα αυτά, η απόδοση της ταξινόμησης δεν επηρεάζεται μόνο από τον τύπο της επίθεσης, αλλά και από τον τύπο του καταναλωτή. Για παράδειγμα, υπάρχουν καταναλωτές στο σύνολο των χιλίων, οι οποίοι για ένα μεγάλο χρονικό διάστημα μηδενίζουν τις καταναλώσεις τους, με αποτέλεσμα ο αλγόριθμος να τις ταξινομεί ως απάτη. Αυτό συμβαίνει για διάφορους λόγους, όπως αλλαγή της κατοικίας, παύση λειτουργίας μια επιχείρησης, κλπ. Ως εκ τούτου, αφού γίνεται η ταξινόμηση, σε περίπτωση μη προσδοκώμενων αποτελεσμάτων ομαδοποιούνται οι αντίστοιχοι καταναλωτές σε μία ξεχωριστή βάση δεδομένων για συνέχιση της μελέτης και ανάλυσης. Γενικότερα, ο αλγόριθμος ταξινόμησης λειτουργεί σωστά, με την προβλεπόμενη απόδοση.

4.3 Μελέτη ως προς το χρόνο επίθεσης

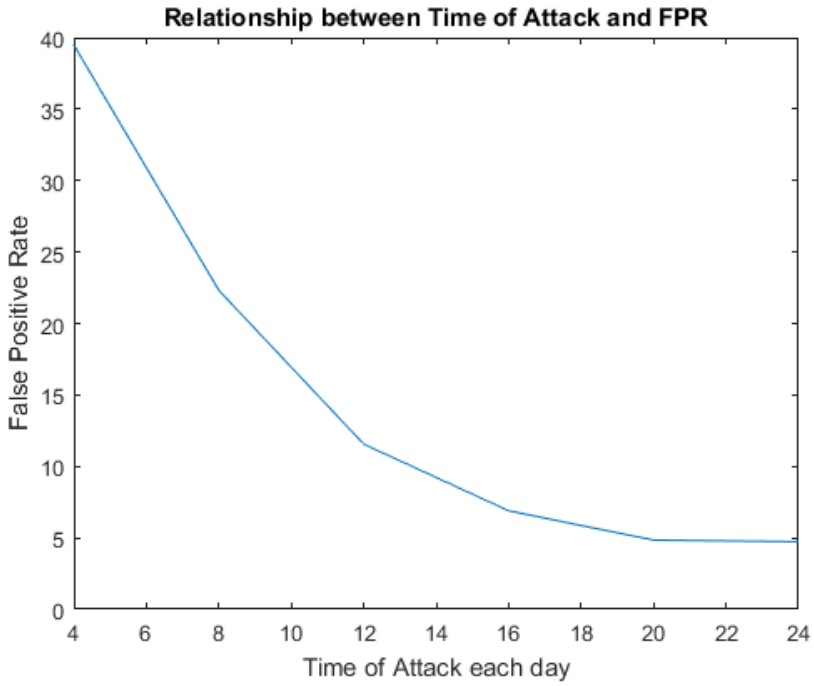
4.3.1 Περιπτώσεις επίθεσης

Σε αυτή τη μελέτη γίνεται παραμετροποίηση της διάρκειας επίθεσης. Δηλαδή, για μία σταθερού τύπου επίθεση, για παράδειγμα πολύ έντονη της τάξης 90% κλοπής των δεδομένων, αναλύθηκαν επιθέσεις σε 4 ώρες σε μια μέρα, 8 ώρες, 12, 16, 20 και τέλος 24 ώρες. Τα αποτελέσματα της κάθε μελέτης φαίνονται στον παρακάτω πίνακα δεικτών.

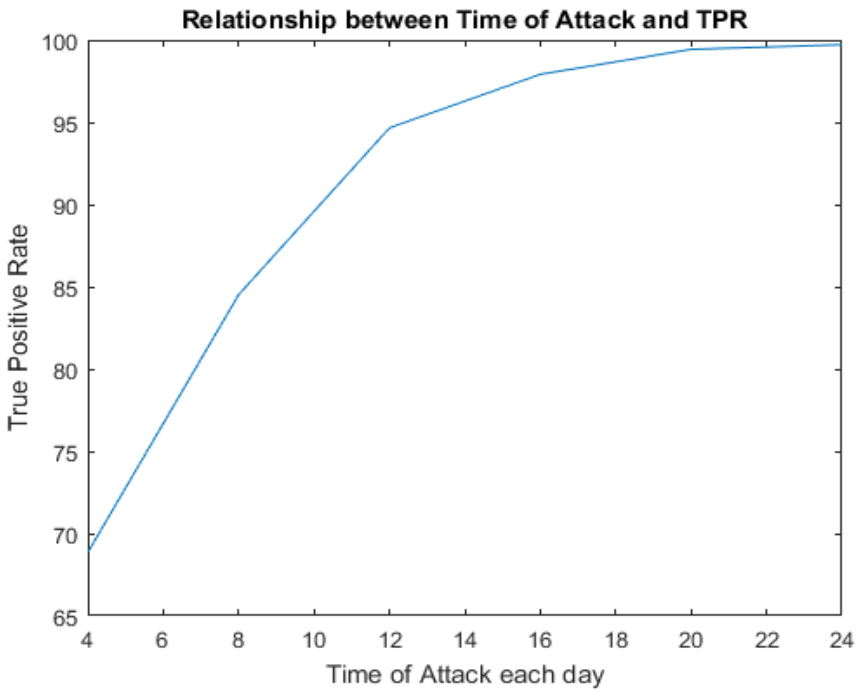
Πίνακας 4.22 : Αποτελέσματα ταξινόμησης διαφόρων δοκιμών ως προς την ώρα επίθεσης

Ώρες/ημέρα	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
4	64,36	39,48	68,87	65,34	29,39
8	80,97	22,32	84,53	81,71	62,21
12	91,49	11,56	94,67	92,03	83,11
16	95,48	6,90	97,92	95,81	91,02
20	97,27	4,85	99,44	97,53	94,59
24	97,48	4,74	99,72	97,73	94,98

Ακολούθως, στα παρακάτω σχήματα, απεικονίζεται η μεταβολή του FPR, και TPR, σε ποσοστά επί τις εκατό, σε σχέση με τις ώρες εφαρμογής της απάτης.



Σχήμα 4.18 : Διάγραμμα Χρόνου Επίθεσης-FPR



Σχήμα 4.19 : Διάγραμμα Χρόνου Επίθεσης-TPR

4.3.2 Σχόλια και συμπεράσματα της μελέτης ως προς το χρόνο επίθεσης

Σε αυτή την πειραματική διαδικασία γίνεται ανάλυση της επίδρασης της δειγματοληπτικής επιλογής των ωρών επίθεσης, ανά ημέρα, για την μελέτη ανίχνευσης απάτης. Μια αύξηση της απόδοσης του αλγόριθμου ταξινόμησης παρατηρείται, στον Πίνακα 4.22, των αποτελεσμάτων, καθώς αυξάνονται οι ώρες επίθεσης. Οι δείκτες βελτιώνονται κατά 2-3 μονάδες, καθώς αυξάνονται οι ώρες ανά τέσσερις, ενώ παρατηρείται μια μικρότερη αλλαγή στη διάρκεια από 18 έως 24 ώρες. Δηλαδή, ύστερα από ένα κατώφλι στην επιλογή των ημερών, η απόδοση του ταξινομητή σταθεροποιείται. Για παράδειγμα[24], ένας καταναλωτής θέλει να κλέψει 5kW από την ημερήσιά του κατανάλωση με ομοιόμορφο διαχωρισμό του ποσού σε όλες τις ώρες της ημέρας. Οι αλλαγές σε 24 ωριαίες μετρήσεις της ημερήσιας ενεργειακής ζήτησης είναι λιγότερο εμφανείς, από όταν 5kW επεκτείνονται σε 16 και 20 ώρες. Ωστόσο, για λιγότερο από 16 ώρες επίθεσης, το πρότυπο κατανάλωσης δεν μπορεί να μοντελοποιηθεί με ακρίβεια.

4.4 *Μελέτη συνδυασμού επιθέσεων*

4.4.1 Περίπτωση συνδυασμού επιθέσεων του 90% και 50% των δεδομένων

Σε αυτό τον τύπο επίθεσης χρησιμοποιείται μία φορά ο αρχικός πίνακας κάθε καταναλωτή, δειγματοληπτικά και σε αριθμό του μισού των μετρήσεων εφαρμόζεται επίθεση της τάξης του 90% σε 24 ώρες. Δεύτερη φορά χρησιμοποιείται το άλλο μισό των δεδομένων για επίθεση της τάξης του 50% σε 24 ώρες. Στο τέλος, συγχωνεύονται οι δύο πίνακες με αποτέλεσμα να διπλασιάζεται ο όγκος των ημερών για κάθε καταναλωτή, δηλαδή περιλαμβάνονται οι μέρες όλες με επίθεση και χωρίς επίθεση. Τέλος, διαχωρίζεται το δείγμα εκπαίδευσης (training set) για το SVM με το 70 % του συνόλου και το άλλο 30% για το δείγμα δοκιμής (test set). Σε αυτό το σημείο χρειάζεται πάλι προσοχή, ώστε στο training set να έχει ίσο αριθμό γνήσιων και αλλοιωμένων ημερών για καλύτερη εκπαίδευσή του.

Τα αποτελέσματα του SVM ήταν:

Πίνακας 4.23 : Αποτελέσματα ταξινόμησης συνδυασμού επιθέσεων(80%&50%)

Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
91,34	11,14	93,83	91,72	82,69

4.4.2 Περίπτωση συνδυασμού επιθέσεων του 50% και 20% των δεδομένων

Σε αυτό τον τύπο επίθεσης δοκιμάζεται πρώτη φορά στον αρχικό πίνακα κάθε καταναλωτή, δειγματοληπτικά και σε αριθμό τον μισό των μετρήσεων εφαρμόζεται επίθεση της τάξης του 50% και για δεύτερη φορά στο άλλο μισό επίθεση της τάξης του 20%. Ομοίως, προκύπτει ο διπλάσιος όγκος ημερών για κάθε καταναλωτή, οι μέρες όλες με επίθεση και χωρίς επίθεση. Τέλος, επιλέγεται δείγμα εκπαίδευσης για το SVM το 70 % του συνόλου και το άλλο 30% για το δείγμα δοκιμής.
Τα αποτελέσματα του SVM ήταν:

Πίνακας 4.24 : Αποτελέσματα ταξινόμησης συνδυασμού επιθέσεων(50%&20%)

Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
75,19	22,86	73,36	74,87	50,6

4.4.3 Σχόλια και συμπεράσματα της μελέτης συνδυασμού επιθέσεων

Στις ενότητες 4.4.1-4.4.2 μελετήθηκε η δοκιμή με συνδυασμό διαφορετικών τύπων επίθεσης. Παρατηρείται μία σαφώς καλύτερη απόδοση στην πρώτη περίπτωση ισχυρότερων επιθέσεων σε σχέση με την δεύτερη, ήπιων επιθέσεων. Ωστόσο, η απόδοση δεν δίνει τα ίδια αποτελέσματα με την δοκιμή επίθεσης μόνο στο 90% των

δεδομένων. Στην περίπτωση συνδυασμού ήπιων επιθέσεων (50% και 20%) οι δείκτες αξιολόγησης της ταξινόμησης χειροτερεύουν, καθώς πρόκειται για περιπτώσεις επίθεσης στις οποίες η αλλοίωση των ημερών είναι ελάχιστη και δύσκολα ανιχνεύσιμη.

4.5 Μελέτη με διαφορετική επίθεση σε Training και Test Set

4.5.1 Περίπτωση επίθεσης του 90% και 50% των δεδομένων στο Training Set και 20% στο Test Set

Σε αυτή την δοκιμή η εκπαίδευση του μοντέλου ταξινόμησης έγινε για διαφορετικού τύπου επίθεσης, και μάλιστα συνδυασμών (90% και 50%), σε σχέση με την δοκιμή (20%). Δηλαδή, η εκπαίδευση έγινε για συνδυασμό έντονης και μέτριας επίθεσης και η δοκιμή για μια ήπια.
Τα αποτελέσματα που δόθηκαν από τον αλγόριθμο:

Πίνακας 4.25 : Αποτελέσματα ταξινόμησης 1η περίπτωση διαφορετικού Training-Test Set

Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
57,55	11,17	26,28	36,68	15,11

4.5.2 Περίπτωση επίθεσης του 20% και 50% στο Training Set Και 90% στο Test Set

Αντιστοίχως με την παραπάνω δοκιμή παρουσιάζονται τα αποτελέσματα της ταξινόμησης με αντίστροφη διαδικασία, δηλαδή εκπαίδευση με ασθενέστερων τύπων επίθεσης και δοκιμή σε ισχυρότερο τύπο.

Πίνακας 4.26 : Αποτελέσματα ταξινόμησης 2η περίπτωση διαφορετικού Training-Test Set

Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
89,65	18,31	97,60	89,91	79,29

4.5.3 Σχόλια και συμπεράσματα για τη μελέτη διαφορετικής επίθεσης στο Training και Test Set

Ο αλγόριθμος εκπαιδεύτηκε με διαφορετικού τύπου επίθεσης στα δεδομένα από ότι δοκιμάστηκε. Αρχικά, παρατηρείται καλύτερη απόδοση του αλγόριθμου στην δεύτερη περίπτωση, δηλαδή ο αλγόριθμος εκπαιδεύτηκε με ήπια επίθεση. Το γεγονός

ότι ήταν καλύτερη η απόδοση οφείλεται στο ότι, αφού εκπαιδεύτηκε σε ήπιες αλλαγές των δεδομένων, όταν δοκιμάστηκε σε ισχυρότερες επιθέσεις ήταν εύκολα διαχωρίσιμα τα δεδομένα. Σε αντίθεση, στην πρώτη δοκιμή ο αλγόριθμος εκπαιδεύτηκε να διαχωρίζει έντονες επιθέσεις με αποτέλεσμα να μην αποδίδει στη δοκιμή. Μάλιστα, παρατηρείται μία πολύ κακή εικόνα της απόδοσης, ως προς την ακρίβεια και την ανίχνευση των ημερών με απάτη. Ενώ, το αποτέλεσμα της ανίχνευσης ημερών χωρίς απάτες, οι οποίες λανθασμένα ταξινομήθηκαν με απάτη (FPR), αυξήθηκε κατά 70%. Αυτό αποδίδεται στο γεγονός ότι, μπόρεσε να διακρίνει της γνήσιες ημέρες καλύτερα από ότι τις αλλοιωμένες.

4.6 Μελέτη ως προς την ωριαία διάρκεια των μετρήσεων

Σε αυτήν την παράγραφο για την επιλογή της επίθεσης, χρησιμοποιείται ένα ρεαλιστικό σενάριο. Εφαρμόζεται για τον κάθε καταναλωτή διαφορετικού τύπου επίθεση, αλλά με παράγοντα αλλοίωσης από μια κατανομή βήτα, με τιμές κοντά στο 0.2 (80% επίθεση δεδομένων). Η διάρκεια είναι τυχαία για τον καθένα, μεταξύ 16 και 24 ωρών, αλλά σταθερή ως προς τις μέρες του καθενός. Τα αποτελέσματα φαίνονται ακολούθως:

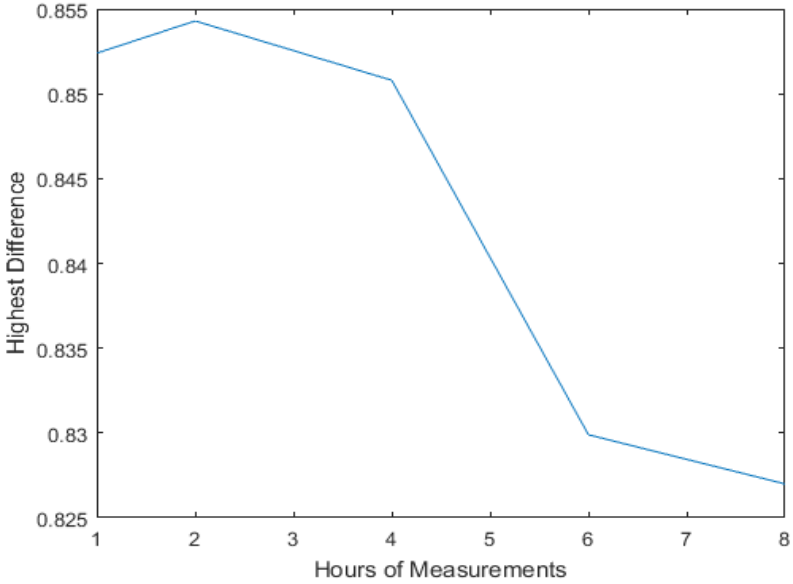
4.6.1 Ώρες μετρήσεων

Τα αποτελέσματα της ταξινόμησης φαίνονται στον Πίνακα 4.27.

Πίνακας 4.27 : Αποτελέσματα ταξινόμησης μελέτης διάρκειας των μετρήσεων

Μετρήσεις/ημέρα	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
Ωριαίες	92,58	10,26	95,50	93,05	85,24
Δίωρες	92,68	7,81	93,24	92,74	85,43
Τετράωρες	92,51	6,52	91,60	92,27	85,08

Στο παρακάτω σχήμα απεικονίζεται η μεταβολή του HD (Highest Difference) σε σχέση με τις ώρες μετρήσεων. Το HD είναι η διαφορά των ποσοστών TPR και FPR,.



Σχήμα 4.20 : Γραφική παράσταση Highest Difference -Hours of Measurements

4.6.2 Σχόλια και συμπεράσματα από τη μελέτη ως προς τη χρονική διάρκεια των μετρήσεων

Σε αυτήν την ενότητα εξετάζεται ένα ρεαλιστικό σενάριο, δηλαδή κάθε καταναλωτής να έχει διαφορετικό παράγοντα αλλοίωσης ακολουθούμενο μία κατανομή βήτα έντονων επιθέσεων, εφαρμογή σε τυχαία διάρκεια σε κάθε ημερήσιο διάνυσμα αλλά σταθερός παράγοντας ως προς τις μέρες και τις ώρες κάθε καταναλωτή. Οι μετρήσεις στην αρχή είναι ωριαίες, όπως γίνεται η ανάλυση μέχρι τώρα. Στη συνέχεια, γίνεται αθροιστικός υπολογισμός, ώστε οι μετρήσεις να είναι δίωρες ή τετράωρες αντίστοιχα. Στο Σχήμα4.20 φαίνεται η μεταβολή του δείκτη HD σε σχέση με την μεταβολή των μετρήσεων. Αυτό, το οποίο παρατηρείται και παρουσιάζει ενδιαφέρον είναι, ότι καθώς συνεχίζεται η ανάλυση σε δίωρες, τετράωρες και περαιτέρω μετρήσεις ο δείκτης αρχίζει να μειώνεται. Το γεγονός αυτό οφείλεται στο ότι, όσες περισσότερες είναι οι μετρήσεις τόσο πιο πλήρες διαμορφώνεται το πρότυπο κατανάλωσης για την ημέρα. Ενώ, όταν οι μετρήσεις προστίθενται, ώστε να υπάρχουν δίωρες και τετράωρες μετρήσεις τα δεδομένα συγχωνεύονται και αλλοιώνεται η καθαρή εικόνα της κατανάλωσης.

4.7 *Μελέτη με βάση εξαγωγή χαρακτηριστικών*

Σε αυτήν την παράγραφο παρουσιάζονται τα αποτελέσματα των δοκιμών ταξινόμησης με την χρήση χαρακτηριστικών. Όπως αναλύθηκε στο Κεφάλαιο 3, η εξαγωγή χαρακτηριστικών βοηθάει στην μείωση της διάστασης του όγκου των δεδομένων. Οι περιπτώσεις που μελετήθηκαν ήταν οι ίδιες με των παραγράφων 4.2-4.3 και φαίνονται παρακάτω.

4.7.1 Περίπτωση έντονης επίθεσης, της τάξης του 90% των δεδομένων

Σε αυτή την δοκιμή, αφού προσομοιωθεί η απάτη, συγκεκριμένα στο 90% των δεδομένων, γίνεται υπολογισμός των χαρακτηριστικών βάσει των μετρήσεων κατανάλωσης και αντίστοιχα διαμορφώνονται οι πίνακες των καταναλωτών για είσοδο στον ταξινομητή.

Τα αποτελέσματα, που δόθηκαν από την ταξινόμηση, φαίνονται στον Πίνακα 4.28.

Πίνακας 4.28 : Αποτελέσματα ταξινόμησης απάτης του 90% των δεδομένων με εξαγωγή χαρακτηριστικών

Ώρες/ημέρα	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
10 ώρες	85,83	13,58	85,27	84,90	71,69
10-24 ώρες	91,17	8,14	90,45	90,30	82,31
24 ώρες	96,18	4,35	96,68	95,41	92,33

4.7.2 Περίπτωση μέτριας επίθεσης, της τάξης του 50% των δεδομένων

Στην παράγραφο 4.7.2 αναλύεται η περίπτωση επίθεσης στο 50% των δεδομένων κατανάλωσης για διάφορες χρονικές περιόδους, από 10 ώρες έως 24 ώρες. Τα αποτελέσματα της ταξινόμησης φαίνονται στον Πίνακα 4.29.

Πίνακας 4.29 : Αποτελέσματα ταξινόμησης απάτης του 50% των δεδομένων με εξαγωγή χαρακτηριστικών

Ώρες/ημέρα	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
10 ώρες	68,29	31,48	68,28	67,29	36,8
10-24 ώρες	78,12	21,08	77,07	77,07	55,99
24 ώρες	87,23	13,36	87,83	86,83	74,47

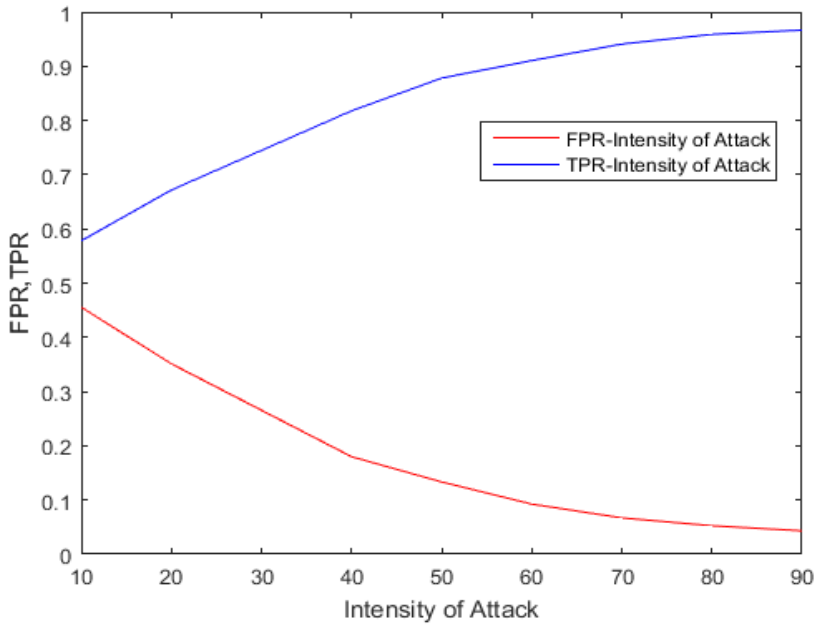
4.7.3 Περίπτωση ήπιας επίθεσης, της τάξης του 20 %

Στην παράγραφο 4.7.3 αναλύεται η περίπτωση επίθεσης στο 20% των δεδομένων κατανάλωσης για διάφορες χρονικές περιόδους, από 10 ώρες έως 24 ώρες. Τα αποτελέσματα της ταξινόμησης φαίνονται στον Πίνακα 4.30.

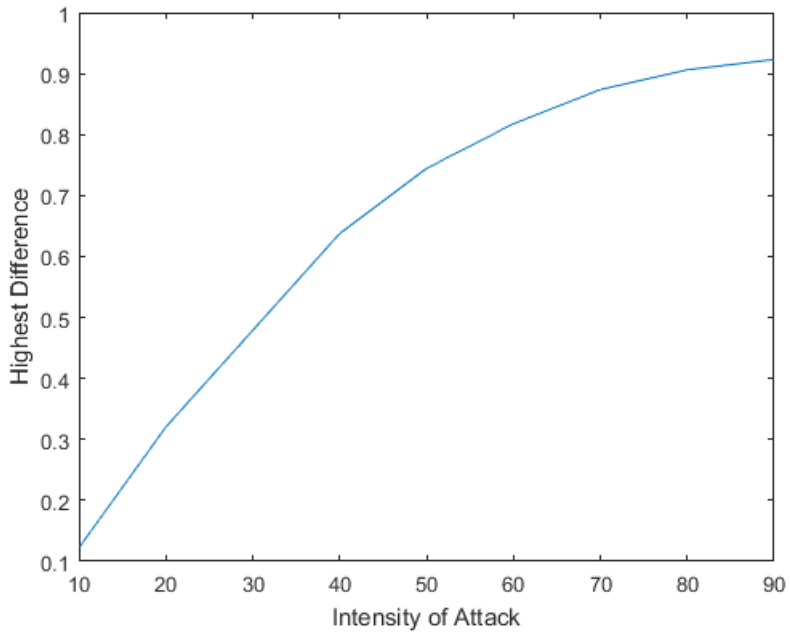
Πίνακας 4.30 : Αποτελέσματα ταξινόμησης απάτης του 20% των δεδομένων με εξαγωγή χαρακτηριστικών

‘Ωρες/ημέρα	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
10 ώρες	55,10	45,89	56,65	54,48	10,76
10-24 ώρες	60,79	40,22	62,10	62,10	60,17
24 ώρες	65,91	35,13	67,19	65,32	32,07

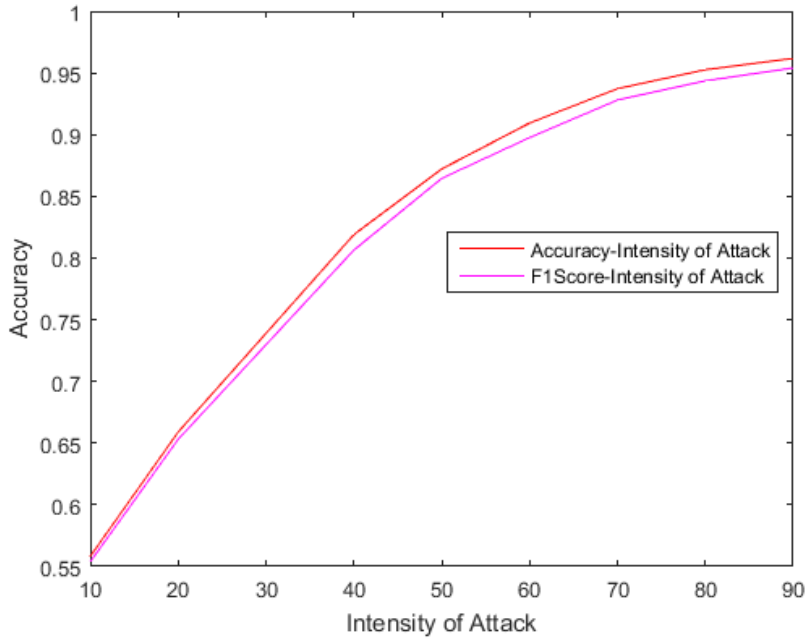
Παρακάτω απεικονίζονται οι μεταβολές του ποσοστού των ψευδώς θετικών (False Positive Rate,FPR), των αληθών θετικών (True Positive Rate,TPR), του δείκτη Highest Difference (HD) και της ακρίβειας από τους δείκτες Accuracy και F1-Score, ανάλογα με την ένταση της επίθεσης (Intensity of Attack). Από 10% έως 100% των καταναλώσεων ήταν οι επιλογές στην απάτη και εφαρμογή στις 24 ώρες κάθε ημέρας, με εξαγωγή χαρακτηριστικών.



Σχήμα 4.21 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 24 ωρών με εξαγωγή χαρακτηριστικών



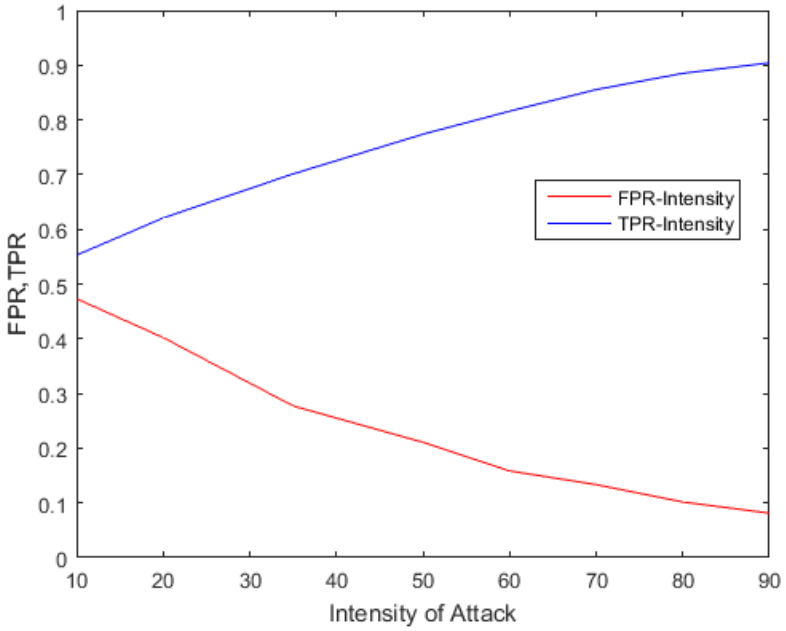
Σχήμα 4.22: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια 24 ωρών με εξαγωγή χαρακτηριστικών



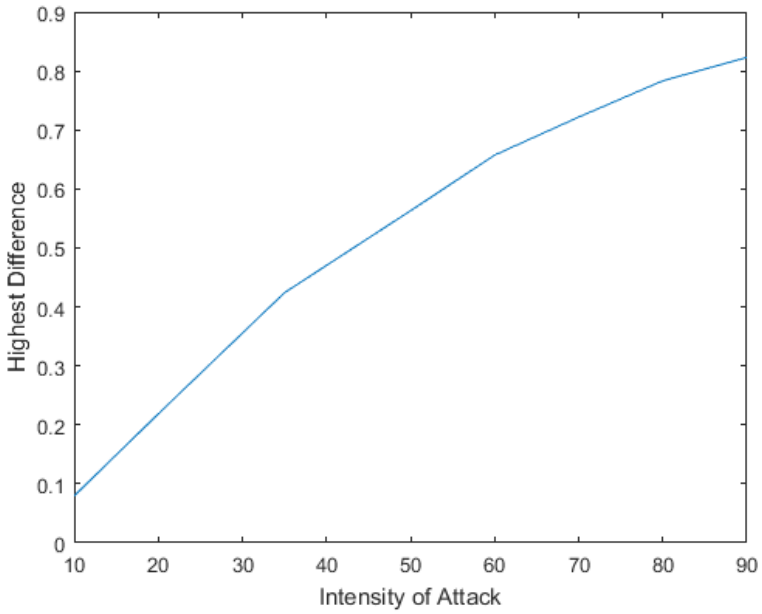
Σχήμα 4.23 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 24 ωρών με εξαγωγή χαρακτηριστικών

Στα παρακάτω γραφήματα απεικονίζονται οι μεταβολές του ποσοστού των ψευδώς θετικών (False Positive Rate,FPR), των αληθών θετικών (True Positive Rate,TPR),

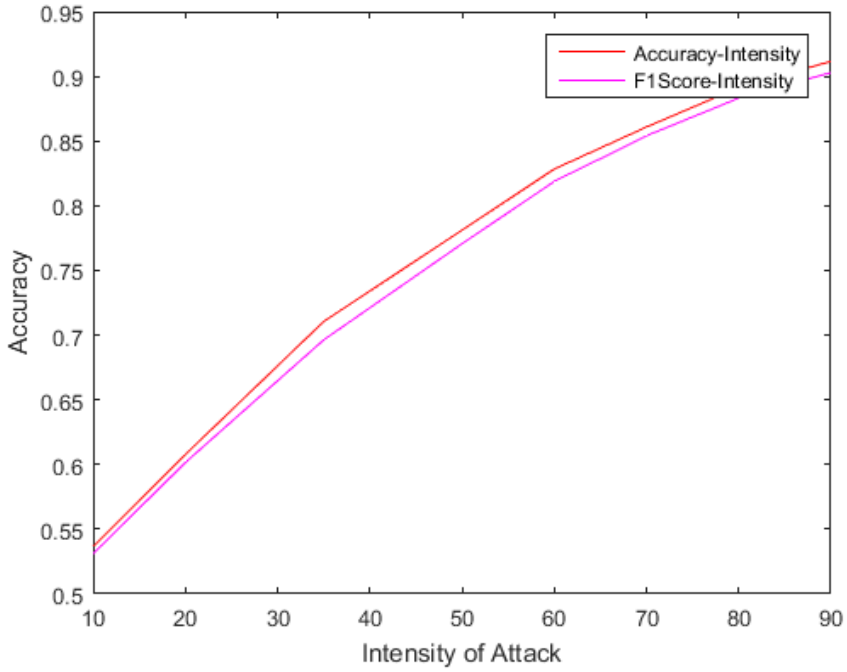
του δείκτη Highest Difference (HD) και της ακρίβειας από τον δείκτη Accuracy και F1-Score, ανάλογα με την ένταση της επίθεσης (Intensity of Attack). Από 10% έως 100% των καταναλώσεων ήταν οι επιλογές στην απάτη και εφαρμογή σε ένα τυχαία διάστημα ανάμεσα σε 10 και 24 ώρες, με εξαγωγή χαρακτηριστικών.



Σχήμα 4.24 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια από 10 έως 24 ώρες με εξαγωγή χαρακτηριστικών

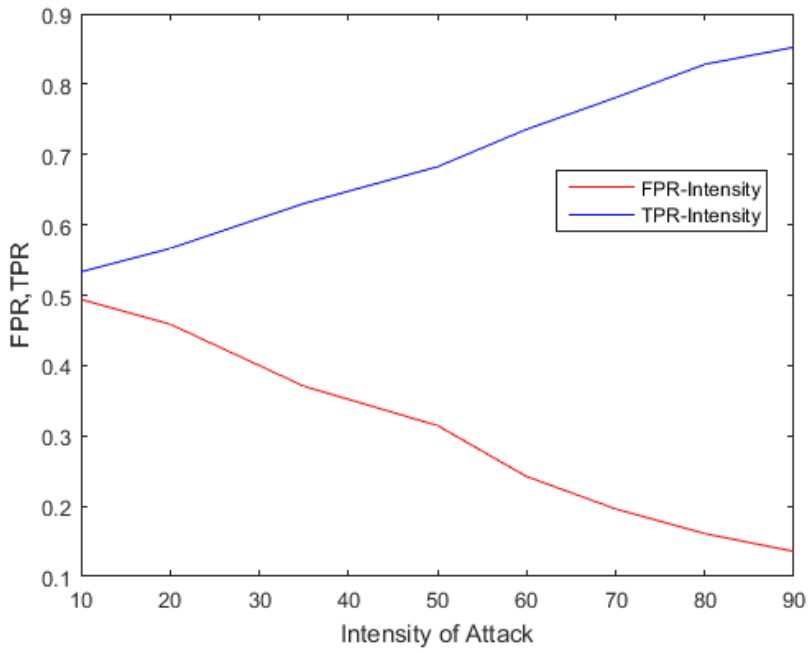


Σχήμα 4.25: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια από 10 έως 24 ώρες με εξαγωγή χαρακτηριστικών

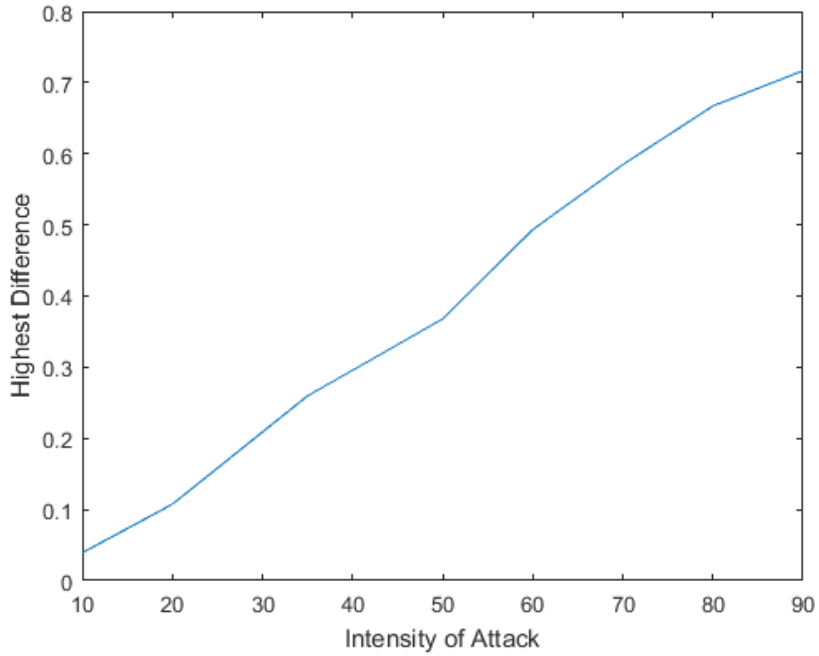


Σχήμα 4.26 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια από 10 έως 24 ώρες με εξαγωγή χαρακτηριστικών

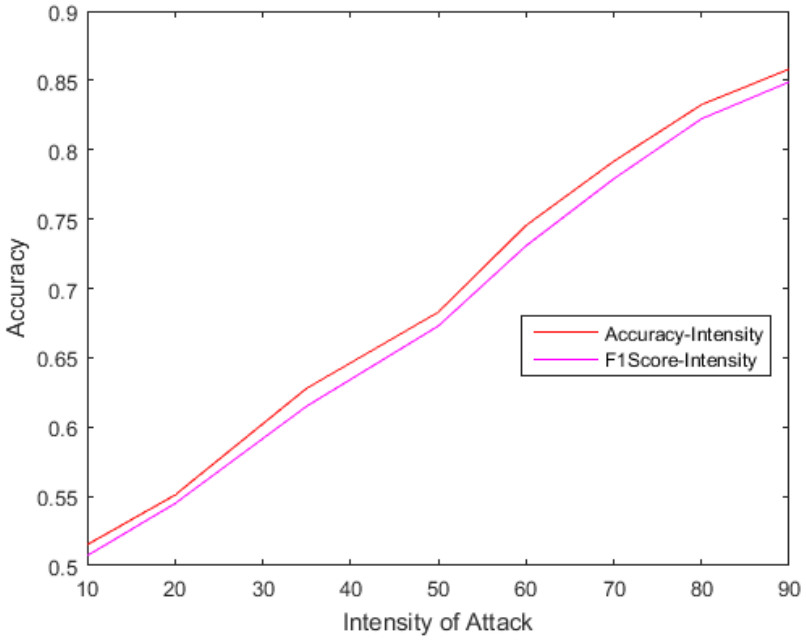
Στα παρακάτω γραφήματα απεικονίζονται οι μεταβολές του ποσοστού των ψευδώς θετικών (False Positive Rate,FPR), των αληθών θετικών (True Positive Rate,TPR), του δείκτη Highest Difference (HD) και της ακρίβειας από τον δείκτη Accuracy και F1-Score, ανάλογα με την ένταση της επίθεσης (Intensity of Attack). Από 10% έως 100% των καταναλώσεων ήταν οι επιλογές στην απάτη και εφαρμογή σε ένα τυχαίο διάστημα ίσο με 10 ώρες, με εξαγωγή χαρακτηριστικών.



Σχήμα 4.27 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 10 ωρών με εξαγωγή χαρακτηριστικών



Σχήμα 4.28: Γραφική παράσταση Highest Difference-Intensity of Attack για χρονική διάρκεια 10 ωρών με εξαγωγή χαρακτηριστικών



Σχήμα 4.29 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 10 ωρών με εξαγωγή χαρακτηριστικών

4.7.4 Κατανομή Βήτα

Σε αυτή την παράγραφο γίνεται ανάλυση παραγόντων αλλοίωσης των δεδομένων ακολουθούμενων κάποιων κατανομών, και συγκεκριμένη κατανομών βήτα. Όπως και στην ενότητα 4.2.4.1. επιλέγονται δύο κατανομές για έντονες επιθέσεις και για ήπιες επιθέσεις. Αφού εφαρμοστεί η προσομοίωση της απάτης για 24 ώρες στη μέρα, εξάγονται τα χαρακτηριστικά και ακολουθεί η ταξινόμηση. Τα αποτελέσματα της οποίας φαίνονται στον Πίνακα 4.31.

Πίνακας 4.31 : Αποτελέσματα ταξινόμησης για επίθεση από κατανομή βήτα(beta) με εξαγωγή χαρακτηριστικών

Κατανομή	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
Beta(α=1,b=3)	93,06	7,51	93,58	92,29	86,07
Beta(α=7,b=3)	73,31	31,63	78,76	74,64	47,13

4.7.5 Κανονική Κατανομή

Κατά τον ίδιο τρόπο σε αυτή την παράγραφο χρησιμοποιείται η κανονική κατανομή. Επιλέγονται τρεις περιπτώσεις κατανομών ανάλογα με τη μέση τιμή και την τυπική απόκλιση. Οι παράμετροι αυτές είναι τέτοιες, ώστε να αναφέρονται σε μία έντονη επίθεση, σε μία μέτρια έντασης και σε μία ασθενέστερη. Η προσομοίωση της

απάτης έγινε ομοίως σε 24 ώρες και τα αποτελέσματα απεικονίζονται στον Πίνακα 4.32.

Πίνακας 4.32 : Αποτελέσματα ταξινόμησης για επίθεση από κανονική κατανομή(Normal) με εξαγωγή χαρακτηριστικών

Κατανομή	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
Normal μ=0.25,σ=0.1	94,21	6,57	94,96	93,48	88,39
Normal μ=0.5,σ=0.1	86,81	13,77	87,42	86,05	73,65
Normal μ=0.8,σ=0.07	65,71	35,47	67,15	65,17	31,68

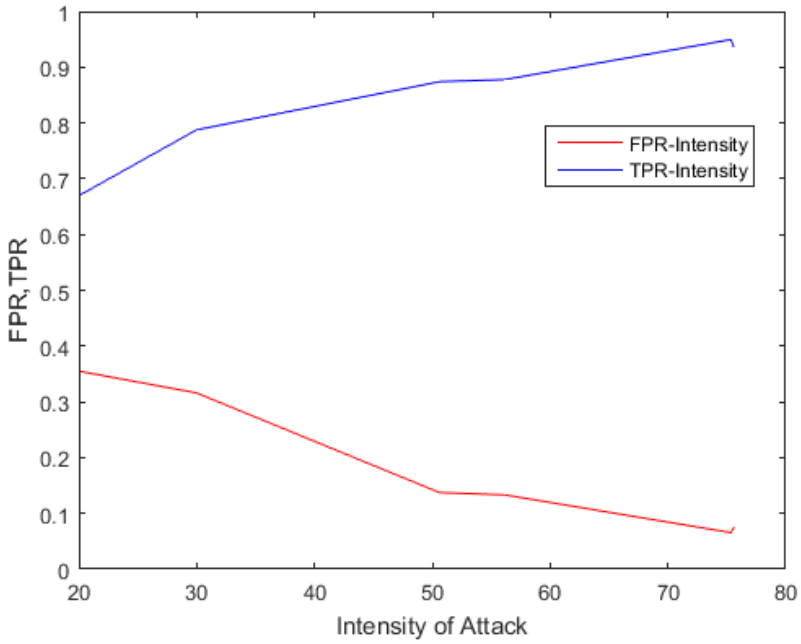
4.7.6 Τυχαία κατανομή

Ομοίως, σε αυτήν την παράγραφο γίνεται ανάλυση με παράγοντες αλλοίωσης από μία τυχαία κατανομή. Η τυχαία κατανομή είναι στο διάστημα [0.1-0.9] με ίση πιθανότητα για κάθε παράγοντα. Η εφαρμογή της επίθεσης έγινε σε διάρκεια 24 ωρών και τα αποτελέσματα της ταξινόμησης φαίνονται στον Πίνακα 4.33.

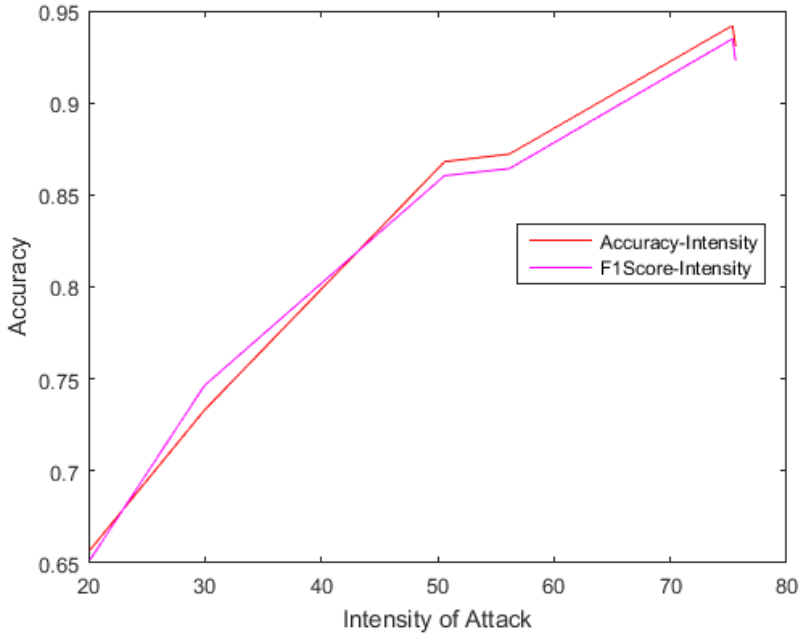
Πίνακας 4.33 : Αποτελέσματα ταξινόμησης για επίθεση από τυχαία κατανομή(random) με εξαγωγή χαρακτηριστικών

Κατανομή	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
Random [0.1-0.9]	87,22	13,33	87,80	86,44	74,47

Στη συνέχεια, απεικονίζονται η σχέση των δεικτών FPR,TPR και ακρίβειας με το μέσο παράγοντα αλλοίωσης από τις παραπάνω κατανομές.



Σχήμα 4.30 : Γραφική Παράσταση TPR-Intensity of Attack (μπλε) και FPR-Intensity of Attack (κόκκινο) για χρονική διάρκεια 24 ωρών με παράγοντες αλλοίωσης από κατανομές από εξαγωγή χαρακτηριστικών



Σχήμα 4.31 : Γραφικές Παραστάσεις ακρίβειας: Accuracy-Intensity of Attack και F1Score-Intensity of Attack για χρονική διάρκεια 24 ωρών με παράγοντας αλλοίωσης από κατανομές από εξαγωγή χαρακτηριστικών

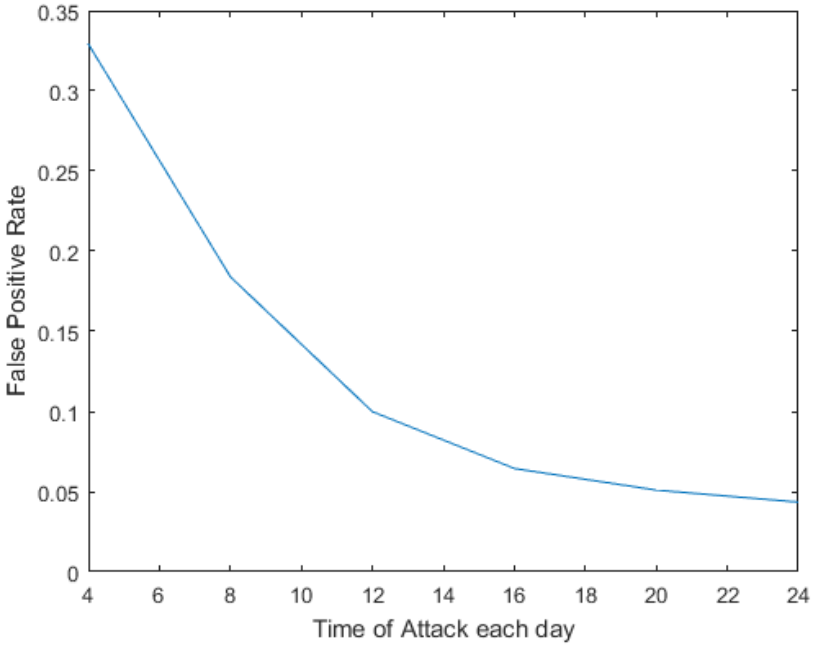
4.7.7 Μελέτη ως προς το χρόνο επίθεσης

Σε αυτή τη μελέτη γίνεται παραμετροποίηση της διάρκειας επίθεσης. Δηλαδή, για μία σταθερού τύπου επίθεση, για παράδειγμα πολύ έντονη της τάξης 90% κλοπής των δεδομένων, αναλύθηκαν περιπτώσεις με 4 ώρες επίθεσης σε μια μέρα, 8 ώρες, 12, 16, 20 και τέλος 24 ώρες. Ύστερα εξάγονται τα χαρακτηριστικά και γίνεται η ταξινόμηση. Τα αποτελέσματα για κάθε μελέτη φαίνονται στον παρακάτω πίνακα δεικτών.

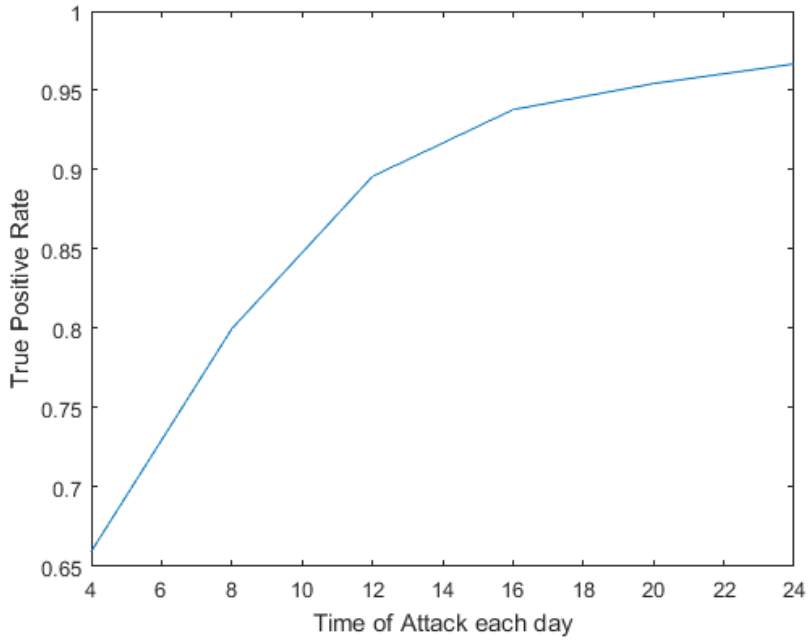
Πίνακας 4.34 : Αποτελέσματα ταξινόμησης διαφόρων δοκιμών ως προς την ώρα επίθεσης με εξαγωγή χαρακτηριστικών

Ώρες/ημέρα	Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
4	66,35	32,91	65,96	65,18	33,05
8	80,75	18,40	79,99	79,71	61,59
12	89,80	9,99	89,59	88,95	79,57
16	93,69	6,44	93,80	92,90	87,36
20	95,19	5,10	95,45	94,41	90,35
24	96,18	4,35	96,68	95,41	92,33

Τα παρακάτω γραφήματα απεικονίζουν την μεταβολή των ποσοστών ψευδώς θετικών (FPR) και αληθώς θετικών (TPR) σε σχέση με την διάρκεια της επίθεσης μέσα στη μέρα.



Σχήμα 4.32 : Διάγραμμα Χρόνου Επίθεσης-FPR με εξαγωγή χαρακτηριστικών



Σχήμα 4.33 : Διάγραμμα Χρόνου Επίθεσης-TPR με εξαγωγή χαρακτηριστικών

4.7.8 Σχόλια και συμπεράσματα από τη μελέτη με χαρακτηριστικά

Στις παραγράφους 4.7.1-4.7.7 γίνεται μελέτη και εκτενής παρουσίαση των αποτελεσμάτων από τις ταξινομήσεις διαφορών δοκιμών επίθεσης. Τα χαρακτηριστικά για την ταξινόμηση εξάγονται από τις μετρήσεις των ημερήσιων διανυσμάτων κάθε ημέρας του καταναλωτή και αφορούν στατιστικά μεγέθη, όπως η επίδραση της μέσης τιμής τεσσάρων περιόδων μέσα στην ημέρα, η επίδραση της τυπικής απόκλισης, η αιχμή ζήτησης, η συνολική ζήτηση, η ασυμμετρία και η κύρτωση. Σε κάθε ξεχωριστή δοκιμή, παρουσιάζονται οι δείκτες εκτίμησης της ταξινόμησης από τον αλγόριθμο με SVM, δηλαδή η ακρίβεια, οι δείκτες FPR,TPR,HD και οι συγκεντρωτικοί πίνακες σύγχυσης. Ακόμα, παρουσιάζονται οι γραφικές παραστάσεις των δεικτών σε σχέση με τον τύπο της επίθεσης ως προς την ένταση, την χρονική διάρκεια κλπ.

Τα αποτελέσματα συμπίπτουν με εκείνα των παραγράφων 4.2.1-4.2.4. Δηλαδή σε έντονες επιθέσεις και μεγάλης χρονικής διάρκειας η ταξινόμηση είναι αποδοτική και διαχωρίζει με ικανοποιητικό τρόπο τις ημέρες, ενώ σε ασθενέστερες επιθέσεις και μικρότερης χρονικής διάρκειας τα αποτελέσματα δεν είναι ικανοποιητικά. Επίσης, παρατηρείται μία μικρή απόκλιση σε σχέση με τις δοκιμές χωρίς εξαγωγή χαρακτηριστικών. Αυτό οφείλεται στην επιλογή των χαρακτηριστικών. Συμπεραίνεται πως με επιλογή περισσότερων χαρακτηριστικών πιθανότατα η απόδοση του αλγορίθμου θα ήταν μεγαλύτερης ακρίβειας. Στην επόμενη ενότητα

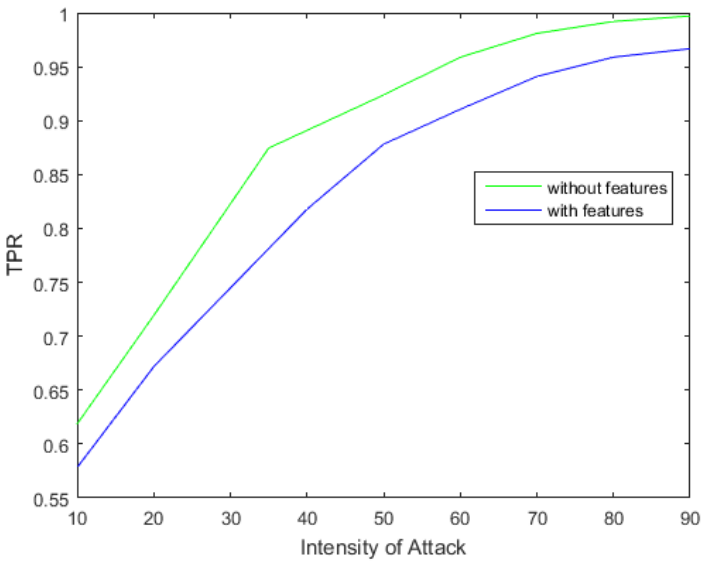
γίνεται συγκριτική μελέτη των τεχνικών χωρίς χαρακτηριστικά και με εξαγωγή χαρακτηριστικών.

4.8 Συγκριτική μελέτη των δοκιμών χωρίς εξαγωγή χαρακτηριστικών και με εξαγωγή χαρακτηριστικών

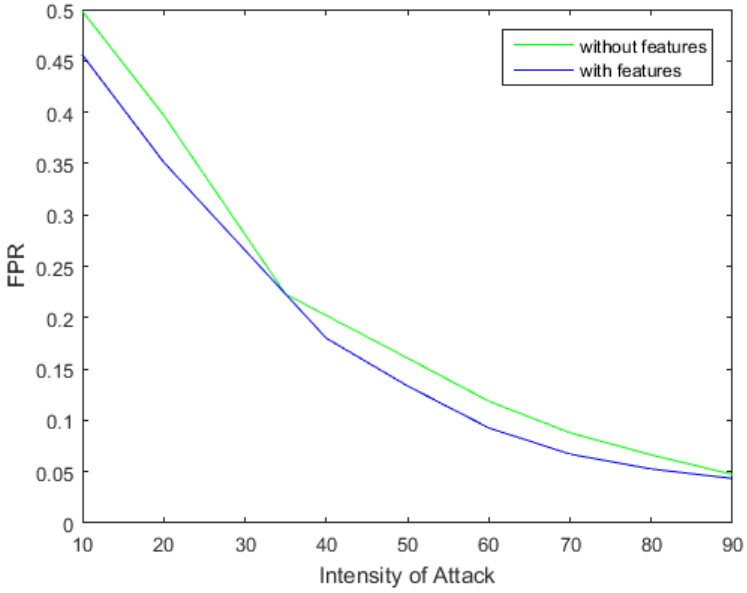
Σύμφωνα με τις μελέτες που διεξήχθησαν στις παραγράφους 4.2 έως 4.7, στην ενότητα αυτή γίνεται σύγκριση των δοκιμών με δεδομένα μετρήσεων κατανάλωσης και δεδομένα από εξαγωγή χαρακτηριστικών. Οι ενότητες 4.2 έως 4.6 αναφέρονται στη μελέτη δεδομένων με χαρακτηριστικά τις μετρήσεις κατανάλωσης από τον διαθέσιμο σύνολο δεδομένων. Στην ενότητα 4.7 παρουσιάζονται τα αποτελέσματα της ταξινόμησης για δεδομένα με στατιστικά χαρακτηριστικά βάσει των αρχικών μετρήσεων κατανάλωσης. Έτσι, σε αυτήν την ενότητα παρατίθενται διαγράμματα που αναφέρονται στην μεταβολή των δεικτών (FPR,TPR,Accuracy κλπ) στις δύο περιπτώσεις για την εξακρίβωση του ποια από τις δύο τεχνικές αποδίδει καλύτερα.

Αρχικά, μελετούνται οι περιπτώσεις επίθεσης με μεταβλητή ένταση της. Η μεταβλητότητα αυτή αφορά το ποσοστό κλοπής δεδομένων (90%, 50%, 20%) και τον χρόνο εφαρμογής της επίθεσης. Έτσι, οι δείκτες από τις περιπτώσεις με χαρακτηριστικά και χωρίς, ήταν:

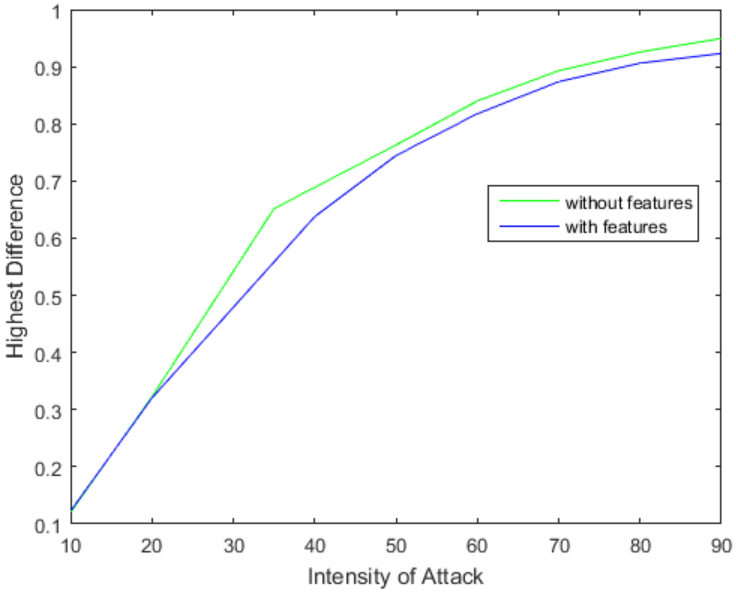
- <u>Αλλοίωση για 24 ώρες στο ημερήσιο διάνυσμα</u>



Σχήμα 4.34 : Γραφική Παράσταση TPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και TPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για 24 ώρες

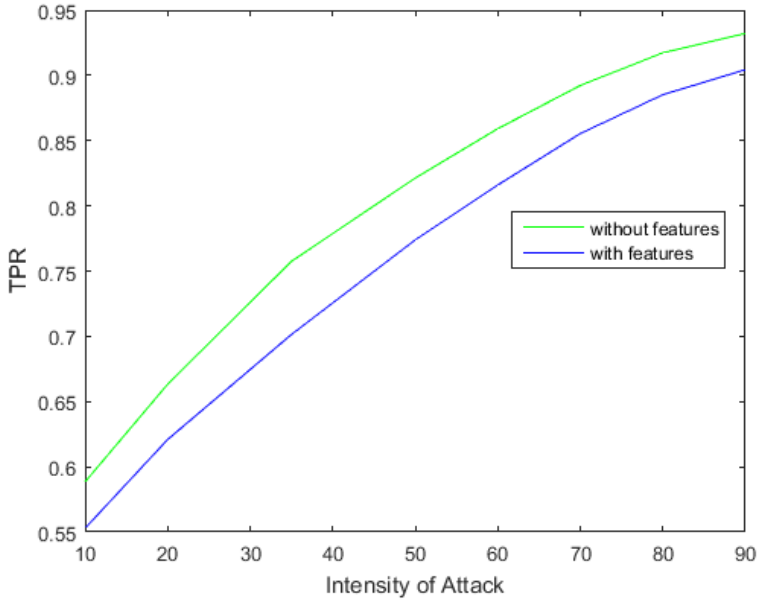


Σχήμα 4.35 : Γραφική Παράσταση FPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και FPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για 24 ώρες

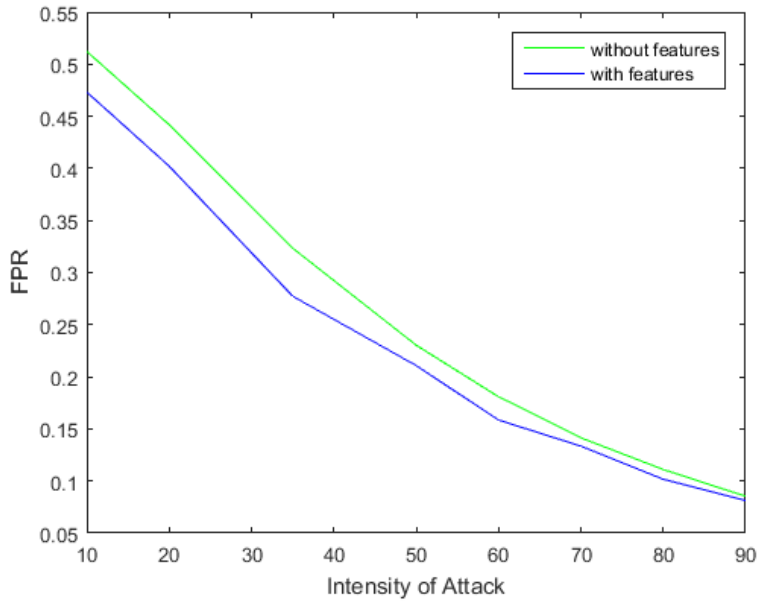


Σχήμα 4.36 : Γραφική Παράσταση Highest Difference-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και Highest Difference-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για 24 ώρες

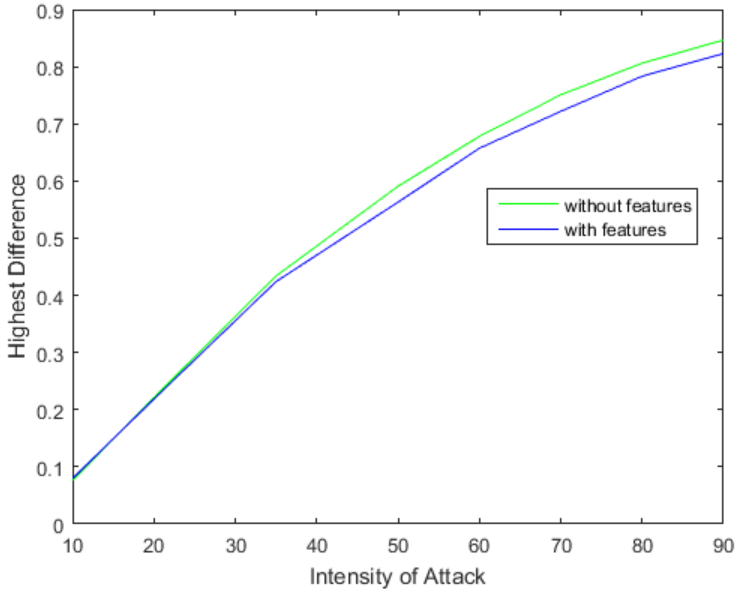
- <u>Αλλοίωση για τυχαίο διάστημα από 10 έως 24 ώρες στο ημερήσιο διάνυσμα</u>



Σχήμα 4.37 : Γραφική Παράσταση TPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και TPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για διάστημα 10-24 ωρών

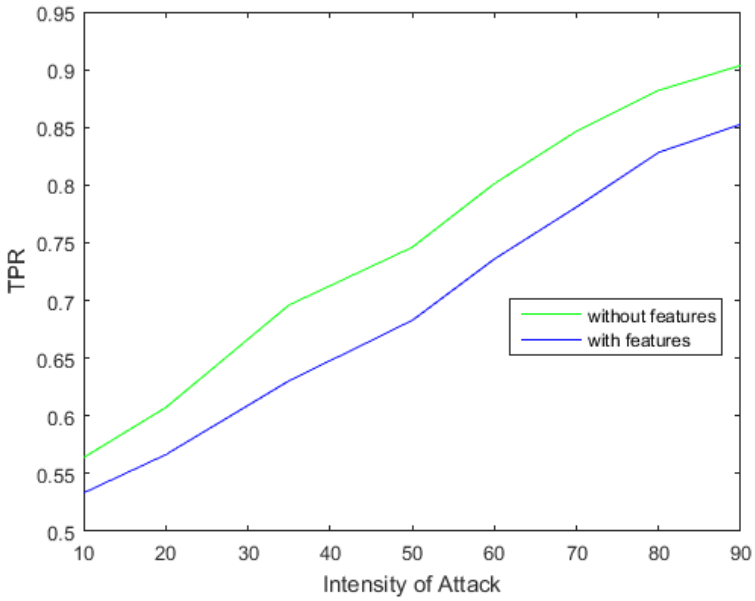


Σχήμα 4.38 : Γραφική Παράσταση FPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και FPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για διάστημα 10-24 ωρών

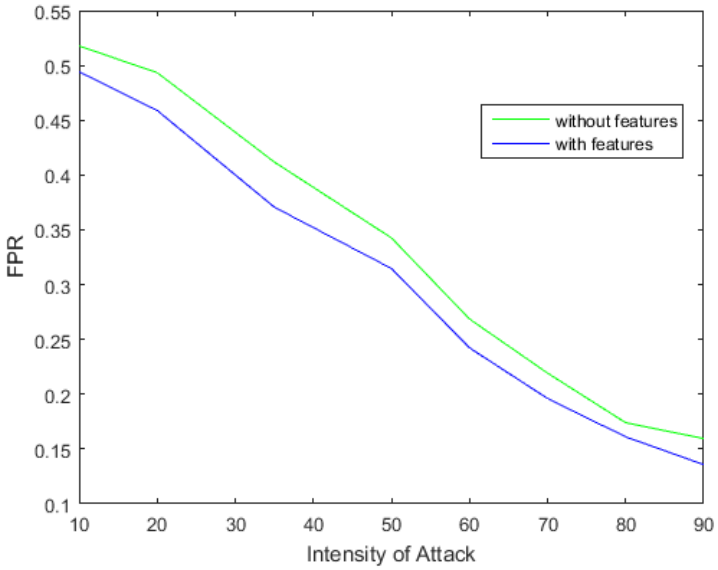


Σχήμα 4.39 : Γραφική Παράσταση Highest Difference-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και Highest Difference-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για διάστημα 10-24 ωρών

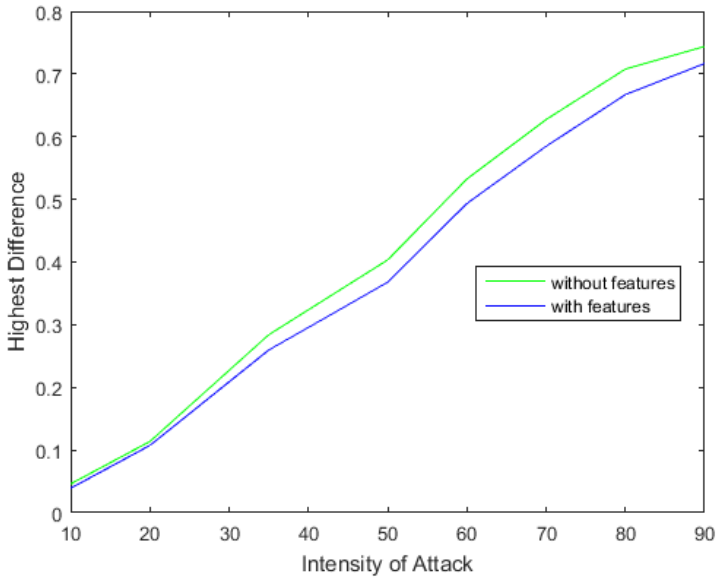
- <u>Αλλοίωση για τυχαίο διάστημα 10 ωρών στο ημερήσιο διάνυσμα</u>



Σχήμα 4.40 : Γραφική Παράσταση TPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και TPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για σταθερό διάστημα 10 ωρών

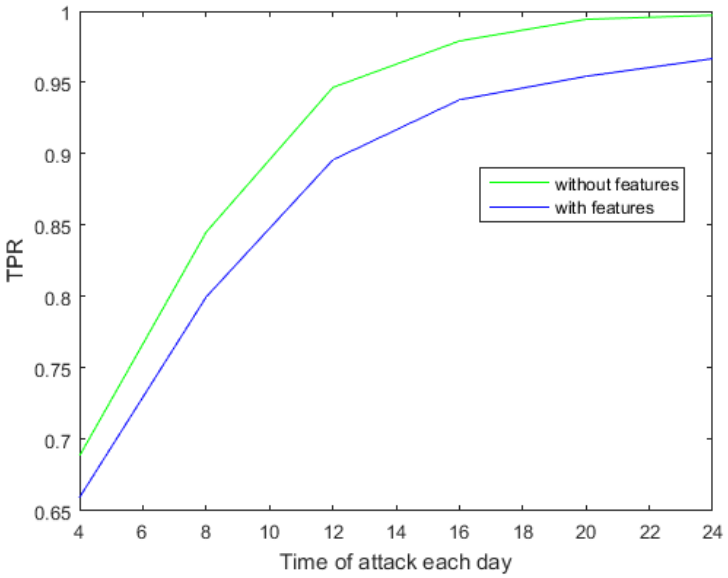


Σχήμα 4.41 : Γραφική Παράσταση FPR-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και FPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για σταθερό διάστημα 10 ωρών

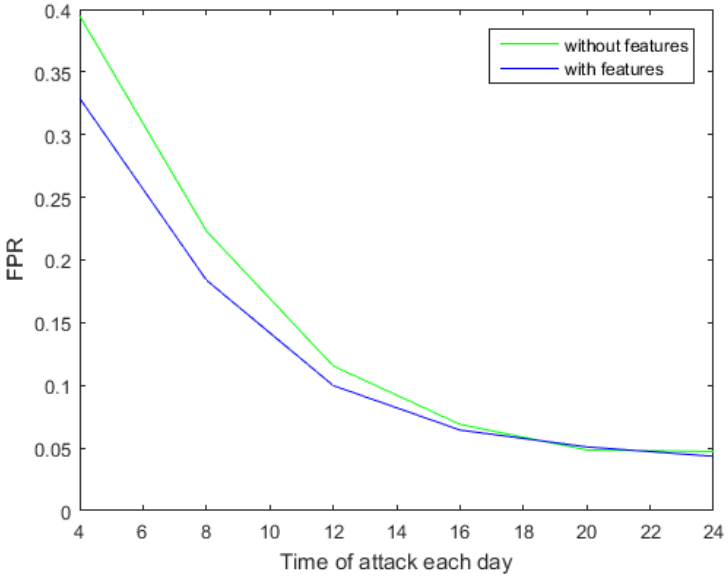


Σχήμα 4.42 : Γραφική Παράσταση Highest Difference-Intensity of Attack χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και Highest Difference-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε), για σταθερό διάστημα 10 ωρών

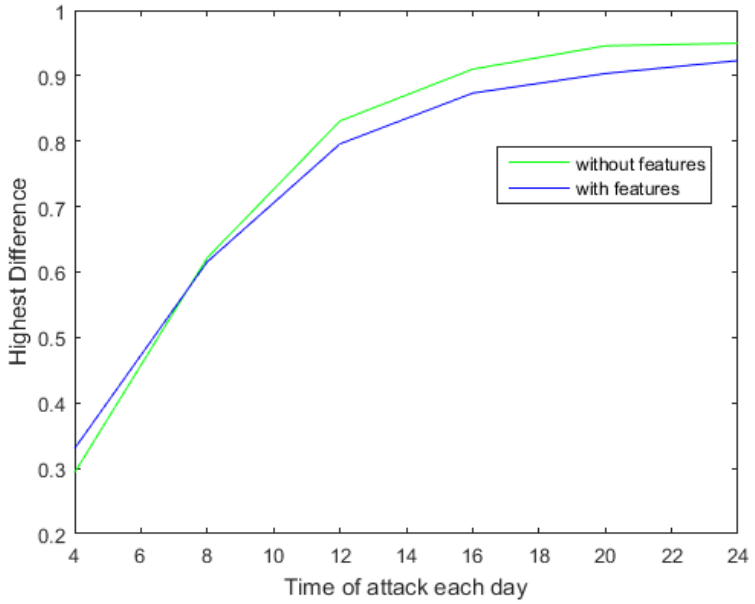
Στην συνέχεια, συγκρίνονται τα αποτελέσματα για ένα σταθερό τύπο επίθεσης, συγκεκριμένα έντονης επίθεσης, της τάξης του 90%, για διάφορες ώρες. Οι ώρες που επιλέχθηκαν να εφαρμοστεί επίθεση ήταν 4, 8, 12, 16, 20 και τέλος, 24 ώρες. Οι παρακάτω γραφικές δείχνουν την μεταβολή των δεικτών ταξινόμησης δεδομένων μετρήσεων κατανάλωσης και δεδομένων με εξαγωγή χαρακτηριστικών βάσει των αρχικών.



Σχήμα 4.43 : Γραφική Παράσταση TPR-Time of attack each day χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και TPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε)



Σχήμα 4.44 : Γραφική Παράσταση FPR-Time of attack each day χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και FPR-Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε)



Σχήμα 4.45 : Γραφική Παράσταση Highest Difference -Time of attack each day χωρίς εξαγωγή χαρακτηριστικών (πράσινο) και Highest Difference -Intensity of Attack με εξαγωγή χαρακτηριστικών (μπλε)

- <u>Σχόλια και Συμπεράσματα</u>

Σύμφωνα με τα αποτελέσματα των παραπάνω ταξινομήσεων προκύπτουν ορισμένα συμπεράσματα σχετικά με τις ταξινομήσεις με χαρακτηριστικά τις μετρήσεις κατανάλωσης και με χαρακτηριστικά τα στατιστικά στοιχεία αυτών. Προκύπτει ότι και οι δύο μέθοδοι λειτουργούν με τον ίδιο τρόπο. Δηλαδή, η ταξινόμηση έχει υψηλή ακρίβεια, χαμηλό ποσοστό ψευδώς θετικών ταξινομήσεων (FPR) και υψηλό ποσοστό αληθώς θετικών ταξινομήσεων (TPR) σε ισχυρές επιθέσεις, οι οποίες είναι εύκολα ανιχνεύσιμες και διαχωρίσιμες. Αντιθέτως, σε περιπτώσεις ήπιων επιθέσεων ο ταξινομητής δεν διαχωρίζει καλά τις ημέρες με απάτη και εκείνες χωρίς απάτη. Η ένταση της επίθεσης αφορά τόσο τον παράγοντα αλλοίωσης των δεδομένων όσο και τη χρονική διάρκεια εφαρμογής της. Ωστόσο, υπάρχουν διαφοροποιήσεις στις δύο μεθόδους. Η ταξινόμηση χωρίς στατιστικά χαρακτηριστικά δίνει ποσοστό αληθώς θετικών ενδείξεων περίπου, κατά 5% καλύτερα από την ταξινόμηση με χαρακτηριστικά, δηλαδή ανιχνεύει κατά 5% καλύτερα τις ημέρες με απάτη. Η διαφορά αυτή, του 5%, παρατηρείται σε όλες τις περιπτώσεις μελέτης. Από την άλλη, ο δείκτης των ψευδώς θετικών ταξινομήσεων προκύπτει χειρότερος κατά 3-5% στην ταξινόμηση χωρίς χαρακτηριστικά έναντι εκείνης με εξαγωγή χαρακτηριστικών. Αυτό σημαίνει ότι ο ταξινομητής δεν ανίχνευσε επιτυχώς τις ημέρες χωρίς απάτη και τις ταξινόμησε λανθασμένα ως ημέρες με απάτη, κατά 3-5% έναντι τις μεθόδου με χαρακτηριστικά. Ωστόσο, ο δείκτης Highest Difference, δηλαδή η διαφορά TPR και FPR, παρατηρείται να είναι

σχεδόν ίσος στις δύο περιπτώσεις. Δηλαδή, η διαφορά των μεταβολών στο τέλος είναι η ίδια.

Από τις δύο μεθόδους ταξινόμησης, εκείνη χωρίς εξαγωγή χαρακτηριστικών ανίχνευσε καλύτερα τις ημέρες με απάτη, ενώ απέδωσε χειρότερα στην ανίχνευση των ημερών χωρίς απάτη και λανθασμένα τις ταξινόμησε με απάτη. Η επιλογή χαρακτηριστικών, όπως μέση τιμή, τυπική απόκλιση, ασυμμετρία, κύρτωση, αιχμή, συνολική ζήτηση και η επίδραση κάθε περιόδου στο ημερήσιο διάνυσμα, παρατηρείται ότι βοήθησε ώστε να μοντελοποιηθεί καλύτερα το πρότυπο κατανάλωσης μιας ημέρας και να ανιχνευθούν οι ημέρες χωρίς απάτη. Ωστόσο, στις ημέρες που εφαρμόστηκε απάτη, τα στατιστικά μεγέθη δεν βοήθησαν στην ακριβέστερη διατύπωση του προτύπου. Επομένως, οι συνολικές αποδόσεις των ταξινομητών συγκλίνουν, αλλά επιλέγεται η περίπτωση χωρίς εξαγωγή χαρακτηριστικών, αφού ανιχνεύει περισσότερες μέρες απάτης, και δίνει μεγαλύτερο Highest Difference για ισχυρές επιθέσεις.

Η τεχνική με εξαγωγή κατάλληλων χαρακτηριστικών μπορεί να βελτιωθεί με την εισαγωγή επιπλέον στατιστικών ποσοτήτων για καλύτερη αναγνώριση των προτύπων κατανάλωσης.

4.9 Μελέτη σε 5000 καταναλωτές

Σε αυτή την παράγραφο γίνεται ανάλυση δεδομένων για ανίχνευση απάτης σε 5000 καταναλωτές. Ο αρχικός όγκος δεδομένων περιελάμβανε το συγκεκριμένο ποσό καταναλωτών. Επιλέγεται ρεαλιστικό σενάριο επίθεσης και εξάγονται τα αντίστοιχα αποτελέσματα όπως περιγράφεται παρακάτω.

4.9.1 Περίπτωση επίθεσης

Η πρώτη δοκιμή επίθεσης αφορά μια έντονη επίθεση, της τάξης του 90% των δεδομένων και σε 24 ώρες μέσα στη μέρα. Όπως διαπιστώθηκε σε προηγούμενες ενότητες προσδοκάται μια καλή απόδοση του αλγόριθμου ταξινόμησης. Τα αποτελέσματα της μελέτης φαίνονται στον Πίνακα 4.35 και στον Πίνακα 4.36.

Πίνακας 4.35 : Περίπτωση έντονης επίθεσης, της τάξης του 90% των δεδομένων για 5000 καταναλωτές

Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
97,67	4,41	99,78	97,91	95,37

- **Confusion Matrix**

Πίνακας 4.36 : Confusion Matrix για απάτη 24 ωρών στο 90% για 5000 καταναλωτές

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	275441	12775
Πραγματική τάξη=1	646	287841

Στη συνέχεια, αναλύεται ένα ρεαλιστικό σενάριο επίθεσης, δηλαδή ο παράγοντας αλλοίωσης να ακολουθεί μια κατανομή. Συγκεκριμένα, η κατανομή που επιλέχθηκε ήταν κατανομή βήτα έντονων επιθέσεων και εφαρμογή σε 24 ώρες μέσα στη μέρα. Ακόμα, ο παράγοντας αλλοίωσης είναι διαφορετικός για κάθε καταναλωτή αλλά σταθερός στον καθένα ως προς τις ημέρες και τις ώρες εφαρμογής. Τα αποτελέσματα της ταξινόμησης φαίνονται στον Πίνακα 4. 37 και Πίνακα 4.38.

Πίνακας 4.37 : Περίπτωση επίθεσης από κατανομή βήτα για 5000 καταναλωτές

Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
94,18	8,65	97,05	94,59	88,4

- **Confusion Matrix**

Πίνακας 4.38 : Confusion matrix επίθεσης από κατανομή βήτα για 5000 καταναλωτές

	Προβλεπόμενη τάξη=0	Προβλεπόμενη τάξη=1
Πραγματική τάξη=0	263368	24998
Πραγματική τάξη=1	8540	279797

Τέλος, από την τελευταία μελέτη εξήχθησαν χαρακτηριστικά και προέκυψαν τα ακόλουθα αποτελέσματα.

Πίνακας 4.39 : Περίπτωση επίθεσης από κατανομή βήτα για 5000 καταναλωτές με εξαγωγή χαρακτηριστικών

Accuracy(%)	FPR(%)	TPR(%)	F1 (%)	HD(%)
92,87	7,47	93,29	91,99	85,82

4.9.2 Σχόλια και συμπεράσματα από την μελέτη 5000 καταναλωτών

Στην ενότητα 4.8 μελετήθηκε η ανάλυση 5000 καταναλωτών για ανίχνευση απάτης, δηλαδή όλο το σύνολο καταναλωτών που ήταν διαθέσιμο. Τα αποτελέσματα ήταν αναμενόμενα, δηλαδή για έντονη επίθεση η ταξινόμηση πραγματοποιείται ικανοποιητικά, ομοίως και για περίπτωση επίθεσης από κάποια κατανομή. Ύστερα, γίνεται μελέτη με εξαγωγή χαρακτηριστικών και τα συμπεράσματα συμπίπτουν με την ανάλυση που έγινε για το μικρότερο σύνολο των 1000 καταναλωτών.

Κεφάλαιο
5
Συμπεράσματα και Βελτιωτικές Προτάσεις

5.1 Συμπεράσματα

Στο τέταρτο κεφάλαιο παρουσιάζονται τα αποτελέσματα της ταξινόμησης διαφόρων περιπτώσεων απάτης σύμφωνα με τον βαθμό αλλοίωσης. Ο βαθμός αλλοίωσης αναφερόταν στην ένταση της επίθεσης, δηλαδή στην τιμή του παράγοντα αλλοίωσης, στην χρονική διάρκεια εφαρμογής επίθεσης, στον συνδυασμό τύπων επίθεσης και στις περιπτώσεις διαφορετικής επίθεσης στο δείγμα εκπαίδευσης του αλγόριθμου και στο δείγμα δοκιμής. Τέλος, αφού εξετάστηκαν οι δοκιμές, αυτές σε 1000 καταναλωτές, εφαρμόζονται ρεαλιστικά σενάρια για 5000 καταναλωτές. Η διαδικασία ανάλυσης, η οποία ακολουθήθηκε και σύμφωνα με την οποία κατασκευάστηκε ο αλγόριθμος για την εκπόνηση της εργασίας, παρουσιάζεται στο τρίτο κεφάλαιο. Η διαδικασία αυτή, ξεκινάει από την διαχείριση των δεδομένων, όπως την μείωση του όγκου κάνοντας τις ημίωρες μετρήσεις σε ωριαίες για βελτίωση της υπολογιστικής πολυπλοκότητας. Στην συνέχεια, κάθε καταναλωτής αντιπροσωπεύεται από έναν ετήσιο πίνακα στο οποίο κάθε γραμμή αναφέρεται σε ημερήσιο διάνυσμα και στο τέλος του πίνακα προστίθεται μία στήλη με τιμές «0» και «1», δείχνοντας με «0» τα ημερήσια διανύσματα που δεν έχουν αλλοιωθεί λόγω απάτης και με «1» εκείνα με απάτη. Γίνεται προσομοίωση απάτης στα αρχικά δεδομένα με δειγματοληπτική επιλογή των ημερών και σε αριθμό τον μισό του συνόλου δεδομένων κάθε καταναλωτή. Ύστερα, από αυτό το βήμα χωρίζεται ο κάθε πίνακας, έτσι ώστε το 70% να αναφέρεται στο δείγμα εκπαίδευσης του μοντέλου ταξινόμησης και το υπόλοιπο 30% στο δείγμα δοκιμής. Αφού γίνει βελτιστοποίηση των παραμέτρων του ταξινομητή SVM στα δείγματα εκπαίδευσης και στην συνέχεια εκπαιδευτεί το μοντέλο, ακολουθεί η δοκιμή του ταξινομητή στα νέα δεδομένα, εξάγοντας αποτελέσματα από τους πίνακες σύγχυσης(Confusion Matrices), σύμφωνα με τους οποίους προκύπτουν οι δείκτες ακρίβειας(Accuracy, F1-Score) και τα ποσοστά αληθών και ψευδών ενδείξεων απάτης (TPR,FPR, ,HD).

Η ταξινόμηση με μηχανές διανυσμάτων υποστήριξης (SVM) και συγκεκριμένα του δυαδικού SVM έχει στόχο να διαχωρίσει όσο τον δυνατόν καλύτερα τα δεδομένα στις δύο τάξεις. Αρχικά, γίνεται δοκιμή κλοπής στο 90% των δεδομένων για διάφορες ώρες μες στην ημέρα, οι οποίες ήταν 24, άρα όλο το ημερήσιο διάνυσμα, τυχαίες από 10 έως 24 ώρες και 10 ώρες. Ύστερα, έγινε η ίδια ανάλυση σε επίθεση στο 50% και 20% των δεδομένων. Ακόμα, χρησιμοποιήθηκαν

παράγοντες αλλοίωσης που ακολούθησαν γνωστές κατανομές, όπως βήτα, κανονική και τυχαία. Αυτό, το οποίο αξίζει να σημειωθεί ως συμπέρασμα είναι το γεγονός ότι όσο πιο έντονη είναι η επίθεση και όσες περισσότερες ώρες μέσα στην ημέρα εφαρμόζεται, τόσο πιο αποδοτικά λειτουργεί ο ταξινομητής. Ενώ αντίθετα, όσο πιο ήπιες είναι οι επιθέσεις, άρα τα αλλοιωμένα δεδομένα πλησιάζουν σαν πρότυπα τα γνήσια, τόσο πιο δύσκολα ο ταξινομητής συγκλίνει στον διαχωρισμό των δύο τάξεων, με αποτελέσματα χειρότερη απόδοση. Ο ταξινομητής, επομένως, λειτουργεί σωστά και η απόδοσή του εξαρτάται κάθε φορά από τον τύπο της επίθεσης.

Όπως αποδείχθηκε από τις δοκιμές εφαρμογής απάτης σε διάφορες ώρες στο ημερήσιο διάνυσμα, οι επιθέσεις από 18 έως 24 ώρες ανιχνεύονται με παρόμοια ακρίβεια και ο αλγόριθμος ταξινόμησης σταθεροποιείται στην απόδοσή του. Αρκεί, δηλαδή, η μελέτη μίας απάτης που διενεργείται για τουλάχιστον 18 ώρες μέσα στη μέρα για να δώσει ικανοποιητική ακρίβεια.

Δεδομένου, ότι η ταξινόμηση παρουσιάζει καλύτερα αποτελέσματα σε έντονες επιθέσεις και διαχωρίζει τις δύο τάξεις, όταν το δείγμα εκπαίδευσης αποτελείται από ισχυρές επιθέσεις, αδυνατεί να ταξινομήσει αποδοτικά δείγμα δοκιμής ασθενέστερων επιθέσεων. Αντιθέτως, όταν το δείγμα εκπαίδευσης αποτελείται από μετρήσεις με μικρό βαθμό αλλοίωσης, τότε ο ταξινομητής σε δείγμα δοκιμής ισχυρών επιθέσεων μπορεί να διαγνώσει καλύτερα τις ημέρες που διαφοροποιούνται από τις γνήσιες/απαραβίαστες ημέρες.

Η ταξινόμηση με εξαγωγή στατιστικών χαρακτηριστικών, όπως η μέση ισχύς, η τυπική απόκλιση, η επίδραση της μέσης ζήτησης κάθε περιόδου μέσα στη ημέρα, η συνολική κατανάλωση και η αιχμή της ημέρας, αποδίδει παρόμοια με την ταξινόμηση καθαρών μετρήσεων κατανάλωσης. Ωστόσο, από αναλυτική σύγκριση των δύο μεθόδων επιλέγεται εκείνη στην οποία δεν εξάγονται χαρακτηριστικά.

Τέλος, σε κάθε είδους ταξινόμηση χρειάζεται η μελέτη του κάθε καταναλωτή, ώστε να μην περιέχει μειωμένες μετρήσεις από το σύνολο ή μηδενικές μετρήσεις για μεγάλο χρονικό διάστημα, το οποίο μπορεί να μην είναι αποτέλεσμα δόλιων επεμβάσεων. Σε αυτή την περίπτωση η ταξινόμηση δεν παρουσιάζει τα προσδοκώμενα αποτελέσματα. Η καλύτερη αντιμετώπιση του προβλήματος αυτών των καταναλωτών είναι να ξεχωρίζονται και να αντιμετωπίζονται σαν ειδική κατηγορία για περαιτέρω ανάλυση.

5.2 Βελτιωτικές Προτάσεις

Καταλήγοντας, η διαδικασία ανάλυσης των δεδομένων έξυπνων μετρητών για ανίχνευση απάτης μπορεί να επεκταθεί σε επιπλέον τρόπους διαχείρισης των

δεδομένων. Ως επέκταση της ανάλυσης που πραγματοποιήθηκε απορρέουν τα εξής ζητήματα για μελλοντική διερεύνηση:

- **Εφαρμογή Multi-Class SVM:** Στην εργασία χρησιμοποιήθηκε ο αλγόριθμος ταξινόμησης SVM με διαχωρισμό δύο τάξεων: η τάξη επίθεσης και η τάξη χωρίς επίθεση. Αντί αυτού, θα μπορούσε να χρησιμοποιηθεί ο αλγόριθμος Multi-Class SVM, σύμφωνα με τον οποίο γίνεται διαχωρισμός των δεδομένων στην τάξη χωρίς επίθεση και στις τάξεις διαφόρων τύπων επιθέσεων. Σε αυτήν την περίπτωση η κάθε ξεχωριστή τάξη επίθεσης αναφέρεται σε έναν συγκεκριμένο βαθμό αλλοίωσης των δεδομένων.

- **Εφαρμογή One-class SVM:** Η ταξινόμηση με One-class SVM, λειτουργεί με εκπαίδευση του αλγόριθμου μόνο σε γνήσια δεδομένα και δοκιμάζεται σε δεδομένα γνήσια και δεδομένα με απάτη. Έτσι, το αποτέλεσμα της ταξινόμησης αφορά το κατά πόσο ο αλγόριθμος ανίχνευσε την τάξη, στην οποία εκπαιδεύτηκε και όποια άλλη προέκυψε, θεωρήθηκε ως ανίχνευση ανωμαλίας (outliers).

- **Εφαρμογή κατηγοριοποίησης(clustering):** Σε αυτή την εφαρμογή, θα μπορούσε να χρησιμοποιηθεί ο αλγόριθμος Fuccy C-Means clustering. Σύμφωνα με τον αλγόριθμο αυτό, πριν την ταξινόμηση των δεδομένων γίνεται μια κατηγοριοποίηση τους σε ομάδες ανάλογα με τα πρότυπα κατανάλωσης που παρουσιάζουν. Τα δεδομένα μπορούν να ομαδοποιηθούν ανάλογα της χρήσης ενέργειας του κάθε καταναλωτή, για παράδειγμα, ομάδα κατοικιών, επιχειρήσεων, βιομηχανιών. Η ομαδοποίηση βασίζεται στην εποχικότητα, στην ζήτηση των καθημερινών και σαββατοκύριακων, καθώς και στα διάφορα διαστήματα της ημέρας. Σε αυτή τη μελέτη αποτελεί σημαντική διαδικασία η εξαγωγή κατάλληλων χαρακτηριστικών.

- **Εφαρμογή ταξινόμησης σε καταναλωτές:** Στην εργασία έγινε ανάλυση για ανίχνευση απάτης σε ημερήσια διανύσματα καταναλωτών και η είσοδος του ταξινομητή ήταν ο ετήσιος πίνακας του καθένα. Ενδιαφέρον αποτελεί η μελέτη ταξινόμησης σε ετήσια διανύσματα καταναλωτών. Δηλαδή, η είσοδος του SVM να αποτελεί πίνακες, των οποίων στις γραμμές (τα δείγματα προς ταξινόμηση) είναι οι καταναλωτές και στις στήλες είναι η ωριαίες μετρήσεις τους για ενάμιση χρόνο. Έτσι, ο αλγόριθμος ταξινόμησης καλείται να διαχωρίσει τους καταναλωτές, που διαπράττουν απάτη και τους τίμιους. Σε αυτή την περίπτωση, μπορεί να εφαρμοστεί και η κατηγοριοποίηση όπως αναφέρθηκε, Multi-class SVM και One-class SVM, καθώς επίσης η εξαγωγή κατάλληλων στατιστικών χαρακτηριστικών για μείωση του όγκου των μετρήσεων, λαμβάνοντας υπόψη την εποχικότητα, τις ώρες και τις ημέρες αιχμής ζήτησης σε όλη την διάρκεια του χρόνου.

Βιβλιογραφία

1. Depuru, Soma Shekara Sreenadh Reddy, Lingfeng Wang, and Vijay Devabhaktuni. "Smart meters for power grid: Challenges, issues, advantages and status." *Renewable and sustainable energy reviews* 15.6 (2011): 2736-2742.

2. Yan, Ye, Yi Qian, and Hamid Sharif. "A secure and reliable in-network collaborative communication scheme for advanced metering infrastructure in smart grid." *2011 IEEE Wireless Communications and Networking Conference*. IEEE, 2011.

3. McDaniel, Patrick, and Stephen McLaughlin. "Security and privacy challenges in the smart grid." *IEEE Security and Privacy* 7.3 (2009): 75-77.

4. Jiang, Rong, et al. "Energy-theft detection issues for advanced metering infrastructure in smart grid." *Tsinghua Science and Technology* 19.2 (2014): 105-120.

5. McLaughlin, Stephen, Dmitry Podkuiko, and Patrick McDaniel. "Energy theft in the advanced metering infrastructure." *International Workshop on Critical Information Infrastructures Security*. Springer Berlin Heidelberg, 2009.

6. King, Chris S. "The economics of real-time and time-of-use pricing for residential consumers." *American Energy Institute, Tech. Rep* (2001).

7. IEE Report, UTILITY-SCALE SMART METER DEPLOYMENTS, PLANS, & PROPOSALS http://www.edisonfoundation.net/iee/documents/iee_smartmeterrollouts_0512.pdf

8. Navani, J. P., N. K. Sharma, and Sonal Sapra. "Technical and non-technical losses in power system and its economic consequence in Indian economy."*International Journal of Electronics and Computer Science Engineering* 1.2 (2012): 757-761.

9. Salinas, Sergio, Ming Li, and Pan Li. "Privacy-preserving energy theft detection in smart grids: A P2P computing approach." *IEEE Journal on Selected Areas in Communications* 31.9 (2013): 257-267.

10. Depuru, Soma Shekara Sreenadh Reddy, Lingfeng Wang, and Vijay Devabhaktuni. "Electricity theft: Overview, issues, prevention and a smart meter based approach to control theft." *Energy Policy* 39.2 (2011): 1007-1015.

11. Secure, interoperable functionality for power line carrier based infrastructure http://www.ee.co.za/article/secure-interoperable-functionality-power-line-carrier-based-infrastructures.html

12. Pyasi, Aditya, and Vishal Verma. "Improvement in electricity distribution efficiency to mitigate pollution IEEE ISEE (May 2008)." *2008 IEEE International Symposium on Electronics and the Environment*. IEEE, 2008.

13. Antmann, Pedro. "Reducing technical and non-technical losses in the power sector." *Background paper for the WBG Energy Strategy* (2009).

14. Lu, Rongxing, et al. "Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications." *IEEE Transactions on Parallel and Distributed Systems* 23.9 (2012): 1621-1631.

15. Begovic, Miroslav, et al. "Impact of distribution efficiency on generation and voltage stability." *System Sciences, 2000. Proceedings of the 33rd Annual Hawaii International Conference on*. IEEE, 2000.

16. Industrial Control Systems Security
http://siis.cse.psu.edu/smartgrid.html

17. McLaughlin, Stephen, et al. "A multi-sensor energy theft detection framework for advanced metering infrastructures." *IEEE Journal on Selected Areas in Communications* 31.7 (2013): 1319-1330.

18. Hearst, Marti A., et al. "Support vector machines." *IEEE Intelligent Systems and their Applications* 13.4 (1998): 18-28.

19. Vapnik, Vladimir Naumovich, and Vlamimir Vapnik. *Statistical learning theory*. Vol. 1. New York: Wiley, 1998.

20. Nagi, J., et al. "Detection of abnormalities and electricity theft using genetic support vector machines." *TENCON 2008-2008 IEEE Region 10 Conference*. IEEE, 2008.

21. Genetic Algorithms
https://en.wikipedia.org/wiki/Genetic_algorithm

22. Muniz, Cyro, et al. "Irregularity detection on low tension electric installations by neural network ensembles." *2009 International Joint Conference on Neural Networks*. IEEE, 2009.

23. Mashima, Daisuke, and Alvaro A. Cárdenas. "Evaluating electricity theft detectors in smart grid networks." *International Workshop on Recent Advances in Intrusion Detection*. Springer Berlin Heidelberg, 2012.

24. Jokar, Paria, Nasim Arianpoo, and Victor CM Leung. "Electricity theft detection in AMI using customers' consumption patterns." *IEEE Transactions on Smart Grid* 7.1 (2016): 216-226.

25. Khoo, Benjamin, and Ye Cheng. "Using RFID for anti-theft in a Chinese electrical supply company: A cost-benefit analysis." *Wireless Telecommunications Symposium (WTS), 2011*. IEEE, 2011.

26. Xiao, Zhifeng, Yang Xiao, and David Hung-Chang Du. "Non-repudiation in neighborhood area networks for smart grid." *IEEE Communications Magazine*51.1 (2013): 18-26.

27. Liu, Ting, et al. "A novel method to detect bad data injection attack in smart grid." *INFOCOM, 2013 Proceedings IEEE*. IEEE, 2013.

28. Huang, Shih-Che, Yuan-Liang Lo, and Chan-Nan Lu. "Non-technical loss detection using state estimation and analysis of variance." *IEEE Transactions on Power Systems* 28.3 (2013): 2959-2966.

29. Amin, Saurabh, Galina A. Schwartz, and Hamidou Tembine. "Incentives and security in electricity distribution networks." *International Conference on Decision and Game Theory for Security*. Springer Berlin Heidelberg, 2012.

30. Jindal, Anish, et al. "Decision Tree and SVM-Based Data Analytics for Theft Detection in Smart Grid." *IEEE Transactions on Industrial Informatics* 12.3 (2016): 1005-1016.

31. Hybrid decision tree-SVM model https://www.researchgate.net/figure/222527188_fig3_Figure-3-Hybrid-decision-tree-SVM-model

32. Haykin, Simon S., et al. *Neural networks and learning machines*. Vol. 3. Upper Saddle River, NJ, USA:: Pearson, 2009.

33. Nagi, Jawad, et al. "Nontechnical loss detection for metered customers in power utility using support vector machines." *IEEE transactions on Power Delivery* 25.2 (2010): 1162-1171.

34. Cristianini, Nello, and John Shawe-Taylor. *An introduction to support vector machines and other kernel-based learning methods*. Cambridge university press, 2000.

35. Vapnik, Vladimir. *The nature of statistical learning theory*. Springer Science & Business Media, 2013.

36. Oskoei, Mohammadreza Asghari, and Huosheng Hu. "Support vector machine-based classification scheme for myoelectric control applied to upper limb."*IEEE transactions on biomedical engineering* 55.8 (2008): 1956-1965.

37. Hyperplane through two linearly separable classes http://cse-wiki.unl.edu/wiki/index.php/Support_Vector_Machines

38. Chang, Chih-Chung, and Chih-Jen Lin. "LIBSVM: a library for support vector machines." *ACM Transactions on Intelligent Systems and Technology (TIST)*2.3 (2011): 27.

39. https://en.wikipedia.org/wiki/Confusion_matrix

40. Machine Learning-Confusion Matrix https://computersciencesource.wordpress.com/2010/01/07/year-2-machine-learning-confusion-matrix/

41. Receiver Operating Characteristic
https://en.wikipedia.org/wiki/Receiver_operating_characteristic

42. The Receiver Operating Characteristic(ROC) Curve
http://crsouza.com/2009/12/discriminatory-power-analysis-by-receiver-operating-characteristic-curves-part-1-of-2-theory/

43. Swets, John A. "Measuring the accuracy of diagnostic systems." *Science*240.4857 (1988): 1285-1293.

44. ROC Graph
http://www2.cs.uregina.ca/~dbd/cs831/notes/ROC/ROC.html

45. Data Mining(Computer Science)
https://www.britannica.com/technology/data-mining

46. K-fold Cross-Validation
http://scriptslines.com/blog/k-fold-cross-validation/

47. Data from the Commission for Energy Regulation
https://www.ucd.ie/issda/data/commissionforenergyregulationcer/

48. Han, Jiawei, Jian Pei, and Micheline Kamber. *Data mining: concepts and techniques*. Elsevier, 2011.

49. Feature extraction
https://en.wikipedia.org/wiki/Feature_extraction

50. Cross Validation
https://en.wikipedia.org/wiki/Cross-validation_(statistics)#k-fold_cross-validation

51. Beta Distribution
http://www.ntrand.com/beta-distribution/

52. The normal distribution
https://wiki.uiowa.edu/display/bstat/The+Normal+Distribution

53. Haben, Stephen, Colin Singleton, and Peter Grindrod. "Analysis and clustering of residential customers energy behavioral demand using smart meter data."*IEEE Transactions on Smart Grid* 7.1 (2016): 136-144.

54. Xing, Zhengzheng, Jian Pei, and Eamonn Keogh. "A brief survey on sequence classification." *ACM SIGKDD Explorations Newsletter* 12.1 (2010): 40-48.

55. Κονταξής, Γ., and Ν. Χατζηαργυρίου. "Κέντρα Ελέγχου Ενέργειας." *Αθήνα: Εκδόσεις ΕΜΠ* (2003): 26-32