Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών

Μεταπτυχιακό Πρόγραμμα Σπουδών
Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

Ανίχνευση μη εξουσιοδοτημένων εξερχόμενων κλήσεων VoIP σε πραγματικό χρόνο

Παναγιώτης Παναγιώτου

Επιβλέπων Καθηγητής
Δρ. Σταύρος Σιαηλής

Μάιος 2017

Ανοικτό Πανεπιστήμιο Κύπρου

Σχολή Θετικών και Εφαρμοσμένων Επιστημών
Μεταπτυχιακό Πρόγραμμα Σπουδών

Πληροφοριακά και Επικοινωνιακά Συστήματα

Μεταπτυχιακή Διατριβή

Ανίχνευση μη εξουσιοδοτημένων εξερχόμενων κλήσεων VoIP σε πραγματικό χρόνο

Παναγιώτης Παναγιώτου

Επιβλέπων Καθηγητής
Δρ. Σταύρος Σιαηλής

Η παρούσα μεταπτυχιακή διατριβή υποβλήθηκε προς μερική εκπλήρωση των απαιτήσεων για απόκτηση μεταπτυχιακού τίτλου σπουδών στα Πληροφοριακά και Επικοινωνιακά Συστήματα από τη Σχολή Θετικών και Εφαρμοσμένων Επιστημών του Ανοικτού Πανεπιστημίου Κύπρου.

Μάιος 2017

Περίληψη

Οι κλήσεις απάτης σε VoIP υπηρεσίες αποτελούν ένα μεγάλο πρόβλημα στις εταιρίες τηλεπικοινωνιών, αφού τους επιφέρουν ζημίες εκατομμυρίων ευρώ. Παρά το γεγονός ότι τα συστήματα ασφαλείας των εταιριών έχουν αναπτυχθεί αρκετά, παρουσιάζεται μεγάλη δυσκολία στον εντοπισμό των κακόβουλων χρηστών στα δίκτυα τηλεφωνίας VoIP. Έτσι, στην παρούσα εργασία αποφασίσαμε να δώσουμε έμφαση στον εντοπισμό των κλήσεων απάτης (fraud calls), οι οποίες είναι κλήσεις που γίνονται από τρίτους χωρίς τη γνώση του νομίμου διαχειριστή της υπηρεσίας.

Ο στόχος της παρούσας μεταπτυχιακής εργασίας είναι η έρευνα του κατά πόσο είναι δυνατό με τη χρήση Τεχνητής Νοημοσύνης να εντοπίσουμε και να αντιμετωπίσουμε άμεσα τις κλήσεις απάτης σε ένα δίκτυο τηλεφωνίας VoIP μεγάλης εταιρίας τηλεπικοινωνιών της Κύπρου.

Για τον εντοπισμό των κλήσεων απάτης δημιουργήσαμε μια εφαρμογή χρησιμοποιώντας τον αλγόριθμο μη εποπτείας (unsupervise) ESOINN. Η εφαρμογή προσαρμόστηκε κατάλληλα στα δεδομένα τηλεφωνικών κλήσεων CDRs που μας παρείχε μεγάλη εταιρία τηλεπικοινωνιών της Κύπρου. Υλοποιήθηκαν τρία σενάρια πιθανών κλήσεων απάτης. Ο αλγόριθμος δεν ανταποκρίθηκε στις προσδοκίες μας, αφού δεν έχει το επιθυμητό ποσοστό επιτυχίας. Και στα τρία σενάρια που υλοποιήσαμε το ποσοστό επιτυχίας στον εντοπισμό των κλήσεων απάτης παρέμεινε στο 66,66%. Παρόλ' αυτά, είναι ένας γρήγορος αλγόριθμος ο οποίος με μια περαιτέρω έρευνα και επεξεργασία των δεδομένων θα μπορούσε να δώσει καλύτερα αποτελέσματα για τον εντοπισμό κλήσεων απάτης.

Λέξεις κλειδιά: Κλήσεις απάτης, VoIP, ESOINN, Τεχνητή Νοημοσύνη, Μηχανή Μάθησης.

Summary

Fraud voice calls to VoIP services are a major problem for telecommunication companies since they cause the loss of millions euros. Although company security systems have been developed quite a bit, there is a great deal of difficulty in detecting malicious users on a VoIP telephony network. That way, in this work we have decided to focus on identifying fraud calls, which are calls made by a third party without the knowledge of the legal manager of the service.

This master dissertation aim is to investigate whether it is possible with the use of Artificial Intelligence to detect and deal directly with fraud calls in a VoIP telephony network of a large telecommunications company in Cyprus.

To detect fraud calls, we have created an application using the ESOINN unsupervised algorithm. The application was appropriately adapted to the CDRs telephone data that were provided by a large telecommunication operator in Cyprus. Three scenarios of possible fraud calls have been implemented. The algorithm did not meet our expectations, since it did not have the desired success rate, in all three scenarios we implemented the success rate in detecting fraud calls remained at 66.66%. However, it is a fast algorithm which under further research and processing of data could provide better results in detecting fraud calls.

Key words: Fraud calls, VoIP, ESOINN, Artificial Intelligence, Lear

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον Υπεύθυνο Καθηγητή μου Δρ. Σταύρο Σιαηλή για την καθοδήγηση την οποία μου παρείχε, ώστε να επιτευχθεί η ολοκλήρωση και η παράδοση της παρούσας μεταπτυχιακής διατριβής.

Τέλος, θα ήθελα να εκφράσω τις θερμές μου ευχαριστίες προς την οικογένεια και τους φίλους μου, για την θερμή τους συμπαράσταση καθ' όλη τη διάρκεια διεκπεραίωσης της παρούσας μεταπτυχιακής διατριβής.

Περιεχόμενα

Κεφάλαιο 1 Εισαγωγή 1
1.1 Σκοπός και Στόχος της Διατριβής 1
1.1.1 Σκοπός 1
1.1.2 Στόχος 2
1.2 Μεθοδολογία και Περιγραφή Κεφαλαίου 2
1.2.1 Μεθοδολογία 2
1.2.2 Περιγραφή Κεφαλαίων 2

Κεφάλαιο 2 VoIP - Μηχανές Μάθησης 3
2.1 Εισαγωγή στην VoIP 3
2.1.1 Δίκτυα VoIP 3
2.1.2 Αρχιτεκτονική πρωτοκόλλων VoIP 4
2.1.3 Πρωτόκολλα 4
2.1.5 Ασφάλεια συστημάτων VoIP 18
2.2 Machine Learning - Μηχανές Μάθησης 34
2.2.1 Τι είναι Μηχανική Μάθηση; 34
2.2.2 Κατηγορίες μηχανισμών μάθησης 35

Κεφάλαιο 3 Βιβλιογραφική Ανασκόπηση 39

Κεφάλαιο 4 Μεθοδολογία 46
4.1 Τεχνητά Νευρωνικά Δίκτυα 46
4.2 SOM - Self-organizing map 49
4.3 SOINN - Self-Organizing Incremental Neural Networks 52
4.4 ESOINN - Enhanced Self-Organizing Incremental Neural Networks 55

Κεφάλαιο 5 Εφαρμογή Ανίχνευσης Κλήσεων Απάτης 60
5.1 Εισαγωγή 60
5.2 Εργαλεία για την υλοποίηση της εφαρμογής 61

5.3 Λειτουργία εφαρμογής 62
5.3.1 Ανάκτηση και επεξεργασία των Δεδομένων 62
Επεξεργασία Δεδομένων 64
5.3.2 Κανονικοποίηση(Normalize) 67
5.3.3 Λειτουργία ESOINN 72
Κεφάλαιο 6 Εκπαίδευση – Αποτελέσματα –Συμπεράσματα 74
6.1 Εκπαίδευση αλγόριθμου 74
6.2 Πειραματική Διαδικασία 75
6.3 Αποτελέσματα 76
6.4 Συμπεράσματα 79

Κεφάλαιο 7 Επίλογος 82
7.1 Μελλοντική Δουλειά 83

Βιβλιογραφία 84

Εικόνες

Εικόνα 2.1 Ροή μιας κλήσης μεταξύ δύο τερματικών σημείων 5
Εικόνα 2.2 Cisco PGW2200 6
Εικόνα 2.3 Οικογένεια πρωτοκόλλων 8
Εικόνα 2.4 Ευπάθειες του VOIP 8
Εικόνα 2.5 Πηγές και αιτίες των ευαίσθητων σημείων 13
Εικόνα 2.6 Επίθεση DOS 13
Εικόνα 2.7 Registration Hijacking 15
Εικόνα 2.8 Επιθέσεις Proxy Impersonation 16
Εικόνα 2.9 Man-In-The-middle επίθεση 17
Εικόνα 2.10 DTLS απώλεια πακέτου και αναμετάδοση 23
Εικόνα 2.11 Εφαρμογή του IPSec σε ένα SIP περιβάλλον 25
Εικόνα 2.12 Κλειδί αυθεντικοποίησης δρομολογημένο από τον gatekeeper 29
Εικόνα 2.13 Αυθεντικοποίηση του H.235.6 RTP για το antispam 31
Εικόνα 2.14 Τοποθέτηση πύλης ασφαλείας 34
Εικόνα 2.15 Γραφική παράσταση αλγόριθμου επιτηρούμενης μάθησης 36
Εικόνα 2.16 Επιτηρούμενη Μάθηση για φιλτράρισμα spam email 36
Εικόνα 2.17 Γραφική παράσταση αλγόριθμου επιτηρούμενης μάθησης 37
Εικόνα 2.18 Τρόπος λειτουργίας ενισχυτικής μάθησης 38
Εικόνα 4.1 Σχηματική αναπαράσταση του ενός νευρώνα 47
Εικόνα 4.2 Παράδειγμα νευρωνικού δικτύου 47
Εικόνα 4.3 Αρχιτεκτονική του νευρωνικού δικτύου SOM 50
Εικόνα 4.4 Πλέγματα SOM 51
Εικόνα 4.5 Τρόπος εκμάθησης των δύο επιπέδων στον SOINN 52
Εικόνα 4.6 Διάγραμμα ροής της διαδικασίας μάθησης SOINN 53
Εικόνα 4.7 Διάγραμμα ροής του ESOINN 55
Εικόνα 4.8 Υπολογισμός απόστασης ενός κόμβου από τους γείτονες 57
Εικόνα 4.9 Υπολογισμός σημείου του κόμβου 58
Εικόνα 4.10 Υπολογισμός συσσωρευμένου σημείου 58
Εικόνα 4.11 Υπολογισμός μέσων συσσωρευμένων σημείων (πυκνότητα) 59
Εικόνα 5.1 Eclipse Luna 61
Εικόνα 5.2 Καταγραφή της ώρας που τρέχει η εφαρμογή 62
Εικόνα 5.3 Αποθήκευση Δεδομένων σε Λίστα 63
Εικόνα 5.4 Table Destination 64
Εικόνα 5.5 Έλεγχος για εντοπισμό του κωδικού της χώρας όπου πραγματοποιείται η κλήση 65
Εικόνα 5.6. Έλεγχος της ώρας κλήσης και ενίσχυση της τιμής 66
Εικόνα 5.7 Έλεγχος της διάρκειας της κλήσης και ενίσχυση της τιμής 66
Εικόνα 5.8 Αποθήκευση χαρακτηριστικών της κλήσης σε λίστα 67
Εικόνα 5.9 Μαθηματικός τύπος κανονικοποίησης δεδομένων 69

Εικόνα 5.10 κανονικοποίηση δεδομένων 69
Εικόνα 5.11 Αποθήκευση κανονικοποιημένων δεδομένων και κλήσεων αλγόριθμου 70
Εικόνα 5.12 Αρχείο με κανονικοποιημένες τιμές 71
Εικόνα 5.13 Κάλεσμα από τον αλγόριθμο του αρχείου του χρήστη που εξετάζουμε 72
Εικόνα 5.14 Συσταδοποίηση και δημιουργία νέου αρχείου με το αποτέλεσμα 72
Εικόνα 5.15 Αποτελέσμα του ESOINN σε txt file 73

Πίνακες

Πίνακας 2.1 Συστάσεις ασφαλείας 28
Πίνακας 6.1 Αποτελέσματα 1ου σεναρίου 76
Πίνακας 6.2 Αποτελέσματα 2ου σεναρίου 77
Πίνακας 6.3 Αποτελέσματα 3ου σεναρίου 78
Πίνακας 6.4 Συγκεντρωτικά αποτελέσματα 79
Πίνακας 6.5 Σύγκριση αποτελεσμάτων 79

Γραφήματα

Γράφημα 6.1 Αποτελέσματα εκπαίδευσης ESOINN 75

Κεφάλαιο 1 Εισαγωγή

1.1 Σκοπός και Στόχος της Διατριβής

1.1.1 Σκοπός

Η VoIP τεχνολογία είναι ένας τρόπος επικοινωνίας σε πραγματικό χρόνο που έχει φέρει καινοτόμες αλλαγές στον τομέα των τηλεπικοινωνιών. Με την πάροδο του χρόνου οι παραδοσιακές τηλεφωνικές γραμμές αποσύρονται σταδιακά, καθώς οι επιχειρήσεις και τα νοικοκυριά παγκοσμίως αποδέχονται τα οφέλη και τις υπηρεσίες που τους προσφέρει η VoIP τεχνολογία. Η VoIP τεχνολογία γίνεται συχνά στόχος κακόβουλων χρηστών, οι οποίοι προσπαθούν να εισχωρήσουν στα συστήματα VoIP και να τα εκμεταλλευτούν.

Οι πάροχοι τηλεπικοινωνιακών υπηρεσιών είναι δύσκολο να ανακαλύψουν αν υπάρχουν κακόβουλοι χρήστες που χρησιμοποιούν την τηλεφωνική γραμμή του πελάτη τους. Ο εντοπισμός μπορεί να γίνει μετά από καιρό και συνήθως μετά από παράπονα του χρήστη για χρεώσεις σε κλήσεις που δεν έχει κάνει. Από τη στιγμή που είναι δύσκολος ο εντοπισμός του εισβολέα στη VoIP, έχει δοθεί έμφαση στον εντοπισμό των κλήσεων απάτης. Σύμφωνα με την CFCA (Communications Fraud Control Association), το οικονομικό κόστος των κλήσεων απάτης παγκοσμίως για το 2015 ανέρχονταν στα $38.1 δισεκατομμύρια δολάρια. Ποσό που είναι μειωμένο κατά 18% σε σχέση με το 2013, αλλά δεν παύει να είναι πολύ μεγάλο. [CFCA, 2016]

Η παρούσα διατριβή έχει σκοπό να σχεδιάσει και να υλοποιήσει ένα λογισμικό σύστημα ανίχνευσης και καταστολής των μη εξουσιοδοτημένων κλήσεων, μέσω της τεχνολογίας VoIP (Voice Over IP), με τη χρήση CDR(Call Detail Record) και άλλων εργαλείων ανοιχτού κώδικα. Το προσδοκώμενο αποτέλεσμα είναι να σχεδιάσουμε ένα λογισμικό σύστημα που να μπορεί να δημιουργεί ένα προφίλ για κάθε χρήστη της υπηρεσίας VoIP, συλλέγοντας πληροφορίες για το πού τηλεφωνά και σε περίπτωση που εντοπιστεί κάποια ύποπτη κλήση που να μη συμβαδίζει με το προφίλ του χρήστη, να διακόπτεται από το σύστημα.

1.1.2 Στόχος

Ο στόχος της μεταπτυχιακής αυτής εργασίας είναι ο όσο το δυνατόν πιο αποτελεσματικός και άμεσος εντοπισμός των κλήσεων απάτης στο δίκτυο τηλεφωνίας VoIP σε μία μεγάλη εταιρία τηλεπικοινωνιών της Κύπρου. Για τον σκοπό αυτό προτείνεται μια μεθοδολογία για συλλογή και ανάλυση των δεδομένων από τα CDRs της εταιρίας, με τη χρήση του αλγόριθμου τεχνητής νοημοσύνης ESOINN (ενισχυμένα αυτό-οργανωμένα αυξητικά νευρωνικά δίκτυα). Για την υλοποίηση της μεθοδολογίας που ακολουθήθηκε, χρησιμοποιήσαμε τη γλώσσα προγραμματισμού Java με σκοπό την εξαγωγή συμπερασμάτων.

1.2 Μεθοδολογία και Περιγραφή Κεφαλαίου

1.2.1 Μεθοδολογία

Για την υλοποίηση της εφαρμογής χρησιμοποιήσαμε τα CDRs 2 μηνών μεγάλης εταιρίας τηλεπικοινωνιών της Κύπρου. Με τη χρήση του αλγόριθμου εκμάθησης (learning algorithm) ESOINN και χρησιμοποιώντας τη γλώσσα προγραμματισμού Java σε περιβάλλον Eclipse Luna Release (4.4.0), αναλύσαμε τα χαρακτηριστικά που κρίναμε κατάλληλα από τα CDRs και δημιουργήσαμε ένα προφίλ για κάθε χρήστη της υπηρεσίας VoIP. Στη συνέχεια, συγκρίναμε τα χαρακτηριστικά κάθε κλήσης με το προφίλ του χρήστη. Η ομαδοποίηση των κλήσεων που έκανε ο αλγόριθμος μας έδωσε τη δυνατότητα να χαρακτηρίσουμε μια κλήση ως καλή ή ως πιθανή κλήση απάτης.

1.2.2 Περιγραφή Κεφαλαίων

Η παρούσα μεταπτυχιακή διατριβή χωρίζεται σε 7 κεφάλαια. Στο κεφάλαιο 2, αναλύουμε την τεχνολογία VoIP, καθώς και τις μηχανές μάθησης (machine learning). Ακολούθως στο κεφάλαιο 3, κάνουμε μια βιβλιογραφική ανασκόπηση σε σημαντικές έρευνες σχετικές με τον εντοπισμό των κλήσεων απάτης. Αναφέρουμε τις μεθόδους και τις διαδικασίες που χρησιμοποίησαν άλλοι ερευνητές. Στο κεφάλαιο 4, αναλύουμε τη μεθοδολογία που ακολουθήσαμε για τη δική μας πρόταση. Στο κεφάλαιο 5, περιγράφουμε την υλοποίηση της εφαρμογής. Στο κεφάλαιο 6, παραθέτουμε τα αποτελέσματα που προέκυψαν και τα συμπεράσματά μας και στην συνέχεια τα συγκρίνουμε με τα αποτελέσματα άλλων ερευνών. Τέλος στο κεφάλαιο 7, κάνουμε μια σύνοψη της έρευνας και προτείνουμε βήματα για μελλοντική βελτίωση της εφαρμογής που κάναμε.

Κεφάλαιο 2 VoIP - Μηχανές Μάθησης

2.1 Εισαγωγή στην VoIP

2.1.1 Δίκτυα VoIP

Υπάρχουν πολλοί τρόποι να υλοποιηθεί ένα VoIP δίκτυο. Μπορεί να υλοποιηθεί πάνω σε οποιοδήποτε IP δίκτυο όπως LAN, WLAN , WAN, δορυφορικό δίκτυο Internet. Ένα VoIP δίκτυο, μπορεί επίσης να διασυνδεθεί με δίκτυα PSTN (public switched telephone network), καθώς και με δίκτυα κινητής τηλεφωνίας. Τα στοιχεία που μπορούν να χρησιμοποιηθούν σε ένα δίκτυο VoIP είναι ποικίλα, όπως συμβατικά τηλέφωνα, ATA, gateways, gatekeepers, PBX και VoIP hard/ soft phones.

Η ATA (Analog Terminal Adapter) είναι συσκευή μέσω της οποίας μια συμβατική τηλεφωνική συσκευή μπορεί να συνδεθεί με ένα VoIP δίκτυο. Μετατρέπει το αναλογικό σήμα του τηλεφώνου σε VoIP κίνηση και αντίστροφα. Πρακτικά, ένα συμβατικό τηλέφωνο με ATA είναι το ίδιο λειτουργικό με ένα VoIP hard phone. Η ATA μερικές φορές αναφέρεται και ως gateway.

Τα VoIP hard phones είναι τερματικές τηλεφωνικές συσκευές με τις οποίες ο χρήστης μπορεί να επικοινωνήσει μέσω τεχνολογιών VoIP. Μπορεί να έχουν και τη μορφή λογισμικού (soft phones). Τα VoIP phones, ανάλογα με τις διεπαφές δικτύου που έχουν, μπορούν να συνδεθούν κατευθείαν στο αντίστοιχο δίκτυο (όπως Ethernet, WiFi).

Η επικοινωνία με τη βοήθεια του VoIP μπορεί να πραγματοποιηθεί είτε απ' ευθείας μεταξύ χρηστών VoIP τερματικών, είτε μεταξύ χρηστών συμβατικών τηλεφωνικών υπηρεσιών (σταθερών ή κινητών) και χρηστών VoIP τερματικών. Στην τελευταία περίπτωση, χρειάζεται και κάποιος πάροχος υπηρεσιών VoIP (VoIP service provider). Επίσης, πολλές εταιρίες παροχής τηλεφωνίας χρησιμοποιούν VoIP για τη μετάδοση της κίνησης μεταξύ των κέντρων τους (back bone δίκτυο), με τους χρήστες να χρησιμοποιούν συμβατικά τηλέφωνα και τηλεφωνικές γραμμές.[Ρενέση Ειρήνη, 2008]

2.1.2 Αρχιτεκτονική πρωτοκόλλων VoIP

Το VoIP, όπως υπονοεί το όνομά του, χρησιμοποιεί το Internet Protocol (IP) για τη μετάδοση φωνής. Αυτό σημαίνει πως χρειάζεται ως μέσο μετάδοσης οποιοδήποτε IP δίκτυο, ανεξαρτήτως των πρωτοκόλλων επιπέδου σύνδεσης δεδομένων και φυσικού επιπέδου. Δηλαδή, στο επίπεδο δικτύου χρησιμοποιείται πάντα το πρωτόκολλο IP, ενώ στα χαμηλότερα επίπεδα χρησιμοποιείται οποιοδήποτε πρωτόκολλο (Ethernet, WiFi κ.α.).

Στο επίπεδο μεταφοράς και συνόδου μπορεί να υπάρχουν διαφοροποιήσεις ανάλογα με την υλοποίηση. Η λειτουργία ενός συστήματος VoIP σε μια σύνοδο θα μπορούσε να χωριστεί σε δύο μέρη. Το πρώτο μέρος είναι η δημιουργία και μετάδοση πακέτων φωνής και το δεύτερο ο έλεγχος της κλήσης VoIP.

Για τη μετάδοση πακέτων φωνής, στη συντριπτική πλειοψηφία των εφαρμογών, χρησιμοποιείται το επίπεδο μεταφοράς RTP (Real time Transport Protocol) πάνω από το UDP (User Datagram Protocol). Τον Μάρτιο του 2006 προτάθηκε από τον οργανισμό IETF ένα νέο πρωτόκολλο, το DCCP (Datagram Congestion Control Protocol), που μπορεί να χρησιμοποιηθεί για τη μετάδοση πακέτων φωνής ενός VoIP συστήματος. Δεν υπάρχουν όμως ακόμη εμπορικές εφαρμογές που να το χρησιμοποιούν.

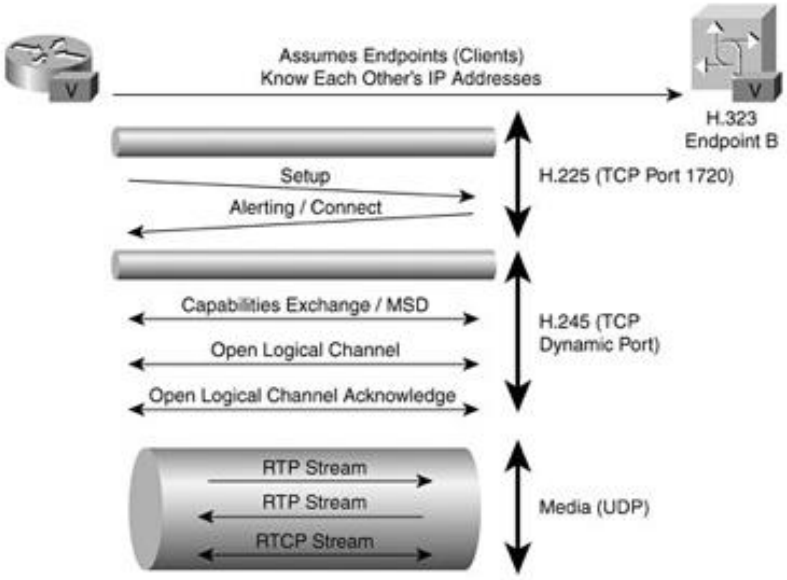
Για τον έλεγχο της κλήσης χρησιμοποιούνται πρωτόκολλα επιπέδου συνόδου τα οποία έχουν την ευθύνη για την αρχικοποίηση (call setup), την τροποποίηση και τον τερματισμό μιας VoIP κλήσης. Τα πιο διαδεδομένα πρωτόκολλα συνόδου είναι το SIP(Session Initiation Protocol), το σύνολο πρωτοκόλλων H.323 και το MEGACO/H.248. Αυτά τα πρωτόκολλα χρησιμοποιούν το TCP και το UDP στο επίπεδο μεταφοράς.[Ρενέση Ειρήνη, 2008]

2.1.3 Πρωτόκολλα

Τα κύρια VoIP πρωτόκολλα ελέγχου κλήσεων είναι το SIP, H.323, MGCP και H.248/MEGACO. Μια άλλη πολύ δημοφιλής επέκταση της VoIP τηλεφωνίας είναι το Peer to Peer (P2P), το οποίο χρησιμοποιείται από το Skype, όμως ακόμα δεν έχει επικυρωθεί ως πρότυπο τηλεφωνίας. Πιο κάτω θα αναλύσουμε εν συντομία τις διαφορές μεταξύ αυτών των πρωτοκόλλων ελέγχου κλήσεων.

H.323

Το H.323 είναι μια σύσταση ITU-T που ορίζει τον τρόπο με τον οποίο η πολυμεσική πληροφορία μεταφέρεται πάνω από δίκτυα πακέτων. Το H.323 χρησιμοποιεί υπάρχοντα πρότυπα, όπως το Q.931, για να επιτύχει τους στόχους του. Είναι ένα σύνθετο πρωτόκολλο, που δεν δημιουργήθηκε για την απλή ανάπτυξη εφαρμογών αλλά για να επιτρέψει στις εφαρμογές πολυμέσων να τρέξουν πάνω σε αναξιόπιστα δίκτυα δεδομένων. Η μεταφορά φωνής είναι μόνο μια από τις εφαρμογές για το H.323.

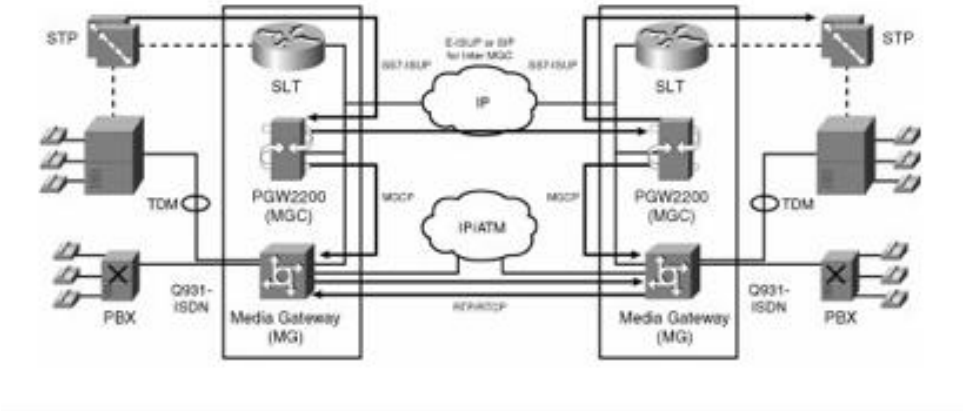


Εικόνα 2.1 Ροή μιας κλήσης μεταξύ δύο τερματικών σημείων.[Ρενέση Ειρήνη, 2008]

Οι εφαρμογές απαιτούν αρκετό κόπο εάν πρόκειται να κλιμακώνονται με το H.323. Παραδείγματος χάρη, για να ολοκληρωθεί μια μεταφορά κλήσης απαιτείται ένα ξεχωριστό πρότυπο (H.450.2). Τα SGCP και MGCP, όμως, μπορούν να ολοκληρώσουν μια μεταφορά κλήσης με μια απλή εντολή, γνωστή ως τροποποίηση της σύνδεσης (MDCX) στην πύλη ή το τερματικό σημείο.

MGCP (Evolution from SGCP and IPDC)

Τα SGCP και MGCP αναπτύχθηκαν για να επιτρέψουν σε μια κεντρική συσκευή, γνωστή ως Media Gateway Controller (MGC) ή softswitch, να ελέγξει τα τερματικά σημεία ή τις Media Gateways (MGs). Η ανάπτυξη εφαρμογών είναι δυνατή μέσω της χρήσης βασικών APIs, τα οποία διασυνδέονται με τα MGCs και προσφέρουν πρόσθετες λειτουργίες (όπως αναμονή κλήσης) και εφαρμογές.



Εικόνα 2.2 Cisco PGW2200. [Ρενέση Ειρήνη, 2008]

Η Cisco έκδοση αυτής της τεχνολογίας είναι περισσότερο γνωστή ως δύο διαφορετικά προϊόντα: Cisco PGW2200 και Cisco BTS10200. Το Cisco PGW2200, ο πράκτορας κλήσεων που περιγράφεται εδώ, αποτελείται από πολλά διαφορετικά στοιχεία όπως Cisco Media Gateway Controller (MGC), Cisco Signaling Link Terminals (SLT), διακόπτης LAN για την IP αλληλεπίδραση των στοιχείων του Cisco PGW2200 και ούτω καθεξής. Σ' αυτό το σενάριο, το ολόκληρο IP δίκτυο λειτουργεί σαν ένας μεγάλος εικονικός διακόπτης, με το PGW να ελέγχει όλα τα MGs. Το σχήμα 2.2 δείχνει πώς ένα τυπικό σχέδιο δικτύων λειτουργεί με έναν εικονικό διακόπτη που τρέχει MGCP.

Τα MGCs έχουν μια εσωτερική σύνδεση για να παρέχουν τις υπηρεσίες κλάσης. Τα MGCs λαμβάνουν σήματα από το SS7 δίκτυο και λένε στα MGs πότε να αρχικοποιήσουν τις IP συνδέσεις και ποια άλλα MGs πρέπει να κάνουν το ίδιο. [Ρενέση Ειρήνη, 2008]

SIP

Το SIP περιγράφεται καλύτερα από το RFC 3261, το οποίο είναι ένα πρωτόκολλο ελέγχου (σηματοδότησης) στο στρώμα εφαρμογών για τη δημιουργία, τροποποίηση, και τερματισμό των συνόδων με έναν ή περισσότερους συμμετέχοντες. Υπάρχουν όμως πολυάριθμα πρόσθετα RFCs, που αναπτύσσονται από την IETF κοινότητα, τα οποία συμπληρώνουν το βασικό RFC για να προσφέρουν νέα χαρακτηριστικά με το SIP να λειτουργεί ως πρωτόκολλο για έλεγχο της συνόδου στο VoIP, στα PacetCable Multimedia (PCMM) και στα ασύρματα βασισμένα στη τηλεφωνία δίκτυα επιχειρήσεων.

Οι SIP προσκλήσεις χρησιμοποιούνται για να δημιουργήσουν συνόδους και να μεταφέρουν περιγραφές της συνόδου που επιτρέπουν στους συμμετέχοντες να συμφωνήσουν σε ένα σύνολο συμβατών τύπων πολυμέσων. Το SIP εκμεταλλεύεται στοιχεία που αποκαλούνται proxy εξυπηρετητές για να βοηθήσει σε αιτήματα δρομολόγησης στην τρέχουσα τοποθεσία του χρήστη , στην επικύρωση και έγκριση χρηστών για πρόσβαση στις υπηρεσίες και στην εφαρμογή πολιτικών δρομολόγησης. [Ρενέση Ειρήνη, 2008]

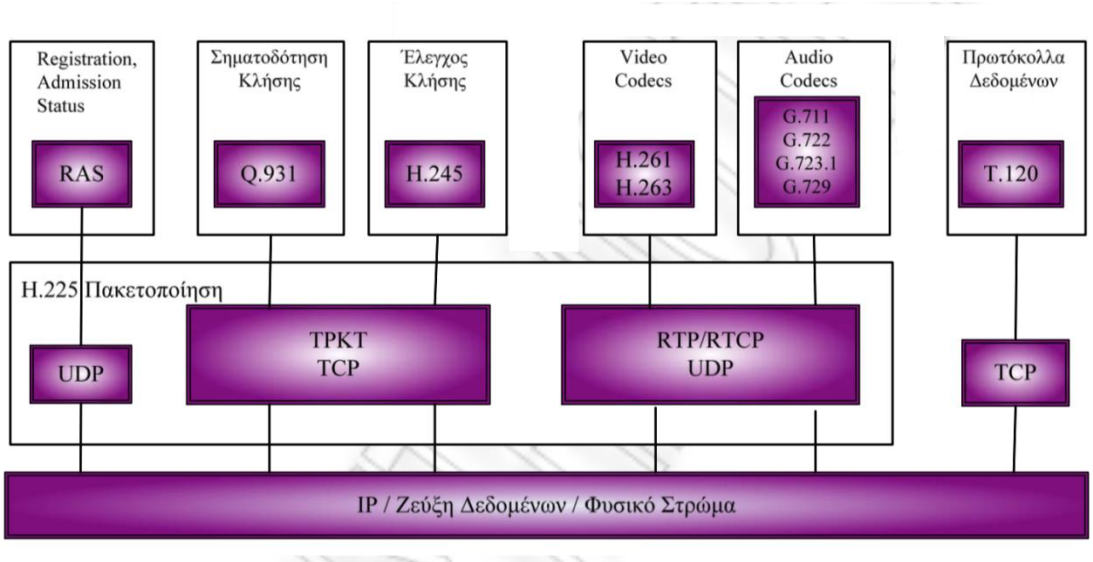
H.248/MEGACO

Το MGCP/MEGACO κατέρριψε το H.323 πρότυπο φύλαξης πυλών και αφαίρεσε τον έλεγχο σηματοδοσίας από τις πύλες, τοποθετώντας τον σε έναν πολυμεσικό ελεγκτή πυλών (MGC) ή softswitch. Αυτή η συσκευή θα έλεγχε πολλαπλές «πολυμεσικές πύλες». Αυτό ήταν μια αποσύνθεση της H.323 αρχιτεκτονικής σε SS7, δημιουργώντας νοημοσύνη σηματοδοσίας που θα μπορούσε να ενεργήσει ως peer στις SS7 οντότητες.

Στην αρχιτεκτονική MGCP/MEGACO, η νοημοσύνη αφαιρείται από τα πολυμέσα. Είναι ένα πρωτόκολλο αφέντη-σκλάβου (master-slave) όπου ο “αφέντης” έχει τον απόλυτο έλεγχο και ο “σκλάβος” εκτελεί απλά τις εντολές. Ο “αφέντης” είναι ο πολυμεσικός ελεγκτής πυλών, ή softswitch ή πράκτορας κλήσης και ο “σκλάβος” είναι η πύλη πολυμέσων [αυτή μπορεί να είναι μια πύλη VoIP, ένα DSLAM , ένας δρομολογητής Multiprotocol Label Switching (MPLS), ένα IP τηλέφωνο και ούτω καθεξής]. Αυτό είναι σε αντίθεση με την peer-to-peer φύση του SIP και άλλων προτύπων όπως το Skype, όπου ένας πελάτης μπορεί άμεσα να καθιερώσει μια σύνοδο με έναν άλλο πελάτη.

Το MEGACO δίνει εντολή στην πύλη πολυμέσων να συνδέσει τις ροές που προέρχονται έξω από ένα δίκτυο πακέτων σε μια ροή πακέτων όπως RTP. Η αρχιτεκτονική, εντούτοις, απαιτεί ως πρωτόκολλο για την επικοινωνία μεταξύ των ελεγκτών πυλών πολυμέσων (MGC) και το SIP. Τα συστατικά κλειδιά του MEGACO είναι τα ακόλουθα[Ρενέση Ειρήνη, 2008]:

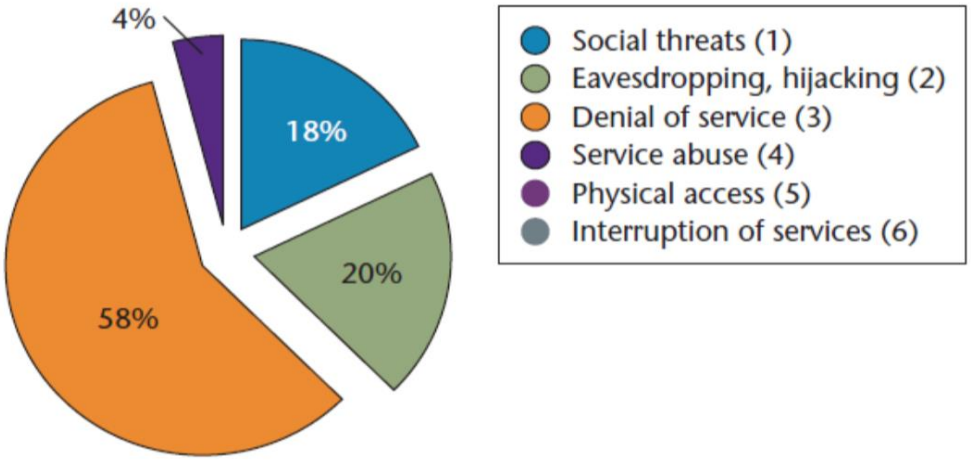
• Πύλη σηματοδοσίας (Signaling Gateway – SG)
• Ελεγκτής Πύλης Πολυμέσων (Media Gateway Control – MGC)
• Πύλη Πολυμέσων (Media Gateway – MG)



Εικόνα 2.3 Οικογένεια πρωτοκόλλων. [Φαφούλα Ιωάννα, 2008]

2.1.4 Επιθέσεις σε VoIP

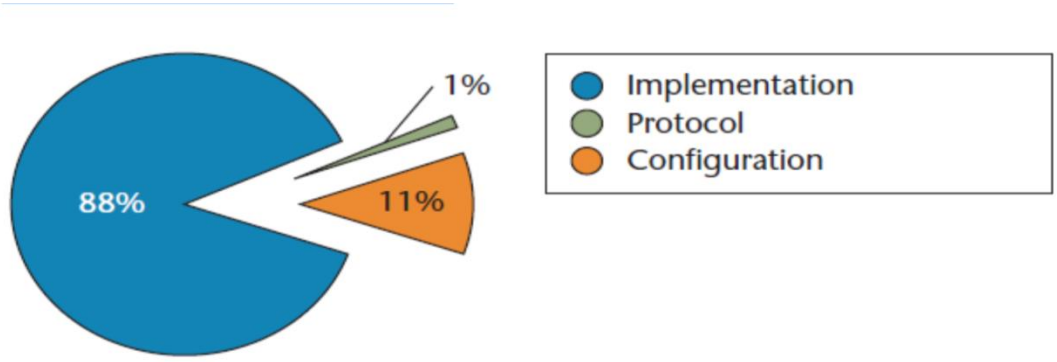
Υπάρχουν πολλών ειδών επιθέσεις VoIP που, σύμφωνα με έρευνα που έγινε στα πλαίσια του vampire project χρηματοδοτούμενο από το Γαλλικό Εθνικό Γραφείο Έρευνας (ANR) για την καλύτερη κατανόηση της ασφάλειας του VoIP, χωρίζονται σε έξι τύπους ευπάθειας. Οι τύποι ευπάθειας, όπως απεικονίζονται και στην πιο κάτω εικόνα, χρησιμοποίουν την ταξινόμηση του VoIP Security Alliance (VoIPSA). Παρατηρείται ότι τα περισσότερα προβλήματα αφορούν επιθέσεις denial of service (DoS), συνήθως μέσω του εξυπηρετητή ή του εξοπλισμού του χρήστη.



Εικόνα 2.4 Ευπάθειες του VOIP. [Αστέριος Αλμπανάκη, 2011]

Αν και πλέον θεωρητικά υπάρχει η γνώση για την προστασία των εφαρμογών του εξυπηρετητή, δεν είναι και τόσο σαφές το πώς μπορούν να προστατευτούν οι τελικές συσκευές. Την κατάσταση χειροτερεύει το γεγονός ότι σπάνια γίνεται αναβάθμιση του firmware του VoIP εξοπλισμού σε μη επιχειρηματικά περιβάλλοντα. Ακόμη ένα ενδιαφέρον συμπέρασμα που φαίνεται από την εικόνα 2.3 είναι ότι η παρακολούθηση της κυκλοφορίας (traffic eavesdropping) και η πειρατεία (hijacking) αποτελούν περίπου το 1/5 των απειλών. Πιο συγκεκριμένα, τα περισσότερα από τα πιο πάνω προβλήματα μπορεί να δίνουν τη δυνατότητα στους επιτιθέμενους για ανάλυση της κίνησης του δικτύου, μέσω της πρόσβασης στη συσκευή του χρήστη ή στο log του εξυπηρετητή, χωρίς όμως να τους επιτρέπουν άμεσα να ΄΄κρυφακούσουν΄΄ τις συνομιλίες.

Οι περισσότερες απειλές πηγάζουν από προβλήματα εφαρμογής, όπως φαίνεται και στην εικόνα 2.4. Παρόλ' αυτά το μεγαλύτερο πλήθος πηγών των ερωτήσεων προέρχεται από λάθος ρυθμίσεις, [όπως οι προεπιλεγμένες ρυθμίσεις (default settings) για το λογισμικό του διαχειριστή], από μη ασφαλείς και όχι καλά ρυθμισμένες υπηρεσίες που τρέχουν στην τελική συσκευή του χρήστη (όπως η εξ αποστάσεως πρόσβαση προγραμμάτων εντοπισμού σφαλμάτων σε VoIP συσκευές χωρίς authentication) αλλά και από πρόσβαση σε απαγορευμένες υπηρεσίες μέσω εναλλακτικών διεπαφών (Web front end). Επίσης, πρέπει να σημειωθεί ότι είναι λίγα τα ευαίσθητα σημεία πρωτοκόλλων που επιτρέπουν επιθέσεις DoS ή toll fraud. Τα προβλήματα αυτά αναφέρθηκαν πριν από λίγα χρόνια, γεγονός που προκαλεί έκπληξη, δεδομένου ότι τα πρότυπα (standards documents) έχουν δημοσιευτεί εδώ και πολύ καιρό. [Αστέριος Αλμπανάκης ,2011]



Εικόνα 2.5 Πηγές και αιτίες των ευαίσθητων σημείων. [Αστέριος Αλμπανάκη, 2011]

Είδη επιθέσεων

Πιο κάτω γίνεται αναφορά των κυριότερων επιθέσεων χρησιμοποιώντας την ταξινόμηση του VoIP Security Alliance (VoIPSA)

Κοινωνικές απειλές -Social Threats

SPIT

Το Voice Spam ή Spam over Internet Telephony (SPIT) είναι ένα πρόβλημα παρόμοιο με το email spam που όσο πάει επηρεάζει περισσότερο το VoIP. Με το SPIT εννοούμε τις μαζικές και ακούσιες κλήσεις που παράγονται αυτόματα. Να σημειώσουμε ότι οι κλασσικές τηλεφωνικές πωλήσεις δεν θεωρούνται SPIT.

Στις συνηθισμένες τηλεπωλήσεις χρησιμοποιούνται auto-dialers, οι οποίοι καλούν νούμερα μέχρι να σηκώσει το τηλέφωνο κάποιος. Τότε μεταφέρεται η γραμμή σε έναν εκπρόσωπο της εταιρίας ο οποίος άρχιζε την προσπάθεια του για να κάνει την πώληση. Αυτοί οι auto-dialers μπορούν και ξεχωρίζουν τη φωνή κάποιου που απαντά στην κλήση από τη φωνή που ακούγεται στο μήνυμα του αυτόματου τηλεφωνητή.

Οι απειλές SPIT είναι σαν τις τηλεπωλήσεις αλλά με μεγαλύτερη συχνότητα. Μπορούμε να τις συγκρίνουμε με την συχνότητα των spams.

Ένας σημαντικός τομέας που το SPIT υπερτερεί από τις τηλεπωλήσεις είναι το κόστος του. Για να λειτουργήσει ένα απλό τηλεφωνικό κέντρο που θα μπορεί να καλεί ταυτόχρονα 100 πιθανούς πελάτες και να έχει 10 τηλεφωνικές συσκευές σε περίπτωση που απαντήσει κάποιος το τηλεφώνημα, θα χρειαστεί ένα ανάλογο PBX. Στο SPIT, το κόστος αυτό μειώνεται δραματικά. Το κόστος για να στηθεί το PBX είναι μικρότερο, καθώς αντί για T1 γραμμές γίνεται χρήση ευρυζωνικών συνδέσεων. Έτσι δίνεται η δυνατότητα να γίνουν πολύ περισσότερες κλήσεις ταυτόχρονα. Οι κλήσεις αυτές πραγματοποιούνται αυτόματα. Ως εκ τούτου μειώνεται το προσωπικό, αφού δεν χρειάζεται να μιλήσει κάποιος από την εταιρία στην αρχή (όπως γίνεται με τις τηλεπωλήσεις) αλλά μόνο όταν ενδιαφέρεται ο υποψήφιος πελάτης. Ένας ακόμη λόγος είναι η μικρή χρέωση των VoIP κλήσεων και των πακέτων που προσφέρουν οι εταιρίες παροχής υπηρεσιών VoIP, το κόστος παραμένει χαμηλό.[Αστέριος Αλμπανάκης ,2011]

Υποκλοπές

Σε αυτό το είδος των επιθέσεων χρησιμοποιούνται εργαλεία σύλληψης και ανάλυσης της κίνησης του δικτύου, όπως το Ethereal, για να κάνει sniffing στα μηνύματα σηματοδοσίας και τα πολυμεσικά ρεύματα (media streams) σε μια συνομιλία. Τα συλληφθέντα RTP πακέτα που ανταλλάσσονται από τα UDP ή TCP πρωτόκολλα αποκωδικοποιούνται και μετατρέπονται σε αρχεία ήχου. Πιο κάτω γίνεται αναφορά στη διαδικασία που ακολουθείται για τη σύλληψη και την αποκωδικοποίηση των πακέτων φωνής:

- Πρώτα παραλαμβάνονται και αποκωδικοποιούνται τα πακέτα RTP.
- Έπειτα, η σύνοδος αναλύεται με την επιλογή ενός ρεύματος προς ανάλυση και επανασυναρμολόγηση με το κατάλληλο εργαλείο ανάλυσης.
- Και στο τέλος, το ρεύμα μετατρέπετε σε αρχείο ήχου.

Οι 4 βασικές επιθέσεις υποκλοπής είναι οι:

- Sniffing του αρχείου διαμόρφωσης TFTP.
- Number harvesting.
- Call pattern tracking
- Conversation eavesdropping.

Για να πραγματοποιηθούν αυτές οι επιθέσεις, ο κακόβουλος χρήστης χρειάζεται πρόσβαση στο σημείο του δικτύου που βρίσκεται η VoIP κίνηση. Αυτό μπορεί να γίνει από παντού, από ένα τελικό σημείο VoIP (υπολογιστή με softphone ή τηλέφωνο) μέχρι και μέσω πρόσβασης στο VoIP proxy/gateway μέσω ασύρματου δικτύου.

Sniffing του αρχείου διαμόρφωσης TFTP

Το πρωτόκολλο Trivial File Transfer Protocol (TFTP) είναι ένα πολύ απλό πρωτόκολλο που χρησιμοποιείται για τη μεταφορά αρχείων μέσω του Διαδικτύου. Δεδομένου ότι είναι πολύ απλό, η ποσότητα μνήμης που χρειάζεται για να λειτουργήσει είναι μικρή. Αυτό είναι πολύ σημαντικό για την εποχή που εμφανίστηκε, διότι η μνήμη των υπολογιστών τότε ήταν ιδιαιτέρως περιορισμένη. Το TFTP χρησιμοποιήθηκε κυρίως για την έναρξη (booting) διαφόρων δρομολογητών (routers), οι οποίοι δεν είχαν σκληρούς δίσκους ή δισκέτες για να αποθηκεύσουν το λειτουργικό σύστημα. Σήμερα χρησιμοποιείται για τη μεταφορά μικρών αρχείων μεταξύ των υπολογιστών ενός δικτύου. Τα περισσότερα IP τηλέφωνα βασίζονται σε ένα εξυπηρετητή TFTP για να κατεβάσουν το αρχείο ρυθμίσεων για την ενεργοποίηση τους. Συνήθως αυτό περιέχει κωδικούς για να συνδεθεί απευθείας το τηλέφωνο (με telnet, web interface κ.α.) και να το διαχειριστεί ο εκάστοτε χρήστης του. Ο

επιτιθέμενος παρακολουθεί την κίνηση. Όταν ένα τηλέφωνο κατεβάζει αυτό το αρχείο μπορεί να έχει πρόσβαση σε αυτούς τους κωδικούς έτσι ώστε να ρυθμίσει εκ νέου και να ελέγξει το IP τηλέφωνο.

Number Harvesting

Ο επιτιθέμενος παρακολουθεί παθητικά τις εισερχόμενες και εξερχόμενες κλήσεις του χρήστη και δημιουργεί μια βάση δεδομένων με τους τηλεφωνικούς αριθμούς. Αυτή η βάση μπορεί να χρησιμοποιηθεί για πιο προχωρημένες επιθέσεις VoIP, όπως τον χειρισμό σηματοδότησης (Signaling manipulation).

Call Pattern Tracking

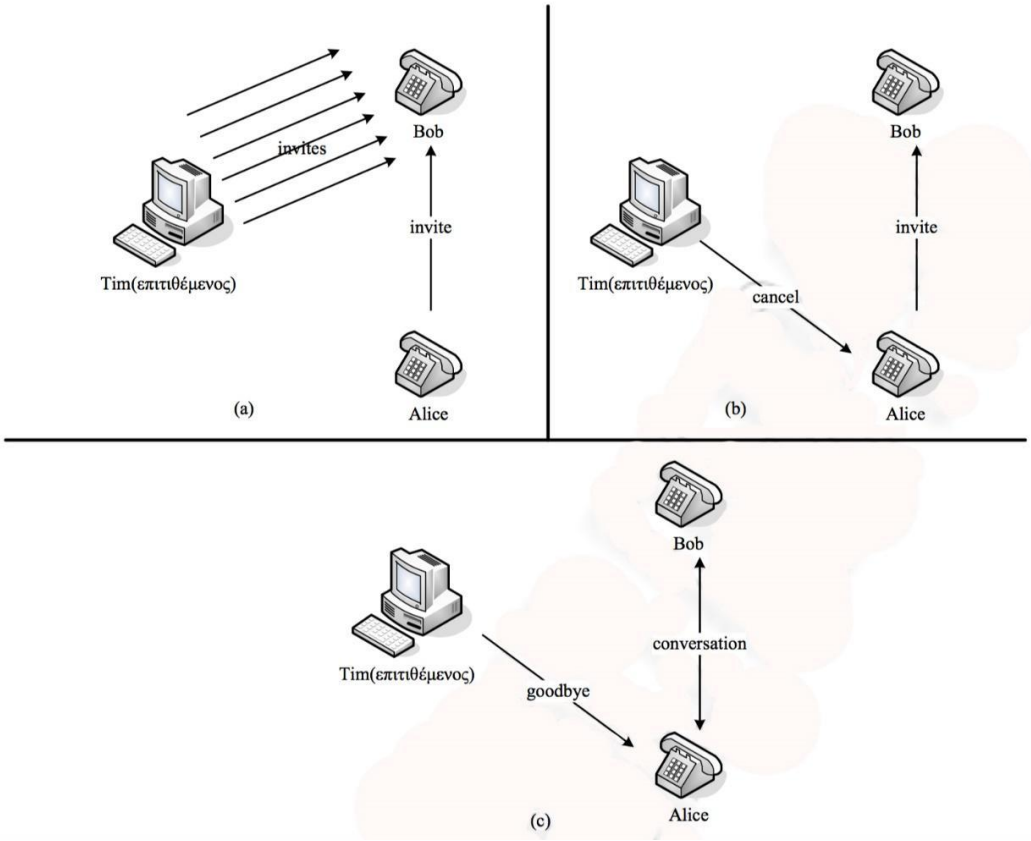
Η συγκεκριμένη επίθεση πάει ένα βήμα παραπέρα από το number harvesting, για να εντοπίσει ποιος μιλάει με ποιόν, ακόμα και αν η συνομιλία είναι σε κρυπτογραφημένη μορφή. Εφαρμόζεται στην επιβολή του νόμου, αν καταφέρουν να αναγνωριστούν εγκληματικές ενέργειες. Μέσω αυτής της επίθεσης ο κακόβουλος χρήστης είναι σαν να υποκλέπτει την αναλυτική κατάσταση κλήσεων του κινητού τηλεφώνου ενός προσώπου.

Conversation Eavesdropping and Analysis

Η επίθεση αυτή περιγράφει έναν επιτιθέμενο ο οποίος ηχογραφεί έναν ή και τους δύο συνομιλητές σε μια συνομιλία. Πέρα από ότι μπορεί απλά να ακούσει τη συνομιλία, μπορεί επίσης, χρησιμοποιώντας κατάλληλα εργαλεία, να μεταφράσει τους ηχητικούς τόνους που πατήθηκαν στην κλήση. Οι τόνοι, γνωστοί ως dual-tone multifrequency (DTMF) χρησιμοποιούνται από τους χρήστες για εισαγωγή κωδικών ή άλλων πληροφοριών πιστοποίησης όπως η ταυτότητα, όταν η κλήση γίνεται για παράδειγμα σε μια τράπεζα ή σε κάποιον οργανισμό που χρειάζεται να δώσουμε προσωπικά στοιχεία με αυτόν τον τρόπο. Παίρνοντας αυτή την πληροφορία ο επιτιθέμενος είναι σε θέση να χρησιμοποιήσει αυτούς τους αριθμούς για να αποκτήσει πρόσβαση σε λογαριασμούς μέσω τηλεφώνου. [Αστέριος Αλμπανάκης ,2011]

Σκόπιμη διακοπή υπηρεσιών

Denial of Service (DOS Attack)
Οι επιτιθέμενοι κάνοντας κακή χρήση του πρωτοκόλλου σηματοδοσίας διεξάγουν denial of service επιθέσεις. Υπάρχουν 2 περιπτώσεις. Στην πρώτη οι επιτιθέμενοι δημιουργούν ένα μεγάλο αριθμό αιτημάτων εγκατάστασης κλήσης που χρειάζονται τη δύναμη επεξεργασίας του proxy server, με αποτέλεσμα να υπερφορτώνεται. Στη δεύτερη περίπτωση, οι επιτιθέμενοι χρησιμοποιούν την ακύρωση των εκκρεμών σημάτων εγκατάστασης κλήσης συμπεριλαμβανομένης της αποστολής των CANCEL, GOODBYE ή PORT UNREACHABLE μηνυμάτων. Αυτό καθιστά το τηλέφωνο να μην είναι σε θέση να ολοκληρώσει τις κλήσεις ή να κλείσει. Ο συγκεκριμένος τύπος επίθεσης ευνοείται από την πολυπλοκότητα των πρωτοκόλλων σηματοδοσίας.



Εικόνα 2.6 Επίθεση DOS.[Φαφούλα Ιωάννα, 2008]

Επιθέσεις κατακλυσμού UDP

Επειδή η διεύθυνση πηγής του UDP πακέτου μπορεί να πλαστογραφηθεί, αυτή η επίθεση προτιμάται για να πραγματοποιηθεί κατακλυσμός εύρος ζώνης. Η πλαστογράφηση επιτρέπει στον επιτιθέμενο να προσπεράσει firewalls και άλλες συσκευές φιλτραρίσματος. Όλες σχεδόν οι SIP συσκευές υποστηρίζουν UDP, γι' αυτό θεωρούνται ως μια πετυχημένη επιλογή για επίθεση. Πολλές VoIP συσκευές μπορούν να αχρηστευθούν, αν ένας κατακλυσμός UDP πακέτων έχει σαν στόχο την πόρτα του SIP (5060) ή ακόμα και τυχαίες πόρτες.

Επιθέσεις κατακλυσμού TCP SYN

Είναι επιθέσεις που καταστρέφουν τη χειραψία τριπλής κατεύθυνσης (3-way handshake) για να κατακλύσουν ένα στόχο με διαχείριση σύνδεσης. Σε αυτό το είδος της επίθεσης, ο επιτιθέμενος στέλνει έναν κατακλυσμό από πακέτα SYN με ψεύτικη IP διεύθυνση πηγής. Το θύμα απαντάει με ένα SYN-ACK στον αποστολέα (ο οποίος δεν υπάρχει). Για να μπορέσει να ολοκληρωθεί η TCP σύνδεση, το θύμα περιμένει για μια χρονική περίοδο για ένα ACK πακέτο από την πηγή αποστολής. Αυτό το πακέτο δε στέλνεται ποτέ, με αποτέλεσμα ο πίνακας συνδέσεων του θύματος να γεμίζει και να χρησιμοποιεί όλους τους διαθέσιμους πόρους με αυτές τις άκυρες αιτήσεις. Σαν αποτέλεσμα έχουμε έναν διακομιστή, τηλέφωνο ή δρομολογητή που δε μπορεί να ξεχωρίσει τα DoS πακέτα από τα γνήσια SYN για τις πραγματικές VoIP συνδέσεις.

Επιθέσεις κατακλυσμού ICMP και Smurf

Το Internet Control Message Protocol (ICMP) επιτρέπεται από τα περισσότερα firewalls και routers για διαγνωστικούς σκοπούς. Ωστόσο, το ICMP προσφέρει τη δυνατότητα αποστολής μεγάλης ποσότητας ICMP κίνησης. Ακόμα μια κακή χρήση του είναι η πλαστογράφηση της ταυτότητας της IP διεύθυνσης της πηγής και των ping διευθύνσεων εκπομπής σε μια ποικιλία δικτύων που επιτρέπουν εκπομπές οδηγούμενες από IP. Το όνομα αυτής της επίθεση είναι smurf και περιλαμβάνει έναν κατακλυσμό από γνήσιες απαντήσεις ICMP αυτών των δικτύων προς το θύμα που πλαστογραφήθηκε. Σε τέτοιες επιθέσεις οι περισσότερες εφαρμογές Internet καταρρέουν.

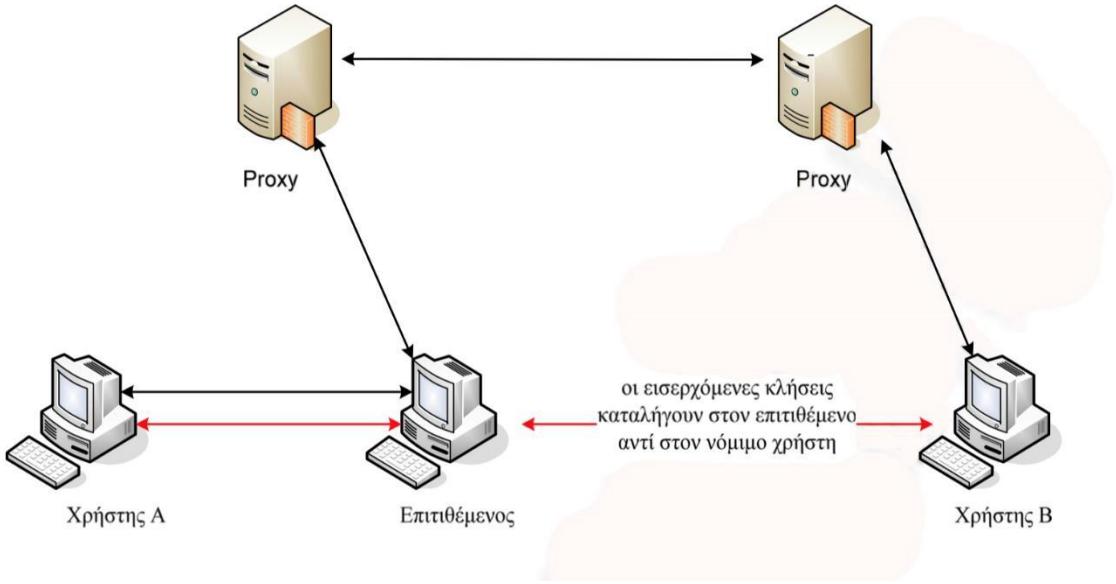
Worm και Ιοί υπερκάλυψης

Υπερκάλυψη (Oversubscription) είναι όταν οι ανάγκες των εφαρμογών για εύρος ζώνης έχουν υπερβεί τις δυνατότητες του δικτύου. Αυτό μπορεί να προκύψει από επιθέσεις κατακλυσμού DoS ή κακή διαχείριση QoS. Το ξέσπασμα worms και ιών στο δίκτυο μπορεί να καταναλώσει όλο το διαθέσιμο εύρος ζώνης σαν παρενέργεια του "σκαναρίσματος" για άλλους ευαίσθητους πελάτες προκειμένου να τους μολύνει. Ακόμα και μερικά μόνο μηχανήματα σε έναν οργανισμό να έχουν μολυνθεί από ένα

worm, μπορούν να επιβαρύνουν το διαθέσιμο εύρος ζώνης.

Επιθέσεις Registration Hijacking

Η Registration hijacking επίθεση συμβαίνει όταν ένας επιτιθέμενος αντιγράφει έναν έγκυρο χρήστη UA (User Agent) σε έναν registrar και αντικαθιστά τη νόμιμη εγγραφή με τη δική του διεύθυνση. Αυτή η επίθεση αναγκάζει τις εισερχόμενες κλήσεις που προορίζονται για τον UA να σταλθούν στον ψεύτικο χρήστη. Η Registration hijacking επιτρέπει στις εισερχόμενες κλήσεις να κλαπούν και να απαντηθούν από έναν επιτιθέμενο. Επίσης, δίνει τη δυνατότητα σε έναν επιτιθέμενο να μπει ενδιάμεσα και να καταγράψει τη σηματοδότηση και τον ήχο.



Εικόνα 2.7 Registration Hijacking. [Φαφούλα Ιωάννα, 2008]

Επιθέσεις Message Tampering

Η επίθεση Message tampering πραγματοποιείται όταν ο επιτιθέμενος παρεμποδίζει και τροποποιεί την ανταλλαγή πακέτων μεταξύ των SIP τμημάτων. Η επίθεση μπορεί να πραγματοποιηθεί μέσω της registration hijacking, της proxy impersonation, ή μιας επίθεσης σε οποιοδήποτε έμπιστο συστατικό που επεξεργάζεται τα SIP μηνύματα, όπως proxy, media gateway, ή firewall.

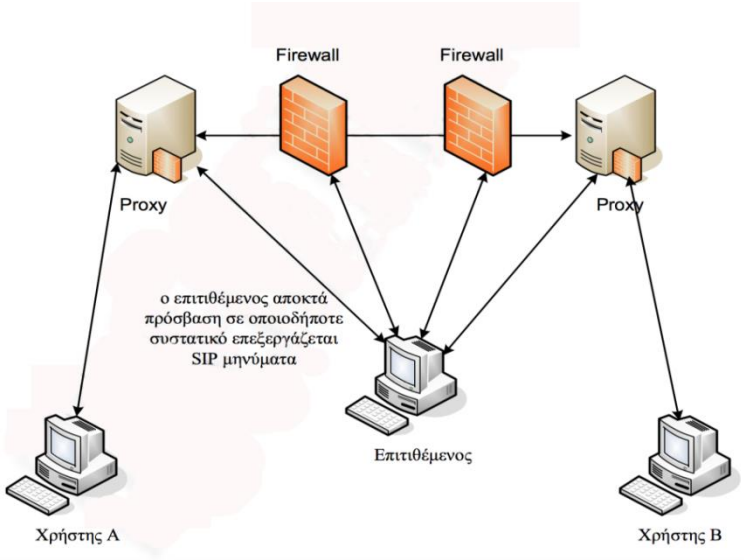
Επιθέσεις Session Tear Down

Η Session tear down πραγματοποιείται όταν ένας επιτιθέμενος παρατηρεί τη σηματοδοσία μιας κλήσης και έπειτα στέλνει τροποποίημενα SIP BYE αιτήματα στους συμμετέχοντες UAs. Στις περισσότερες SIP UAs η αυθεντικοποίηση δεν απαιτείται να είναι ισχυρή, έτσι επιτρέπει σε έναν επιτιθέμενο να στείλει κατάλληλα επεξεργασμένα BYE αιτήματα στους δύο UAs, τερματίζοντας βιαίως την κλήση. [Αστέριος Αλμπανάκης ,2011]

Παρακολούθηση και τροποποίηση

Επιθέσεις Proxy Impersonation

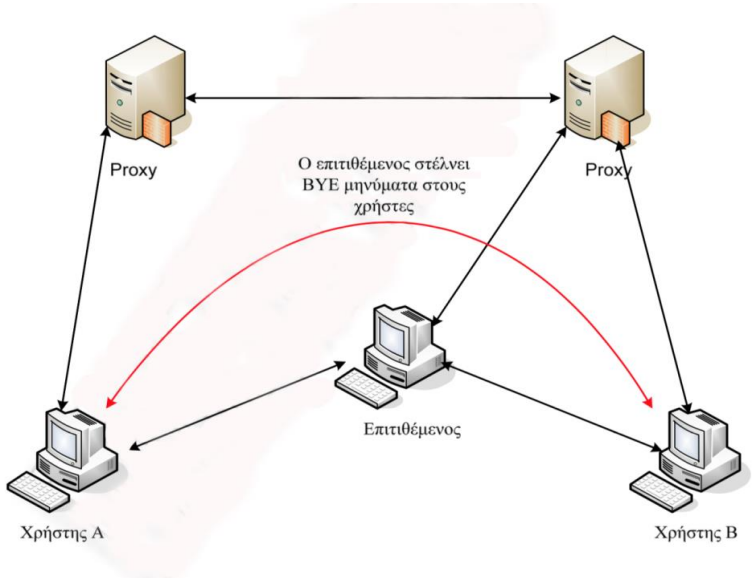
Επίθεση Proxy impersonation αναφέρεται στην περίπτωση που ένας επιτιθέμενος ξεγελά έναν από τους SIP UAs (User Agents) ή τους proxies, ώστε να επικοινωνήσουν με ένα proxy απατεώνων. Εάν ένας επιτιθέμενος καταφέρει να μιμηθεί έναν proxy, τότε έχει πρόσβαση στα SIP μηνύματα και έχει τον πλήρη έλεγχο της κλήσης. Οι UAs και οι proxies κανονικά επικοινωνούν χρησιμοποιώντας το UDP και δεν απαιτούν ισχυρή αυθεντικοποίηση για να επικοινωνήσουν με ένα άλλο proxy. Ένας proxy απατεώνων μπορεί να παρεμβληθεί στο ρεύμα σηματοδοσίας μέσω διαφόρων τρόπων, συμπεριλαμβανομένης της Domain Name Service (DNS) spoofing, της Address Resolution Protocol (ARP) cache spoofing, ή απλά αλλάζοντας τη διεύθυνση του proxy για ένα SIP τηλέφωνο. Ένας τέτοιος proxy έχει τον ολικό έλεγχο πάνω στις κλήσεις και μπορεί να εκτελέσει τους ίδιους τύπους επιθέσεων που αναφέρθηκαν πιο πάνω στην registration hijacking.



Εικόνα 2.8 Επιθέσεις Proxy Impersonation. [Φαφούλα Ιωάννα, 2008]

Man-In-The-middle επίθεση

Η Man-in-the-middle είναι μια αρκετά διαδεδομένη επίθεση που πραγματοποιεί μια τριπλή επικοινωνία μεταξύ των δύο μερών που προσπαθούν να επικοινωνήσουν και του επιτιθέμενου ανάμεσά τους. Καθ' όλη τη διάρκεια της επικοινωνίας, τα δύο συμβαλλόμενα μέρη δεν αντιλαμβάνονται τη συμμετοχή του επιτιθέμενου. Έτσι ο επιτιθέμενος πετυχαίνει τη δρομολόγηση της κυκλοφορίας μεταξύ των δύο συμβαλλόμενων μέσω αυτού. Οι πληροφορίες που ανταλλάσσονται παρεμποδίζονται, τροποποιούνται ή και διαβάζονται.



Εικόνα 2.9 Man-In-The-middle επίθεση. [Φαφούλα Ιωάννα, 2008]

Replay Attack

Μια τέτοια επίθεση χρησιμοποιεί τα sniffing εργαλεία πάνω στα πακέτα ενός δικτύου και μπορεί να πραγματοποιήσει replay επιθέσεις με τη σύλληψη πληροφοριών σε μια σύνοδο επικοινωνίας. Οι πληροφορίες που συλλαμβάνονται μπορούν να αναμεταδωθούν άθικτες ή παραποιημένες για να επιτύχουν τον σκοπό του επιτιθέμενου. Οικονομικοί οργανισμοί, όπως οι τράπεζες και τα λογιστικά γραφεία, που αναπτύσσουν την VoIP εφαρμογή μπορεί να βιώσουν μια κατάσταση κατά την οποία ευαίσθητα δεδομένα, όπως αριθμοί λογαριασμών, πληροφορίες πιστωτικών καρτών, μπορούν να κλαπούν από τους απατεώνες Διαδικτύου. Από την άποψη της διοίκησης συστημάτων, η σύνδεση των χρηστών σε αυτό προσφέρει ένα πολύ καλό

περιβάλλον για τις replay επιθέσεις. Σ’ αυτή την περίπτωση, ο επιτιθέμενος συλλαμβάνει το όνομα και τον κωδικό πρόσβασης του χρήστη και τα χρησιμοποιεί για να συνδεθεί ως νόμιμος χρήστης όποτε αυτός θέλει. Για την εξάλειψη τέτοιων επιθέσεων είναι αρκετά βοηθητική η ακεραιότητα των πακέτων. Η χρονοσήμανση (timestamping), είναι ένα χαρακτηριστικό που υποστηρίζεται από το RTP σε ένα συγχρονισμένο περιβάλλον μετριάζεται το replay επιθέσεις με τη βοήθεια του μηχανισμού προστασίας ακεραιότητας όπως οι συναρτήσεις hash MD5 και SHA -1.
[Αστέριος Αλμπανάκης, 2011]

Κατάχρηση υπηρεσιών
Η κατάχρηση υπηρεσιών περιλαμβάνει τις παρακάτω επιθέσεις:

Κατάχρηση τηλεδιάσκεψης
Η κατάχρηση τηλεδιάσκεψης (Call Conference Abuse) χρησιμοποιείται από τους κακόβουλους χρήστες προκειμένου να αποκρύψουν την ταυτότητά τους και να διαπράξουν κάποια απάτη.

Απάτη μέσω υπηρεσιών υψηλής χρέωσης
Η απάτη μέσω υπηρεσιών υψηλής χρέωσης (Premium Rate Service Fraud) είναι μια μέθοδος μέσω της οποίας αυξάνεται η χρήση της υπηρεσίας του VoIP χωρίς τη συγκατάθεση του χρήση και αποσκοπεί μόνο στην αύξηση του λογαριασμού που θα πληρώσει το θύμα. Ο κακόβουλος χρήστης, σε τέτοιου είδους επιθέσεις, πραγματοποιεί κλήσεις σε χώρες με υψηλές χρεώσεις ή προορισμούς υψηλού κινδύνου (Κούβα, Νιγηρία, Πακιστάν).

Αποφυγή πληρωμής ή τροποποίηση
Η αποφυγή πληρωμής ή τροποποίηση του λογαριασμού (Improper Bypass or Adjustments to Billing) είναι μια μέθοδος που χρησιμοποιείται από τους κακόβουλους χρήστες με σκοπό να αποφύγουν να πληρώσουν την υπηρεσία Voip ή για να αποκρύψουν την ταυτότητά τους όταν διαπράξουν κάποια απάτη, τροποποιώντας τα αρχεία του αναλυτικού λογαριασμού χρέωσής τους. [Αστέριος Αλμπανάκης ,2011]

2.1.5 Ασφάλεια συστημάτων VoIP

Σ’ αυτά τα συστήματα πρέπει να παρέχεται επαρκής αυθεντικοποίηση των κλήσεων, άλλα και end-to-end μέτρα ακεραιότητας και εμπιστευτικότητας.
Αν δεν υλοποιηθούν αυτά τα χαρακτηριστικά ασφαλείας, τότε θα παρουσιαστούν

πολλά κενά ασφαλείας ικανά για κακόβουλη ζημία. Επιπλέον, η ασφάλεια στα συστήματα VoIP είναι ένα πολύπλοκο ζήτημα, λόγω των πολλών παραμέτρων και συστατικών που το απαρτίζουν. Η χρήση του VoIP σήμερα προϋποθέτει τη συνεργασία των δικτύων μεταγωγής κυκλώματος και των δικτύων μεταγωγής πακέτων, επομένως η μελέτη της ασφάλειας θα πρέπει να περιλαμβάνει και τα δύο αυτά επίπεδα, τουλάχιστον για όσο ακόμα συνυπάρχουν.

Μέτρα Ασφαλείας

Μια πολιτική ασφαλείας καθορίζει:

- Ποια ομάδα ή ποιο άτομο είναι υπεύθυνο για την εφαρμογή της πολιτικής ασφαλείας.
- Ρόλους και ευθύνες.
- Διαχείριση Κινδύνων.
- Ταξινόμηση της πληροφορίας.
- Έλεγχο Πρόσβασης.
- Φυσική Ασφάλεια.
- Κανόνες Συμμόρφωσης.
- Monitoring των Εξυπηρετητών, δικτύων και συστημάτων

Εξίσου σημαντικό είναι η τήρηση ορισμένων κανόνων ασφαλείας όπως:

- Κατάργηση ή διαγραφή όλων των μη απαραίτητων υπηρεσιών και δομικών στοιχείων του συστήματος.
- Περιορισμός πρόσβασης μόνο στις απαραίτητες υπηρεσίες που χρειάζεται ένας εργαζόμενος.
- Χρήση των πρόσφατων εκδόσεων λογισμικού σε κάθε σύστημα (Updated).
- Authentication κάθε απόπειρας για διαχείριση και κρυπτογράφηση της απομακρυσμένης πρόσβασης για διαχείριση συστημάτων (SSH ή IPSec).
- Αποφυγή της χρήσης των προεπιλεγμένων κωδικών πρόσβασης (default password).
- Υλοποίηση της VPN πρόσβασης για όσους από τους υπαλλήλους απαιτείται η απομακρυσμένη πρόσβαση σε πόρους των κεντρικών συστημάτων.

Επίσης κρίνεται απαραίτητη μια ad hoc network management η οποία έχει:

- Χρήση των ήδη υπαρχόντων εργαλείων διαχείρισης δικτύου δεδομένων για το ενοποιημένο δίκτυο.
- Διαχωρισμό της κίνησης διαχείρισης από την υπόλοιπη κίνηση δικτύου.

Το authenticantion από την πλευρά του χρειάζεται:

- Χρήση τηλεφωνικών συσκευών που διαθέτουν user authentication.
- Υλοποίηση device authentication με ARP και 802.1X.
- Κεντρικοποιημένη διαχείριση χρηστών: χρήση Active Directory ή LDAP για authentication στις εφαρμογές και VoIP υπηρεσίες.
- Authentication μέσω DHCP (Dynamic Host Configuration Protocol).

FireWalls

Τα firewalls είναι είτε συσκευές, είτε λογισμικό και είναι ο κύριος μηχανισμός προστασίας από τις διάφορες απειλές στα συστήματα επικοινωνίας VoIP. Καθορίζονται από εμάς ως γνωστές IP διευθύνσεις, πόρτες και υπηρεσίες (services) και με βάση τις εισόδους αυτές τα firewalls επιτρέπουν ή αποτρέπουν την κίνηση από και προς εμάς. Λειτουργούν με βάση το NAT (Network Address Translation), σύμφωνα με το οποίο μία εξωτερική διεύθυνση αντιστοιχεί σε πολλές εσωτερικές διευθύνσεις. Αυτό τους προσδίδει μεγαλύτερη προστασία από εξωτερικές επιθέσεις.

Port Scan

Είναι μια συστηματική διαδικασία που προσπαθεί να προσδιορίσει όλες τις ανοικτές πόρτες και διαθέσιμες υπηρεσίες σε έναν TCP/IP host. Οι περισσότεροι κακόβουλοι χρήστες χρησιμοποιούν το Port Scans για να μπορέσουν να εντοπίσουν έναν χρήστη-στόχο. Έτσι ο κακόβουλος χρήστης μπορεί να πετύχει τον πλήρη έλεγχο του χρήστη. Μια ασφαλής τεχνική, λοιπόν, για την αποφυγή του κινδύνου αυτού είναι το κλείσιμο όλων των πόρτων που δε λαμβάνουν μέρος στην επικοινωνία.

Voip VPN

Το VoIP VPN συνδυάζει δύο τεχνολογίες, το VoIP και το VPN (Virtual Private Network) και έτσι προσφέρει μια ασφαλή μέθοδο για τη μεταφορά της φωνής. Συγκεκριμένα, ο VoIP gateway-router μετατρέπει το αναλογικό σήμα της φωνής σε ψηφιακό, βάζει το σήμα σ’ ένα IP πακέτο και στη συνέχεια εφαρμόζει κρυπτογράφηση. Έπειτα, το πακέτο δρομολογείται μέσω του VPN tunnel. Ο αποστολέας αποκρυπτογραφεί το πακέτο και στη συνεχεία μετατρέπει το ψηφιακό σήμα σε αναλογικό, το οποίο και μεταδίδεται από το ακουστικό του VoIP τηλεφώνου. [Αστέριος Αλμπανάκης ,2011]

Μέτρα ασφαλείας σε επίπεδο πρωτοκόλλων

Προστασία του SIP

Τα πρωτόκολλα που μπορούν να χρησιμοποιηθούν για την παροχή της ακεραιότητας και της εμπιστευτικότητας των μηνυμάτων SIP σηματοδοσίας ενάντια στις διάφορες επιθέσεις είναι το IPSec, S/MIME, TLS, και DTLS. Σημαντικό ρόλο για την υιοθέτηση των πρωτοκόλλων ασφαλείας παίζει η ευκολία της εφαρμογής και η δυνατότητα εξέλιξής τους.

SIP Authentication

Για την προστασία στην αυθεντικοποίηση και την επανάληψη των μηνυμάτων αιτήματος για την εγγραφή, την έναρξη και τη λήξη μίας συνόδου το SIP χρησιμοποιεί το HTTP Digest Authentication. Συγκεκριμένα, τα SIP πιστοποιητικά αυθεντικοποίησης είναι σημαντικά μέσα για μια συγκεκριμένη περιοχή, η οποία διαχειρίζεται τα πιστοποιητικά των χρηστών της, αλλά δεν μπορεί να τα εξουσιοδοτήσει σε άλλες περιοχές εκτός αν υπάρχει μια καθορισμένη σχέση εμπιστοσύνης

Transport Layer Security

Ένα από τα πιο αποδεκτά πρωτόκολλα για την υποστήριξη της εμπιστευτικότητας του στρώματος μεταφοράς είναι το TLS. Παρέχει τη δυνατότητα να εκτελεσθεί αμοιβαία αυθεντικοποίηση, εμπιστευτικότητα, και ακεραιότητα. Αποτελείται από δύο στρώματα: το πρωτόκολλο TLS Record και το πρωτόκολλο TLS Handshake. [Αστέριος Αλμπανάκης ,2011]

Datagram Layer Security

Το πρωτόκολλο Datagram Transport Layer Security, αναπτύχθηκε για να καλύψει την ανάγκη για παροχή προστασίας ισοδύναμης με το TLS στα πρωτόκολλα του επιπέδου εφαρμογής που χρησιμοποιούν το UDP ως πρωτόκολλο μεταφοράς, όπως κάνει το SIP. Το DTLS είναι παρόμοιο με το TLS σε πολλά σημεία, συμπεριλαμβανομένου του περιορισμού απαίτησης μιας νέας εγκατάστασης συνόδου μεταξύ των hops ώστε να προστατευθούν τα SIP μηνύματα από ένα τελικό σημείο σε ένα άλλο.

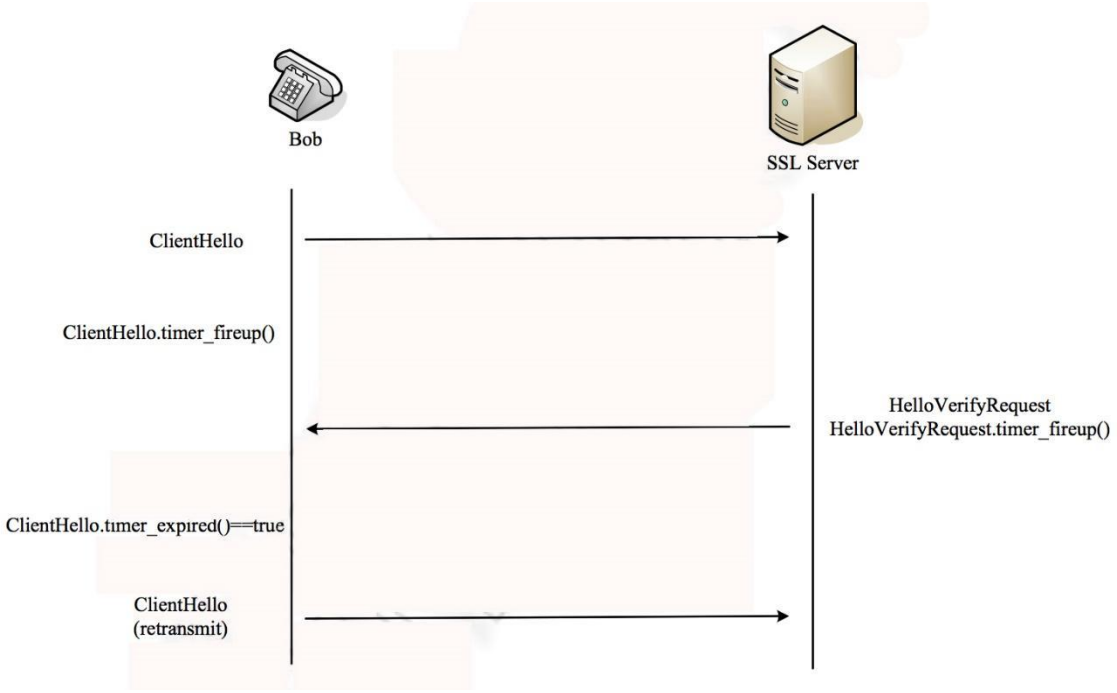
Μια κύρια διαφορά μεταξύ του TLS και του DTLS είναι ότι το DTLS παρέχει έναν μηχανισμό που μπορεί να χειριστεί την αναξιοπιστία που συσχετίζεται με το UDP, όπως η πιθανότητα απώλειας πακέτων ή της επαναδιάταξης. Εάν η απώλεια πακέτων συμβεί κατά τη διάρκεια μιας TLS handshake, η σύνδεση δεν ολοκληρώνεται. Το TLS Record Layer, όπου πραγματοποιείται η κρυπτογράφηση δεδομένων, απαιτεί τα αρχεία να παραλαμβάνονται και να υποβάλλονται σε επεξεργασία με διαδοχική σειρά. Εάν το αρχείο n δεν παραληφθεί, τότε το αρχείο n + 1 δεν μπορεί να αποκρυπτογραφηθεί επειδή το TLS στρώμα κρυπτογράφησης κυκλοφορίας χρησιμοποιεί το CBC (Cipher Block Chaining), το οποίο απαιτεί τη γνώση του προηγούμενου αρχείου για να αποκρυπτογραφήσει το επόμενο αρχείο στην ακολουθία.

Ένας άλλος περιορισμός του TLS είναι ότι χρησιμοποιεί μία MAC (Message Authentication Code) για κάθε αρχείο για την προστασία ενάντια στην επανάληψη και στην επαναδιάταξη. Χρησιμοποιώντας τους αριθμούς ακολουθίας των αρχείων που είναι μοναδικοί για κάθε αρχείο, παράγεται η MAC. Έτσι, εάν συμβεί απώλεια πακέτων, η ανίχνευση της επανάληψης καθίσταται άχρηστη.

Το DTLS έχει σχεδιαστεί για να υπερνικήσει τους περιορισμούς του TLS με την παροχή των εξής:

- Αξιοπιστία κατά τη διάρκεια της DTLS handshake.
- Ανίχνευση επανάληψης πακέτων.

Για να εξισορροπήσει τις συνθήκες απώλειας πακέτων, το DTLS παρέχει ένα χρονόμετρο αναμετάδοσης Όταν ένας client διαβιβάσει το ClientHello μήνυμα, αρχίζει το χρονόμετρο και περιμένει ένα HelloVerifyResponse μήνυμα από τον server. Ο server διατηρεί επίσης ένα χρονόμετρο μετάδοσης μηνυμάτων. Εάν το χρονόμετρο του client λήξει, υποθέτει ότι είτε το ClientHello είτε το HelloVerifyResponse χάθηκε και αναμεταδίδει το ClientHello μήνυμα. Στην πιο κάτω εικόνα βλέπουμε πως απεικονίζεται η απώλεια πακέτου και το σενάριο αναμετάδοσης.



Εικόνα 2.10 DTLS απώλεια πακέτου και αναμετάδοση.[Φαφούλα Ιωάννα, 2008]

Το πρωτόκολλο DTLS βοηθάει στην αντιμετώπιση μερικών ζητημάτων που σχετίζονται με τις εφαρμογές πολυμέσων, τη στιγμή που παρέχει προστασία στα μηνύματα σηματοδοσίας και media. Για να γίνει η εφαρμογή του σε συγκεκριμένο περιβάλλον θα ήταν σωστό να ξέρουμε της δυνατότητες και τους περιορισμούς του. [Φαφούλα Ιωάννα, 2008]

Δυνατότητες:

- Πιο εύκολο να εφαρμοστεί σε σύγκριση με τα πρωτόκολλα ασφαλείας S/MIME και IPSec.
- Κληρονομεί αποδεδειγμένες ιδιότητες ασφάλειας από το TLS.
- Οι μηχανισμοί που παρέχει του δίνουν τη δυνατότητα να αντισταθμίσει τους περιορισμούς του TLS για την αξιοπιστία της handshake και την ανίχνευση επανάληψης.
- Η χρήση των cookies προσφέρει προστασία ενάντια στις DOS επιθέσεις.

Περιορισμοί:

- Χρειάζεται την εγκατάσταση μιας νέας crypto συνεδρίας μεταξύ των ενδιάμεσων hops, παρόμοια με το TLS.
- Απαιτεί μια PKI υποδομή για να επιβάλει την αμοιβαία αυθεντικοποίηση.
- Δεν παρέχει άμεση εμπιστευτικότητα από άκρο σε άκρο. Απαιτεί τον τερματισμό και τη δημιουργία μιας νέας συνεδρίας σε κάθε hop (μεταξύ των SIP proxy ή SBCs).

S/MIME

Τα Secure/Multipurpose Internet Mail Extensions, που καθορίζονται στο RFC 3851, έχουν τη δυνατότητα να παρέχουν την από άκρο σε άκρο ακεραιότητα, εμπιστευτικότητα, και επικύρωση για τα πρωτόκολλα εφαρμογής όπως το SMTP και το SIP. Αυτό το πρωτόκολλο καθορίζει ένα σύνολο μηχανισμών με σκοπό να κωδικοποιήσει και να αντιπροσωπεύσει τα σύνθετα σχήματα μηνυμάτων όπως τα συνημμένα πολυμέσων (audio clips) και γλωσσικούς χαρακτήρες (ελληνικά, κινεζικά) μαζί με άλλα πρωτόκολλα όπως το SMTP ή το SIP. Το S/MIME μήνυμα είναι βασισμένο πάνω στο MIME, αλλά ενσωματώνει τα PKCS πρότυπα για να επιτύχει τους στόχους ασφάλειάς του. Αυτός ο συνδυασμός (MIME και S/MIME) παρέχει ένα πολύ καλό επίπεδο ευελιξίας στην υποστήριξη της ανταλλαγής σύνθετων μηνυμάτων μαζί με τη συντήρηση ενός συνόλου στόχων ασφάλειας, συμπεριλαμβανομένης της ακεραιότητας, της εμπιστευτικότητας, και της αυθεντικότητας. Ταυτόχρονα, η δυνατότητα να παρασχεθεί μια τόσο λεπτομερή προστασία κάνει την εφαρμογή πιο πολύπλοκη.

Το πρωτόκολλο S/MIME παρέχει προστασία σε πιο λεπτομερές επίπεδο στα μηνύματα σηματοδοσίας από άλλα πρωτόκολλα. Την ίδια στιγμή, η πολυπλοκότητα της εφαρμογής του S/MIME στην προστασία των μηνυμάτων σηματοδοσίας είναι ένας σημαντικός παράγοντας στον περιορισμό των εφαρμογών του στα περισσότερα περιβάλλοντα. Στη συνέχεια αναφέρουμε τις δυνατότητες και τους περιορισμούς του.[Φαφούλα Ιωάννα, 2008]

Δυνατότητες:

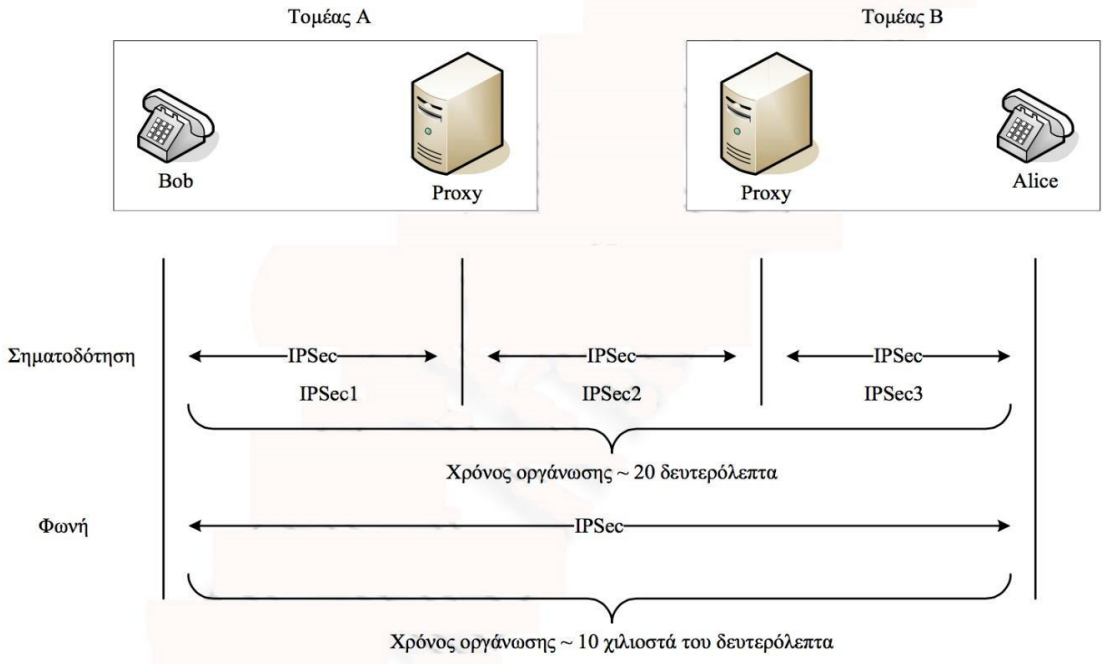
- Δεν εξαρτάται από το πρωτόκολλο μεταφοράς και μπορεί να χρησιμοποιηθεί είτε με το UDP, είτε με το TCP.
- Η ευελιξία που παρέχει είναι μεγάλη, λόγω της δυνατότητας προστασίας τμημάτων των SIP μηνυμάτων.
- Παρέχει εμπιστευτικότητα, ακεραιότητα και επικύρωση από άκρο σε άκρο.

Περιορισμοί:

- Χρειάζεται περισσότερη προσπάθεια για να εφαρμοστεί λόγω της πολυπλοκότητας και των απαιτήσεων υποδομής του, έναντι άλλων πρωτοκόλλων όπως TLS ή DTLS.
- Δεν είναι ευρέως αναπτυσσόμενο.
- Επειδή απαιτεί μια PKI υποδομή, η εξέλιξή του είναι αμφισβητήσιμη.

IPSec

Το IPSec είναι ένα αποδεδειγμένο και ευρέως αναπτυγμένο πρωτόκολλο ασφάλειας και παρέχει προστασία σε όσες εφαρμογές χρησιμοποιούν για πρωτόκολλο μεταφοράς το UDP ή το TCP. Το IPSec, μπορεί να χρησιμοποιηθεί σε tunnel ή στον τρόπο μεταφοράς για να προστατεύσει το ωφέλιμο φορτίο του. Το IPSec μπορεί να παρέχει εμπιστευτικότητα, ακεραιότητα, και επικύρωση για τα μηνύματα της σηματοδοσίας και των media, δημιουργώντας ασφαλή tunnels μεταξύ των τελικών σημείων. Στην πιο κάτω εικόνα βλέπουμε τη χρήση του IPSec σε ένα SIP περιβάλλον.



Εικόνα 2.11 Εφαρμογή του IPSec σε ένα SIP περιβάλλον. [Φαφούλα Ιωάννα, 2008]

Υπάρχουν περιπτώσεις που τα IPSec tunnels πρέπει να ξαναδημιουργηθούν εξαιτίας

λαθών του δικτύου, αποτυχιών του λογισμικού ή του υλικού, αδράνειας, ή επαναδιαπραγμάτευσης κλειδιών που μπορεί να έχει επίπτωση στις κλήσεις. Ωστόσο, το IPSec μπορεί επαρκώς να προστατεύσει την VoIP κυκλοφορία μεταξύ των δικτύων στα οποία τα IPSec tunnels δημιουργούνται εκ των προτέρων. Τυπικά, τα IPSec tunnels παραμένουν σταθερά μεταξύ των μακρινών περιοχών, επειδή υπάρχει πάντα κυκλοφορία και τα tunnels δεν λήγουν λόγω αδράνειας. Στα VoIP τηλέφωνα κάτι τέτοιο δεν ισχύει, επειδή μπορεί να χρησιμοποιούν το IPSec για να προστατεύσουν τα μηνύματα σηματοδοσίας και media. Για να το λύσουν αυτό, οι εφαρμογές στέλνουν συχνά μηνύματα εγγραφής στον τοπικό τους registrer για να διατηρήσουν το IPSec tunnel. [Φαφούλα Ιωάννα, 2008]

Το IPSec είναι αποτελεσματικό στην παροχή της αυθεντικοποίησης και της εμπιστευτικότητας των μηνυμάτων που μεταφέρουν τη σηματοδοσία και τα media. Την ίδια στιγμή, υπάρχουν περιορισμοί που μπορούν να έχουν επίπτωση στην απόδοση της επικοινωνίας των πολυμέσων. Πιο κάτω αναφέρουμε τις δυνατότητες και τις αδυναμίες που έχει, οι οποίες πρέπει να ληφθούν υπόψη κατά τη διάρκεια της σχεδίασης ή της υλοποίησης μιας εφαρμογής πολυμέσων:

Δυνατότητες:

- Αποδεδειγμένο πρωτόκολλο ασφαλείας και ευρέως αναπτυσσόμενο
- Λειτουργεί στο στρώμα δικτύου, έτσι έχει τη δυνατότητα να υποστηρίξει τα UDP,TCP, SIP, και RTP.
- Παρέχει προστασία συμβολοσειράς ενάντια στις διάφορες επιθέσεις όπως eavesdropping, masquerading, DOS, και άλλες.
- Παρέχει εμπιστευτικότητα, ακεραιότητα και επικύρωση.

Περιορισμοί:

- Χρειάζεται περισσότερη προσπάθεια για να εφαρμοστεί λόγω της πολυπλοκότητας και των απαιτήσεων υποδομής του έναντι άλλων πρωτοκόλλων όπως TLS ή DTLS.
- Χρειάζεται μια PKI υποδομή για να υποστηρίξει την επικύρωση, την ακεραιότητα, και την εμπιστευτικότητα της ακριανής συσκευής.
- Τα ενδιάμεσα συστατικά πρέπει να είναι έμπιστα.
- Δεν έχει καλή διαβάθμιση στα μεγάλα κατανεμημένα δίκτυα και στις κατανεμημένες εφαρμογές.

Προστασία H.323

Το H.323, όπως προαναφέραμε σε πιο πάνω ενότητα, είναι μια οικογένεια συστάσεων της ITU από την οποία τα H.225.0, H.245, και H.235.x μας ενδιαφέρουν περισσότερο. Η H.225 σύσταση έχει δύο υποσύνολα, ένα από τα οποία συζητά το RAS (Remote Access Service) αλλά και άλλες σηματοδοσίες κλήσης. Η σηματοδοσία κλήσης χρησιμοποιείται μεταξύ των H.323 τελικών σημείων για την εγκατάσταση και τον τερματισμό συνδέσεων και είναι παρόμοια με τη Q.931 σύσταση της ITU. Η RAS χρησιμοποιείται από τους gatekeepers για τη διαχείριση των τελικών σημείων που βρίσκονται μέσα στη ζώνη τους. Τα τελικά σημεία πρέπει να χρησιμοποιούν το RAS για να μπορέσουν να εγγραφούν στον αντίστοιχο gatekeeper και να αποκτήσουν πρόσβαση στους πόρους και τις υπηρεσίες δικτύου.

Μια αρχιτεκτονική διαφορά που προκύπτει μεταξύ του RAS και της σηματοδοσίας κλήσης είναι ότι το RAS μεταφέρεται μέσω του UDP, ενώ η σηματοδοσία κλήσης μπορεί να υποστηριχθεί από UDP και TCP. Γι' αυτό, διαφορετικές επιθέσεις ισχύουν σε κάθε μια με μεταβλητούς βαθμούς επιτυχίας.

Η H.245 προδιαγραφή είναι ένα πρωτόκολλο ελέγχου που χρησιμοποιείται μεταξύ δύο ή περισσότερων τελικών σημείων για να διαχειριστεί τα ρεύματα δεδομένων μεταξύ των συμμετεχόντων στην κάθε συνεδρία. Κύριος στόχος της είναι να διαπραγματευτεί τις παραμέτρους των δεδομένων μεταξύ των τελικών σημείων, όπως η RTP IP διεύθυνση, πόρτες, codecs (G729, G.711). Και τα τρία πρωτόκολλα, το H.225 , το RAS, και το H.245, χρησιμοποιούνται για τη δημιουργία, την τροποποίηση, και τον τερματισμό των συνεδριών.

Η σύσταση H.235 συζητά τις υπηρεσίες ασφάλειας όπως την αυθεντικοποίηση και την κρυπτογράφηση δεδομένων για τα συστήματα H.323, που χρησιμοποιούν τα H.245 και H.225.0 για τη δημιουργία σύσκεψης δύο σημείων ή περισσότερων. Η τελευταία έκδοση της σύστασης H.235 (v4) χωρίζει τις συστάσεις ασφάλειας από το H.235.1 μέχρι το H.235.9 τμήμα. Ο πιο κάτω πίνακας παρέχει μια λίστα με τις συστάσεις και τον αντίστοιχο στόχο της κάθε μίας.

Σύσταση	Περιγραφή
H.235.0	Πλαίσιο ασφαλείας για συστήματα πολυμέσων της Η σειράς (Η.323 και άλλα βασισμένα στο Η.245)
H.235.1	Προφίλ βασικής ασφάλειας
H.235.2	Προφίλ ασφάλειας υπογραφής
H.235.3	Υβριδικό προφίλ ασφάλειας
H.235.4	Άμεση και επιλεκτική δρομολογημένη ασφάλεια κλήσης
H.235.5	Προφίλ ασφάλειας για την RAS αυθεντικοποίηση χρησιμοποιώντας αδύναμα κοινά μυστικά
H.235.6	Προφίλ κρυπτογράφησης φωνής με την «εγγενή» Η.235/Η.245 διαχείριση κλειδιών
H.235.7	Προφίλ ασφαλείας MIKEY + SRTP
H.235.8	Ανταλλαγή κλειδιών για το SRTP σε ασφαλή κανάλια σηματοδοσίας
H.235.9	Πύλη ασφαλείας υποστηρίζοντας το Η.323

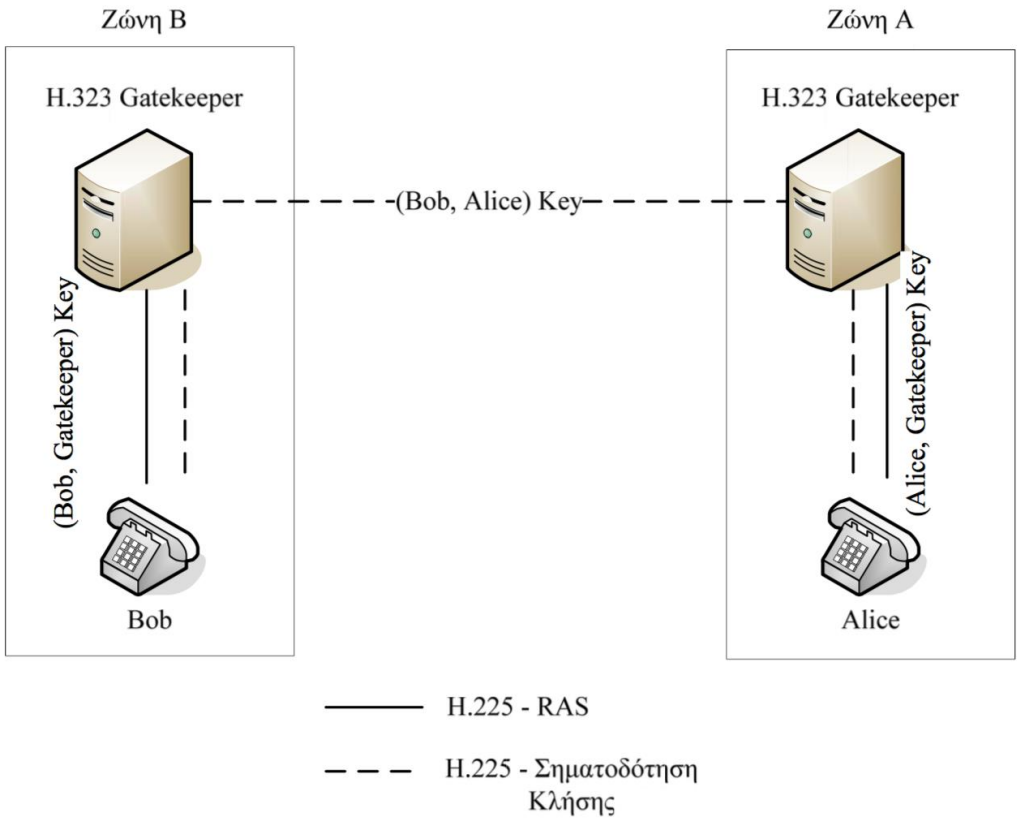
Πίνακας 2.1 Συστάσεις ασφαλείας

Ένα από τα κύρια πλεονεκτήματα του Η.235 είναι η δυνατότητα ενσωμάτωσης του υλικού κλειδιών για την προστασία του ρεύματος της σηματοδοσίας και των media κατά τη διάρκεια των μηνυμάτων για την εγκατάσταση της κλήσης. Η αμοιβαία αυθεντικοποίηση και η ανταλλαγή κλειδιών συμβαίνουν πριν από την ολοκλήρωση της εγκατάστασης της κλήσης. Μια τυπική Η.323 εγκατάσταση χρησιμοποιώντας το Η.235 διαρκεί μεταξύ 300 και 400ms ανάλογα με την εφαρμογή. [Φαφούλα Ιωάννα, 2008]

Η.235.1- Προφίλ βασικής ασφάλειας

Το end-point και ο gatekeeper χρησιμοποιούν ένα μυστικό κλειδί. Ο gatekeeper χρησιμοποιεί αυτό το κλειδί για να επαληθεύσει τα μηνύματα που αποστέλλονται από το end-point. Η αυθεντικοποίηση εφαρμόζεται χρησιμοποιώντας ένα HMAC- SHA1-96 αλγόριθμο για να παράγει έναν 20-byte τεμαχισμένο κωδικό πρόσβασης. Η αυθεντικοποίηση μεταξύ του τελικού σημείου και του gatekeeper είναι βασισμένη σε ένα ευδιάκριτο κλειδί, το οποίο μπορεί να είναι διαφορετικό από το κλειδί που χρησιμοποιείται για να προστατεύσει τη σηματοδοσία κλήσης. Σε κάποιες περιπτώσεις, απαιτείται να υπάρχουν δύο ευδιάκριτα κλειδιά που να χρησιμοποιούνται για να προστατεύσουν τα RAS μηνύματα και τα μηνύματα σηματοδοσίας κλήσης.

Το μειονέκτημα σε αυτό προφίλ είναι η διαχείριση του συνόλου των κοινών κλειδιών. Τα κλειδιά θα πρέπει να αποθηκεύονται σε μια κεντρική θέση (back- end service), γεγονός που το καθιστά το πιο ευάλωτο μέρος όλου του συστήματος. [Αστέριος Αλμπανάκη, 2011; Φαφούλα Ιωάννα, 2008]



Εικόνα 2.12 Κλειδί αυθεντικοποίησης δρομολογημένο από τον gatekeeper. [Φαφούλα Ιωάννα, 2008]

H.235.2 - Προφίλ ασφάλειας υπογραφής

Παρέχει έλεγχο ταυτότητας, ακεραιότητα του μηνύματος και μη αποκήρυξη χρησιμοποιώντας ασύμμετρες μεθόδους, όπως ψηφιακές υπογραφές σε κάθε μήνυμα, χρησιμοποιώντας τους SHA1 ή MD5 ως hashing αλγόριθμους. Αυτή η σύσταση παρέχει καλύτερη δυνατότητα εξέλιξης και διαχείρισης σε σύγκριση με το Προφίλ βασικής ασφαλείας, επειδή μπορεί να χρησιμοποιηθεί ασύμμετρη αυθεντικοποίηση για περιβάλλοντα με πολλά τερματικά (παραδείγματος χάριν μεγάλο

δίκτυο επιχειρήσεων). Εκτός από την ακεραιότητα και την αυθεντικοποίηση, η μη απόρριψη μπορεί να υποστηριχθεί επειδή η χρήση των πιστοποιητικών είναι εφικτή. Συγχρόνως, αυτός ο μηχανισμός μπορεί να χρησιμοποιηθεί για την ανταλλαγή ενός κοινού μυστικού κλειδιού ώστε να χρησιμοποιηθεί στην κρυπτογράφηση της RTP κυκλοφορίας (φωνή ή βίντεο). [Αστέριος Αλμπανάκη, 2011; Φαφούλα Ιωάννα, 2008]

H.235.3 - Υβριδικό προφίλ ασφαλείας
Το υβριδικό προφίλ ασφαλείας αποτελεί τον συνδυασμό του προφίλ βασικής ασφάλειας και ασφάλειας υπογραφής, με σκοπό τη δημιουργία ενός εξελικτικού προφίλ βασισμένου στα PKI πιστοποιητικά. Συνδυάζει τις δυνατότητες και από τα δύο προφίλ για να υποστηρίξει μια μεγάλη VoIP ανάπτυξη σε βαθμό επιχειρήσεων Αυτό το προφίλ εξουσιοδοτεί τη χρήση ενός GK-routed προτύπου, όπου όλα τα μηνύματα δρομολογούνται μέσω του τοπικού gatekeeper αντί να διαβιβαστούν άμεσα στα τελικά σημεία. Για να προσαρμοστούν η κινητικότητα του χρήστη και οι χρονικά εξαρτώμενες εφαρμογές, χρησιμοποιείται η μέθοδος της γρήγορης σύνδεσης σηματοδοσίας κλήσης. Επιπλέον, υποστηρίζει τη σύναξη των H.245 μηνυμάτων ελέγχου κλήσης μαζί με τα H.225.0 μηνύματα σηματοδοσίας κλήσης, το οποίο παρέχει έμφυτη ασφάλεια. [Αστέριος Αλμπανάκη, 2011; Φαφούλα Ιωάννα, 2008]

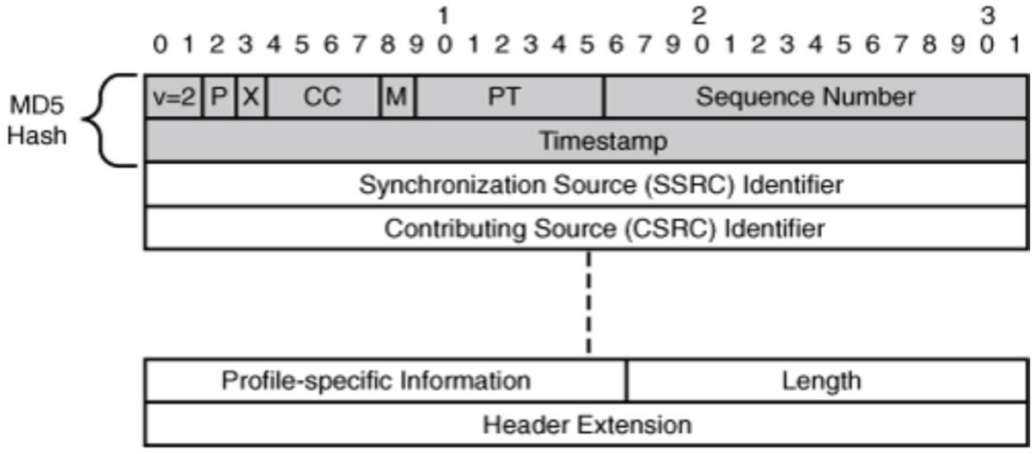
H.235.4 - Προφίλ άμεσης δρομολόγησης
Ισχύει για περιβάλλον όπου οι άμεσες κλήσεις δρομολογούνται χρησιμοποιώντας τον gatekeeper ως προς την επίλυση διευθύνσεων. Ο gatekeeper χρησιμεύει ως κέντρο διανομής κλειδιών (key distribution center - KDC), στέλνοντας δυο πακέτα, ένα που περιέχει το βασικό υλικό κρυπτογραφημένο με το κλειδί αυτό που καλεί και το άλλο κρυπτογραφημένο με το κλειδί του κληθέντα. Τα πακέτα περιέχουν ένα κλειδί συνόδου (session key), που χρησιμοποιούνται για την επικοινωνία μεταξύ των δύο άκρων που συμμετέχουν στην κλήση. [Αστέριος Αλμπανάκη, 2011; Φαφούλα Ιωάννα, 2008]

H.235.5 - Προφίλ ασφάλειας για την RAS
Το προφίλ αυτό εισάγει ένα πλαίσιο στο οποίο ένα τελικό σημείο και ο gatekeeper του ή μεταξύ δύο gatekeeper, μπορούν να χρησιμοποιήσουν τα αρχικά RAS μηνύματα για να διαπραγματευτούν ένα σύνολο ισχυρών κοινών μυστικών μεταξύ τους και να χρησιμοποιήσουν αυτά τα μυστικά για να μπορέσουν να κρυπτογραφήσουν και να πιστοποιήσουν τα επιλεγμένα μέρη του επόμενου RAS και των μηνυμάτων σηματοδοσίας κλήσης. Αυτή η μέθοδος ισχύει μόνο για την gatekeeper-routed σηματοδοσία, όχι για την άμεση δρομολόγηση σηματοδοσίας.

Δύο προφίλ υπάρχουν σε αυτό το πλαίσιο:

- Συγκεκριμένο προφίλ ασφάλειας (Specific security profile - SP1), το όποιο χρησιμοποιείται για να κατασκευάσει ένα κοινό μυστικό ισοδύναμο με έναν 80-bit τυχαίο αριθμό.
- Βελτιωμένο προφίλ ασφάλειας (Improved Security Profile – SP2), το όποιο είναι βασισμένο στο SP1 αλλά παρέχει βελτιώσεις για την προστασία από τις επιθέσεις replay και λεξικού. [Αστέριος Αλμπανάκη, 2011; Φαφούλα Ιωάννα, 2008]

H.235.6 - Προφίλ κρυπτογράφησης φωνής
Αυτό το προφίλ χρησιμοποιείται για να προστατεύει κλειδιά που χρησιμοποιούνται για την κρυπτογράφηση media (RTP/RTCP) packets. Το προφίλ κρυπτογράφησης ανταλλάσσεται μεταξύ των τελικών σημείων ως τμήμα της τελικής διαπραγμάτευσης των δυνατοτήτων ασφαλείας. Έχει τη δυνατότητα να χρησιμοποίησει διάφορους αλγορίθμους κρυπτογράφησης, συμπεριλαμβανομένων των AES, RC2, DES, ή 3DES χρησιμοποιώντας την OFB (Output Feed Back) μέθοδο. Η διαπραγμάτευση των αλγορίθμων κρυπτογράφησης εκτελείται μέσω του H.245, όπου κάθε αλγόριθμος κρυπτογράφησης μπορεί να εφαρμοστεί σε έναν συγκεκριμένο codec και μαζί να διαμορφώσουν μια ευδιάκριτη ικανότητα για το τελικό σημείο. Αυτή η λεπτομέρεια επιτρέπει στα τελικά σημεία να διαβαθμίσουν τις επικοινωνίες τους σε μεγάλα κατανεμημένα περιβάλλοντα με άλλα τελικά σημεία όπως απαιτείται. [Αστέριος Αλμπανάκη, 2011; Φαφούλα Ιωάννα, 2008]



Εικόνα 2.13 Αυθεντικοποίηση του H.235.6 RTP για το antispam. [Φαφούλα Ιωάννα, 2008]

H.235.7 - Προφίλ ασφάλειας χρησιμοποιώντας τα MIKEY + SR
Το H.235.7 αποτελείται από τα ακόλουθα δύο προφίλ ασφαλείας:

- Βασισμένο σε συμμετρικό κλειδί (Symmetric key-based), υποδομή ασφαλείας που υποστηρίζει πολλαπλούς gatekeepers.
- Βασισμένο σε ασύμμετρο κλειδί (Asymmetric key-based) ,υποδομή ασφάλειας (PKI) που υποστηρίζει πολλαπλούς gatekeepers.

Τα MIKEY μηνύματα μεταφέρονται μαζί με τα H.245 handshake μηνύματα σηματοδοσίας κατά μήκος στα τελικά σημεία, διαφανή στους ενδιάμεσους gatekeepers. Τα handshake μηνύματα περιλαμβάνουν τα TerminalCapabilitySet, RequestMode, OpenLogicalChannel και MiscellaneousCommand. Το πρωτόκολλο MIKEY μπορεί να εφαρμοστεί στο επίπεδο συνόδου με το H.32 και στο media επίπεδο. Επίσης, το προφίλ παρέχει τη δυνατότητα διαπραγμάτευσης του υλικού κλειδιών με τη χρήση των συμμετρικών και ασύμμετρων τεχνικών. Στην περίπτωση όπου τα προ-κοινά κλειδιά χρησιμοποιούνται για να υποστηρίξουν το MIKEY, το προφίλ βασικής ασφάλειας εφαρμόζεται μεταξύ των hops.

Με αυτό το σενάριο, μια σχέση εμπιστοσύνης έχει εδραιωθεί χρησιμοποιώντας κοινά μυστικά μεταξύ κάθε hop και του προφίλ βασικής ασφάλειας. Αν και αυτή η διαμόρφωση μπορεί να είναι αποτελεσματική για τις μικρές ομάδες, δεν είναι εξελικτική για τις επικοινωνίες στα μεγάλα κατανεμημένα περιβάλλοντα. Για την υποστήριξη των επικοινωνιών σε μεγάλα κατανεμημένα περιβάλλοντα, πρέπει να χρησιμοποιηθεί ένας εξελικτικός μηχανισμός για τη δυναμική διαπραγμάτευση των κρυπτογραφικών κλειδιών.[Αστέριος Αλμπανάκη, 2011; Φαφούλα Ιωάννα, 2008]

H.235.8 - Ανταλλαγή κλειδιών για το SRTP σε ασφαλή κανάλια σηματοδοσίας**.**
Το H.235.8 παρέχει τους μηχανισμούς για την υποστήριξη της ανταλλαγής κλειδιών μαζί με τις παραμέτρους της αυθεντικοποίησης και του αλγορίθμου κρυπτογράφησης για τα SRTP ρεύματα μεταξύ των τερματικών H.323. Εστιάζει στις επικοινωνίες μονής εκπομπής και η ITU σκοπεύει να ερευνήσει τις επιλογές για πολλαπλής εκπομπής στο μέλλον.

Το πεδίο SrtpCryptoCapability χρησιμοποιείται για τη γνωστοποίηση των ικανοτήτων του SRTP που υποστηρίζονται από το H.323 τερματικό και μπορούν να χρησιμοποιηθούν κατά τη διάρκεια της διαπραγμάτευσης. Αυτό το υπό- πεδίο είναι μέσα στο genericH235SecurityCapability πεδίο και κάτω από τον encryptionAuthenticationAndIntegrity κλάδο του H.245 μηνύματος. Το

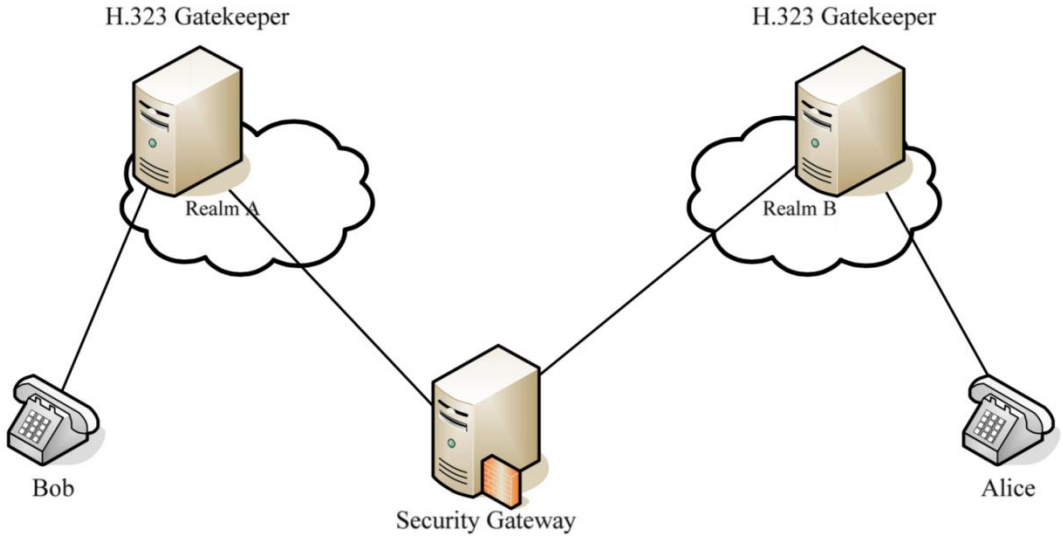
SrtpCryptoCapability περιέχει το SrtpCryptoInfo υπό-πεδίο που περιέχει τις παραμέτρους της crypto-ακολουθίας και της συνεδρίας που χρησιμοποιείται στην αντίστοιχη συνεδρία πολυμέσων, η οποία περιέχει μια SrtpCryptoInfo δομή και μια SrtpKeys δομή με μία ή περισσότερες SrtpKeyParameters.

Οι κρυπτογραφικές μετατροπές εξορισμού για το H.235.8 είναι οι AES με την μέθοδο μέτρησης και χρησιμοποιούν το μήκος των 128-bit. Ο κώδικας αλγόριθμου της αυθεντικοποίησης μηνυμάτων είναι ο SHA1, με μήκος 80-bit ή 32-bit. Επίσης, η AES f8 υποστηρίζεται με κλειδί των 128-bit και η SHA1 με μήκος 80-bit για το UMTS (Universal Mobile Telecommunications System). [Αστέριος Αλμπανάκη, 2011; Φαφούλα Ιωάννα, 2008]

H.235.9 - Πύλη ασφαλείας

Οι έλεγχοι ασφαλείας που καθορίζονται στις H.235.x συστάσεις, παρέχουν επαρκή υποστήριξη στην προστασία ενάντια στις διάφορες επιθέσεις και στην δημιουργία ασφαλών επικοινωνιών μεταξύ των συμμετεχόντων ενός H.323 δικτύου. Κάποιες από τις επιθέσεις περιλαμβάνουν την παραποίηση και την παραπλάνηση μηνυμάτων, την eavesdropping, και το SPIT. Συγχρόνως, αυτοί οι έλεγχοι ασφαλείας παρεμποδίζουν τις ροές κλήσης που διασχίζουν τα τμήματα δικτύου, όπως τα firewalls ή ALGs (application layer gateways), τροποποιούν τα μηνύματα της σηματοδοσίας και των media που ανταλλάσσονται. Το H.323 δεν είναι το μόνο πρωτόκολλο που επηρεάζεται από αυτήν την κατάσταση. Παρόμοια ζητήματα συνδέονται με τη SIP σηματοδοσία, όπου οι πληροφορίες της μεταφοράς μηνυμάτων, όπως οι IP διευθύνσεις και πόρτες, αλλάζουν από μια ενδιάμεση συσκευή. [Αστέριος Αλμπανάκη, 2011; Φαφούλα Ιωάννα, 2008]

Το H.235.9 πρέπει να εδραιώσει μια σχέση εμπιστοσύνης με τον τοπικό gatekeeper που χρησιμεύει για τη λήψη, την επεξεργασία, την τροποποίηση και τη διαβίβαση των μηνυμάτων της σηματοδοσίας και των media. Η σχέση αυτή εδραιώνεται όταν η πύλη ασφαλείας εγγράφεται στον τοπικό gatekeeper. Αυτή η σχέση εμπιστοσύνης επιτρέπει στην πύλη ασφαλείας να αποκτήσει πρόσβαση στο κλειδί αυθεντικοποίησης που διαπραγματεύεται μεταξύ του gatekeeper και του τελικού σημείου που θέλει να διαβιβάσει μηνύματα της σηματοδοσίας ή των media. Η κατοχή πρόσβασης στο κλειδί αυθεντικοποίησης επιτρέπει στην πύλη ασφαλείας να παραποιεί μη ιδιωτικά δεδομένα στα μηνύματα σηματοδοσίας και να αναπαραγάγει πληροφορίες αυθεντικοποίησης του μηνύματος πριν να το διαβιβάζει στον προορισμό του. Στην πιο κάτω εικόνα φαίνεται η τοποθέτηση της πύλης ασφαλείας.



Εικόνα 2.14 Τοποθέτηση πύλης ασφαλείας. [Φαφούλα Ιωάννα, 2008]

2.2 Machine Learning - Μηχανές Μάθησης

2.2.1 Τι είναι Μηχανική Μάθηση;

Ο κλάδος της τεχνητής νοημοσύνης που ασχολείται με τη μελέτη ή τη δημιουργία συστημάτων που έχουν την ικανότητα να “μαθαίνουν” από τα δεδομένα που τους δίνονται ονομάζεται μηχανική μάθηση (Machine Learning). Ό Arthur Samuel το 1959 έδωσε όρισε τη μηχανική μάθησης ως «ένα πεδίο μελέτης που δίνει στους ηλεκτρονικούς υπολογιστές τη δυνατότητα να μαθαίνουν χωρίς να έχουν ρητά προγραμματιστεί».

Η μηχανική μάθηση ασχολείται με όλες τις διαδικασίες που αναθέτουμε στους ηλεκτρονικούς υπολογιστές, που είναι πιο σύνθετες από τη διεκπεραίωση απλών προδιαγεγραμμένων και προγραμματισμένων διαδικασιών. Τα προβλήματα της μηχανικής μάθησης προς το παρόν εστιάζονται σε ένα ή σε περιορισμένο αριθμό δυνατοτήτων κάθε φορά. Οι εφαρμογές της μηχανικής μάθησης δίνουν τη δυνατότητα σε ένα σύστημα να κατηγοριοποιεί δεδομένα, να αναγνωρίζει χαρακτήρες ή πρόσωπα, να αναγνωρίζει ή να προσομοιώνει την ανθρώπινη φωνή, να αναλύει και να βγάζει συμπεράσματα από μια εικόνα. Επίσης, μέσα στα αντικείμενα μελέτης της

μηχανικής μάθησης είναι η ανίχνευση εισβολών σε δίκτυα ή η επιβεβαίωση απάτης, η ανάπτυξη παιχνιδιών, ο επαναπροσδιορισμός της διεπαφής χρήστη σύμφωνα με τις προτιμήσεις του χρήστη, οι μηχανές αναζήτησης (google), τα recommended systems, τα συστήματα εξαγωγής πληροφορίας και άλλες εφαρμογές. Ένα σύστημα μηχανικής μάθησης μπορεί να επεξεργαστεί δεδομένα από πίνακες, λίστες, εικόνες, χαρακτήρες ή ακόμη και συνδυασμός.

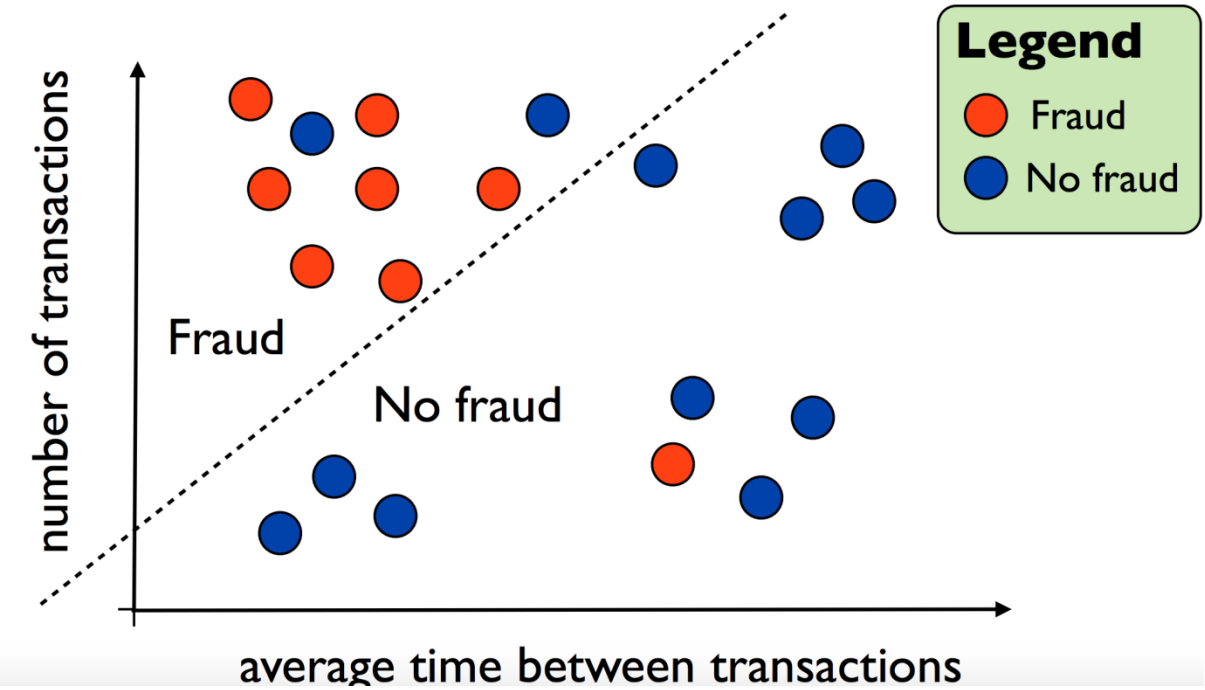
Υπάρχουν ποικίλα προβλήματα που καλείται να λύσει η μηχανική μάθηση. Το πιο σύνηθες πρόβλημα είναι αυτό της δυαδικής ταξινόμησης. Η μελέτη της έχει οδηγήσει σε πληθώρα εφαρμογών, αλγορίθμων, αλλά και θεωρητικών συμπερασμάτων. Σε μια ταξινόμηση τέτοιου είδους, το σύστημα καλείται να αποφασίσει σε ποια από τις δύο κλάσεις ανήκει το στοιχείο από το σύνολο των δεδομένων που επεξεργάζεται και να του δώσει την κατάλληλη τιμή ανάλογα με την κλάση. Ένα άλλο πρόβλημα είναι αυτό της πολλαπλής ταξινόμησης, αφού χρειάζεται μεγάλη προσοχή στην εφαρμογή του, ειδικά όταν τυγχάνει εφαρμογής σε δεδομένα που χρειάζονται λεπτό και ακριβή χειρισμό (π.χ ιατρικά δεδομένα). Άλλα προβλήματα που επιλύονται είναι προβλήματα οπισθοδρόμησης (π.χ. εκτίμηση μετοχής την επόμενη μέρα), προσέγγισης της δομής (π.χ. στην ταξινόμηση ιστοσελίδων), προσέγγισης της κατανομής, πρόβλεψης συμπεριφοράς ενός στοιχείου, δεδομένου ενός προτύπου ή πρόβλεψης ασυνήθιστης συμπεριφοράς, δεδομένου ενός προτύπου (π.χ. εντοπισμός κλήσεων απάτης , ανίχνευση εσωτερικών απειλών). [Alexandropoulou Chariklia, 2013]

2.2.2 Κατηγορίες μηχανισμών μάθησης

Οι μηχανισμοί μάθησης συνήθως ταξινομούνται σε τρεις κατηγορίες, ανάλογα με το είδος του εκπαιδευτικού συστήματος ή την ανατροφοδότηση που είναι διαθέσιμη στο σύστημα εκμάθησης.

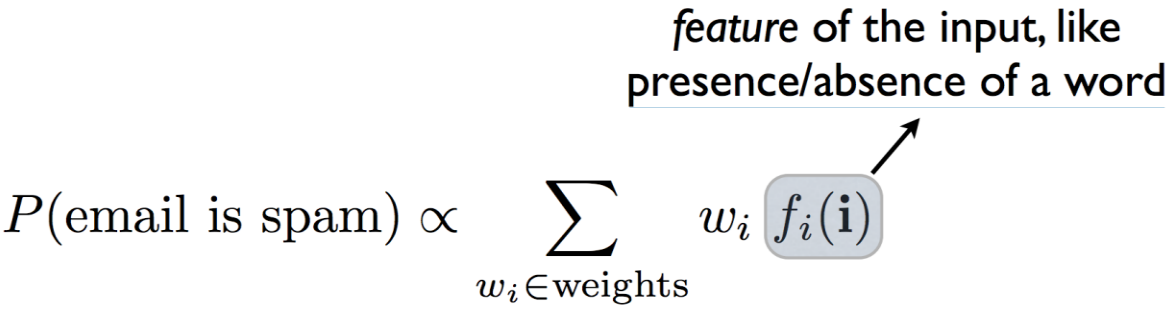
Επιτηρούμενη μάθηση (supervised learning)

Στην επιτηρούμενη μάθηση το υπολογιστικό πρόγραμμα δέχεται τις εισόδους, καθώς και τα επιθυμητά αποτελέσματα από έναν “δάσκαλο” και ο στόχος είναι να μάθει ο αλγόριθμος έναν γενικό κανόνα προκειμένου να αντιστοιχίσει τις εισόδους με τα αποτελέσματα.



Εικόνα 2.15 Γραφική παράσταση αλγόριθμου επιτηρούμενης μάθησης. [Pierre Lison, 2012]

Ένα παράδειγμα επιτηρούμενης μάθησης είναι το φιλτράρισμα των spam email. Σε σύστημα φιλτραρίσματος ανεπιθύμητων μηνυμάτων μπορεί για παράδειγμα να αποκτά βάρη “weights” που συνδέονται με κάθε πιθανή αγγλική λέξη. Έτσι, όσο υψηλότερο είναι το βάρος, τόσο μεγαλύτερη είναι η πιθανότητα το μήνυμα ηλεκτρονικού ταχυδρομείου να είναι spam. Ο αλγόριθμος εκμάθησης θα προσαρμόσει αυτά τα βάρη, ώστε να ταιριάζουν στα δεδομένα. [Richard A et al, 2010]



Εικόνα 2.16 Επιτηρούμενη Μάθηση για φιλτράρισμα spam email. [Pierre Lison, 2012]

Υπάρχουν αρκετοί αλγόριθμοι επιτηρούμενης μάθησης, μερικοί από αυτούς είναι:

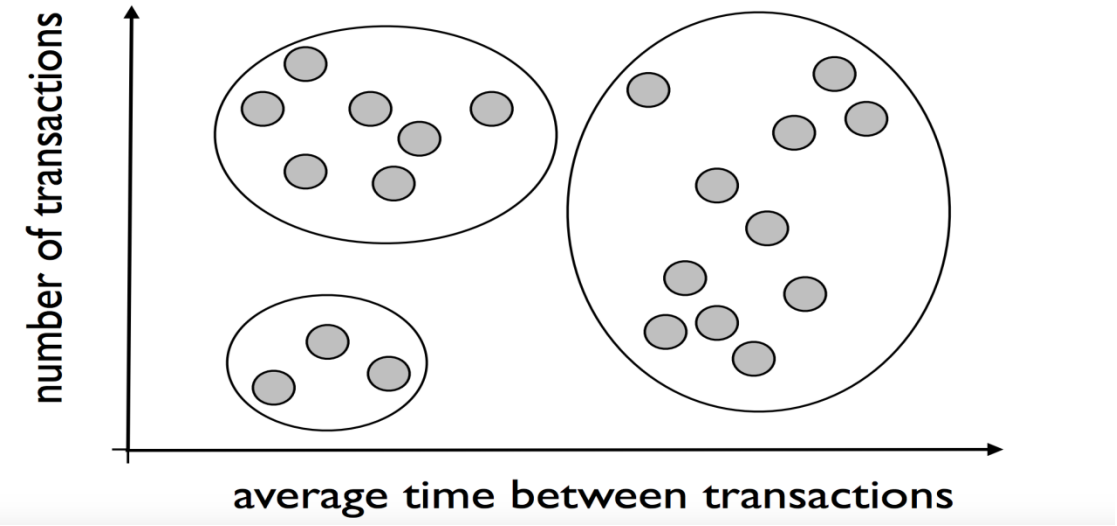
- Naive Bayes classifier
- Support Vector Machines (SVMs)

Μη επιτηρούμενη μάθηση (unsupervised learning)

Σε αυτή την κατηγορία δεν παρέχεται κάποια “εμπειρία” στον αλγόριθμο μάθησης, που πρέπει να βρει μόνος του τη δομή των δεδομένων εισόδου. Η μη επιτηρούμενη μάθηση μπορεί να είναι είτε αυτοσκοπός ή το μέσο για κάποιο αποτέλεσμα.

Μερικές φορές, δεν έχουμε πρόσβαση σε οποιαδήποτε τιμή εξόδου, έχουμε απλά μια συλλογή από παραδείγματα εισόδου. Σ’ αυτή την περίπτωση, προσπαθούμε να μάθουμε τα υποκείμενα μοντέλα των δεδομένων μας.

- Να κάνουμε συσχετισμό μεταξύ των χαρακτηριστικών
- Να συσσωρεύσουμε το σύνολο δεδομένων μας σε λίγες ομάδες που συμπεριφέρονται με παρόμοιο τρόπο και να εντοπίσουμε τις υπερβάσεις.



Εικόνα 2.17 Γραφική παράσταση αλγόριθμου μη επιτηρούμενης μάθησης. [Pierre Lison, 2012]

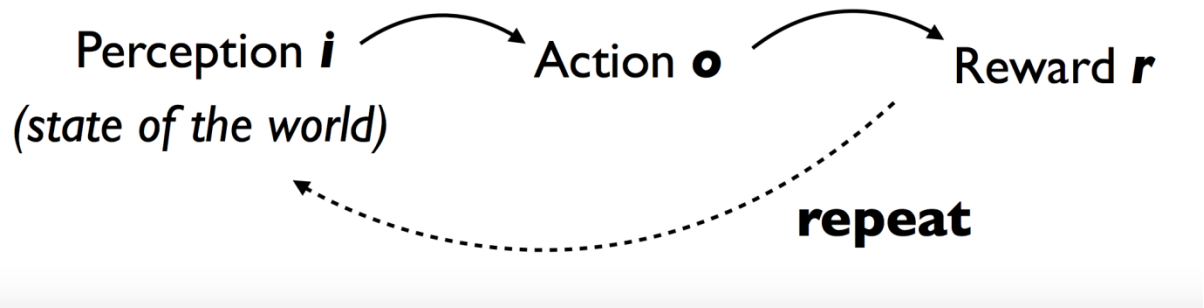
Ένα παράδειγμα εφαρμογής αυτής της κατηγορίας αλγορίθμου είναι και ο εντοπισμός των τηλεφωνικών κλήσεων απάτης. Δεν καθορίζεται από πριν το επιθυμητό αποτέλεσμα, βγάζοντας συμπεράσματα από τις ομαδοποιήσεις των αποτελεσμάτων που προκύπτουν. [Richard A et al, 2010]

Υπάρχουν αρκετοί αλγόριθμοι επιτηρούμενης μάθησης, μερικοί από αυτούς είναι:

- K-means clustering
- HCA (Hierarchical Cluster Analysis)
- Generative adversarial networks (GANs)
- Expectation–maximization (EM)
- ESOINN
- SOM (Self-organizing map)

Ενισχυτική μάθηση (reinforcement learning)

Ενισχυτική είναι η μάθηση όταν ένα πρόγραμμα υπολογιστή αλληλεπιδρά με ένα δυναμικό περιβάλλον στο οποίο πρέπει να επιτευχθεί ένας συγκεκριμένος στόχος, χωρίς να υπάρχει “δάσκαλος” να τον ενημερώνει αν έχει επιτευχθεί ό στόχος.



Εικόνα 2.18 Τρόπος λειτουργίας ενισχυτικής μάθησης. [Pierre Lison, 2012]

Ένα καλό παράδειγμα της ενισχυτικής μάθησης είναι η ρομποτική. Εφαρμόζοντας αλγόριθμο ενισχυτικής μάθησης η μηχανή αλληλεπιδρά σε δυναμικό περιβάλλον προσπαθώντας να επιτευχθεί ο στόχος που τέθηκε. [Richard Aet al, 2010]

Υπάρχουν αρκετοί αλγόριθμοι ενισχυτικής μάθησης, μερικοί από αυτούς είναι:

- Q-learning
- DTR (Dynamic Treatment Regime)
- TD (Temporal difference learning)

Κεφάλαιο 3 Βιβλιογραφική Ανασκόπηση

Η ανίχνευση απάτης στο διαδίκτυο αποτελεί ένα από τα πιο μεγάλα προβλήματα της νέας τεχνολογικής εποχής. Όλο και περισσότεροι χρήστες εκθέτουν προσωπικά στοιχεία στο διαδίκτυο και γίνονται στόχοι κακόβουλων χρηστών. Ένα σημαντικό πρόβλημα που επιφέρει ζημιές εκατομμυρίων ευρώ στις εταιρίες τηλεπικοινωνιών είναι οι κλήσεις απάτης (frauds calls) οι οποίες πραγματοποιούνται μέσω της υπηρεσίας VoIP. Στο πλαίσιο του τομέα των τηλεπικοινωνιών, ως κλήση απάτης ορίζεται μια τηλεφωνική κλήση που είτε δεν υπάρχει πρόθεση πληρωμής της ή γίνεται μέσω κλοπής της υπηρεσίας. Η πιο δύσκολη πτυχή της καταπολέμησης της απάτης είναι να γίνει έγκαιρα η αναγνώρισή της.

Στο άρθρο [Richard A et al, 2010] αναφέρεται ότι ένα σύστημα ανίχνευσης απάτης πρέπει να είναι ευέλικτο έτσι ώστε να ανταποκρίνεται γρήγορα και αποτελεσματικά σε διάφορους τύπους απάτης. Γίνεται αναφορά στις διεθνείς κλήσεις, όπου λόγω υψηλού κόστους προτείνεται οι έλεγχοι να επικεντρώνονται σε αυτή την κατεύθυνση. Επίσης, διαπιστώνεται πόσο σημαντικό είναι να γίνεται άμεσα ο εντοπισμός της κλήσης απάτης (ακόμη και την ίδια στιγμή), ώστε να παρθούν από τις εταιρίες τηλεπικοινωνιών διορθωτικά μέτρα άμεσα. Βάση του άρθρου, για να δημιουργηθεί μια τέτοια εφαρμογή πρέπει να έχουμε μια συνεχή πηγή πληροφοριών για κάθε κλήση, μια βάση δεδομένων για την αποθήκευση των δεδομένων, αλγόριθμους ανίχνευσης, ανθρώπους που θα διεξάγουν ελέγχους για πιθανές κλήσεις απάτης, καθώς και εργαλεία οπτικοποίησης ώστε να βοηθούν τη διάγνωση. Η εφαρμογή παρατηρεί τις κλήσεις ανά ώρα της ημέρας, ανά ημέρα της εβδομάδας, τη διάρκεια των κλήσεων, τον προορισμό των κλήσεων, τους πιο συχνούς προορισμούς των κλήσεων, τους συχνότερους αριθμούς τηλεφώνου που καλεί ο χρήστης και κατά πόσο χρεώνονται οι κλήσεις. Σε μεγάλα συστήματα ανάλυσης δεδομένων δεν υπάρχει τρόπος να αποσυνδεθεί η ίδια η ανάλυση των δεδομένων από την αποθήκευση, τη διαχείριση και την αποτύπωσή τους. Ως εκ τούτου, οι ερευνητές επισημαίνουν την ανεπάρκεια επεξεργασίας και ανάλυσης δεδομένων σε πραγματικό χρόνο και υπογραμμίζουν την αναγκαιότητα του ανθρώπινου δυναμικού στον εντοπισμό αυτών των κλήσεων, αναφέροντας ότι τα εργαλεία ανίχνευσης θα πρέπει να διευκολύνουν και όχι να αντικαθιστούν τον άνθρωπο. Πιστεύουμε ότι ένα τομέας που θα μπορούσε να τύχει

διαφορετικής προσέγγισης είναι οι διεθνείς κλήσεις. Μια διεθνής κλήση μεγάλου κόστους είναι πιο πιθανό να είναι αποτέλεσμα απάτης, κυρίως λόγω του κόστους της. Θα ήταν καλύτερα η έμφαση να δίνεται στον εντοπισμό των διαφορετικών κλήσεων από τις συνήθεις κλήσεις του εκάστοτε χρήστη, αφού οι κλήσεις αυτές μπορεί να είναι διεθνείς ή και κλήσεις εσωτερικού. Έχουν γίνει πολλές έρευνες με διάφορους αλγόριθμους ανίχνευσης κλήσεων άπατης. Θα αναφερθούμε σε μερικές από αυτές στη συνέχεια αυτού του κεφαλαίου.

Η ερεύνα των [Igor Ruiz-Agundez et al,2011] ασχολείται με τον αλγόριθμο Simple Exaction Maximization (EM). Επέλεξαν τον συγκεκριμένο αλγόριθμο επειδή υποστηρίζει ονομαστικά, δυαδικά, κενά και αριθμητικά χαρακτηριστικά, καθώς επίσης επιτρέπει και τη διαχείριση ελλιπών δεδομένων ή ενοποιημένων χαρακτηριστικών. Αυτό το πλεονέκτημα του συγκεκριμένου αλγορίθμου δίνει τη δυνατότητα για καλύτερη ανάγνωση και επεξεργασία των δεδομένων. Επιπρόσθετα, γίνεται χρήση του αλγόριθμου ΕΜ γιατί με βάση τα χαρακτηριστικά των δεδομένων που είχαν στη διάθεση τους οι ερευνητές, θα γινόταν καλύτερη ανάλυση των δεδομένων. Είναι σημαντικό να γνωρίζουμε καλά την κατάσταση των δεδομένων που θα χρησιμοποιήσουμε ώστε να κάνουμε σωστή επιλογή αλγορίθμου. Ο ΕΜ υποστηρίζει όλους τους τύπους χαρακτηριστικών τους οποίους χρησιμοποίησαν οι ερευνητές και αναγνωρίζει επίσης τον αριθμό των συστάδων στα οποία έπρεπε να διαιρείται το σύνολο των δεδομένων. Θεωρήθηκε σημαντικό επίσης για την επιλογή το μέτρο εγγύτητας (δηλαδή κατά πόσο όμοια είναι δύο σημεία δεδομένων) και το κριτήριο συγκέντρωσης (δηλαδή η συνάρτηση κόστους) αυτού του αλγορίθμου για υπολογισμούς. Ένας ακόμη λόγος που προτιμήθηκε αυτός ο αλγόριθμος είναι γιατί η μέθοδος της στοιχειώδους ομαδοποίησης είναι η μόνη που με τα δεδομένα που διέθεταν μπορούσε να δημιουργήσει ένα σαφές μοντέλο αναπαράστασης της γνώσης που περιγράφει τη συσσωμάτωση με τέτοιο τρόπο, ώστε να μπορεί εύκολα να γίνει ορατή και κατανοητή. Ο αλγόριθμος ομαδοποιεί τις κλήσεις με βάση τα CDRs που είχαν στη διάθεση τους σε 10 διαφορετικές συστάδες, ένα πολύ ικανοποιητικό αποτέλεσμα για τους ερευνητές, αφού είχαν ποσοστό επιτυχίας 96.22%. Στην ουσία ο συγκεκριμένος αλγόριθμος χώρισε τις κλήσεις σε 10 διαφορετικά προφίλ. Οι ερευνητές θα μπορούσαν να επεξεργαστούν καλύτερα τα δεδομένα ώστε να αντλήσουν περισσότερες πληροφορίες, όπως για παράδειγμα να διαχωρίσουν την ημερομηνία σε χρονιά, μήνα, ημέρα και ώρα. Επίσης, θα ήταν προτιμότερο τα CDRs που χρησιμοποιήθηκαν να αντιστοιχούν σε χρονικό διάστημα μεγαλύτερο του ενός μηνός. Σ' αυτήν την έρευνα παρατηρείται έλλειψη λεπτομερών δεδομένων, αλλά και χρήση μη πραγματικών δεδομένων από κάποιον τηλεπικοινωνιακό πάροχο, έτσι δεν

μπορούμε να ξέρουμε την ακρίβεια του EM σε πραγματικές συνθήκες. Κάλο θα ήταν να γίνεται αναφορά στον χρόνο που χρειάστηκε ο αλγόριθμος για δώσει το αποτέλεσμα. Στην έρευνα που έχουμε κάνει γίνεται λεπτομερής επεξεργασία των δεδομένων και τα CDRs που χρησιμοποιούμε είναι διάρκειας 2 μηνών.

Στην έρευνα των [Ahmed Aljarray and Abdulla Abouda, 2014] εξετάζεται ο εντοπισμός των κλήσεων απάτης σε κλήσεις που πραγματοποιούνται από κινητά τηλέφωνα με την μέθοδο “δέντρο αποφάσεων” (Decision Tree). Χρησιμοποίησαν 6 χαρακτηριστικά (Subscriber number(MSISDN), Other party called, CellIDin use by the subscriber, Date and time tge call was made, Duratation of the Call) από τα CDRs και δείγμα κλήσεων της χρονικής περιόδου μεταξύ Οκτωβρίου και Νοεμβρίου του 2014, προσπαθώντας να εντοπίσουν κυρίως τις κλήσεις απάτης που γίνονται με τη μέθοδο SIMBox. Στην παρούσα έρευνα οι ερευνητές αναφέρουν ότι όσο πιο μεγάλο είναι το δείγμα κλήσεων τόσο πιο ακριβή είναι τα αποτελέσματα που θα έχουν, φτάνοντας στο 97,95% σωστών αποτελεσμάτων. Τα δέντρα αποφάσεων είναι ισχυρά και δημοφιλή εργαλεία που χρησιμοποιούνται για την ταξινόμηση και την πρόβλεψη, αντιπροσωπεύουν κανόνες, οι οποίοι μπορούν να γίνουν κατανοητοί από τους ανθρώπους και να χρησιμοποιηθούν στα συστήματα γνώσης. Οι αλγόριθμοι επαγωγής δέντρων αποφάσεων λειτουργούν αναδρομικά. Πρώτα, πρέπει να επιλεγεί ένα χαρακτηριστικό ως κόμβος (root node), με σκοπό να δημιουργηθεί το πιο αποδοτικό δέντρο (δηλαδή το μικρότερο δέντρο). Ο κόμβος πρέπει να χωρίζει αποτελεσματικά τα δεδομένα έτσι ώστε να μην καταλήγει σε λάθος αποφάσεις. Η συγκεκριμένη έρευνα ασχολείται με ένα είδος απάτης που την κάνει πολύ στοχευμένη. Θεωρούμε ότι χρησιμοποιήθηκε ένα μικρό χρονικό δείγμα κλήσεων 2 μηνών. Η μέθοδος με δέντρα αποφάσεων μπορεί να αποφέρει θετικά αποτελέσματα αλλά θεωρούμε ότι λόγω του μεγάλου όγκου διαφορετικών δεδομένων που θα προκύψουν σε βάθος χρόνου, θα γίνουν πολύ περίπλοκα τα δέντρα (δυσανάγνωστα για τον άνθρωπο) και πιο αργά αφού θα υπάρχουν αρκετοί κόμβοι για να ληφθεί στο τέλος η σωστή απόφαση. Θα πρέπει να εξεταστεί κατά πόσο είναι εφικτή και κατά πόσο θα επηρεάσει μια μελλοντική αλλαγή των χαρακτηριστικών που ελέγχονται, ή ακόμα και μια αλλαγή του αριθμού των χαρακτηριστικών.

Ο ερευνητής [Olusola Adeniyi Abidogun,2005] ασχολείται με τη μη επιτηρούμενη (non supervisor) μάθηση δύο νευρωνικών δικτύων, τον αλγόριθμο αυτό-οργανωμένων χαρτών SOM (self-organizing map) και τον αλγόριθμο μακράς βραχυπρόθεσμης μνήμης LSTM (Long short-term memory). Ο σκοπός της έρευνας ήταν να διαπιστωθεί

αν ο LSTM μπορεί να χρησιμοποιηθεί για μη επιτηρούμενη μάθηση στην αναγνώριση κλήσεων απάτης με μεγάλο όγκο δεδομένων. Έτσι, χρησιμοποιήθηκαν κλήσεις από κινητά χρονικής διάρκειας 6 μηνών (227.318 κλήσεις) από 500 διαφορετικούς χρήστες. Ο SOM βοηθάει στην κατανόηση των δεδομένων των κλήσεων και στην αρχική αναζήτηση πιθανών εξαρτήσεων αλλά ο LSTM, διατηρώντας παράλληλα τη χρονική σειρά της ακολουθίας, αναδεικνύει τα κυριότερα χαρακτηριστικά των σχετικών προτύπων κλήσεων. Ο LSTM παρέχει καλύτερη ομαδοποίηση των κλήσεων από τον SOM και τα αποτελέσματα που εξάγει είναι σε πιο ευανάγνωστη μορφή οπότε είναι και πιο εύκολο για τον χρήστη να βγάλει τα συμπεράσματά του. Ο ερευνητής χρησιμοποίησε ένα αλγόριθμο, τον SOM, που χρησιμοποιείται συχνά σε παρόμοια προβλήματα και τον σύγκρινε με τον LSTM. Χρησιμοποίησε δείγμα κλήσεων με παρόμοια χαρακτηριστικά με αυτά που χρησιμοποιήσαμε κι εμείς στην έρευνά μας. Οι τιμές των χαρακτηριστικών που δεν είναι σε ώρες αιχμής θα μπορούσαν να ενισχυθούν ώστε να δίνεται στον αλγόριθμο μεγαλύτερη τιμή για να γίνονται πιο εμφανείς οι ύποπτες κλήσεις. Ένα σημαντικό πλεονέκτημα αυτής της έρευνας είναι ο μεγάλος αριθμός κλήσεων που είχε στη διάθεσή του ο ερευνητής, που τον βοήθησε να βγάλει πιο ακριβή αποτελέσματα. Θα μπορούσε να γίνει αναφορά στα ποσοστά(%) επιτυχίας των αλγορίθμων έτσι ώστε να μπορούν να συγκριθούν.

Σύμφωνα με την έρευνα [Ledisi G. Kabari,2016],υπάρχουν πολλών ειδών επιθέσεις και η ανίχνευσή τους μπορεί να γίνει σε πολλά επίπεδα. Οι απειλές σε ένα τηλεπικοινωνιακό δίκτυο είναι δυναμικές και έτσι οι οι κακόβουλοι χρήστες μπορούν να ελίσσονται, δηλαδή να αλλάζουν τον τρόπο των επιθέσεων. Η συγκερκιμένη έρευνα εστιάζει στην ανίχνευση συνδρομών απάτης (Subscription Fraud), που έχουν σκοπό να εκμεταλλευτούν τις υπηρεσίες τηλεπικοινωνίας που προσφέρονται, χωρίς να πληρώσουν ή προσφέροντας τις υπηρεσίες σε 3ους με σκοπό το κέρδος. Έτσι σε αυτήν την έρευνα, χρησιμοποιώντας τον αλγόριθμο Naive Bayesian, τα προσωπικά δεδομένα συνδρομητών (ηλικία, φύλο, ημερομηνία εγγραφής, πακέτο σύνδεσης) και τα CDRs, γίνεται έλεγχος κατά πόσο μπορούν να εντοπιστούν οι συνδρομές απάτης. Ο αλγόριθμος έχει τη δυνατότητα να χειριστεί ελλιπή στοιχεία, καλύπτοντάς τα με τον μέσο όρο του χαρακτηριστικού που εξετάζεται κάθε φορά. Αυτό μπορεί να διευκολύνει την εξαγωγή αποτελεσμάτων αλλά μπορεί να επιφέρει κάποια αλλοίωση που ίσως επηρεάσει τα αποτελέσματα. Η εκπαίδευση του αλγορίθμου ασχολείται με ένα μικρό αριθμό συνδρομών (21), επομένως δεν μπορούμε να θεωρήσουμε τα αποτελέσματά του αξιόπιστα. Παρόλο που ο αλγόριθμος Naive Bayesian είναι εύκολος στη χρήση του, αφού με μία απλή σάρωση μπορεί να δώσει αποτελέσματα, δεν συστήνεται για συνεχή έλεγχο μεγάλων δεδομένων.

Σε αυτή την έρευνα [Sandra Kübler et al, 2015] εξετάζεται ένας μεγάλος αριθμός κλήσεων απάτης που παρατηρήθηκε το 2014 στην Γερμανία. Αυτές οι κλήσεις πραγματοποιήθηκαν μέσω συσκευών δρομολόγησης AVM FRITZ!Boxes, από κακόβουλους χρήστες σε προορισμούς στο εξωτερικό. Σ' αυτήν την έρευνα δόθηκε έμφαση στις κλήσεις εξωτερικού. Έτσι δημιουργήθηκαν 2 κατηγόριες κλήσεων εξωτερικού για κάθε χρήστη, η "IntCallsPattern" που όλες οι κλήσεις είναι συνδεδεμένες με διεθνή προορισμό σε ώρες που ταιριάζουν με το προφίλ του χρήστη και η "IntCallsAfterHoursPattern" πού όλες οι κλήσεις είναι συνδεδεμένες με διεθνή προορισμό αλλά έχουν διεξαχθεί σε ώρες που δεν ταιριάζουν με το προφίλ του χρήστη. Τα δεδομένα που είχαν στη διάθεση τους οι ερευνητές ήταν 7 εβδομάδων και οι εξερχόμενες κλήσεις ανέρχονταν στα 2.749.860. Για να δημιουργηθεί το προφίλ των χρηστών χρησιμοποιήθηκαν οι αλγόριθμοι ομαδοποίησης K-Means, EM και SOM μέσω του εργαλείου WEKA και κλήσεις χρονικού διαστήματος 1 εβδομάδας για τις όποιες δεν υπήρχε αναφορά για κλήσεις απάτης. Από τις 2.749.860 κλήσεις που ελέγχθηκαν οι 17110 ήταν κλήσεις απάτης. Στην έρευνα γίνεται αναφορά σε ένα χρήστη - τηλεφωνικό κέντρο του οποίου δεν υπολογίστηκαν οι κλήσεις του γιατί δεν είχει ξεκάθαρο προφίλ λόγω των πολλών και ακανόνιστων κλήσεων εξωτερικού. Έτσι έγινε έλεγχος για 13.503 κλήσεις απάτης με επιτυχία 98,4% και αποτυχία 0,01%. Είναι πολύ σημαντικό να γνωρίζουμε τα δεδομένα με τα οποία δουλεύουμε, για να μπορούμε να αποκλείσουμε κάποια που μπορεί να επηρεάσουν αρνητικά τα αποτελέσματά μας. Η έρευνα όπως αναφέραμε πιο πάνω περιορίζεται σε 2 κατηγορίες κλήσεων εξωτερικού του χρήστη, ενω υπάρχει η δυνατότητα για περισσότερες. Θα ήταν καλύτερα να μην κατηγοριοποιούνται τα αποτελέσματα των χρηστών, αφού κάθε χρήστης μπορεί να αποτελεί μια ξεχωριστή κατηγορία με τα δικά του ειδικά χαρακτηριστικά.

Μια άλλη έρευνα [Pilsung Kang, 2014] ασχολείται με τον αλγόριθμο One-NB (One-Class Naive Bayesian), για να ελέγξει κατα πόσο μπορεί να προσφέρει καλύτερα αποτελέσματα έχοντας μικρότερο δείγμα κλήσεων απάτης. Η σύγκριση γίνεται με τους αλγόριθμους Gauss, MoG, K-Means, Parzen και K-NN. Επίσης, στην έρευνα αυτή γίνεται προσπάθεια να παραχθούν καλύτερα αποτελέσματα χρησιμοποιώντας λιγότερα χαρακτηριστικά από τα CDRs. Τα δεδομένα της έρευνας δόθηκαν από ένα κορεάτικο πάροχο τηλεπικοινωνιών. Χρησιμοποιήθηκαν 14 χαρακτηριστικά από τα CDRs και κλήσεις χρονικού διαστήματος 1 μήνα. Στις κλήσεις των πρώτων 2 βδομάδων αντιστοιχούσε σχεδόν το 50% των κλήσεων απάτης (1η εβδομάδα - 46.33%, 2η εβδομάδα - 49.55%), της 3ης εβδομάδας αντιστοιχούσε το 16.42% και της

4ης εβδομάδας το 4.47%. Έτσι με αυτά τα δεδομένα μπόρεσαν να ελέγξουν την αξιοπιστία του One-NB μέσα σε ένα περιβάλλον με μεγάλο αλλά και μικρό ποσοστό κλήσεων απάτης. Για τη βελτίωση της απόδοσης ανίχνευσης κλήσεων απάτης χρησιμοποιήθηκε ο genetic algorithm (GA) για την επιλογή σημαντικών μεταβλητών. Ο GA βρίσκει ένα σύνολο ψευδό-βέλτιστων (pseudo-optimal) μεταβλητών εισόδου που βασίζονται σε μια εξελικτική μέθοδο αναζήτησης. Στην έρευνα σημειώνεται ότι ο αλγόριθμος One-NB μαζί με τον GA χρησιμοποίησε κατά μέσο όρο 3,33 μεταβλητές, ενώ ο αμέσως επόμενος αλγόριθμος ήταν ο Gauss με 3,67 μεταβλητές. Τα αποτελέσματα της έρευνας χωρίζονται αναλόγως του ποσοστού κλήσεων απάτης που πραγματοποιήθηκαν εβομαδιαία. Η πρώτη εβδομάδα χρησιμοποιήθηκε για εκπαίδευση. Οι επομένες 3 εβδομαδες χρησιμοποίηθηκαν για τον έλεγχο των αλγορίθμων, σε 3 στάδια. Την 2η εβδομάδα, με ποσοστό κλήσεων απάτης 49,55%, τα πιο επιτυχή αποτελέσματα τα είχε ο αλγόριθμος Gauss (0.9721) , ο One-NB είχε ένα κάλο ποσοστό(0.9689), αλλά όχι το καλύτερο. Την 3η βδομάδα, με ποσοστό κλήσεων απάτης (16,42%), την καλύτερη απόδοση την είχε ο One-NB με ποσοστό 0.8893 και την 4η βδομάδα, με ποσοστό κλήσεων απάτης (4,47%), ο αλγόριθμος που εξετάζεται είχε την υψηλότερη επιτυχία (0.7564) με αρκετή διαφορά από τον δεύτερο, k-NN, που είχε ποσοστό 0.7327. Στην έρευνα επισημαίνεται πόσο σημαντικό είναι έστω και το 1% καλύτερου αποτελέσματος στη συγκεκριμένη περίπτωση, από τη στιγμή που γίνονται δισεκατομμύρια κλήσεις την βδομάδα. Τα στοιχεία της έρευνας δείχνουν ότι μπορεί να γίνει πολύ καλός εντοπισμός των κλήσεων απάτης, ακόμα και όταν υπάρχουν σε μικρό ποσοστό οι κλήσεις αυτές. Η ερεύνα δείχνει επίσης πόσο σημαντική είναι η σωστή ανάγνωση των χαρακτηριστικών των CDRs, αφού με τη βοήθεια του GA πέτυχαν την ελάχιστη δυνατή χρήση τους με το καλύτερο δυνατό αποτέλεσμα. Θα ήταν σημαντικό όμως να γνωρίζουμε τον χρόνο που χρειάζεται ο αλγόριθμος για να δώσει τα σωστά αποτελέσματα και ακόμα καλύτερα ο χρόνος που χρειάζεται σε συνδυασμό με τον GA αλλά και χωρίς αυτόν. Σε αυτή την έρευνα εξετάζονται δισεκατομμύρια κλήσεις και είναι πολύ σημαντικός παράγοντας ο χρόνος εντοπισμού των κλήσεων απάτης.

Για την επεξεργασία των δεδομένων όσο και για τον εντοπισμό των κλήσεων απάτης χρειαζόμαστε γρήγορους και αποτελεσματικούς αλγόριθμους. Αυτό επισημαίνεται στην έρευνα των [Abdikarim Hussein Elmiet al, 2014] όπου γίνεται έλεγχος των αλγορίθμων artificial neural network (ANN) και Support Vector Machine (SVM) για την ταχύτητα και την ακρίβεια των αποτελεσμάτων που μπορούν να μας δώσουν. Τα δεδομένα που λήφθησαν από τα CDRs δεν χρησιμοποιήθηκαν άμεσα για την εξόρυξη δεδομένων, δεδομένου ότι ενδέχεται να περιέχουν αναξιόπιστα αλλά και δεδομένα με

θόρυβο (noise) ή άσχετα και περιττά δεδομένα. Πριν από την ανάπτυξη του μοντέλου, τα δεδομένα υποβλήθηκαν σε διαδικασία προεπεξεργασίας, όπως η εξαγωγή χαρακτηριστικών, η ενσωμάτωση δεδομένων, ο χειρισμός δεδομένων που λείπουν, καθώς και η αναγνώριση και αφαίρεση των περιττών δεδομένων. Μετά το πέρας της επεξεργασίας, οι ερευνητές δημιούργησαν ένα σύνολο από εννέα χαρακτηριστικά προκειμένου να ανιχνευθεί η απάτη του SIMBox που αφορά κλήσεις της κινητής τηλεφωνίας. Γίνεται αναφορά στα multilayer perceptron (MLP) που χρησιμοποιούν οι αλγόριθμοι ANN και SVM, τονίζοντας πως είναι μια ελπιδοφόρα λύση σε προβλήματα αυτού του είδους, καθώς μπορούν να διαχειριστούν πολύπλοκα μοτίβα μέσα σε δεδομένα με θόρυβο. Ο αλγόριθμος ANN έχει έναν αριθμό εισόδων και μία έξοδο, συνδυάζει όλες τις τιμές εισόδου, πραγματοποιεί ορισμένους υπολογισμούς και στη συνέχεια ενεργοποιεί μια τιμή εξόδου. Υπάρχουν διάφοροι τρόποι συνδυασμού των χαρακτηριστικών εισόδων. Μία από τις πιο δημοφιλείς μεθόδους είναι το σταθμισμένο άθροισμα, όπου το άθροισμα κάθε τιμής εισόδου πολλαπλασιάζεται με ένα σχετικό βάρος. Ο αλγόριθμος SVM βασίζεται στην ιδέα της διαρθρωτικής διαχείρισης κινδύνων (Structural Risk Management - SRM). Το SVM είναι μια σχετικά νέα υπολογιστική μέθοδος μάθησης που κατασκευάστηκε με βάση τον ταξινομητή της θεωρητικής μάθησης της στατιστικής. Δημιουργεί ένα υπέρ-επίπεδο χρησιμοποιώντας ένα γραμμικό μοντέλο για να εφαρμόσει μη γραμμικά όρια κλάσης, μέσω κάποιων μη γραμμικών διανυσμάτων εισόδου χαρτογράφησης σε ένα χώρο υψηλών διαστάσεων. Στη σύγκριση των αλγορίθμων όσον αφορά την ακρίβεια, τον χρόνο και το σφάλμα γενίκευσης, τα αποτελέσματα της απόδοσης του αλγόριθμου SVM για τον χειρισμό της ανίχνευσης απάτης είναι πολύ καλύτερα από αυτά του αλγόριθμου ANN. Στα αποτελέσματα της έρευνας βλέπουμε ότι ο αλγόριθμος ANN έχει RMSE 0,104, επιτυχία 98,7% και χρόνο 17,17 δευτερόλεπτα. Αντίθετα ο SVM, που παρόλο πού έχει παρόμοιες τιμές στο RMSE με 0,105 και Accuracy 98,9%, έχει μεγάλη διαφορά στον χρόνο με 5,68 δευτερόλεπτα, περίπου στο ⅓ από τον ANN. Σε αυτήν την έρευνα φαίνεται πόσο σημαντική είναι η σωστή αξιοποίηση των δεδομένων, αλλά και πόσο σημαντικό ρόλο παίζει ο χρόνος διεκπεραίωσης του ελέγχου.

Κεφάλαιο 4 Μεθοδολογία

Στο κεφάλαιο αυτό γίνεται αναφορά στα νευρωνικά δίκτυα και αναλύεται η μεθοδολογία που χρησιμοποιήθηκε για τον εντοπισμό των κλήσεων απάτης. Παρουσιάζεται ο αλγόριθμος μη επιτηρούμενης μάθησης Enhanced Self-Organizing Incremental Neural Networks – ESOINN, που ανήκει στην κατηγορία των τεχνικών νευρωνικών δικτύων. Ο αλγόριθμος ESOINN είναι η εξέλιξη του αλγορίθμου SOINN (Self-Organizing Incremental Neural Networks).

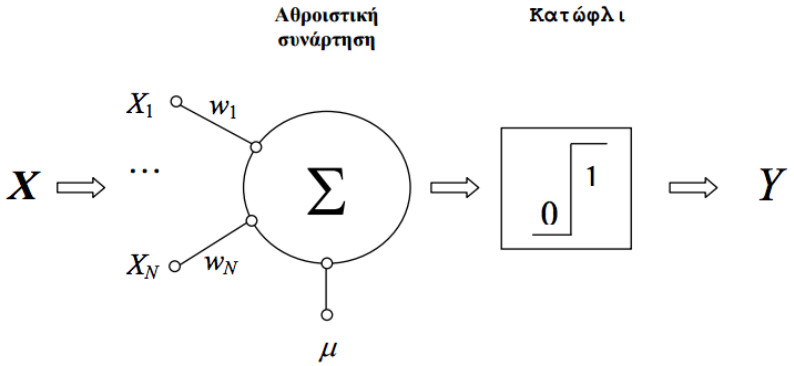
4.1 Τεχνητά Νευρωνικά Δίκτυα

Τα τεχνητά νευρωνικά δίκτυα (Artificial Neural Networks) αποτελούν μια μέθοδο μοντελοποίησης σύνθετων προβλημάτων πρόβλεψης με μεγάλο αριθμό εξαρτημένων μεταβλητών. Τα νευρωνικά δίκτυα χρησιμοποιούν ένα σύνολο κόμβων παρόμοιων με τους νευρώνες του ανθρώπινου εγκεφάλου. Οι κόμβοι συνδέονται μεταξύ τους σε ένα δίκτυο το οποίο έχει τη δυνατότητα να αναγνωρίζει πρότυπα μέσα σε ένα σύνολο δεδομένων μόλις αυτά παρουσιαστούν, δηλαδή το δίκτυο μπορεί να μαθαίνει από την εμπειρία που αποκτά.

Μια σημαντική μονάδα των τεχνητών νευρωνικών δικτύων είναι ο νευρώνας (perceptron), ο οποίος έχει σαν είσοδο ένα διάνυσμα πραγματικών τιμών και σχηματίζει ένα γραμμικό συνδυασμό των τιμών αυτών. Έπειτα παίρνει τιμή 1, αν ο συνδυασμός αυτός είναι μεγαλύτερος από κάποιο όριο και -1 σε κάθε άλλη περίπτωση. Γι' αυτό, αν $o(x_1...x_n)$ είναι ο νευρώνας που έχει σαν είσοδο το διάνυσμα $(x_1..x_n)$, τότε μπορούμε να το γράψουμε:

$o(x_1...x_n) = 1$ αν $w_0+w_1x_1+w_2x_2+...w_nx_n > 0$, αλλιώς σε οποιαδήποτε άλλη περίπτωση $o(x_1...x_n)= -1$.

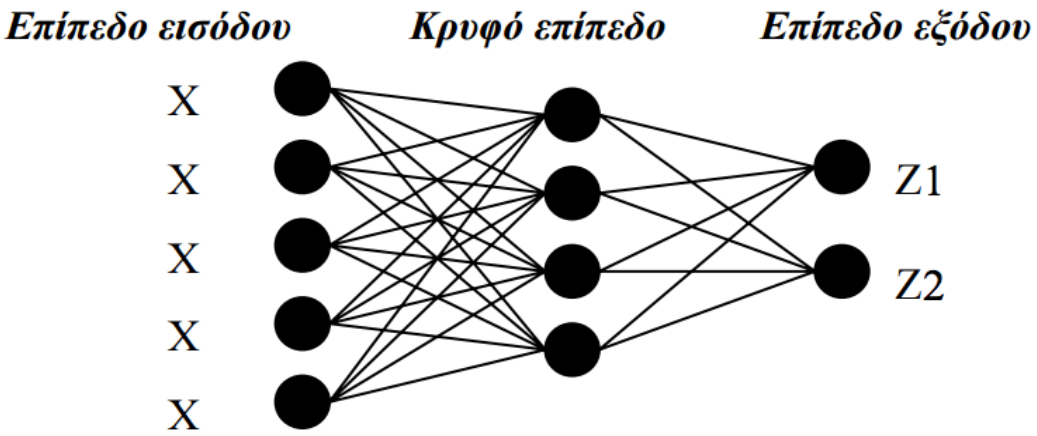
Οι τιμές w_i ονομάζονται βάρη και ορίζουν την επιρροή που έχει κάθε είσοδος x_i στη διαμόρφωση του γραμμικού συνδυασμού.



Εικόνα 4.1 Σχηματική αναπαράσταση του ενός νευρώνα. [Σωτήρης Β. Κωτσιαντής, 2005]

Νευρωνικά δίκτυα

Η αρχιτεκτονική των νευρωνικών δικτύων χαρακτηρίζεται από ένα δίκτυο του οποίου οι κόμβοι κατανέμονται σε ένα επίπεδο εισόδου (input layer), σε ένα επίπεδο εξόδου(output layer) και σε ένα ή περισσότερα ενδιάμεσα κρυμμένα επίπεδα (hidden layers). Η δομή των νευρωνικών δικτύων είναι ανάλογη με την πιο κάτω εικόνα 4.2.



Εικόνα 4.2 Παράδειγμα νευρωνικού δικτύου. [Σωτήρης Β. Κωτσιαντής, 2005]

Στο νευρωνικό δίκτυο, κάθε ένας από τους κόμβους εισόδου αναπαριστά και μία ανεξάρτητη μεταβλητή εισόδου. Στη συνέχεια, κάθε κόμβος εισόδου συνδέεται με όλους τους άλλους κόμβους στο πρώτο κρυμμένο επίπεδο. Οι κόμβοι του κρυμμένου επιπέδου συνδέονται με κόμβους ενός άλλου κρυμμένου επιπέδου ή με κόμβους στο επίπεδο εξόδου(αν δεν υπάρχει άλλο επίπεδο μετά). Οι κόμβοι στο επίπεδο εξόδου αναπαριστούν μια ή περισσότερες μεταβλητές εξόδου, αναλόγως του προβλήματος.

Οι κόμβοι του νευρωνικού δικτύου ονομάζονται επίσης νευρώνες, ενώ οι δεσμοί ονομάζονται «συνάψεις». Σε κάθε σύναψη αντιστοιχεί ένα βάρος που ονομάζεται «συνοπτικό βάρος». Συνεπώς, η αρχιτεκτονική ή τοπολογία ενός νευρωνικού δικτύου προσδιορίζεται από τον αριθμό των κόμβων, τον αριθμό των κρυμμένων επιπέδων και τον τρόπο που οι κόμβοι συνδέονται μεταξύ τους. Ο αριθμός των κρυμμένων επιπέδων και κόμβων και ενδεχομένως, τα όρια μέσα στα οποία θα κυμαίνονται τα συνοπτικά βάρη είναι στοιχεία που προσδιορίζονται στη φάση σχεδιασμού του νευρωνικού δικτύου. Συνήθως, δεν χρησιμοποιούνται σε ένα νευρωνικό δίκτυο παραπάνω από ένα κρυφά επίπεδα, καθώς έχει παρατηρηθεί ότι η χρήση περισσότερων αυξάνει κατά πολύ τον χρόνο εκπαίδευσης χωρίς να συνεπάγεται και με αντίστοιχη αύξηση της απόδοσης του δικτύου.

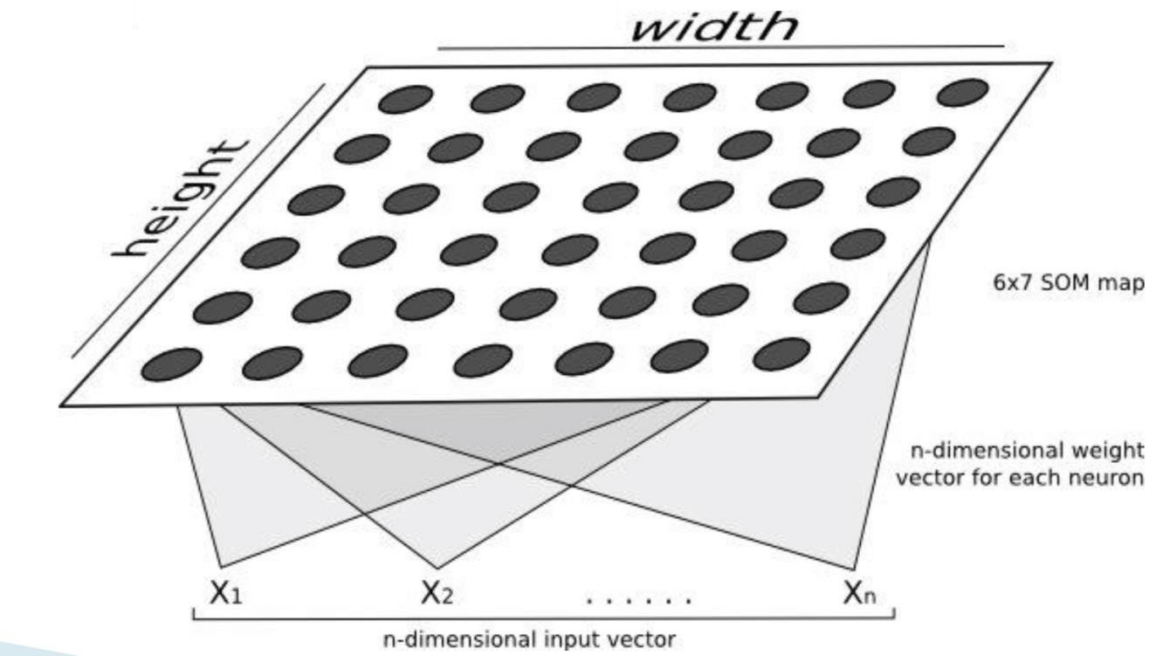
Όπως είπαμε, κάθε κόμβος στο κρυφό επίπεδο είναι πλήρως συνδεδεμένος με τις εισόδους, γεγονός που σημαίνει ότι το πεδίο βασίζεται σε όλες τις εισόδους τις οποίες και συνδυάζει στις τιμές εξόδου. Ο συνδυασμός αυτός ονομάζεται συνάρτηση ενεργοποίησης του κόμβου. Η συνάρτηση ενεργοποίησης αποτελείται από δύο μέρη. Το πρώτο μέρος είναι η συνάρτηση σύνδεσης (combination function), η οποία συνδυάζει όλες τις εισόδους σε μία απλή τιμή. Το δεύτερο μέρος της συνάρτησης είναι η συνάρτηση μεταφοράς (transfer function), η οποία μεταφέρει την τιμή της συνάρτησης σύνδεσης στην έξοδο. [Σωτήρης Β. Κωτσιαντής, 2005]

4.2 SOM - Self-organizing map

Ο αλγόριθμος SOM αυτο-οργάνωσης χαρτών άρχισε να χρησιμοποιείτε το 1981 από τον Kohonen. Στην αρχική έκδοση του αλγορίθμου ο Kohonen όρισε ένα δίκτυο νευρώνων, των οποίων η διασύνδεση χωρίζεται σε δύο τμήματα: ένα απλό στρώμα συσσωρευτικής μνήμης μεταξύ των εισόδων και των νευρώνων και ένα πλευρικό στρώμα που διασυνδέει τους νευρώνες τοπικά. Ο σκοπός του συνεταιριστικού στρώματος συνίσταται στην κωδικοποίηση των συναπτικών βαρών προκειμένου να δημιουργηθεί διαδοχικά μια συνειρμική μνήμη, ανάλογα με τις διαδοχικές παρουσιάσεις των εισροών. Το δεύτερο στρώμα πραγματοποιεί ένα είδος βελτίωσης της αντίθεσης που δημιουργεί ένα σύμπλεγμα με κέντρο γύρω από το τοπικό μέγιστο της απόκρισης σε ένα ερέθισμα εισόδου. Ο συνδυασμός των δύο στρωμάτων, που συνδέεται με έναν κατάλληλο κανόνα προσαρμογής, οδηγεί σε μια χωρική διάταξη των νευρώνων στο σύστημα συντεταγμένων βάρους στο οποίο γειτονικοί νευρώνες ανταποκρίνονται σε γειτονικά ερεθίσματα.

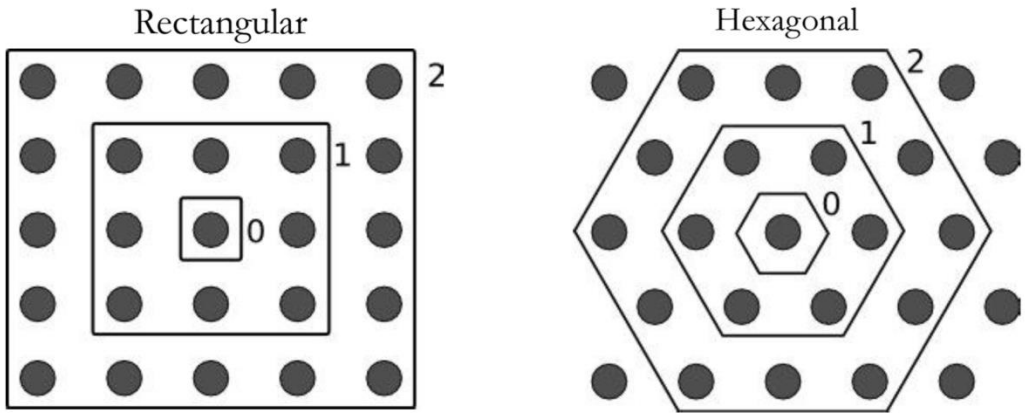
Ο βαθμός πλευρικής σύζευξης μεταξύ των νευρώνων στο δεύτερο στρώμα ορίζεται από τη λειτουργία "Mexican hat". Σε απόσταση βραχυχρόνιας πλευρικής σύζευξης η λειτουργία είναι διεγερτική, ενώ είναι ανασταλτική σε μεγάλη απόσταση. Η φάση χαλάρωσης που ακολουθεί τη δημιουργία της δραστηριότητας των νευρώνων συγκλίνει σε μια σταθερή κατάσταση με το σχηματισμό ενός συμπλέγματος δραστηριότητας γύρω από τον μέγιστο νευρώνα δραστηριότητας. Αυτή η διαδικασία είναι το πιο υπεύθυνο φαινόμενο για την αυτό-οργάνωση.

Οι πρώτες εφαρμογές του SOM αφορούσαν κυρίως τον τομέα της μηχανικής. Σταδιακά ο αλγόριθμος έγινε περισσότερο αποδεκτός ως μία τυποποιημένη μέθοδος ανάλυσης δεδομένων σε μια μεγάλη ποικιλία τομέων που μπορούν να αξιοποιήσουν τη μάθηση χωρίς επίβλεψη: ομαδοποίηση, οπτικοποίηση, οργάνωση δεδομένων, χαρακτηρισμός και εξερεύνηση.



Εικόνα 4.3 Αρχιτεκτονική του νευρωνικού δικτύου SOM
[Bruno Silva, 2008]

Ένας χάρτης αυτό-οργάνωσης αποτελείται από στοιχεία που ονομάζονται κόμβοι (νευρώνες). Σε κάθε κόμβο συνδέεται ένας φορέας βάρους της ίδιας διάστασης με τους φορείς δεδομένων εισόδου και μια θέση στο χώρο του χάρτη. Η συνήθης διάταξη κόμβων είναι μια δισδιάστατη τακτική απόσταση σε ένα εξαγωνικό (hexagonal) ή ορθογώνιο (rectangular) πλέγμα. Ο SOM περιγράφει την αντιστοίχιση ενός χώρου υψηλότερων διαστάσεων προς ένα μικρότερο χώρο-χάρτη. Η διαδικασία για την τοποθέτηση ενός διανύσματος από το χώρο δεδομένων στον χάρτη είναι να βρεθεί ο κόμβος με το διάνυσμα βάρους που βρίσκεται πλησιέστερα (με τη μικρότερη απόσταση μέτρησης) στον διανυσματικό χώρο δεδομένων.



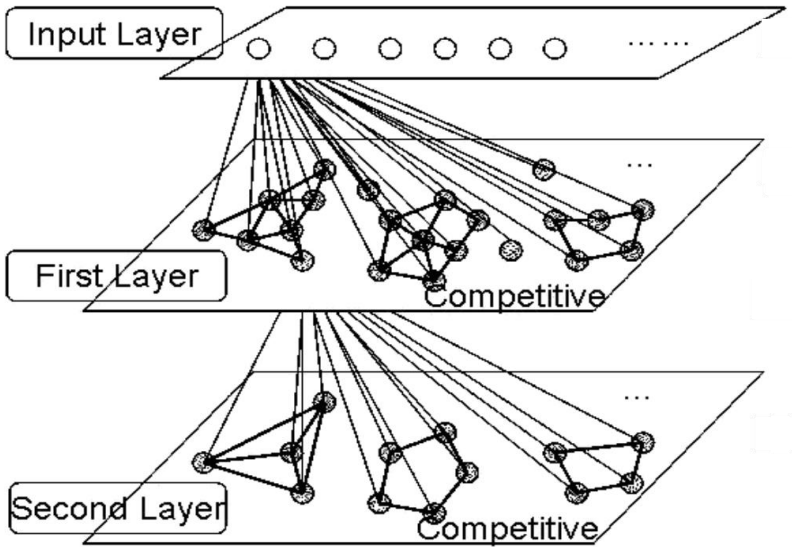
Εικόνα 4.4 Πλέγματα SOM. [Bruno Silva, 2008]

Η εκπαίδευση χρησιμοποιεί ανταγωνιστική μάθηση. Όταν ένα παράδειγμα εκπαίδευσης τροφοδοτείται στο δίκτυο, υπολογίζεται η ευκλείδεια απόσταση σε όλους τους φορείς βάρους. Ο νευρώνας του οποίου ο φορέας βάρους είναι περισσότερο παρόμοιος με την είσοδο ονομάζεται μονάδα καλύτερης αντιστοίχισης (Best Machine Unit). Τα βάρη του BMU και των νευρώνων που βρίσκονται κοντά του στο SOM πλέγμα προσαρμόζονται προς το διάνυσμα εισόδου. Το μέγεθος της αλλαγής μειώνεται με τον χρόνο και με την απόσταση (εντός του πλέγματος) από τον ανελκυστήρα. Ο τύπος ενημέρωσης για έναν νευρώνα k με τον φορέα βάρους W_k είναι : $W_k(t+1)= W_k(t) + \alpha(t)h_{ck}(t)[x(t)] - W_k(t)]$. [Pierre Demartines,1992; Bruno Silva ,2008]

4.3 SOINN - Self-Organizing Incremental Neural Networks

Ο αλγόριθμος SOINN παρουσιάστηκε από τους Furao και Hasegawa το 2006. Βασίζεται στη γενική ιδέα των χαρτών αυτό- οργάνωσης και της αυξητικής μάθησης.

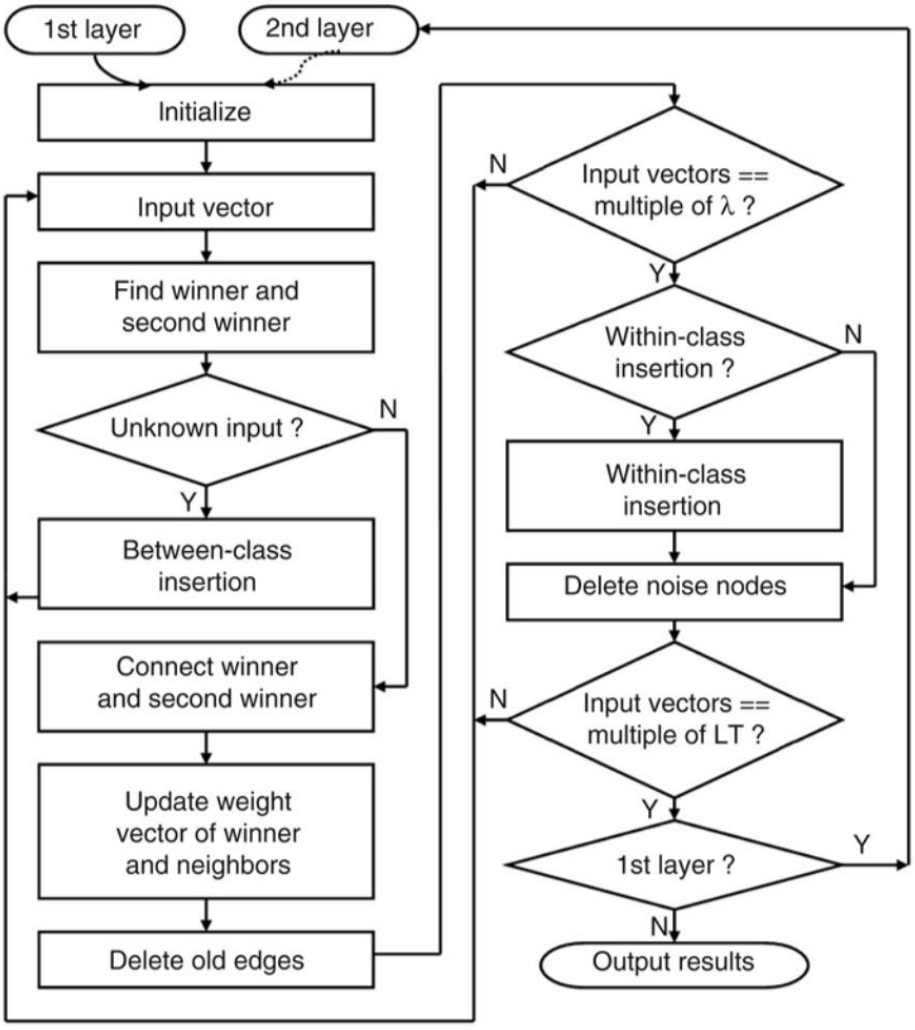
Υιοθετεί ένα δίκτυο δύο επιπέδων. Το πρώτο στρώμα μαθαίνει την κατανομή πυκνότητας των δεδομένων εισόδου και χρησιμοποιεί κόμβους και ακμές για να αντιπροσωπεύει τη διανομή. Το δεύτερο στρώμα διαχωρίζει τις συστάδες ανιχνεύοντας την περιοχή χαμηλής πυκνότητας των δεδομένων εισόδου και χρησιμοποιεί λιγότερους κόμβους από το πρώτο στρώμα για να αντιπροσωπεύει την τοπολογική δομή των δεδομένων εισόδου. Όταν ολοκληρωθεί η εκμάθηση του δεύτερου επιπέδου, το SOINN αναφέρει τον αριθμό των συστάδων και δίνει τυπικούς κόμβους πρωτοτύπου κάθε συμπλέγματος. Επίσης, υιοθετεί τον ίδιο αλγόριθμο μάθησης για το πρώτο και το δεύτερο επίπεδο. Ο τρόπο λειτουργίας των δύο επιπέδων φαίνεται στην εικόνα 4.1. [Shen Furaoa et al, 2007]



Εικόνα 4.5 Τρόπος εκμάθησης των δύο επιπέδων στον SOINN.
[F. Shen O. Hasegawa., 2009]

Όταν ένα διάνυσμα εισόδου δίνεται στον SOINN, αυτός βρίσκει τον πλησιέστερο

κόμβο (νικητή) και τον δεύτερο πλησιέστερο κόμβο (δεύτερο νικητή) του φορέα εισαγωγής. Στη συνέχεια, κρίνει αν ο φορέας εισαγωγής ανήκει στο ίδιο σύμπλεγμα του νικητή ή του δεύτερου νικητή χρησιμοποιώντας το κριτήριο κατωφλίου ομοιότητας. Το πρώτο στρώμα του SOINN προσαρμοστικά ενημερώνει το όριο ομοιότητας κάθε κόμβου, επειδή η κατανομή δεδομένων εισόδου είναι άγνωστη. Εάν ο κόμβος i έχει γειτονικούς κόμβους, το όριο ομοιότητας Ti υπολογίζεται χρησιμοποιώντας τη μέγιστη απόσταση μεταξύ κόμβου i και των γειτονικών κόμβων του.[F. Shen O. Hasegawa., 2009]



Εικόνα 4.6 Διάγραμμα ροής της διαδικασίας μάθησης SOINN. [Shen Furaoa et al, 2007]

Ο αλγόριθμος παρόλο που θεωρείται ένας καλός αλγόριθμος έχει κάποιες ελλείψεις - αδυναμίες:

- Είναι δύσκολο να επιλέξουμε πότε να σταματήσει την εκμάθηση πρώτης στρώσης και να ξεκινήσουμε τη δεύτερη.

- Για το δεύτερο στρώμα, εάν τα μαθησιακά αποτελέσματα του πρώτου στρώματος έχουν αλλάξει, όλα τα μαθησιακά αποτελέσματα του δεύτερου στρώματος θα καταστραφούν, με αποτέλεσμα να απαιτείται επανακατάρτιση του δεύτερου στρώματος. Έτσι το δεύτερο στρώμα SOINN είναι ακατάλληλο για διαδικτυακή βαθμιαία μάθηση.

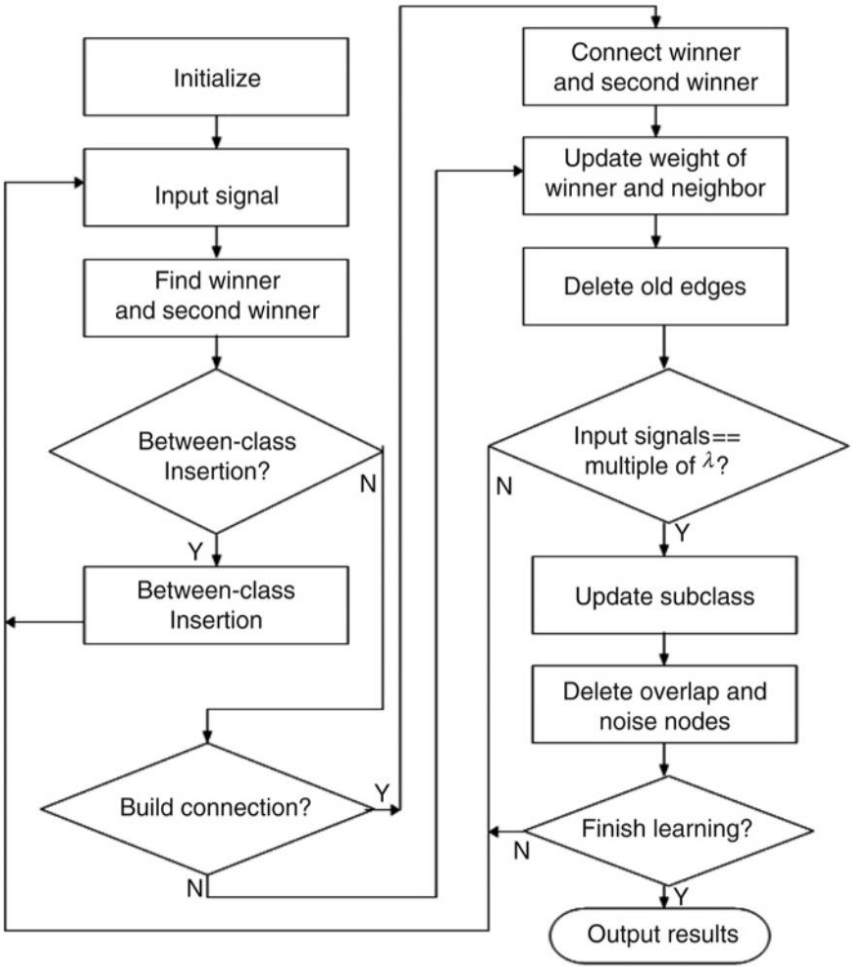
- Η εισαγωγή εντός της κλάσης είναι απαραίτητη για το δεύτερο στρώμα του SOINN. Ωστόσο, απαιτούνται πολλές παράμετροι καθορισμένες από τον χρήστη.

- Ο SOINN δεν είναι σταθερός, δεν μπορεί να χωρίσει καλά καλυπτόμενες περιοχές υψηλής πυκνότητας. [Shen Furaoa et al, 2007]

4.4 ESOINN - Enhanced Self-Organizing Incremental Neural Networks

Όπως προαναφέραμε, ο ESOINN είναι η εξέλιξη του SOINN βασισμένη στις αδυναμίες που αναφέραμε παραπάνω.

Για την επίλυση των προαναφερθέντων ελλείψεων, αφαιρέθηκε το δεύτερο στρώμα του SOINN και σχεδιάστηκαν μερικές τεχνικές για να βοηθηθεί ο SOINN μονής στρώσης και να αποκτήσει ακόμη καλύτερα αποτελέσματα ομαδοποίησης από αυτά του SOINN δύο επιπέδων.



Εικόνα 4.7 Διάγραμμα ροής του ESOINN. [Shen Furaoa et al, 2007]

Συγκρίνοντας τα σχήματα 1 και 2 βλέπουμε ότι ο ESOINN υιοθετεί μόνο ένα μονοστρωματικό δίκτυο. Για την εισαγωγή μεταξύ κατηγοριών, ο ESOINN υιοθετεί το ίδιο σχήμα με τον SOINN. Για την οικοδόμηση μιας σύνδεσης μεταξύ των κόμβων, αντίθετα με τον SOINN, ο ESOINN προσθέτει μια προϋπόθεση για να κρίνει αν χρειάζεται η σύνδεση. Μετά από επαναλήψεις εκμάθησης λ, ο ESOINN χωρίζει τους κόμβους σε διαφορετικές υποκατηγορίες και διαγράφει τις άκρες που βρίσκονται σε καλυπτόμενες περιοχές. Ο ESOINN δεν επιτυγχάνει την εισαγωγή μέσα στην κλάση επειδή υιοθετεί μόνο μια μονοστρωματική δομή. Η εισαγωγή μέσα στην κλάση επιτυγχάνεται ελάχιστα.

Η απομάκρυνση του δεύτερου στρώματος καθιστά τον ESOINN πιο κατάλληλο για εργασίες στο διαδίκτυο ή ακόμα και στη δια βίου μάθηση από τον SOINN δύο επιπέδων. Αποφεύγει επίσης τη δύσκολη επιλογή του πότε πρέπει να σταματήσει η μάθηση του πρώτου στρώματος και να ξεκινήσει η δεύτερη στρώση μάθησης. Η αφαίρεση της εισαγωγής εντός της κλάσης εξαλείφει πέντε παραμέτρους που καθορίζονται από τον χρήστη.

Χρησιμοποιώντας ένα μονοστρωματικό δίκτυο για να πάρει τη θέση της δικτυακής δομής δύο επιπέδων του SOINN, ο ESOINN μπορεί να πραγματοποιήσει καθαρή διαδεδομένη μάθηση στο διαδίκτυο. Με τον καθορισμό των συνθηκών για την οικοδόμηση μιας σύνδεσης μεταξύ των κόμβων, ο ESOINN μπορεί να διαχωρίσει τις καλυπτόμενες κατηγορίες υψηλής πυκνότητας. Στην πραγματικότητα, ο ESOINN υιοθετεί μόνο την εισαγωγή μεταξύ των κλάσεων για να πραγματοποιήσει τη βαθμιαία μάθηση. Ο ESOINN συνειδητοποιεί εύκολα μια λύση και απαιτεί λιγότερες παραμέτρους από το SOINN. Επίσης, χρησιμοποιώντας ορισμένες τεχνικές εξομάλυνσης ο ESOINN είναι πιο σταθερός από το SOINN. Ο ESOINN ανήκει στους αλγορίθμους μη επιβλεπόμενης μάθησης (unsupervised learning). Με την αξιολόγηση της περιοχής επικάλυψης, ο ESOINN μπορεί να αποκτήσει ικανοποιητικά αποτελέσματα μάθησης.

Η πυκνότητα κόμβου(Node density) μπορεί να οριστεί χρησιμοποιώντας τον τοπικό συσσωρευμένο αριθμό δειγμάτων: εάν πολλά δείγματα εισόδου βρίσκονται κοντά στον κόμβο, η πυκνότητα του κόμβου είναι υψηλή. Εάν λίγα δείγματα εισόδου βρίσκονται κοντά στον κόμβο, η πυκνότητα αυτού του κόμβου είναι χαμηλή. Για τον λόγο αυτό, κατά τη διάρκεια μιας περιόδου μάθησης, μετριέται πόσες φορές ένας κόμβος έχει κερδίσει και αυτή η μέτρηση χρησιμοποιείται ως πυκνότητα κόμβου. Αυτός ο ορισμός για την "πυκνότητα του χρόνου" είναι ο ορισμός της πυκνότητας που υιοθετείται από αλγορίθμους, όπως ο SOINN. Η πυκνότητα δημιουργεί τα ακόλουθα

προβλήματα:

- Υπάρχουν πολυάριθμοι κόμβοι που βρίσκονται στην περιοχή υψηλής πυκνότητας, που σημαίνει ότι στην περιοχή υψηλής πυκνότητας η πιθανότητα ένας κόμβος να είναι νικητής δεν θα είναι σημαντικά υψηλότερος από αυτόν στην περιοχή χαμηλής πυκνότητας. Έτσι, δεν μπορούμε απλά να χρησιμοποιήσουμε τους "χρόνους νίκης" για να μετρήσουμε την πυκνότητα.

- Σε διαδικασίες αυξητικής μάθησης, ορισμένοι κόμβοι που δημιουργούνται σε προηγούμενα στάδια δεν θα είναι και πάλι νικητές για μεγάλο χρονικό διάστημα. Χρησιμοποιώντας τον ορισμό των "χρόνων νίκης", τέτοιοι κόμβοι θα μπορούσαν να κριθούν ως κόμβοι χαμηλής πυκνότητας σε μεταγενέστερο στάδιο μάθησης.

Στον ESOINN, χρησιμοποιείται ένας νέος ορισμός της πυκνότητας για να λύσουμε τα πιο πάνω προβλήματα. Η βασική ιδέα είναι η ίδια με τον τοπικό συσσωρευμένο αριθμό δειγμάτων, με τη διαφορά ότι ορίζεται ένα σημείο, καθορίζεται η θέση του με έναν αριθμό και χρησιμοποιείται στον μέσο όρο του συσσωρευμένου σημείου ενός κόμβου για να περιγραφεί η πυκνότητά του.Εξετάζουμε την σχέση μεταξύ των κόμβων όταν υπολογίζεται με το σημείο p ενός κόμβου. Αρχικά υπολογίζουμε τη μέση απόσταση d τi του κόμβου i από τους γείτονές του (είκ 4.8) και στη συνέχεια υπολογίζεται το σημείο του κόμβου i.

$$\bar{d}_i = \frac{1}{m} \sum_{j=1}^{m} \| \boldsymbol{W}_i - \boldsymbol{W}_j \|.$$

Εικόνα 4.8 Υπολογισμός απόστασης ενός κόμβου από τους γείτονες.
[Shen Furaoa et al, 2007]

$$p_i = \begin{cases} \dfrac{1}{(1+\bar{d}_i)^2} & \text{if node } i \text{ is } winner \\ 0 \quad \text{if node } i \text{ is not } winner. \end{cases}$$

Εικόνα 4.9 Υπολογισμός σημείου το κόμβου. [Shen Furaoa et al, 2007]

Με τον ορισμό του σημείου γίνεται γνωστό ότι αν η μέση απόσταση του κόμβου i στους γείτονές του είναι μεγάλη, τότε ο αριθμός των κόμβων σε αυτήν την περιοχή είναι χαμηλός. Κατά συνέπεια, η κατανομή των κόμβων είναι αραιή και η πυκνότητα σε αυτήν την περιοχή θα είναι χαμηλή. Έτσι παρέχονται χαμηλά σημεία στον κόμβο i. Αν η μέση απόσταση d ti είναι μικρή, αυτό σημαίνει ότι ο αριθμός των κόμβων σε αυτήν την περιοχή είναι υψηλός, η πυκνότητα στην περιοχή αυτή θα είναι υψηλή. Δίνονται υψηλά σημεία στον κόμβο i. Προσθέτουμε 1 στον παρονομαστή του σημείου για να γίνει η τιμή του σημείου μικρότερη από 1.

Όταν γίνει η πρώτη επανάληψη, υπολογίζουμε μόνο τα σημεία για τον κόμβο i, όταν αυτός είναι ο νικητής. Τα σημεία άλλων κόμβων σε αυτή την επανάληψη είναι 0. Επομένως, για μια επαναληπτική περίοδο, τα συσσωρευμένα σημεία για τον νικητή θα αλλάξουν, αλλά τα συσσωρευμένα σημεία για άλλους κόμβους παραμένουν χωρίς καμία αλλαγή. Τα συσσωρευμένα σημεία si υπολογίζονται με το άθροισμα των βαθμών για τον κόμβο i κατά τη διάρκεια μιας περιόδου μάθησης.

$$s_i = \sum_{j=1}^{n} \left(\sum_{k=1}^{\lambda} p_i \right).$$

Εικόνα 4.10 Υπολογισμός συσσωρευμένου σημείου. [Shen Furaoa et al, 2007]

$$h_i = \bar{s_i} = \frac{1}{N} s_i = \frac{1}{N} \sum_{j=1}^{n} \left(\sum_{k=1}^{\lambda} p_i \right).$$

Εικόνα 4.11 Υπολογισμός μέσων συσσωρευμένων σημείων (πυκνότητα).
[Shen Furaoa et al, 2007]

Σε αυτή την εξίσωση (εικ 4.11), το N αντιπροσωπεύει τον απολογισμό της περιόδου κατά την οποία τα συσσωρευμένα σημεία si είναι μεγαλύτερα από 0. Πρέπει να σημειωθεί ότι το N δεν είναι απαραιτήτως ίσο με n. Δεν χρησιμοποιείται το n για να πάρει τη θέση του N, επειδή για τη βαθμιαία μάθηση κατά τη διάρκεια μερικών περιόδων μάθησης τα συσσωρευμένα σημεία si είναι 0. Εάν χρησιμοποιηθεί το n για τον υπολογισμό των μέσων συσσωρευμένων σημείων, η πυκνότητα κάποιων παλαιών μαθηματικών κόμβων θα μειωθεί. Χρησιμοποιώντας το N για τον υπολογισμό των μέσων συσσωρευμένων σημείων, ακόμη και κατά τη διάρκεια της δια βίου μάθησης, η πυκνότητα των παλαιών μαθηματικών κόμβων θα παραμείνει αμετάβλητη εάν δεν εισαχθούν στο σύστημα νέα σήματα κοντά στον κόμβο. Ωστόσο, για ορισμένες εφαρμογές είναι απαραίτητο να ξεχαστούν πολύ παλιές πληροφορίες. Σε τέτοιες περιπτώσεις πρέπει να χρησιμοποιήσουμε μόνο n για να πάρουμε τη θέση του N. Έτσι, μπορούμε να συνεχίσουμε να μαθαίνουμε νέες γνώσεις και να ξεχνάμε την πολύ παλιά γνώση. [Shen Furaoa et al, 2007]

Κεφάλαιο 5 Εφαρμογή Ανίχνευσης Κλήσεων Απάτης

5.1 Εισαγωγή

Οι εταιρίες που ασχολούνται με εφαρμογές για την ανίχνευση κλήσεων απάτης διαθέτουν πολλά εργαλεία.

Τα εργαλεία αυτά χωρίζονται σε δύο κατηγορίες:

1. Εργαλεία πρόληψης, όπου τοποθετούνται εξειδικευμένα τείχη προστασίας (firewalls), φίλτρα και άλλα εργαλεία. Το κομμάτι της πρόληψης εστιάζει στο να δημιουργήσει υψηλή προστασία στο τηλεφωνικό σύστημα, ώστε να είναι αποτρεπτικό προς τους hackers να “εισβάλουν” σε αυτό.

2. Εργαλεία ανίχνευσης. Ο στόχος σ΄αυτή την κατηγορία είναι να εντοπιστούν οι κλήσεις απάτης όσο πιο γρήγορα γίνεται.

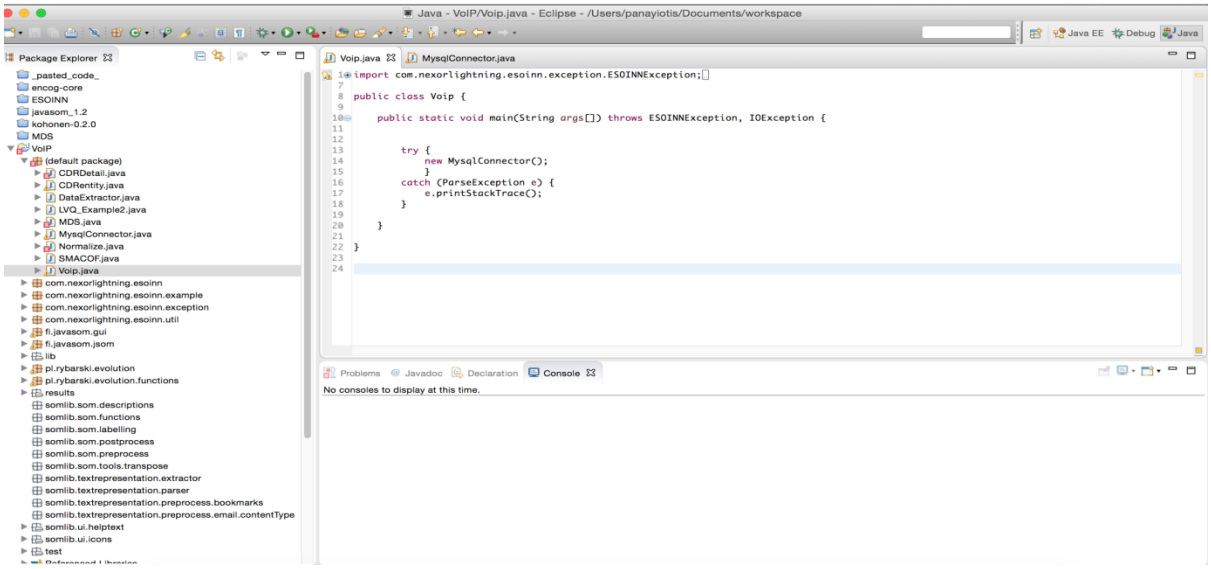
Τα εργαλεία που χρησιμοποιούνται για τη διάγνωση των κλήσεων απάτης χρησιμοποιούν τη μέθοδο συσταδοποίησης. Η εφαρμογή που παρουσιάζουμε χρησιμοποιεί αυτήν τη μέθοδο εντοπισμού με τη βοήθεια του αλγόριθμου ESOINN.
Στην πορεία της έρευνας, σε συνεργασία με τον τηλεπικοινωνιακό πάροχο που μας δίνει CDRs, έχουν εντοπιστεί μεγάλα κενά στον εντοπισμό των κλήσεων απάτης. Παρακάτω, θα παρουσιάσουμε την εφαρμογή που δημιουργήσαμε με σκοπό την ανίχνευση των κλήσεων απάτης όταν υπάρχει διαφοροποίηση στο προφίλ των κλήσεων του χρήστη.

5.2 Εργαλεία για την υλοποίηση της εφαρμογής

Η εφαρμογή αναπτύχθηκε στο περιβάλλον σε Eclipse Luna Release (4.4.0) και χρησιμοποιήθηκε η γλώσσα προγραμματισμού Java.

Χρησιμοποιήθηκαν CDRs από τη βάση δεδομένων σε μορφή CSV αρχείο και κωδικοποίηση των γραμμάτων σε «UTF-8» που είναι βοηθητικό για την ομαλή αποθήκευση και ανάκτηση ειδικών χαρακτήρων. Στη συνέχεια, τα αρχεία έγιναν import σε μια εφαρμογή διαχείρισης βάσεων δεδομένων σε MySql την Sequel Pro version 1.1. Η διαδικασία import, export και η διαχείριση των CDRs έγιναν σε virtual machine με λειτουργικό σύστημα Debian GNU/Linux 8.2 (jessie) και τεχνικά χαρακτηριστικά : RAM 8GB , CORES 4, STORAGE 100GB.

Επιλέχθηκε να γίνει η εργασία μέσω του virtual machine έτσι ώστε να αποφευχθεί πιθανή ανάκτηση των προσωπικών δεδομένων των πελατών από τρίτους, κάτι που θα προκαλούσε προβλήματα στην έρευνα, στους πελάτες, άλλα και στην εταιρία. Γι' αυτό τον λόγο δεν χρησιμοποιήθηκε VPN (virtual private network).



Εικόνα 5.1 Eclipse Luna

5.3 Λειτουργία εφαρμογής

5.3.1 Ανάκτηση και επεξεργασία των Δεδομένων

Ανάκτηση Δεδομένων
Στο πρώτο κομμάτι της εφαρμογής επιλέγουμε τα recods με τα οποία και θα ασχοληθούμε, δηλαδή κάνουμε τα ανάλογα sql queary στην βάση όπου καθορίζουμε το εύρος των ημερομηνιών και ποια fields θα χρειαστούμε για τα CDRs μας.

Παράδειγμα query:
SELECT callStart, callEnd, BParty FROM CDR_ARCHIVE WHERE signallingStart BETWEEN" + "'" + ss1 + "' AND"+ "'" + ss2 + "'

Εδώ βλέπουμε ότι ζητάμε από τη βάση να μας φέρει τα fields:

- callStart είναι η ώρα που ξεκίνησε η συνομιλία, δηλαδή που απαντήθηκε το τηλέφωνο.
- callEnd είναι η ώρα που τελείωσε η συνομιλία.
- BParty είναι το τηλέφωνο που καλέστηκε

Μετά καθορίζουμε τις ώρες που θέλουμε να ελέγξουμε

- signallingStart είναι η ώρα που ξεκίνησε η κλήση, είναι διαφορετική από την ώρα που απαντήθηκε το τηλέφωνο. Στις μεταβλητές ss1και ss2 μπορούμε να ορίσουμε μεταξύ ποιων ωρών θέλουμε να γίνει ο έλεγχος.

Έχοντας μεριμνήσει να αποθηκεύεται η ώρα κάθε φορά που τρέχει η εφαρμογή μας μπορούμε να καθορίσουμε την ώρα που θα γίνεται ο έλεγχος (signallingStart).

```
//Get the last time when the script run
String dateQuery = "SELECT scriptTime FROM MASTER_VOIP";
ResultSet oldTime = stmt.executeQuery(dateQuery);

Update the scriptTime
String scriptDate =  "UPDATE  MASTER_VOIP SET scriptTime =" + "'" + newTime + "'";
int updateDate = stmt.executeUpdate(scriptDate);
```

Εικόνα 5.2 Καταγραφή της ώρας που τρέχει η εφαρμογή.

Αυτό έγινε στην προσπάθειά μας να τρέξουμε την εφαρμογή μας σε πραγματικό χρόνο, κατά την οποία εντοπίστηκαν οι εξής δυσκολίες:

- Τα CDRs δημιουργούνται όταν ολοκληρωθεί η κλήση, έτσι δεν μπορούσαμε να ελέγξουμε μια κλήση που δεν είχε τερματιστεί.
- Λόγω του μεγάλου όγκου δεδομένων στη βάση με τα live δεδομένα αλλά και του VM που είχαμε στη διάθεση μας, υπήρχε μεγάλη καθυστέρηση με τα αποτελέσματα από το sql query που κάναμε.

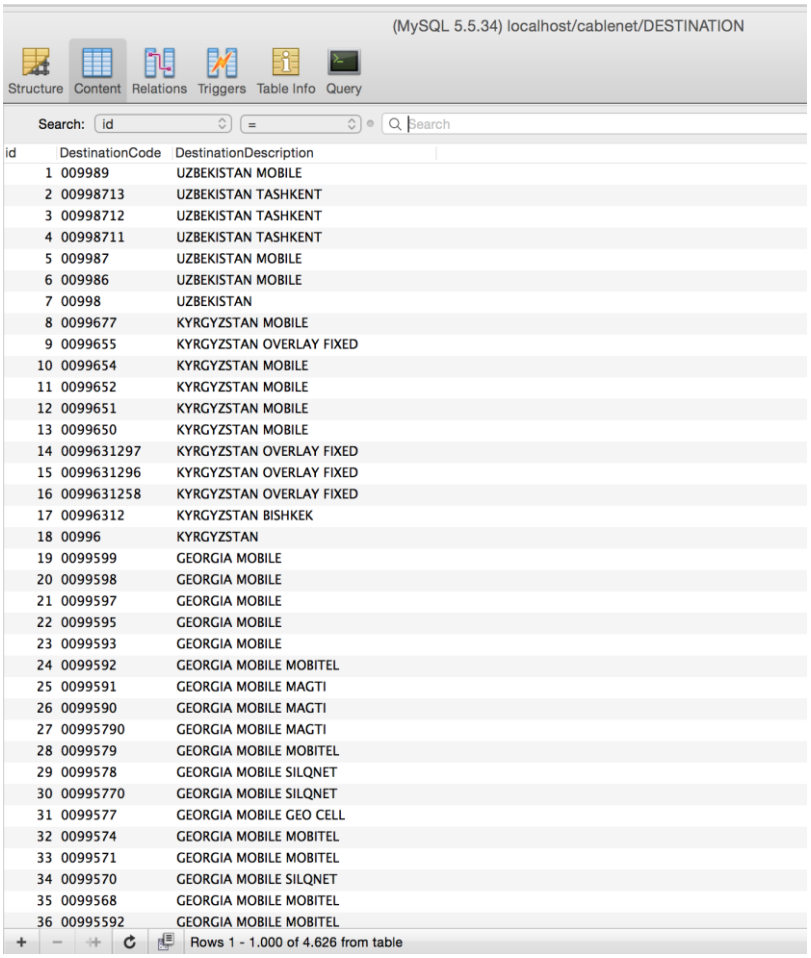
Τα αποτελέσματα που θα μας φέρει το Sql query τα αποθηκεύουμε σε μία λίστα.

```
ResultSet rs = stmt.executeQuery(query);

ResultSetMetaData rsmd = (ResultSetMetaData) rs.getMetaData();
  int colCount = rsmd.getColumnCount();

  ArrayList <String []>l = new ArrayList();
  int num = 1;
  String bp = "";
  // loop for the data from the query to temp[]
  while (rs.next()) {

    String []temp = new String[3];
    temp[0] = rs.getString(1);
    temp[1] = rs.getString(2);
    temp[2] = rs.getString(3);


    bp = temp[2] ;
    l.add(temp);

  }
```

Εικόνα 5.3 Αποθήκευση Δεδομένων σε Λίστα.

Επεξεργασία Δεδομένων

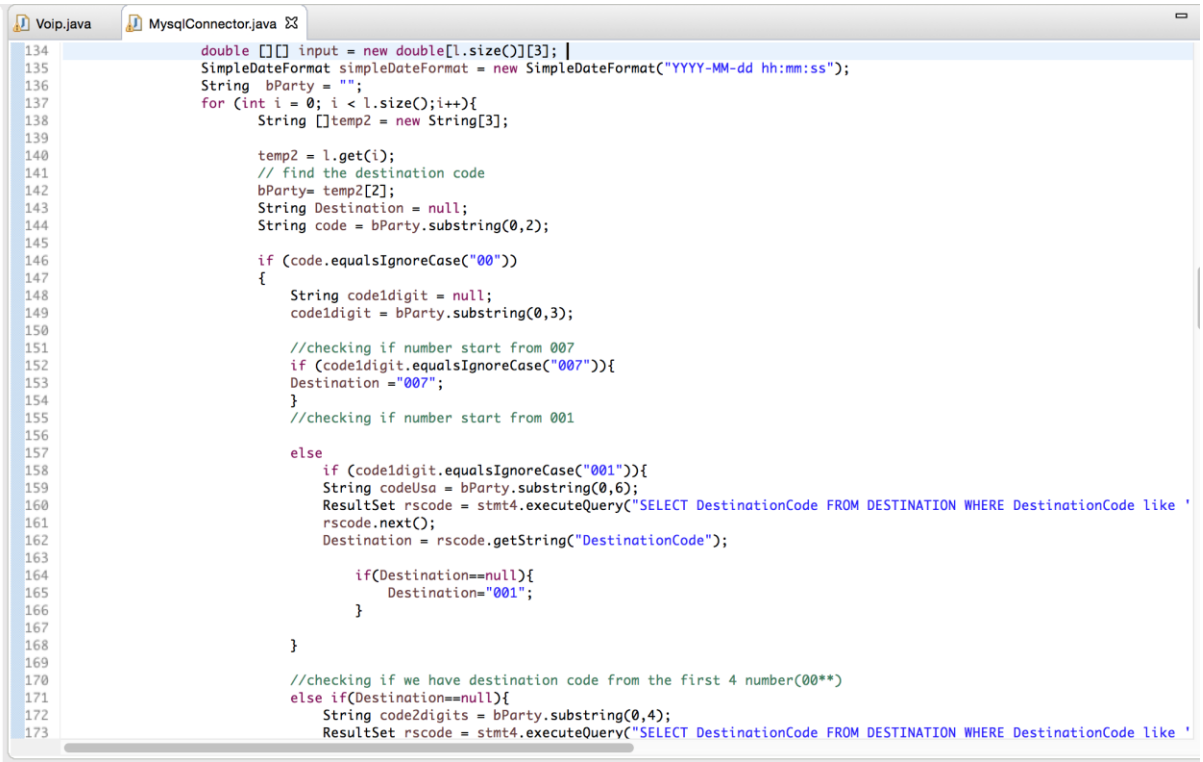
Η πρώτη επεξεργασία γίνεται στο BParty, όπου βρίσκεται ο αριθμός που καλείται από τον χρήστη. Είναι πολύ σημαντικό να ξέρουμε με ακρίβεια τον κωδικό της χώρας, γί' αυτό δημιουργήσαμε έναν έλεγχο χρησιμοποιώντας το table "DESTINATION" από τη βάση μας, όπου υπάρχουν καταχωρημένοι όλοι οι κωδικοί χωρών.



id	DestinationCode	DestinationDescription
1	009989	UZBEKISTAN MOBILE
2	00998713	UZBEKISTAN TASHKENT
3	00998712	UZBEKISTAN TASHKENT
4	00998711	UZBEKISTAN TASHKENT
5	009987	UZBEKISTAN MOBILE
6	009986	UZBEKISTAN MOBILE
7	00998	UZBEKISTAN
8	0099677	KYRGYZSTAN MOBILE
9	0099655	KYRGYZSTAN OVERLAY FIXED
10	0099654	KYRGYZSTAN MOBILE
11	0099652	KYRGYZSTAN MOBILE
12	0099651	KYRGYZSTAN MOBILE
13	0099650	KYRGYZSTAN MOBILE
14	0099631297	KYRGYZSTAN OVERLAY FIXED
15	0099631296	KYRGYZSTAN OVERLAY FIXED
16	0099631258	KYRGYZSTAN OVERLAY FIXED
17	00996312	KYRGYZSTAN BISHKEK
18	00996	KYRGYZSTAN
19	0099599	GEORGIA MOBILE
20	0099598	GEORGIA MOBILE
21	0099597	GEORGIA MOBILE
22	0099595	GEORGIA MOBILE
23	0099593	GEORGIA MOBILE
24	0099592	GEORGIA MOBILE MOBITEL
25	0099591	GEORGIA MOBILE MAGTI
26	0099590	GEORGIA MOBILE MAGTI
27	00995790	GEORGIA MOBILE MAGTI
28	0099579	GEORGIA MOBILE MOBITEL
29	0099578	GEORGIA MOBILE SILQNET
30	00995770	GEORGIA MOBILE SILQNET
31	0099577	GEORGIA MOBILE GEO CELL
32	0099574	GEORGIA MOBILE MOBITEL
33	0099571	GEORGIA MOBILE MOBITEL
34	0099570	GEORGIA MOBILE SILQNET
35	0099568	GEORGIA MOBILE MOBITEL
36	00995592	GEORGIA MOBILE MOBITEL

Εικόνα 5.4 Table Destination.

Ο έλεγχος που προαναφέραμε γίνεται επειδή δεν υπάρχει η πληροφορία από τα CDRs σε ποια χώρα γίνεται η κλήση, λόγω του ότι τα CDRs που χρησιμοποιούμε είναι πριν από την τιμολόγηση, δηλαδή πριν γίνει η χρέωση από τα συστήματα της εταιρίας για την κλήση στον πελάτη.



Εικόνα 5.5 Έλεγχος για εντοπισμό του κωδικού της χώρας όπου πραγματοποιείται η κλήση.

Στη συνέχεια επεξεργαζόμαστε τα fields callStart και callEnd. Ελέγχουμε αν υπάρχουν NULL data. Αυτό μπορεί να συμβεί αν το τηλέφωνο δεν απαντήθηκε. Αν η τιμή τους callStart είναι “null” βάζουμε την τιμή “0000-00-00 00:00:00” στο callStart και στο callEnd. Ο καθορισμός τιμής στα συγκεκριμένα “null data” γίνεται γιατί στη συνέχεια μετατρέπουμε αυτές τις τιμές σε δευτερόλεπτα και βρίσκουμε τη διαφορά τους αφαιρώντας το callStart με το callEnd. Αυτός είναι ο χρόνος που διήρκεσε η κλήση, που επίσης δεν μας δίνεται από τα CDRs για τον λόγο που αναφέραμε παραπάνω.

Για να ενισχύσουμε τη δύναμη των τιμών που παίρνουμε από τα CDRs. Ορίσαμε κάποιες μεταβλητές normal = 0.1, risk1 = 0.50, risk2 = 0.75, risk3 = 1.5. Τις τιμές αυτές τις χρησιμοποιούμε για να δώσουμε έμφαση σε ώρες που η κλήση μπορεί να θεωρηθεί ύποπτη.

```
if (hour>=8 & hour <=18)
{
    dhour= (hour * normal );
}

else if (hour >= 19 & hour <=21)

{
    dhour= (hour * risk1 );
}

else if (hour>= 22 & hour <=24)

{
    dhour= (hour * risk2 );
}


else{
    dhour= (hour * risk3 );
}
```

Εικόνα 5.6. Έλεγχος της ώρας κλήσης και ενίσχυση της τιμής.

Παρόμοιος έλεγχος γίνεται και για τον χρόνο ομιλίας, που ανάλογα με τη διάρκεια της κλήσης πολλαπλασιάζεται με την ανάλογη τιμή.

```
//convert to seconds
long seconds = (date2.getTime()-date1.getTime())/1000;
long CallStart = date1.getTime()/1000;
System.out.println("CallStart: "+CallStart);
long CallEnd = date2.getTime()/1000;

//duration
long average= CallEnd - CallStart;
Double duration=(double)Math.round(average);

if (duration < 15.0)
{
 duration=duration*normal;
}

else if (duration > 15.0 & duration < 45.0 )
{
      duration=duration*risk1;

}
else if (duration > 45.0 & duration < 60.0 )
{
     duration=duration*risk2;
}
else
{
     duration=duration*risk3;

}
```

Εικόνα 5.7 Έλεγχος της διάρκειας της κλήσης και ενίσχυση της τιμής.

Στο τέλος όλα τα χαρακτηριστικά αποθηκεύονται σε μία λίστα.

```
}

input[i][0] = (double)Math.round(duration);
input[i][1] = Double.parseDouble(Destination);
input[i][2] = bparty;
input[i][3] =  dhour;
```

Εικόνα 5.8 Αποθήκευση χαρακτηριστικών της κλήσης σε λίστα.

5.3.2 Κανονικοποίηση(Normalize)

Η κανονονικοποίηση (normalaization) στις βάσεις δεδομένων είναι ένας πολύ ανεπτυγμένος τομέας από την εισαγωγή του τεχνητού κώδικα του Codd σε κανονικές μορφές το 1970. Οι Bernstein (1976), Diederich and Milton (1988), Concepcion and Villafuerte (1990) και Rosenthal and Reiner (1994) πρότειναν αλγόριθμους και εργαλεία που να συνδέουν μια κανονικοποιημένη βάση δεδομένων χρησιμοποιώντας λειτουργικές εξαρτήσεις. Ο Maier (1988) έδειξε ότι η κανονικοποίηση της σχεσιακής θεωρίας μοντέλου δεδομένων τείνει να είναι περίπλοκη για τους μέσους σχεδιαστές μοντέλων. Οι Jarvenpaa και Macesky (1989) και οι Bock και Ryan (1993) έδειξαν ότι το σχεσιακό μοντέλο δεδομένων οδηγεί σε κακή απόδοση σχεδιαστή.

Η κλασική τεχνική κανονονικοποίησης της βάσης δεδομένων συχνά βασίστηκε στον ορισμό των κανονικών μορφών. Ορισμένα εγχειρίδια βάσεων δεδομένων περιλαμβάνουν αλγόριθμους κανονικοποίησης για να βρουν την κανονική κάλυψη με την αφαίρεση των εξωγενών χαρακτηριστικών των λειτουργικών εξαρτήσεων (Functional Dependencies) και στη συνέχεια να μετατρέψουν κάθε λειτουργία εξάρτησης σε κανονικό κάλυμμα σε μια σχέση / πίνακα. [Kung ,et al,2006]

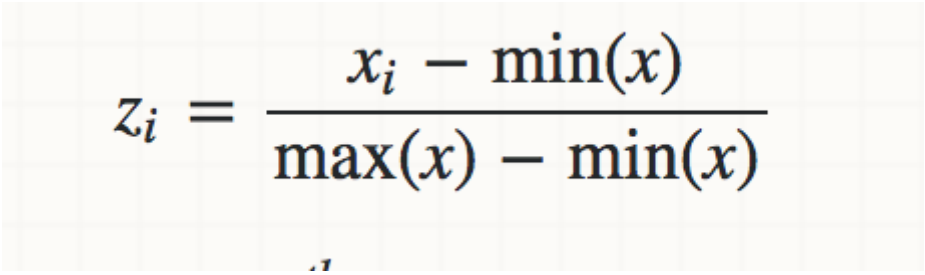
Υπάρχουν 3 βασικοί διαφορετικοί τύποι κανονικοποίησης.

Πρώτη κανονική φόρμα (1NF)
Σύμφωνα με την πρώτη κανονική φόρμα, δύο σειρές δεδομένων δεν πρέπει να περιέχουν επαναλαμβανόμενη ομάδα πληροφοριών, δηλαδή κάθε σετ στήλης πρέπει να έχει μια μοναδική τιμή, έτσι ώστε να μην μπορούν να χρησιμοποιηθούν πολλαπλές στήλες για την ανάκτηση της ίδιας σειράς. Κάθε πίνακας θα πρέπει να είναι οργανωμένος σε σειρές και κάθε σειρά θα πρέπει να έχει ένα πρωτεύων κλειδί που να το διακρίνει ως μοναδικό. Το κύριο κλειδί είναι συνήθως μία στήλη αλλά μερικές φορές μπορεί να συνδυαστούν περισσότερες από μία στήλες για να δημιουργηθεί ένα μόνο πρωτεύων κλειδί.

Δεύτερη κανονική φόρμα (2NF)
Σύμφωνα με τη δεύτερη κανονική φόρμα, δεν πρέπει να υπάρχει κάποια μερική εξάρτηση οποιασδήποτε στήλης στο πρωτεύων κλειδί. Αυτό σημαίνει ότι για έναν πίνακα που έχει συνενώσει το πρωτεύων κλειδί, κάθε στήλη στον πίνακα που δεν είναι μέρος του πρωτεύοντος κλειδιού πρέπει να εξαρτάται από το σύνολο του κλειδιού που έχει συναρμολογηθεί για την ύπαρξή του. Εάν οποιαδήποτε στήλη εξαρτάται μόνο από ένα μέρος του κλειδιού, τότε ο πίνακας αποτυγχάνει στη δεύτερη κανονική φόρμα.

Τρίτη κανονική φόρμα (3NF)
Στην τρίτη κανονική φόρμα ισχύει ότι κάθε μη ιδιόκτητο χαρακτηριστικό (non-prime) του πίνακα πρέπει να εξαρτάται από το πρωτεύων κλειδί ή μπορούμε να πούμε ότι δεν πρέπει σε καμία περίπτωση ένα χαρακτηριστικό μη πρωτεύοντος κλειδιού να προσδιορίζεται από ένα άλλο μη πρωτεύων χαρακτηριστικό. Επομένως, αυτή η μεταβατική λειτουργική εξάρτηση θα πρέπει να αφαιρεθεί από τον πίνακα και επίσης ο πίνακας θα πρέπει να εφαρμόζει τον τύπο 2NF. [Jargalsaikhan Alyeksandr,2017]. Στη βάση δεδομένων που χρησιμοποιούμε στην εργασία μας εφαρμόζεται η τρίτη κανονική φόρμα.

Η κανονονικοποίηση πέρα από τις βάσεις δεδομένων χρησιμοποιείται και στην ανάλυση δεδομένων. Η διαδικασία της κανονικοποίησης δεδομένων είναι πολύ σημαντική, γιατί με αυτόν τον τρόπο μπορούν οι αλγόριθμοι να διαβάσουν και να αναλύσουν μεγάλα και διαφορετικού τύπου δεδομένα πιο εύκολα.



$$z_i = \frac{x_i - \min(x)}{\max(x) - \min(x)}$$

Εικόνα 5.9 Μαθηματικός τύπος κανονικοποίησης δεδομένων.

Στην εφαρμογή για την κανονονικοποίηση δεδομένων χρησιμοποιήσαμε την κανονονικοποίηση από τον αλγόριθμο MDS(Multidimensional scaling). Καταλήξαμε σε αυτό λόγω του ότι ήταν υλοποιημένος σε java όπως και ο αλγόριθμός μας, τα δεδομένα εισόδου είναι σε μορφή “double”. Τα αποτελέσματά του επίσης ήταν στην ίδια μορφή, που μας εξυπηρετούσε και στον αλγόριθμο αφού και τα δεδομένα εισόδου του ESOINN είναι “double”.

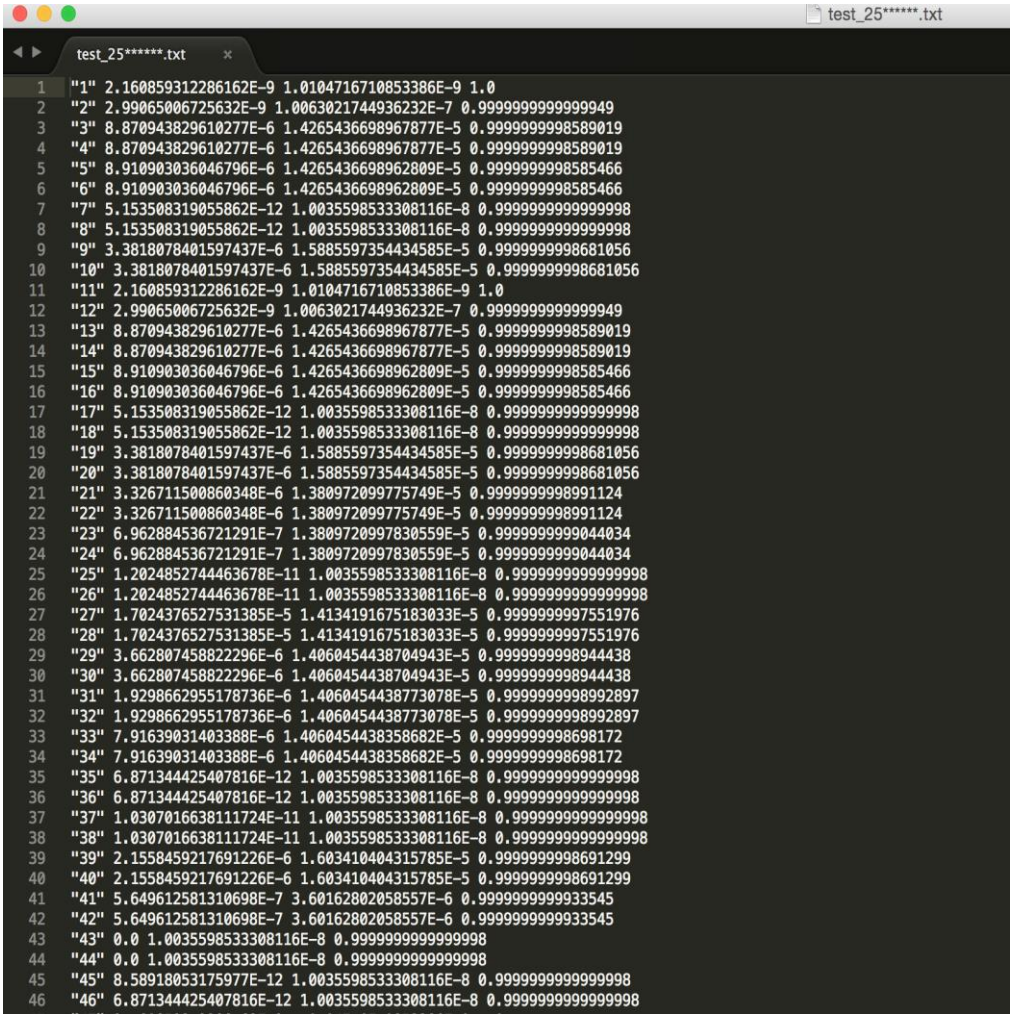
```
                input[i][0] = (double)Math.round(duration);
                input[i][1] = Double.parseDouble(Destination);
                input[i][2] = bparty;
                input[i][3] =  dhour;


        }

    //normalize the data
    Data.normalize(input);
```

Εικόνα 5.10 Κανονονικοποίηση δεδομένων.

Όταν ολοκληρωθεί η διαδικασία της κανονικοποίησης, τα δεδομένα καταχωρούνται ένα - ένα σε ένα text αρχείο, το οποίο είναι διαφορετικό για κάθε χρήστη που εξετάζουμε. Πρέπει να σημειώσουμε ότι για κάθε εγγραφή που γίνεται μέσα στο αρχείο καλείται ο αλγόριθμος, έτσι γίνεται ο έλεγχος των δεδομένων της κλήσης συγκρίνοντάς τα μόνο με τα προηγούμενα που είναι καταχωρημένα στο αρχείο.

```
//print the data in text file
    try {


        for(int x=0; x<n; x++) {  // output all coordinates
            PrintWriter writer = new PrintWriter(new BufferedWriter(new FileWriter("/Users/panayiotis/Documents/workspace/VOIP/test/test_"+u
            LineNumberReader  lnr = new LineNumberReader(new FileReader(new File("/Users/panayiotis/Documents/workspace/VOIP/test/test_"+use
            lnr.skip(Long.MAX_VALUE);
            lines = lnr.getLineNumber();
            lnr.close();
            String row = "";
             String string = String.format("%s" ,x);

             for(int j=0; j<4; j++) {
                 row = row + input[x][j] + " ";
             }
             writer.println("\""+(lines+1)+"\" "+row);

             lines++;
             writer.close();
             Esoinn(user,lines);

         }
```

Εικόνα 5.11 Αποθήκευση κανονικοποιημένων δεδομένων και κλήσεων αλγόριθμου.



Εικόνα 5.12 Αρχείο με κανονικοποιημένες τιμές.

5.3.3 Λειτουργία ESOINN

Ο αλγόριθμος, όπως αναφέραμε και πιο πριν, καλείται από την εφαρμογή κάθε φόρα που γίνεται μια νέα εγγραφή στο αρχείο του χρήστη που εξετάζουμε. Στη συνέχεια, αφού πάρει από την εφαρμογή τον αριθμό του χρήστη (αριθμό τηλεφώνου) και τη γραμμή του record, θα φορτώσει το αρχείο που αντιστοιχεί στον χρήστη και θα εξετάσει τα δεδομένα.

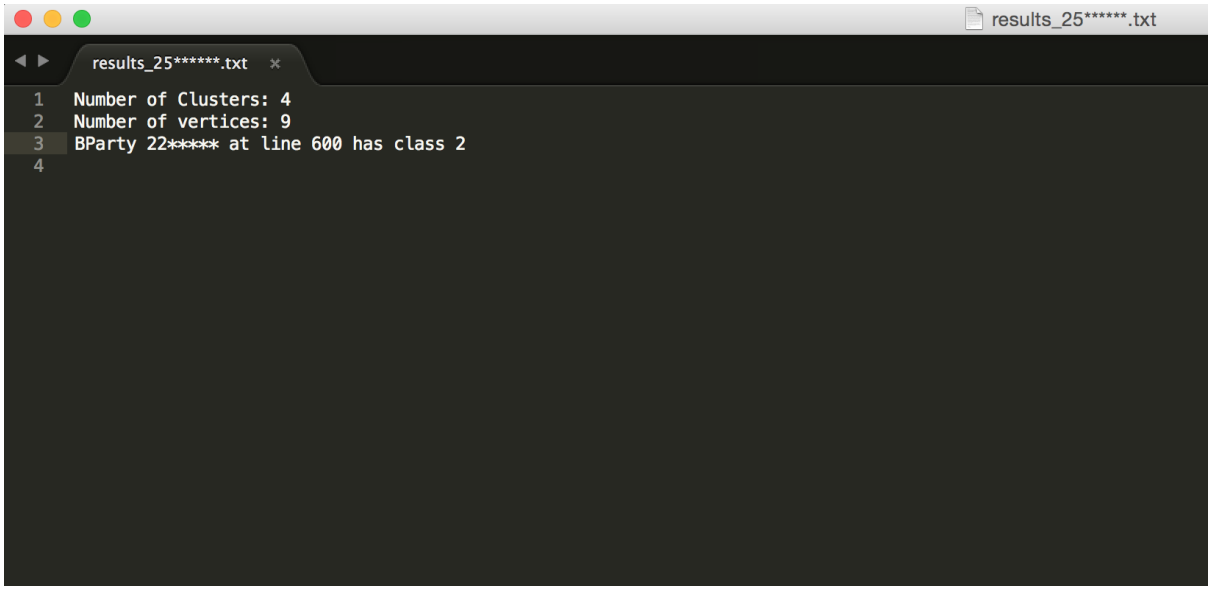
```
//esoinn
public void Esoinn(String user,int lines2) throws IOException, ESOINNException, InterruptedException {

    FileInputStream fis;
    BufferedInputStream bis;
    DataInputStream dis;
    int lines ;
    LineNumberReader  lnr = new LineNumberReader(new FileReader(new File("/Users/panayiotis/Documents/workspace/VOIP/test/test_"+user+".txt"))); 
    lnr.skip(Long.MAX_VALUE);
    lines = lnr.getLineNumber();


    lnr.close();
    double[][] badData = new double[1][4];
    File file = new File("/Users/panayiotis/Documents/workspace/VOIP/test/test_"+user+".txt"); //_"+user+"
    ESOINN model = new ESOINN(4);
    try {
```

Εικόνα 5.13 Κάλεσμα από τον αλγόριθμο το αρχείο του χρήστη που εξετάζουμε.

Ο αλγόριθμος διαβάζει όλες τις γραμμές του αρχείου, τις ομαδοποιεί και στο τέλος δημιουργεί ένα αρχείο για το record που εξετάζεται. Το αρχείο αυτό περιέχει το Cluster, το Vertices και το Class.

```
fis = new FileInputStream(file);

// Here BufferedInputStream is added for fast reading.
bis = new BufferedInputStream(fis);
dis = new DataInputStream(bis);
int row = 0;
int k = 0;
for (int line = 0; line < lines; line++) {

    String l = dis.readLine();
    String[] feat = l.split(" ");


    double[] features = new double[feat.length - 1];
    for (int i = 1; i <= features.length; i++) {
        features[i - 1] = Double.parseDouble(feat[i]);

                badData[k][i - 1] = features[i - 1];


     }


    row++;
    model.process(features);
    double inp[] = new double[4];


    PrintWriter results = new PrintWriter("/Users/panayiotis/Documents/workspace/VOIP/results/results_"+user+"_"+lines+"("+line+").txt", "UTF-8");
    results.println("Number of Clusters: "+model.getNumberOfClusters());
    results.println("Number of vertices: "+model.getNumberOfVertices());
    results.println("Line: "+lines);
```

Εικόνα 5.14 Συσταδοποίηση και δημιουργία νέου αρχείου με το αποτέλεσμα.



Εικόνα 5.15 Αποτελέσμα του ESOINN σε txt file.

Από τα αρχεία που δημιουργούνται για κάθε CDR μπορούμε να βγάλουμε τα συμπεράσματά μας, συγκρίνοντας τα 3 στοιχεία που μας δίνει ο αλγόριθμος.

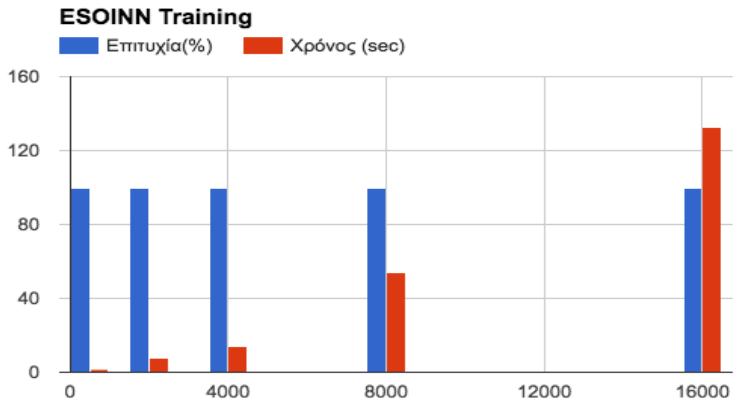
Κεφάλαιο 6 Εκπαίδευση – Αποτελέσματα –Συμπεράσματα

Στην πειραματική διαδικασία εξετάσαμε την απόδοση του αλγορίθμου μη επιτηρούμενης μάθησης ESOINN. Υλοποιήσαμε την εφαρμογή και τη διαμορφώσαμε έτσι, ώστε να χρησιμοποιήσουμε όσο καλύτερα γινόταν τα δεδομένα που είχαμε στη διάθεσή μας, με στόχο να εντοπίσουμε τις πιθανές κλήσεις απάτης. Διαπιστώθηκε ότι η εκπαίδευση του αλγορίθμου δεν ήταν εύκολη υπόθεση, αφού χρειάστηκε να πραγματοποιήσουμε αρκετές δοκιμές αλλάζοντας και τροποποιώντας τις μεταβλητές που εισαγάγαμε στον αλγόριθμο.

6.1 Εκπαίδευση αλγορίθμου

Για την εκπαίδευση του αλγορίθμου χρησιμοποιήθηκαν 16000 κλήσεις από τον μήνα Φεβρουάριο.

Η εκπαίδευση έγινε σε 5 στάδια, για 500, 2000, 4000, 8000 και 16000 CDRs, χωρίς την ύπαρξη κλήσεων απάτης. Στην πιο κάτω γραφική παράσταση βλέπουμε τον χρόνο που χρειάστηκε ο αλγόριθμος για την κάθε περίπτωση και το ποσοστό επιτυχίας. Σε όλες τις περιπτώσεις το ποσοστό επιτυχίας είναι 100%, διότι όπως προείπαμε δεν υπήρχαν κλήσεις απάτης. Αλλά και οι κλήσεις που εξετάσαμε αφορούσαν όλους τους χρήστες με κατά μέσο όρο κλήσεων λιγότερες από 30, έτσι δεν μπορούσε ο αλγόριθμος να κάνει την ομαδοποιήση των κλήσεων αυτών για να έχουμε αποτελέσματα.



Γράφημα 6.1 Αποτελέσματα εκπαίδευσης ESOINN.

6.2 Πειραματική Διαδικασία

Για την πειραματική διαδικασία χρησιμοποιήσαμε CDRs από τον Φεβρουάριο του 2016 μέχρι και τον Μάρτιο του 2016. Για τη συγκεκριμένη χρονική περίοδο δεν υπήρχε ενημέρωση από την εταιρία για κάποια αποδεδειγμένη κλήση απάτης. Όπως είδαμε και στην εκπαίδευση του αλγορίθμου διαπιστώθηκε ότι δεν μπορούσε να γίνει έλεγχος για όλους τους χρήστες, λόγω του ότι οι περισσότεροι είχαν μικρό αριθμό κλήσεων. Έτσι επιλέχθηκε ένας συγκεκριμένος χρήστης που είχε 3010 κλήσεις. Σ' αυτόν τον χρήστη εφαρμόσαμε τρία σενάρια, τροποποιώντας τα CDRs για να δημιουργήσουμε 15 "ψευδείς" κλήσεις απάτης.

Οι τροποποιήσεις έγιναν και στα 3 σενάρια στα ίδια records, δηλαδή οι γραμμές που υπέστησαν αλλαγές ήταν οι 441, 1000, 1429, 2181, 2751, 3001, 3002, 3003, 3004, 3005, 3006, 3007, 3008, 3009 και 3010. Ο τρόπος επιλογής των records έγινε σκόπιμα γιατί θέλαμε να δούμε πώς αντιδρά ο αλγόριθμος σε διάσπαρτες αλλά και σε συνεχόμενες κλήσεις απάτης.

Στο 1ο σενάριο, όλα τα records είχαν τις ίδιες τιμές στα χαρακτηριστικά που εξετάσαμε Bparty: 009955508321, callStart: 2016-03-29 20:42:55, callEnd:2 016-03-29 23:44:14.

Στο 2ο σενάριο, τα πρώτα 5 records (441,1000,1429, 2181 και 2751) είχαν τιμές: BParty009955508321, callStart: 2016-03-24 01:45:53, callEnd: 2016-03-24 03:45:5. Τα υπόλοιπα records 3001-3010 είχαν Bparty: 009955508321, callStart: 2016-03-29

20:42:55, callEnd:2 016-03-29 23:44:14.

Στο 3ο σενάριο, όπως και στο πρώτο, όλα τα records είχαν την ίδια τιμή αλλά με πιο μεγάλες τιμές από αυτό. BParty: 009955508321, callStart: 2016-03-24 01:45:53, callEnd: 2016-03-24 03:45:53.

Όπως παρατηρούμε, οι τιμές έχουν συγκεκριμένα χαρακτηριστικά. Το BParty είναι ο αριθμός τον οποίο καλεί ο χρήστης με κωδικό “009955”, που είναι ο κωδικός κινητών τηλεφώνων στην Γεωργία. Τα άλλα 2 χαρακτηριστικά είναι η ώρα που ξεκίνησε - απαντήθηκε η κλήση (callStart) και η ώρα που ολοκληρώθηκε (callEnd). Αυτά είναι τα χαρακτηριστικά στα οποία έγιναν οι αλλαγές και στα τρία σενάρια που υλοποιήσαμε, με σκοπό να δούμε πώς αντιδρά ο αλγόριθμος με τις ενισχύσεις των τιμών των χαρακτηριστικών.

6.3 Αποτελέσματα

Αποτελέσματα για το 1ο σενάριο.

Fraud Call	**Clusters**	**Vertices**	**Class**
441	11	33	6
1000	10	37	0
1429	7	25	0
2181	11	36	5
2751	9	28	1
3001	15	52	14
3002	15	52	14
3003	16	54	15
3004	16	54	15
3005	9	30	0
3006	9	30	0
3007	10	32	9
3008	10	32	9
3009	10	32	9
3010	10	32	9

Πίνακας 6.1 Αποτελέσματα 1ου σεναρίου

Σχόλια για τα αποτελέσματα του 1ου σεναρίου

Όπως βλέπουμε στον πιο πάνω πίνακα ο αλγόριθμος δεν ομαδοποίησε όλες τις κλήσεις απάτης μαζί, έστω και αν είχαν τις ίδιες τιμές. Όμως, έχουμε αρκετά θετικά στοιχεία, που είναι τα εξής:

1. Οι κλήσεις (3001,3002), (3003,3004), (3005,3006), (3007-3010), ομαδοποιήθηκαν ξεχωριστά με μεγαλύτερη επιτυχία. Ο αλγόριθμος δε στοχοποίησε “καλές” κλήσεις μαζί με τις προαναφερθείσες κλήσεις απάτης, δίνοντας στις κλήσεις απάτης διαφορετικές τιμές (Clusters, Vertices, Class).
2. Η κλήση 441 έχει τα ίδια χαρακτηριστικά με μία “καλή” κλήση, την 2055. Αυτό δεν είναι απόλυτα σωστό. Με τον τρόπο όμως που λειτουργεί ο αλγόριθμός μας, ο οποίος υπενθυμίζουμε ότι συγκρίνει την κλήση που εξετάζει με τις προηγούμενες κλήσεις, μας δείχνει ότι ομαδοποίησε ξεχωριστά τη συγκεκριμένη κλήση και την “ξεχώρισε” από τις προηγούμενες.

Αποτελέσματα για το 2ο σενάριο.

Fraud Call	**Clusters**	**Vertices**	**Class**
441	11	33	6
1000	10	37	0
1429	7	25	0
2181	12	35	5
2751	8	30	5
3001	10	27	0
3002	11	29	6
3003	11	29	6
3004	11	29	6
3005	11	29	6
3006	11	29	6
3007	11	29	6
3008	11	29	6
3009	11	29	6
3010	11	29	6

Πίνακας 6.2 Αποτελέσματα 2ου σεναρίου.

Σχόλια για τα αποτελέσματα του 2ο σενάριο

Όπως βλέπουμε και σε αυτό το σενάριο, ο αλγόριθμος δεν ομαδοποίησε όλες τις κλήσης απάτης μαζί. Η διαφορά σε αυτό το σενάριο είναι ότι οι πρώτες 5 κλήσεις απάτης έχουν πιο έντονα χαρακτηριστικά απάτης.

1. Τα χαρακτηριστικά ομαδοποίησης της κλήσης 441 είναι μοναδικά, γι' αυτό τον λόγο θεωρείται επιτυχής ο εντοπισμός. Επίσης, οι κλήσεις απάτης 3002-3010 ομαδοποιήθηκαν μαζί, χωρίς όμως να ομαδοποιηθεί μαζί τους κάποια "καλή" κλήση.

2. Η κλήση 2181 έχει τα ίδια χαρακτηριστικά με μία "καλή" κλήση, την 2919. Όπως έγινε και στο προηγούμενο σενάριο με την κλήση 441, δεν είναι απόλυτα σωστός ο αλγόριθμος αφού ομαδοποίησε μια "κακή" κλήση με μια κλήση απάτης.

Αποτελέσματα για το 3ο σενάριο.

Fraud Call	**Clusters**	**Vertices**	**Class**
441	11	33	6
1000	10	37	0
1429	7	25	0
2181	12	35	5
2751	8	30	5
3001	10	27	0
3002	11	29	6
3003	11	29	6
3004	11	29	6
3005	11	29	6
3006	11	29	6
3007	11	29	6
3008	11	29	6
3009	11	29	6
3010	11	29	6

Πίνακας 6.3 Αποτελέσματα 3ου σεναρίου.

Σχόλια για τα αποτελέσματα του 3ου σενάριο
Στο τελευταίο μας σενάριο, όπως προαναφέραμε, και οι 15 κλήσεις έχουν υψηλές τιμές. Όπως βλέπουμε από τον πίνακα, και σε αυτό το σενάριο ο αλγόριθμος δεν ομαδοποίησε όλες τις κλήσεις απάτης μαζί. Αυτό το σενάριο έχει τα ίδια αποτελέσματα με το 2ο. Οι κλήσεις 441, 3002-3010 ομαδοποιήθηκαν χωριστά από τις καλές κλήσεις, γι' αύτο το λόγο έχουμε το ίδιο ποσοστό επιτυχίας.

6.3.1 Συγκεντρωτικά Αποτελέσματα

Σενάριο	Επιτυχία (%)	Χρόνος σε δευτερόλεπτα
1	66.66%	33.858
2	66.66%	33.858
3	66.66%	33.858

Πίνακας 6.4 Συγκεντρωτικά αποτελέσματα

Στη συνέχεια κάνουμε σύγκριση των αποτελεσμάτων με 2 άλλες έρευνες, η έρευνα των [Igor Ruiz-Agundez et al, 2011] με το αλγόριθμο EM και η εφαρμογή WEKA [Sandra Kübler et al, 2015] που συνδυάζει 3 αλγόριθμους (k-Means, EM και SOM) μάζι. Επειδή το ποσοστό επιτυχίας των τριών σεναρίων που δημιουργήσαμε είναι το ίδιο και στις 3 περιπτώσεις, η σύγκριση θα γίνει με αυτό το ποσοστό.

Αλγόριθμοι	ESOINN	EM	WEKA
Επιτυχία (%)	66.66	96.22	98,4

Πίνακας 6.5 Σύγκριση αποτελεσμάτων.

Είναι εμφανές ότι ο αλγόριθμός μας έχει το πιο χαμηλό ποσοστό επιτυχίας. Άξιο αναφοράς είναι ότι η εφαρμογή WEKA με τον συνδυασμό τριών αλγορίθμων έχει σχεδόν 100% επιτυχία. Είναι σημαντικό να αναφέρουμε ότι οι δύο έρευνες που επιλέχθηκαν έχουν διαφορετικό σύνολο δεδομένων από την δική μας έρευνα. Η επιτυχία των αλγορίθμων σχετίζεται με την ποιότητα των δεδομένων που εξετάζουν. Έτσι, μπορεί να υπάρξει διαφοροποίηση στο ποσοστό επιτυχίας σε περίπτωση που το δείγμα ελέγχου είναι διαφορετικό. Λόγο της μη διαθεσιμότητας των αλγορίθμων και έλλειψης χρόνου, δεν έγινε δυνατό να εξετάσουμε τα δικά μας δεδομένα με τον αλγόριθμο EM και την εφαρμογή WEKA για να μπορέσουμε να έχουμε σωστά συμπεράσματα για την επιτυχία του ESOINN. Θα επιδιώξουμε να γίνει ένας τέτοιος έλεγχος σε μελλοντική δουλειά.

6.4 Συμπεράσματα

Το ποσοστό επιτυχίας και στα τρία σενάρια είναι 66,66%, δηλαδή ο αλγόριθμος είχε επιτυχία στα ⅔ των κλήσεων απάτης. Αναλύοντας τα αποτελέσματα που παραθέσαμε στους πιο πάνω πίνακες, το 1ο σενάριο είναι αυτό με τη λιγότερη επιτυχία γιατί παρόλο που είχε το ίδιο ποσοστό με τα άλλα δύο σενάρια, τις τελευταίες 10 κλήσεις δεν τις ομαδοποίησε όλες μαζί. Στα σενάρια 2 και 3, παρ' όλες τις διαφορές στις τιμές των κλήσεων απάτης δεν αλλοιώθηκε το αποτέλεσμα, με τη μόνη διαφορά ότι στο σενάριο 2 η κλήση 2181 έχει κάποια χαρακτηριστικά που μπορεί να θεωρηθεί πιθανή κλήση απάτης. Επίσης, είναι σημαντικό να αναφέρουμε ότι και στα τρία σενάρια ο χρόνος ολοκλήρωσης του ελέγχου ήταν 33.858 δευτερόλεπτα, χρόνος πολύ ικανοποιητικός.

Όπως καταδεικνύουν τα αποτελέσματα, δεν υπήρχε ουσιαστική διαφοροποίηση των αποτελεσμάτων σε σχέση με το σενάριο που ακολουθήθηκε. Έτσι, καταλήγουμε στο συμπέρασμα ότι οι μεγάλες διαφορές στα χαρακτηριστικά που εισάγουμε δεν επηρεάζουν και τόσο τον αλγόριθμο.

Είναι φανερή η αστοχία του αλγόριθμού μας σε σχέση με τους άλλους δύο που συγκρίναμε ως προς το ποσοστό επιτυχίας. Μελετώντας τις έρευνες και τα αποτελέσματα των αλγορίθμων φαίνεται ότι τα στοιχεία που τους βοήθησαν για να έχουν τόσο μεγάλη ακρίβεια ήταν η σωστή εκπαίδευση που έγινε αλλά και ο μεγάλος αριθμός κλήσεων που είχαν στη διάθεσή τους. Ακόμη, θα πρέπει να εξεταστεί και η πιθανότητα για συνδυασμό αλγορίθμων, αφού αυτή η μεθοδολογία φαίνεται να είχε πολύ καλά αποτελέσματα στην εφαρμογή WEKA που εξετάσαμε πιο πάνω.

Για μελλοντική έρευνα θα μπορούσαμε να βασιστούμε σε ένα βασικό συμπέρασμα και αυτό είναι ότι ο αλγόριθμος λειτουργεί καλύτερα όταν υπάρχουν συνεχόμενες κλήσεις απάτης. Αν και οι συνεχόμενες κλήσεις απάτης (σε μικρό χρονικό διάστημα) σε σύστηματα VoIP είναι σύνηθες φαινόμενο, θα ήταν καλό να εξεταστεί περαιτέρω ως πιθανή αδυναμία του αλγόριθμου. Θα πρέπει να γίνει περαιτέρω έρευνα ως προς την εκπαίδευση του αλγορίθμου, μέσω της οποίας θα μπορούσαμε να πάρουμε πιο επιτυχή αποτελέσματα.

Επίσης, ο έλεγχος θα ήταν καλό να γίνει με περισσότερα δεδομένα για να έχουμε πιο “σωστά” αποτελέσματα, αν και ρεαλιστικά ένας μέσος χρήστης κάνει πολύ λιγότερες κλήσεις σε σχέση με το δείγμα που ελέγξαμε. Για έναν τέτοιο έλεγχο σε όλους τους χρήστες του συστήματος θα πρέπει να εξεταστεί η πιθανότητα να έχουμε ακριβή αποτελέσματα με όσο μικρότερο δείγμα κλήσεων γίνεται, ή να αναπαράγουμε “ψεύτικα” δεδομένα με βάση τα λίγα πραγματικά που έχει ο εκάστοτε χρήστης.

Κεφάλαιο 7 Επίλογος

Ο εντοπισμός των κλήσεων απάτης σε ένα τηλεφωνικό δίκτυο VoIP είναι ένα σημαντικό πρόβλημα που αντιμετωπίζουν οι εταιρίες τηλεπικοινωνιών. Στην παρούσα μεταπτυχιακή διατριβή αναφέραμε πώς λειτουργεί η τεχνολογία VoIP. Επίσης αναφερθήκαμε στις μηχανές μάθησης και στις κατηγορίες τους. Οι πάροχοι τηλεπικοινωνιακών υπηρεσιών δίνουν περισσότερη έμφαση στον εντοπισμό των κλήσεων απάτης παρά στον εντοπισμό των κακόβουλων χρηστών. Γι΄αυτό τον λόγο, υλοποιήθηκε ένα σύστημα ανίχνευσης κλήσεων απάτης βασισμένο στο δίκτυο μιας μεγάλης εταιρίας τηλεπικοινωνιών της Κύπρου.

Το σύστημα είναι δομημένο έτσι, ώστε να έχει πρόσβαση και να διαβάζει τα δεδομένα των τηλεφωνικών κλήσεων CDRs από τη βάση δεδομένων της εταιρίας για όλους τους χρήστες του δικτύου. Από την ανάλυση των δεδομένων μπορούμε να κατηγοριοποιούμε τις κλήσεις του κάθε χρήστη, δίνοντας μας έτσι τις πιθανές κλήσεις απάτης. Για την ανάλυση των CDRs αναπτύχθηκε μια εφαρμογή η οποία χρησιμοποιεί τον αλγόριθμο μη επιτηρούμενης μάθησης ESOINN.

Πραγματοποιήσαμε δοκιμές μέσω της εφαρμογής που αναφέρθηκε παραπάνω σε δείγμα κλήσεων που προέρχονται από έναν συγκεκριμένο πελάτη, ο οποίος πραγματοποίησε 3010 κλήσεις σε συνεχόμενο διάστημα δύο μηνών. Ερευνήσαμε τρία διαφορετικά σενάρια στα οποία δημιουργήσαμε 15 διαφορετικές κλήσεις απάτης στο κάθε ένα. Από τα αποτελέσματα μας προκύπτει ότι ο αλγόριθμος αναγνωρίζει ένα όχι και τόσο ικανοποιητικό ποσοστό κλήσεων απάτης . Το ποσοστό επιτυχίας του αλγόριθμου και στα τρία σενάρια ήταν 66% και με χρόνο υλοποίησης 33.85 δευτερόλεπτα. Επομένως, συμπεραίνουμε ότι δεν αναγνωρίζει ικανοποιητικά το ποσοστό των κλήσεων απάτης αλλά έχει δώσει αρκετά καλά στοιχεία ώστε να συμπεράνουμε πως είναι μια περίπτωση που αξίζει να αναπτυχθεί περαιτέρω και είναι πολύ πιθανόν να δώσει καλύτερα αποτελέσματα.

7.1 Μελλοντική Δουλειά

Κρίνεται αναγκαία η περαιτέρω ανάλυση των δεδομένων, ώστε να δίνονται περισσότερα χαρακτηριστικά για επεξεργασία, που ίσως δημιουργήσουν δυσκολία στον αλγόριθμο αλλά θα υπάρξει μια καλύτερη εικόνα για το προφίλ του κάθε χρήστη. Επίσης, θα πρέπει να εξεταστεί το πώς θα μπορέσουμε να έχουμε ένα αξιόπιστο προφίλ για χρήστες με ελάχιστο μέσο όρο κλήσεων, κάτι που προκαλεί πρόβλημα στη διεξαγωγή συμπερασμάτων από τον αλγόριθμο.

Κατά την πειραματική διαδικασία, παρατηρήθηκε καθυστέρηση στην εξαγωγή των CDRs από τη βάση δεδομένων. Θα μελετήσουμε τη συγκεκριμένη αδυναμία, για την οποία όμως δεν ευθύνεται ο αλγόριθμος, ώστε να δουλεύει πιο γρήγορα η εφαρμογή. Πιθανώς η χρήση μιας μηχανής με περισσότερα RAM και καλύτερο επεξεργαστή, καθώς και η χρήση indexes στα CDRs να βελτιώσει την ταχύτητα της ανάγνωσης των δεδομένων.

Επίσης, διαπιστώθηκε ότι ο αλγόριθμος έχει καλύτερη απόδοση όταν υπάρχουν συνεχόμενες πιθανές κλήσεις απάτης. Αυτό θα πρέπει να το εξετάσουμε με περισσότερα δεδομένα και με διαφορετική σειρά των κλήσεων απάτης, ώστε να δούμε πώς αντιδρά σε πιο σύνθετα σενάρια.

Τέλος, σκοπεύουμε να διαμορφώσουμε την εφαρμογή έτσι, ώστε να καλείται αυτόματα από τα συστήματα της εταιρίας και ο έλεγχος των κλήσεων να γίνεται ανά τακτά χρονικά διαστήματα 5 λεπτών. Επιπλέον, πολύ σημαντικό για την ανάγνωση των αποτελεσμάτων είναι να ενσωματώσουμε γραφικές παραστάσεις έτσι ώστε να γίνει πιο φιλικό προς τον χρήστη του συστήματος.

Βιβλιογραφία

Communications Fraud Control Association (CFCA).2016, Announces Results of worldwide telecom fraud survey., Available at: <http://www.cfca.org/pdf/survey/2015_CFCA_Global_Fraud_Loss_Survey_Press_Release.pdf> , [Accessed at 20/12/2016].

Ρενέση Ειρήνη.,2008., Μελέτη και ανάπτυξη εφαρμογής voip (Voice over IP) η΄ VVoip(Voice & video over IP) με τη χρήση του Sip πρωτοκόλλου., Πανεπιστήμιο Πατρών., pp 9-35.

Αστέριος Αλμπανάκης.,2011.,Ζητήματα και απαιτήσεις ασφάλειας συστημάτων VoIP Πανεπιστήμιο Μακεδονίας., pp30-66

Φαφούλα Ιωάννα., 2008., ΑΣΦΑΛΕΙΑ VOIP., Πανεπιστήμιο Πειραιά., pp 21-100.

Alexandropoulou Chariklia., 2013.,Comparative Study of Graph-Based SemiSupervised Machine Learning Algorithms on Classification Problems with Extreme Class Imbalance",University of Pireas., pp 8-10.

Pierre Lison.,2013.,An introduction to machine learning., HiOA., pp 14-26.

Richard A et al., 2010 Fraud Detection in Telecommunications: History and Lessons Learned., Statistics Research Department AT&T Labs-Research Florham Park.

Igor Ruiz-Agundez et al.,2011., NETWORK PLANNING OF A VOIP-CABLE PBX The Use of Data Profiling Techniques for an Efficient Network Planning., Deusto Institute of Technology.

Ahmed Aljarray and Abdulla Abouda., 2014.,Analysis and Detection of Fraud in International Calls Using Decision Tree., Almadar Aljadid R&D Office.

Olusola Adeniyi Abidogun.,2005., Data Mining, Fraud Detection and Mobile Telecommunications: Call Pattern Analysis with Unsupervised Neural Networks., University of the Western Cape.

Ledisi G. Kabari.,2016., Telecommunications Subscription Fraud Detection Using

Naïve Bayesian Network., International Journal of Computer Science and Mathematical Theory.

Sandra Kübler et al., 2015., Toll Fraud Detection in Voice over IP Networks Using Communication Behavior Patterns on Unlabeled Data., University of Nairobi School of Computing and Informatics.

Pilsung Kang., 2014., One-Class Naıve Bayesian Classifier for Toll Fraud Detection., IEICE TRANS. INF. & SYST.

Abdikarim Hussein Elmi et al., 2014., Classification of SIM Box Fraud Detection Using Support Vector Machine and Artificial Neural Network., International Journal of Innovative Computing.

Σωτήρης Β. Κωτσιαντής.,2005.,Ομάδες ταξινομιτων για την αύξηση της ακρίβειας των μεθόδων μηχανικής μάθησης και εξόρυξης γνώσης.,Πανεπιστήμιο Πατρών.,pp 70-73.

Pierre Demartines.,1992., Kohonen Self-Organizing Maps: Is the Normalization Necessary?., Polytechnic School of La Usanne., pp 1-3.

Bruno Silva.,2008., New University of Lisbon.

Shen Furaoa et al., 2007., An enhanced self-organizing incremental neural network for online unsupervised learning., Available at: <https://www.researchgate.net/publication/601346>., pp.1-6. [Accessed at 10/2/2017].

F. Shen O. Hasegawa., 2009. Self-organizing incremental neural network and its application. Nanjing University - Tokyo Institute of Technology., pp 24-29.

Kung, Hsiang-Jui and Tung and Hui-Lien.,2006., A Web-Based Tool to Enhance Teaching/Learning Database Normalization., SAIS. pp 1-2.

Jargalsaikhan Alyeksandr., Database design & Normalization (1NF, 2NF, 3NF)., Available at: <https://www.slideshare.net/jagaarj/database-design-normalization>., [Accessed at 19/05/2017].