ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Μελέτη και ανάπτυξη VoIP τηλεφωνίας και των εφαρμογών της

Ονοματεπώνυμο : Νικολόπουλος Νικόλαος

ΑΜ : 37944

Εξάμηνο : 21ο

Τμήμα : Ηλεκτρονικά Υπολογιστικά Συστήματα

Υπεύθυνος Καθηγητής : Βελώνη Αναστασία

Περίληψη

Σε παγκόσμιο επίπεδο, η συγχώνευση των δικτύων δεδομένων και τηλεφωνίας, με στόχο τη μείωση του κόστους επικοινωνίας, αποτελεί μια από τις βασικές προτεραιότητες για πολλές εταιρείες και οργανισμούς. Για το λόγο αυτό, η χρήση της πλεονάζουσας χωρητικότητας των ευρυζωνικών δικτύων τηλεφωνίας και μετάδοσης δεδομένων, καθώς και του Διαδικτύου και των εταιρικών intranet, έχουν αναδειχθεί ως εναλλακτικές λύσεις παλαιότερων δαπανηρών συστημάτων επικοινωνίας. Ταυτόχρονα, όλο και περισσότερες εταιρείες αντιλαμβάνονται την αξία της μετάβασης στην τηλεφωνία μέσω του Διαδικτύου ή δικτύων διαδικτυακού πρωτοκόλλου (Internet Protocol - IP) ώστε να μειωθούν τα κόστη τηλεφώνου και τηλεομοιοτυπίας (fax) και να μπουν οι βάσεις για προηγμένες εφαρμογές πολυμέσων. Η παροχή υψηλής ποιότητας τηλεφωνίας μέσω δικτύων IP είναι ένα από τα βασικά βήματα σύγκλισης υπηρεσιών όπως τηλεφωνίας, fax, βίντεο και δεδομένων επικοινωνίας.

Η τεχνολογία τηλεφωνίας μέσω Διαδικτύου ή δικτύων IP (Voice over IP – VoIP) ποικίλλει ανάλογα με την πολυπλοκότητα: από απλά πακέτα λογισμικού προσωπικών υπολογιστών που μεταδίδουν ψηφιακή φωνή σε ένα δίκτυο, μέχρι πιο περίπλοκα προϊόντα hardware υλικού και λογισμικού. Όλα αυτά τα προϊόντα επικεντρώνονται κυρίως στη χρήση του πρωτοκόλλου IP, ως μηχανισμού φωνητικής μεταφοράς εντός του διαύλου επικοινωνίας, παρέχοντας επικοινωνία χαμηλού κόστους. Παρά το ουσιαστικό πλεονέκτημά της, η τηλεφωνία μέσω VoIP αντιμετωπίζει αρκετά προβλήματα που πρέπει να ληφθούν υπόψη, όπως η καθυστέρηση (delay), η διακύμανση καθυστέρησης (jitter), η απώλεια πακέτων δεδομένων και η ακύρωση ηχούς (echo cancellation). Έτσι, κατά το σχεδιασμό και την υλοποίηση ενός δικτύου VoIP, εκτός από τα θέματα διαλειτουργικότητας και αξιοπιστίας του δικτύου θα πρέπει να εξετάζονται λεπτομερέστατα και τα προβλήματα αυτά. Παρόλα αυτά, η χρήση του VoIP από εταιρίες και οργανισμούς κρίνεται λογικότερη, λαμβάνοντας υπόψη το λόγο κόστους και ωφελειών ως προς τα όποια ζητήματα που πιθανό μπορεί να προκύψουν.

Σκοπός της παρούσας εργασίας, είναι η παρουσίαση μιας σύντομης επισκόπησης της τεχνολογίας VoIP και πώς αυτή μπορεί αυτή να εφαρμοστεί, για την ενοποίηση των δικτύων δεδομένων και τηλεφωνίας. Βασικούς άξονες θα αποτελέσουν τα κύρια χαρακτηριστικά και η τυπική αρχιτεκτονική hardware υλικού και λογισμικού, ενώ θα καλυφθούν και τα περισσότερα ζητήματα που παρουσιάζονται σε ένα σύστημα VoIP, όπως τα τεχνικά προβλήματα και τα θέματα που αφορούν την ποιότητα αλλά και την ασφάλεια της υπηρεσίας. Επιπρόσθετα, θα γίνει μια σύντομη περίληψη των προτύπων και των πρωτοκόλλων επικοινωνίας που χρησιμοποιούνται στο VoIP. Τέλος, θα αναφερθούν και κάποιες από τις πολλές και σημαντικές εφαρμογές της τεχνολογίας.

Λέξεις κλειδιά: Ασφάλεια, ποιότητα QoS, πρωτόκολλο H.323, RTCP, RTP, SIP, VoIP

Abstract

Integrating data and voice networks in order to reduce communication costs, is one of the key priorities for many companies and organizations worldwide. For this reason, the use of excess capacity on broadband voice and data transmission networks as well as the use of the Internet and corporate intranets have emerged as alternatives to previously used costly communication systems. At the same time, more and more companies perceive the value of transporting voice over Internet Protocol networks in order to reduce telephone and fax costs and to put the foundations for advanced multimedia applications. Providing high-quality IP telephony is one of the key steps for convergence of services such as telephony, fax, video and data communication.

Voice over IP (VoIP) technology varies depending on complexity: from simple PC software packages that transmit digital voice over a network to more complicated hardware and software products. All of these products are primarily focused on the use of the IP protocol as a voice transfer mechanism within the communication channel, providing low cost communication. Despite its most important advantage, VoIP faces several problems that need to be considered, such as delay, jitter, packet loss and echo cancellation. Thus, when designing and implementing a VoIP network, in addition to network interoperability and reliability issues, these problems should also be examined in detail. However, the use of VoIP by companies and organizations is considered more reasonable, taking into account the cost-benefit ratio of any issues that may arise.

The purpose of this paper is to present a brief overview of VoIP technology and how this can be applied to the integration of data and telephony networks. Core axes will be the main features and standard hardware and software architecture, and will cover most of the issues in a VoIP system, such as technical issues and issues of quality and security of service. Additionally, a short summary of the standards and communication protocols used in VoIP will be made. Finally, some of the many and important applications of technology will be mentioned.

Keywords: H.323, QoS, RTCP, RTP, security, SIP, VoIP

Περιεχόμενα

Πίνακας εικόνων

1 Εισαγωγή

1.1 Θεωρητικό υπόβαθρο

Στη σύγχρονη εποχή, το μεγαλύτερο κομμάτι της επικοινωνίας γίνεται σε ψηφιακή μορφή και τα δεδομένα μεταφέρονται μέσω δικτύων δεδομένων μεταγωγής πακέτων (Packet Switched Data Network – PSDN), στα οποία η επικοινωνία γίνεται σε διάφορες πλατφόρμες όπως IP, ασύγχρονου τρόπου μεταφοράς (Asynchronous Transfer Mode - ATM) και αναμετάδοσης πλαισίου (Frame Relay). Με δεδομένο ότι στα δίκτυα αυτά η μεταφορά των δεδομένων είναι πολύ πιο γρήγορη από ότι η μετάδοση της φωνής σε ένα συμβατικό τηλεφωνικό δίκτυο, το ενδιαφέρον της ακαδημαϊκής και ερευνητικής κοινότητας στράφηκε προς τη μεταφορά της φωνητικής επικοινωνίας μέσω των δικτύων δεδομένων. Για το λόγο αυτό, έγινε μια προσπάθεια χρήσης της πλεονάζουσας χωρητικότητας των ευρυζωνικών δικτύων τηλεφωνίας και μετάδοσης δεδομένων, καθώς και του Διαδικτύου και των εταιρικών intranet, ως εναλλακτικές λύσεις παλαιότερων δαπανηρών συστημάτων επικοινωνίας.

Η τηλεφωνία VoIP ορίζεται ως: *«η δυνατότητα πραγματοποίησης τηλεφωνικών κλήσεων και αποστολής φαξ μέσω δικτύων δεδομένων IP με κατάλληλη ποιότητα υπηρεσιών (QoS) και μεγαλύτερο λόγο κόστους/όφελους»* [1]. Το VoIP είναι μια μορφή μετάδοσης που επιτρέπει σε οποιοδήποτε άτομο να πραγματοποιεί τηλεφωνικές κλήσεις μέσω ευρυζωνικής διαδικτυακής σύνδεσης. Με τον τρόπο αυτό, οποιοσδήποτε χρήστης μπορεί να πραγματοποιεί και να λαμβάνει κλήσεις μέσω του Διαδικτύου, τόσο προς / από άλλους χρήστες που έχουν την ίδια δυνατότητα, αλλά και προς / από συμβατικές συσκευές, συνήθως με χρέωση υπηρεσίας. Σε ορισμένες υπηρεσίες VoIP για την πραγματοποίηση μιας κλήσης απαιτείται η χρήση ειδικής τηλεφωνικής συσκευής VoIP. Το VoIP μπορεί επίσης να περιγραφεί ως μια ξεχωριστή λύση που επιτρέπει τη μετάδοση φωνητικών σημάτων μέσω σύνδεσης στο Διαδίκτυο και όχι μέσω της παραδοσιακής τηλεφωνικής γραμμής [2]. Η τεχνολογία VoIP αποτελεί μια πιθανή εναλλακτική λύση και συμπλήρωμα των παραδοσιακών τηλεφωνικών συστημάτων μέσω του δημόσιου τηλεφωνικού δικτύου μεταγωγής (Public Switched Telephone Network – PSTN), παρέχοντας μια ευέλικτη και οικονομικά αποδοτική λύση στις φωνητικές επικοινωνίες. Βασικές διαφορές μεταξύ των κλήσεων VoIP και PSTN εμφανίζονται στον Πίνακα 1. [3]

Οι κατασκευάστριες εταιρίες εξοπλισμού είδαν το VoIP ως μια νέα ευκαιρία καινοτομίας και ανταγωνισμού. Η πρόκληση γι' αυτές ήταν η μετατροπή του οράματος σε πραγματικότητα, αναπτύσσοντας νέο εξοπλισμό με δυνατότητα VoIP. Για τους παρόχους υπηρεσιών Διαδικτύου (Internet Service Providers - ISP), η δυνατότητα εισαγωγής τιμολογίων βάσει της χρήσης και η αύξηση του όγκου κυκλοφορίας δεδομένων εντός των δικτύων τους, ήταν στοιχεία πολύ ελκυστικά. Από την άλλη πλευρά, οι χρήστες (άτομα και εταιρίες) έδειξαν ιδιαίτερο ενδιαφέρον για

την ενσωμάτωση εφαρμογών φωνής και δεδομένων καθώς και τα οφέλη, από άποψη κόστους, που θα προέκυπταν από αυτήν.

Πίνακας 1: Σύγκριση ποιότητας κλήσεων PSTN και VoIP [3]

	Κλήσεις PSTN	**Κλήσεις VoIP**
Μεταγωγή (Switching)	Κυκλώματος (στην από άκρο σ' άκρο δεσμευμένη γραμμή)	Πακέτων
Ρυθμός μετάδοσης δεδομένων (Bit Rate)	28.8kbps (με παρουσία modem)	~14 kbps (μόνο κατά την ομιλία και ανάλογα τον κωδικοποιητή)
Καθυστέρηση μεταφοράς (Latency)	Μικρότερη των 100ms	200-700ms (ανάλογα με τη συνολική κίνηση του δικτύου IP)
Εύρος ζώνης (Bandwidth)	Εγγυημένο (Dedicated)	Δυναμικά κατανεμημένο (Dynamical allocated)
Κόστος πρόσβασης/τιμολόγηση	Μηνιαία χρέωση ανά γραμμή με προστιθέμενη ανά λεπτό χρήση	Κόστος της IP υποδομής και του εξοπλισμού (υβριδικές IP/PBX και IP τ/φ συσκευές)
Εξοπλισμός	Απλές τ/φ συσκευές (λιγότερο δαπανηρές)	Προγραμματιζόμενες τ/φ συσκευές (δαπανηρές)
Ποιότητα υπηρεσιών (QoS)	Υψηλή(εξαιρετικά μικρές απώλειες)	Χαμηλή και μεταβλητή (ανάλογα με την απώλεια πακέτων και την καθυστέρηση του δικτύου)
Διαθεσιμότητα δικτύου	99.999% διαθέσιμο	Απροσδιορίστου επιπέδου αξιοπιστίας
Ασφάλεια (Security)	Υψηλό επίπεδο λόγω της δεσμευμένης ζεύξης	Δυνατότητα υποκλοπών

Στις σημερινές εφαρμογές VoIP, τα αναλογικά σήματα φωνής υποβάλλονται σε δειγματοληψία και κωδικοποιούνται χρησιμοποιώντας κωδικοποιητή, στη συνέχεια ενσωματώνονται σε ένα πακέτο IP και μεταφέρονται μέσω της διαδικτυακής υποδομής με τον ίδιο τρόπο που μεταφέρονται τα πακέτα δεδομένων [4].

Η ιστορία του VoIP ξεκίνησε με επικοινωνία μεταξύ ελάχιστων χρηστών υπολογιστών μέσω του Διαδικτύου. Αρχικά, για την πραγματοποίηση οποιασδήποτε κλήσης VoIP ήταν απαραίτητη η σύνδεση ενός μικροφωνοακουστικού στους υπολογιστές των εμπλεκόμενων χρηστών. Πριν την πραγματοποίηση οποιασδήποτε τηλεφωνικής επικοινωνίας ήταν απαραίτητη η πρότερη ειδοποίηση για την ώρα που θα γινόταν η κλήση [5]. Τον Νοέμβριο του 1977, η Τακτική Δύναμη Μηχανικών Διαδικτύου (Internet Engineering Task Force – IETF) δημοσίευσε τις προδιαγραφές του πρωτοκόλλου φωνητικού δικτύου (Network Voice Protocol - NVP). Το έγγραφο αυτό απεικόνιζε τη δυνατότητα ανάπτυξης και υλοποίησης ασφαλών και υψηλής ποιότητας καθώς και μικρού εύρους ζώνης, πραγματικού χρόνου και πλήρως αμφίδρομων ψηφιακών φωνητικών επικοινωνιών μέσω δικτύων PSDN [2]. Στα μέσα της δεκαετίας του 90, οι τεχνολογικές εξελίξεις στον τομέα της πληροφορικής και των δικτύων οδήγησε στην αύξηση των δικτύων IP και στην εκτεταμένη χρήση των προσωπικών υπολογιστών. Η πεποίθηση ότι το VoIP θα μπορούσε να έχει σημαντικές επιπτώσεις στην αγορά είχε ως αποτέλεσμα μεγάλες προσδοκίες που οδήγησαν στη

διανομή του πρώτου πακέτου λογισμικού. Στα πρώτα στάδια της, η τεχνολογία VoIP δεν αναπτύχθηκε πλήρως και παρατηρήθηκε ένα μεγάλο χάσμα μεταξύ του μάρκετινγκ και της τεχνολογικής πραγματικότητας. Για το λόγο αυτό, οι τεχνικές ελλείψεις σταμάτησαν οποιαδήποτε σημαντική εξέλιξη ή αλλαγές στο VoIP. Ωστόσο, στις αρχές της δεκαετίας του 2010, το VoIP συνέχισε την τεχνολογική και εμπορική πρόοδό του. Δημιουργήθηκαν πρωτόκολλα σηματοδοσίας που χρησιμοποιούνται για τη ρύθμιση και αποκοπή κλήσεων, τη μεταφορά δεδομένων που απαιτούνται για τον εντοπισμό χρηστών και τη διερεύνηση δυνατότητας κλήσεων [5]. Με τον τρόπο αυτό, τελειοποιήθηκαν πολλές από τις ατέλειες και αντιμετωπίστηκαν πολλά από τα ζητήματα της τεχνολογίας.

Ένα βασικό πλεονέκτημα του VoIP είναι η πραγματοποίηση κλήσεων μεγάλων αποστάσεων με πολύ φθηνές τιμές. Στις κλήσεις αυτές περιλαμβάνονται και οι κλήσεις εξωτερικού καθώς υπάρχει η ευελιξία χρησιμοποίησης του ίδιου αριθμού σε διάφορα μέρη του κόσμου [6]. Επίσης, η συνεχιζόμενα αυξανόμενη υιοθέτηση των IP δικτύων στην υποδομή των παρόχων δικτύων επικοινωνίας και στα ιδιωτικά εταιρικά δίκτυα των επιχειρήσεων και των οργανισμών, δημιουργεί τις κατάλληλες προϋποθέσεις χρήσης της τεχνολογίας VoIP, με αποτέλεσμα να διευκολύνεται σε μεγάλο βαθμό η επικοινωνία μεταξύ των εργαζομένων, είτε εργάζονται στο χώρο της εταιρίας, είτε εργάζονται από το σπίτι, είτε ταξιδεύουν. Το VoIP μπορεί επίσης να αυξήσει την εταιρική αποτελεσματικότητα.

Παρόλο που το VoIP, υποστηρίζοντας τηλεφωνικές κυρίως επικοινωνίες με χρήση IP, έχει γίνει ελκυστικό κυρίως για το χαμηλό κόστος και τη χαμηλή τιμολόγηση του Διαδικτύου, η τεχνολογία του δεν έχει αναπτυχθεί σε τέτοιο σημείο που να μπορεί να αντικαταστήσει τις παρεχόμενες υπηρεσίες και την ποιότητα του δημόσιου δικτύου. Όπως αναφέρθηκε, στο VoIP, το φωνητικό σήμα ψηφιοποιείται, συμπιέζεται και τεμαχίζεται σε πακέτα τα οποία αποστέλλονται με άλλα πακέτα στο δίκτυο PSDN. Στο άκρο λήψης, τα ανασυγκροτημένα πακέτα φτάνουν ως κανονική φωνητική κλήση. Ζητούμενο στο VoIP είναι η επιτυχημένη μετάδοση της φωνής μέσω των δικτύων PSDN. Ωστόσο, η υλοποίηση της τεχνολογίας μέσω των διαφόρων προϊόντων που έχουν δημιουργηθεί και κατασκευαστεί δεν είναι τόσο απλή, λόγω της μεγάλης γκάμας προτύπων που χρησιμοποιούνται, των διαφορετικών απαιτήσεων των χρηστών και των ζητημάτων της διαλειτουργικότητας και της επεκτασιμότητας που έχουν προκύψει.

Ορισμένα από τα πλεονεκτήματα και τα μειονεκτήματα του συστήματος VoIP είναι τα εξής [7]:

Ι) Πλεονετήματα

- Χαμηλό κόστος
- Ευελιξία
- Παρέχει φωνητικό ταχυδρομείο (voice mail) και προώθηση κλήσεων
- Δωρεάν υπηρεσίες (συνήθως στη σύνδεση υπολογιστή με υπολογιστή)

- Οι χρήστες μπορούν να κάνουν κλήσεις VoIP (κλήσεις μεγάλων αποστάσεων & διεθνείς κλήσεις) από οπουδήποτε
- Εύκολη υλοποίηση και εγκατάσταση
- Αξιοποίηση της χωρητικότητας του δικτύου
- Συνεργασία και ολοκλήρωση με άλλες διαθέσιμες υπηρεσίες μέσω Διαδικτύου

II) Μειονεκτήματα

- Οι χρήστες δεν μπορούν να πραγματοποιήσουν κλήσεις κατά τη διάρκεια διακοπής ρεύματος. Στην περίπτωση αυτή η παρουσία UPS θα μπορούσε να περιορίσει το ζήτημα
- Περιορισμός σύνδεσης στις υπηρεσίες έκτακτης ανάγκης
- Εξαρτάται από την κατάσταση σύνδεσης στο Διαδίκτυο
- Το δίκτυο IP δεν εγγυάται ποιότητα QoS στις υπηρεσίες φωνητικής επικοινωνίας

Σε γενικές γραμμές, οι τρόποι σύνδεσης δύο χρηστών μέσω τις τεχνολογίας VoIP μπορεί να είναι σύνδεση υπολογιστή με υπολογιστή, σύνδεση τηλεφωνικής συσκευής με τηλεφωνική συσκευή και σύνδεση υπολογιστή με υπολογιστή [7]. Επομένως, η τηλεφωνία μπορεί να είναι ψηφιακού ή αναλογικού τύπου. Σε περίπτωση αναλογικού τύπου, η σύνδεση της τηλεφωνικής συσκευής θα πρέπει να πραγματοποιείται μέσω προσαρμογέων που μετατρέπουν τα αναλογικά σήματα σε ψηφιακή μορφή.

1.2 Σκοπός της πτυχιακής εργασίας

Η φωνητική επικοινωνία αποτελεί και θα συνεχίσει να αποτελεί αναπόσπαστο κομμάτι όλων των ανθρώπων. Επομένως είναι σημαντικό να γίνει φθηνή και προσιτή. Για να γίνει αξιόπιστη και πιο προσιτή οικονομικά σε σχέση με το δημόσιο τηλεφωνικό δίκτυο μεταγωγής (PSTN), η αλλαγή είναι αναπόφευκτη ώστε να συμβαδίζει με την παγκόσμια τεχνολογική αλλαγή. Η τηλεφωνία VoIP είναι ένας τρόπος επικοινωνίας και μια τεχνολογία που επιτρέπει στους χρήστες να πραγματοποιούν τηλεφωνικές κλήσεις μέσω ενός δικτύου IP, παρέχοντας αξιόπιστες και οικονομικά πιο προσιτές λύσεις.

Σκοπός της παρούσας πτυχιακής εργασίας είναι μια ανάλυση του VoIP σε τέτοιο επίπεδο ώστε να λυθούν οι όποιες εταιρικές ανησυχίες σχετικά με την εφαρμογή του. Οι ανησυχίες αυτές αφορούν την ποιότητα των υπηρεσιών του (QoS) καθώς και τα θέματα ασφάλειας που μπορούν να προκύψουν στις διάφορες εφαρμογές του. Για το λόγο αυτό, παρουσιάζεται μια σύντομη εισαγωγή της τεχνολογίας VoIP που αφορά την αρχιτεκτονική δομή του δικτύου, χωρίς όμως να γίνεται ανάλυση των διαφόρων τύπων υλοποίησής του. Επιπλέον, εξετάζονται τα πρωτόκολλα και οι κωδικοποιητές που χρησιμοποιεί και ταυτόχρονα γίνεται μια σύγκριση των πρωτοκόλλων αυτών. Επίσης, αναφέρονται τα πλεονεκτήματα της τεχνολογίας, χωρίς να παραλείπονται τα

ζητήματα που αφορούν την υλοποίησή της και είναι σχετικά με την ασφάλεια και την ποιότητα των παρεχόμενων υπηρεσιών.

Για την αναζήτηση της βιβλιογραφίας θα χρησιμοποιηθούν οι βάσεις δεδομένων Google Scholar και Google, όσο και ανασκοπήσεις από διάφορες μελέτες, άρθρα και πηγές μέσω του Διαδικτύου.

1.3 Δομή της πτυχιακής εργασίας

Στα πλαίσια της παρούσας πτυχιακής εργασίας, για την μελέτη και ανάπτυξη της τηλεφωνίας VoIP και των εφαρμογών της, επιλέχθηκε μια δομή που οργανώνεται σε έξι κεφάλαια. Το πρώτο εισαγωγικό κεφάλαιο καλύπτει μια βιβλιογραφική ανασκόπηση των βασικών στοιχείων της τεχνολογίας VoIP, μια σύντομη ιστορική αναδρομή της εξέλιξης της τεχνολογίας, καθώς και το σκοπό της εργασίας. Το υπόλοιπο της παρούσας πτυχιακής οργανώνεται ως εξής:

Το δεύτερο κεφάλαιο ασχολείται με την αρχιτεκτονική δομή της τεχνολογίας VoIP και τη λειτουργική της διαδικασία, δίνοντας έμφαση στον εξοπλισμό που χρησιμοποιείται στη διαδικασία αυτή.

Στο τρίτο κεφάλαιο, εξηγούνται λεπτομερώς οι τεχνικές κωδικοποίησης και τα πρωτόκολλα που υλοποιούν την τεχνολογία VoIP. Στο κεφάλαιο παρουσιάζονται επίσης οι ελλείψεις των πρωτοκόλλων αυτών, που προκύπτουν μέσω της μεταξύ τους σύγκρισης.

Το τέταρτο κεφάλαιο ασχολείται με τα θέματα της ποιότητας υπηρεσιών (QoS) της τεχνολογίας VoIP. Τα θέματα αυτά αναλύονται με παράλληλη παρουσίαση τρόπων αντιμετώπισής τους για την παροχή της απαιτούμενης ποιότητας QoS σε ένα δίκτυο VoIP.

Το πέμπτο κεφάλαιο ασχολείται με την ασφάλεια και τα ζητήματα ασφάλειας που μπορεί να αντιμετωπίσει η VoIP τηλεφωνία στα διάφορα δίκτυα υλοποίησής της. Αρχικά γίνεται μια παρουσίαση των ευπαθειών των συστημάτων VoIP. Στη συνέχεια γίνεται μια αναφορά στις επιθέσεις ασφάλειας που σχετίζονται με τα πρωτόκολλα και τις συσκευές VoIP. Το κεφάλαιο ολοκληρώνεται με την εξέταση του προφίλ ασφάλειας των πρωτοκόλλων VoIP και με την παρουσίαση των βασικών συστατικών ασφαλείας που έχουν σχεδιαστεί για να βοηθήσουν στην ανάπτυξη αξιόπιστων και ασφαλών συστημάτων VoIP.

Στο έκτο κεφάλαιο παρουσιάζεται μια μικρή σύνοψη και ανάλυση των δημοφιλέστερων σύγχρονων εφαρμογών VoIP.

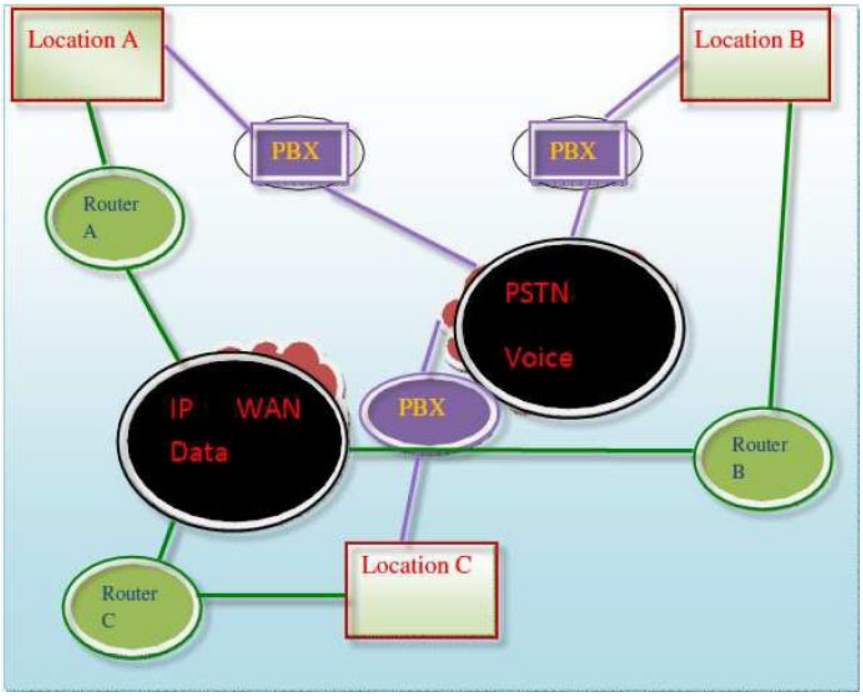
Τέλος, η εργασία ολοκληρώνεται με κάποια συμπεράσματα που προκύπτουν από την μελέτη και ανάπτυξη της τηλεφωνίας VoIP και των εφαρμογών της.

2 Τεχνολογία VoIP

2.1 Αρχιτεκτονική δομή VoIP

Το VoIP είναι μια από τις πιο κοινές και φθηνές τεχνολογίες τηλεφωνικής επικοινωνίας μικρών και μεγάλων αποστάσεων. Φιλοσοφία της τεχνολογίας είναι η μετάδοση ψηφιοποιημένων φωνητικών δεδομένων μέσω δικτύου IP, ώστε να δίνεται η δυνατότητα στους χρήστες του Διαδικτύου, να πραγματοποιούν τηλεφωνικές συνομιλίες. Το φωνητικό σήμα του καλούντος κωδικοποιείται κατάλληλα στο ένα άκρο του καναλιού επικοινωνίας και μεταδίδεται με τη μορφή IP πακέτων. Στο άλλο άκρο του καναλιού επικοινωνίας, στο λήπτη, τα πακέτα αυτά αποκωδικοποιούνται και μετασχηματίζονται σε φωνητικό σήμα.

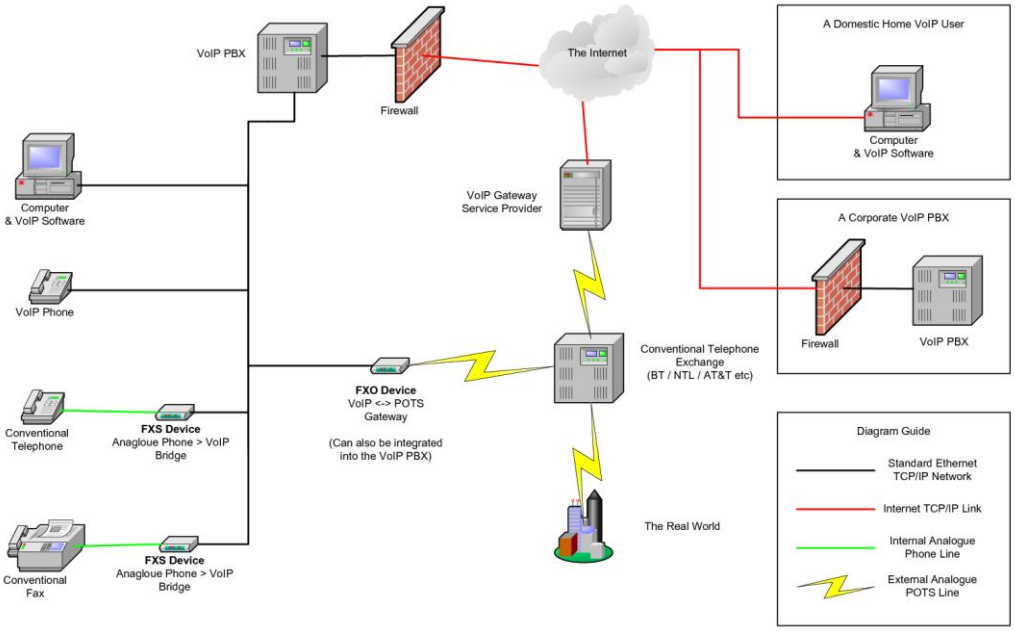
Το απλό διάγραμμα που φαίνεται στην εικόνα 1 απεικονίζει σε γενικές γραμμές αυτή τη φιλοσοφία του VoIP. Οι κλήσεις VoIP ξεκινούν από μια θέση Α και στη συνέχεια, αν γίνονται μέσω δικτύου IP, διασχίζουν τον δρομολογητή (router) Α, ενώ διαφορετικά οδηγούνται προς το τ/φ κέντρο PBX (Private Branch Exchange) για να μεταφερθούν μέσω του δικτύου PSTN. Στην περίπτωση που χρησιμοποιηθεί το δίκτυο PSTN, η τηλεφωνική κλήση δρομολογείται στο PBX προορισμού και στη συνέχεια στη θέση Γ. Αντίθετα, αν χρησιμοποιηθεί το δίκτυο IP, η κλήση από τον δρομολογητή Α οδηγείται στο δρομολογητή C μέσω του IP WAN DATA, από όπου και τερματίζει στην τοποθεσία προορισμού.



Εικόνα 1: *Φιλοσοφία συστήματος VoIP [8]*

Στην εικόνα 2 παρουσιάζεται η αρχιτεκτονική δομή των κλήσεων VoIP που γίνονται με χρήση μιας IP τηλεφωνικής συσκευής, με περισσότερες λεπτομέρειες. Ο

πρώτος χρήστης (καλών) πληκτρολογεί τον τ/φ αριθμό της κλήσης στο ψηφιακό πληκτρολόγιο της συσκευής. Ο αριθμός αυτός μετατρέπεται σε δυαδικό κώδικα, ο οποίος με τη σειρά του μετατρέπεται σε πακέτα IP που μεταδίδονται προς το τοπικό δίκτυο (LAN). Τα πακέτα, στη συνέχεια, οδηγούνται προς το δρομολογητή, ο οποίος αναλύει τη IP διεύθυνση του προορισμού και τα προωθεί στο δίκτυο IP. Στο σημείο αυτό, η κλήση δρομολογείται ανάλογα με τη φύση του προορισμού, για παράδειγμα, αν ο προορισμός είναι μια απλή τ/φ συσκευή, τότε προωθείται προς μια πύλη PSTN η οποία τη μεταβιβάζει στο σωστό προορισμό. Αντίθετα, αν η κλήση είναι αμιγώς VoIP, τότε θα προωθηθεί προς το σχετικό δρομολογητή που αναλύει τη διεύθυνση IP και την κατευθύνει προς το ανάλογο τοπικό δίκτυο LAN. Τέλος, στην περίπτωση αυτή, η κλήση οδηγείται στο IP τηλέφωνο του καλούμενου.

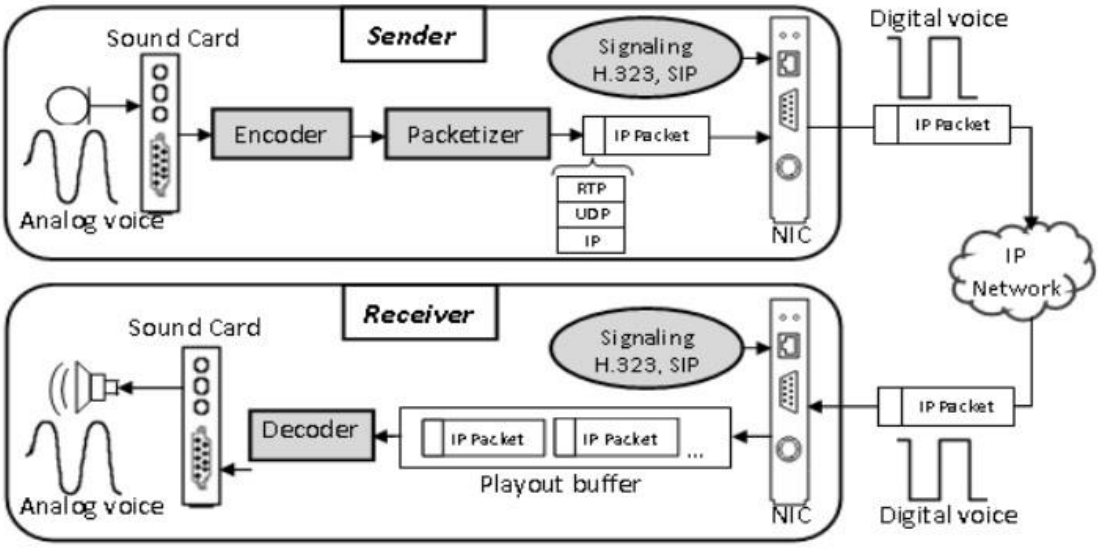


Εικόνα 2: *Αρχιτεκτονική δομή VoIP [9]*

2.2 Λειτουργία VoIP

Το VoIP χρησιμοποιεί το πρωτόκολλο IP για τη μετάδοση φωνής ως πακέτα δεδομένων μέσω δικτύων IP. Η διαδικασία αυτή περιλαμβάνει την ψηφιοποίηση της φωνής, την απομόνωση ανεπιθύμητων σημάτων θορύβου και στη συνέχεια τη συμπίεση του φωνητικού σήματος, χρησιμοποιώντας αλγορίθμους/κωδικοποιητές συμπίεσης. Μετά τη συμπίεση, η φωνή πακετοποιείται για να αποσταλεί μέσω ενός δικτύου IP. Σε κάθε πακέτο ενσωματώνεται μια κεφαλίδα, η οποία περιέχει τη διεύθυνση προορισμού, έναν αριθμό ακολουθίας και δεδομένα για τον έλεγχο σφαλμάτων. Τα πρωτόκολλα σηματοδότησης προστίθενται σε αυτό το στάδιο, για να επιτευχθούν αυτές οι απαιτήσεις μαζί με όλες τις υπόλοιπες απαιτήσεις διαχείρισης κλήσεων. Όταν ένα πακέτο φωνής φτάνει στον προορισμού, ο αριθμός ακολουθίας επιτρέπει στα πακέτα να τοποθετηθούν με τη σωστή σειρά και στη συνέχεια η εφαρμογή των αλγορίθμων αποσυμπίεσης οδηγεί στην ανάκτηση των δεδομένων από

τα πακέτα. Στο σημείο αυτό πραγματοποιείται διαχείριση συγχρονισμού και καθυστέρησης ώστε να διασφαλιστεί η ορθότητα του λαμβανόμενου σήματος. Το jitter buffer χρησιμοποιείται για την αποθήκευση των πακέτων που φθάνουν μέσω διαφόρων δρομολογίων, αποθηκεύοντας έτσι τα πακέτα που φτάνουν αργά [10]. Όλη αυτή η λειτουργική διεργασία του VoIP περιλαμβάνει πολλές ενδιάμεσες διατάξεις, όπως φαίνεται και από την εικόνα 3.



Εικόνα 3: *Διεργασία VoIP [7]*

Πιο αναλυτικά, η συνολική λειτουργία του VoIP συνοψίζεται στα ακόλουθα βήματα, στα οποία αναφέρονται και τα διάφορα TCP/IP στρώματα καθώς και κάποια πρωτόκολλα που συμμετέχουν:

- ***Ψηφιοποίηση φωνής:*** Το VoIP χρησιμοποιεί το πρωτόκολλο IP για τη μετάδοση του φωνητικού σήματος με τη μορφή πακέτων δεδομένων μέσω δικτύων IP. Επομένως, όπως ακριβώς συμβαίνει και στο συμβατικό σύστημα PSTN, η επικοινωνία VoIP απαιτεί μια συσκευή εισόδου ήχου, όπως ένα μικρόφωνο, για την σύλληψη του ηχητικού σήματος. Στη συνέχεια, το αναλογικό φωνητικό σήμα μετατρέπεται σε ψηφιακό μέσω ενός μετατροπέα αναλογικού σε ψηφιακό σήμα (Analog to Digital Converter – A/D Converter)
- ***Κωδικοποίηση ψηφιοποιημένου ήχου:*** Πριν από την αποστολή του ψηφιακού σήματος στο δίκτυο μεταγωγής πακέτων, είναι απαραίτητη η κωδικοποίηση και η συμπίεση του σήματος αυτού. Τα παραδοσιακά τηλεφωνικά δίκτυα χρησιμοποιούν παλμοκωδική διαμόρφωση (Pulse Code Modulation - PCM) 8K δειγμάτων ανά δευτερόλεπτο. Δείγματα των 12 bit συμπιέζονται και επεκτείνονται από έναν μη γραμμικό πίνακα αναζήτησης σε λέξεις των 8 bit δίνοντας μια μεταδιδόμενη ταχύτητα 8kbit/s. Η συμπίεση που συνήθως χρησιμοποιείται από ένα IP τηλέφωνο είναι της τάξεως των 16 προς 1 (δηλαδή από 128kbit/s έως 8kbit/s) και επομένως είναι μεγαλύτερη αυτής που επιτυγχάνεται με διαμόρφωση PCM. Στην περίπτωση μάλιστα που το

τηλέφωνο IP βρίσκεται εντός τοπικού δικτύου LAN, και όταν υπάρχει επαρκές εύρος ζώνης, δεν υπάρχει ανάγκη συμπίεσης

- ***Πακετοποίηση:*** Μετά τη συμπίεση, η φωνή πακετοποιείται για την αποστολή της μέσω του IP δικτύου. Η πρώτη πακετοποίηση υλοποιείται στο στρώμα εφαρμογών (application layer) χρησιμοποιώντας πρωτόκολλο μεταφοράς πραγματικού χρόνου (Real-time Transport Protocol - RTP). Με τον τρόπο αυτό, τα φωνητικά πακέτα τελικά μετατρέπονται σε πακέτα δεδομένων και αποστέλλονται στο στρώμα μεταφοράς (transport layer) (Εικ. 4)

- ***Στρώμα μεταφοράς:*** Το στρώμα μεταφοράς παρέχει τους κανόνες που απαιτούνται για την αποστολή των δεδομένων. Αν και για την μεταφορά των δεδομένων μέσω του Διαδικτύου, οι περισσότερες τεχνολογίες χρησιμοποιούν το πρωτόκολλο ελέγχου μετάδοσης (Transmission Control Protocol - TCP), το οποίο εγγυάται την παράδοση και την ακεραιότητα των δεδομένων, το VoIP δεν χρειάζεται μια τέτοια είδους εγγύηση παράδοσης και για το λόγο αυτό, το IP δίκτυο σε VoIP μεταδόσεις μπορεί να χρησιμοποιήσει ένα εναλλακτικό και ταχύτερο πρωτόκολλο στρώματος μεταφοράς, το πρωτόκολλο δεδομενογράμματος χρήστη (User Datagram Protocol - UDP). Σε στρώμα μεταφοράς με πρωτόκολλο UDP, τα δεδομένα μεταδίδονται με τη μορφή datagram. Κάθε datagram περιέχει τη διεύθυνση προέλευσης, τη διεύθυνση προορισμού και έναν αριθμό ακολουθίας και δρομολογείται ανεξάρτητα μέσω του δικτύου. Τα λαμβανόμενα πακέτα επανασυναρμολογούνται στο άκρο της λήψης

- ***Στρώμα δικτύου:*** Τα πακέτα δεδομένων αποστέλλονται στο στρώμα δικτύου (network layer) με τη μορφή datagram. Στο στρώμα αυτό χρησιμοποιείται το πρωτόκολλο διαδικτύου (Internet Protocol – IP) που καθορίζει τη σύνδεση μεταξύ δύο υπολογιστών μέσω του Διαδικτύου και παρέχει την κατάλληλη δρομολόγηση των datagram μεταξύ δύο οποιωνδήποτε κόμβων, με έλεγχο για διαφθορά (corruption) και απώλεια (loss)

- ***Στρώμα εφαρμογών:*** Μόλις τα δεδομένα VoIP φθάσουν στον προορισμό τους, μέσω της αντίθετης σειράς στρωμάτων από αυτή που υπάρχει κατά την αποστολή τους (Εικ. 4), το στρώμα εφαρμογών το αντιλαμβάνεται και τα προωθεί προς το λήπτη. Στο στρώμα εφαρμογών, η τεχνολογία VoIP χρησιμοποιεί πρωτόκολλα σηματοδοσίας (H.323, SIP, και MGCP) για τη δημιουργία σύνδεσης μεταξύ των άκρων της κλήσης, καθώς και πρωτόκολλα μέσων (RTP, RTCP και RTSP) για τη σωστή διαχείριση των δεδομένων πραγματικού χρόνου, όπως είναι τα δεδομένα ήχου ή βίντεο. Τα πιο συχνά χρησιμοποιούμενα πρωτόκολλα στο στρώμα εφαρμογών για το VoIP είναι τα SIP και RTP

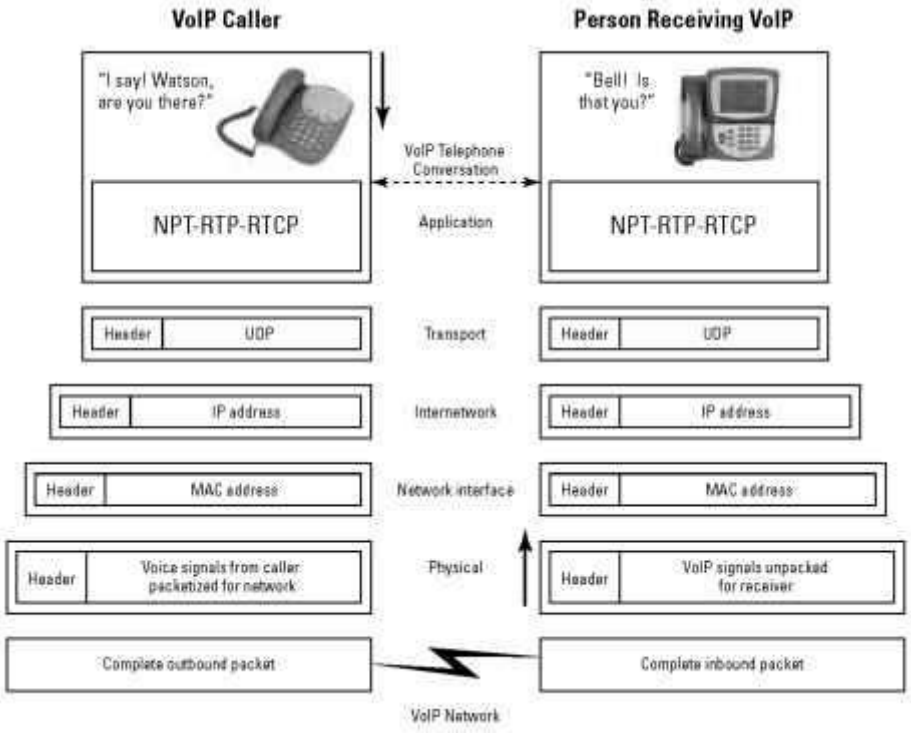
- ***Σηματοδοσία:*** Στο επίπεδο εφαρμογών, το σύστημα σηματοδοσίας εκτελεί τις ακόλουθες διεργασίες [11]:

  1. Βρίσκει τη διεύθυνση IP προορισμού

2. Αφού εντοπίσει τη διεύθυνση IP προορισμού δημιουργεί επικοινωνία με το συγκεκριμένο συμβαλλόμενο μέρος της κλήσης

3. Μετά την ανταλλαγή μηνυμάτων διαπραγμάτευσης, το πρωτοκόλλου IP πραγματοποιεί φωνητική συμπίεση, διαμορφώνει το μήκος και σφραγίζει χρονικά τα πακέτα και αρχίζει την επικοινωνία. Ωστόσο, η διαδικασία αυτή καθίσταται πιο περίπλοκη εάν το σύστημα σηματοδοσίας πρέπει να υποστηρίξει επικοινωνία με κάποια πύλη μεταξύ του Διαδικτύου και του δικτύου PSTN. Οι πύλες είναι συσκευές που επιτρέπουν την πραγματοποίηση κλήσεων προς και από άλλα τηλεφωνικά δίκτυα, τα οποία υλοποιούνται μεταξύ του Διαδικτύου και του δικτύου PSTN. Φυσικά, μια πύλη δεν μπορεί να υποστηρίξει τον ίδιο αριθμό χρηστών που μπορεί ακόμα και το μικρότερο τοπικό τηλεφωνικό κέντρο. Στην περίπτωση εξερχόμενων κλήσεων, το τηλέφωνο VoIP καταγράφει τον αριθμό τηλεφώνου και τη διεύθυνση IP της πύλης. Αλλά στην περίπτωση που η κλήση γίνει από το δίκτυο PSTN προς το Διαδίκτυο είναι μάλλον ανέφικτο για τον χρήστη του δικτύου PSTN να εισάγει τον αριθμό τηλεφώνου της πύλης και στη συνέχεια τη διεύθυνση IP του χρήστη που θέλει να καλέσει

- ***Αναπαραγωγή ήχου:*** Τέλος στο άκρο λήψης, τα πακέτα αποσυναρμολογούνται για την εξαγωγή των δεδομένων, στη συνέχεια τα δεδομένα μετατρέπονται σε αναλογικό φωνητικό σήμα, το οποίο αποστέλλεται στην κάρτα ήχου του υπολογιστή ή στο τηλέφωνο VoIP του λήπτη



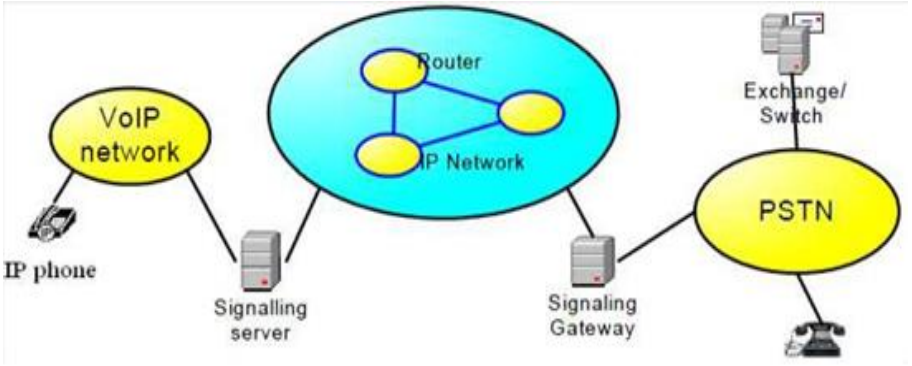
Εικόνα 4: *Το TCP/IP μοντέλο του VoIP [12]*

2.3 Εξοπλισμός τεχνολογίας VoIP

Ένα σύστημα τηλεφωνίας μέσω διαδικτύου περιλαμβάνει τρεις τύπους εξοπλισμού [13, 14]:

- ***Τερματικά συστήματα:*** είναι ηλεκτρονικές συσκευές τις οποίες οι πελάτες ή οι χρήστες τοποθετούν στο χώρο τους για την πραγματοποίηση κλήσεων
- ***Πύλες μέσων:*** είναι συσκευές που επιτρέπουν την πραγματοποίηση κλήσεων μεταξύ των τηλεφωνικών δικτύων
- ***Διακομιστές σηματοδοσίας:*** χειρίζονται τον έλεγχο στρώματος εφαρμογών της δρομολόγησης των μηνυμάτων σηματοδοσίας

Ένα τερματικό σύστημα μπορεί να πραγματοποιήσει ή να δεχθεί μια κλήση, καθώς και να απορρίπτει ή να προωθεί τις εισερχόμενες κλήσεις. Όταν ένα τερματικό σύστημα πραγματοποιεί μια κλήση, η αίτηση πραγματοποίησης κλήσης μπορεί να προωθηθεί μέσα από πολλαπλές διαδρομές, μέσω του εξοπλισμού του δικτύου. Αρχικά, το σύστημα πραγματοποίησης κλήσης θα πρέπει να αποφασίσει πού να στείλει τα αιτήματά του. Οι επιλογές είναι δύο: μπορεί να ρυθμιστεί έτσι ώστε όλα τα αιτήματά του να μεταβούν στο τοπικό διακομιστή ή μπορεί να χρησιμοποιήσει τη διεύθυνση προορισμού για να εντοπίσει έναν απομακρυσμένο διακομιστή σηματοδοσίας ή ένα τελικό σύστημα, στα οποία μπορεί να στείλει άμεσα το αίτημα (Εικ. 5). Μόλις το αίτημα φτάσει σε κάποιο διακομιστή σηματοδοσίας, ο συγκεκριμένος διακομιστής χρησιμοποιεί τη βάση δεδομένων τοποθεσίας χρήστη, την τοπική πολιτική, την ανάλυση DNS ή άλλες μεθόδους για τον προσδιορισμό του επόμενου διακομιστή σηματοδοσίας ή του συστήματος τερματισμού, στο οποίο θα πρέπει να αποσταλεί το αίτημα. Ένα αίτημα μπορεί να περάσει από πολλούς διακομιστές σηματοδοσίας, ο αριθμός των οποίων ποικίλλει: από κανένα (στην περίπτωση που τα τερματικά συστήματα επικοινωνούν απευθείας) μέχρι το μέγιστο αριθμό διακομιστών που υπάρχει στο δίκτυο.



Εικόνα 5*: Γενικευμένο μοντέλο [15]*

Μια πύλη μέσων (media gateway) λειτουργεί ως μονάδα μετάφρασης μεταξύ των διαφόρων τηλεπικοινωνιακών δικτύων, όπως τα PSTN, τα ασύρματα δίκτυα νέας γενιάς (2G, 3G και 4G) ή τα τ/φ κέντρα PBX. Οι πύλες μέσων, επίσης, ενεργοποιούν

τις επικοινωνίες πολυμέσων μέσω πολλαπλών πρωτοκόλλων μεταφοράς όπως τα ATM και IP. Οι πύλες αυτές, που συνήθως αναφέρονται επίσης και ως πύλες VoIP, είναι συσκευές που γεφυρώνουν τα συμβατικά τηλεφωνικά δίκτυα με τα τηλεφωνικά δίκτυα VoIP, καθώς φυσικά και τους αντίστοιχους εξοπλισμούς τους. Άλλη λειτουργία των πυλών VoIP είναι και η μετατροπή των φωνητικών σημάτων με πολυπλεξία διαίρεσης χρόνου (Time Division Multiplexing – TDM) σε πρωτόκολλο VoIP. Μια τυπική πύλη μέσων περιλαμβάνει τουλάχιστον μια θύρα σύνδεσης συμβατικού τηλεφώνου (RJ12) και τουλάχιστον μία θύρα Ethernet (RJ45) [16].

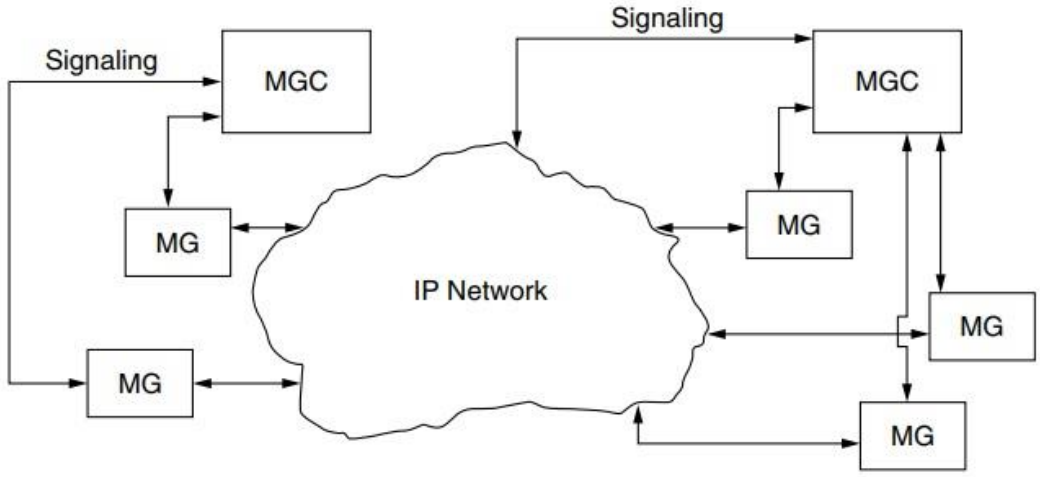
Από τη στιγμή που η πύλη μέσων συνδέει διαφορετικούς τύπους δικτύων, μία από τις κύριες λειτουργίες της είναι η δυνατότητα υποστήριξης όλων των διαφορετικών τεχνικών μετάδοσης και κωδικοποίησης. Οι λειτουργίες ροής πολυμέσων, όπως η ακύρωση ηχούς, η κωδικοποίηση DTMF (Dual Tone Multi Frequency) και η αποστολή τόνων, βρίσκονται επίσης στις πύλες VoIP.

Οι πύλες μέσων αποτελούν μέρος του φυσικού στρώματος μεταφοράς (physical transport layer) (Εικ. 4). Ρυθμίζονται από μια λειτουργία ελέγχου κλήσης που βρίσκεται στους ελεγκτές των πυλών μέσων (Media Gateway Controller – MGC). Μια πύλη μέσων, με τον αντίστοιχο ελεγκτή της, είναι απαραίτητος εξοπλισμός για την πραγματοποίηση της πακετοποίησης του φωνητικού σήματος. Ένας μεγάλος αριθμός των λειτουργιών των πυλών μέσων είναι οι εξής [16]:

- A/D μετατροπή του αναλογικού καναλιού φωνής (λειτουργία γνωστή και ως συμπίεση)
- Υποστήριξη διαφόρων ειδών δικτύων πρόσβασης, συμπεριλαμβανομένων των μέσων σύνδεσης όπως ο χαλκός, οι οπτικές ίνες, οι συχνότητες ασύρματης επικοινωνίας και το καλώδιο της καλωδιακής τηλεόρασης (CATV)
- Δυνατότητα χειρισμού πολλών πρωτοκόλλων διεπαφής φωνής και δεδομένων
- Παροχή διεπαφών μεταξύ των πυλών μέσων και των ελεγκτών τους. Κάτι τέτοιο απαιτεί την ικανότητα υποστήριξης ενός εκ των τεσσάρων πρωτοκόλλων SIP, H.323, MGCP και Megaco (H.248)
- Δυνατότητα χειρισμού των διεργασιών μεταγωγής και επεξεργασίας μέσων με βάση τα πρότυπα των δικτύων PCM, ATM και IP
- Μεταφορά φωνής, όπως τυπικό PCM, ATM, RTP/RTCP με βάση το IP και frame relay

Ο ελεγκτής πύλης ή ο ελεγκτής πύλης μέσων (MGC) πραγματοποιεί τη διαδικασία σηματοδοσίας στα κυκλώματα VoIP. Αυτή η λειτουργία απεικονίζεται στην εικόνα 6. Ένας ελεγκτής MGC μπορεί να ελέγξει πολλές πύλες, αλλά για τη βελτίωση της αξιοπιστίας και της διαθεσιμότητας του δικτύου, αρκετοί ελεγκτές MGC μπορούν να χρησιμοποιηθούν με λειτουργία αλληλεπικάλυψης των πυλών που ελέγχουν. Με τον τρόπο αυτό, εάν κάποιος αποτύχει να λειτουργήσει, μπορούν άλλοι να αναλάβουν τις λειτουργίες του. Με απλά λόγια, μετά την πραγματοποίηση μια

τηλεφωνικής σύνδεσης, η σύνδεση αυτή διατηρείται μέχρι την ολοκλήρωση της συνομιλίας των χρηστών [16].



***Εικόνα 6**: Ο ελεγκτής MGC παρέχει διεπαφή σηματοδότησης στις πύλες μέσων και επομένως σε ολόκληρο το IP δίκτυο [16]*

3 Κωδικοποιητές φωνής & Πρωτόκολλα VoIP

3.1 Κωδικοποιητές φωνής

Οι κωδικοποιητές φωνής είναι συσκευές ή προγράμματα κωδικοποίησης / αποκωδικοποίησης μιας ροής φωνητικών ψηφιακών δεδομένων ή ενός φωνητικού σήματος και είναι ευρέως γνωστοί με την ονομασία CODEC (Coder – DECoder) ή speech codec [17]. Στην αγορά κυκλοφορούν πολλά είδη codec. Παρόλα αυτά οι περισσότερες συσκευές VoIP χρησιμοποιούν τους codec οι οποίοι έχουν τυποποιηθεί από διεθνείς φορείς, όπως η Διεθνή Ένωση Τηλεπικοινωνιών (ITU), και είναι αποδεκτοί παγκοσμίως για λόγους διαλειτουργικότητας μεταξύ των διάφορων κατασκευαστών. Οι codec παρουσιάζουν διαφορετικές αποδόσεις και επιπτώσεις στην ποιότητα της φωνής ανάλογα με το βαθμό συμπίεσης που εφαρμόζουν. Υψηλός βαθμός συμπίεσης οδηγεί σε υψηλότερη καθυστέρηση συμπίεσης και αυξάνει την ευαισθησία απωλειών, σε σύγκριση με τους codec με χαμηλή ή μηδενική συμπίεση. Αντίθετα, οι codec με υψηλό βαθμό συμπίεσης έχουν μικρότερες απαιτήσεις εύρους ζώνης και επομένως παρουσιάζουν μεγαλύτερη απόδοση σε καταστάσεις συμφόρησης δικτύου.

Με βάση την αρχή λειτουργίας τους, οι codec μπορούν να ταξινομηθούν στις εξής τρεις κύριες κατηγορίες [18]:

- ***Codec κυματομορφής (waveform codecs)***: η αρχή λειτουργία τους βασίζεται στην τεχνική PCM. Δεν χρησιμοποιούν καθόλου την πηγή του σήματος και προσπαθούν να παράγουν ένα ψηφιακό σήμα, του οποίου η κυματομορφή να πλησιάζει όσο το δυνατόν περισσότερο σε αυτήν του αρχικού αναλογικού σήματος. Είναι εξαιρετικά απλοί και ικανοί να παρέχουν καλή ποιότητα ήχου ακόμα και σε χαμηλούς ρυθμούς κωδικοποίησης (γύρω στα 16 kbps), αλλά δύσκολα χρησιμοποιούνται για χαμηλότερες ταχύτητες. Σε αυτή τη κατηγορία ανήκει ο codec G.711
- ***Codec μοντελοποίησης (parametric ή voice coders - vocoders)***: η αρχή λειτουργίας τους βασίζεται στην μοντελοποίηση της ανθρώπινης ομιλίας. Η χρήση ενός βαθυπερατού φίλτρου δημιουργεί την αίσθηση μιας «συνθετικής» φωνής στην έξοδο του codec, γεγονός που οδηγεί σε χαμηλότερη ποιότητα, σε σύγκριση με τους codec κυματομορφής. Βασικό τους πλεονέκτημα είναι η επίτευξη πολύ χαμηλών ρυθμών κωδικοποίησης (της τάξης των 2,4 kbps)
- ***Υβριδικοί codec (hybrid codecs)***: συνδυάζουν τις δύο παραπάνω τεχνικές, επιτυγχάνοντας καλύτερη ποιότητα φωνής και μέτρια συμπίεση (της τάξης των 2 – 12 kbps). Σε αυτή την κατηγορία ανήκουν οι περισσότεροι σύγχρονοι codec, ανάμεσα στους οποίους συγκαταλέγεται και ο G.729

Επομένως, για τις εφαρμογές VoIP είναι απαραίτητη η επιλογή του κατάλληλου codec, ώστε να επιτευχθεί η καλύτερη ποιότητα φωνής με τις χαμηλότερες απαιτήσεις εύρους ζώνης [7]. Τρεις από τους πιο δημοφιλείς codec που χρησιμοποιούνται στην τηλεφωνία VoIP είναι οι G.711, G.723 και G.729.

3.1.1 G.711

Ο G.711 είναι ένας από τους πιο κοινούς και βασικούς codec που χρησιμοποιείται από μεγάλο αριθμό κατασκευαστών. Χρησιμοποιεί παλμοκωδική διαμόρφωση (PCM), μια τεχνική με την οποία επιτυγχάνεται ρυθμός κωδικοποίησης 64 kbps. Ο συγκεκριμένος codec συμπιέζει το πλάτος του φωνητικού σήματος με λογαριθμικό τρόπο. Στο άκρο του λήπτη, η διαδικασία αντιστρέφεται (αποσυμπίεση). Παρόλα αυτά η χρήση της λογαριθμικής καμπύλης για τιμές πλάτους κοντά στη μηδενική, αποτελεί μια ιδιαίτερα δύσκολη υπολογιστική διαδικασία. Για το λόγο αυτό, σε χαμηλές τιμές πλάτους του φωνητικού σήματος, ο G.711 έχει τη δυνατότητα να καλύπτει και τις δύο μεθόδους “A-law” και “μ-law” [18].

Η μέθοδος “A-law” αφορά τη χρήση μιας μίξης γραμμικής και λογαριθμικής συμπίεσης, ενώ η “μ-law” χρησιμοποιεί μια μετατοπισμένη λογαριθμική καμπύλη για τη συμπίεση αυτή. Οι μέθοδοι αυτές αποτελούν σύνθετα σχήματα κωδικοποίησης που καταφέρνουν να πραγματοποιήσουν μεγαλύτερη συμπίεση σήματος, χωρίς καμιά απώλεια κατά την αποσυμπίεση. Στην Βόρεια Αμερική και στην Ιαπωνία χρησιμοποιείται ως επί το πλείστον η μέθοδος “μ-law”, ενώ στην Ευρώπη και στον υπόλοιπο κόσμο η “A-law” [15].

Ο G.711 είναι ένας codec που απαιτεί χαμηλή πολυπλοκότητα υπολογισμών και προσφέρει πολύ καλή ποιότητα φωνής, με αμελητέα καθυστέρηση. Ωστόσο, η κατανάλωση των 64 kbps ανά κατεύθυνση είναι υψηλή σε σύγκριση με άλλους codec.

3.1.2 G.723

Υπάρχουν δύο τύποι codec G.723 που διατίθενται στην αγορά, ο ένας με ρυθμό κωδικοποίησης 5,3 kbps και ο άλλος με 6,3 kbps. Για το λόγο αυτό συμβολίζονται ως G.723r53 και G.723r63, αντίστοιχα. Ο υψηλότερος ρυθμός κωδικοποίησης αντιστοιχεί σε καλύτερη ποιότητα ήχου, ενώ ο χαμηλότερος ρυθμός παρέχει υποδεέστερη ποιότητα, αλλά μπορεί να υποστηριχθεί από μια αρχιτεκτονική συστήματος με μεγαλύτερη ευελιξία. Και οι δύο τύποι τρόποι μετάδοσης είναι ενσωματωμένοι στον codec. Στους συγκεκριμένους codec δίνεται η δυνατότητα μεταπήδησης σε διαφορετικό ρυθμό κωδικοποίησης κάθε 30 ms (frame boundary), καθώς επίσης και η δυνατότητα επιλογής λειτουργίας μεταβαλλόμενου ρυθμού κωδικοποίησης, με χρήση ασύγχρονης μετάδοσης και “γεμίσματος θορύβου” (noise fill) στον χρόνο που δεν υπάρχει μετάδοση ήχου [19].

Οι codec G.723 είναι ειδικά σχεδιασμένοι για τη μεταφορά σημάτων ήχου, στο φάσμα της ανθρώπινης ομιλίας, έχοντας ιδιαίτερα καλύτερη απόδοση σε χαμηλότερο ρυθμό κωδικοποίησης. Αντίθετα, οι συγκεκριμένοι codec δεν αποδίδουν σε

περιπτώσεις μεταφοράς μουσικών ήχων, κάτι που θα μπορούσε να βελτιωθεί με τη χρήση κατάλληλων αλγορίθμων.

3.1.3 G.729

Ο codec G.729 δειγματοληπτεί τη φιλτραρισμένη ζώνη φωνής στα 8 kHz με ανάλυση (resolution) των 16 bit και χρησιμοποιεί επιπλέον αλγόριθμο συμπίεσης για να παρέχει ρυθμό κωδικοποίησης των 8 kbps. Με τον τρόπο αυτό βελτιστοποιεί το εύρος ζώνης που χρησιμοποιείται για κάθε σύνδεση. Κανονικά απαιτεί υψηλή πολυπλοκότητα υπολογισμών, που εισάγει μια σχετικά χαμηλή καθυστέρηση. Ο G.729 μεταδίδεται με χρήση του πρωτοκόλλου πραγματικού χρόνου (RTP) μέσω των πρωτοκόλλων UDP και IP, ενώ το overhead που εισάγεται στην επικοινωνία VoIP μέσω της κεφαλίδας RTP/UDP/IP είναι αρκετά μεγάλο [15].

Ο ακόλουθος πίνακας 2 συνοψίζει τα χαρακτηριστικά των codec που αναφέρθηκαν.

Πίνακας 2: Σύνοψη των χαρακτηριστικών των codec που χρησιμοποιούνται στο VoIP [7]

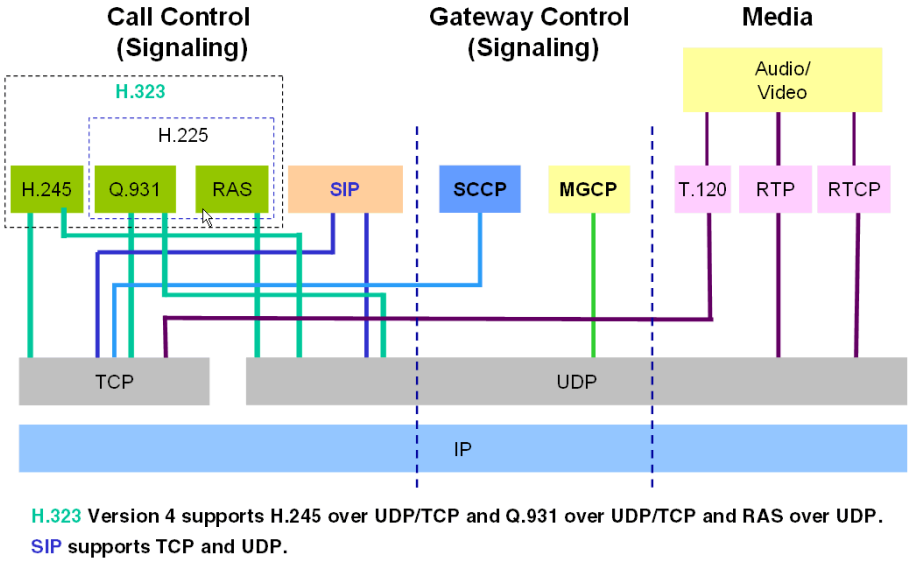
Πρότυπο Codec	Τεχνική συμπίεσης	Ρυθμός κωδικοποίησης (kbps)	Καθυστέρηση κωδικοποίησης (ms)	Ανοχή απωλειών (%)
G.711	Παλμοκωδική διαμόρφωση (PCM)	64 (χωρίς συμπίεση)	0,13 (ουσιαστικά αμελητέα)	7-10
G.723r53	Αλγεβρική κωδικοδιεγειρόμενη γραμμική πρόλεξη (Algebraic Code Excited Linear Prediction - ACELP)	5,3	περίπου 67,5	<1
G.723r63	Κβαντισμός πολλαπλών παλμών μέγιστης πιθανότητας (Multi Pulse Maximum Likelihood Quantization – MPMLQ)	6,3	περίπου 67,5	<1
G.729	Τεχνική CSACEIP (Conjugate Structure Algebraic Code-Excited Linear Prediction)	8	περίπου 25	<2

3.2 Πρωτόκολλα VoIP

Μετά την επεξεργασία του φωνητικού σήματος από τους codec, η κωδικοποιημένη φωνή που προκύπτει θα πρέπει να μεταφερθεί προς το άλλο άκρο της συνομιλίας. Για τη μεταφορά αυτών των δεδομένων απαιτείται η χρήση πρωτοκόλλων, γεγονός που αποδεικνύει ότι η ύπαρξη τους είναι εξίσου σημαντική με αυτήν των codec για την πραγματοποίηση μιας πλήρους επικοινωνίας.

Τα πρωτόκολλα είναι σύνολα κανόνων ή διαδικασιών που χρησιμοποιούνται και στα δύο άκρα επικοινωνίας σε ένα δίκτυο. Στην τηλεφωνία μέσω Διαδικτύου τα δεδομένα μεταδίδονται με τη μορφή datagram. Κάθε datagram περιέχει τη διεύθυνση

προέλευσης, τη διεύθυνση προορισμού και έναν αριθμό ακολουθίας. Επίσης ακολουθεί ανεξάρτητη διαδρομή εντός του δικτύου για να φτάσει στον προορισμό του. Στο άκρο λήψης, το σύνολο των datagram που φτάνουν, επανασυναρμολογούνται για να δημιουργηθεί το σύνολο των δεδομένων που απεστάλησαν από το άκρο εκπομπής. Το Διαδίκτυο έχει σχεδιαστεί με τέτοιο τρόπο ώστε να παρέχεται αξιοπιστία στην μεταφορά των datagram, χωρίς να λαμβάνονται υπόψη οι καθυστερήσεις. Οι μεταδόσεις των δεδομένων στο Διαδίκτυο περνούν, όπως έχει ήδη αναφερθεί, από πολλά στρώματα και στα δύο άκρα της επικοινωνίας. Το στρώμα δικτύου υποστηρίζει το πρωτόκολλο IP, το οποίο δημιουργεί τη σύνδεση μεταξύ δύο υπολογιστών. Το πρωτόκολλο IP είναι υπεύθυνο για τη δρομολόγηση δεδομένων μεταξύ οποιωνδήποτε δύο κόμβων, παρέχοντας παράλληλα έλεγχο για διαφθορά και απώλεια των δεδομένων αυτών. Το στρώμα μεταφοράς παρέχει τους κανόνες που απαιτούνται για την αποστολή των δεδομένων και το επίπεδο εφαρμογών καθορίζει τον τρόπο με τον οποίο θα γίνει η επεξεργασία των δεδομένων μόλις αυτά φτάσουν στον προορισμό τους.



Εικόνα 7: *Σύνοψη των πρωτοκόλλων του στρώματος εφαρμογών του VoIP [20]*

Τα περισσότερα δεδομένα που ταξιδεύουν μέσω Διαδικτύου, χρησιμοποιούν το πρωτόκολλο TCP στο στρώμα μεταφοράς, επειδή εγγυάται την παράδοση και την ακεραιότητα των δεδομένων. Το TCP υποστηρίζει επίσης την εκ νέου διαβίβαση των χαμένων δεδομένων καθώς και μηνύματα επιβεβαίωσης για την ορθή λήψη τους. Τα αιτήματα εκ νέου αποστολής των χαμένων δεδομένων δημιουργούν επιπρόσθετη καθυστέρηση, γεγονός που καθιστά το TCP ένα πρωτόκολλο που δεν ενδείκνυται σε περιπτώσεις σταθερής μετάδοσης δεδομένων. Από τη στιγμή που το VoIP δεν χρειάζεται κανενός είδους εγγύηση παράδοσης των δεδομένων, όπως αυτή που παρέχει το TCP, μπορεί να χρησιμοποιηθεί ως εναλλακτική και ταυτόχρονα ταχύτερη λύση, το πρωτόκολλο UDP. Το UDP δεν υποστηρίζει επαναμετάδοση των χαμένων δεδομένων, ούτε απαιτεί την αποστολή μηνυμάτων επιβεβαίωσης. Έτσι, το UDP λειτουργεί πιο αποτελεσματικά από το TCP σε δίκτυα IP συγκεκριμένου εύρους ζώνης, στα οποία παρατηρείται συχνά το φαινόμενο της συμφόρησης. Μόλις τα

δεδομένα VoIP φτάσουν στον προορισμό τους, υποβάλλονται σε κατάλληλη επεξεργασία στο στρώμα εφαρμογών για να μπορέσουν τελικά να φτάσουν στο λήπτη με την κατάλληλη μορφή.

Στο στρώμα εφαρμογών, το VoIP χρησιμοποιεί πρωτόκολλα σηματοδοσίας, (H.323, SIP και MGCP) για τη δημιουργία συνδέσεων μεταξύ των άκρων επικοινωνίας, και πρωτόκολλα μέσων, (RTP, RTCP και RTSP) για τη διαχείριση των δεδομένων πραγματικού χρόνου, όπως είναι τα δεδομένα ήχου ή βίντεο (Εικ. 7). Στη συνέχεια του κεφαλαίου θα αναλυθούν μόνο τα πρωτόκολλα που χρησιμοποιούνται στο στρώμα εφαρμογών.

3.3 Πρωτόκολλα σηματοδοσίας

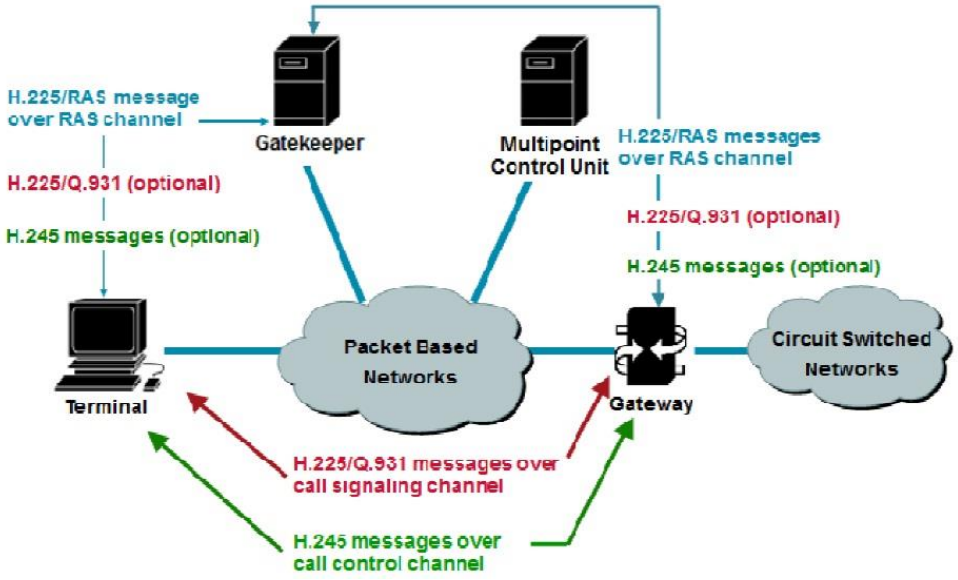
Στα συστήματα VoIP, η σηματοδοσία κλήσης χρησιμοποιείται με σκοπό τη δημιουργία συνδέσεων μεταξύ των τελικών σημείων ή μεταξύ ενός τελικού σημείου και μιας συσκευής ελέγχου κλήσης, που είναι γνωστή με την ονομασία gatekeeper. Μόλις ένας χρήστης δηλαδή, καλέσει έναν αριθμό τηλεφώνου, η σηματοδοσία θα προσδιορίσει την κατάσταση του καλούμενου (διαθέσιμος ή κατειλημμένος) για την πραγματοποίηση της κλήσης. Τα πρωτόκολλα σηματοδοσίας VoIP χωρίζονται σε δύο κατηγορίες [14]:

- ***Πρωτόκολλα ελέγχου συνόδου***: Τα πρωτόκολλα αυτά είναι υπεύθυνα για τη δημιουργία, τη διατήρηση και τη διακοπή των συνόδων κλήσεων. Είναι επίσης υπεύθυνα για τον καθορισμό των παραμέτρων της συνόδου (codec, ήχους κλήσεως, δυνατότητες εύρους ζώνης, κλπ.) Τα κύρια πρωτόκολλα ελέγχου συνόδου στο δίκτυο IP είναι τα H.323 και SIP
- ***Πρωτόκολλα ελέγχου μέσων***: Τα πρωτόκολλα αυτά είναι υπεύθυνα για τη δημιουργία και διακοπή των συνδέσεων των μέσων. Χρησιμοποιούνται για να ανοίγουν και να κλείνουν τα pinhole των μέσων στις πύλες VoIP και για να επεξεργάζονται τις ειδοποιήσεις που έρχονται από τις πύλες αυτές. Όπως έχει ήδη αναφερθεί, οι πύλες μέσων αποτελούν εξοπλισμό του VoIP, που λειτουργεί ως μέσο μεταφοράς μεταξύ των δικτύων IP και PSTN και ελέγχονται από τους ελεγκτές πυλών μέσων. Ο έλεγχος των μέσων που διέρχονται από τις πύλες αυτές γίνεται με χρήση του πρωτοκόλλου ελέγχου μέσων (Media Control Protocol – MCP). Τα δύο βασικά πρωτόκολλα ελέγχου μέσων που χρησιμοποιούνται στο VoIP είναι τα MGCP και Megaco (H.248).

3.3.1 H.323

Το πρωτόκολλο H.323 καθορίζει τον εξοπλισμό, τα πρωτόκολλα και τις διαδικασίες που παρέχουν υπηρεσίες επικοινωνίας πολυμέσων, όπως οι επικοινωνίες ήχου, βίντεο και δεδομένων σε πραγματικό χρόνο μέσω δικτύων μεταγωγής πακέτων, συμπεριλαμβανομένου του Διαδικτύου [14]. Το H.323 αποτελεί μέρος μιας οικογένειας που έχει συσταθεί από την ITU, την οικογένεια πρωτοκόλλων H.32x, που υποστηρίζει την επικοινωνία πολυμέσων μέσω διαφόρων δικτύων. Το H.323 μπορεί

να εφαρμοστεί σε ποικιλία εφαρμογών, όπως η καθαρά τηλεφωνική επικοινωνία (IP τηλεφωνία), η επικοινωνία ήχου και εικόνας (βίντεο τηλεφωνία), η επικοινωνία ήχου και δεδομένων καθώς και η επικοινωνία ήχου, βίντεο και δεδομένων. Μπορεί επίσης να εφαρμοστεί σε υπηρεσίες επικοινωνίας πολυσημειακών-πολυμέσων.



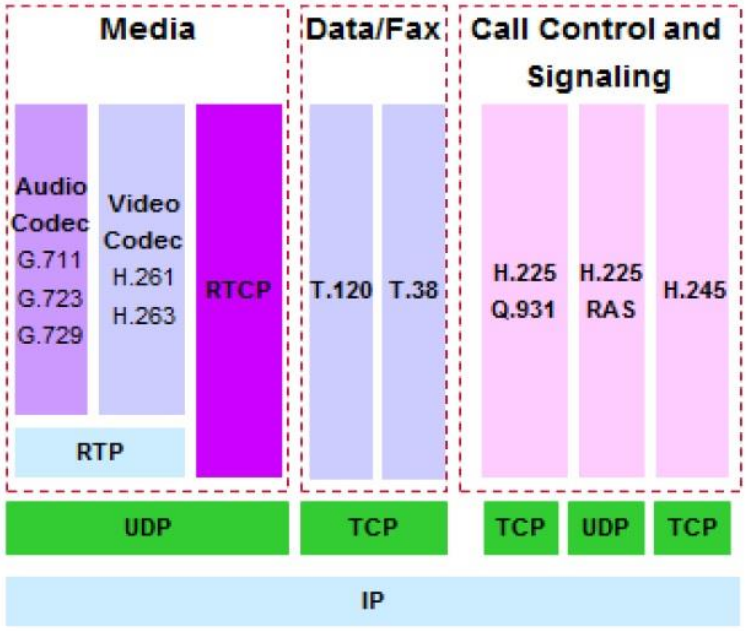
Εικόνα 8: *Εξοπλισμός H.323 και σηματοδοσία [15]*

I) Συστατικά μέρη H.323

Το πρότυπο H.323 αποτελείται από τα ακόλουθα συστατικά μέρη [21]:

- ***Τερματικά:*** Ένα τερματικό H.323 μπορεί να έχει αμφίδρομη επικοινωνία πραγματικού χρόνου με άλλο τερματικό H.323, πύλη, ή μονάδες MCU. Αυτή η επικοινωνία αποτελείται από διεργασίες ελέγχου, αποστολή μηνυμάτων ή μεταφορά ήχου, εικόνας, βίντεο ή / και απλών δεδομένων μεταξύ δύο τερματικών. Ένα τερματικό μπορεί να υποστηρίξει όλες τις εφαρμογές που υποστηρίζει το H.323, όπως καθαρά τηλεφωνική επικοινωνία, επικοινωνία ήχου και εικόνας, κλπ.
- ***Πύλες (Gateways – GW):*** Οι πύλες GW αποτελούν εξοπλισμό H.323 του δικτύου, που επιτρέπει την ενδοεπικοινωνία μεταξύ δικτύων IP και παλαιότερων δικτύων μεταγωγής κυκλωμάτων, όπως το ISDN και το PSTN. Παρέχουν, επίσης, τη χαρτογράφηση σηματοδοσίας καθώς και δυνατότητες αλλαγής κωδικοποίησης (transcoding)
- ***Gatekeeper (GK):*** Το gatekeeper (GK) είναι μια συσκευή H.323 του δικτύου που παίζει το ρόλο του κεντρικού διαχειριστή υπηρεσιών VoIP στα άκρα της επικοινωνίας. Ο συγκεκριμένος εξοπλισμός μεταφράζει τις διευθύνσεις IP και ελέγχει την πρόσβαση στο δίκτυο για H.323 τερματικά, GW και μονάδες MCU. Μπορεί επίσης να παρέχει και άλλες υπηρεσίες στις συσκευές αυτές, όπως διαχείριση του εύρους ζώνης και εντοπισμό των πυλών

- ***Μονάδες ελέγχου πολλαπλών σημείων (Multipoint Control Units – MCU):*** Οι μονάδες MCU είναι εξοπλισμός H.323 του δικτύου που παρέχει την ικανότητα σε τρία ή περισσότερα τερματικά και GW, να συμμετέχουν σε διασκέψεις πολλών σημείων. Μπορεί επίσης να συνδέσει δύο τερματικά σε διάσκεψη point-to-point, η οποία αργότερα μπορεί να εξελιχθεί σε διάσκεψη πολλαπλών σημείων. Μια μονάδα MCU αποτελείται από δύο μέρη, έναν υποχρεωτικό ελεγκτή πολλαπλών σημείων (Multipoint Controller - MC) και έναν προαιρετικό επεξεργαστή πολλαπλών σημείων (Multipoint Processor - MP). Στην απλούστερη περίπτωση, μια μονάδα MCU μπορεί να αποτελείται μόνο από ένα MC
- ***Ελεγκτές πολλαπλών σημείων (MC):*** Οι MC είναι συσκευές H.323 του δικτύου που ελέγχουν τρεις ή περισσότερους τερματικούς σταθμούς που συμμετέχουν σε διάσκεψη πολλαπλών σημείων. Μπορεί επίσης να συνδέσουν δύο τερματικά σε διάσκεψη point-to-point, η οποία αργότερα μπορεί να εξελιχθεί σε διάσκεψη πολλαπλών σημείων. Οι MC παρέχουν τη δυνατότητα διαπραγμάτευσης όλων των τερματικών σταθμών για την επίτευξη κοινού επιπέδου επικοινωνιών. Μπορούν επίσης να ελέγξουν τις πηγές της διάσκεψης, αλλά δεν πραγματοποιούν μίξεις ή μεταγωγές ήχου, βίντεο και δεδομένων
- ***Επεξεργαστές πολλαπλών σημείων (MP):*** Οι MP είναι εξοπλισμός H.323 του δικτύου που παρέχει την κεντρική επεξεργασία των ροών ήχου, βίντεο και / ή δεδομένων των διασκέψεων πολλαπλών σημείων. Παρέχουν τη δυνατότητα μιξαρίσματος, μεταγωγής ή άλλης επεξεργασίας των ροών των μέσων που ελέγχονται από τον MC. Οι MP μπορεί να επεξεργαστούν μια μεμονωμένη ροή μέσων ή πολλές ροές μέσων ανάλογα με τον τύπο της διάσκεψης



Εικόνα 9: *Στρώματα πρωτοκόλλων H.323 [15]*

ΙΙ) Πρωτόκολλα Η.323

Το Η.323 είναι ένα πρωτόκολλο που επιτρέπει τη επικοινωνία πολυμέσων σε πραγματικό χρόνο και εξαρτάται από διάφορα άλλα πρότυπα και πρωτόκολλα, κυριότερα από τα οποία είναι [16]:

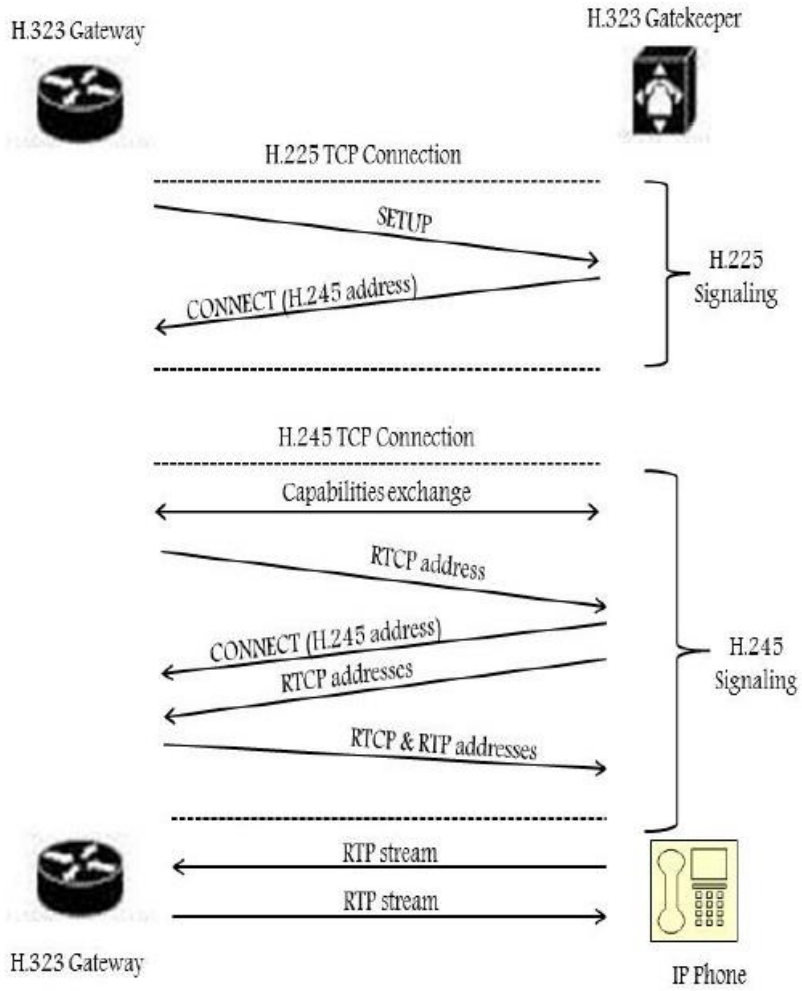
- ***Codec ήχου***: Οι codec ήχου κωδικοποιούν το ηχητικό σήμα του μικροφώνου που βρίσκεται στο Η.323 τερματικό μετάδοσης και αποκωδικοποιούν τον παραλαμβανόμενο κωδικοποιημένο ήχο που αποστέλλεται στο ηχείο του Η.323 τερματικού λήψης. Επειδή ο ήχος είναι η ελάχιστη υπηρεσία που παρέχεται από το πρότυπο Η.323, όλα τα Η.323 τερματικά θα πρέπει να διαθέτουν τουλάχιστον έναν codec ήχου, όπως ορίζεται στην σύσταση G.711 της ITU (κωδικοποίηση ήχου στα 64 kbps). Τα Η.323 τερματικά μπορούν επίσης να υποστηρίξουν και άλλες συστάσεις που αφορούν τα codec ήχου, όπως τις G.722 (κωδικοποίηση ήχου στα 64, 56 και 48 kbps), G.723.1 (κωδικοποίηση ήχου στα 5,3 και 6,3 kbps), G.728 (κωδικοποίηση ήχου στα 16 kbps) και G.729 (κωδικοποίηση ήχου στα 8 kbps)

- ***Codec βίντεο***: Οι codec βίντεο κωδικοποιούν το σήμα βίντεο της κάμερας που βρίσκεται στο Η.323 τερματικό μετάδοσης και αποκωδικοποιούν το παραλαμβανόμενο κωδικοποιημένο βίντεο που αποστέλλεται στην οθόνη του Η.323 τερματικού λήψης. Από τη στιγμή που η υποστήριξη του βίντεο για το Η.323 είναι προαιρετική, η υποστήριξη των codec βίντεο είναι επίσης προαιρετική. Ωστόσο, κάθε Η.323 τερματικό που παρέχει βίντεο επικοινωνίες θα πρέπει να υποστηρίζει την κωδικοποίηση και αποκωδικοποίηση βίντεο, όπως καθορίζεται στη σύσταση Η.261 της ITU

- ***Η.225 (Registration, Admission & Status – RAS):*** Πρόκειται για ένα πρωτόκολλο που χρησιμοποιείται μεταξύ των τελικών σημείων (τερματικών και πυλών) και των gatekeeper, για την πραγματοποίηση των διαδικασιών εγγραφής, ελέγχου εισόδου, αλλαγών του εύρους ζώνης, κατάστασης και αποσύνδεσης. Ένα κανάλι RAS ανταλλάσσει μηνύματα RAS. Αυτό το κανάλι σηματοδοσίας ανοίγει μεταξύ ενός τελικού σημείου και ενός gatekeeper, πριν από τη δημιουργία οποιωνδήποτε άλλων καναλιών επικοινωνίας

- ***Η.225 σηματοδοσία κλήσης:*** Δημιουργεί σύνδεση μεταξύ δύο τελικών σημείων Η.323. Αυτό επιτυγχάνεται με την ανταλλαγή μηνυμάτων πρωτοκόλλου Η.225 στο κανάλι σηματοδοσίας κλήσης. Το κανάλι αυτό ανοίγει μεταξύ δύο τελικών σημείων Η.323 ή μεταξύ ενός τελικού σημείου και του gatekeeper (Εικ. 10)

- ***Η.245 έλεγχος σηματοδοσίας***: Αυτά τα μηνύματα ελέγχου αποστέλλονται μεταξύ δύο τερματικών Η.232 και περιέχουν πληροφορίες σχετικές με την ανταλλαγή δυνατοτήτων και με το άνοιγμα και το κλείσιμο των λογικών καναλιών που χρησιμοποιούνται για τη μεταφορά των ροών μέσων. Επίσης, τα μηνύματα αυτά μπορεί να είναι μηνύματα ελέγχου ροής, γενικές εντολές ή απλές ενδείξεις της κατάστασης του καναλιού επικοινωνίας



Εικόνα 10: *Σενάριο κλήσης H.232 [14]*

3.3.2 SIP

Το πρωτόκολλο εκκίνησης συνόδου (Session Initiation Protocol – SIP) αναπτύχθηκε από την IETF ως απάντηση στη σύσταση H.323 της ITU. Η IETF πίστευε ότι το H.323 ήταν ανεπαρκές για την εξέλιξη της IP τηλεφωνίας, διότι η δομή εντολών του είναι πολύπλοκη και η αρχιτεκτονική του είναι κεντρικοποιημένη και μονολιθική [14]. Το SIP είναι ένα πρωτόκολλο ελέγχου του στρώματος εφαρμογών που μπορεί να δημιουργήσει, να τροποποιήσει και να τερματίσει συνόδους πολυμέσων ή κλήσεις [22].

Η αρχιτεκτονική του SIP είναι παρόμοια με αυτή του HTTP (πρωτόκολλο πελάτη-διακομιστή). Τα αιτήματα δημιουργούνται από τον πελάτη και αποστέλλονται στο διακομιστή. Ο διακομιστής επεξεργάζεται το εκάστοτε αίτημα και στη συνέχεια στέλνει μια απάντηση στον πελάτη. Το SIP έχει μηνύματα INVITE και ACK που καθορίζουν τη διαδικασία ανοίγματος ενός αξιόπιστου καναλιού, πάνω από το οποίο μπορούν να μεταφερθούν μηνύματα ελέγχου κλήσεων. Το SIP κάνει ελάχιστες υποθέσεις σχετικά με το υποκείμενο πρωτόκολλο μεταφοράς και παρέχει από μόνο του αξιοπιστία, χωρίς να εξαρτάται από την αξιοπιστία του TCP. Το SIP εξαρτάται από το πρωτόκολλο περιγραφής συνόδου (Session Description Protocol - SDP) για τη

διεξαγωγή διαπραγματεύσεων σχετικά με την αναγνώριση codec. Υποστηρίζει τις περιγραφές των συνόδων που δίνουν τη δυνατότητα στους συμμετέχοντες να συμφωνήσουν σε ένα σύνολο συμβατών τύπων μέσων. Υποστηρίζει επίσης την κινητικότητα των χρηστών μέσω χρήσης διακομιστή μεσολάβησης (proxy server) και ανακατεύθυνσης των αιτημάτων προς την τρέχουσα θέση του χρήστη. Οι υπηρεσίες που παρέχει το SIP περιλαμβάνουν [23]:

- ***Θέση χρήστη***: προσδιορισμός του τελικού συστήματος που θα χρησιμοποιηθεί για επικοινωνία
- ***Ρύθμιση κλήσης***: καθορισμός των παραμέτρων κλήσης και στα δύο άκρα της επικοινωνίας
- ***Διαθεσιμότητα χρηστών***: προσδιορισμός της προθυμίας του καλούμενου μέρους για επικοινωνία
- ***Δυνατότητες χρήστη***: προσδιορισμός των μέσων και των παραμέτρων τους που θα χρησιμοποιηθούν
- ***Διαχείριση κλήσεων***: μεταφορά και τερματισμός κλήσεων

Ι) Συστατικά μέρη πρωτοκόλλου SIP

Ένα σύστημα που χρησιμοποιεί SIP μπορεί να θεωρηθεί ότι αποτελείται από συστατικά μέρη που μπορούν να χωριστούν σε δύο μεγάλες ομάδες: το μοντέλο πελάτη/διακομιστή (client/server model) και τα μεμονωμένα στοιχεία δικτύου.

Το πρότυπο RFC3261 ορίζει τον πελάτη και τον διακομιστή ως εξής [22]:

- ***Πελάτης***: Ως πελάτης μπορεί να οριστεί οποιοδήποτε στοιχείο του δικτύου που στέλνει αιτήματα SIP και λαμβάνει απαντήσεις SIP. Οι πελάτες ενδέχεται να μην αλληλεπιδρούν άμεσα με τον χρήστη. Οι πελάτες και οι μεσολαβητές (proxy) των πρακτόρων χρηστών (user agent) είναι πελάτες
- ***Διακομιστής***: Ως διακομιστής δικτύου ορίζεται το στοιχείο που λαμβάνει αιτήματα για να εξυπηρετήσει και αποστέλλει απαντήσεις για τα αιτήματα αυτά. Παραδείγματα διακομιστών είναι οι διακομιστές μεσολάβησης, οι διακομιστές πρακτόρων χρηστών, οι διακομιστές ανακατεύθυνσης και οι καταχωρητές

Ως μεμονωμένα στοιχεία μιας τυπικής διαμόρφωσης SIP μπορούν να θεωρηθούν τα εξής [14]:

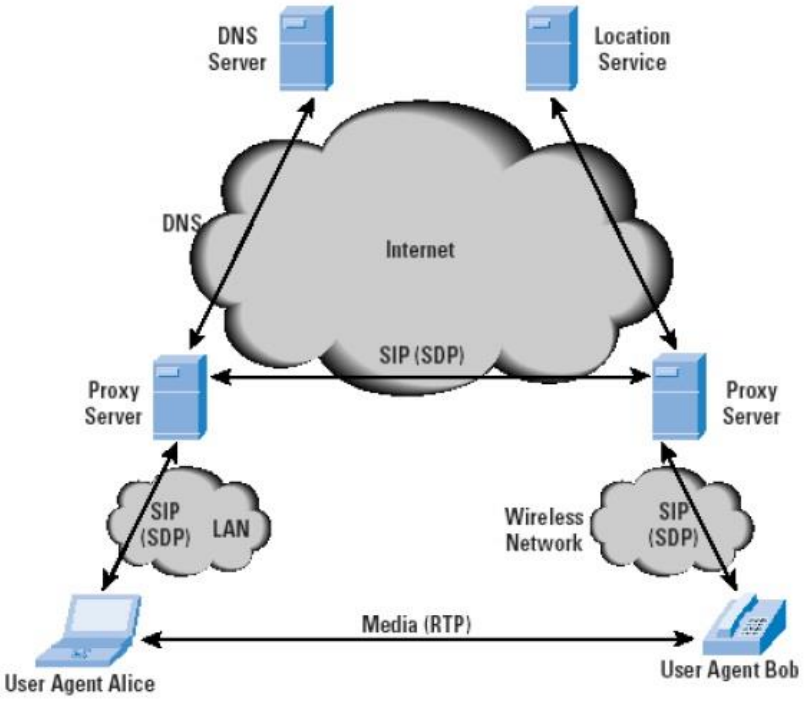
- ***Πράκτορες χρηστών***: Είναι εφαρμογές που αλληλεπιδρούν με τον χρήστη και περιέχουν πελάτες πρακτόρων χρηστών (User Agent Client - UAC) και διακομιστές πρακτόρων χρηστών (Server Agent Client - UAS). Ένας UAC εκκινεί αιτήματα SIP τα οποία λαμβάνει ένας UAS επιστρέφοντας απαντήσεις για λογαριασμό του χρήστη
- ***Καταχωρητής***: Είναι ένας διακομιστής SIP που δέχεται μόνο αιτήματα καταχώρησης, τα οποία έχουν εκδοθεί από τους πράκτορες χρηστών για την

ενημέρωση μιας βάσης δεδομένων τοποθεσίας και στα οποία αναφέρονται πληροφορίες επαφής του χρήστη που προσδιορίζεται στο αίτημα

- ***Διακομιστής μεσολάβησης***: Είναι μια ενδιάμεση οντότητα που ενεργεί τόσο ως διακομιστής για τους πράκτορες χρηστών μέσω διαβίβασης αιτημάτων SIP, όσο και ως πελάτης σε άλλους διακομιστές SIP, υποβάλλοντας τα αιτήματα που τους διαβιβάστηκαν εξ ονόματος των πρακτόρων χρηστών ή των διακομιστών μεσολάβησης

- ***Διακομιστής ανακατεύθυνσης***: Είναι ένας διακομιστής SIP που βοηθά στον εντοπισμό των πρακτόρων χρηστών παρέχοντας εναλλακτικές θέσεις, όπου ο χρήστης μπορεί να είναι προσβάσιμος, δηλαδή παρέχει υπηρεσίες χαρτογράφησης διευθύνσεων. Απαντά σε ένα αίτημα SIP που προορίζεται για μια διεύθυνση, με μια λίστα με νέες διευθύνσεις. Ένας διακομιστής ανακατεύθυνσης δεν δέχεται κλήσεις, δεν προωθεί αιτήματα και δεν εκκινεί τίποτα από μόνος του

- ***Υπηρεσία τοποθεσίας***: Η υπηρεσία αυτή χρησιμοποιείται από έναν διακομιστή ανακατεύθυνσης ή ένα διακομιστή μεσολάβησης SIP για την απόκτηση πληροφοριών σχετικά με την πιθανή τοποθεσία (-ες) ενός καλούντος. Για το σκοπό αυτό, η υπηρεσία τοποθεσίας διατηρεί μια βάση δεδομένων χαρτογράφησης των διευθύνσεων SIP και IP



Εικόνα 11: *Συστατικά μέρη και πρωτόκολλα SIP [15]*

Στην εικόνα 11 παρουσιάζονται κάποια από συστατικά μέρη του SIP και ο τρόπος με τον οποίο σχετίζονται μεταξύ τους, καθώς και τα πρωτόκολλα που χρησιμοποιούνται. Ένας πράκτορας χρήστη που ενεργεί ως πελάτης (στην προκειμένη περίπτωση ο UAC Alice), χρησιμοποιεί το SIP για να ρυθμίσει μια

σύνοδο με έναν πράκτορα χρήστη, που ενεργεί ως διακομιστής (στην περίπτωση αυτή ο UAS Bob). Ο διάλογος της εκκίνησης συνόδου χρησιμοποιεί SIP και περιλαμβάνει έναν ή περισσότερους διακομιστές μεσολάβησης για την προώθηση αιτημάτων και απαντήσεων μεταξύ των δύο πρακτόρων χρήστη. Οι πράκτορες χρήστη κάνουν επίσης χρήση του SDP, το οποίο χρησιμοποιείται για να περιγράψει τη σύνοδο των μέσων [11].

Οι διακομιστές μεσολάβησης μπορούν επίσης να ενεργήσουν και ως διακομιστές ανακατεύθυνσης, αν απαιτείται. Στην περίπτωση ανακατεύθυνσης, ο διακομιστής μεσολάβησης πρέπει να συμβουλευτεί τη βάση δεδομένων της υπηρεσίας τοποθεσίας, η οποία ενδέχεται και να μην είναι συνεγκατεστημένη με αυτόν. Η επικοινωνία μεταξύ του διακομιστή μεσολάβησης και της υπηρεσίας τοποθεσίας είναι πέρα από το πεδίο εφαρμογής του προτύπου SIP. Το Σύστημα Ονομάτων Τομέων (Domain Name System - DNS) είναι επίσης ένα σημαντικό μέρος της λειτουργίας του πρωτοκόλλου SIP. Συνήθως, ένας πράκτορας UAC κάνει ένα αίτημα χρησιμοποιώντας το όνομα τομέα του διακομιστή UAS, και όχι την IP διεύθυνσή του. Ο διακομιστής μεσολάβησης πρέπει να συμβουλευτεί έναν διακομιστή DNS, για να βρει τον διακομιστή μεσολάβησης του αντίστοιχου τομέα [11].

II) Πρωτόκολλα SIP

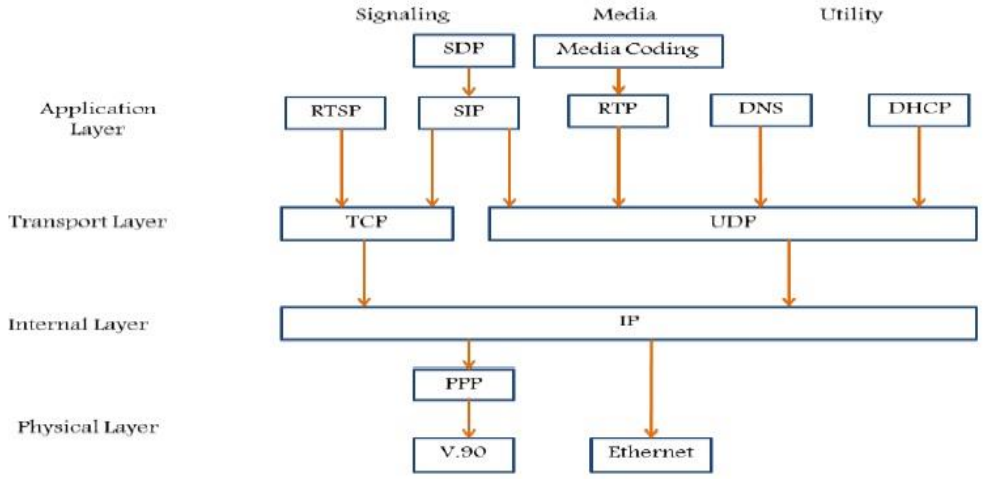
Αν και το SIP μπορεί να χρησιμοποιήσει το TCP, τις περισσότερες φορές τρέχει πάνω από το UDP για λόγους απόδοσης, παρέχοντας τους δικούς του μηχανισμούς αξιοπιστίας [14]. Αν είναι επιθυμητός ένας ασφαλής μηχανισμός μεταφοράς με κρυπτοκάλυψη, τα μηνύματα SIP μπορούν εναλλακτικά να μεταφερθούν μέσω του πρωτοκόλλου ασφάλειας στρώματος μεταφοράς (Transport Layer Security - TLS) [13].

Το πρωτόκολλο SIP είναι άρρηκτα συνδεδεμένο με το πρωτόκολλο SDP, που ορίζεται στο πρότυπο RFC 2327 [24]. Περιγράφει το περιεχόμενο των συνόδων, συμπεριλαμβανομένων των εφαρμογών πολυμέσων, της τηλεφωνίας και του ραδιοφώνου μέσω Διαδικτύου. Το πρωτόκολλο SDP περιλαμβάνει πληροφορίες σχετικά με [24]:

- ***Ροές μέσων***: Μια σύνοδος μπορεί να περιλαμβάνει πολλές ροές διαφορετικού περιεχομένου. Το SDP ορίζει τον ήχο, το βίντεο, τα δεδομένα, τον έλεγχο και την εφαρμογή ως τύπους ροών, παρόμοιοι με τους τύπους MIME που χρησιμοποιούνται στην αλληλογραφία μέσω Διαδικτύου
- ***Διευθύνσεις:*** Το SDP υποδεικνύει τις διευθύνσεις προορισμού των ροών μέσων. Οι διευθύνσεις αυτές μπορεί να είναι και διευθύνσεις πολυδιανομής (multicast)
- ***Θύρες:*** Για κάθε ροή, καθορίζονται οι αριθμοί θύρας UDP για αποστολή και λήψη

- ***Τύποι ωφέλιμου φορτίου:*** Για κάθε τύπο ροής μέσων που χρησιμοποιείται (για παράδειγμα, τηλεφωνία), ο τύπος ωφέλιμου φορτίου (payload) υποδεικνύει τις μορφές μέσων που μπορούν να χρησιμοποιηθούν κατά τη διάρκεια της περιόδου συνόδου
- ***Χρόνοι έναρξης και λήξης:*** Οι χρόνοι αυτοί εφαρμόζονται στις συνόδους εκπομπής broadcast, για παράδειγμα, τηλεοπτικό ή ραδιοφωνικό πρόγραμμα. Σε τέτοιες περιπτώσεις υποδεικνύονται οι ώρες έναρξης, διακοπής και επανάληψης της συνόδου
- ***Προέλευση εκπομπής (Originator):*** Στην περίπτωση εκπομπών broadcast, δίνονται πληροφορίες επαφής που καθορίζουν τον originator. Κάτι τέτοιο μπορεί να είναι χρήσιμο εάν ένας δέκτης αντιμετωπίσει τεχνικές δυσκολίες

Παρόλο που το SDP διαθέτει τη δυνατότητα περιγραφής του περιεχομένου πολυμέσων, του λείπουν οι μηχανισμοί με τους οποίους δύο μέρη θα συμφωνήσουν σχετικά με τις παραμέτρους που θα χρησιμοποιηθούν. Το πρότυπο RFC 3264 αποκαθιστά αυτήν την έλλειψη, καθορίζοντας ένα απλό μοντέλο προσφοράς / απάντησης, με το οποίο δύο μέρη ανταλλάσσουν μηνύματα SDP, για να επιτευχθεί συμφωνία σχετικά με τη φύση του προς μετάδοση περιεχομένου πολυμέσων [22]. Μετά την ανταλλαγή και την αναγνώριση ορθότητας των πληροφοριών αυτών, όλοι οι συμμετέχοντες γνωρίζουν τις διευθύνσεις IP όλων των συμμετεχόντων, τη διαθέσιμη χωρητικότητα μετάδοσης και τον τύπο του μέσου. Στη συνέχεια, η μετάδοση δεδομένων αρχίζει, χρησιμοποιώντας ένα κατάλληλο πρωτόκολλο μεταφοράς. Συνήθως χρησιμοποιείται το RTP. Κατά τη διάρκεια της συνόδου, οι συμμετέχοντες μπορούν να κάνουν αλλαγές στις παραμέτρους της, που μπορεί να αφορούν τους τύπους νέων μέσων ή τη συμμετοχή στη σύνοδο νέων μερών. Οι αλλαγές αυτές υποδεικνύονται μέσω αποστολής μηνυμάτων SIP.



Εικόνα 12: *Πρωτόκολλα SIP [14]*

3.3.3 Σύγκριση μεταξύ H.323 και SIP

Κατά την εξέλιξη του VoIP, έχει υπάρξει μεγάλη αντιπαράθεση σχετικά με την ανωτερότητα των πρωτοκόλλων H.323 και SIP στη σηματοδοσία της IP τηλεφωνίας. Επί του παρόντος δεν υπάρχει σαφής νικητής, αλλά ούτε κι έχει προκύψει κάποιο άλλο πρωτόκολλο που να μπορεί να αμφισβητήσει την θέση αυτών των δύο.

Οι κύριες διαφορές των δύο πρωτοκόλλων είναι οι εξής [11, 23]:

- ***Πολυπλοκότητα:*** Όσον αφορά την πολυπλοκότητα, το H.323 φαίνεται να είναι το πιο πολύπλοκο από τα δύο πρωτόκολλα. Το H.323 ορίζει εκατοντάδες στοιχεία, ενώ το SIP έχει μόνο 37 κεφαλίδες μικρού αριθμού τιμών και παραμέτρων. Το H.323 χρησιμοποιεί μια δυαδική αναπαράσταση των μηνυμάτων του με βάση την γλώσσα αφηρημένης περιγραφής δεδομένων (Abstract Syntax Notation 1 - ASN.1) και τους κανόνες κωδικοποίησης PER (Packed Encoding Rules). Η γλώσσα ASN.1 γενικά απαιτεί την ανάλυση ειδικών γεννητριών κώδικα. Αντίθετα, το SIP χρησιμοποιεί απλή μορφή εντολών και μηνυμάτων και μορφή κειμένου παρόμοια με HTTP και RTSP. Αυτές οι συμβολοσειρές κειμένου είναι εύκολο να αποκωδικοποιηθούν και, ως εκ τούτου, ο εντοπισμός σφαλμάτων (debugging) γίνεται πολύ πιο εύκολα. Επίσης, το σύνολο των μηνυμάτων του SIP είναι πολύ μικρότερο του H.323. Άλλο πλεονέκτημα του SIP είναι ότι χρησιμοποιεί ένα μόνο αίτημα που περιέχει όλες τις απαραίτητες πληροφορίες, ενώ πολλές από τις υπηρεσίες H.323 απαιτούν αλληλεπίδραση μεταξύ των συστατικών μερών που περιλαμβάνονται στο πρότυπο
- ***Συμβατότητα:*** Το H323 είναι ένα αυστηρό πρωτόκολλο όσον αφορά τη συμβατότητα. Απαιτεί πλήρως προς τα πίσω συμβατότητα, γεγονός που σημαίνει ότι η όποια μεταγενέστερη έκδοση του H323 πρέπει να είναι συμβατή με την προηγούμενη. Σε ένα σύστημα H323, μια πύλη της Cisco πρέπει να συνεργάζεται με ένα τερματικό που παράγεται από την Lucent λόγω τυποποίησης των εφαρμογών. Αντίθετα, το SIP είναι ένα ανοιχτό πρωτόκολλο και εύκολο να επεκταθεί. Δεν απαιτεί πλήρως προς τα πίσω συμβατότητα, δηλαδή η όποια μεταγενέστερη έκδοση δεν χρειάζεται να υποστηρίζει όλες τις δυνατότητες των προηγούμενων εκδόσεων. Οι συσκευές SIP μπορούν να γίνουν εύκολα συμβατές με συστήματα άλλων κατασκευαστών, με απλή ανταλλαγή πληροφοριών σχετικά με τις δυνατότητές τους, όπως οι μέθοδοι κωδικοποίησης ή τα μηνύματα που χρησιμοποιούν. Μετά την ανταλλαγή αυτών των πληροφοριών, οι δύο συσκευές μπορούν να συνεργαστούν μόνο στην κοινή δυνατότητά τους
- ***Επεκτασιμότητα:*** Το χαρακτηριστικό της επεκτασιμότητας είναι σημαντικό καθώς η χρήση του Διαδικτύου και των υπηρεσιών του, τείνουν να αυξάνονται συνεχώς. Όσον αφορά την επεκτασιμότητα, τα δύο πρωτόκολλα διαφέρουν σε δύο βασικά σημεία:

1. ***Μεγάλοι αριθμοί τομέων:*** Καθώς το H.323 προοριζόταν αρχικά να χρησιμοποιηθεί σε ένα μόνο LAN, παρουσιάζει κάποια προβλήματα επεκτασιμότητας, παρά το γεγονός ότι οι νεότερες εκδόσεις ορίζουν την έννοια των ζωνών και τις διαδικασίες εύρεσης της θέσης του χρήστη σε αυτές (μέσω του ονόματος του ηλεκτρονικού ταχυδρομείου). Το H.323 δεν παρέχει εύκολο τρόπο πραγματοποίησης ανίχνευσης βρόχου σε περιπτώσεις σύνθετης αναζήτησης σε πολλούς τομείς, καθώς η διαδικασία αυτή μπορεί να γίνει μόνο stateful με αποθήκευση των μηνυμάτων, διαδικασία που δεν είναι όμως επεκτάσιμη. Το SIP, ωστόσο, χρησιμοποιεί μια μέθοδο ανίχνευσης βρόχου, ελέγχοντας το ιστορικό του μηνύματος μέσω των πεδίων κεφαλίδας, τα οποία μπορούν να εκτελεστούν με τρόπο stateless

2. ***Επεξεργασία διακομιστή:*** Μια συναλλαγή SIP μέσω διαφόρων διακομιστών και πυλών μπορεί να είναι stateful ή stateless. Αυτό σημαίνει ότι οι μεγάλοι, backbone διακομιστές που χειρίζονται μεγάλη κυκλοφορία μπορεί να είναι stateless για να μειωθούν οι απαιτήσεις μνήμης. Το στοιχείο αυτό μπορεί να συνδυαστεί με την ικανότητα χρήσης του UDP, καθώς το UDP δεν απαιτεί κάποια συγκεκριμένη κατάσταση σύνδεσης. Το H.323, από την άλλη, απαιτεί οι gatekeeper να είναι stateful. Επιπλέον, οι συνδέσεις στο H.323 βασίζονται στο TCP, πράγμα που σημαίνει ότι ο gatekeeper θα πρέπει να διατηρεί τις συνδέσεις του κατά τη διάρκεια μιας κλήσης.

- ***Κινητικότητα:*** Η υπηρεσία της προσωπικής κινητικότητας υποστηρίζεται και από τα δύο πρωτόκολλα, αλλά η υποστήριξη του H.323 είναι πιο περιορισμένη. Το SIP μπορεί, χρησιμοποιώντας οποιαδήποτε αυθαίρετη διεύθυνση URL, να ανακατευθύνει ή να μεσολαβήσει οποιοδήποτε εισερχόμενο αίτημα σε διάφορες τοποθεσίες. Σε κάθε τοποθεσία μπορούν να μεταφερθούν διάφορες πληροφορίες που αφορούν τον καλούντα, όπως η γλώσσα που ομιλείται, το αν η κλήση γίνεται από κινητό ή σταθερό τηλέφωνο, από το σπίτι ή από επιχείρηση κλπ. Το SIP υποστηρίζει επίσης «αναζητήσεις» πολλών αλμάτων για έναν χρήστη. Αυτό σημαίνει ότι οι διακομιστές μπορούν να μεσολαβούν για ένα αίτημα σε έναν ή περισσότερους πρόσθετους διακομιστές σε αναζήτηση του καλούντος. Ένας διακομιστής SIP μπορεί επίσης να μεσολαβεί για ένα αίτημα σε πολλούς διακομιστές παράλληλα, μια διαδικασία γνωστή και ως forking proxy, γεγονός που καθιστά την αναζήτηση πιο γρήγορη. Αντίθετα το H.323 μπορεί απλά να ανακατευθύνει έναν καλούντα για να δοκιμάσει διάφορες άλλες διευθύνσεις. Εδώ, οι προτιμήσεις κλήσεων είναι σταθερές και δεν είναι δυνατόν να αλλάξουν. Το H.323 δεν σχεδιάστηκε για λειτουργία ευρείας περιοχής, δεν μπορεί να υποστηρίξει μεταβίβαση κλήσης και, όπως προαναφέρθηκε προηγούμενα, δεν έχει μηχανισμό ανίχνευσης βρόχου. Τέλος, το H.323 δεν επιτρέπει σε έναν gatekeeper να μεσολαβήσει για ένα αίτημα σε πολλούς διακομιστές

- ***Υπηρεσίες:*** Τα δύο πρωτόκολλα δεν παρέχουν τις ίδιες υπηρεσίες. Εκτός από τις υπηρεσίες ελέγχου κλήσεων, τόσο το SIP όσο και το H.323 παρέχουν υπηρεσίες ανταλλαγής δυνατοτήτων. Από την άποψη αυτή, το H.323 παρέχει ένα πολύ πιο πλούσιο ρεπερτόριο λειτουργιών. Τα τερματικά μπορούν να εκφράσουν την ικανότητά τους να εκτελούν διάφορες κωδικοποιήσεις και αποκωδικοποιήσεις που βασίζονται στις παραμέτρους του codec και στο σύνολο των codec που χρησιμοποιούνται. Αντίθετα, το SIP χρησιμοποιεί μόνο την ένδειξη των βασικών δυνατοτήτων του δέκτη. Αυτό σημαίνει ότι το SIP στέλνει μια λίστα με τις κωδικοποιήσεις που υποστηρίζονται και η καλούμενη πλευρά θα πρέπει να επιλέξει οποιοδήποτε υποσύνολο αυτών

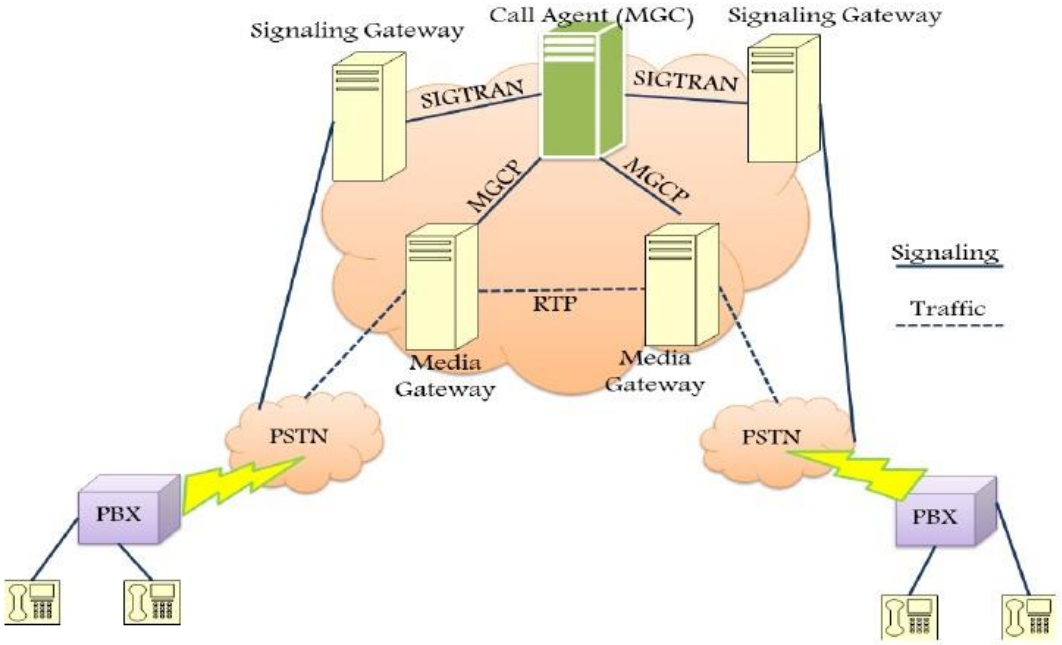
Στον πίνακα 3 αναφέρονται συγκεντρωτικά, οι κύριες διαφορές μεταξύ των H.323 και SIP, που αναφέρθηκαν παραπάνω.

ΠΙΝΑΚΑΣ 3: Σύγκριση των πρωτοκόλλων H.323 και SIP

Χαρακτηριστικό	H.323	SIP
Πολυπλοκότητα	Αρκετά μεγάλη	Συγκριτικά μικρότερη
Κωδικοποίηση	Δυαδική κωδικοποίηση ASN.1 PSN	Κωδικοποίηση βάσει κειμένου UTF-8
Επεκτασιμότητα	Περιορισμένη	Εύκολη, μη περιορισμένη
Συμβατότητα	Απαιτείται πλήρως προς τα πίσω συμβατότητα	Δεν απαιτείται πλήρως προς τα πίσω συμβατότητα
Κλιμακωσιμότητα	Λιγότερο κλιμακούμενο (state full, TCP)	Περισσότερο κλιμακούμενο (stateless, UDP)
Πρωτόκολλο μεταφοράς	Μόνο TCP	TCP, UDP ή άλλα
Δυνατότητα συνεδρίας	Απαιτείται MCU	Με χρήση IP multicast
Υπηρεσίες	Παροχή λειτουργικών δυνατοτήτων πλούσιας γκάμας	Απλή γκάμα λειτουργικών δυνατοτήτων
Ανίχνευση βρόγχων	Δύσκολη (state full)	Συγκριτικά εύκολη (stateless)
Διευθυνσιοδότηση	Πιο ευέλικτη (E.164 scheme, H.323 ID alias, κλπ)	SIP URL
Κινητικότητα	Πιο περιορισμένη (δεν υποστηρίζει forking proxy)	Πιο ευέλικτη και ταχεία (υποστηρίζει forking proxy)
Έλεγχος συνεδρίας	Υποστηρίζεται	Δεν υποστηρίζεται

3.3.4 MGCP

Το πρωτόκολλο ελέγχου πύλης μέσων (Media Gateway Control Protocol – MGCP) χρησιμοποιείται για την επικοινωνία μεταξύ των ξεχωριστών στοιχείων μιας αποσυνδεθείσας πύλης VoIP και αποτελεί συμπληρωματικό πρωτόκολλο των SIP και H.323. Εντός του MGCP, ο ελεγκτής MGC, ή πιο γνωστός ως πράκτορας κλήσης (Call Agent – CA), είναι υποχρεωτικός, καθώς. Η πύλη MG (Media Gateway) αγνοεί τις κλήσεις / συνόδους και δεν διατηρεί τις καταστάσεις κλήσης. Αντίθετα, εκτελει εντολές που αποστέλλονται από τους πράκτορες CA. Το πρωτόκολλο MGCP υποθέτει ότι οι πράκτορες CA συγχρονίζονται μεταξύ τους στέλνοντας συνεκτικές εντολές στις πύλες MG υπό τον έλεγχό τους. Το MGCP δεν διαθέτει μηχανισμό για τον συγχρονισμό των πρακτόρων CA. Οι πύλες MG λειτουργούν ως slave και ο ελεγκτής MGC λειτουργεί ως master, συνθέτοντας έτσι ένα master / slave πρωτόκολλο [14].



Εικόνα 13: *Αρχιτεκτονική MGCP [14]*

3.3.5 Megaco/H.248

Το Megaco/H.248 είναι ένα πρωτόκολλο ελέγχου κλήσεων που επικοινωνεί μεταξύ ενός ελεγκτή πύλης και μιας πύλης. Εξέλιξε και αντικατέστησε το απλό πρωτόκολλο ελέγχου πύλης (Simple Gateway Control Protocol - SGCP) και το MGCP. Το Megaco αντιμετωπίζει τη σχέση μεταξύ μιας πύλης MG και ενός ελεγκτή MGC. Τόσο το Megaco όσο και το MGCP είναι πρωτόκολλα χαμηλού επιπέδου, που καθοδηγούν τις πύλες MG στη σύνδεση των ροών, που προέρχονται εκτός των δικτύων κυψέλης (στην περίπτωση ασύρματου VoIP) ή των δικτύων πακέτων δεδομένων, σε μια ροή πακέτων ή κυψελών που διέπεται από το πρωτόκολλο RTP [25].

3.3.6 Σύγκριση μεταξύ MGCP και Megaco/H.248

Το Megaco/H.248 προσφέρει τις ακόλουθες βασικές βελτιώσεις σε σχέση με το MGCP [15]:

- Υποστηρίζει υπηρεσίες πολυμέσων και διασκέψεις πολλαπλών σημείων
- Παρέχει βελτιωμένη σύνταξη για πιο αποτελεσματική επεξεργασία σημασιολογικών μηνυμάτων
- Παρέχει επιλογές μεταφοράς TCP και UDP
- Επιτρέπει κωδικοποίηση κειμένου ή δυαδικών ψηφίων και διαμορφωμένη διαδικασία επέκτασης για βελτιωμένη λειτουργικότητα

Το Megaco/H.248 έχει την ίδια αρχιτεκτονική με το MGCP (Εικ. 13). Οι εντολές είναι παρόμοιες, αλλά η κύρια διαφορά είναι ότι οι εντολές H.248 ισχύουν για τερματισμούς σε σχέση με ένα πλαίσιο αντί για μεμονωμένες συνδέσεις, όπως συμβαίνει στο MGCP. Οι συνδέσεις επιτυγχάνονται με την τοποθέτηση δύο ή περισσότερων τερματισμών σε ένα κοινό πλαίσιο. Αυτή η έννοια του πλαισίου είναι που διευκολύνει την υποστήριξη των κλήσεων πολυμέσων και διασκέψεων. Το πλαίσιο μπορεί να θεωρηθεί ως μια γέφυρα ανάμιξης, που υποστηρίζει πολλαπλές ροές μέσων για βελτιωμένες υπηρεσίες πολυμέσων.

Στον πίνακα 4 συνοψίζονται οι βασικές διαφορές των πρωτοκόλλων MGCP και Megaco/H.248

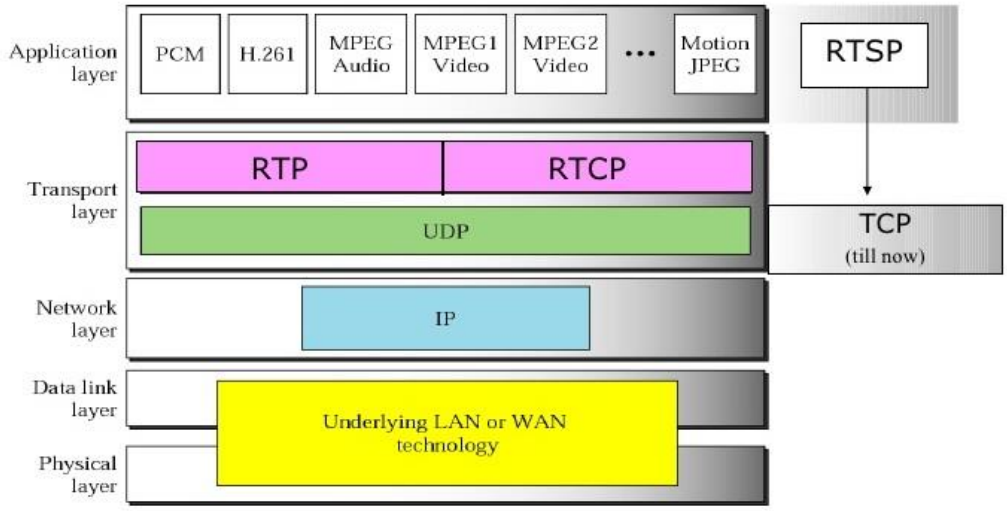
ΠΙΝΑΚΑΣ 4: Βασικές διαφορές πρωτοκόλλων MGCP και Megaco/H.248 [15]

MGCP	Megaco /H.248
Μια κλήση αναπαριστάται ως άκρα μεμονωμένων συνδέσεων	Μια κλήση αναπαριστάται ως τερματισμοί εντός ενός πλαισίου κλήσης
Οι τύποι κλήσεων είναι σημείου με σημείο και πολυσημειακές	Οι τύποι κλήσεων περιλαμβάνουν οποιοδήποτε συνδυασμό πολυμέσων και συνεδριάσεων
Σύνταξη κειμένου	Σύνταξη δυαδικού κειμένου
Στρώμα μεταφοράς UDP	Στρώμα μεταφοράς TCP ή UDP
Ορισμένο από τη Cisco και σε κυκλοφορία από την IETF	Ορισμένο από τις IETF και ITU

3.4 Πρωτόκολλα πραγματικού χρόνου

Μέσω του Διαδικτύου μεταφέρονται πολλά είδη δεδομένων, καθένα από τα οποία έχει διαφορετικά χαρακτηριστικά και απαιτήσεις. Για παράδειγμα, μια εφαρμογή μεταφοράς αρχείων απαιτεί τη μεταφορά ενός ποσοστού δεδομένων εντός κάποιου αποδεκτού χρονικού διαστήματος, ενώ στην περίπτωση της τηλεφωνίας μέσω Διαδικτύου, τα περισσότερα πακέτα θα πρέπει να φτάσουν στο δέκτη σε λιγότερο από

0,3 δευτερόλεπτα. Αν το εύρος ζώνης του δικτύου είναι ικανοποιητικό, τότε η εκάστοτε υπηρεσία θα καταβάλει κάθε δυνατή προσπάθεια για να πληροί όλες αυτές τις απαιτήσεις. Αν όμως οι πόροι δεν επαρκούν, οι υπηρεσίες πραγματικού χρόνου θα αντιμετωπίσουν πολλά προβλήματα, λόγω της εμφάνισης συμφόρησης [26].



Εικόνα 14: *Στρώμα πρωτοκόλλων για υπηρεσίες πολυμέσων [27]*

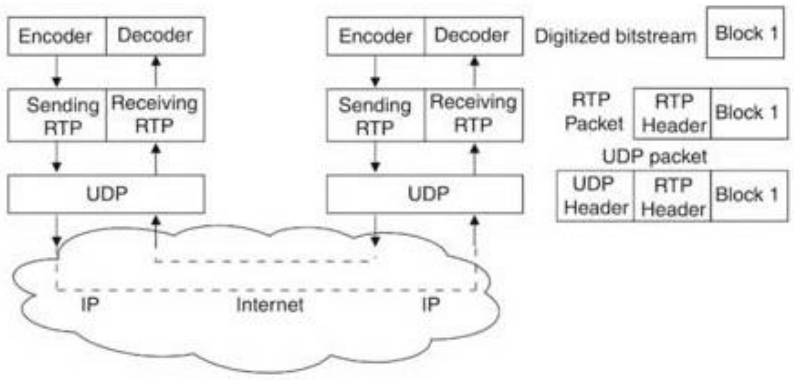
Λύση για τη μεταφορά πολυμέσων μέσω του Διαδικτύου αποτελεί η ταξινόμηση της κίνησης του δικτύου, η απονομή προτεραιοτήτων σε διαφορετικές εφαρμογές και η πραγματοποίηση κρατήσεων. Η ομάδα εργασίας ολοκληρωμένων υπηρεσιών του IETF (Internet Engineering Task Force) ανέπτυξε το πρότυπο RFC 1633, ένα βελτιωμένο μοντέλο υπηρεσιών του Διαδικτύου, που ονομάζεται Ολοκληρωμένες Υπηρεσίες (Integrated Services), και περιλαμβάνει υπηρεσίες πραγματικού χρόνου [28]. Οι υπηρεσίες πραγματικού χρόνου δίνουν τη δυνατότητα στα δίκτυα IP να παρέχουν ποιότητα υπηρεσιών (QoS) στις εφαρμογές πολυμέσων. Οι υπηρεσίες αυτές βασίζονται στα εξής πρωτόκολλα:

- Πρωτόκολλο μεταφοράς σε πραγματικό χρόνο (Real-time Transport Protocol - RTP)
- Πρωτόκολλα ελέγχου σε πραγματικό χρόνο (Real-Time Control Protocol – RTCP)
- Πρωτόκολλο ροής σε πραγματικό χρόνο (Real-Time Streaming Protocol - RTSP)

Οι ολοκληρωμένες υπηρεσίες επιτρέπουν σε εφαρμογές να διαμορφώνουν και να διαχειρίζονται μια ενιαία υποδομή για εφαρμογές πολυμέσων και παραδοσιακών εφαρμογών. Το μοντέλο αυτό αποτελεί μια ολοκληρωμένη προσέγγιση παροχής εφαρμογών, με το είδος των υπηρεσιών που απαιτείται και με την ποιότητα που επιλέγεται.

3.4.1 Πρωτόκολλο RTP

Το πρωτόκολλο RTP είναι το πρωτόκολλο IP που μεταδίδει δεδομένα ήχου και βίντεο σε πραγματικό χρόνο. Το RTP δεν εγγυάται την παράδοση των δεδομένων αυτών σε πραγματικό χρόνο, αλλά παρέχει μηχανισμούς για την αποστολή και τη λήψη εφαρμογών υποστήριξης των δεδομένων ροής. Στην εικόνα 15 παρουσιάζεται ένα σχηματικό διάγραμμα της λειτουργίας του πρωτοκόλλου.



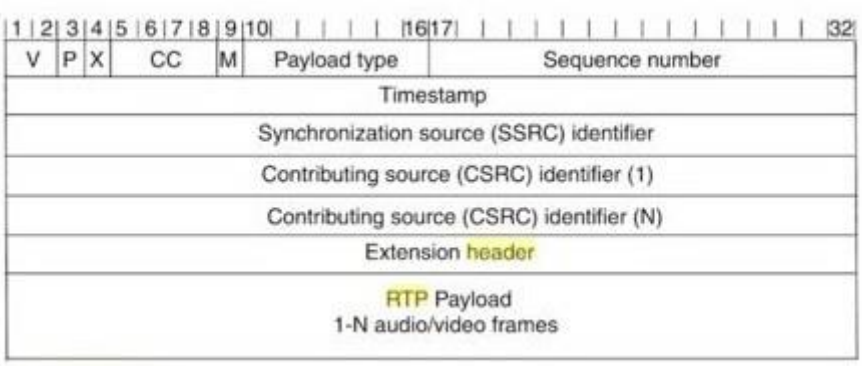
Εικόνα 15: *Το πρωτόκολλο RTP [29]*

Στην περίπτωση του VoIP, το RTP τρέχει πάνω από το πρωτόκολλο UDP, που χρησιμοποιείται ως στρώμα μεταφοράς και απλά παρέχει μια άμεση μέθοδο αποστολής και λήψης δεδομένων σε ένα δίκτυο IP, χωρίς όμως έλεγχο ανάκτησης σφαλμάτων. Έτσι, δεν μπορεί να ενημερώσει την εκάστοτε εφαρμογή για τυχόν απώλειες δεδομένων κατά την παράδοση των πακέτων, ενώ παράλληλα στέλνει τα δεδομένα με τυχαία σειρά, χωρίς καμία εγγύηση παράδοσης. Κάθε αναδιάταξη των δεδομένων στη σωστή μορφή, όπως ήταν δηλαδή κατά την αποστολή, γίνεται από το RTP.

Κατά τη μετάδοση των ροών δεδομένων, το πρωτόκολλο πρέπει να χειριστεί κάποιες ανεπιθύμητες, αλλά πολύ πιθανόν εμφανιζόμενες συνθήκες:

- Το δίκτυο μπορεί να αποσυνδέσει τα πακέτα
- Μερικά πακέτα μπορεί να χαθούν
- Μπορεί να υπάρξει εμφάνιση jitter (διακύμανση του χρόνου μεταξύ των αφίξεων των πακέτων).

Από τα τρία αυτά ζητήματα, το RTP στοχεύει στην επίλυση μόνο δύο, την ανακολουθία των πακέτων και το jitter (χρησιμοποιώντας αριθμούς ακολουθίας και χρονικές σημάνσεις). Στην περίπτωση απώλειας πακέτων, το πρωτόκολλο προτιμά το "πραγματικό-απρόσμενο" από την αξιοπιστία. Εάν κάποια πακέτα χαθούν, χάθηκαν, αφού είναι πιο σημαντική η μετάδοση της ροής σε πραγματικό χρόνο. Αυτός είναι και ο λόγος για τον οποίο το RTP τρέχει πάνω από UDP, αφού το TCP δεν είναι κατάλληλο για πρωτόκολλα πραγματικού χρόνου, λόγω του χαρακτηριστικού της αναμετάδοσης που το χαρακτηρίζει.



Εικόνα 16: *Κεφαλίδα πακέτου RTP [29]*

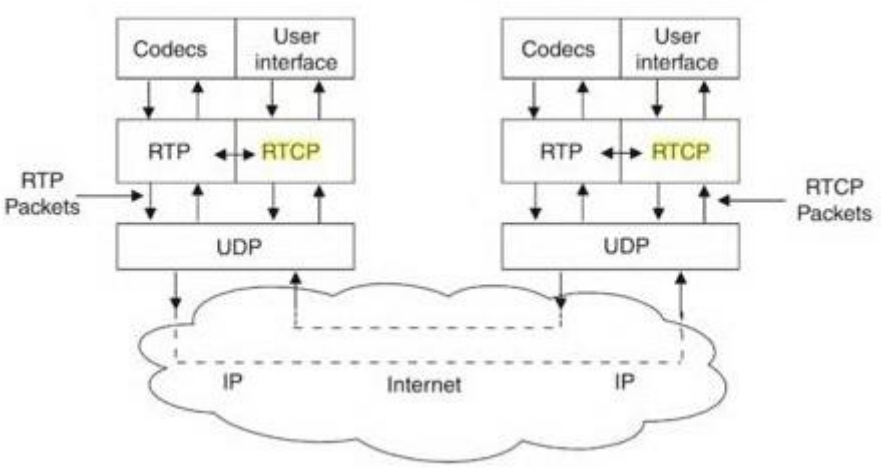
Στην εικόνα 16 παρουσιάζεται μια απλοποιημένη μορφή της κεφαλίδας των πακέτων RTP. Τα πιο σημαντικά από τα πεδία της είναι τα εξής [29]:

- ***Τύπος ωφέλιμου φορτίου (Payload type – PT):*** Αφορά τον τύπο των δεδομένων που μεταφέρονται στο πακέτο. Το πεδίο PT είναι των 7 bit, επομένως παίρνει τιμές μεταξύ 0 και 127. Κάθε στατική τιμή αντιπροσωπεύει και ανάλογο τύπο δεδομένων, για παράδειγμα το "0" αντιπροσωπεύει το G.711 μ-Law, το "8" αντιπροσωπεύει το G.711 A-Law και το "18" το G.729. Το διάστημα μεταξύ των τιμών 96 και 127 προορίζεται για δυναμικούς τύπους ωφέλιμου φορτίου. Για τους τύπους αυτούς θα πρέπει να γίνεται διαπραγμάτευση από το εκάστοτε πρωτόκολλο σηματοδοσίας, που χρησιμοποιείται για τον καθορισμό της κλήσης VoIP (π.χ. SIP ή H.323)
- ***Αριθμός ακολουθίας (Sequence number):*** Ο αριθμός αυτός (16 bit) ξεκινά από μια τυχαία τιμή και αυξάνεται με την αποστολή κάθε πακέτου RTP. Με τον τρόπο αυτό δίνεται η δυνατότητα εντοπισμού των πακέτων που δεν λήφθηκαν με τη σειρά
- ***Χρονική σήμανση (Timestamp):*** Όμοια με τον αριθμό ακολουθίας, η τιμή της χρονική σήμανση ξεκινάει από τυχαίο αριθμό (32 bit). Η συχνότητα του ρολογιού εξαρτάται από τον τύπο του ωφέλιμου φορτίου. Η συχνότητα αυτή είναι 8 kHz (ηχητικό σήμα στενής ζώνης) και η χρονική σήμανση είναι η μέτρηση των τμημάτων κατά τη δειγματοληψία του πρώτου ηχητικού δείγματος του ωφέλιμου φορτίου
- ***Πηγή συγχρονισμού (Synchronization Source - SSRC):*** Η τιμή του πεδίου αυτού (32 bit) επιλέγεται τυχαία, με την πρόθεση δύο πηγές συγχρονισμού εντός της ίδιας συνόδου RTP να μην έχουν το ίδιο αναγνωριστικό SSRC. Στην περίπτωση που μια ροή δημιουργείται από τη μίξη πολλών διαφορετικών ροών, τα αναγνωριστικά των πηγών που συμμετέχουν, μπορούν να αναγράφονται στα πεδία CSRC, ενώ το πεδίο CC (4 bit) δίνει τον αριθμό των συμβαλλόντων πηγών. Ωστόσο, στην πράξη, αυτό δεν χρησιμοποιείται πολύ

Στην πιο τυπική κατάσταση (δεν υπάρχουν πεδία CSRC, ούτε κάποια επέκταση επικεφαλίδας), η κεφαλίδα του RTP αποτελείται από 12 byte. Στο VoIP, τα πακέτα φωνής εισάγονται σε πακέτα δεδομένων χρησιμοποιώντας RTP, τα οποία με τη σειρά τους εισάγονται μέσα σε πακέτα UDP.

3.4.2 Πρωτόκολλο RTCP

Το RTCP, σε συνδυασμό με το RTP, χρησιμοποιείται για τη μετάδοση πληροφοριών ελέγχου της συνόδου RTP. Τα πακέτα RTCP αποστέλλονται μόνο κατά διαστήματα, δεδομένου ότι υπάρχει σύσταση ότι η κίνηση RTCP θα πρέπει να καταναλώνει λιγότερο από το 5% του εύρους ζώνης της συνόδου [29]. Η σχέση του πρωτοκόλλου με τα υπόλοιπα στρώματα παρουσιάζεται στην Εικ. 17.



Εικόνα 17: *Το πρωτόκολλο RTCP [29]*

Οι πιο σημαντικοί τύποι περιεχομένου που μεταφέρονται στα πακέτα RTCP, περιλαμβάνουν πληροφορίες για τους συμμετέχοντες στην κλήση (για παράδειγμα, όνομα και διεύθυνση ηλεκτρονικού ταχυδρομείου) και στατιστικά στοιχεία σχετικά με την ποιότητα της μετάδοσης (για παράδειγμα χρόνος του jitter και ο αριθμός των χαμένων πακέτων). Η αναφορά που αποστέλλεται από έναν συμμετέχοντα που αποστέλλει και λαμβάνει δεδομένα, ονομάζεται αναφορά αποστολέα (Sender Report - SR), ενώ οι αναφορές που αποστέλλονται από συμμετέχοντες που απλά λαμβάνουν μόνο ροές RTP ονομάζονται αναφορές παραλήπτη (Receiver Report - RR) [29].

Το RTCP εκτελεί τέσσερις λειτουργίες [30]:

- Παρέχει ανατροφοδότηση σχετικά με την ποιότητα της κατανομής των δεδομένων. Αυτό αποτελεί αναπόσπαστο μέρος του ρόλου του RTP ως πρωτόκολλο μεταφοράς και σχετίζεται με τις λειτουργίες ελέγχου ροής και συμφόρησης άλλων πρωτοκόλλων μεταφοράς
- Φέρει ένα σταθερό αναγνωριστικό επιπέδου μεταφοράς για μια πηγή RTP, γνωστό με την ονομασία κανονικό όνομα (Canonical NAME – CNAME). Δεδομένου ότι το αναγνωριστικό SSRC μπορεί να μεταβληθεί σε περίπτωση που διαπιστωθεί κάποια διένεξη ή επανεκκίνηση ενός προγράμματος, οι

δέκτες απαιτούν το CNAME για να παρακολουθούν κάθε συμμετέχοντα. Οι δέκτες ενδέχεται επίσης να απαιτούν το CNAME για τη συσχέτιση πολλαπλών ροών δεδομένων, από ένα δεδομένο συμμετέχοντα σε ένα σύνολο σχετικών RTP συνόδων, για παράδειγμα να συγχρονίσουν ένα βίντεο με τον ήχο

- Οι πρώτες δύο λειτουργίες απαιτούν από όλους τους συμμετέχοντες να στέλνουν πακέτα RTCP, επομένως ο ρυθμός πρέπει να ελέγχεται ώστε το RTP να μπορεί να αυξήσει τον αριθμό των συμμετεχόντων. Από τη στιγμή που κάθε συμμετέχοντας στέλνει πακέτα ελέγχου σε όλους τους άλλους, ο καθένας μπορεί ανεξάρτητα να παρατηρήσει τον αριθμό των συμμετεχόντων. Αυτός ο αριθμός χρησιμοποιείται για τον υπολογισμό του ρυθμού με τον οποίο αποστέλλονται τα πακέτα

- Μια προαιρετική λειτουργία είναι η μεταβίβαση ελάχιστων πληροφοριών ελέγχου συνόδου, για παράδειγμα το αναγνωριστικό των συμμετεχόντων που θα εμφανίζεται στη διεπαφή του χρήστη. Αυτή η λειτουργία είναι πιθανόν να είναι χρήσιμη σε "χαλαρά ελεγχόμενες" συνόδους όπου οι συμμετέχοντες εισέρχονται και εξέρχονται χωρίς έλεγχο αυθεντικοποίησης μέλους ή διαπραγμάτευση παραμέτρων

Οι πρώτες τρεις λειτουργίες θα πρέπει να χρησιμοποιούνται σε όλα τα περιβάλλοντα, αλλά κυρίως σε περιβάλλον IP multicast. Οι σχεδιαστές εφαρμογών RTP θα πρέπει να αποφεύγουν μηχανισμούς που να μπορούν να λειτουργήσουν μόνο σε λειτουργία unicast και δεν μπορούν να κλιμακωθούν. Η μετάδοση του RTCP μπορεί να ελέγχεται ξεχωριστά για αποστολείς και δέκτες, σε περιπτώσεις όπως οι μονοκατευθυντικές ζεύξεις, όπου η ανάδραση από τους δέκτες δεν είναι δυνατή.

3.4.3 Πρωτόκολλο RTSP

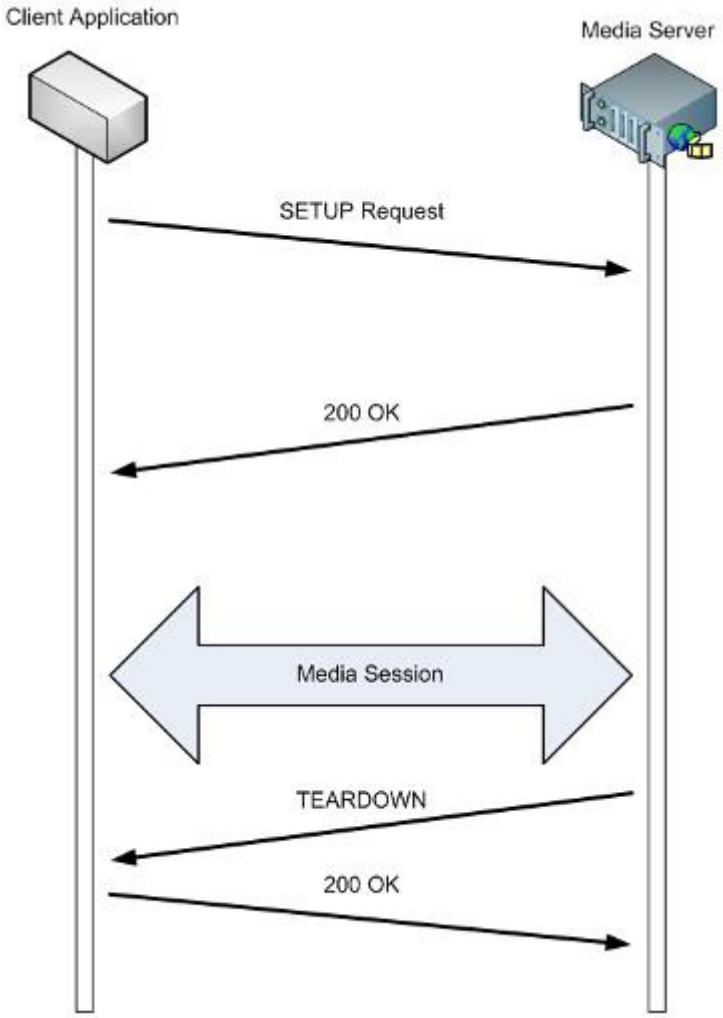
Το RTSP ορίζεται από το πρότυπο RFC2326 και αποτελεί ένα πρωτόκολλο πελάτη-διακομιστή που παρέχει έλεγχο της παράδοσης των ροών πολυμέσων σε πραγματικό χρόνο. Ο έλεγχος αυτός περιλαμβάνει απομακρυσμένες λειτουργίες όπως παύση, γρήγορη κίνηση προς τα εμπρός ή προς τα πίσω και επιλογή σημείου, λειτουργίες που μοιάζουν με αυτές ενός DVD player [29]. Παρέχει τα μέσα επιλογής διαύλων παράδοσης (όπως UDP, multicast UDP και TCP) και μηχανισμούς παράδοσης με βάση το RTP. Το RTSP δημιουργεί και ελέγχει συνεχόμενες ροές μέσων ήχου και βίντεο μεταξύ των διακομιστών μέσων και των πελατών. Ένας διακομιστής μέσων παρέχει υπηρεσίες αναπαραγωγής ή εγγραφής των ροών αυτών, ενώ ένας πελάτης ζητά τη συνεχόμενη ροή των δεδομένων από το διακομιστή μέσων. Βάσει των λειτουργιών του, που αναφέρθηκαν παραπάνω, το RTSP λειτουργεί ως "τηλεχειριστήριο δικτύου" μεταξύ του διακομιστή και του πελάτη [30].

Το πρωτόκολλο υποστηρίζει τις ακόλουθες λειτουργίες [30]:

- ***Ανάκτηση μέσων από το διακομιστή μέσων:*** Ο πελάτης μπορεί να αιτηθεί μιας περιγραφής της παρουσίασης και να ζητήσει από τον διακομιστή να

δημιουργήσει μια σύνοδο για να στείλει τα ζητούμενα δεδομένα. Ο διακομιστής μπορεί είτε να προβεί σε multicast παρουσίαση είτε να την στείλει στον πελάτη χρησιμοποιώντας unicast

- ***Πρόσκληση ενός διακομιστή μέσων σε μια διάσκεψη:*** Ο διακομιστής μέσων μπορεί να προσκληθεί σε διάσκεψη για την αναπαραγωγή μέσων ή την καταγραφή μιας παρουσίασης
- ***Προσθήκη μέσων σε υπάρχουσα παρουσίαση:*** Ο διακομιστής ή ο πελάτης μπορούν να ενημερώνονται αμοιβαία για τυχόν πρόσθετα μέσα που έχουν καταστεί διαθέσιμα



Εικόνα 18: *Σύνοδος RTSP ανάμεσα σε έναν πελάτη κι ένα διακομιστή μέσων [31]*

Με βάση το πρότυπο RFC 2326, τα σημαντικότερα χαρακτηριστικά του RTSP είναι τα εξής [32]:

- Αποτελεί πρωτόκολλο επιπέδου εφαρμογής με σύνταξη και λειτουργίες που μοιάζουν με του HTTP, αλλά λειτουργεί για ήχο και βίντεο
- Χρησιμοποιεί διευθύνσεις URL όπως αυτές στο HTTP

- Ένας διακομιστής RTSP πρέπει να διατηρεί καταστάσεις, χρησιμοποιώντας μεθόδους όπως οι SETUP και TEARDOWN (Εικ. 18)
- Σε αντίθεση με το HTTP, στο RTSP τόσο οι διακομιστές όσο και οι πελάτες μπορούν να εκδώσουν αιτήματα
- Εφαρμόζεται σε πολλές πλατφόρμες λειτουργικών συστημάτων και επιτρέπει διαλειτουργικότητα μεταξύ πελατών και διακομιστών από διαφορετικούς κατασκευαστές

4 Ποιότητα υπηρεσιών VoIP

4.1 Θέματα ποιότητας QoS

Κατά τη δημιουργία της τεχνολογίας VoIP, τα θέματα ποιότητας υπηρεσίας (QoS) δεν λήφθηκαν υπόψη και αυτό επειδή η τεχνολογία IP παραμένει αναποτελεσματική στην υποστήριξη της κυκλοφορίας δεδομένων, με τους αυστηρούς περιορισμούς της ποιότητας QoS, πόσο μάλλον όταν αυτά τα δεδομένα αφορούν φωνή και βίντεο [33]. Έτσι, ανάμεσα στα μειονεκτήματα της τεχνολογίας VoIP, που αναφέρθηκαν στο εισαγωγικό κεφάλαιο της παρούσας εργασίας, οι ανησυχίες σχετικά με την ποιότητα QoS ίσως να μπορούν να θεωρηθούν ως οι πιο σοβαρές.

Λόγω της φύσης της τεχνολογίας VoIP, τα πακέτα δεδομένων που αποστέλλονται μέσω δικτύου IP αντιμετωπίζουν διάφορα θέματα μετάδοσης, όπως η καθυστέρηση (delay), η διακύμανση καθυστέρησης (jitter), η απώλεια πακέτων δεδομένων και η ακύρωση ηχούς (echo cancellation) [34]. Η αντιμετώπιση των προβλημάτων μετάδοσης, και επομένως η δυνατότητα της τεχνολογίας VoIP να υποστηρίξει αναδυόμενες εφαρμογές πολυμέσων με αυστηρούς περιορισμούς QoS, απαιτεί την ανάπτυξη κατάλληλων μηχανισμών QoS.

Η μεταφορά δεδομένων φωνής είναι πολύ ευαίσθητη σε θέματα καθυστέρησης και απώλειας πακέτων, αλλά και σε άλλα είδη καθυστέρησης μεταβλητής μορφής. Τα αποτελέσματα αυτών των προβλημάτων εμφανίζονται με τη μορφή αστάθειας ήχου, απώλειας ήχου, ηχούς ή απαράδεκτα μεγάλων παύσεων κατά τη συνομιλία, που προκαλούν επικαλύψεις φωνής των δύο συνομιλητών [34, 35]. Για το λόγο αυτό, η ποιότητα QoS θεωρείται ίσως ως το πιο σημαντικό χαρακτηριστικό ανάπτυξης ενός επιτυχημένου συστήματος VoIP.

Ως ποιότητα QoS ορίζεται η ικανότητα του δικτύου να παρέχει καλύτερες ή "ειδικές" υπηρεσίες σε επιλεγμένους χρήστες και εφαρμογές, εις βάρος άλλων χρηστών και εφαρμογών [36]. Η ανάπτυξη ενός συστήματος με ποιότητα QoS δίνει εγγυήσεις εύρους ζώνης, ελαχιστοποιώντας την καθυστέρηση και το jitter στις περιπτώσεις μεταφοράς δεδομένων προτεραιότητας, όπως είναι τα δεδομένα φωνής. Οι εγγυήσεις αυτές δίνονται όχι με δημιουργία πρόσθετου εύρους ζώνης, αλλά με τον έλεγχο του τρόπου με τον οποίο το διαθέσιμο εύρος ζώνης χρησιμοποιείται από τις διάφορες εφαρμογές και τα πρωτόκολλα στο δίκτυο. Στην πραγματικότητα, αυτό συχνά σημαίνει ότι οι εφαρμογές δεδομένων και τα πρωτόκολλα δεν έχουν πρόσβαση στο εύρος ζώνης, όταν αυτό είναι αναγκαίο για τη μεταφορά δεδομένων VoIP. Μια τέτοια άρνηση πρόσβασης στο εύρος ζώνης δεν έχει μεγάλες επιπτώσεις στη μεταφορά δεδομένων του δικτύου, από τη στιγμή που γενικά οι καθυστερήσεις ή οι απώλειες πακέτων δεν επηρεάζουν τόσο πολύ άλλες εφαρμογές όσο τις εφαρμογές VoIP.

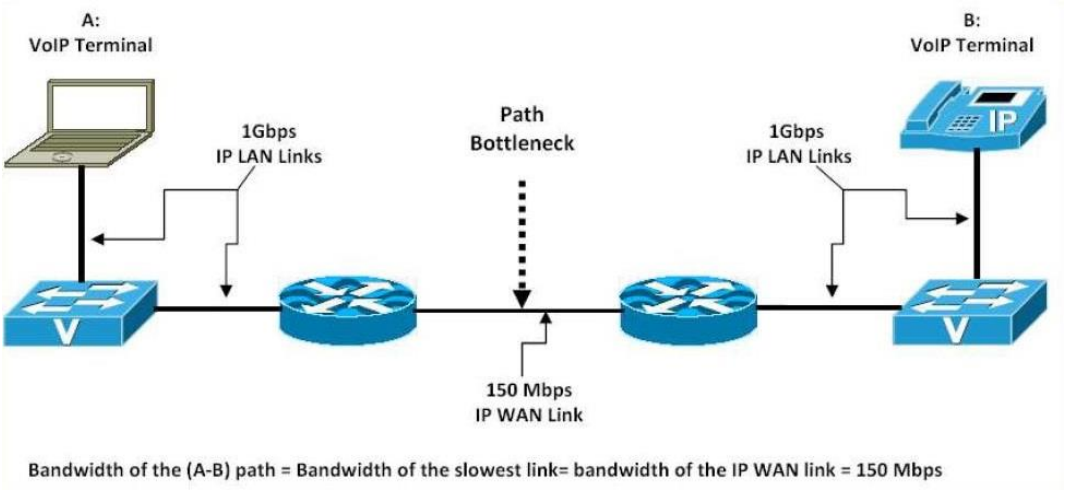
Τα κύρια θέματα που πρέπει να αντιμετωπιστούν σε ένα δίκτυο VoIP με ποιότητα QoS και η ικανοποιητική μετάδοση του ήχου μέσω του δικτύου IP είναι τα εξής [36]:

- το εύρος ζώνης
- η καθυστέρηση του δικτύου
- η διακύμανση της καθυστέρησης, και
- η απώλεια πακέτων

Τα ζητήματα αυτά θα αναλυθούν στις επόμενες ενότητες του κεφαλαίου με παράλληλη παρουσίαση τρόπων αντιμετώπισής τους για την παροχή της απαιτούμενης ποιότητας QoS σε ένα δίκτυο VoIP.

4.2 Εύρος ζώνης

Το εύρος ζώνης ενός μέσου μετάδοσης (οπτική ίνα, ομοαξονικό καλώδιο, κ.λπ.) ορίζει τη χωρητικότητα μετάδοσης δεδομένων σε bit ανά δευτερόλεπτο. Το εύρος ζώνης μιας διαδρομής δικτύου που αποτελείται από διαφορετικούς τύπους ζεύξεων (LAN και WAN) αντιστοιχεί στο εύρος ζώνης της βραδύτερης ζεύξης της διαδρομής (δηλαδή στη ζεύξη με το μικρότερο εύρος ζώνης, με άλλα λόγια στο σημείο συμφόρησης (bottleneck) του δικτύου). Τα bottleneck προκαλούν συμφόρηση στην κυκλοφορία των δεδομένων εντός του δικτύου, γεγονός που έχει ως αποτέλεσμα προβλήματα στην ποιότητα QoS για στις περιπτώσεις που η μεταφορά αντιστοιχεί σε δεδομένα ήχου. Στην εικόνα 19, παρουσιάζεται ένα παράδειγμα στο οποίο φαίνεται η διαδρομή δικτύου μεταξύ δύο τερματικών VoIP σε ένα δίκτυο IP. Στο παράδειγμα αυτό σημειώνεται η πιθανότερη θέση εμφάνισης bottleneck, καθώς επίσης και ο υπολογισμός του εύρους ζώνης της διαδρομής που αντιστοιχεί στο εύρος ζώνης της βραδύτερης ζεύξης στο θεωρούμενο μονοπάτι (δηλαδή της ασύρματης ζεύξης) [33].



Εικόνα 19: *Σημείο συμφόρησης (bottleneck) δικτύου [33]*

Για την ικανοποιητική μεταφορά των δεδομένων ήχου μέσω ενός δικτύου IP, και ως εκ τούτου την ενίσχυση της ανάπτυξης ενός επιτυχημένου συστήματος VoIP, το ζήτημα της συμφόρησης θα πρέπει να αποφεύγεται. Ως τρόποι αντιμετώπισης του ζητήματος της συμφόρησης μπορεί να θεωρηθούν η αύξηση του εύρους ζώνης, η

ιεράρχηση προτεραιοτήτων στη μεταφορά δεδομένων και η συμπίεση των δεδομένων [37]

Ι) Αύξηση εύρους ζώνης

Ο καλύτερος τρόπος αύξησης του εύρους ζώνης είναι μέσω αύξησης της ικανότητας της ζεύξης να φιλοξενεί όλες τις εφαρμογές και τους χρήστες, κάτι που επιτυγχάνεται με προσθήκη κάποιου επιπλέον εύρους ζώνης. Παρόλο που η λύση αυτή ακούγεται απλή, η αύξηση της ικανότητας σύνδεσης είναι δαπανηρή και χρειάζεται χρόνο να εφαρμοστεί. Ευτυχώς, διάφοροι μηχανισμοί QoS μπορεί να χρησιμοποιηθούν για την αποτελεσματική αύξηση του διαθέσιμου εύρους ζώνης, για εφαρμογές προτεραιότητας.

ΙΙ) Προτεραιότητα στην μετάδοση των ευαίσθητων στην καθυστέρηση δεδομένων

Η ιεράρχηση προτεραιοτήτων στη μεταφορά δεδομένων αποτελεί το δεύτερο τρόπο αντιμετώπισης του ζητήματος της συμφόρησης. Μια τέτοια ιεράρχηση μπορεί να πραγματοποιηθεί μέσω διαφόρων διαδικασιών, η σειρά των οποίων είναι η εξής:

- Ταξινόμηση της μεταφοράς δεδομένων σε διαφορετικές κατηγορίες σύμφωνα με τους περιορισμούς QoS, όσον αφορά την καθυστέρηση, το jitter και την απώλεια πακέτων
- Ορισμός του επιπέδου προτεραιότητας κάθε κατηγορίας μεταφοράς δεδομένων. Στην περίπτωση αυτή, το υψηλότερο επίπεδο προτεραιότητας εκχωρείται στην κατηγορία εφαρμογών πραγματικού χρόνου, όπως είναι οι εφαρμογές VoIP και οι τηλεδιασκέψεις
- Εξασφάλιση της μεταφοράς των δεδομένων μέσω του δικτύου βάσει των προτεραιοτήτων που έχουν δοθεί. Η εκχώρηση υψηλού επιπέδου προτεραιότητας, στις εφαρμογές πραγματικού χρόνου, όπως το VoIP, μπορεί να είναι αρκετή για την δέσμευση εύρους ζώνης, ικανού για την υποστήριξη των απαιτήσεων QoS τους. Στην περίπτωση αυτή οι υπόλοιπες εφαρμογές θα πάρουν ότι μέρος του εύρους ζώνης έχει απομείνει

ΙΙΙ) Συμπίεση δεδομένων

Για τη συμπίεση δεδομένων και επομένως την αναγκαιότητα λιγότερου εύρους ζώνης, έχουν προταθεί διάφορες τεχνικές. Οι πιο σημαντικές από τις τεχνικές αυτές είναι οι εξής:

- ***Συμπίεση ωφέλιμου φορτίου:*** Με τη συμπίεση του ωφέλιμου φορτίου του πακέτου, μειώνεται και το συνολικό μέγεθος των δεδομένων και επομένως της κυκλοφορίας εντός του δικτύου. Αυτή η μέθοδος συμπίεσης, δεν επηρεάζει τις κεφαλίδες, πράγμα που την καθιστά κατάλληλη για ζεύξεις που απαιτούν την αναγνωσιμότητα της κεφαλίδας, για τη σωστή δρομολόγηση των πακέτων
- ***Συμπίεση κεφαλίδας:*** Στις point-to-point ζεύξεις IP όπου οι πληροφορίες της κεφαλίδας δεν είναι απαραίτητες για τη δρομολόγηση των πακέτων, η

συμπίεση της κεφαλίδας μπορεί να αποτελέσει εύχρηστη λύση συμπίεσης των δεδομένων

Παρόλο που μπορεί να αυξήσει το διαθέσιμο εύρος ζώνης, η συμπίεση δεδομένων απαιτεί χρόνο και πόρους της CPU, στοιχεία τα οποία μπορεί να αυξήσουν περισσότερο τη συνολική καθυστέρηση του δικτύου.

4.3 Καθυστέρηση δικτύου

Ως καθυστέρηση δικτύου ορίζεται ο συνολικός χρόνος που χρειάζεται ένα πακέτο για να μεταφερθεί από μια πηγή, σε ένα συγκεκριμένο προορισμό μέσω του δικτύου. Η καθυστέρηση του δικτύου, αποτελείται κυρίως από τα εξής είδη καθυστέρησης [37]:

- ***Καθυστέρηση επεξεργασίας:*** αφορά το χρόνο που χρειάζεται ένας δρομολογητής να λάβει ένα πακέτο από μια διεπαφή εισόδου και να το τοποθετήσει στην ουρά της κατάλληλης διεπαφής εξόδου. Η καθυστέρηση επεξεργασίας εξαρτάται κυρίως από την αρχιτεκτονική και την ταχύτητα επεξεργασίας του δρομολογητή
- ***Καθυστέρηση ουράς:*** αφορά τον χρόνο αναμονής του πακέτου στην ουρά εξόδου ενός δρομολογητή. Λόγω των σημείων συμφόρησης, η καθυστέρηση στην ουρά εξαρτάται από το φορτίο κυκλοφορίας, την ταχύτητα επεξεργασίας, το εύρος ζώνης της διεπαφής εξόδου και το μηχανισμό λειτουργίας της ουράς
- ***Καθυστέρηση τοποθέτησης σε σειρά:*** αφορά το χρόνο που απαιτείται για την τοποθέτηση ενός πακέτου στο φυσικό μέσο μεταφοράς
- ***Καθυστέρηση διάδοσης:*** αφορά το χρόνο που χρειάζεται ένα σήμα για να μεταφερθεί από το μέσο που χρησιμοποιείται και εξαρτάται από τον τύπο του μέσου και τον τύπο του σήματος που μεταφέρει τα δεδομένα

Η καθυστέρηση δικτύου μπορεί να αυξηθεί λόγω της εμφάνισης σημείων συμφόρησης, ακατάλληλων ουρών ή σφαλμάτων ρύθμισης των ενεργών στοιχείων του δικτύου. Αυξημένη καθυστέρηση δικτύου μπορεί να δημιουργήσει θέματα ποιότητας QoS ειδικά στις εφαρμογές που παρουσιάζουν ευαισθησία σε καθυστερήσεις, όπως το VoIP. Η προδιαγραφή ITU-T G.114 συνιστά ότι η καθυστέρηση δικτύου από άκρο σε άκρο δεν πρέπει να υπερβαίνει τα 150 ms [37].

Κατά καιρούς, έχουν εξεταστεί διαφορετικές στρατηγικές ελαχιστοποίησης της καθυστέρησης που μπορεί να παρουσιαστεί σε ένα δίκτυο IP, στοχεύοντας στην πραγματοποίηση μιας IP τεχνολογίας, ικανής να υποστηρίζει εφαρμογές πραγματικού χρόνου με αυστηρούς περιορισμούς, όσον αφορά την καθυστέρηση. Η καθυστέρηση δικτύου μπορεί να ελαχιστοποιηθεί χρησιμοποιώντας τις ίδιες στρατηγικές που χρησιμοποιούνται για την αύξηση του διαθέσιμου εύρους ζώνης [36-38].

Ι) Αύξηση της ταχύτητας μετάδοσης των δικτυακών συνδέσεων

Η αύξηση της ταχύτητας μετάδοσης των συνδέσεων και ζεύξεων ενός δικτύου βοηθάει στη μείωση των καθυστερήσεων τοποθέτησης στη σειρά και μετάδοσης και συνεπώς στη μείωση της συνολικής καθυστέρησης του δικτύου.

II) Αύξηση της ταχύτητας επεξεργασίας των κόμβων

Η αύξηση της ταχύτητας επεξεργασίας των κόμβων του δικτύου επιτρέπει τη μείωση της καθυστέρησης επεξεργασίας, η οποία με τη σειρά της βοηθά στη μείωση της καθυστέρησης στην ουρά και συνεπώς στην μείωση της καθυστέρησης δικτύου από άκρο σε άκρο.

III) Προτεραιότητα στην μετάδοση των ευαίσθητων στην καθυστέρηση δεδομένων

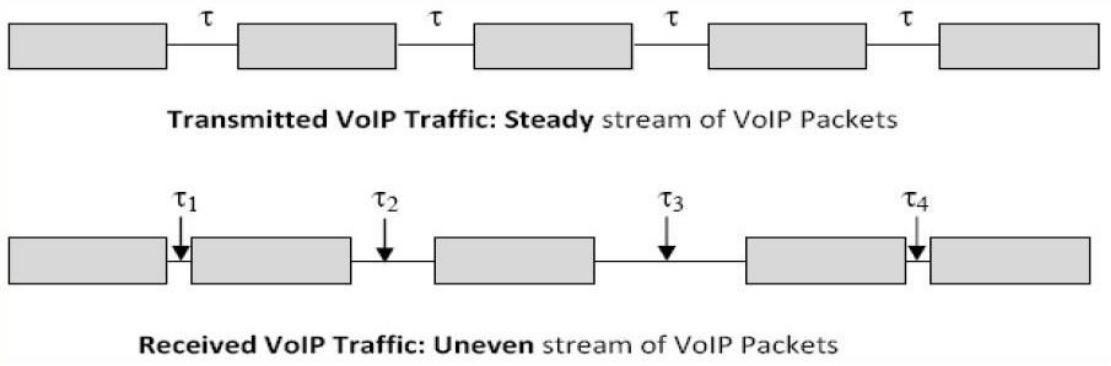
Αυτή η προσέγγιση βοηθά στη μείωση της καθυστέρησης στην ουρά, των ευαίσθητων στην καθυστέρηση δεδομένων, όπως είναι τα δεδομένα φωνής. Η εφαρμογή προτεραιοτήτων βοηθά στην υποστήριξη των αυστηρών περιορισμών καθυστέρησης τέτοιων εφαρμογών.

IV) Συμπίεση μεταφερόμενων δεδομένων

Όπως έχει ήδη αναφερθεί, η συμπίεση των μεταφερόμενων δεδομένων συνεισφέρει στην μείωση του όγκου των δεδομένων, που μεταδίδονται μέσω του δικτύου, γεγονός που μειώνει το φορτίο κίνησης δικτύου και συνεπώς μειώνει τις καθυστερήσεις ουράς και τοποθέτησης σε σειρά.

4.4 Διακύμανση καθυστέρησης

Το jitter ορίζεται ως διακύμανση του χρόνου άφιξης των λαμβανόμενων πακέτων. Από την πλευρά αποστολής, τα πακέτα αποστέλλονται έχοντας ομοιόμορφα κενά μεταξύ τους και με συνεχή ροή. Εξαιτίας των σημείων συμφόρησης που παρουσιάζονται σε πολλά σημεία του δικτύου μεταφοράς, αυτή η σταθερή ροή μπορεί να γίνει ανομοιογενής, επειδή η καθυστέρηση κάθε πακέτου ποικίλλει αντί να παραμένει σταθερή. Στην εικόνα 20 παρουσιάζεται σχηματικά το φαινόμενο του jitter.



Εικόνα 20: *Φαινόμενο jitter [33]*

Το φαινόμενο του jitter μπορεί να δημιουργήσει αρκετά προβλήματα στις φωνητικές εφαρμογές, όπως διακοπές της φωνής ή παρουσία έντονου "τραυλίσματος" (stutter), τα οποία μπορεί να είναι πολύ ενοχλητικά για τους συνομιλητές. Με σκοπό την επαρκή μεταφορά των φωνητικών δεδομένων μέσω των IP δικτύων, η προδιαγραφή ITU-T G.114 συνιστά ως ανώτερη τιμή του jitter τα 30ms κατά μέσο όρο [37].

Με δεδομένα τα ενοχλητικά αποτελέσματα του jitter, δημιουργήθηκε ένας μηχανισμός ποιότητας QoS, γνωστός ως de-jitter ή μηχανισμός αποθήκευσης των καθυστερήσεων [37, 38]. Εφαρμοζόμενος στη διεπαφή εισόδου του άκρου λήψεως, ο μηχανισμός αυτός βασίζεται στη χρήση ενός συγκεκριμένου buffer, γνωστού ως de-jitter buffer, με σκοπό την επιβράδυνση και την τοποθέτηση σωστών διαστημάτων μεταξύ των ληφθέντων πακέτων πριν τη μεταφορά τους στο στρώμα εφαρμογών της λήψης. Αν και βοηθάει στη μείωση του φαινομένου jitter, ο μηχανισμός αυτός επηρεάζει τη συνολική καθυστέρηση του δικτύου.

4.5 Απώλεια δεδομένων

Ο κύριος λόγος για την απώλεια πακέτων που μεταφέρονται μέσω ενός δικτύου IP είναι η συμφόρηση του δικτύου. Τα χαμένα πακέτα δεδομένων μπορούν να ανακτηθούν μέσω αναμετάδοσης. Ωστόσο, τα χαμένα πακέτα φωνής δεν μπορούν να ανακτηθούν με αναμετάδοση, επειδή οι εφαρμογές φωνής πρέπει να είναι πραγματικού χρόνου. Ως εκ τούτου, οι μηχανισμοί QoS θα πρέπει να λαμβάνουν υπόψη την ελαχιστοποίηση της απώλειας των πακέτων φωνής. Για μια αποτελεσματική ανάπτυξη της εφαρμογής VoIP, η προδιαγραφή ITU-T G.114 συνιστά ότι το συνολικό άθροισμα των πακέτων που χάνονται για μια φωνητική κλήση, δεν πρέπει ποτέ να υπερβαίνει το 1% [37].

Η απώλεια των πακέτων δεδομένων φωνής μπορεί να ελαχιστοποιηθεί χρησιμοποιώντας τις στρατηγικές πρόληψης συμφόρησης δικτύου, προτεραιότητας των δεδομένων φωνής και απόκρυψης λόγω απώλειας πακέτων [36-38].

Ι) Πρόληψη συμφόρησης δικτύου

Για την αποτροπή εμφάνισης συμφόρησης στο δίκτυο μπορούν να χρησιμοποιηθούν οι εξής διαδικασίες [39]:

- ***Αύξηση του εύρους ζώνης δικτύου:*** μια τέτοια αύξηση μπορεί να επιτευχθεί μέσω αύξησης της χωρητικότητας μετάδοσης των συνδέσεων, της χωρητικότητας αποθήκευσης των δρομολογητών και της ταχύτητας επεξεργασίας των δρομολογητών του δικτύου
- ***Μείωση του φορτίου κυκλοφορίας:*** μια τέτοια μείωση μπορεί να επιτευχθεί μέσω συμπίεσης των μεταφερόμενων δεδομένων, της διαμόρφωσης της κυκλοφορίας ώστε να παρουσιάζεται καθυστέρηση (π.χ. η διαμόρφωση ροής ενός διακομιστή FTP από 512 kbps στα 256 kbps) και του ελέγχου των

εισερχομένων κλήσεων (μια κλήση είναι δυνατή μόνο σε περίπτωση διαθεσιμότητας επαρκούς εύρους ζώνης)

- ***Έλεγχος κυκλοφορίας:*** αφορά την απόρριψη πακέτων χαμηλής προτεραιότητας ώστε να αποτρέπεται η συμφόρηση. Το επίπεδο προτεραιότητας καθορίζεται μέσω ενός κατώτατου ορίου. Το εργαλείο σταθμισμένης τυχαίας πρόωρης ανίχνευσης (Weighted Random Early Detection - WRED) μπορεί να χρησιμοποιηθεί γι' αυτό το λόγο, ξεκινώντας την απομάκρυνση των πακέτων χαμηλής προτεραιότητας πριν από την εμφάνιση συμφόρησης

II) Προτεραιότητα δεδομένων φωνής

Ο μηχανισμός προτεραιότητας δεδομένων φωνής αφορά την καθυστέρηση ή την απομάκρυνση πακέτων δεδομένων χαμηλής προτεραιότητας με σκοπό την παροχή εγγυήσεων σχετικά με το απαιτούμενο εύρος ζώνης για τη μετάδοση των δεδομένων αυτών.

III) Απόκρυψη απώλειας πακέτων

Παρά την εφαρμογή των παραπάνω μηχανισμών που στοχεύουν στη μείωση των απωλειών των φωνητικών πακέτων, η πλήρης εξάλειψη των εν λόγω απωλειών δεν είναι εφικτή. Οι απώλειες των πακέτων φωνής γίνονται αντιληπτές στους συνομιλητές μέσω των κενών που παρουσιάζονται στη συνομιλία. Για το λόγο αυτό δημιουργήθηκε ο μηχανισμός απόκρυψης απώλειας πακέτων (Packet Loss Concealment - PLC), ο οποίος χρησιμοποιεί έξυπνο τρόπο ανάλυσης των πακέτων που λείπουν και παράγει αντίστοιχα λογικά πακέτα αντικατάστασης, με σκοπό τη βελτίωση της ποιότητας φωνής. Η τεχνολογία Cisco VoIP χρησιμοποιεί δείγματα των 20 ms ωφέλιμου φωνητικού φορτίου ανά πακέτο VoIP από προεπιλογή. Οι αλγόριθμοι αποτελεσματικής διόρθωσης των codec απαιτούν την απώλεια ενός μόνο πακέτου για οποιαδήποτε δεδομένη στιγμή. Εάν χάνονται περισσότερα πακέτα, ο ακροατής κατανοεί την ύπαρξη κενών κατά την συνομιλία.

4.6 Καθορισμός καθαρότητας φωνής

Τα θέματα ποιότητας QoS όσον αφορά τη χρήση της τεχνολογίας VoIP, σχετίζονται άμεσα με την καθαρότητα και την ευκρίνεια που θα πρέπει να έχει ο ήχος της φωνής στα τερματικά των δύο άκρων της συνομιλίας [37, 39]. Ο εκάστοτε χρήστης της τεχνολογίας VoIP, θα πρέπει να είναι σε θέση να αναγνωρίσει την ταυτότητα και να αισθανθεί τη διάθεση του συνομιλητή του. Επομένως, τα δύο αυτά χαρακτηριστικά είναι ύψιστης σημασίας για τον καθορισμό της ποιότητας QoS και μπορούν να επηρεαστούν από διάφορους παράγοντες, όπως η πιστότητα, η ηχώ, ο πλάγιος τόνος και ο θόρυβος περιβάλλοντος.

I) Πιστότητα

Ως πιστότητα (fidelity) ορίζεται ο βαθμός στον οποίο το δίκτυο που μεταφέρει τη φωνή, αναπαράγει με ακρίβεια το μεταδιδόμενο φωνητικό σήμα. Η πιστότητα

εξαρτάται από τη ζώνη συχνοτήτων δειγματοληψίας και τους λόγους συμπίεσης. Όταν λαμβάνεται δείγμα ήχου χρησιμοποιώντας τη ζώνη συχνοτήτων 300-3400 Hz, (narrow band) το οποίο στη συνέχεια υπόκειται σε μεγάλο βαθμό συμπίεσης, τότε ο αναπαραγώμενος ήχος θεωρείται χαμηλής πιστότητας. Αντίθετα, όταν γίνεται δειγματοληψία χρησιμοποιώντας τη ζώνη συχνοτήτων 50-7000 Hz (wide band) και η μεταφορά γίνεται με μικρότερο λόγο συμπίεσης, τότε το αναπαραγώμενο ηχητικό σήμα θεωρείται υψηλής πιστότητας.

Η ανθρώπινη φωνή καλύπτει τη ευρεία ζώνη συχνοτήτων (50-7000 Hz). Η δειγματοληψία φωνής που χρησιμοποιεί τη στενή ζώνη αποφέρει μια αποδεκτή ποιότητα QoS αφού το 90% των σημαντικότερων στοιχείων της ανθρώπινης φωνής, περιέχονται στο συγκεκριμένο φάσμα. Αντίθετα, η δειγματοληψία με τη χρήση της ευρείας ζώνης προσφέρει μια πιο καθαρή και πληρέστερη ακουστικά αναπαραγωγή του φωνητικού σήματος, αλλά με κόστος υψηλότερες απαιτήσεις εύρους ζώνης.

II) Ηχώ

Η ηχώ είναι αποτέλεσμα της μη προσαρμογής της σύνθετης ακουστικής αντίστασης στη διαδρομή μετάδοσης. Η ηχώ είναι πάντα παρούσα, ακόμη και στα παραδοσιακά δίκτυα τηλεφωνίας, αλλά σε επίπεδο που δεν μπορεί να ανιχνευθεί από το ανθρώπινο αυτί. Τα στοιχεία που κάνουν την ηχώ αντιληπτή είναι το πλάτος (η ένταση της ηχούς) και η καθυστέρηση (ο χρόνος που μεσολαβεί μεταξύ της στιγμής που παράγεται η φωνή και του ανακλώμενου ηχητικού σήματος). Η μείωση των ενοχλητικών αποτελεσμάτων του φαινομένου της ηχούς, μπορεί να επιτευχθεί μέσω χρήσης ενός συγκεκριμένου συστήματος, γνωστού ως suppressor ή καταστολέας ηχούς.

III) Πλάγιος τόνος

Ο πλάγιος τόνος αναφέρεται στο γεγονός ότι το τηλέφωνο επιτρέπει στους ομιλητές να ακούσουν τον ήχο ομιλίας τους, στο ακουστικό της τηλεφωνικής συσκευής που χρησιμοποιούν. Χωρίς πλάγιο τόνο, ο ομιλητής μένει με την εντύπωση ότι το τηλέφωνο δεν λειτουργεί. Επομένως, στις εφαρμογές VoIP, ο πλάγιος τόνος πρέπει να υφίσταται.

IV) Θόρυβος περιβάλλοντος

Ο θόρυβος του background αντιστοιχεί σε έναν ήχο χαμηλής έντασης που ακούγεται από την άλλη άκρη της σύνδεσης για να αποφευχθεί η ψευδαίσθηση ότι η κλήση έχει αποσυνδεθεί. Επομένως, στις εφαρμογές VoIP, ο θόρυβος του background πρέπει να υφίσταται.

5 Ανάλυση θεμάτων ασφάλειας της τεχνολογίας VoIP

5.1 Τρωτά σημεία των συστημάτων VoIP

Όσον αφορά την ασφάλεια ενός συστήματος ή ενός δικτύου, με τον όρο τρωτό σημείο ή ευπάθεια εννοείται ένα ελάττωμα ή μια αδυναμία που μπορεί να εκμεταλλευτεί ένας εισβολέας για να πραγματοποιήσει μια επίθεση. Το VoIP ως σύστημα μπορεί να παρουσιάσει δύο τύπους ευπάθειας [38, 40]. Ο πρώτος τύπος αφορά τα τρωτά σημεία της υποδομής (δίκτυο, λειτουργικό σύστημα, διακομιστής ιστού, κ.α.) που χρησιμοποιείται για την ανάπτυξη των εφαρμογών του VoIP. Ο άλλος τύπος αφορά την ευπάθεια που παρουσιάζουν τα πρωτόκολλα και οι συσκευές VoIP, όπως το IP τηλέφωνο, η πύλη, ο διακομιστής πολυμέσων, ο ελεγκτής σηματοδότησης, κ.λπ.

Στις επόμενες υποενότητες θα παρουσιαστούν οι πηγές των τρωτών σημείων καθώς και τα ευάλωτα μέρη ενός συστήματος VoIP.

5.1.1 Πηγές ευπάθειας συστημάτων VoIP

Σε ένα σύστημα VoIP ως πηγές ευπάθειας μπορούν να θεωρηθούν οι εξής [12]:

- ***Υποδομή IP δικτύου:*** Σε ένα σύστημα VoIP, όλη η κυκλοφορία μεταβιβάζεται μέσω δικτύων IP, γεγονός που συνεπάγεται ότι η οποιαδήποτε ευπάθεια των δικτύων IP, όπως ο κακόβουλος κατακερματισμός των δεδομένων ή οι ιοί του δικτύου, κληροδοτείται και στο σύστημα VoIP

- ***Δημόσια δίκτυα:*** Στις περισσότερες περιπτώσεις, η κυκλοφορία του συστήματος VoIP μεταφέρεται μέσω του Διαδικτύου όπου ανώνυμοι άνθρωποι συμπεριλαμβανομένων των χάκερ μπορεί να μεταφέρουν και να λάβουν κακόβουλα δεδομένα

- ***Ανοικτά πρωτόκολλα VoIP:*** Τα περισσότερα πρωτόκολλα VoIP, όπως το SIP ή το H.323, είναι τυποποιημένα και ανοικτά στο κοινό. Ως εκ τούτου, ένας εισβολέας μπορεί να δημιουργήσει κακόβουλο πρόγραμμα πελάτη ή διακομιστή με βάση την προδιαγραφή του πρωτοκόλλου προκειμένου να αποκτήσει πρόσβαση σε διακομιστές VoIP ή σε πελάτες. Επιπλέον, το γεγονός ότι τα πρωτόκολλα VoIP είναι ανοικτά βοηθά τους επίδοξους εισβολείς να εντοπίσουν και να επωφεληθούν από τις ευπάθειές τους

- ***Ενσωμάτωση φωνής και δεδομένων:*** Παρά τα όποια σημαντικά οφέλη, η ενσωμάτωση της φωνής στην κυκλοφορία δεδομένων του ίδιου δικτύου οδηγεί σε νέα τεχνικά ζητήματα. Στην πραγματικότητα, η ενοποίηση της κυκλοφορίας με διαφορετικές απαιτήσεις ποιότητας QoS και ασφάλειας, καθιστούν την επίλυση

θεμάτων, όπως η ασφάλεια, η μεταγωγή, η ρύθμιση της ουράς, κλπ. πιο περίπλοκη και δύσκολη

- ***Έλλειψη ειδικών μηχανισμών ασφαλείας:*** Ενώ πολλοί μηχανισμοί ασφαλείας δεδομένων, όπως τα τείχη προστασίας, μπορεί να ενισχύσουν την ασφάλεια των συστημάτων VoIP, η λειτουργία τους εξακολουθεί να μην είναι αρκετή για την προστασία των συστημάτων VoIP από τις σύγχρονες κακόβουλες επιθέσεις

- ***Μεταφορά δεδομένων σε πραγματικό χρόνο:*** Σε αντίθεση με τις κοινές υπηρεσίες επικοινωνίας, όπως το ηλεκτρονικό ταχυδρομείο, η υπηρεσία VoIP απαιτεί τη μεταφορά δεδομένων σε πραγματικό χρόνο, γεγονός που συνεπάγεται ύπαρξη σημαντικών περιορισμών ποιότητας QoS όσον αφορά την καθυστέρηση του πακέτου και το φαινόμενο jitter. Ως εκ τούτου, η οποιαδήποτε καθυστέρηση πακέτου ή εμφάνιση jitter μπορεί να γίνει αντιληπτή από τους χρήστες και να επηρεάσει τη συνολική ποιότητα QoS. Ένας επιτιθέμενος μπορεί να επιβαρύνει το φορτίο του δικτύου VoIP (δημιουργώντας για παράδειγμα πλημμύρες Calla) και να επηρεάσει την παρεχόμενη ποιότητα QoS και επομένως την αξιοπιστία του συστήματος

- ***Εκτεθειμένες διεπαφές:*** Η ανάπτυξη της πλειοψηφίας των σύγχρονων συστημάτων VoIP βασίζεται στην αρχιτεκτονική πελάτη-διακομιστή. Ακόμη και αν οι διακομιστές VoIP βρίσκονται σε προστατευμένο δίκτυο, οι μονάδες διασύνδεσης που λαμβάνουν αιτήματα κλήσεων είναι ανοιχτές στους πελάτες που βρίσκονται σε ανοιχτό ή δημόσιο δίκτυο. Αυτό επιτρέπει στους επιτιθέμενους να πραγματοποιήσουν σάρωση θυρών για την ανεύρεση των εκτεθειμένων μονάδων διασύνδεσης και στη συνέχεια να εξαπολύσουν επιθέσεις ασφάλειας (για παράδειγμα επιθέσεις DoS) αποστέλλοντας κακόβουλα δεδομένα

- ***Κινητικότητα τερματικών:*** Το τηλεφωνικό σύστημα PSTN εκχωρεί ξεχωριστές τηλεφωνικές γραμμές για κάθε μεμονωμένο αριθμό. Έτσι, ένας επιτιθέμενος θα πρέπει να έχει φυσική πρόσβαση για να μπορέσει να παραποιήσει την ταυτότητα (τον αριθμό τηλεφώνου ή τη γραμμή) ενός χρήστη του τηλεφωνικού συστήματος PSTN. Σε αντίθεση με την τεχνολογία PSTN, τα τηλεφωνικά συστήματα VoIP υποστηρίζουν την κινητικότητα των τερματικών, γεγονός που καθιστά την προστασία ενάντια στην παραποίηση της ταυτότητας (spoofing) δυσκολότερη

5.1.2 Ευπάθειες εξοπλισμού

Μια σύντομη επισκόπηση των κύριων ευπαθών στοιχείων που συμμετέχουν στην ανάπτυξη ενός τακτικού συστήματος VoIP είναι η ακόλουθη [38, 40]:

- ***Λειτουργικό σύστημα:*** Οι εφαρμογές VoIP επηρεάζονται από τρωτά σημεία των λειτουργικών συστημάτων πάνω από τα οποία εκτελούνται. Οι ευπάθειες των λειτουργικών συστημάτων μπορούν κάλλιστα να αποδειχθούν από τις συχνές κυκλοφορίες patch ασφαλείας για όλα ανυπερθέτως τα συστήματα (Windows, Unix, Linux)

- ***Εφαρμογές VoIP:*** Ακόμα και οι ίδιες οι εφαρμογές VoIP (Skype, Google Talk, κ.λπ.) μπορεί να παρουσιάζουν προβλήματα ασφάλειας εξαιτίας ελαττωμάτων ή σφαλμάτων (bugs), τα οποία θα μπορούσαν να κάνουν την υπηρεσία VoIP ανασφαλή

- ***Πρωτόκολλα VoIP:*** Η ανάπτυξη μιας εφαρμογής VoIP περιλαμβάνει ένα πρωτόκολλο σηματοδοσίας (H323, SIP) και ένα πρωτόκολλο μεταφοράς μέσων (RTP, RTCP). Τα πρωτόκολλα αυτά είναι ευάλωτα σε διάφορα είδη επιθέσεων, γεγονός που μπορεί να επηρεάσει την υπηρεσία VoIP που παρέχεται βάσει αυτών των πρωτοκόλλων

- ***Διασύνδεση διαχείρισης:*** Για σκοπούς διαχείρισης, η πλειοψηφία του εξοπλισμού VoIP έχει διαφορετικές διεπαφές υπηρεσιών, όπως SNMP, SSH, Telnet και HTTP. Μια διεπαφή υπηρεσίας μπορεί να αποτελέσει πηγή ευπάθειας, ειδικά η ρύθμισή της έχει γίνει απρόσεκτα. Για παράδειγμα, εάν μια συσκευή VoIP χρησιμοποιεί το προεπιλεγμένο αναγνωριστικό / κωδικό πρόσβασης για τη διεπαφή διαχείρισης, αποτελεί εύκολη λεία κακόβουλης επίθεσης

- ***Διακομιστής TFTP:*** Πολλές συσκευές VoIP κατεβάζουν τις ρυθμίσεις τους από ένα διακομιστή TFTP. Ένας εισβολέας θα μπορούσε εύκολα με παραποίηση της σύνδεσης να παρουσιαστεί ως διακομιστής TFTP και στη συνέχεια να διανείμει μια κακόβουλη διαμόρφωση του εξοπλισμού VoIP

- ***Συσκευή πρόσβασης:*** Όλη η κυκλοφορία VoIP μεταφέρεται μέσω των συσκευών πρόσβασης (π.χ. switch ή router) που είναι υπεύθυνες για τη μεταγωγή ή τη δρομολόγησή της. Οι εκτιθέμενες συσκευές πρόσβασης θα μπορούσαν να δημιουργήσουν σοβαρά ζητήματα ασφάλειας επειδή έχουν πλήρη έλεγχο των πακέτων

- ***Δίκτυο:*** Η κυκλοφορία VoIP επηρεάζεται από τις ευπάθειες του δικτύου IP μέσω του οποίου μεταδίδεται. Μια ευπάθεια του δικτύου μπορεί να οφείλεται σε κακή ρύθμιση των παραμέτρων μιας συσκευής (switch, δρομολογητής, τείχος προστασίας, κ.λπ.) ή σε ένα σφάλμα ενός από τα εμπλεκόμενα πρωτόκολλα (IP, UDP, κλπ)

5.2 Επιθέσεις κατά της ασφάλειας των συστημάτων VoIP

Ο οποιοσδήποτε χάκερ θα μπορούσε να εκμεταλλευτεί τα τρωτά σημεία των συστημάτων VoIP που παρουσιάστηκαν στην προηγούμενη ενότητα για να πραγματοποιήσει οποιουδήποτε είδους επίθεση. Οι επιτιθέμενοι θα μπορούσαν κάλλιστα να δημιουργήσουν προβλήματα στην υπηρεσία VoIP μέσω πραγματοποίησης πλημμύρας δεδομένων, να συλλέξουν πληροφορίες προσωπικών δεδομένων μέσω παρακολούθησης της σηματοδοσίας κλήσης ή του ίδιου του περιεχομένου κλήσεων, να κάνουν υποκλοπές κλήσεων μέσω πλαστοπροσωπίας των διακομιστών ή των χρηστών, να πραγματοποιήσουν ψευδείς κλήσεις με ψεύτικες ταυτότητες κ.ο.κ.

Η κατηγοριοποίηση των επιθέσεων κατά της ασφάλειας ενός δικτύου γενικότερα μπορεί να γίνει με πολλούς τρόπους. Για παράδειγμα, η πρώτη έκδοση του σχεδίου IETF ταξινόμησε τις επιθέσεις αυτές στις ακόλουθες τέσσερις κατηγορίες [12]:

- Επιθέσεις παρακολούθησης και τροποποίησης
- Επιθέσεις διακοπής υπηρεσίας
- Επιθέσεις κατάχρησης υπηρεσιών και
- Κοινωνικές επιθέσεις

Οι Thermos και Takanen ταξινόμησαν τις επιθέσεις κατά της ασφάλειας των συστημάτων VoIP στις ακόλουθες κατηγορίες [40]:

- Επιθέσεις διακοπής της υπηρεσίας και ενόχλησης
- Επιθέσεις υποκλοπής και ανάλυσης της κυκλοφορίας
- Επιθέσεις μεταμφίεσης και πλαστοπροσωπίας
- Επιθέσεις μη εξουσιοδοτημένης πρόσβασης και απάτης

Επίσης, ο P. Patrick ταξινομεί τις επιθέσεις αυτές στις εξής τέσσερις κατηγορίες [38]:

- Επιθέσεις κατά της διαθεσιμότητας
- Επιθέσεις κατά της εμπιστευτικότητας
- Επιθέσεις κατά της ακεραιότητας και
- Επιθέσεις κατά του κοινωνικού πλαισίου

Στις επόμενες υποενότητες θα γίνει μια σύντομη παρουσίαση και επισκόπηση των επιθέσεων κατά της ασφάλειας των συστημάτων VoIP με βάση την τελευταία ταξινόμηση, η οποία θεωρείται και η πιο περιεκτική σε σύγκριση με τις άλλες δύο.

5.2.1 Επιθέσεις κατά της διαθεσιμότητας

Οι επιθέσεις κατά της διαθεσιμότητας στοχεύουν στη διακοπή της υπηρεσίας VoIP, συνήθως με τη μορφή άρνησης εξυπηρέτησης (DoS). Οι κυριότερες επιθέσεις κατά της διαθεσιμότητας είναι οι εξής [38]:

- ***Πλημμύρισμα κλήσης (Call Flooding):*** Ο επιτιθέμενος πλημμυρίζει με δεδομένα (σήματα ή μέσα) το στοχευόμενο σύστημα (για παράδειγμα, διακομιστή VoIP, πελάτη και υποκείμενη υποδομή), γεγονός που καταστρέφει το σύστημα ή μειώνει σημαντικά την απόδοσή του

- ***Μη συμβατικά μηνύματα (Malformed messages):*** Ένας εισβολέας μπορεί να δημιουργήσει και να στείλει μη συμβατικά μηνύματα στον στοχευόμενο διακομιστή ή πελάτη με σκοπό τη διακοπής της υπηρεσίας. Ένα μη συμβατικό μήνυμα είναι μήνυμα πρωτοκόλλου με λανθασμένη σύνταξη. Με τη λήψη ενός τέτοιου είδους απροσδόκητου μηνύματος, ο διακομιστής μπορεί να βρεθεί σε σύγχυση και να αντιδράσει με πολλούς διαφορετικούς τρόπους ανάλογα με την εφαρμογή. Οι τυπικές

επιπτώσεις μιας τέτοιας επίθεσης είναι η δημιουργία ατέρμονα βρόγχου, η υπερχείλιση του buffer, η αδυναμία επεξεργασίας των κανονικών μηνυμάτων και το κρασάρισμα του συστήματος

- ***Ψευδή μηνύματα (Spoofed Messages):*** Ένας εισβολέας μπορεί να εισάγει ψευδή μηνύματα σε μια συγκεκριμένη σύνοδο VoIP με σκοπό τη διακοπή της λειτουργίας της υπηρεσίας ή την κλοπή της ίδιας της συνόδου. Τυπικό παράδειγμα επίθεσης με ψευδή μηνύματα είναι ο τερματισμός κλήσης (call teardown). Στην περίπτωση τέτοιας επίθεσης ο επιτιθέμενος δημιουργεί και στέλνει ένα μήνυμα τερματισμού κλήσης (για παράδειγμα SIP Bye) σε μια συσκευή επικοινωνίας για τη διακοπή μιας περιόδου κλήσης. Πριν την εξαπόλυση της επίθεσης, απαιτείται η κλοπή των πληροφοριών της περιόδου σύνδεσης (Call-ID)

- ***Πειρατεία κλήσης (Call Hijacking):*** Η επίθεση αυτή πραγματοποιείται όταν ο επιτιθέμενος παίρνει τον έλεγχο κάποιων από τις συναλλαγές μεταξύ ενός τερματικού VoIP και του δικτύου. Οι συναλλαγές αυτές μπορεί να αφορούν την εγγραφή, τη ρύθμιση κλήσης, τη ροή μέσων κλπ.. Αυτού του είδους επίθεση μπορεί να προκαλέσει σοβαρά θέματα διακοπής υπηρεσίας, όπως την απενεργοποίηση των νόμιμων χρηστών που χρησιμοποιούν την υπηρεσία VoIP. Όπως συμβαίνει και στην επίθεση τερματισμού κλήσης, πριν την εξαπόλυση της επίθεσης, απαιτείται η κλοπή των πληροφοριών της περιόδου σύνδεσης, αλλά η πραγματική μορφή των δύο επιθέσεων και του αντίκτυπού τους είναι διαφορετική. Τυπικά παραδείγματα πειρατείας κλήσης είναι η πειρατεία καταχώρισης (registration hijacking) και η πειρατεία συνόδου μέσων (media session hijacking)

- ***Κατάχρηση QoS (QoS Abuse):*** Κατά τη διάρκεια της ρύθμισης της κλήσης, τα τερματικά VoIP διαπραγματεύονται τα στοιχεία της κλήσης, όπως τον τύπο του μέσου, το ρυθμό κωδικοποίησης του codec και τον τύπο του ωφέλιμου φορτίου. Ο επιτιθέμενος μπορεί να παρέμβει σε αυτή τη διαπραγμάτευση και να κάνει κατάχρηση της ποιότητας QoS, αντικαθιστώντας, διαγράφοντας ή τροποποιώντας τους codec ή τον τύπο του ωφέλιμου φορτίου. Άλλη μέθοδος κατάχρησης της ποιότητας QoS είναι η εξάντληση του περιορισμένου εύρους ζώνης με χρήση κακόβουλου εργαλείου έτσι ώστε οι νόμιμοι χρήστες να μην μπορούν να χρησιμοποιήσουν το διαθέσιμο εύρος ζώνης για την υπηρεσία τους

5.2.2 Επιθέσεις εναντίον εμπιστευτικότητας

Οι επιθέσεις κατά της εμπιστευτικότητας δίνουν τη δυνατότητα στους επιτιθέμενους για μη εξουσιοδοτημένη καταγραφή των μέσων, της ταυτότητας, των μοτίβων και των διαπιστευτηρίων, στοιχεία τα οποία μπορούν να χρησιμοποιηθούν σε μεταγενέστερες μη εξουσιοδοτημένες συνδέσεις ή άλλες ενέργειες παραπλάνησης. Οι κύριοι τύποι των επιθέσεων εμπιστευτικότητας είναι οι εξής [38]:

- ***Υποκλοπές μέσων (Media Eavesdropping):*** Πρόκειται για επιθέσεις μη εξουσιοδοτημένης πρόσβασης στα πακέτα των μέσων. Οι επιθέσεις αυτές μπορούν τυπικά να πραγματοποιηθούν με δύο τρόπους. Ο πρώτος αφορά τη διακύβευση μιας συσκευής πρόσβασης (π.χ. ένα switch επιπέδου 2) και την αντιγραφή των

στοχευόμενων μέσων σε μια αντίστοιχη συσκευή του επιτιθέμενου. Ο άλλος τρόπος αφορά την πραγματοποίηση υποκλοπών στο φυσικό μέσο μεταφοράς των δεδομένων, ένας τρόπος ο οποίος είναι παρόμοιος με την θρυλική τεχνική tapping στα δίκτυα PSTN. Για παράδειγμα, ο επιτιθέμενος μπορεί να αποκτήσει πρόσβαση στην γραμμή T1, χωρίζοντάς την με φυσικό τρόπο σε δύο σήματα

- ***Παρακολούθηση μοτίβων κλήσεων:*** Η παρακολούθηση μοτίβων κλήσεων αφορά τη μη εξουσιοδοτημένη ανάλυση της κίνησης VoIP (κίνηση από / σε οποιοδήποτε συγκεκριμένο κόμβο ή δίκτυο), έτσι ώστε ο επιτιθέμενος να μπορεί να βρει στοιχεία για συσκευές, πληροφορίες πρόσβασης (IP / θύρα), πρωτόκολλα ή οποιαδήποτε ευπάθεια του δικτύου

- ***Εξόρυξη δεδομένων:*** Η γενική έννοια της εξόρυξης δεδομένων στο VoIP αφορά τη μη εξουσιοδοτημένη συλλογή αναγνωριστικών, όπως το όνομα χρήστη, ο αριθμός τηλεφώνου, ο κωδικός πρόσβασης, η διεύθυνση URL, η διεύθυνση ηλεκτρονικού ταχυδρομείου, αναγνωριστικά που αντιπροσωπεύουν τα τηλέφωνα, τους κόμβους διακομιστών, τα συμβαλλόμενα μέρη ή τους οργανισμούς του δικτύου. Αυτές οι πληροφορίες μπορούν να χρησιμοποιηθούν για μεταγενέστερες μη εξουσιοδοτημένες συνδέσεις, όπως διακοπές υπηρεσίας, επιθέσεις εμπιστευτικότητας, ψευδείς κλήσεις, κ.λπ.

5.2.3 Επιθέσεις κατά της ακεραιότητας

Μια επίθεση κατά της ακεραιότητας αφορά την υποκλοπή και τροποποίηση της κίνησης που μεταφέρεται (μηνύματα σηματοδοσίας ή πακέτα μέσων) εντός του δικτύου. Η τροποποίηση αυτή μπορεί να αφορά τη διαγραφή, την έγχυση ή την αντικατάσταση συγκεκριμένων πληροφοριών στα μηνύματα ή στα μέσα VoIP. Οι κυριότερες επιθέσεις κατά της ακεραιότητας των μηνυμάτων σηματοδοσίας ή των μέσων είναι οι εξής [38]:

- ***Αναδρομολόγηση κλήσης:*** Πρόκειται για μη εξουσιοδοτημένη αλλαγή δρομολόγησης της κλήσης με μεταβολή των πληροφοριών δρομολόγησης στα μηνύματα σηματοδοσίας. Το αποτέλεσμα της αναδρομολόγησης κλήσεων είναι ο αποκλεισμός νόμιμων ή η εισβολή παράνομων οντοτήτων στη διαδρομή του σήματος κλήσης ή του μέσου

- ***Έγχυση μέσων:*** Πρόκειται για μη εξουσιοδοτημένη μέθοδο εισαγωγής νέων μέσων σε ένα ενεργό κανάλι μέσων. Συνέπεια της έγχυσης μέσων είναι η ακρόαση κάποιας διαφήμισης, θορύβου ή απόλυτης σιγής από τον χρήστη / θύμα στη μέση της συνομιλίας

- ***Αποδόμηση μέσων:*** Πρόκειται για μη εξουσιοδοτημένη μέθοδο χειρισμού των μέσων ή των πακέτων ελέγχου μέσων μιας ήδη δημιουργημένης συνόδου επικοινωνίας, με σκοπό τη μείωση της ποιότητας QoS. Για παράδειγμα, ένας επιτιθέμενος υποκλέπτει πακέτα RTCP και αλλάζει τον αύξοντα αριθμό τους ώστε το μέσο να αναπαραχθεί με λανθασμένη ακολουθία στο τερματικό λήψης, κάτι που υποβαθμίζει την ποιότητα της επικοινωνίας

5.2.4 Επιθέσεις κατά του κοινωνικού πλαισίου

Μια επίθεση κατά του κοινωνικού πλαισίου επικεντρώνεται στη χειραγώγηση του κοινωνικού πλαισίου μεταξύ των οντοτήτων που επικοινωνούν. Με τον τρόπο αυτό, ο επιτιθέμενος παρουσιάζεται ως αξιόπιστη οντότητα και μπορεί να μεταφέρει ψευδείς πληροφορίες στο στοχευόμενο χρήστη (θύμα). Οι τυπικότερες επιθέσεις κατά του κοινωνικού πλαισίου είναι οι εξής [38]:

- ***Παραποίηση (Misrepresentation):*** Αντιστοιχεί στην εκ προθέσεως παρουσίαση ψεύτικων στοιχείων ταυτότητας, εξουσίας, δικαιωμάτων ή ακόμα και περιεχομένου με σκοπό την εξαπάτηση του στοχευόμενου χρήστη (θύμα) ή συστήματος. Οι επιθέσεις παραποίησης ταυτότητας αφορούν τη μέθοδο παρουσίασης μιας ταυτότητας με ψευδείς πληροφορίες, όπως ψεύτικο όνομα καλούντος, οργάνωσης, ηλεκτρονικής διεύθυνσης ή πληροφοριών παρουσίας. Οι επιθέσεις παραποίησης εξουσίας ή δικαιωμάτων αφορούν τη μέθοδο παρουσίασης ψευδών πληροφοριών σε ένα σύστημα ελέγχου ταυτότητας με σκοπό την απόκτηση άδειας πρόσβασης ή την παράκαμψη του συστήματος ελέγχου ταυτότητας. Οι επιθέσεις παραποίησης περιεχομένου αφορούν τη μέθοδο παρουσίασης ψευδούς περιεχομένου ως προερχόμενο από αξιόπιστη πηγή προέλευσης. Το περιεχόμενο αυτό μπορεί να είναι πλαστοπροσωπία φωνής, βίντεο, κειμένου ή εικόνας του καλούντος

- ***Ανεπιθύμητη κλήση ή παρουσία:*** Ως ανεπιθύμητη κλήση (call spam) ορίζεται ένα σύνολο ανεπιθύμητων μηνυμάτων προσπάθειας εκκίνησης συνόδου (αιτήματα INVITE), με σκοπό την απόπειρα δημιουργίας μιας φωνητικής επικοινωνίας ή επικοινωνίας βίντεο. Αν ο χρήστης απαντήσει σε μια τέτοια κλήση, ο επιτιθέμενος προχωρά στην αναμετάδοση των μηνυμάτων του μέσω της ροής μέσων πραγματικού χρόνου. Ως ανεπιθύμητη παρουσία (presence spam) ορίζεται ένα σύνολο ανεπιθύμητων αιτημάτων παρουσίας (π.χ. αιτήματα SIP SUBSCRIBE) με σκοπό την είσοδο του επιτιθέμενου στον "κατάλογο φίλων" ενός χρήστη. Αν κάτι τέτοιο πραγματοποιηθεί, ο επιτιθέμενος μπορεί να προχωρήσει σε ανεπιθύμητες κλήσεις (αιτήματα INVITE)

- ***Ηλεκτρονικό ψάρεμα (Phishing):*** Πρόκειται για μια παράνομη απόπειρα απόκτησης των προσωπικών πληροφοριών ενός χρήστη (για παράδειγμα, ταυτότητα, κωδικός πρόσβασης, αριθμός τραπεζικού λογαριασμού, πληροφορίες πιστωτικής κάρτας), στην οποία ο επιτιθέμενος εμφανίζεται ως αξιόπιστη οντότητα. Μια τυπική μέθοδος εξαπόλυσης μιας τέτοιας επίθεσης είναι η επιλογή των στοχευόμενων χρηστών και η δημιουργία αιτημάτων (π.χ. SIP INVITE) με ψευδή ταυτότητα έμπιστου μέρους για επικοινωνία. Όταν ο στοχευόμενος χρήστης δεχθεί το αίτημα κλήσης, ο επιτιθέμενος παρέχει ψευδείς πληροφορίες (για παράδειγμα, ανακοίνωση της τραπεζικής πολιτικής) και ζητά τα προσωπικά στοιχεία του χρήστη. Ορισμένες πληροφορίες, όπως το όνομα και ο κωδικός πρόσβασης του χρήστη μπορεί να μην είναι άμεσα χρήσιμες για τον επιτιθέμενο, αλλά μπορεί να χρησιμοποιηθούν για πρόσβαση σε περισσότερες πληροφορίες, χρήσιμες για την επίτευξη ολικής κλοπής ταυτότητας

5.3 Δυνατότητες ασφάλειας των πρωτοκόλλων VOIP

Η αποτροπή των επιθέσεων που περιγράφηκαν στην προηγούμενη ενότητα και ως εκ τούτου η προσπάθεια ανάπτυξης ασφαλών συστημάτων VoIP, γίνεται μέσω συγκεκριμένων κανόνων ασφαλείας που εμπεριέχουν τα πρωτόκολλα VoIP (SIP, H.323) οι οποίοι μπορούν να συνδυαστούν με άλλα πρωτόκολλα ασφαλείας (IPSec, SRTP, κλπ.) [38, 40]. Στις επόμενες υποενότητες, θα γίνει παρουσίαση μιας σύντομης επισκόπησης σχετικά με τις δυνατότητες ασφάλειας των κυρίαρχων πρωτοκόλλων στα σύγχρονα συστήματα VoIP.

5.3.1 Δυνατότητες ασφάλειας του πρωτοκόλλου H.323

Η ασφάλεια που μπορεί να παρέχει το H.323 περιγράφεται από το πρότυπο H.235 της ITU-T με τίτλο "Ασφάλεια και κρυπτογράφηση των τερματικών πολυμέσων της σειράς Η" [38, 40]. Σκοπός του συγκεκριμένου προτύπου είναι η εξασφάλιση της αυθεντικότητας, της ιδιωτικότητας και της ακεραιότητας του πρωτοκόλλου H-323. Η χρήση του προτύπου ασφαλείας καθορίζεται μέσα από προφίλ τα οποία ορίζονται από διαφορετικά παραρτήματα του προτύπου:

- ***Παράρτημα D:*** Καθορίζει ένα βασικό και απλό προφίλ ασφάλειας που βασίζεται στον κωδικό πρόσβασης. Το προφίλ παρέχει ασφάλεια βασικού επιπέδου με απλά μέσα, χρησιμοποιώντας κρυπτογραφικές τεχνικές ασφάλειας με βάση τον κωδικό πρόσβασης. Το συγκεκριμένο προφίλ εφαρμόζεται σε περιβάλλοντα όπου κάθε είδους εξοπλισμός H.323 (τερματικό, gatekeeper, πύλη ή MCU) έχει το δικό συμμετρικό κλειδί το οποίο λειτουργεί ως κωδικός πρόσβασης. Ο έλεγχος ταυτότητας και η ακεραιότητα για τα πρωτόκολλα H.225 (RAS, και Q931) και tunnelled H.245 παρέχεται με χρήση του HMAC-SHA1-96 hash, η λειτουργία του οποίου βασίζεται στον κωδικό πρόσβασης. Προαιρετικά, αυτό το βασικό προφίλ ασφάλειας μπορεί να συνδυαστεί με ένα προφίλ ασφάλειας με φωνητική κρυπτογράφηση που χρησιμοποιεί το πρότυπο κρυπτογράφησης δεδομένων (Data Encryption Standard - DES). Οι ροές ήχου μπορούν να κρυπτογραφηθούν χρησιμοποιώντας το προφίλ ασφάλειας κρυπτογράφησης φωνής και τη διαδικασία ανταλλαγής κλειδιών Diffie-Hellman που χρησιμοποιείται για έλεγχο ταυτότητας

- ***Παράρτημα E:*** Περιγράφει ένα προφίλ ασφαλείας που βασίζεται στις ψηφιακές υπογραφές. Οι οντότητες H323 μπορούν να εφαρμόσουν το συγκεκριμένο προφίλ ασφάλειας για περαιτέρω ασφάλεια ή όποτε απαιτείται. Το προφίλ ψηφιακών υπογραφών, εφαρμόζεται συνήθως σε περιβάλλοντα με ενδεχομένως μεγάλο αριθμό τερματικών σταθμών όπου το προφίλ κωδικού πρόσβασης είναι ανέφικτο. Το προφίλ ασφάλειας ψηφιακών υπογραφών ξεπερνά τους περιορισμούς του βασικού προφίλ ασφάλειας του παραρτήματος D

- ***Παράρτημα F:*** Περιγράφει ένα αποδοτικό και επεκτάσιμο υβριδικό προφίλ ασφάλειας που βασίζεται στη χρήση του δημόσιου κλειδιού PKI. Με τον τρόπο αυτό συνδυάζει την ανάπτυξη ψηφιακών υπογραφών του παραρτήματος Ε με το βασικό

προφίλ ασφάλειας του παραρτήματος D. Με το συγκεκριμένο προφίλ, οι ψηφιακές υπογραφές χρησιμοποιούνται μόνο εφόσον είναι απολύτως απαραίτητο, διαφορετικά χρησιμοποιούνται οι εξαιρετικά αποδοτικές συμμετρικές τεχνικές ασφαλείας του βασικού προφίλ. Το υβριδικό προφίλ ασφάλειας ξεπερνά τους περιορισμούς της βασικού προφίλ του παραρτήματος D καθώς και ορισμένα μειονεκτήματα του παραρτήματος E, όπως η ανάγκη για μεγαλύτερο εύρος ζώνης και οι αυξημένες ανάγκες απόδοσης για επεξεργασία

5.3.2 Δυνατότητες ασφάλειας πρωτοκόλλου SIP

Το πρωτόκολλο SIP περιέχει διάφορα χαρακτηριστικά ασφάλειας, όπως η επαλήθευση μηνυμάτων, η κρυπτογράφηση μηνυμάτων, η κρυπτογράφηση μέσων, η ασφάλεια του στρώματος μεταφοράς και η ασφάλεια του στρώματος δικτύου [38, 40]. Από αυτά, μόνο η επαλήθευση μηνυμάτων διασφαλίζεται από το πρωτόκολλο SIP, ενώ τα υπόλοιπα επιτρέπονται από άλλα πρωτόκολλα ασφάλειας, όπως τα S/MIME, SRTP/SRTCP, TLS και IPSec.

- ***Επαλήθευση ή Έλεγχος ταυτότητας μηνύματος:*** Το SIP εξασφαλίζει τον έλεγχο ταυτότητας των μηνυμάτων σηματοδοσίας (REGISTER, INVITE και BYE) ώστε να αποτρέψει τις επιθέσεις υποκλοπής καταχώρησης, τις μη εξουσιοδοτημένες κλήσεις, τις επιθέσεις DoS και τις επιθέσεις ενόχλησης

- ***Κρυπτογράφηση μηνυμάτων:*** Το SIP βασίζεται στο πρωτόκολλο S/MIME (Secure Multipurpose Internet Mail Extensions) για την κρυπτογράφηση των κεφαλίδων των μηνυμάτων σηματοδοσίας (εκτός από τις κεφαλίδες "Via" και "Route"), κάτι που ενισχύει την απ' άκρο σ' άκρο εμπιστευτικότητα και ακεραιότητα και τον έλεγχο ταυτότητας μεταξύ των συμμετεχόντων. Το S/MIME παρέχει την ευελιξία για περισσότερο λεπτομερή προστασία των πληροφοριών κεφαλίδας στα μηνύματα SIP καθώς επιτρέπει την επιλεκτική προστασία των πεδίων των μηνυμάτων SIP

- ***Κρυπτογράφηση μέσων:*** Το πρωτόκολλο SRTP (Secure RTP) εξασφαλίζει την κρυπτογράφηση των πακέτων μέσων με σκοπό την παροχή εγγύησης εμπιστευτικότητας και ακεραιότητας της ανταλλαγής μέσων

- ***Ασφάλεια επιπέδου μεταφοράς (TLS):*** Το πρωτόκολλο TLS παρέχει ασφάλεια στρώματος μεταφοράς των μηνυμάτων SIP (αιτήματα, απαντήσεις). Στην πραγματικότητα, το TLS εξασφαλίζει την κρυπτογράφηση του συνόλου των αιτημάτων και των απαντήσεων SIP, κάτι που εξασφαλίζει την εμπιστευτικότητα και την ακεραιότητα των μηνυμάτων

- ***Ασφάλεια επιπέδου δικτύου:*** Το SIP βασίζεται στη χρήση του IPSec στο στρώμα δικτύου με σκοπό την ενίσχυση της ασφάλεια των επικοινωνιών μέσω δικτύου IP. Για το σκοπό αυτό χρησιμοποιείται κρυπτογράφηση και έλεγχος ταυτότητας των δεδομένων. Το IPSec είναι πολύ χρήσιμο για την παροχή ασφάλειας μεταξύ των οντοτήτων SIP, ειδικά μεταξύ ενός πράκτορα χρήστη (UA) και ενός πληρεξουσίου διακομιστή

5.3.3 Δυνατότητες ασφαλείας πρωτοκόλλου RTP/RTCP

Το ασφαλές πρωτόκολλο RTP (Secure RTP - SRTP) ορίζει ένα προφίλ του πρωτοκόλλου RTP, με σκοπό την παροχή εμπιστευτικότητας, ακεραιότητας αλλά και τον έλεγχο ταυτότητας των ροών μέσων σε εφαρμογές unicast και multicast. Εκτός από την προστασία των πακέτων RTP, το SRTP παρέχει προστασία και στις ροές RTCP. Οι σχεδιαστές του SRTP επικεντρώθηκαν στην ανάπτυξη ενός πρωτοκόλλου που μπορεί να προσφέρει επαρκή προστασία στις ροές μέσων αλλά και να διατηρεί της βασικές ιδιότητες υποστήριξης των ενσύρματων και ασύρματων δικτύων στα οποία μπορεί να υφίστανται περιορισμοί εύρους ζώνης και μεταφορών.

5.4 Συσκευές ασφάλειας VoIP

Εκτός από τις δυνατότητες ασφάλειας των πρωτοκόλλων VoIP, συγκεκριμένες συσκευές έχουν σχεδιαστεί με σκοπό την ενίσχυση της ασφάλειας των συστημάτων VoIP [38, 40]. Η ασφάλεια που μπορούν να παρέχουν οι εν λόγω συσκευές αφορά τον έλεγχο πρόσβασης, την ανίχνευση εισβολών, την προστασία από επιθέσεις DoS, κλπ. Παραδείγματα αυτών των συσκευών θα παρουσιαστούν στις επόμενες υποενότητες.

5.4.1 Τείχος προστασίας VoIP-aware

Το τείχος προστασίας αποτελεί μια από τις βασικότερες συσκευές ασφάλειας σε ένα δίκτυο IP επιτρέποντας την προστασία του εσωτερικού δικτύου από εξωτερικές επιθέσεις. Η γενική λειτουργία του αφορά τον αποκλεισμό ορισμένων τύπων κίνησης βάσει της διεύθυνσης IP προέλευσης/προορισμού, το χρησιμοποιούμενο πρωτόκολλο μεταφοράς (TCP, UDP), τον αριθμό θύρας προέλευσης/προορισμού, την κατεύθυνση της κυκλοφορίας (είσοδος, έξοδος) και τον τύπο κίνησης (RTP, HTTP, SMTPP). Η διαχείριση της κυκλοφορίας VoIP μπορεί να πραγματοποιηθεί μέσω ενός τυπικού ή ενός VoIP-aware τείχους προστασίας. Σε σύγκριση με ένα τυπικό τείχος προστασίας που χειρίζεται πακέτα μόνο στα στρώματα δικτύου και μεταφοράς, ένα VoIP-aware τείχος προστασίας έχει την πρόσθετη δυνατότητα επιθεώρησης και χειρισμού πακέτων VoIP στο στρώμα εφαρμογών [38].

Στην πραγματικότητα, ένα τείχος προστασίας VoIP-aware πραγματοποιεί τις εξής λειτουργίες:

- ***Έλεγχος μηνυμάτων πρωτοκόλλου:*** Αφορά τον έλεγχο της ακεραιότητας των μηνυμάτων πρωτοκόλλου (μηνύματα SIP) και τον αποκλεισμό του originator στην περίπτωση ανίχνευσης τυχόν μη συμβατικών μηνυμάτων

- ***Προστασία από επιθέσεις DoS:*** Αφορά την ανίχνευση οποιουδήποτε μηνύματος πλημμύρας και τον αποκλεισμό του originator για ένα συγκεκριμένο χρονικό διάστημα, βάσει μιας καθορισμένης πολιτικής. Η πολιτική αυτή μπορεί να περιλαμβάνει έναν συγκεκριμένο αριθμό προσπαθειών κλήσης ανά δευτερόλεπτο, μηνυμάτων ανά δευτερόλεπτο, μη έγκυρων μηνυμάτων κ.λπ.

- ***Έλεγχος χρήσης του εύρους ζώνης:*** Αφορά την εκχώρηση μέγιστου εύρους ζώνης για κάθε τερματικό (ή ομάδα) και τον αποκλεισμό οποιουδήποτε τερματικό που προσπαθεί να χρησιμοποιήσει μεγαλύτερο εύρος ζώνης

5.4.2 Μεταφραστής διευθύνσεων δικτύου

Ο μεταφραστής διευθύνσεων δικτύου (Network Address Translation - NAT) αποτελεί μια μέθοδο σύνδεσης πολλών υπολογιστών στο Διαδίκτυο (ή σε οποιοδήποτε άλλο IP δίκτυο) με χρήση μιας και μόνο διεύθυνσης IP [38, 40]. Η μέθοδος αυτή επιτρέπει στους οικιακούς χρήστες και στις μικρές επιχειρήσεις να συνδέσουν το δίκτυό τους με το Διαδίκτυο φτηνά και αποτελεσματικά. Ο μεταφραστής NAT παρέχει αυτόματη προστασία που ομοιάζει αυτής ενός τείχους προστασίας χωρίς ιδιαίτερη ρύθμιση. Η προστασία αυτού του είδους επιτρέπει συνδέσεις που προέρχονται μόνο από το εσωτερικό δίκτυο, πράγμα που σημαίνει ότι, για παράδειγμα, ένας εσωτερικός πελάτης μπορεί να συνδεθεί με εξωτερικό διακομιστή FTP, αλλά ένας εξωτερικός πελάτης δεν μπορεί να συνδεθεί με έναν εσωτερικό διακομιστή FTP, επειδή δεν το επιτρέπει ο NAT. Μια τέτοια σύνδεση θα μπορούσε να πραγματοποιηθεί μέσω της εισερχόμενης χαρτογράφησης, η οποία χαρτογραφεί ορισμένες πολύ γνωστές θύρες TCP (21 για FTP) σε συγκεκριμένες εσωτερικές διευθύνσεις, κάνοντας έτσι υπηρεσίες όπως το FTP ή το Web διαθέσιμες αλλά με ελεγχόμενο τρόπο.

5.4.3 Ελεγκτής συνόρων συνόδου

Ο ελεγκτής συνόρων συνόδου (Session Border Controller - SBC) είναι μια συσκευή ελέγχου που βρίσκεται στο σύνορο δύο συνόδων δικτύου [38, 40]. Μια σύνοδος δικτύου μπορεί να είναι ένα δίκτυο πρόσβασης, ένας πυρήνας δίκτυο, κλπ. Για παράδειγμα, για έναν πάροχο υπηρεσιών VoIP, υπάρχουν δύο σύνορα δικτύου: ένα μεταξύ του δικτύου πρόσβασης του πελάτη και του πυρήνα δικτύου (το δίκτυο του παροχέα υπηρεσιών) και το άλλο μεταξύ του πυρήνα δικτύου και του δικτύου άλλου παρόχου υπηρεσιών (δίκτυο από ομότιμους χρήστες).

Ο ρόλος του ελεγκτή ενός συνόρου συνόδου είναι η επίλυση των όποιων θεμάτων μπορούν να υπάρχουν στα σύνορα αυτά, όπως αυτά της διαλειτουργικότητας και της ασφάλειας. Τα θέματα διαλειτουργικότητας οφείλονται βασικά στην αλληλεπίδραση των συνόδων δικτύου που χρησιμοποιούν διαφορετικές συσκευές και πρωτόκολλα. Τα θέματα ασφάλειας υφίστανται κυρίως λόγω της έκθεσης μιας συνόδου δικτύου (για παράδειγμα του πυρήνα δικτύου) σε άλλες συνόδους δικτύου (ένα δίκτυο ομότιμων χρηστών ή ένα δίκτυο πρόσβασης πελατών), την οποία μπορεί να εκμεταλλευτεί κάποιος κακόβουλος χρήστης δημιουργώντας μια σύνοδο δικτύου με σκοπό την επίθεση στους πόρους (διακομιστή VoIP, διακομιστή μεσολάβησης, κ.λπ.) άλλης συνόδου δικτύου.

6 Εφαρμογές τεχνολογίας VoIP

6.1 Εφαρμογές και υπηρεσίες VoIP

Για τους μεμονωμένους χρήστες, οι υπηρεσίες VoIP είναι συχνά φθηνότερες από την παραδοσιακή δημόσια υπηρεσία τηλεφωνικού δικτύου (PSTN) και μπορούν να αφαιρέσουν τους όποιους γεωγραφικούς περιορισμούς των παραδοσιακών τηλεφωνικών συσκευών, καθώς, για παράδειγμα, μια τηλεφωνική συσκευή με κωδικό αριθμό περιοχής της Νέας Υόρκης μπορεί να καλεί στο Τόκιο και η χρέωση να είναι τοπικής κλήσης. Για τις επιχειρήσεις, το VoIP ενσωματώνει τις ξεχωριστές γραμμές τηλεφωνίας και δεδομένων, διοχετεύοντας και τους δύο τύπους κίνησης μέσω του δικτύου IP. Με τον τρόπο αυτό, παρέχεται στον χρήστη ένα είδος τηλεφωνίας με μια σειρά προηγμένων υπηρεσιών.

Τα softphone είναι λογισμικά πελάτη για την πραγματοποίηση και λήψη κλήσεων φωνής και βίντεο, μέσω του δικτύου IP, που είναι εφοδιασμένα με τις τυπικές λειτουργίες των περισσότερων παραδοσιακών τηλεφωνικών συσκευών και συνήθως επιτρέπουν την ενσωμάτωση των τηλεφώνων VoIP και USB. Τα περισσότερα softphone λειτουργούν με βάση το ανοικτό πρωτόκολλο SIP που υποστηρίζει διάφορους codec [41].

Η δημοφιλέστερη εφαρμογή της τηλεφωνίας VoIP, το Skype, λειτουργεί με ιδιωτικό πρωτόκολλο δικτύωσης, αλλά το πρόσθετο λογισμικό τηλεφωνικού συστήματος (PBX), μπορεί να επιτρέψει σε ένα τηλεφωνικό σύστημα που βασίζεται σε SIP να συνδεθεί στο δίκτυο Skype [42]. Το Skype οδήγησε στην δημιουργία μιας πλειάδας εφαρμογών VoIP, που επιτρέπουν την ουσιαστική αντικατάσταση των παραδοσιακών τηλεφωνικών δικτύων με ψηφιακές φωνητικές κλήσεις μέσω του Διαδικτύου, άμεσα μηνύματα και τηλεδιασκέψεις. Οι υπηρεσίες των συστημάτων VoIP, εκτός από τα στελέχη επιχειρήσεων που χρησιμοποιούν εφαρμογές telepresence και τηλεδιάσκεψης για να μειώσουν τα έξοδα ταξιδίου, μπορούν να χρησιμοποιηθούν από σχεδόν κάθε χρήστη του Διαδικτύου, όπως οι online gamers που συνδυάζουν ένα εύκολο μέσο επικοινωνίας με το παιχνίδι ή μέλη οικογενειών που βρίσκονται μακριά και αναζητούν ένα μέσο για να έρθουν σε επαφή με τα αγαπημένα τους πρόσωπα, χωρίς αυτή η επικοινωνία να τους στοιχίσει τα μαλλιά της κεφαλής τους [43].

Τα σύγχρονα προγράμματα ηλεκτρονικής συνομιλίας περιλαμβάνουν επικοινωνίες φωνής και βίντεο. Άλλες εφαρμογές λογισμικού VoIP περιλαμβάνουν διακομιστές διασκέψεων, συστήματα ενδοεπικοινωνίας, διακομιστές εγγραφής κλήσεων, υπαγόρευση κλήσεων, υπηρεσίες εικονικής ανταλλαγής συναλλάγματος (FXO) και υπηρεσίες προσαρμοσμένου λογισμικού τηλεφωνίας, που υποστηρίζουν ταυτόχρονα συστήματα VoIP και PSTN, όπως τα συστήματα IVR (Interactive Voice Response) [44]. Κάποιες από τις εφαρμογές VoIP λειτουργούν με βάση το Διαδίκτυο, οι περισσότερες όμως είναι αυτόνομες εφαρμογές.

Στις επόμενες ενότητες θα παρουσιαστούν οι δημοφιλέστερες σύγχρονες εφαρμογές VoIP.

6.2 Skype

Το Skype διαθέτει τεράστια βάση χρηστών, με περισσότερα από 300 εκατομμύρια συνδρομητές. Οι δωρεάν ομιλίες ήχου και βίντεο Skype-to-Skype, οι ομαδικές κλήσεις, καθώς και τα μηνύματα κειμένου και φωνής είναι υπηρεσίες που μπορούν να καλύψουν τις ανάγκες επικοινωνίας του μέσου χρήστη. Ο χρήστης έχει τη δυνατότητα να γραφτεί στη συνδρομητική εφαρμογή Skype Credit και να ενεργοποιήσει πιο προηγμένα εργαλεία και υπηρεσίες, όπως προώθηση κλήσεων, αποστολή μηνυμάτων SMS, αναγνωριστικό καλούντος, αριθμό Skype, κλήση σταθερού δικτύου ή κινητά τηλέφωνα σε όλο τον κόσμο και τηλεδιάσκεψη. Επιπλέον, το Skype for Business μπορεί να ενσωματωθεί στο Office 365 και να λειτουργήσει μέσω ενός διακομιστή Lync, οπότε τα μηνύματα και οι κλήσεις πραγματοποιούνται εντός του intranet της επιχείρησης, εκτός και αν η επικοινωνία γίνεται προς ή από κάποιο εξωτερικό χρήστη [43].

Τα κυριότερα χαρακτηριστικά του Skype είναι τα εξής [45]:

- ***Λειτουργικό σύστημα:*** Linux(περιορισμένης λειτουργικότητας), macOS, Windows (2000-XP-Vista-7-Mobile), BREW, Windows Phone, Android, iPhone, PSP
- ***Άδεια χρήσης:*** Λογισμικό κλειστού κώδικα
- ***Κόστος:*** Δωρεάν
- ***Πρωτόκολλο:*** Το πρωτόκολλο SIP δεν υποστηρίζεται απευθείας ούτε από την εφαρμογή αλλά ούτε και από το δίκτυο Skype. Η σύνδεση στο δίκτυο Skype μέσω SIP είναι δυνατή μόνο με χρήση πρόσθετου λογισμικού PBX του Skype Connect και εναλλακτικού λογισμικού/hardware υλικού πελάτη SIP
- ***Codec:*** SILK
- ***Κωδικοποίηση:*** TLS
- ***Μέγιστος αριθμός ομότιμων μελών συνδιάσκεψης (χρηστών):*** 25 (από την έκδοση 3.6.0.216 και μετά)

- ***Δυνατότητες εφαρμογής:*** Συνδιάσκεψη, μεταφορά αρχείων και βίντεο, φωνητικό ταχυδρομείο, συνδέσεις παραδοσιακών τ/φ συσκευών με το Skype, επιπρόσθετες P2P επεκτάσεις (games, whiteboard, κλπ.) (ανάλογα με την πλατφόρμα)
- ***Τελευταίες εκδόσεις:*** Windows UWP (14.36.52.0 στις 13 Δεκέμβρη 2018), Windows desktop (8.36.0.52 στις 13 Δεκέμβρη 2018), macOS (8.34.0.78 στις 13 Νοέμβρη 2018), Linux (8.34.0.78 στις 13 Νοέμβρη 2018), Android 6 και μεταγενέστερο (8.36.0.76 στις 5 Ιανουαρίου 2019), iOS & watchOS (8.35.0.71 στις 3 Δεκέμβρη 2018)

6.3 ooVoo

Το ooVoo είναι μια υπηρεσία άμεσων μηνυμάτων και φωνητικών/βίντεο κλήσεων, που παρέχει άμεση ανταλλαγή μηνυμάτων, συνομιλία με κείμενο, κλήσεις βίντεο και τηλεδιάσκεψη 12 συμμετεχόντων. Άλλες ενδιαφέρουσες λειτουργίες της εφαρμογής είναι η δυνατότητα πρόσκλησης χρηστών που δεν χρησιμοποιούν το ooVoo σε κλήσεις, η δημιουργία κουμπιού προγράμματος περιήγησης “Call Me”, καθώς και η κοινή χρήση αρχείων και οθόνης, υπηρεσία που είναι ιδιαίτερα χρήσιμη για συνεργατική εργασία και online συναντήσεις. Οι συνδρομητές με χρήση προπληρωμένης κάρτας, έχουν τη δυνατότητα πραγματοποίηση κλήσεων σε σταθερά, σε περισσότερες από 70 χώρες (με λογική χρέωση), καθώς και τη σύνδεση χρηστών σταθερής τηλεφωνίας σε κλήσεις συνδιάσκεψης (μόνο για ήχο). Τέλος, η υπηρεσία λειτουργεί και σε Android και iOS φορητές συσκευές [43].

Τα κυριότερα χαρακτηριστικά του ooVoo είναι τα εξής [45]:

- ***Λειτουργικό σύστημα:*** macOS, iOS, Windows, Android
- ***Άδεια χρήσης:*** Λογισμικό κλειστού κώδικα
- ***Κόστος:*** Δωρεάν
- ***Πρωτόκολλο:*** SIP, RTP και RTCP
- ***Μέγιστος αριθμός ομότιμων μελών συνδιάσκεψης (χρηστών):*** 12
- ***Δυνατότητες εφαρμογής:*** Ενσωμάτωση βιβλίου διευθύνσεων, εγγραφή/εξαγωγή κλήσεων, σίγαση, αναμονή, αναγνώριση καλούντος
- ***Τελευταία έκδοση:*** 4.2.9 τον Μάρτη 2013

6.4 Viber

Η εφαρμογή Viber εκτός από τις πλατφόρμες iOS και Android, μπορεί να χρησιμοποιηθεί και από τον προσωπικό υπολογιστή ή το laptop των χρηστών, με την προϋπόθεση ότι έχει δημιουργηθεί λογαριασμός Viber στο κινητό τηλέφωνο ή το tablet. Στη συνέχεια, ο συγχρονισμός των επαφών και του ιστορικού κλήσεων γίνεται αυτόματα και στιγμιαία. Η εφαρμογή υποστηρίζει μια υπηρεσία δυναμικής μεταφοράς κλήσης, η οποία επιτρέπει την εναλλαγή λειτουργίας της εφαρμογής από τον υπολογιστή στο κινητό τηλέφωνο και το αντίστροφο, κατά την πραγματοποίηση, λήψη ή και κατά τη διάρκεια μιας κλήσης. Υποστηρίζεται επίσης η δυνατότητα λειτουργίας ομαδικής συνομιλίας και κλήσης σε όλες τις εκδόσεις της εφαρμογής [43].

Τα κυριότερα χαρακτηριστικά του Viber είναι τα εξής [45]:

- ***Λειτουργικό σύστημα:*** Linux, macOS, Windows, Android, Bada, BlackBerry OS, iOS, Series 40, Symbian, Windows Phone
- ***Άδεια χρήσης:*** Λογισμικό κλειστού κώδικα
- ***Δυνατότητες εφαρμογής:*** Μηνύματα κειμένου, εικόνας και βίντεο προς όλους, φωνητικές κλήσεις μόνο σε iPhone, Android και Windows Phone της Microsoft (ανάλογα με την πλατφόρμα)
- ***Τελευταίες εκδόσεις:*** Android (WhatsApp 9.5.0.6 στις 21 Αυγούστου 2018), iOS (8.7.1 στις 21 Απριλίου 2018), Windows Mobile (6.6.1 στις 26 Απριλίου 2018), BlackBerry 10 OS (4.3.0.728 στις 23 Απριλίου 2014)

6.5 Jitsi

Το Jitsi είναι ένα ελεύθερο και ανοικτού κώδικα πρόγραμμα Java, για VoIP και ανταλλαγή άμεσων μηνυμάτων. Εκτελείται σε Windows, Mac, και τις περισσότερες πλατφόρμες Linux. Το Jitsi πληροί της έξι από τις επτά προϋποθέσεις ασφαλής αποστολής μηνυμάτων του Electronic Frontier Foundation (EFF). Το Jitsi βέβαια, συνιστάται για πιο έμπειρους χρήστες που δεν έχουν προβλήματα στη μεταβολή αρχείων ρυθμίσεων και κλειδιών κρυπτογράφησης, καθώς μόνο με τον τρόπο αυτό

είναι δυνατή η απόκτηση μιας προσαρμοσμένης εμπειρίας ασφάλειας από κακόβουλες επιθέσεις, όπως το snooping [43].

Τα κυριότερα χαρακτηριστικά του Jitsi είναι τα εξής [45]:

- ***Λειτουργικό σύστημα:*** Linux, macOS, Windows (όλα υποστηριζόμενα από Java), καθώς και Android (πειραματικό στάδιο)
- ***Άδεια χρήσης:*** Apache
- ***Κόστος:*** Δωρεάν
- ***Πρωτόκολλο:*** SIP-SIMPLE, XMPP-Jingle STUN ICE, TURN
- ***Codec:*** SILK, G.722, Speex, Opus, G.711 (PCMU/PCMA), iLBC, GSM, G.729, H.264, H.263, VP8
- ***Κωδικοποίηση:*** ZRTP, SRTP, OTR, TLS
- ***Δυνατότητες εφαρμογής:*** Μηνύματα κειμένου, τηλεφωνία ήχου-βίντεο, καταγραφή κλήσεων
- ***Τελευταία έκδοση:*** 2.10 στις 5 Φλεβάρη 2017

6.6 MicroSIP

Το MicroSIP είναι μια δωρεάν φορητή εφαρμογή ανοικτού κώδικα, που υποστηρίζεται από C και C ++. Το MicroSIP διαθέτει μια πολύ μινιμαλιστική προσέγγιση σε κάθε πτυχή. Το μέγεθος της εφαρμογής είναι μικρότερο από 2,5MB και η χρήση της μνήμης RAM είναι μικρότερη από 5MB. Έχει ρυθμιζόμενη κρυπτογράφηση TLS/STRP, για χρήστες με γνώμονα την προστασία της ιδιωτικότητας. Η διαμόρφωσή του αποθηκεύεται σε ένα μόνο αρχείο INI, καθιστώντας την προσαρμογή και τη φορητότητα σχετικά εύκολη για τους έμπειρους χρήστες. Το MicroSIP υποστηρίζει φωνητικές/βίντεο κλήσεις, αλλά η διεπαφή Spartan της MicroSIP δεν υποστηρίζει περιττά χαρακτηριστικά, όπως emojis και αυτοκόλλητα. Είναι μια εφαρμογή που πραγματικά συνιστάται για πιο προχωρημένους χρήστες [43].

Τα κυριότερα χαρακτηριστικά του MicroSIP είναι τα εξής [45]:

- ***Λειτουργικό σύστημα:*** Windows
- ***Άδεια χρήσης:*** GPL
- ***Κόστος:*** Δωρεάν
- ***Πρωτόκολλο:*** SIP, STUN, ICE, SIMPLE
- ***Codec:*** Speex, iLBC, GSM, G.711, G.722, G.729, SILK, Linear PCM
- ***Κωδικοποίηση:*** TLS, SRTP
- ***Δυνατότητες εφαρμογής:*** φωνητικές/βίντεο κλήσεις
- ***Τελευταία έκδοση:*** 3.9.18 στις 28 Σεπτέμβρη 2018

6.7 Linphone

Το Linphone είναι μία ανοιχτή εφαρμογή πελάτη VoIP και SIP, που αναπτύχθηκε αρχικά για πλατφόρμες Linux, αλλά τώρα υποστηρίζει και τις Windows, Mac, iOS και Android. Μπορεί να χρησιμοποιηθεί για φωνητικές/βίντεο κλήσεις και μπορεί να εκτελεστεί σε πρόγραμμα περιήγησης. Το Linphone έχει σχεδιαστεί για να υποστηρίζει ηχητικές και HD κλήσεις βίντεο, διαχείριση και μεταφορά κλήσεων, κλήσεις συνδιάσκεψης, κοινή χρήση αρχείων και άλλα [43].

Τα κυριότερα χαρακτηριστικά του Linphone είναι τα εξής [45]:

- ***Λειτουργικό σύστημα:*** Linux, Windows, macOS, Android, iPhone, BlackBerry
- ***Άδεια χρήσης:*** GPL
- ***Κόστος:*** Δωρεάν

- ***Πρωτόκολλο:*** SIP
- ***Codec:*** Speex, Opus, G711, GSM, G.722, VP8 (WebM), H263, MPEG4, Theora and H264 (plugin)
- ***Κωδικοποίηση:*** TLS, SRTP, ZRTP
- ***Δυνατότητες εφαρμογής:*** Βίντεο, IM, STUN, εναλλακτική υποστήριξη IPv6 ή IPv4, IPv6 P2P (μετά από την έκδοση 3.5.1-2)
- ***Τελευταία έκδοση:*** 3.11.1 στις 10 Μάρτη 2017

6.8 Discord

Το Discord (Desktop, Android, iOS) είναι μια εφαρμογή VoIP που χρησιμοποιείται κατά κόρο από τους gamers, αλλά αποτελεί και την προτιμώμενη επιλογή πολλών Twich streamers. Ένας λόγος για τον οποίο οι gamers προτιμούν το Discord είναι οι ελάχιστες απαιτήσεις του, καθώς δεν είναι απαραίτητη η λήψη κανενός προγράμματος ή η σύνδεση με κάποιον διακομιστή, αφού όλες οι υπηρεσίες του Discord μπορούν να ρυθμιστούν και να εκτελεστούν χρησιμοποιώντας το πρόγραμμα περιήγησης. Το Discord διαθέτει επίσης πρόσθετα χαρακτηριστικά ασφάλειας, όπως η κρυπτογράφηση και απόκρυψη της διεύθυνσης IP, API Twitch και ενσωμάτωση με το Steam, στοιχεία που το καθιστούν ελκυστικό για τους gamers και τους streamers. Οι προγραμματιστές του Discord υπόσχονται να προσθέσουν περισσότερες δυνατότητες, όπως βίντεο κλήσεις, και μια premium κατηγορία Discord Nitro που θα παρέχει πρόσθετες προσαρμογές, όπως προσαρμοσμένα emote και GIF avatar [43].

Τα κυριότερα χαρακτηριστικά του Discord είναι τα εξής [45]:

- ***Λειτουργικό σύστημα:*** macOS, Android, iOS, Windows, Linux
- ***Άδεια χρήσης:*** Λογισμικό κλειστού κώδικα
- ***Κόστος:*** Δωρεάν, εγγραφή Premium “Nitro” για πρόσθετες δυνατότητες
- ***Codec:*** Opus
- ***Κωδικοποίηση:*** TLS
- ***Μέγιστος αριθμός ομότιμων μελών συνδιάσκεψης (χρηστών):*** 5000
- **Δυνατότητες εφαρμογής:** IM και κοινή χρήση αρχείων εντός παιχνιδιού
- ***Τελευταία έκδοση:*** 02.01.2018 στη 1 Φλεβάρη 2018

6.9 TeamSpeak 3

Το TeamSpeak 3 (Desktop, Android, iOS) είναι μια άλλη κορυφαία εφαρμογή παιχνιδιών VoIP, που χρησιμοποιεί το μοντέλο πελάτη-διακομιστή για να παράγει κάτι παρόμοιο με ένα κανάλι IRC με δυνατότητα φωνής, σε συνδυασμό με σύστημα δικαιωμάτων χρήστη. Κάτι τέτοιο επιτρέπει σε ορισμένους χρήστες την πραγματοποίηση φωνητικών τηλεδιασκέψεων, την ανταλλαγή μηνυμάτων, αλλά και τη δυνατότητα πρόσκλησης και αποκλεισμού άλλων χρηστών. Το TeamSpeak 3 προσφέρει δωρεάν διακομιστές που μπορούν να φιλοξενήσουν μέχρι και 32 ταυτόχρονους χρήστες. Στην περίπτωση συνδρομής, οι χρήστες που μπορούν να υποστηριχθούν ταυτόχρονα φτάνουν τους 512 και η υποστήριξη αυτή γίνεται από δύο εικονικούς διακομιστές. Η εφαρμογή, στην προσπάθειά της να προσελκύσει και άλλους, πλην των gamer, χρήστες, όπως εμπορικούς και εκπαιδευτικούς, έχει ξεκινήσει την εισαγωγή χαρακτηριστικών όπως η πιστοποίηση PPK, η κρυπτογράφηση AES και η υποστήριξη πλατφόρμας Android και iOS [43].

Τα κυριότερα χαρακτηριστικά του TeamSpeak 3 είναι τα εξής [45]:

- ***Λειτουργικό σύστημα:*** Linux, Windows, macOS, FreeBSD, Android, iOS
- ***Άδεια χρήσης:*** Λογισμικό κλειστού κώδικα
- ***Κόστος:*** Δωρεάν
- ***Codec:*** CELT, Speex, Opus
- ***Μέγιστος αριθμός ομότιμων μελών συνδιάσκεψης (χρηστών):*** 32 (χωρίς άδεια χρήσης), 512 (με άδεια χρήσης μικρών δυνατοτήτων, 2000 (με άδεια χρήσης με πλήρεις δυνατότητες)
- ***Δυνατότητες εφαρμογής:*** Ταυτόχρονη συνδιάσκεψη διακομιστών με 3D ηχητικά εφέ, σύστημα κλιμακούμενων δικαιωμάτων, τείχος προστασίας μεταφοράς αρχείων, κοινή χρήση αρχείων εντός παιχνιδιών για παιχνίδια DirectX & OpenGL, λίστα παγκόσμιων δημόσιων διακομιστών, σύστημα plugin
- ***Τελευταία έκδοση:*** 3.1.8

6.10 Mumble

Το Mumble είναι μια δωρεάν εφαρμογή VoIP ανοιχτού κώδικα που είναι συμβατή με πολλές πλατφόρμες και διαθέτει εξαιρετική ποιότητα ήχου και μικρή καθυστέρηση μεταφοράς δεδομένων (latency). Ένα από τα ιδιαίτερα χαρακτηριστικά του, που αποτελεί πόλο έλξης για τους gamers είναι ο ήχος θέσης, χαρακτηριστικό που δίνει

την αίσθηση 3D ήχου (ο ήχος ακούγεται δυνατότερα στο κοντινό περιβάλλον του παίκτη και χαμηλότερα στο γύρω περιβάλλον του). Η επικοινωνία είναι πάντα κρυπτογραφημένη, ενώ η εφαρμογή διαθέτει κι ένα εκτεταμένο σύστημα δικαιωμάτων χρήστη, που επιτρέπει στους διαχειριστές των διακομιστών να παραχωρούν προνόμια και ρόλους στους χρήστες, για να βοηθήσουν στη διαχείριση ενός διακομιστή [43].

Τα κυριότερα χαρακτηριστικά του Mumble είναι τα εξής [45]:

- ***Λειτουργικό σύστημα:*** Linux, macOS, iOS, Windows, Android
- ***Άδεια χρήσης:*** BSD
- ***Κόστος:*** Δωρεάν
- ***Πρωτόκολλο:*** ICE
- ***Codec:*** CELT, Speex, Opus
- ***Κωδικοποίηση:*** TLS & OCB-AES128
- ***Μέγιστος αριθμός ομότιμων μελών συνδιάσκεψης (χρηστών):*** απεριόριστος (με μόνο όριο το εύρος ζώνης και τη μνήμη του διακομιστή)
- ***Δυνατότητες εφαρμογής:*** Συνομιλία με (περιορισμένο) ενσωματωμένο κώδικα HTML, αυτόματος έλεγχος κέρδους, πολύ χαμηλή καθυστέρηση, λίστες ελέγχου πρόσβασης για τη διαχείριση χρηστών, προσαρμόσιμη μεταφορά αρχείων εντός παιχνιδιού για παιχνίδια OpenGL και DirectX, κατευθυντικός ήχος, υποστήριξη Plugin, ενσωματωμένα κανάλια, ακύρωση ηχούς στην περίπτωση χρήσης ακουστικών, λίστα παγκόσμιων δημόσιων διακομιστών, υποστήριξη Logitech G15, push-to-talk και ενεργοποίηση φωνής
- ***Τελευταία έκδοση:*** 1.2.19 στις 27 Γενάρη 2017

6.11 TeamTalk

Το TeamTalk είναι ένα δωρεάν σύστημα διασκέψεων VoIP και φωνητικών κλήσεων, που υποστηρίζεται από τα Windows, Mac και τις πιο διαδεδομένες πλατφόρμες Linux. Για να μπορέσουν να το χρησιμοποιήσουν οι χρήστες, πρέπει να

έχουν έναν λογαριασμό πελάτη αλλά και έναν ρυθμισμένο διακομιστή. Ισχυρός πόλος έλξης του TeamTalk είναι η έκδοση προσβασιμότητας, η οποία επιτρέπει στους χρήστες με προβλήματα όρασης, να χρησιμοποιούν ευκολότερα τις συσκευές ανάγνωσης οθόνης και εφαρμογές κειμένου με ομιλία, ώστε να μπορούν να επικοινωνούν με άλλους χρήστες του TeamTalk [43].

Τα κυριότερα χαρακτηριστικά του TeamTalk είναι τα εξής [45]:

- ***Λειτουργικό σύστημα:*** Linux, macOS, iOS, Windows, Android
- ***Άδεια χρήσης:*** Λογισμικό κλειστού κώδικα
- ***Κόστος:*** Δωρεάν
- ***Πρωτόκολλο:*** Κλειστού κώδικα
- ***Codec:*** WebM, Speex, Opus
- ***Μέγιστος αριθμός ομότιμων μελών συνδιάσκεψης (χρηστών):*** 1000
- ***Δυνατότητες εφαρμογής:*** Βίντεο, κοινή χρήση αρχείων, κοινή χρήση επιφάνειας εργασίας, ροή αρχείων πολυμέσων (MP3, AVI)
- ***Τελευταία έκδοση:*** 5.1.3 τον Μάη 2016

Συμπεράσματα

Η βασική ιδέα της παρούσας πτυχιακής εργασίας είναι η κατανόηση της τεχνολογίας VoIP εξετάζοντας τη βασική δομή, τις αρχές λειτουργίας, τα θεμελιώδη μέρη καθώς και κάποιες από τις σημαντικότερες εφαρμογές της. Η εξέταση της βασικής δομής της τεχνολογίας γίνεται μέσω της σύγκρισής της με τα παραδοσιακά δίκτυα μεταγωγής κυκλώματος (PSTN) και της παρουσίασης των ανώτερων χαρακτηριστικών της. Η τεχνολογία VoIP χρησιμοποιεί τις δυνατότητες μεταγωγής πακέτων του Διαδικτύου, για την παροχή τηλεφωνικών υπηρεσιών. Μεγάλο πλεονέκτημα της μεταγωγής πακέτων είναι ότι το εύρος ζώνης που καταλαμβάνει μεγάλος αριθμός τηλεφωνικών κλήσεων VoIP, αντιστοιχεί σε αυτό μιας μόνο κλήσης PSTN. Επίσης, στη μεταγωγή πακέτων, αντί η δρομολόγηση των δεδομένων να γίνεται μέσω μιας μισθωμένης γραμμής, τα πακέτα δεδομένων ρέουν μέσω πολλαπλών πιθανών διαδρομών ενός χαοτικού δικτύου.

Στα πλαίσια της παρούσας πτυχιακής εργασίας, έγινε παρουσίαση και σύγκριση των πρωτοκόλλων σηματοδότησης VoIP, H.323 (πρότυπο ITU-T) και SIP (Πρότυπο IETF). Παρά το γεγονός ότι και τα δύο πρωτόκολλα σχεδιάστηκαν για εφαρμογές VoIP, ο βασικός τους στόχος είναι πολύ διαφορετικός. Στόχος του H.323 είναι η διαχείριση των φωνητικών κλήσεων και των κλήσεων πολυμέσων, αλλά και διαφόρων άλλων συμπληρωματικών υπηρεσιών. Αντίθετα, το SIP έχει σχεδιαστεί ως πρωτόκολλο γενικής συναλλαγής εκκίνησης συνόδου, χωρίς να περιορίζεται σε συγκεκριμένες υπηρεσίες μέσων, όπως ήχου ή βίντεο. Αν και οι περισσότερες εφαρμογές χρησιμοποιούν το H.323, το SIP μπορεί να θεωρηθεί πολύ καλύτερο πρωτόκολλο, δεδομένης της απλότητας και της επεκτασιμότητάς του. Για το λόγο αυτό, για τις περισσότερες σύγχρονες δωρεάν εφαρμογές VoIP, το SIP αποτελεί την κυρίαρχη τεχνολογία, με τις εφαρμογές soft phone SIP να προτιμώνται κατά κόρο από τους χρήστες.

Στα συστήματα VoIP, η μεταφορά των φωνητικών δεδομένων σε πραγματικό χρόνο απαιτεί την ύπαρξη πρωτοκόλλων πραγματικού χρόνου. Τα πρωτόκολλα αυτά μπορούν να χρησιμοποιηθούν με τα πρωτόκολλα H.323 και SIP. Τα πρωτόκολλα RTP και RTCP χρησιμοποιούνται για τη μεταφορά και τον έλεγχο των δεδομένων σε πραγματικό χρόνο. Αντίθετα, το πρωτόκολλο RTSP παρέχει ελεγχόμενη παράδοση των ροών πολυμέσων. Επίσης, τα συστήματα VoIP που χρησιμοποιούν SIP, περιέχουν και άλλα δύο πρωτόκολλα τα οποία συνδυάζονται με αυτό, όπως το πρωτόκολλο διαφήμισης συνόδου (SAP) και το πρωτόκολλο περιγραφής συνόδου (SDP).

Ο εξοπλισμός ενός συστήματος VoIP αποτελείται από επί μέρους στοιχεία, όπως ο εξοπλισμός τελικού χρήστη, ο εξοπλισμός δικτύου, οι πύλες και οι διακομιστές. Ο εξοπλισμός τελικού χρήστη χρησιμοποιείται για την πρόσβαση στο σύστημα VoIP και την επικοινωνία μεταξύ των χρηστών. Οι διακομιστές σηματοδοσίας ελέγχουν τη δρομολόγηση των μηνυμάτων σηματοδοσίας στο στρώμα εφαρμογών, για την πραγματοποίηση μιας κλήσης VoIP. Η σύνδεση με το δίκτυο μπορεί να είναι

καλωδιακή ή ασύρματη. Από τη στιγμή που η σύγχρονη επικοινωνία βασίζεται στην φορητότητα και την εύκολη πρόσβαση στην πηγή, η τεχνολογία VoIP έχει στραφεί προς αυτή την κατεύθυνση, με αποτέλεσμα, ο εξοπλισμός τελικού χρήστη να μπορεί να αποτελείται από ένα κινητό τηλέφωνο, ένα tablet ή μια εφαρμογή soft phone, η οποία εγκαθίσταται σε έναν υπολογιστή ή σε ένα κινητό τηλέφωνο. Οι εφαρμογές soft phone συνεχώς εξελίσσονται και η δημοτικότητά τους αυξάνεται, αφού, οι περισσότερες τουλάχιστον, είναι δωρεάν, μπορούν να εγκατασταθούν απλούστατα στα smart phone και παρουσιάζουν ευελιξία και εύχρηστα χαρακτηριστικά, σύμφωνα με τη σύγχρονη εποχή. Λόγω, όλων αυτών των χαρακτηριστικών, οι εφαρμογές soft phone SIP προτιμώνται στα σύγχρονα συστήματα VoIP.

Κατά τη δημιουργία της τεχνολογίας VoIP, τα θέματα ποιότητας υπηρεσίας (QoS) δεν ελήφθησαν υπόψη και αυτό επειδή η τεχνολογία IP παραμένει αναποτελεσματική στην υποστήριξη της κυκλοφορίας δεδομένων με τους αυστηρούς περιορισμούς της ποιότητας QoS, πόσο μάλλον όταν αυτά τα δεδομένα αφορούν φωνή και βίντεο. Έτσι, τα θέματα ποιότητας QoS μπορούν να θεωρηθούν ως από τα πιο σοβαρά κατά την ανάπτυξη ενός συστήματος VoIP. Τα θέματα QoS αποτέλεσαν ένα ακόμα ζήτημα στην ανάλυση της τεχνολογίας VoIP, στα πλαίσια της παρούσας εργασίας. Αρχικά έγινε μια ανάλυση των θεμάτων ποιότητας QoS που σχετίζονται με τη χρήση της τεχνολογίας δικτύωσης IP, στη μετάδοση των φωνητικών δεδομένων, καθώς και την καθαρότητα της μεταφοράς της φωνής μέσω τέτοιων δικτύων. Τέλος, παρουσιάστηκαν κάποιοι από τους μηχανισμούς QoS που μπορούν να αντιμετωπίσουν τα όποια θέματα ποιότητας και αφορούν την ευκρίνεια φωνής, την καθυστέρηση των μεταφερόμενων φωνητικών πακέτων, την απώλεια των πακέτων αυτών και την εμφάνιση του φαινομένου jitter.

Η ασφάλεια ενός συστήματος VoIP, αποτελεί ένα ακόμα θέμα, το οποίο αναλύθηκε στα πλαίσια της παρούσας εργασίας. Μια τέτοια ασφάλεια θα πρέπει να ξεκινάει από το εσωτερικό δίκτυο, το οποίο θα πρέπει να προστατεύεται από τις πιθανές απειλές των συνδεδεμένων σε αυτό χρηστών. Η οποιαδήποτε πολιτική ασφάλειας θα πρέπει να περιλαμβάνει επίσης όλες τις ανάγκες ενός συστήματος VoIP. Το φορτίο του συστήματος VoIP θα πρέπει να εξυπηρετείται από το δίκτυο και τους εμπλεκόμενους διακομιστές, διασφαλίζοντας την ύπαρξη και τη διάθεση των κατάλληλων πόρων. Η διεξαγωγή της ανάλυσης κινδύνου καθενός στοιχείου που αποτελεί μέρος του εξοπλισμού ενός συστήματος VoIP, μπορεί να καθορίσει τόσο τα τρωτά σημεία, όσο και τις πιθανές απειλές καθενός από αυτά. Επίσης, μια τέτοια ανάλυση θα μπορέσει να παρέχει και όλες τις απαραίτητες πληροφορίες που απαιτούνται, για τον καθορισμό των κατάλληλων μέτρων ενάντια στις πιθανές επιθέσεις κατά του συστήματος. Το κλειδί για την επιτυχημένη ανάπτυξη οποιουδήποτε συστήματος VoIP, έγκειται στην ύπαρξη σωστής ισορροπίας μεταξύ της ασφάλειας και των αναγκών του συστήματος.

Βιβλιογραφία

[1] Pourghasem J., Karimi S., & Edalatpanah S. (2012) "A Survey of Voice Over Internet Protocol (VOIP) Technology", IJCMSA: Vol. 6, No. 3-4, pp. 53– 62

[2] Sonkar S. K., Singh R., Chauhan R., & Singh A. P. (2012) "A Review Paper: Security on Voice over Internet Protocol from Spoofing attacks", International Journal of Advanced Research in Computer and Communication Engineering, Vol.1, Issue 3, pp: 153-160

[3] Igbal N. & Cheema F. M. (2009) "QoS of VoIP in wireless networks", Degree of Masters in Electrical Engineering with Emphasis on Telecommunication, Blekinge Institute of Technology

[4] Phithakkitnukoon S., Dantu R., & Baatarjav E. A. (2008) "VoIP Security—Attacks and Solutions", Information Security Journal: A Global Perspective, Vol.17, No3, pp: 114-123

[5] Sanneck H., Le N. T. L., Haardt M., & Mohr W. (2001, September) "Selective packet prioritization for wireless Voice over IP", Proc. of Fourth International Symposium on Wireless Personal Multimedia Communication.

[6] Ghafarian A., Draughorne R., Hargraves S., Grainger S., High S., & Jackson C. (2007) "Securing voice over Internet protocol", Journal of Information Assurance and Security, 2, pp: 200-204.

[7] Kazemitabar H., Ahmed S., Nisar K., Said A. & Hasbullah H. (2010) "A Comprehensive review on VoIP over Wireless LAN networks", ISSR Journal, Vol. 2, No. 2, pp: 1-16

[8] Mehdi G. (2009) "Future of VoIP over Wireless in Economic Downturn", Degree of Master of Science in Electrical Engineering, Blekinge Institute of Technology

[9] Tecnicontrol "The VoIP PABX or IP PABX", http://www.tecnicontrol.pt/en/wiki/item.html?id=40-the-voip-pabx-or-ip-pabx (Ανακτήθηκε την 08ΔΕΚ2018)

[10] Paulsen S., Uhl T., & Nowicki K. (2011, October) "Influence of the jitter buffer on the quality of service VoIP", IEEE 3rd International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), pp:. 1-5

[11] Lasrado S. & Gonsalves N. (2015) "A Comparative Study of Signalling Protocols Used In VoIP", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 3, Special Issue 7, pp: 176-180

[12] what-when-how “Looking at the TCP/IP Model (VOIP)”, In Depth Tutorials and Information http://what-when-how.com/voip/looking-at-the-tcpip-model-voip/ (Ανακτήθηκε την 08ΔΕΚ2018)

[13] Lazzez A. (2013) “VoIP technology: Security issues analysis”, arXiv preprint arXiv:1312.2225

[14] Shaw U., & Sharma B. (2016) “A Survey Paper on Voice over Internet Protocol (VOIP)”, International Journal of Computer Applications, Vol. 139, No 2, pp:16-22

[15] Tekin G. (2013) “Voip Over Wireless Networks”, Thesis in Master of Science in Electrical and Electronics Engineering, Applied Electrical and Electronics Program, Graduate School of Natural and Applied Sciences, Dokuz Eylül University

[16] Freeman R. L. (Ed.). (2005) “Fundamentals of telecommunications”, 2nd ed., New Jersey: John Wiley & Sons, Inc. ISBN 978-0-471-7209-35

[17] Rattal S., Badri A., & Moughit M. (2013) “Performance analysis of hybrid codecs G. 711 and G. 729 over signaling protocols H. 323 and SIP”, International Journal of Computer Applications, Vol. 72, No. 3, pp: 29-33

[18] Köster F. (2018) “Multidimensional Analysis of Conversational Telephone Speech”, Springer Singapore, ISBN 978-9-811-0522-48

[19] Stuckmann P. (2003) “The GSM evolution: mobile packet data services”, John Wiley & Sons, ISBN 978-0-470-8485-55

[20] Check Point (2018) “VoIP Administration Guide R80.10”, Check Point Software Technologies Ltd. (Ανακτήθηκε την 08ΔΕΚ2018)

[21] Tuteja D., Jain D., Goyal D., & Sharma D. (2014) “A Survey of Security Protocols on VoIP”, Journal of Basic and Applied Engineering Research, Vol. 1, No 8; pp: 13-16

[22] Rosenberg J., Schulzrinne H., Camarillo G., Johnston A., Peterson J., Sparks R., Handley M, & Schooler E. (2002) “SIP: session initiation protocol”, RFC 3261, https://www.ietf.org/rfc/rfc3261.txt (Ανακτήθηκε την 12ΔΕΚ2018)

[23] Alo U. R. & Firday N. H. (2013) “Voice over Internet Protocol (VOIP): Overview, Direction And Challenges”, Journal of Information Engineering and Applications, Vol. 3, No 4, pp: 18-28

[24] Handley M., Jacobson V., & Perkins C. (2006) “SDP: session description protocol”, RFC 4566, https://tools.ietf.org/html/rfc2327 (Ανακτήθηκε την 12ΔΕΚ2018)

[25] Raj R., Gagneja A., & Singal R. (2012) “Voice over Internet Protocol – The Technology and Its Application”, International Journal of Scientific & Engineering Research, Vol. 3, Issue 5, pp: 1-6

[26] Wang Z. (2014) “Peer-to-Peer multimedia streaming monitoring system”, Master Thesis, Department of Mathematics and Computer Science, Architecture of Information Systems Research Group, Eindhoven University of Technology

[27] Networx Security “RTP Control Protocol”, http://www.networxsecurity.org/members-area/glossary/r/rtcp.html (Ανακτήθηκε την 13ΔΕΚ2018)

[28] Braden R., Clark D., & Shenker S. (1994) “Integrated services in the internet architecture: an overview”, RFC 1633, https://tools.ietf.org/html/rfc1633 (Ανακτήθηκε την 13ΔΕΚ2018)

[29] Zurawski R. (Ed.). (2018) “The industrial information technology handbook”, CRC press, ISBN 978-1-420-0363-36

[30] Javvin Technologies Inc. (2005) “Network Protocols Handbook”, 2nd Ed., ISBN 978-0-974-0945-26

[31] LumenVox “Media Server Connectivity”, https://www.lumenvox.com/knowledgebase/index.php?/article/AA-01647/0/Media-Server-Connectivity.html (Ανακτήθηκε την 13ΔΕΚ2018)

[32] Schulzrinne H., Rao A., & Lanphier R. (1998) “Real time streaming protocol (RTSP)”, RFC 2326, https://tools.ietf.org/html/rfc2326 (Ανακτήθηκε την 13ΔΕΚ2018)

[33] Lazzez A., & Slimani T. (2013) “Deployment of VoIP Technology: QoS Concerns”, arXiv preprint arXiv:1312.2581

[34] Kay T., (2017) “VoIP: Is your network ready?”, Ironton Telephone Company, http://www.ironton.com/images/ITC/SupportFiles//VoIP_Network_Performance.pdf (Ανακτήθηκε την 19ΔΕΚ2018)

[35] Miraz M. H., Molvi S. A., Ganie M. A., Ali M., & Hussein A. H. (2017) “Simulation and analysis of quality of service (QoS) parameters of voice over IP (VoIP) traffic through heterogeneous networks”, arXiv preprint arXiv:1708.01572

[36] Valentine M., (2008) “CCNA Voice Quick Reference”, Cisco Press, ISBN 1-58714-337-2

[37] Froehlich A. (2011) “CVOICE 8.0: Implementing Cisco Unified Communications Voice over IP and QoS v8. 0”, John Wiley & Sons, ISBN 978-0470-91623-0

[38] Patrick P. (2009) “Voice over IP security”, Pearson Education India, Cisco Press, ISBN 978-1-587-0546-93

[39] Joseph V., & Chapman B. (2009) “Deploying QoS for Cisco IP and next generation networks: the definitive guide”, Morgan Kaufmann, ISBN 978-0-080-9225-53

[40] Thermos P., & Takanen A. (2007) “Securing VoIP networks: threats, vulnerabilities, and countermeasures”, Pearson Education, ISBN 978-0-132-7023-00

[41] VoIP-info.org “VoIP Softphones”, A reference guide to all things VOIP https://www.voip-info.org/voip-softphones/ (Ανακτήθηκε την 07IAN2019)

[42] Microsoft “Skype Connect” https://www.skype.com/en/features/skype-connect/ (Ανακτήθηκε την 07IAN2019)

[43] Corpuz J. (2017) “Best VoIP Apps for Your Desktop”, Tom’s Guide https://www.tomsguide.com/us/pictures-story/519-best-voip-apps.html#s1 (Ανακτήθηκε την 07IAN2019)

[44] Tolentino J. (2015) “Enhancing customer engagement with interactive voice response” https://thenextweb.com/future-of-communications/2015/04/20/enhancing-customer-engagement-with-interactive-voice-response/ (Ανακτήθηκε την 07IAN2019)

[45] Wikipedia “Comparison of VoIP software” https://en.wikipedia.org/wiki/Comparison_of_VoIP_software (Ανακτήθηκε την 12IAN2019)