ELECTRONICS AND ELECTRICAL ENGINEERING
ISSN 1392 – 1215 2008. No. 4(84)
ELEKTRONIKA IR ELEKTROTECHNIKA

T170 ELECTRONICS
ELEKTRONIKA

Investigation of VoIP Quality of Service using SRTP Protocol

T. Adomkus, E. Kalvaitis
Telekomunikacijų katedra, Kauno technologijos universitetas
Studentų g. 50, LT-51368 Kaunas, Lietuva, tel. +370 37 300515, faks. +370 37 300504, el.paštas tomas.adomkus@ktu.lt

Introduction

Voice over IP (VoIP) is transforming the telecommunication industry. It offers multiple opportunities such as lower call fees, convergence of voice and data networks, simplification of deployment, and greater integration with multiple applications that offer enhanced multimedia functionality. However, notwithstanding all these technological and economic opportunities, VoIP also brings up new challenges. Among them, security is perhaps the most compelling [1].

Security for Voice over IP (VoIP) can be achieved in different ways and can be divided into two main aspects. Securing the call signalling, i.e. the IP traffic used for establishing the call and securing the call itself here referred to as the media session. In this paper we will focus on the quality of service for the secure media session.

But VoIP has a very special characteristic: it is “time critical”. Time has a tremendous impact on this technology’s ability to provide quality of service, and to transmit meaningful information as well. Consequently, security considerations for VoIP must take additional steps to fulfill specific quality demands. First, the technology requires a very low latency less than 150 ms. Second, packet loss cannot exceed the mark of 3% [2]. Third, the technology is highly sensitive to “unquantifiable disrupting factors such as jitter”. Thence, at the end, all these factors converge and constitute the most critical of all VoIP security vulnerabilities: this technology’s inherent sensitivity to disruptions [1]. So in this paper we will evaluate how we can ensure the secure stream of VoIP service and provide satisfactory quality of service.

Common threats

Therefore, VoIP systems are exposed to many of the same attacks that predate other Internet services for instance, operating systems vulnerabilities, denial of service attacks, spoofing, and so on. Now we will discuss some of the most common threats that prey on VoIP systems [1].

Denial of Service attacks. In a denial of service (DoS) attack, the attacker usually creates a large number of connections or service requests that ultimately overwhelm the target system’s resources. In fact, any kind of traffic that increases the overall network utilization above 60% - 80% may bog down the network and increase the overall delay beyond the QoS threshold. In such conditions, all VoIP services may be down for this particular segment.

Eavesdropping. Eavesdropping is the interception, listening, and/or recording of private conversations between parties. Unfortunately, RTP does not include any mechanism to prevent eavesdropping (such as encryption), which allows an attacker listening the network for instance, with a packet sniffer to intercept, listen, and record VoIP communications.

Man in the Middle attacks. A man-in-the-middle attack occurs when a third party (the attacker) poses as the other party in a communication which allows an attacker to monitor, record, obstruct, or modify passing information.

Call hijack. A call hijack occurs when an attacker effectively controls one end of a VoIP call. Call hijack usually occurs after the call has been set up.

Spoofing attacks. Spoofing attacks are very similar to Call hijack attacks. However, in this case, the attacker assumes total control of the other party’s identity, even before a call has been initiated.

Call fraud. Call fraud attacks are intended to facilitate the illegal use of the VoIP infrastructure to place free phone calls [1].

SRTP protocol

VoIP datagrams are usually transported using the Real-time Transport Protocol (RTP). SRTP is a profile of RTP which aims to provide confidentiality, message authentication, and replay protection to RTP data and control traffic [3]. SRTP uses a single master key to derive keying material via a cryptographically secure hash function [4]. The structure of SRTP packet is shown in the Fig. 1.

RTP header	RTP encrypted payload	MKI	MAC

Fig. 1. SRTP packet. (where: MKI (Master Key Identifier) tells the receiver which key to use. MAC (Message Authentication Code) applies to RTP header and payload)

In distinction to RTP, Secure RTP (SRTP) comes along with several advantages concerning security features. It enables Secure VoIP communication, e.g. in a WLAN or at public Hotspots. It is an alternative to IP Security (IPSec) based Virtual Private Network (VPN) communication and was designed for real-time transmission. SRTP supports symmetric VoIP data encryption with AES to avoid tapping, authentication of the sender to avoid identity-spoofing, integrity checks to avoid unauthorized changes and anti-replay functionality to avoid unauthorized access. All of the provided features (such as encryption and authentication) are optional and can be separately enabled or disabled [5].

In SRTP, a cryptographic context refers to the cryptographic state information maintained by the sender and receiver for the media stream. This includes the master key, session keys and identifiers for encryption and message authentication algorithms, lifetime of session keys, and a rollover counter (ROC) [4].

Each RTP packet consists of a 16-bit sequence number (SEQ) which is monotonically increasing. The rollover counter is maintained by the receiver and is incremented by 1 every time the sequence number wraps around. For a multicast stream with multiple senders, a synchronization source identifier (SSRC) uniquely identifies a sender within a session.

For data encryption, SRTP uses a single cipher, Advanced Encryption Standard (AES), in one of the following two modes: a) Segmented Integer Counter mode, or b) f-8 mode. F-8 mode – a variation of Output feedback mode, enhanced with an altered initialization function [4].

Multimedia Internet KEYing.

MIKEY is another key exchange protocol for SRTP. It can operate in three different modes: pre-shared key with key transport, public key with key transport, public key with authenticated Diffie-Hellman (DH) key exchange. A later extension provides for a DH exchange in the pre-shared key mode.

An advantage of MIKEY is that it allows the key to be negotiated as part of the SDP payload during the session setup phase in SIP. Thus, it requires no extra communication overhead. An obvious disadvantage of MIKEY is that it requires either prior shared secrets, or a separate PKI, with all attendant problems such as certificate dispersal, revocation, and so on [4].

Public Key Infrastructure

For using the encryption functionality, SRTP needs a Public Key Infrastructure (PKI). In cryptography, a PKI is an arrangement that provides for trusted third party vetting of, and vouching for, user identities. It also allows binding of public keys to users. This is usually carried out by software at a central location together with other coordinated software at distributed locations. The public keys are typically in certificates [5].

PKI arrangements enable users to be authenticated to each other, and to use the information in identity certificates (i.e., each other's public keys) to encrypt and decrypt messages travelling to and from. In general, a PKI consists of client software, server software such as a certificate authority, hardware (e.g., smart cards) and operational procedures. A user may digitally sign messages using his private key, and another user can check that signature (using the public key contained in that user's certificate issued by a certificate authority within the PKI). This enables two (or more) communicating parties to establish confidentiality, message integrity and user authentication without having to exchange any secret information in advance. A PKI is a complex structure that is necessary to make secure VoIP phone calls using SRTP. Therefore it is no alternative for private users, because normally only companies can afford to setup this structure to use it with their VoIP phone calls [5].

Diffie-Hellman algorithm

The Diffie-Hellman algorithm depends for its effectiveness on the difficulty of computing discrete logarithms. Briefly, we can define the discrete logarithm in the following way. First, we define primitive root of a prime number p as one whose powers generate all the integers from 1 to $p - 1$. That is, if a is a primitive root of the prime number p, then the numbers

$$a \bmod p, a^2 \bmod p, ..., a^{p-1} \bmod p \qquad (1)$$

are distinct and consist of the integers from 1 through p – 1 in some permutation. For any integer b and a primitive root a of prime number p, one can find a unique exponent i such that

$$b = a^i \bmod p \text{ where } 0 \le i \le (p-1). \qquad (2)$$

The exponent i is referred to as the discrete logarithm, or index, of b for the base a, mod p. This value is denoted as $\text{ind}_{a,p}(b)$ [6].

With this background we can define the Diffie-Hellman key exchange. There are two publicly known numbers: a prime number q and an integer α that is primitive root of q. Suppose the users A and B wish to exchange a key. User A selects a random integer $X_A < q$ and computes $Y_A = \alpha^{X_A} \bmod q$. Similarly, user B independently selects a random integer $X_B < q$ and computes $Y_B = \alpha^{X_B} \bmod q$. Each side keeps the X value private and makes the Y value available publicly to the other side. User A computes the key as $\mathrm{K} = (Y_B)^{X_A} \bmod q$ and user B computes the key as $\mathrm{K} = (Y_A)^{X_B} \bmod q$ [6].

Thus, the two sides have exchanged a secret key. Furthermore, because X_A and X_B are private, an opponent only has the following ingredients to work with: q, a, Y_A and Y_B. Thus, the opponent is forced to take a discrete logarithm to determine the key.

The security of the Diffie-Hellman key exchange lies in the fact that, while it is relatively easy to calculate exponentials modulo a prime, it is very difficult to calculate discrete logarithm. For large primes, the latter task is considered infeasible [6].

Investigation of secure VoIP quality of service.

In this chapter we perform a modelling of VOIP Quality of service, using SRTP protocol to ensure secure call. We are using Opnet Modeler 10.5 software for modelling. The modelling network is illustrated in Fig. 2.

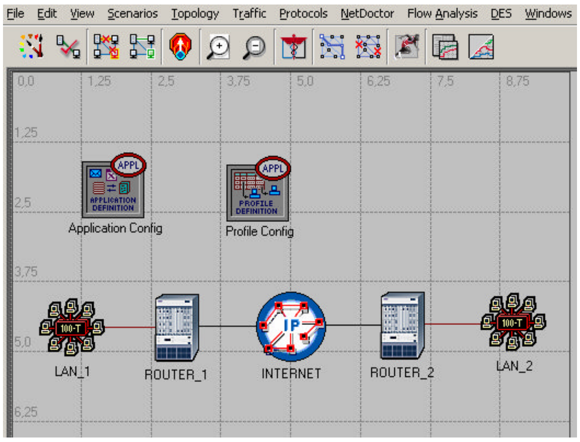

Fig. 2. The modelling network

This network consists of two LAN's, which are connected via internet. Both LAN's connected to internet through ROUTER_1 and ROUTER_2. The link speed between LAN and router is 100 Mb/s, and between the router ant internet is 2 Mb/s. There are 25 users at each LAN's. To ensure VOIP service we are using G.711 codec. The duration of modelling is 15 minutes.

As noted above, VOIP datagrams are usually transported using the Real-time Transport Protocol (RTP). To secure these packets SRTP protocol must be used. To encrypt the information, SRTP protocol uses AES algorithm, and DIffie-Hellman algorithm to securely exchange encryption keys. At our model we are using these two algorithms. The modelling consists of two scenarios. At first – voice information is clear, that's why this information transported via RTP protocol, at second – voice information is encrypted and transported via SRTP.

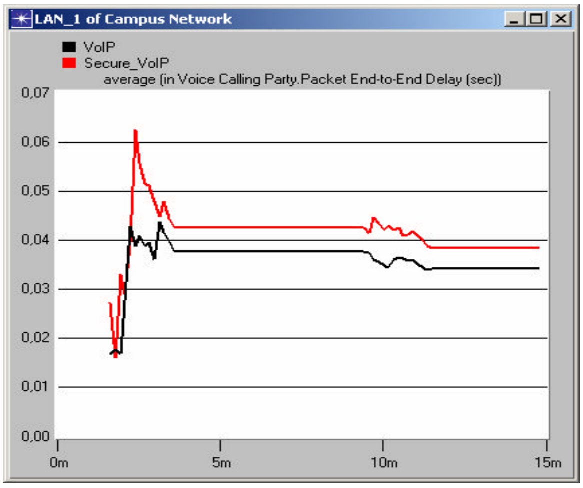

Fig. 3. End to End delay of voice packets

In Fig. 3 we see, that end to end delay of encrypted VOIP stream between different LAN's at the beginning of call session reaches even 63 ms, when at that moment end to end delay of clear voice stream reaches only 43 ms. Exactly at this moment Diffie-Hellman is executing an exchange of public keys between calling parties. End to end delay drop down significantly when key exchange is completed, but in other hand, it's still major than at clear voice stream. The reason is that at voice session AES algorithm is encrypting all voice packets. However, that delay of voice packets not reduces VOIP quality of service significantly, because end to end delay doesn't exceed critical 150 ms value. By this reason average throughput of voice packets and average traffic utilization between end to end users is increased (see Figs. 4 and 5).

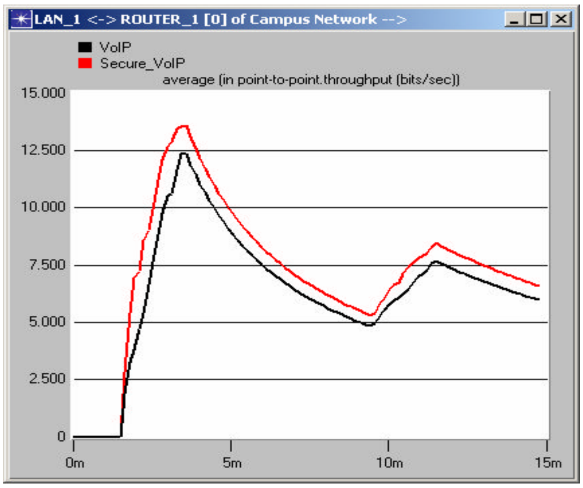

Fig. 4. Average throughput of voice packets between end to end users

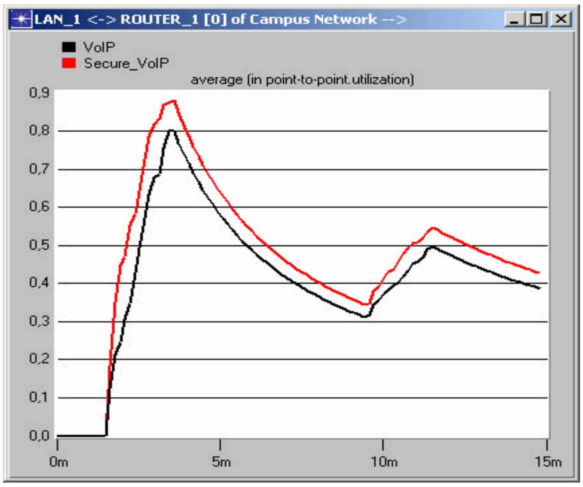

Fig. 5. Average traffic utilization between end to end users

Average voice packets delay at encrypted VOIP stream most increases at the queues of both routers (see Fig. 6). At the beginning of the call, average voice packets delay of encrypted stream reaches even 13.5 ms, while at this moment the average delay of clear voice packets is just 8.5 ms. At the session of encrypted voice, the average delay of voice packets decrease to 5.1 ms, however at this moment it is about two times higher than at clear voice case (2.8 ms). So we can confirm that usage of SRTP protocol influences VoIP quality of service, because average throughput of voice packets, average traffic utilization between end to end users and delay of voice packets increases. But it is very important, that increased delay (most important parameter) doesn't exceed critical 150 ms value, which is prescribed in ITU G.1010 recommendation.

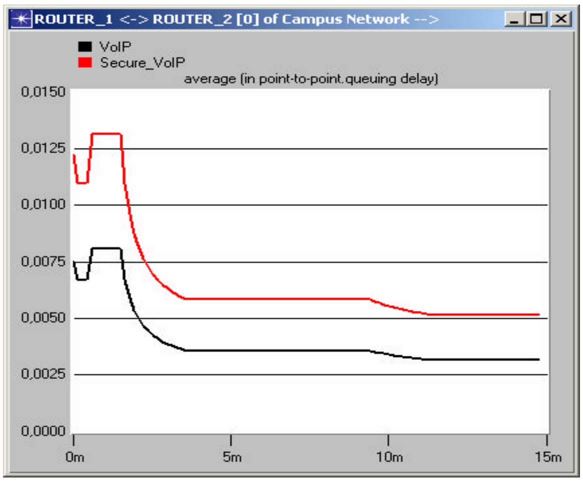

Fig. 6. Average point to point delay at the queues of routers

Accordingly to all modelling results we see, that at encrypted voice session between end to end users, quality of service is ensured, whereas knowing that treads for transmitting clear voice through public internet, we can propose, that it's necessary to use voice encryption.

Conclusions

1. Discussed common treads to VOIP telephony, to ensure protection from them suggested SRTP.
2. Accomplished modelling with RTP and SRTP streams. Identified, that end to end delay of encrypted VOIP stream between different LAN's at the beginning of call session reaches even 63 ms, when at that moment end to end delay of clear voice stream reaches only 43 ms.
3. Observed, that average voice packets delay at encrypted VOIP stream most increases at the queues of both routers till 13.5 ms, while at this moment the average delay of clear voice packets is just 8.5 ms.
4. Accordingly to modelling results we see that in any case the delay of voice packets doesn't exceed critical 150 ms value. So, we can certainly propose, that we can ensure the quality of service for encrypting voice packets.

References

1. **Sotillo S.** Zfone: A New Approach for Securing VoIP Communication // ICTN 4040, 2006. - P. 13.
2. **Kuhn D. R., Walsh Th. J., Fries S**. Security Considerations for Voice Over IP Systems // National Institute of Standards and Technology, Gaithersburg, 2005. - P. 93.
3. **Hersent O., Petit J-P., Gurle D.**. IP Telephony. Deploying Voice Over IP Protocols // John Wiley and Sons, Inc., Publication, 2005. - P. 377.
4. **Gupta P., Shmatikov V.** Security Analysis of Voice-over-IP Protocols // The University of Texas at Austin, 2006. - P. 15.
5. **Muncan M.** Secure telephony: SIP/SRTP (PKI) vs. Zfone vs. Skype // University Konstanz Fachbereich. Konstanz, 2006. – P. 12.
6. **Stallings W**. Cryptography and Network Security. Principles and Practice. Second edition. Prentice-Hall, 1999. - P. 569.

Submitted for publication 2008 02 07

T. Adomkus, E. Kalvaitis. Investigation VoIP quality of service using SRTP protocol // Electronics and Electrical Engineering. – Kaunas: Technologija, 2008. – No. 4(84). – P. 85-88.

Voice over IP (VoIP) is transforming the telecommunication industry. It offers multiple opportunities such as lower call fees, convergence of voice and data networks, simplification of deployment, and greater integration with multiple applications that offer enhanced multimedia functionality. So it is very important to ensure VoIP security and at the same time its quality of service. It's discussed common treads to VoIP telephony at this article, to ensure protection from them suggested SRTP. Accomplished modelling with encrypted voice streams and ascertained the influence to VoIP quality of service of SRTP protocol. Observed, that at various time moments SRTP protocol significantly decrease the quality of service. Ill. 6, bibl. 6 (in English; summaries in English, Russian and Lithuanian).

Т. Адомкус, Е. Калваитис. Исследование качества услуги VoIP с использованием SRTP протокол // Электроника и электротехника. – Каунас: Технология, 2008. - № 4(84). – С. 85-88.

Голос через IP (VoIP) изменяет индустрию радиосвязи. VoIP предлагает множество возможности, такие как более низкие цены за звонок, интеграцию голоса и сетей данных, упрощённую дислокацию и наилучшую интеграцию с множественными применениями, которые предлагают увеличенную функциональность информации. Потому очень важно обеспечить безопасность звонка VoIP и в то же самое время качество обслуживания. В этой статье были проанализированный главные угрозы возникающие звонкам VoIP и для её защиты предложено использовать протокол SRTP. Произведено моделирование шифровых потоков голоса и установлена влияние протокола SRTP на качество звонка VoIP. Замечено, что разными моментами протокол SRTP может значительно уменьшить уровень качеств обслуживания. Ил. 6, библ. 6 (на английском языке; рефераты на английском, русском и литовском яз.).

T. Adomkus, E. Kalvaitis. VoIP paslaugos kokybės tyrimas naudojant SRTP protokolą // Elektronika ir elektrotechnika. – Kaunas: Technologija, 2008. – Nr. 4(84). – P. 85-88.

Balso perdavimas per IP (VoIP) keičia telekomunikacijų pramonę. VoIP suteikia daugybę naujų galimybių: mažėja mokesčiai už skambučius, integruojami balso ir duomenų tinklai, supaprastėja dislokacija, pagerėja integracija su daugialypiais taikymais, kurie padidiną daugialypės informacijos funkcionalumą. Taigi, labai svarbu užtikrinti VoIP skambučio saugumą ir tuo pačiu metu teikiamos paslaugos kokybę. Straipsnyje yra išanalizuotos pagrindinės VoIP telefonijai kylančios grėsmės ir jos apsaugai pasiūlyta naudoti SRTP protokolą. Atliktas šifruotų balso srautų modeliavimas ir nustatyta SRTP protokolo įtaka VoIP paslaugos kokybei. Pastebėta, kad atskirais laiko momentais SRTP protokolas gali gerokai pabloginti paslaugos kokybę. Il. 6, bibl. 6 (anglų kalba; santraukos anglų, rusų ir lietuvių k.).