Analysis of Secure Real Time Transport Protocol on VoIP over Wireless LAN in Campus Environment

Mohd Nazri Ismail
Department of MIIT, University of Kuala Lumpur (UniKL), MALAYSIA
mnazrii@miit.unikl.edu.my

Abstract- **In this research, we propose to implement Secure Real Time Transport Protocol (SRTP) on VoIP services in campus environment. Today, the deployment of VoIP in campus environment over wireless local area network (WLAN) is not considered on security during communication between two parties. Therefore, this study is to analyzed SRTP performance on different VoIP codec selection over wired. We have implemented a real VoIP network in University of Kuala Lumpur (UniKL), Malaysia. We use softphone as our medium communication between two parties in campus environment. The results show that implementation of SRTP is able to improve the VoIP quality between one-to-one conversation and multi conference call (many-to-many). In our experiment, it shows that iLBC, SPEEX and GSM codec are able to improve significantly the multi conference (many-to-many) VoIP quality during conversation. In additional, implementation of SRTP on G.711 and G.726 codec will decrease the multi conference (many-to-many) VoIP quality.**

Keywords- Codecs, Softphone, SRTP, WLAN

I. INTRODUCTION AND RELATED WORKS

University of Kuala Lumpur (UniKL) has implemented a real VoIP over wireless LAN in campus environment. This implementation is not covered any security features. Therefore, the objective of this study is to enable the security function using Secure Real Time Transport Protocol (SRTP). We will study the performance of SRTP on different codec such as G.711, G.726, GSM, iLBC and SPEEX. iLBC is a speech codec developed for robust voice communication over IP, it uses 13.33 Kbps. It provides low delay and high packet loss robustness for low-bit rate codec's. SPEEX codec is open source patent-free audio compression format designed for speech. Codec is an algorithm used to encode and decode the voice conversation. Secure Real Time Transport Protocol (SRTP) defines a profile of Real Time Transport Protocol (RTP), intended to provide encryption, message authentication and integrity and replay protection to the RTP data in both unicast and multicast applications. Previous

work is to evaluate the trade-off existing between quality of service and security when SRTP [6] is employed to protect RTP (Real Time Protocol) sessions on VoIP calls [5]. There is no such study has been conducted on comparison of VoIP one-to-one call and multi conference call (many-to-many) performance using SRTP functionality. With its promise of inclusion, innovation, and growth, VoIP also brings challenges. VoIP is not easy to secure. It suffers all of the problems associated with any Internet application, and VoIP security is complicated by its interconnection to the PSTN. A host of trust, implementation, and operational complexities make securing VoIP particularly complex. In fact, the same aspects that make the VoIP software model so powerful—its flexible, open, distributed design—are what make it potentially problematic [7][8]. Various security requirements have to be met to secure VoIP transmission: Authentication, Privacy and Confidentiality, Integrity, Non repudiation, Non replay and Resource availability [9]. The threats faced by a VoIP are similar to other applications including: unwanted communication (spam), privacy violations (unlawful intercept), impersonation (masquerading), theft-of service, and denial-of-service [10].

II. METHODOLOGY

We have setup a real wireless network environment to analyze and measure implementation of VoIP service using security function (SRTP) at University of Kuala Lumpur (UniKL) in Malaysia. This study posits several research questions: i) what is the STRP performance level of the VoIP over WLAN based on one-to-one call and multi conference call? and ii) which codecs are able to provide better improvement of VoIP conversation?

Figure 2.1 and Figure 2.2 show the flow of VoIP conversation call between one-to-one and multi conference. We measure our voice quality using human perception. Mean Opinion Score (MOS) technique is the best approach to measure and

validate voice quality between one-to-one call and multi conference call. Figure 2.3 shows the measurement of VoIP performance over WLAN using SRTP implementation. We also test on different codecs selection such G.711, G.726, GSM, iLBC and SPEEX.
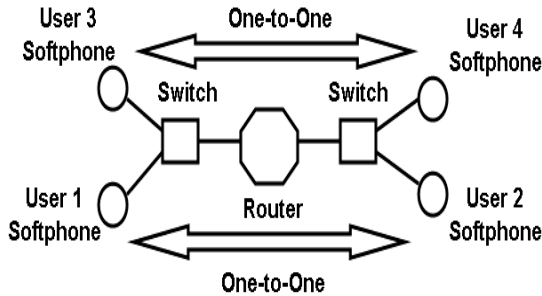

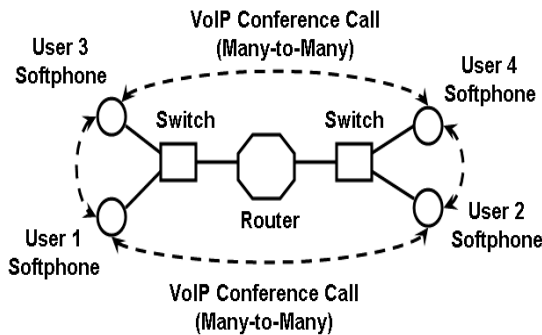Figure 2.1: VoIP over One-to-One Conversation

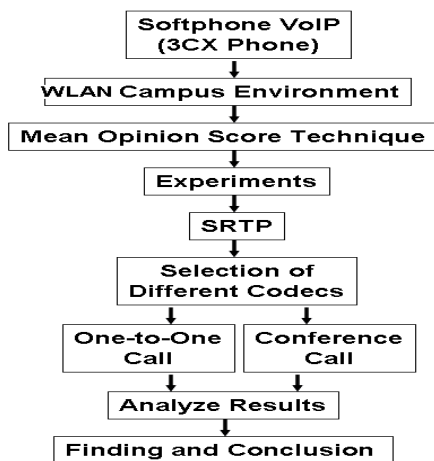Figure 2.2: VoIP over Many-to-Many (Multi Conference) Conversation

Figure 2.3: Measurement and Evaluation of VoIP over WLAN using SRTP Approach

III.   ANALYSIS AND RESULTS

This section measures and compares VoIP performance over WLAN using SRTP function. In voice and video communication, quality usually dictates whether the experience is a good or bad one. Besides the qualitative description we hear, like 'quite good' or 'very bad', there is a numerical method of expressing voice and video quality. It is called Mean Opinion Score (MOS). MOS can be tested using: i) human perception; ii) simulation model; and iii) automated system [1] [2]. MOS gives a numerical indication of the perceived quality of the media received after being transmitted and eventually compressed using codecs. MOS is expressed in one number, from 1 to 5, 1 being the worst and 5 the best. MOS is quite subjective; as it is based figures that result from what is perceived by people during tests (refer to Table 3.1). We will select five different users to evaluate and rate the VoIP performance using SRTP and without SRTP functionality. When users cannot get a dial tone or there are excessive delays in ringing the other party's phone, VoIP performance is unacceptable. Call quality is a function of packet loss rate, delay, and jitter is typically represented as a MOS [3], [4].

Table 3.1: Mean Opinion Score (MOS) Ratings

Mean Opinion Score (MOS) Ratings	
Excellent	5 (Perfect. Like face-to-face conversation or radio reception)
Good	4 (Fair. Imperfections can be perceived, but sound still clear. This is (supposedly) the range for cell phones)
Fair	3 (Annoying)
Poor	2 (Very annoying. Nearly impossible to communicate)
Bad	1 (Impossible to communicate)

Figure 3.1 shows the configuration of codec protocol such as G.711, G.726, GSM, iLBC and SPEEX. This 3CX softphone is able to active 'Echo Cancellation' and 'SRTP'. The VoIP experiments will receive two types of modes: i) one-to-one call conversation; ii) multi conference call (many-to-many). Figure 3.2 shows the result of VoIP one-to-one conversation. Figure 3.3 shows the result of VoIP multi conference (many-to-many) call.
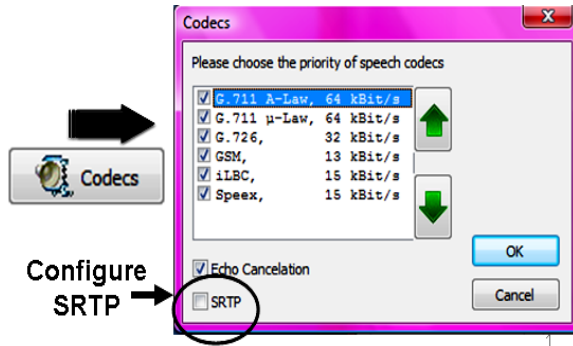
Figure 3.1: 3CX Softphone Codec and SRTP Configuration
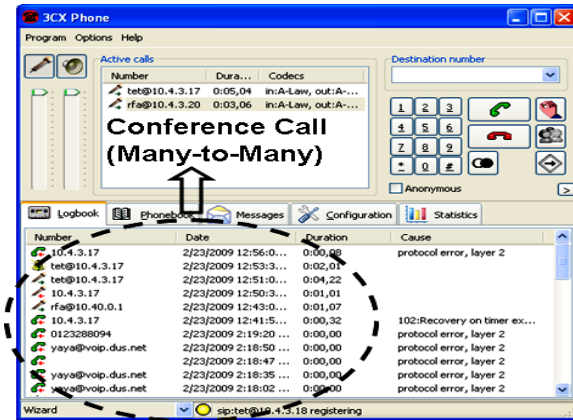

Figure 3.2: One-to-One Call Conversation Result

Figure 3.3: Multi Conference Call (many-to-many) Conversation Result

Most of the users agreed and rates this VoIP without SRTP will provide a good quality for G.711 and G.726 codecs. Other users agreed and rates 4 to 5 ratings for SPEEX codec without using SRTP during multi conference conversation (refer to Table 3.2 and Figure 3.4). After implemented SRTP on VoIP during multi conference session occurs, it shows some

improvement on VoIP quality performance and at the same time able to provide element of security (refer to Table 3.3 and Figure 3.5). The significant improvement is GSM and SPEEX codecs after implemented SRTP.

Table 3.2: Multi Conference without SRTP

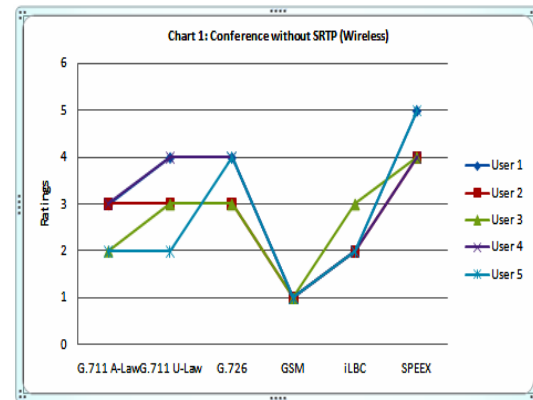| User Codec	User 1	User 2	User 3	User 4	User 5
G.711	3	3	2	3	2
G.726	4	3	3	4	4
GSM	1	1	1	1	1
iLBC	2	2	3	2	2
SPEEX	5	4	4	4	5

Figure 3.4: Users Rate VoIP for Multi Conference Call Without SRTP

Table 3.3: Multi Conference with SRTP

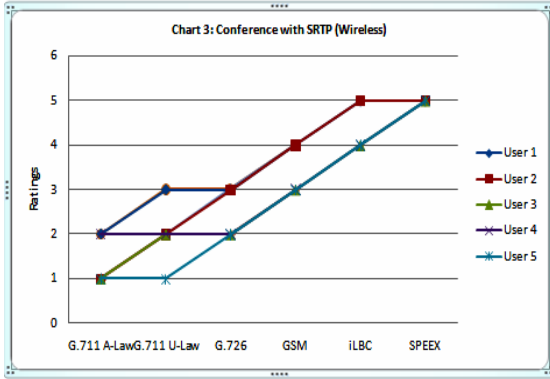| User Codec	User 1	User 2	User 3	User 4	User 5
G.711	2	1	1	2	1
G.726	3	3	2	2	2
GSM	4	4	3	3	3
iLBC	5	5	4	4	4
SPEEX	5	5	5	5	5

Figure 3.5: Users Rate VoIP for Multi
Conference Call With SRTP

Most of the users agreed and rates this VoIP one-to-one call without SRTP will also provide low quality for G.711, G.726 and GSM codecs. Other users agreed and rates 3 and 5 ratings for iLBC and SPEEX codecs without using SRTP during one-to-one call (refer to Table 3.4 and Figure 3.6). After implemented SRTP on VoIP during one-to-one session occurs, it shows significant improvement on VoIP quality performance for G.711, G.726, GSM, iLBC and SPEEX over WLAN (refer to Table 3.5 and Figure 3.7).

Table 3.4: One-to-One Call Without SRTP

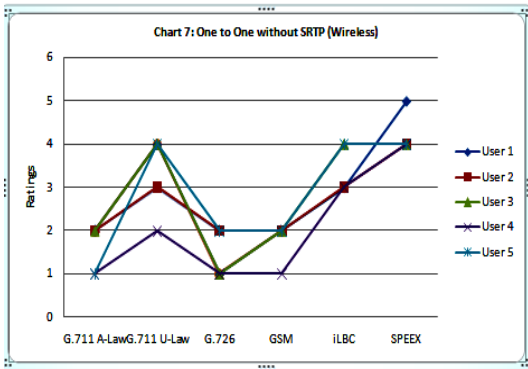| User Codec	User 1	User 2	User 3	User 4	User 5
G.711	2	2	2	1	1
G.726	1	2	1	1	2
GSM	2	2	2	1	2
iLBC	3	3	4	3	4
SPEEX	5	4	4	4	4

Figure 3.6: Users Rate VoIP for One-to-One Call
without SRTP

Table 3.5: One-to-One Call with SRTP

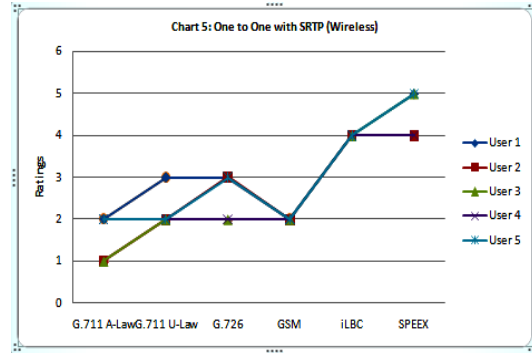| User Codec	User 1	User 2	User 3	User 4	User 5
G.711	2	1	1	2	2
G.726	3	3	2	2	3
GSM	2	2	2	2	2
iLBC	4	4	4	4	4
SPEEX	5	4	5	4	5

Figure 3.7: Users Rate VoIP for One-to-One Call
with SRTP

Figure 3.8 and Figure 3.9 show the average MOS score for VoIP conversation over one-to-one call and multi conference call (many-to-many), respectively.

VoIP Conversation over Multi Conference Call: Before implemented SRTP, the average MOS score for G.711 is 2.5, 3.5 for G.726, 1 for GSM, 2.1 for iLBC and 4.5 for SPEEX. After implemented SRTP, the average MOS score for G.711 and G.726 are decreased the ratings approximately 1 to 2.5. GSM, iLBC and SPEEX codecs show the average MOS score are 3.5, 4.5 and 5. GSM, iLBC and SPEEX codec show the increasing of VoIP performance after implemented SRTP (refer to Figure 3.8).

VoIP Conversation over One-to-One Call: Before implemented SRTP, the average MOS score for G.711 is 1.6, 1.4 for G.726, 1.8 for GSM, 3.5 for iLBC and 4.2 for SPEEX. After implemented SRTP, the average MOS score shows the significant improvement for G.711, G.726, GSM, iLBC and SPEEX codecs. Therefore, implementation of SRTP can improve the VoIP quality performance for one-to-one call over WLAN (refer to Figure 3.9).
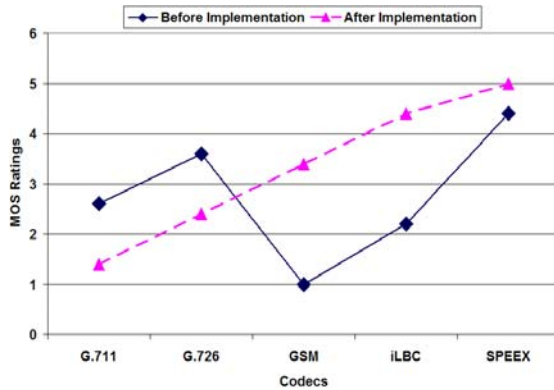
Figure 3.8: VoIP Conversation over Multi
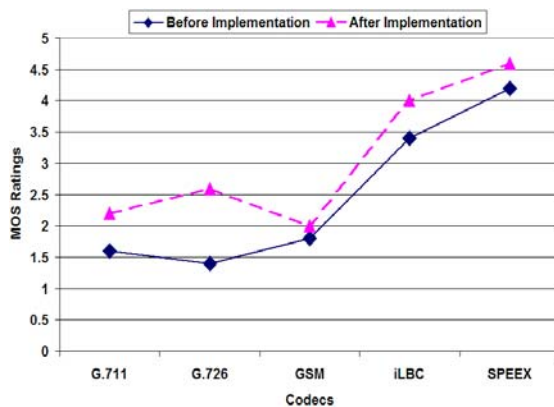Conference Call over WLAN

Figure 3.9: VoIP Conversation over One-to-One
Call over WLAN

IV. CONCLUSION AND FUTURE WORK

Based on the results, implementation of SRTP using GSM, iLBC and SPEEX codecs are able to generate high quality of VoIP conversation WLAN for one-to-one conversation and multi conference call (many-to-many). After implemented SRTP for multi conference call (many-to-many), the MOS result indicates that G.711 and G.726 codec will decrease the performance of VoIP conversation over WLAN. Overall of our finding, it confirms that enable SRTP will improve and increase the quality of one-to-one VoIP conversation and VoIP over multi conference call (only for iLBC, GSM and SPEEX codecs). Since the manual/human MOS tests are quite subjective and less than productive in many ways, there are nowadays a number of software tools that carry out automated MOS testing in a VoIP deployment. Although they lack the human touch, the good thing with these tests is that they take into account all the network

dependency conditions that could influence voice quality. Future work, we will extend our experiment on VoIP over VPN implementation in Campus environment.

References

[1]. Moura N.T.; Vianna B.A.; Albuquergue C.V.N; Rebello V.E.F & Boeres C. "MOS-Based Rate Adaption for VoIP Sources". IEEE International Conference on Communication, pp. 628-633, 2007.
[2]. Masuda M. & Ori K. "Delay Variation Metrics for Speech Quality Estimation of VoIP". Institute of Electronics, Information and Communication Engineers (IEIC) Technical Report, Vol. 101(11), pp. 101-106, 2001.
[3]. R.G. Cole & J.H. Rosenbluth. "Voice over IP Performance Monitoring". SIGCOMM Computer Communication Rev. Vol. 31(2), pp. 9-24, 2001.
[4]. L. Ding & R. Goubran. "Speech Quality Prediction in VoIP Using the Extended e-Model. Global Telecommunication Conference, GLOBECOM '03. IEEE, Vol. 7, pp. 3974-3978, 2003.
[5]. Alexandre P.; Edjair M.; & Edjard M. "Analysis of the Secure RTP Protocol on Voice over Wireless Networks using Extended MedQoS". Proceedings of the 2009 ACM symposium on Applied Computing, pp. 86 – 87, 2009.
[6]. M. Baugher, D. McGrew, M. Naslund, E. Carrara, & K. Norrman. "The Secure Real- Time Transport Protocol (SRTP)". RFC 3711 (Proposed Standard), March 2004.
[7] Douglas C. Sicker & Tom L. "VoIP Security: Not an Afterthought", FEATURE: Q focus: Voice Over IP, Vol. 2(6), pp. 56-64, 2004.
[8] Vesselin I., Theodor T., & Amdt T. "Experiences in VoIP telephone network security policy at the University of Applied Sciences (FHTW) Berlin", Proceedings of the 2007 international conference on Computer systems and technologies, Bulgaria, Vol. 285(3), 2007.
[9] Wafaa B. D., Samir T., & Carole B. "Critical vpn security analysis and new approach for securing voip communications over vpn networks", Proceedings of the 3rd ACM workshop on Wireless multimedia networking and performance modelling,Chania, Crete Island, Greece, pp. 92-96, 2007.
[10] Nekita A. C., & Chhabria S. A. "Multiple design patterns for voice over IP security", Proceedings of the International Conference on Advances in Computing, Communication and Control, Mumbai, India, pp. 530 – 534, 2009.