Implementation of Secure Real Time Transport Protocol on VoIP over Wired In-Campus Network Environment.

Mohd Nazri Ismail

Department of MIIT, University of Kuala Lumpur (UniKL), Malaysia.

E-mail: mnazrii@miit.unikle.edu.my

ABSTRACT

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

(Keywords: secure real time transport protocol, SRTP, softphone®, communications, telecommunications, G.711, G.762, GSM, iLBC, SPEEX, LAN)

INTRODUCTION

University of Kuala Lumpur (UniKL) has implemented a real VoIP over LAN in the campus environment. This implementation is not covered by any security features. Therefore, the objective of this study is to enable the security function using Secure Real Time Transport Protocol (SRTP). This paper studies the performance of SRTP on different codecs such as G.711, G.726, GSM, iLBC and SPEEX. iLBC is a speech codec developed for robust voice communications over IP. It uses 13.33 Kbps and provides low delay and high packet loss robustness for low-bit rate codec's. SPEEX codec is an 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 research has evaluated the trade-offs existing between quality of service and security when SRTP [6] is employed to protect RTP (Real Time Protocol) sessions on VoIP calls [5]. No such study has been conducted on the 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].

METHODOLOGY

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

Figures 1 and 2 show the flow of VoIP conversation call between one-to-one and multi conference points. 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 3 shows the measurement of VoIP performance over SRTP implementation. We also test on different codecs selection such G.711, G.726, GSM, iLBC and SPEEX.

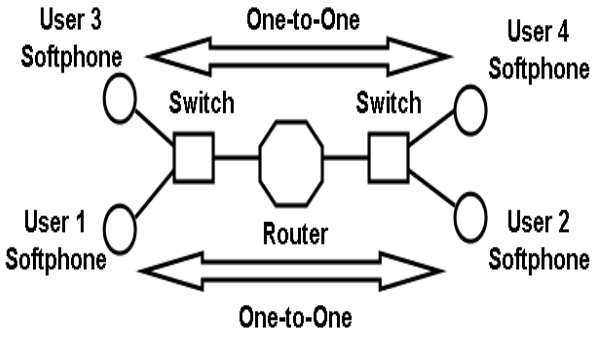

Figure 1: VoIP over LAN Establishment: One-to-One Conversation.

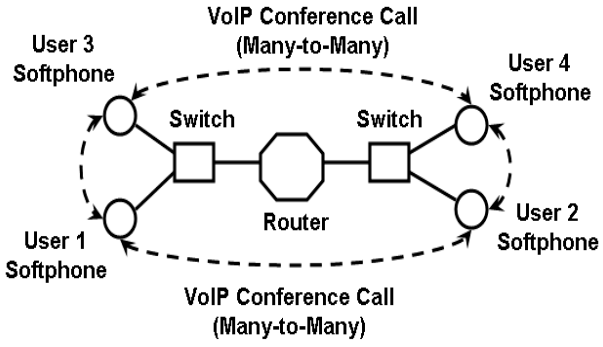

Figure 2: VoIP over LAN Establishment: Many-to-Many (Multi Conference) Conversation.

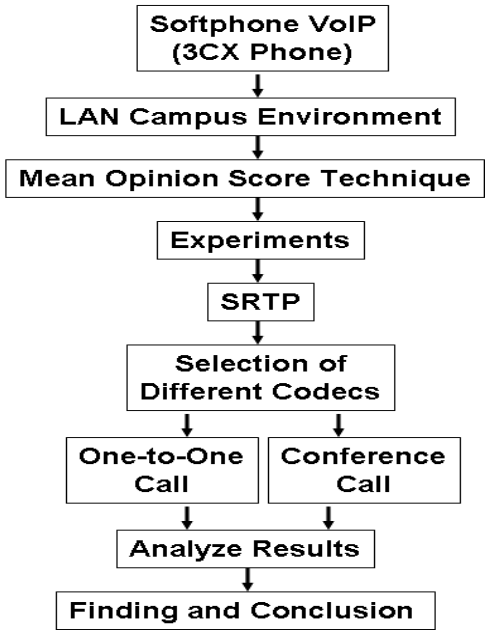

Figure 3: Measurement and Evaluation of VoIP using SRTP Approach.

ANALYSIS AND RESULTS

This section measures and compares VoIP performance over 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 (Table 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 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 4 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 5 shows the result of VoIP one-to-one conversation. Figure 6 shows the result of VoIP multi conference (many-to-many) call.

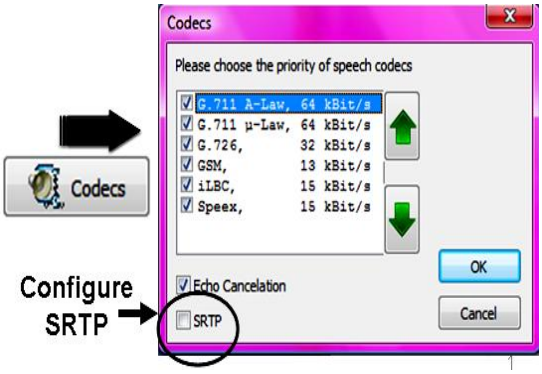

Figure 4: 3CX Softphone Codec and SRTP Configuration.

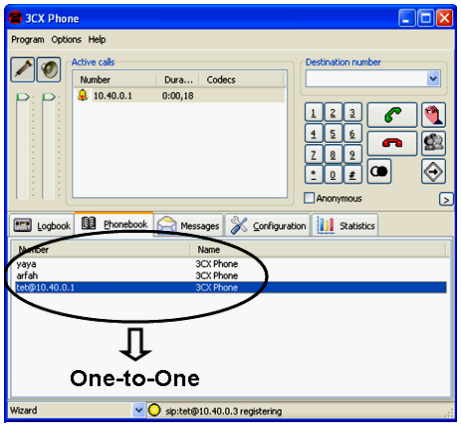

Figure 5: One-to-One Call Conversation Result.

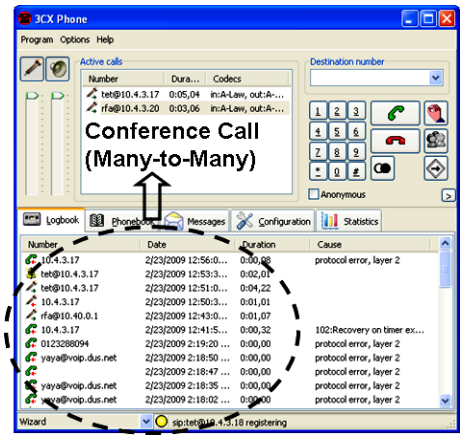

Figure 6: Multi Conference Call (Many-to-Many) Conversation Result.

Most of the users agreed and rates this VoIP without SRTP will provide low quality for G.711, G.726, and GSM codecs. Other users agreed and gave 4 to 5 ratings for iLBC and SPEEX codecs without using SRTP during multi conference conversation (refer to Table 2 and Figure 7). 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 and Figure 8).

Most of the users agreed and rate this VoIP one-to-one call without SRTP as providing low quality for G.711, G.726, and GSM codecs. Other users agreed and rated 3 and 5 ratings for iLBC and SPEEX codecs without using SRTP during one-to-one call (refer to Table 4 and Figure 9). After implemented SRTP on VoIP during one-to-one session occurs, it shows significant improvement on VoIP quality performance (refer to Table 5 and Figure 10).

Table 2: Multi Conference without SRTP.

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

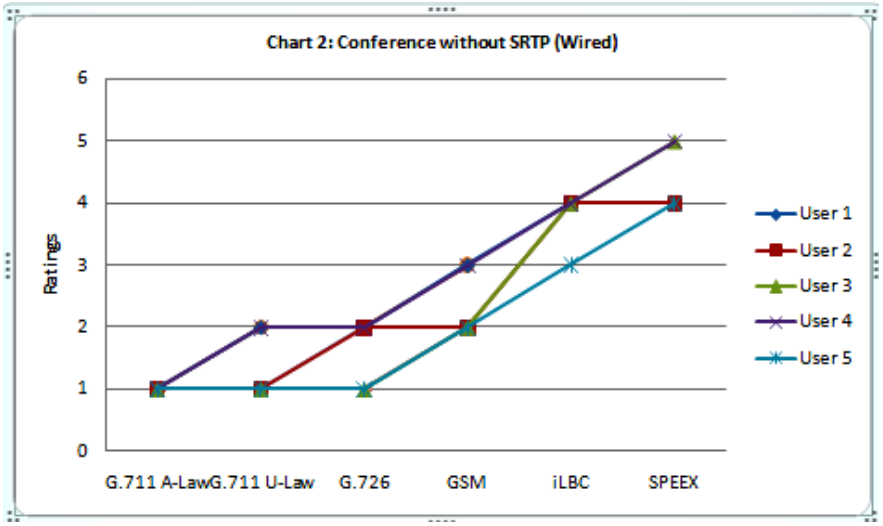

Figure 7: Users Rate VoIP for Multi Conference Call Without SRTP.

Table 3: Multi Conference with SRTP.

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

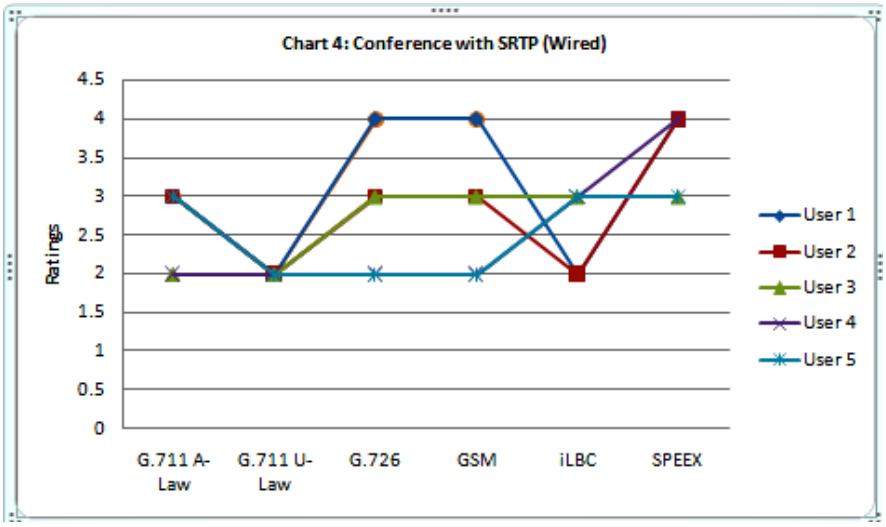

Figure 8: Users Rate VoIP for Multi Conference Call With SRTP.

Table 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

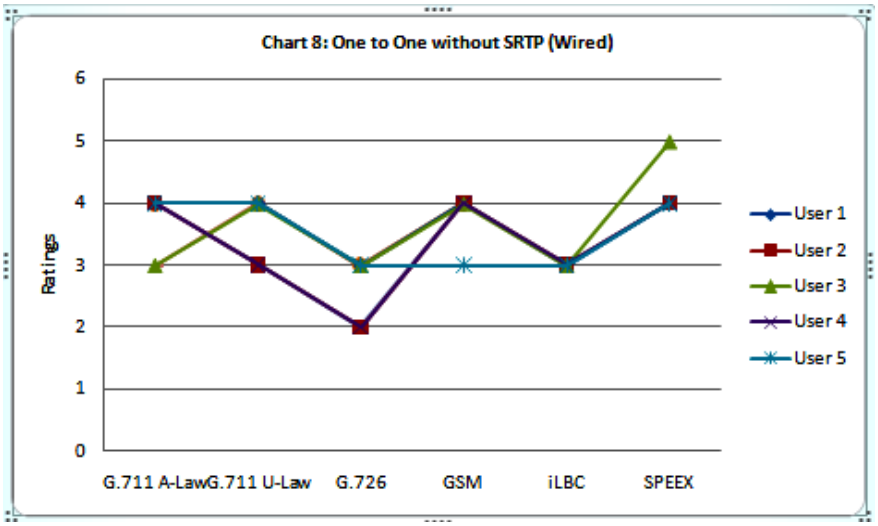

Figure 9: Users Rate VoIP for One-to-One Call without SRTP

Table 5: One-to-One Call with SRTP.

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

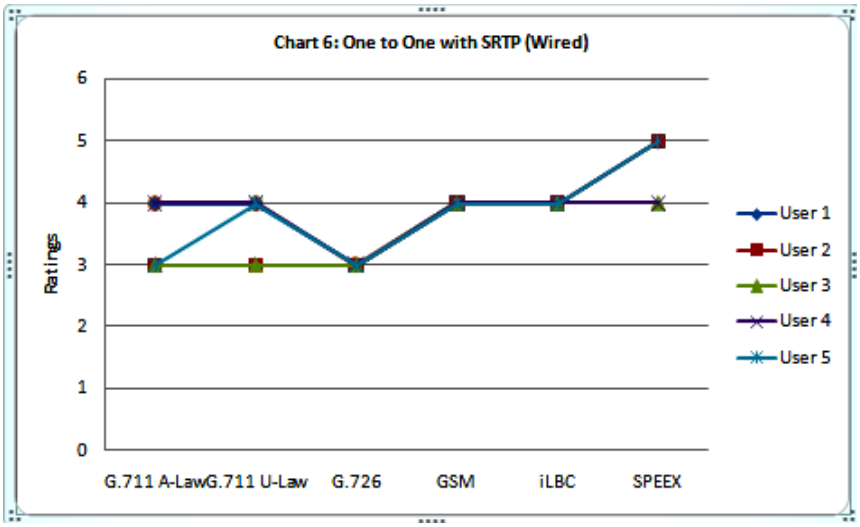

Figure 10: Users Rate VoIP for One-to-One Call with SRTP.

Figures 11 and 12 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 implementing SRTP, the average MOS score for G.711 is 1, 1.5 for G.726, 2.5 for GSM, 3.7 for iLBC, and 4.5 for SPEEX. After implementing SRTP, the average MOS score for G.711, G.726, and GSM are increased to approximately to 3. iLBC and SPEEX codecs show the average MOS scores of 2.5 and 3.5. iLBC and SPEEX codec show a decrease of VoIP performance after implemented SRTP (refer to Figure 11).

VoIP Conversation over One-to-One Call

Before implementing SRTP, the average MOS score for G.711 is 1.5, 1.4 for G.726, 1.8 for GSM, 3.5 for iLBC, and 4.1 for SPEEX. After implementing SRTP, the average MOS score shows 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 (refer to Figure 12).

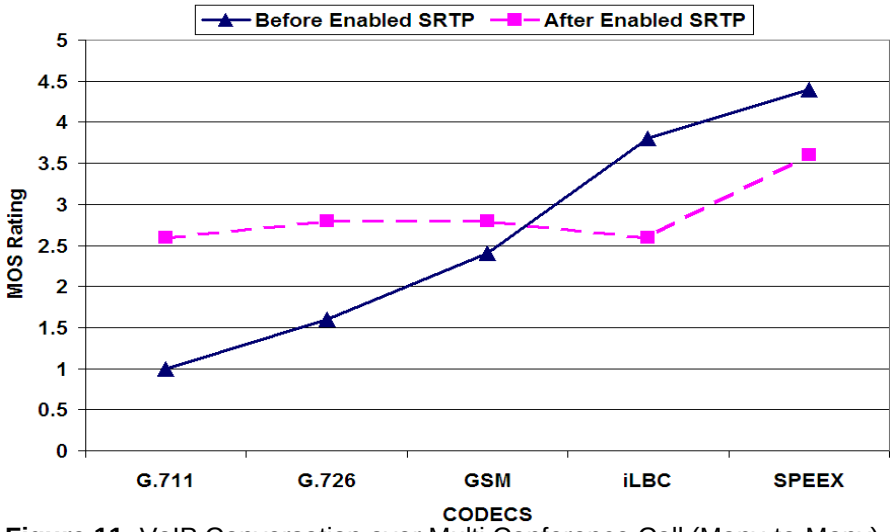

Figure 11: VoIP Conversation over Multi Conference Call (Many-to-Many).

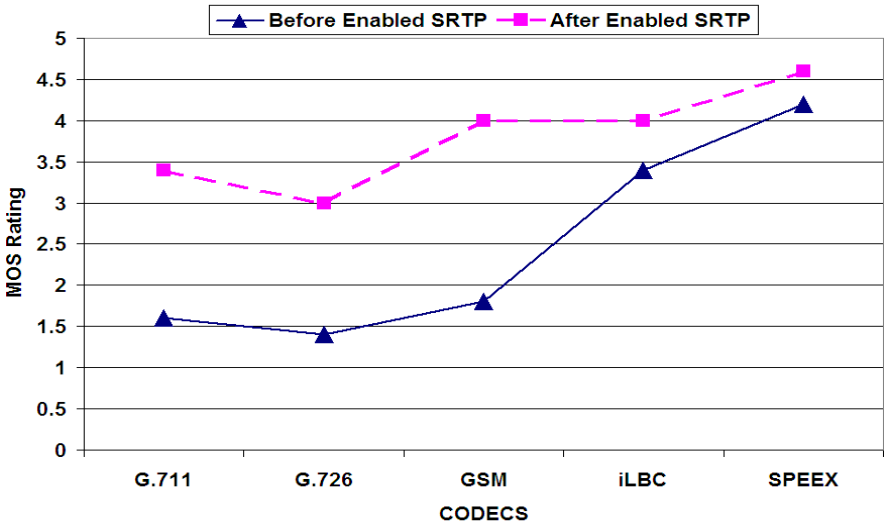

Figure 12: VoIP Conversation over One-to-One Call.

CONCLUSION AND FUTURE WORK

Based on the results presented here, using G.711, GSM, and G.726 codecs are able to generate high quality of VoIP conversation over local area network for one-to-one conversations and multi conference calls (many-to-many). After implementing SRTP for multi conference call (many-to-many), the MOS results indicate that iLBC and SPEEX codec will decrease the performance of VoIP conversation.

Overall our findings confirm that enabling SRTP will improve and increase the quality of one-to-one VoIP conversation and VoIP over multi conference calls (only for G.711, GSM, and G.726 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 about these tests is that they take into account all of the network dependency conditions that could influence voice quality. Some examples are AppareNet Voice, Brix VoIP Measurement Suite, NetAlly, PsyVoIP, and VQmon/EP. Future work, we will extend our experiment on Wireless LAN (WLAN) environment in a campus environment.

REFERENCES

1. Moura, N.T., Vianna, B.A., Albuquergue, C.V.N., Rebello, V.E.F., and Boeres, C. 2007. "MOS-Based Rate Adaption for VoIP Sources". *IEEE International Conference on Communication.* 628-633.

2. Masuda, M. and Ori, K. 2001. "Delay Variation Metrics for Speech Quality Estimation of VoIP". *Institute of Electronics, Information and Communication Engineers (IEIC) Technical Report*. 101(11):101-106.

3. Cole, R.G. and J.H. Rosenbluth. 2001. "Voice Over IP Performance Monitoring". S*IGCOMM Computer Communication Rev*. 31(2):9-24, 2001.

4. Ding, L. and R. Goubran. 2003. "Speech Quality Prediction in VoIP Using the Extended e-Model". *Global Telecommunication Conference, GLOBECOM '03. IEEE*. 7:3974-3978.

5. Alexandre, P., Edjair, M., and Edjard, M. 2009. "Analysis of the Secure RTP Protocol on Voice over Wireless Networks using Extended MedQoS".

6. Baugher, M., D. McGrew, M. Naslund, E. Carrara, and K. Norrman. 2004. "The Secure Real-Time Transport Protocol (SRTP)". RFC 3711 (Proposed Standard), March 2004.

7. Sicker, D.C. and Tom, L. 2004. "VoIP Security: Not an Afterthought", *FEATURE: Q focus: Voice Over IP*. 2(6):56-64.

8. Vesselin, I., Theodor, T., and 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. 285(3).

9. Wafaa B.D., Samir, T., and Carole, B. 2007. "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. 92-96.

10. Nekita, A.C. and Chhabria, S.A. 2009. "Multiple Design Patterns for Voice over IP Security". *Proceedings of the International Conference on Advances in Computing, Communication and Control*: Mumbai, India. 530 – 534.

SUGGESTED CITATION

Ismail, M.N. 2010. "Implementation of Secure Real Time Transport Protocol on VoIP over Wired In-Campus Network Environment". *Pacific Journal of Science and Technology*. 11(1):287-293.

Pacific Journal of Science and Technology