Comparative Analysis and Implementation of Verifiable Secret Sharing Over a Single Path in VoIP Security with Reliable Time Delay

R. Shankar
Assistant Professor, Dept. of Computer Science, Chikkanna Govt. Arts College, Tirupur-2, Tamil Nadu,
shankarcgac@gmail.com
Dr. E.Karthikeyan
Asst. Professor and Head , Department of Computer Science, Govt. Arts College, Udumalpet, Tamil Nadu, India
e_karthi@yahoo.com

----------**ABSTRACT**----------

Voice over Internet Protocol (VoIP) is a new fancy and up growing technology. A major change in telecommunication industry in VoIP. The transmission of Real time voice data is not as easy as ordinary text data. The real time voice transmission faces lot of difficulties. It suffers from packet loss, delay, quality and security. These factors will affects and degrade the performance and quality of a VoIP. This paper addresses the security and network delay of a VoIP Verifiable Secret Sharing algorithm over a single path with reduced time delay. The simulation results show that higher security and reduced packet delay is achieved in terms of end – to – end delay. In this work, suggests that the homomorphism of commitments is not a necessity for computational VSS in the synchronous or in the asynchronous communication setting. A new VSS schemes based merely on the definitional possessions of obligations that are approximately as good as existing VSS schemes based homomorphism commitments. Furthermore, this work has significantly lower communication complexities than their (statistical or perfect) unconditional counterparts. Thus, this proposed technique can be an excellent alternative to unconditional VSS in the future.

Keywords: *VoIP, Secret Sharing, Time Delay, security, single path.*

INTRODUCTION

VoIP systems employ session control and signaling protocols to control the signaling, set-up, and tear-down of calls. The transport audio streams over IP networks by using special media delivery protocols that encode voice, audio, video codecs by streaming media. Support of high fidelity stereo codecs some implementations rely on narrowband and compressed speech. VoIP is available on many smart phones, personal computers, and on Internet access devices. The security concerns of VoIP telephone systems are similar to those of any Internet-connected device. This means that hackers who know about these vulnerabilities can institute denial-of-service attacks, harvest customer data, record conversations and compromise voicemail messages. Compromised VoIP user account or session credentials may enable an attacker to incur substantial charges from third-party services, such as long-distance or international telephone calling.

Interconnected VoIP services also used to make and receive calls to and from traditional landline numbers, usually for a service fee. Some VoIP services require a computer or a dedicated VoIP phone, while others allows using landline phone to place VoIP calls through a special adapter. VoIP may offer features and services that are not available with more traditional telephone services. UseVoIP; decide whether to pay the cost of keeping regular telephone service. And also use computer and VoIP service at the same time. Then take some VoIP services with you when travel and use them via an Internet connection.

The remainder of this is organized as follows. Section 2 summarizes the concepts and literature survey. Section 3 discusses the proposed method, and section 4 provides the experiments with high accuracy. Finally, Section 5 presents the conclusions of the work.

2. LITERATURE SURVEY

Chang *et al* (2000).,this paper presents a mobile agent based VoIP service provision architecture. This architecture is based on the integration of the Grasshopper agent platform, a state of the art mobile agent platform which has been developed for the implementation of advanced telecommunication service environments, and an IETF based VoIP protocol suite, i.e., the Session Initiation Protocol (SIP) and related IETF protocols. [1]

Sengar*et al* (2006)., this article show how this integrated signaling environment can become a security threat to emerging VoIP and PSTN networks. They propose a security solution as a fix. Their proposal goes beyond "Gateway Screening" and "SS7 Gatekeeper" proposed by Telcordia and Verizon respectively to defend vulnerable SS7 network.[2]

Wu, Yu-Sung *et al* (2009) ., in this article, they present the design of an intrusion detection system for VoIP networks. To the best of their knowledge, this is the first comprehensive look at the problem of intrusion detection in VoIP systems. It includes treatment of the challenges faced due to the distributed nature of the system, the nature of the VoIP traffic, and the specific kinds of attacks at such systems.[3]

Fritsch *et al* (2009).,this paper describes the approach and preliminary results from the research project EUX2010sec. The project works closely with VoIP companies and users. It aims at providing better security of open source VoIP installations. The work towards this goal is organized by gathering researchers and practitioners around several scientific activities that range from security modeling and verification up to test-bed testing.[4]

Chan YeobYeun and Al-Marzouqi, S.M. (2009)., VoIP is the ability of transmitting voice using the Internet protocol. This paper addresses an introduction to VoIP, threats of VoIP and studies previous works of secure VoIP. They also propose practical implementations for securing VoIP by using Java and Android.[5]

Pecori*et al* (2012)., the security of the protocols involved in peer-to-peer communications is becoming a fundamental prerequisite for their widespread diffusion. In this paper, they propose a new protocol for establishing a security association between two peers willing to set up a VoIP or multimedia communication through the standard SIP protocol. Their proposal is based on the MIKEY protocol and the Diffie-Hellman algorithm for key establishment, in a ZRTP like way.[6]

Butcher *et al* (2007)., in this paper, they examine and investigate the concerns and requirements of VoIP security. After a thorough review of security issues and defense mechanisms, and also focuses on attacks and countermeasures unique to VoIP systems that are essential for current and future VoIP implantations.[7]

Angrisani*et al* (2011).,the paper presents the design and implementation of a reconfigurable test bed for real time measurements on VoIP systems, which provides the Telecommunication Engineer with means to plan the necessary changes in the network/VoIP platform, eventually reaching a higher level of security. At the same time, the test bed permits to take into account the right balance between security instruments and the required QoS/QoE for real time operations.[8]

Sachin*et al* (2013) in this paper shows that the proposed a method to verify authentication of source IP address. They identify the attacks by comparing IP address, corresponding MAC address and BIOS serial number with register database. Detected spoofing was maintained in a log. Their method is very simple and efficient as it will perform in MANET area.[9]

Johan *et al* (2005) in this paper examined the possibility of establishing a secure VoIP telephone call using SIP. Different security services relevant for VoIP are presented and also argue that end-to-end authentication and encryption should be provided by default. For media protection they evaluate the possibility of using either SRTP or IPSec, and they examine several alternatives of how a secure VoIP call can be established. The solution they suggest is based on SRTP for media protection, S/MIME and MIKEY for end-to-end authentication and keying, and TLS for hop-by-hop protection of SIP messages[10].

Sisalem*et al* (2006) in this article they address the issue of denial of service attacks targeting the hardware and software of voice over IP servers or by misusing specific signaling protocol features. As a signaling protocol they investigate here the session initiation protocol. In this context they mainly identify attacks based on exhaustion of the memory of VoIP servers, or attacks that incur high CPU load.[11]

Talevski*et al* (2007) this paper addresses the issues surrounding VoIP security and mobility through the integration of robust security features into a lightweight VoIP protocol that is tailored for mobile devices. A theoretical approach is realized with the development of a software prototype whose security and mobility properties are analyzed.[12]

Keromytis*et al* (2009) in this paper they present a survey of Voice over IP security research. The goal is to provide a roadmap for researchers seeking to understand existing capabilities and, and to identify gaps in addressing the numerous threats and vulnerabilities present in VoIP systems. They also briefly explained the implications of this research findings with respect to actual vulnerabilities reported in variety VoIP products.[13]

Thomas and Richard Kuhn (2005) Although VoIP offers lower cost and greater flexibility, it can also introduce significant risks and vulnerabilities. This article explains the challenges of VoIP security and outlines steps for helping to secure an organization's VoIP network. The paper shows that the security and more specifically about to protecting one of your precious assets- your privacy.[14]

3. PROPOSED METHODOLOGY

The secrets haring schemes encode data into *shares* such that only certain valid combinations of shares can be used to reconstruct the encoded data, while invalid combinations of shares give no information on the encoded data. By storing these shares at different servers, the encoded data is kept confidential as long as not enough servers are compromised. A major change in telecommunication industry is Voice over Internet Protocol (VoIP). VoIP offers interactive communications. It differs from conventional circuit switched networks. It allows people to communicate with each other at very low rates. In Verifiable Secret Sharing Scheme are taking a multilayered approach of (k, n) threshold scheme where it do not only divide the message into n shares to ensure higher security.

Informally, a verifiable secret sharing protocol must meet the following two requirements:

1. Verifiability constraint: upon receiving a share of the secret, a player must be able to test whether or not it is a valid piece. If a piece is valid, there exists a unique secret which will be output by *Recover* when it is run on any 11 distinct valid pieces.
2. Unpredictability: there is no polynomial-time strategy for picking *t* pieces of the secret, such that they can be used to predict the secret with any perceivable advantage.

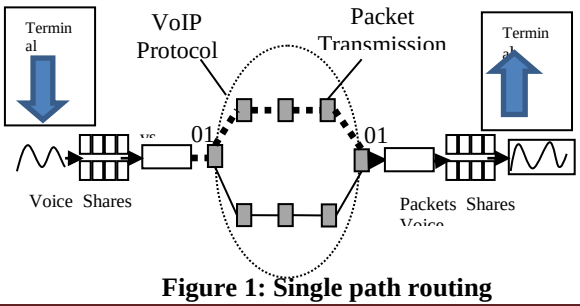

Figure 1: Single path routing

The figure 1 shows the single path routing. The proposed method therefore divides speech data using the secret sharing scheme and transfers the shared data using the single path routing technique to realize secure voice communication over the network. The voice data can be divided into a number of packets. Those packets are transfer from source to destination by integrating VSS with VoIP. The share constructing and share reconstructing is performed for secure sharing. Secret sharing scheme is suitable for proposed method when one would like to encode or decode a message bit by bit.

3.1 Synchronous Vs Asynchronous Communication Model

3.1.1 Synchronous Communication Model

The word synchronous means working together simultaneously, and in the online learning world, chat rooms and online conferences are superior examples of synchronous communication. In a chat room, people's comments to each other are communicated immediately, enabling a simulation-time discussion. Likewise, online conferencing with the advantage of VOIP tools facilitate simulation-time conversations to occur online. Learning from synchronous communication is improved because simulation-time conversations permit people to explore, through writing or talking, the class concepts.

The distributed protocols operate in a sequence of rounds in the synchronous model. In each round, a party performs some local computation, sends messages (if any) to the dealer through the private and authenticated link, and broadcasts some information over the broadcast channel. By the end of the round, it also receives all messages sent or broadcast by the other parties in the same round. In this work synchronous communication model, along with being adaptive and t-bounded, to allow the adversary to be rushing: in every round of communication it can wait to hear the messages of the honest parties before sending (or broadcasting) its own messages. By round complexity of VSS, those mean the number of rounds in the sharing and reconstruction phases of any execution in VoIP application.

3.1.2 Asynchronous Communication Model

In VoIP, to focusing of the asynchronous communication setting where VSS is possible for $n \geq 3t + 1$. The discussion in the related work, all known computational VSS scheme in the asynchronous communication setting rely on homomorphism of commitments. In this work, shows that homomorphism is not necessary for computational VSS in the asynchronous communication setting. To build this research protocol from asynchronous VSS, as it is the only generic and efficient asynchronous VSS scheme known in the literature. Further, with its O (n^2) messages complexity, it is extremely efficient in terms of the number of messages. To modifying this scheme so that it satisfies the VSS properties when the underlying commitment need not be homomorphism. However the existing protocol occasionally does not guarantee that every honest party receives their shares of the secret.

3.1.3 Encryption of shares in VoIP

If there is enough data are received then it performs the construction function in the form of following procedures.

The steps for encoding algorithm are as follows:

Step 1: Get the data to be encoded and the selected key.

Step 2: Create two voice data.

Step 3: Initiate one voice data with numbers from 0 to 255.

Step 4: Fill the other voice data with the selected key.

Step 5: XOR the final key stream with the voice data to be encoded to give cipher text.

3.1.4 Decryption of shares in VoIP

Reconstruction is a process of reversing all that has happened in the construction process. It involves converting the constructed data back to its original form for the receiver's understanding. The same process is performed at the beginning of the encode and decode process. Reconstruction process involves a XOR operation between the encode data and the extracted key, and the end result of such operation is the plain text data (original text).

4. EXPERIMENTAL RESULTS

The networking environment is set up with some nodes in a topology structure, which consists of VoIP flow established between two end points. In this section, express the simulation model of a VoIP application and its implementation in Network Simulator(NS-2). NS-2 is the actual standard simulation tool for the networking community.

The experimental shows the evaluation of simulation networks and results indicate single path of verifiable secret sharing scheme to estimates the actual effort. The important performance metric is End-to-End Delay. It is also called as Packet Latency. This is calculated by the time of packet sent at the sender and received at the receiver. This calculation is not only based on this but also the packets that are successfully delivered at the receiver without any loss of information.

Network Delay is calculated by adding Fixed part Delay with Variable part.

Network Delay = Fixed part + Variable part

Fixed part depends on the performance of the network nodes on the transmission path. Variable part is the time spent in the queues on network load.

Table 1 Shows the network delay for secret sharing

Techniques	Delay (Sec)
Simple VoIP	32
Secure VoIP (VSS)	19

In Table 1 shows the delay values by calculating network delay in secret sharing. In this table the delay time for

standard VoIP scheme are high when compared to this proposed VSS approach.

5. CONCLUSION

Voice over Internet Protocol is a new and up growing technology. A major change in telecommunication industry is VoIP. The transmission of real time voice data is not as easy as ordinary text data. This work addresses the security and packet delivery ratio of a VoIP using verifiable secret sharing algorithm over a single path with reduced packet loss. The simulation results show that higher accuracy and reduced execution time is achieved in terms of end – to – end delay and packet delivery ratio. The user gets bad quality of VoIP at the receiver side. This makes the deployment of real time application a challenging task. To overcome these challenges in VoIP, several solutions have been reported already. To provide end to end security between the source destination pair, the single path routing scheme is introduced. In this work suggested future scope in the area of multi-path routing protocols where the main focus will be on using multiple paths for message/s forwarding.

REFERENCES

1. Akbar, Imran M. "Method and system for providingprivate virtual secure Voice over Internet Protocol communications." U.S. Patent 7,852,831, issued December 14, 2010.
2. Huang, Y. F., S. Tang, and Y. Zhang. "Detection of covert voice-over Internet protocol communications using sliding window-based steganalysis."*Communications, IET* 5, no. 7 (2011): 929-936.
3. Huang, Yongfeng, Shanyu Tang, ChunlanBao, and Yau Jim Yip. "Steganalysis of compressed speech to detect covert voice over Internet protocol channels."*Information Security, IET* 5, no. 1 (2011): 26-32.
4. Chand, Naresh, and Bruce M. Eteson. "Communication network with secure access for portable users." U.S. Patent 8,406,427, issued March 26, 2013.
5. Wu, Tsu-Yang, and Yuh-Min Tseng. "A pairing-based publicly verifiable secret sharing scheme." *Journal of Systems Science and Complexity* 24, no. 1 (2011): 186-194.
6. Pedersen, TorbenPryds. "Non-interactive and information-theoretic secure verifiable secret sharing." In *Advances in Cryptology—CRYPTO'91*, pp. 129-140. Springer Berlin Heidelberg, 1992.
7. Nagano, Takeshi, and Akinori Ito. "Packet Loss Concealment of Voice-over IP Packet using Redundant Parameter Transmission Under Severe Loss Conditions." *Journal of Information Hiding and Multimedia Signal Processing* 5, no. 2 (2014): 285V294.
8. Stadler, Markus. "Publicly verifiable secret sharing." In *Advances in Cryptology—EUROCRYPT'96*, pp. 190-199. Springer Berlin Heidelberg, 1996.
9. Papakotoulas, Anestis. "Voice over Internet Protocol." *Journal of Computations &Modelling* 4, no. 1 (2014): 299-310.
10. Fujisaki, Eiichiro, and Tatsuaki Okamoto. "A practical and provably secure scheme for publicly verifiable secret sharing and its applications." In *Advances in Cryptology—EUROCRYPT'98*, pp. 32-46. Springer Berlin Heidelberg, 1998.
11. Kumaresan, Ranjit, ArpitaPatra, and C. PanduRangan. "The round complexity of verifiable secret sharing: The statistical case." In *Advances in Cryptology-ASIACRYPT 2010*, pp. 431-447. Springer Berlin Heidelberg, 2010.
12. Backes, Michael, Aniket Kate, and ArpitaPatra. "Computational verifiable secret sharing revisited." In *Advances in Cryptology–ASIACRYPT 2011*, pp. 590-609. Springer Berlin Heidelberg, 2011.
13. Harn, Lein, Miao Fuyou, and Chin-Chen Chang. "Verifiable secret sharing based on the Chinese remainder theorem." *Security and Communication Networks* 7, no. 6 (2014): 950-957.
14. Chandrasekar, C., and S. Padmavathy. "Secured Routing Protocol based on Secret Sharing in Voice Systems." *Networking and Communication Engineering*5, no. 1 (2013): 33-38.