# A NEW SECURED VoIP USING VERIFIABLE SECRET SHARING

R. Shankar[1] and E. Karthikeyan[2]
[1]Department of Computer Science, Bharathiar University, Coimbatore, India
[2]Computer Science, Govt. Arts College, Udumalpet, India
E-Mail: shankaran_1973@yahoo.com

**ABSTRACT**

Voice communication carried out using the Internet Protocol (IP) for the transaction is known as Voice over Internet Protocol (VoIP). Voice over Internet Protocol is a technology for communicating using "Internet protocol" instead of traditional analog systems. Some VoIP services need only a regular phone connection, while others allows making telephone calls using an Internet connection instead. Some VoIP services may allows only to call other people using the same service, but others may allow to call any telephone number - including local, long distance, wireless and international numbers. The fundamental idea of secret sharing is the secret message is sending through a single specified path in secured manner, so secrete sharing is must for sharing VoIP messages. There are several secret sharing's used in VoIP, the most secured VoIP is Verifiable Secret Sharing (VSS). Verifiable Secret Sharing is an important primitive in distributed information that allows a dealer to share a secret among huge number of parties. Verifiable secret sharing is a way of giving information to a set of processors such that a quorum of processors is needed to access the information. VSS is a fundamental tool and distributed computing. Experimental result shows thus the proposed method of verifiable secret sharing is much secured because it overcomes the problems from packet loss, delay, security and quality.

**Keywords:** VoIP protocol, verifiable secret sharing, short message services, single path routing, end-to-end delay.

## 1. INTRODUCTION

VoIP is becoming an attractive communications option for consumers. Given the trend towards lower fees for basic broadband service and the brisk adoption of even faster internet offerings, VoIP usage should only gain popularity with time. However, as VoIP usage increases, so will the potential threats to the typical user. While VoIP vulnerabilities are typically similar to the ones users face on the internet, new threats, scams, and attacks unique to IP telephony are now emerging. VoIP is available on many smart phones, personal computers, and on Internet access devices. Using 3G or Wi-Fi may be sent over Calls and SMS text messages. The security concerns of VoIP telephone systems are similar to those of any Internet-connected device.

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. Use VoIP; 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. LITRATURE SURVEY

A method and system for secure Voice over Internet Protocol communications are introduced by Papakotoul as and Anestis (2014). The method and system provide secure VoIP voice calls, video, Instant Messaging (IM), Short Message Services (SMS), or Peer-to-Peer (P2P) communications while maintaining privacy over the Internet and other communications networks such as the Pubic Switched Telephone Network (PSTN) to and from any network device through a virtual private network infrastructure interconnecting private VoIP network devices are shown by Akbar and Imran (2010) and Huang *et al.* (2011).A Verifiable Secret Sharing Scheme (VSS) has been proposed to allow shareholders to verify that their shares are generated by the dealer consistently without compromising the secrecy of both shares and the secret are given by Harn *et al.* (2014). Nagano *et al.* (2014) gives packet Loss Concealment of Voice-over IP Packet.

A communication network includes a Local Area Network (LAN) and a wireless access point coupled to the LAN and associated wireless devices introduced by Chand *et al.* (2013). A Publicly Verifiable Secret Sharing (PVSS) scheme is a verifiable secret sharing scheme with the special property that anyone is able to verify the shares whether they are correctly distributed by a dealer shown by Wu *et al.* (2011). Pedersen and TorbenPryds (1992) show how a number of persons can choose a secret "in the well" and distribute it verifiably among themselves. Verifiable secret sharing has been proposed to achieve security against cheating participants and verify that the shares are correctly distributed is shown by Stadler and Markus (1996).

Fritsch *et al.* (2009) this paper describes the approach and preliminary results of project works closely with Voice-over-IP companies and users. It aims at providing better security of open source VoIP installations. A Publicly Verifiable Secret Sharing (PVSS) scheme, named by Fujisaki *et al.* (1998), is a special VSS scheme in which anyone, not only the shareholders, can verify that the secret shares are correctly distributed. PVSS can provide some interesting properties in the systems using VSS. Kumaresan *et al.* (2010) consider the round complexity of a basic cryptographic task: *verifiable secret sharing*.

Backes *et al.* (2011) present new VSS schemes based only on the definitional properties of commitments that are almost as good as the existing VSS schemes based on homomorphism commitments. Voice over IP is the process of transmission of voice over packet-switched IP networks is one of the most important emerging trends in telecommunications. VOIP has a very different architecture than traditional circuit-based telephony, and these differences result in significant security issues is shown by Chandrasekhar and Padmavathy (2013).

## 3. PROPOSED METHODOLOGY

The secret sharing 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) thresh old 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.

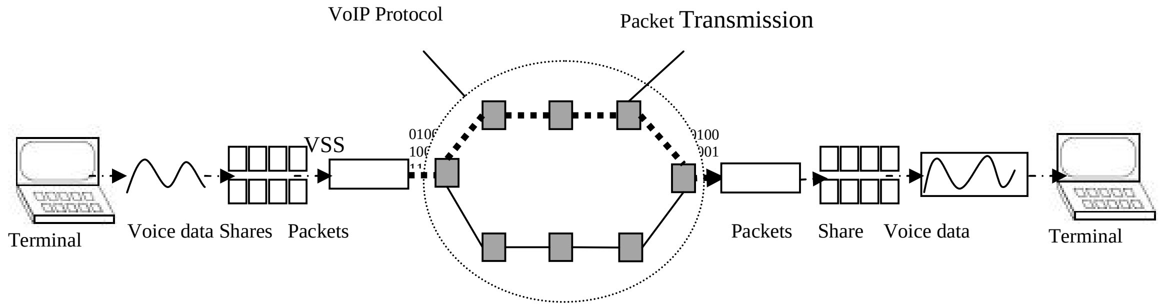

**Figure-1.** Single path routing.

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.

The following steps used for secret sharing performance

**Step-1:** Create set S with VoIP protocol, which includes all the possible network security state vectors

**Step-2:** Calculate values for each elements.

**Step-3:** Create set A, which include all the possible share allocation vectors.

**Step-4:** Distributing the secrets in time domain basis by sending out the shares over a certain period of time.

**Step-5:** If the value assigned is very small, the link will expire too soon. At the same time if the value of lifetime is too big, there may be a route error. This will degrade the overall performance.

**Step-6:** Choosing the optimal value of static life time shows the performance of this algorithm with VoIP.

### 3.1 Verifiable Secret Sharing (VSS)

Verifiable secret sharing is important for secure multiparty computation. Multiparty computation is typically accomplished by making secret shares of the inputs, and manipulating the shares to compute some function.

### 3.1.1 Procedure for VSS

1. The dealer chooses randomly $a_1, \ldots a_t \in Z_p$ and define $f(x) = a_t x^t + \cdots + a_1 x + s$

2. They also pick random polynomials, $g_1(x), \dots, g_{k.n}(x)$, each of degree *t*.
3. They compute $f(\alpha_i), g_j(\alpha_i) for\ 1 \leq i \leq n,\ 1 \leq j \leq k.n$.
4. Then hand over toP$_i$ the data.
5. The secret sharing is encrypted by the standard encryption algorithm using an encryption key *E*.
6. Using encryption key *E* obtained from step 5 we decrypt the encrypted VoIP using the standard scheme which is used for encryption. And finally the original VoIP message is obtained with absolutely no loss.

Verifiable secret sharing enables a communication network to suggest a simultaneous broadcast network. Therefore, they present another protocol for VoIP that achieves this stronger definition using the previous one as a building block. In this research, the final VSS in VoIP increases the communication complexity by a linear factor in n, it is still highly efficient in all complexity measures. These encoders are used in current VoIP communication because they are more robust against packet loss than other methods.

### 3.1.2 Construction of shares in VoIP

If there is enough data's 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 voice 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.

### 3.1.3 Reconstruction of Voice data from Shares

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.

The network delay is calculated as 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.

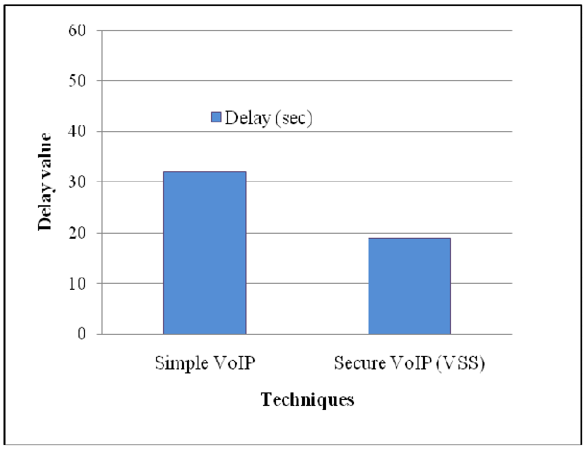

**Figure-2.** The network delay by for secret sharing schemes.

Figure-2 shows that network delay for simple VoIP and secret VoIP. The proposed method of secret VoIP with VSS has less delay rate.

## 5. CONCLUSIONS

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. 2010. Method and system for providing private virtual secure Voice over Internet Protocol communications. U.S. Patent 7,852,831, issued December 14.

[2] Huang Y. F., S. Tang and Y. Zhang. 2011. Detection of covert voice-over Internet protocol communications using sliding window-based steganalysis. Communications, IET. 5(7): 929-936.

[3] Huang Yongfeng., Shanyu Tang., ChunlanBao and Yau Jim Yip. 2011. Steganalysis of compressed speech to detect covert voice over Internet protocol channels. Information Security, IET. 5(1): 26-32.

[4] Chand Naresh and Bruce M. Eteson. 2013. Communication network with secure access for portable users. U.S. Patent 8,406,427, issued March 26.

[5] Wu Tsu-Yang and Yuh-Min Tseng. 2011. A pairing-based publicly verifiable secret sharing scheme. Journal of Systems Science and Complexity. 24(1): 186-194.

[6] Pedersen TorbenPryds. 1992. Non-interactive and information-theoretic secure verifiable secret sharing. In Advances in Cryptology—CRYPTO'91, pp. 129-140. Springer Berlin Heidelberg.

[7] Nagano Takeshi and Akinori Ito. 2014. 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(2): 285V294.

[8] Stadler Markus. 1996. Publicly verifiable secret sharing. In Advances in Cryptology—EUROCRYPT'96. Springer Berlin Heidelberg. pp. 190-199.

[9] Papakotoulas, Anestis. 2014. Voice over Internet Protocol. Journal of Computations & Modelling. 4(1): 299-310.

[10] Fujisaki Eiichiro. and Tatsuaki Okamoto. 1998. A practical and provably secure scheme for publicly verifiable secret sharing and its applications. In Advances in Cryptology—EUROCRYPT'98. Springer Berlin Heidelberg. pp. 32-46.

[11] Kumaresan Ranjit., ArpitaPatra and C. Pandu Rangan. 2010. The round complexity of verifiable secret sharing: The statistical case. In Advances in Cryptology-ASIACRYPT 2010. Springer Berlin Heidelberg. pp. 431-447.

[12] Backes Michael., Aniket Kate and ArpitaPatra. 2011. Computational verifiable secret sharing revisited. In Advances in Cryptology–ASIACRYPT 2011. Springer Berlin Heidelberg. pp. 590-609.

[13] Harn Lein., Miao Fuyou and Chin-Chen Chang. 2014. Verifiable secret sharing based on the Chinese remainder theorem.Security and Communication Networks. 7(6): 950-957.

[14] Chandrasekar C. and S. Padmavathy. 2013. Secured Routing Protocol based on Secret Sharing in Voice Systems. Networking and Communication Engineering. 5(1): 33-38.

[15] Fritsch, Lothar, A-K. Groven and Lars Strand 2009. A holistic approach to open-source VoIP security: Preliminary results from the EUX2010sec project." In Networks, ICN'09 Eight International Conference on, pp. 275-280, IEEE.