VOL. 10, NO. 6, APRIL 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

A NEW SECURED VoIP USING HIERARCHICAL THRESHOLD SECRET SHARING

E. S. Thirunavukkarasu[1] and E. Karthikeyan[2]
[1]Department of Computer Science, Bharathiar University, Coimbatore, India
[2] Department of Computer Science, Government Arts College, Udumalpet, India
E-Mail: arasu_igr@yahoo.co.in

ABSTRACT

Voice over Internet Protocol is a category of hardware and software that enables people to use the Internet as the transmission medium for telephone calls by sending voice data in packets using IP rather than by traditional circuit transmissions of the PSTN. The transmission of real time voice data is not as easy as ordinary text data and the real time voice transmission faces lot of difficulties. It suffers from packet loss, delay, quality and security. One prominent advantage of VoIP is that the telephone calls over the Internet do not incur a surcharge beyond what the user is paying for Internet access, much in the same way that the user doesn't pay for sending individual messages over the Internet. VoIP provides a protected transmission of private voice data between two endpoints. In those settings in VoIP, the participants between secret sharing scheme into a variety of levels. The hierarchical secret sharing is one of the best schemes in VoIP because it is more easy and simple to compute and implement in the real-life. An analysis of the signaling process and a study of simulation results have shown the advanced security enhancements in VoIP.

Keywords: secret sharing scheme, VoIP infrastructure, single path routing, hierarchical threshold secret sharing, packet loss concealment.

1. INTRODUCTION

The data in VoIP networks is a packet switched and interactive network. The traditional Public Switch Telephone Network (PSTN) is circuit switched. The circuit switched network is secure one but the packet switched internet is not. It is designed with less security features. In conventional PSTN the entire communication paths were administered by a few authorized telephone companies. It was therefore difficult for a malicious person to wiretap conversations over telephones because persons who were allowed to access the network were carefully restricted. The recently grown internet protocol telephone or VoIP has multiple intermediates exist between the two endpoints (telephones).

A message is divided into shares which are sending through a single path using proposed hierarchical threshold secret sharing algorithm is implemented to provide reliable data delivery. The fundamental idea of secret sharing is the secret message is sending through a single path routing. The enemy can easily compromise the message by troubling anyone of the nodes all along the path. To solve this, the message is divided into shares or pieces. The pieces are sending through the specified path. A certain number of shares are used to reconstruct the original secret message. This is termed as threshold secret sharing. Any shares less than threshold can not do anything. For instance, using this research proposed scheme, the participants are arranged in a hierarchical structure according to their position or rank and each first level participant as a parent node delegates his power to the lower level hierarchical group members. The group members help to reconstruct the secret shares of their parent nodes in their absence and the secret key is reconstructed even if at least one parent node is present.

The rest of this research work is organized as follows. Section II summarizes the concepts and related works. Section III provides the proposed method, and Section IV discusses the experiments and the achieved results. Finally, Section V presents the conclusions of the work.

2. LITERATURE SURVEY

Zhu *et al* (2013), a Voice-over-IP (VoIP) solution is provided where in a 911 call from a mobile VoIP device is routed directly to the correct Public Safety Answer Point (PSAP) via dedicated trunks, together with correct location information and call-back number. An intelligent bandwidth management scheme for VoIP is given by Yuan *et al* (2014). Nafeesa *et al* (2014) shows two tier protocols for hierarchical access control. Raleigh and Gregory (2014) perform restricting end-user device communications over a wireless access network.

Jackson *et al* (2012), Systems and methods to minimize customer premises equipment downtime in a Voice over Internet Protocol service network are disclosed. A technique to enhance the security of vocal communication over an open network is proposed in this paper. The technique combines a secret sharing scheme and a multipath routing technique on network communication was developed by Nishimura *et al.* (2010). A system for verifying VoIP call routing information was introduced by Jennings *et al* (2012). In one embodiment, a system is provided to restrict VoIP communication was presented by Rosenberg *et al* (2012). Fortescue *et al* (2012) demonstrate a new construction for perfect Quantum Secret Sharing (QSS) schemes based on imperfect “ramp” secret sharing combined with classical encryption, was presented by them. A protocol for member expansion in quantum (*t,n*) threshold secret

sharing schemes was proposed by Yang *et al* (2011). Das *et al.* (2010), present a renewable, multi-use, multi-secret sharing scheme for general access structure based on the one-way collision resistant hash function is presented in which each participant has to carry only one share. Farras *et al.* (2010) exposes and proved that every ideal hierarchical access structure is the port of a represent able matroid and, more specifically, they prove that every ideal structure in this family admits ideal *linear* secret sharing schemes over fields of all characteristics. Ballico *et al.* (2006) represents that secret sharing schemes provide a natural way of addressing security issues in ad hoc networks. Farras *et al.* (2010), Hierarchical secret sharing is among the most natural generalizations of threshold secret sharing, and it has attracted a lot of attention from the invention of secret sharing. Guo *et al* (2012), they consider the problem of secret shadow images with a hierarchical threshold structure, employing Tassa's hierarchical secret sharing to propose a hierarchical threshold secret image sharing scheme. Wei *et al* (2007), in this work, a new dynamic threshold secret sharing scheme was proposed, which is based on bilinear maps.

Figure-1 shows the secret sharing in VoIP protocol. 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 HTSS with VoIP. The share constructing and share reconstructing is performed for secure sharing.

Following procedures are to share the secret information in VoIP.

- Dividing the secret message into N multiple pieces called shares.
- The enemy has to compromise at least T shares.
- Designed for cheating detection and cheater identification.
- Proposed Hierarchical threshold secret sharing scheme is implemented.

3. PROPOSED METHODOLOGY

Voice over Internet Protocol (VoIP) is used to provide secure tunnels to authenticated remote endpoints or servers. VoIP integrate with Hierarchical Threshold Secret Sharing (HTSS). In VoIP using a collection of hierarchical structure causes the threshold secret sharing tribulations.

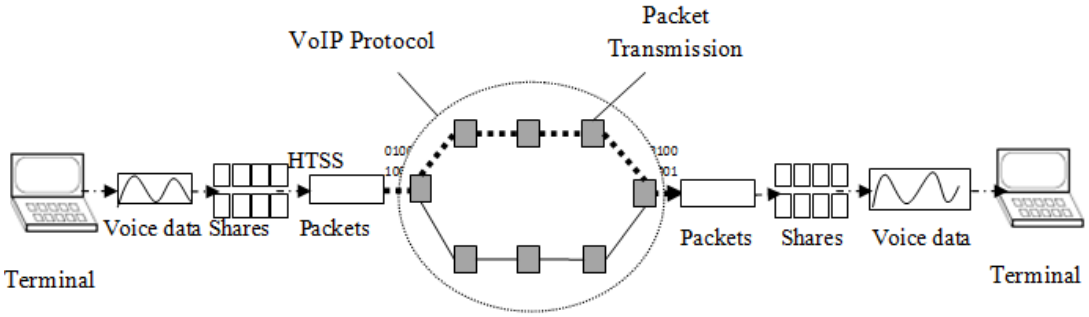

Figure-1. Secret sharing in VoIP protocol.

3.1 Hierarchical threshold secret sharing

The access structure is then determined by a sequence of threshold requirements: a subset of participants is authorized if it has at least k_0 members from the highest level, as well as at least $k_1 > k_0$ members from the two highest levels and so forth. Such problems may occur in settings where the participants differ in their authority or level of confidence and the presence of higher level participants is imperative to allow the recovery of the common secret. Even though secret sharing in hierarchical groups has been studied extensively in the past, none of the existing solutions addresses the simple setting where, say, a bank transfer should be signed by three employees, at least one of whom must be a department manager. This work presents a perfect secret sharing scheme for this problem that, unlike most secret sharing schemes that are suitable for hierarchical structures, is ideal.

3.1.1 Algorithm for HTSS scheme

Consider the hierarchical secret sharing problem (k, n), as defined. Let F be a finite field of size q which is at least as large as the number of possible secrets. Let $k = k_m$ is the overall number of participants that are required for recovery of the secret. Then

a) The dealer selects a random polynomial ,where

$$P(x) = \sum_{i=0}^{k-1} a_i x^i \text{ and } a_0 = S \quad (1)$$

b) The dealer identifies each participant u ∈ U with a field element. For simplicity, the field element that

corresponds to u∈ U will be also denoted by u (whence U may be viewed as a subset of $\mathbb{F}$).

c) The dealer distributes shares to all participants in the following manner: Each participant of the i_{th} level in the hierarchy, u $\in U_i$, $0 \le i \le m$, receives the share $P^{(ki-k)}(u)$, i.e., the (k_{i-1}) (u) derivative of P(x) at x = u, where $k_{-1}= 0$. (A reminder: given a polynomial $P(x) = \sum_{i=0}^{n} a_i x^i$ over any field $\mathbb{F}$, its derivative is defined formally as $P'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$.)

Let (k, n) be a hierarchical threshold secret sharing problem. Assume that the participants in U were assigned identities in F = F_q, q being a prime, in a monotone manner, namely, in concert with condition (u∈Ui, v∈Uj, i< j ⇒u< v), and let N = max U. Finally, assume that

$$2^{-k}.(k+1)^{(k+1)/2}.N^{(k-1)k/2} \ll q = |\mathbb{F}| \quad (2)$$

The hierarchical secret sharing schemes are the Threshold secret sharing which are more scalable, and secure. Secret share update makes the system tolerate long-term intrusions. The HTSS using strengthening safety for VoIP process the location of routers are both wired and wireless networks.

3.1.2 Construction of shares in VoIP

Secured construction is the process of converting original voice into some other format (cipher voice). Following steps are used for encode voice data.

Step-1: Sender reads the input voice and encodes the voice data packets using the receiver's public key to transmit the message.

Step-2: Original voice is constructed and the encode data packets (cipher voice) C is,

$$C = m^e \pmod n$$

Step-3: Now the encoded voice data packets are stored in the database.

3.1.3 Reconstruction of Voice Packets in VoIP

Secured reconstruction is the process of converting the shares into original voice.

Step-1: Receiver receives the encoded data from the database.

Step-2: Decode the encoded voice data packets by computing,

$$m = C^d \pmod n.$$

Step-3: By finding the value of m the receiver can get back the original data by reversing the padding Scheme.

4. EXPERIMENTAL RESULTS

The experimental shows the hierarchical secret sharing scheme with single path routing using Network Simulator-2 (NS-2). The playout buffer distributes speech frames to the decoder, which essentially playbacks them. Some decoders implement Packet Loss Concealment (PLC) methods, which permit missing speech frames to be to some extent recreated by interpolating (correctly received) neighboring frames. PLC techniques can observably cover a limited number of losses in VoIP. 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.

Average End-End delay = Time Delay/Packet Received

Table-1. Accuracy and execution time for HTSS.

Secret sharing scheme	Packet loss rate (%)
Simple VoIP	75
Secured VoIP (HTSS)	49

In Table-1 shows the accuracy and execution time for both existing Shamir's secret sharing and proposed hierarchical threshold secret sharing techniques. The proposed HTSS techniques are more accurate and much low in implementation time.

For example, the following standards must be met:

- The default G.729 codec requires packet loss far less than 1 percent to avoid audible errors. Ideally, there should be no packet loss for VoIP.
- G.711 is a narrowband audio codec that provides toll-quality audio at 64 kbit/s. It recommends less than 150 millisecond (ms) one-way end-to-end delay for high-quality real-time traffic such as voice. (For international calls, one-way delay up to 300 ms is acceptable, especially for satellite transmission. This one-way delay takes propagation delay into consideration-the time required for the signal to travel the distance.)

The voice packets were indiscriminately dropped after the UDP traffic became active; packet loss rate was constantly over 500 packets per second. This is more than 8% of the total packets generated and such a high packet loss rate is detrimental to voice quality 3. Packet loss can be expressed by the following formula,

$$I_{pl} = \left(1 - \frac{N}{DS}\right) * 100\%$$

Where, DS is the difference between the largest and smallest sequence number of N packets. Statistics and calculation of the Real-time Transport Protocol (RTP) packets can be used to calculate this percentage by the following expression. N is the number of instance.

$$DS = LS\text{-}SS+1$$

Where, LS and SS are the largest and smallest sequence numbers, respectively. They are extracted from the RTP header of the sequence number field from the packets received.

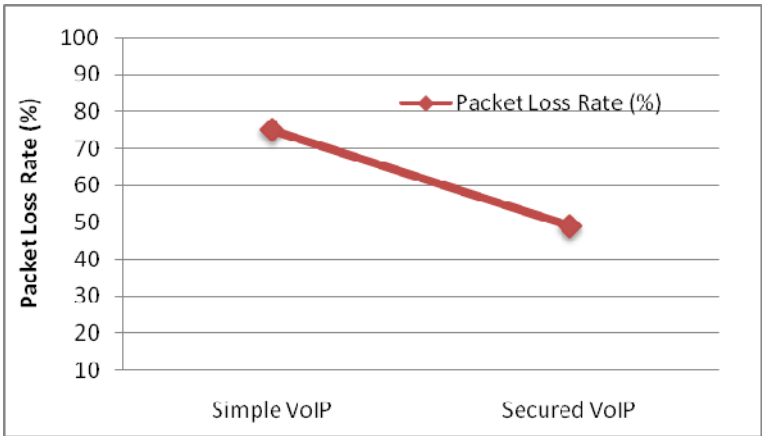

Figure-2. Packet loss rate for secret sharing using Network Simulator-2.

Figure-2 represents the packet loss rate for proposed HTSS technique. Comparing with existing method, the hierarchical threshold secret sharing method is much better in their performance for secret share. The hierarchical features are very efficient for reconstructing the secret information or images without increasing the risk of disclosure.

5. CONCLUSIONS

The streaming of audio or video content over the Internet is a challenging task. This is due to the fact that the Internet is a packet switched network with a service guarantee. The major challenge of the VoIP network is maintaining quality as well as security. This work shows the result in a better performance using the simulator such as NS-2. In single-path routing, only a single route is used between a source and the destination. The performance is satisfied in terms of quality. But the increased Delay and security are again at a greater risk. This scheme reduces the complexity of route discovery process, Reduces routing overhead, heavy traffic, less route error and improved performance. In future work, Multi-path protocols learn routes will use to select more than one path to a destination. These protocols are better for performing load balancing.

ACKNOWLEDGEMENT

We would like to express our special thanks of gratitude to all authorities of Anna University, Chennai as well as all authorities of Government Arts College, Udumalpet for providing us the necessary guidance and facility to carryout present research.

REFERENCES

Zhu Yinjun, Richard Dickinson, Roger Marshall and Steven P. Helme. 2013. Solutions for voice over internet protocol (VoIP) 911 location services. U.S. Patent 8,385,881, issued February 26.

Jackson James, Bernard Ku and Mehrad Yasrebi. 2012. Systems and methods to minimize customer equipment downtime in a voice over internet protocol (VOIP) service network. U.S. Patent 8, 125, 999, issued February 28.

Nishimura Ryouichi, Shun-ichiro Abe, Norihiro Fujita and Yoiti Suzuki. 2010. Reinforcement of VoIP security with multipath routing and secret sharing scheme. Journal of Information Hiding and Multimedia Signal Processing. 1 (3): 204-219.

Jennings Cullen F., Jonathan Rosenberg and Daniel G. Wing. 2012. Using PSTN reachability to verify VoIP call routing information. U.S. Patent 8, 199, 746, issued June 12.

Rosenberg Jonathan David and Cullen F. Jennings. 2012. Restriction of communication in VoIP addresses discovery system. U.S. Patent 8, 274, 968, issued September 25.

Fortescue Ben and Gilad Gour. 2012. Reducing the quantum communication cost of quantum secret sharing. Information Theory, IEEE Transactions on. 58(10): 6659-6666.

Yang Yu-Guang, Yuan Wang, Hai-Ping Chai, Yi-Wei Teng and Hua Zhang. 2011. Member expansion in quantum (< i> t, n</i>) threshold secret sharing schemes. Optics Communications. 284(13): 3479-3482.

Das Angsuman and Avishek Adhikari. 2010. An efficient multi-use multi-secret sharing scheme based on hash function. Applied mathematics letters. 23(9): 993-996.

Farras Oriol and Carles Padró. 2010. Ideal hierarchical secret sharing schemes. In Theory of cryptography. Springer Berlin Heidelberg. pp. 219-236.

Ballico Edoardo, Giulia Boato, Claudio Fontanari and Fabrizio Granelli. 2006. Hierarchical secret sharing in ad hoc networks through birkhoff interpolation. In Advances

in Computer, Information, and Systems Sciences and Engineering. Springer Netherlands. pp. 157-164.

Farras Oriol and Carles Padró. 2010. Ideal hierarchical secret sharing schemes. In Theory of cryptography. Springer Berlin Heidelberg. pp. 219-236.

Guo Cheng, Chin-Chen Chang and Chuan Qin. 2012. A hierarchical threshold secret image sharing. Pattern Recognition Letters. 33(1): 83-91.

Wei C., Xiang, L., Yuebin, B. and Xiaopeng G. 2007. A new dynamic threshold secret sharing scheme from bilinear maps. In: Parallel Processing Workshops, 2007. ICPPW 2007. International Conference on. IEEE. p. 19.

Nafeesa Begum, J., K. Kumar and V. Sumathy. 2014. Two tier protocol for hierarchical access control in medical image transmission. In: Computing for Sustainable Global Development (INDIACom), 2014 International Conference on, pp. 769-775. IEEE.

Raleigh Gregory G. 2014. Restricting end-user device communications over a wireless access network associated with a cost. U.S. Patent Application 14/151,769, filed January 9.

Yuan Zhenhui and Gabriel-Miro Muntean. 2014. iVoIP: an intelligent bandwidth management scheme for VoIP in WLANs. Wireless networks. 20 (3): 457-473.