I J C T A, 10(8), 2017, pp. 567-571 ISSN: 0974-5572

Enhancing Security of Vocal Communication Over Open Network Using Multipath Routing

Sonali Patil[1], Shweta Lokhande[2], Trishala Kamble[3] and Priyanka Dhumal[4]

ABSTRACT

In today's era, communication over network is growing at large extent due to which it has become necessary to offerprotection to the information. Secure voice data sharing and multipath routing is used to increase the security of vocal communication over an open Network. In this paper, a system is proposed which uses the graphical masking algorithm of secret sharing with multipath routing approach. This technique uses the combination of secret sharing with a multiple different paths routing technique for network communication. The secret sharing scheme, proposes a method to share information between two parties by dividing the information into multiple parts and then reassembly of the parts by the receiving party is done to get the original message. Due to multipath routing technique information is passed through different paths. Thus the proposed system reduces load on network channel and also provides high security.

Keywords: Network Security, Information Security, Secret Sharing, graphical masking, multipath routing

1. INTRODUCTION

Day by day audio messages are heavily used for communicating information. Hence security of this audio data is also must. To offer the protection to important voice data, secret sharing plays a major role. In audio secret sharing [5] the important audio data is divided into shares and then these shares are transferred over the network. At the receiver side expected minimum numbers of shares arerequired to gain the original data. Even if anyone not intended person, get the share it will not reveal any original data. In single path routing the shares gets send through single path due to which if attacker attacks that path he can get access to all shares. To overcome this problem multipath routing can be used. In multipath routing the shares of the secret are send over multiple paths and then at receiving end the user receives the shares from multiple paths and then the receiver reassembles the shares and gets the original information. The further part of the paper focuses on literature survey, proposed technique and conclusion.

2. LITERATURE SURVEY

2.1. Shamir's Secret Sharing [2]

In Shamir's secret sharing method is used to divide the secret information amongst a group of participants, each of the participant is allocated a share of the secret. At the sender end the sender divides the secret into multiple shares and at the receiver end the receiver reconstructed the secret using k number of shares. The (k, n) threshold secret sharing, uses k number of shares to construct the data.

[1] Associate Professor Computer Department Pimpri Chinchwad College of Engineering Pune, India, *Email: sonalimpatil@gmail.com*

[2] Student Computer Department Pimpri Chinchwad College of Engineering Pune, India, *Email: lokhandeshweta22@gmail.com*

[3] Student Computer Department Pimpri Chinchwad College of Engineering Pune, India, *Email: kambletrishala@gmail.com*

[4] Student Computer Department Pimpri Chinchwad College of Engineering Pune, India, *Email: dhumalpriyanka20@gmail.com*

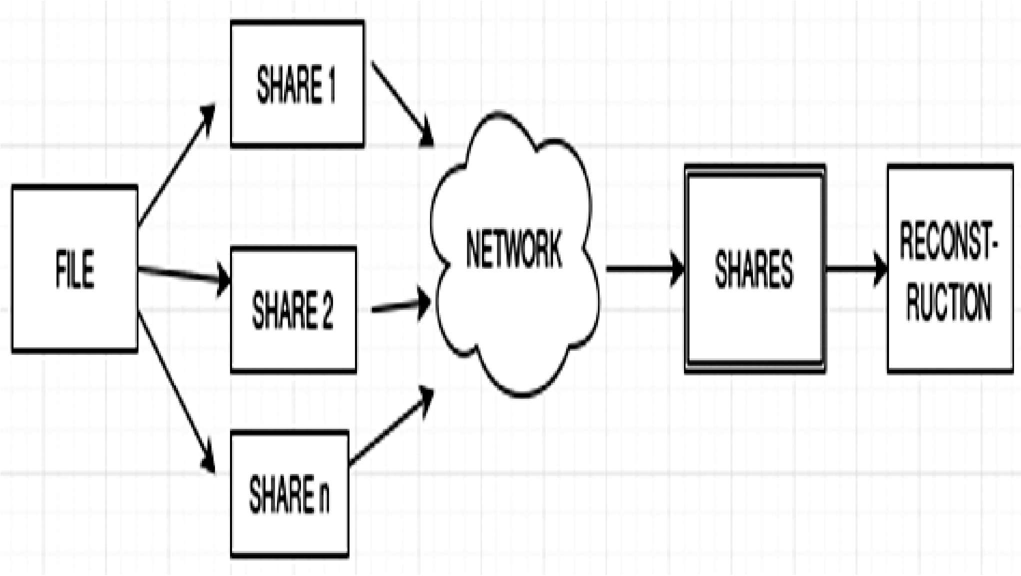

Figure 1: Shamir's Secret Sharing Scheme

Algorithm:Secret Sharing

1. Start
2. To divide a secret message into N pieces, follow the steps:

   a. Select a random k – 1 degree, where polynomial,

   $$q(x) = a0 + a1x + \ldots + ak-1Xk-1$$

   In which a0 is secret data.
3. Send the different shares through multiple paths.
4. Evaluate it using Lagrange's interpolation.
5. Stop

2.2. Graphical Masking [3]

It is (k, n) secret sharing for audio data. This technique uses two operations:

1) ANDing
2) ORing

AND operation is used in construction phase. Random matrix is used as a mask matrix. The original vocal data is ANDed with individual mask in the matrix.Reconstruction is done by ORing the minimal required shares specified by threshold k. In graphical masking two methods are used.

Algorithm:Generate Mask Matrix

1. Initial size of matrix is ${}^{n}C_{k-1}$* n.
2. The matrix is generated where each row has (k-1) zero's and (n-k+1) one's.
3. The generated matrix is transposed to form the final mask matrix having the dimension n* ${}^{n}C_{k-1}$.
4. Each row of this matrix will represent a mask entity.

2.3. Secret sharing scheme for reinforcement of VoIP security [4]

For reinforcement of VoIP security, Shamir's secret sharing scheme is combined with multipath routing.Using the Shamir's scheme the audio data is being divided into shares. These shares are sent over the network via

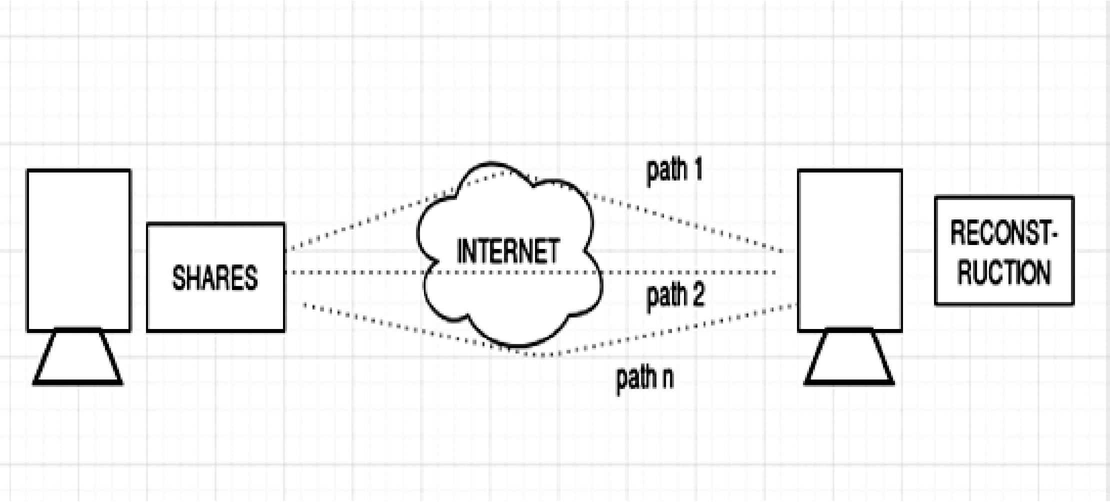

Figure 2: Multipath Routing

multiple paths in the network. The receiver may receive the minimum number of shares from any of the paths in the network. The receiver then applies the shamir's secret sharing algorithm to reconstruct the secret.

Shamir's secret sharing scheme uses single path to send the secret over the network and thereby increases the load on single channel, this may to lead to reveal the secret to the attacker as attacker can get the multiple shares from this single channel.

VOIP used multiple paths in the network to transfer shares, but it uses Shamir's secret sharing technique which is having more computational complexity.[5] [6] also proposed audio secret sharing to provide security to audio data.

This paper proposes a technique which uses multipath with Graphical masking which is explained in next section.

3. PROPOSED TECHNIQUE

A proposed work is audio data sharing through (k, n) secret sharing scheme. In this scheme n number of shares are generated and n number of masks are created. Among n masks any k number of shares can be used to regenerate original message. While generating shares AND operation is used and when the original message needs to be retrieved OR operation is used. While transmitting the shares if the shares are transmitted through single path if any attackers target the path then he may get access to all shares or to number of shares which will lead to recovery of original audio data. So, to overcome this drawback we can transmit the shares through multiple routing paths.

3.1. Concept

Transmitter and receiver are the two end points considered between the open networks. The transmitter takes the original audio message which needs to be share between two parties. Then these audio messages are divided into *n* number of shares using the graphical masking scheme. These generated shared are then transmitted to the receiving end through multipath paths. When the shares are received the original audio message can be retrieved back by using any *k* number of shares.

3.2. Algorithm

Creation of shares from original of data:

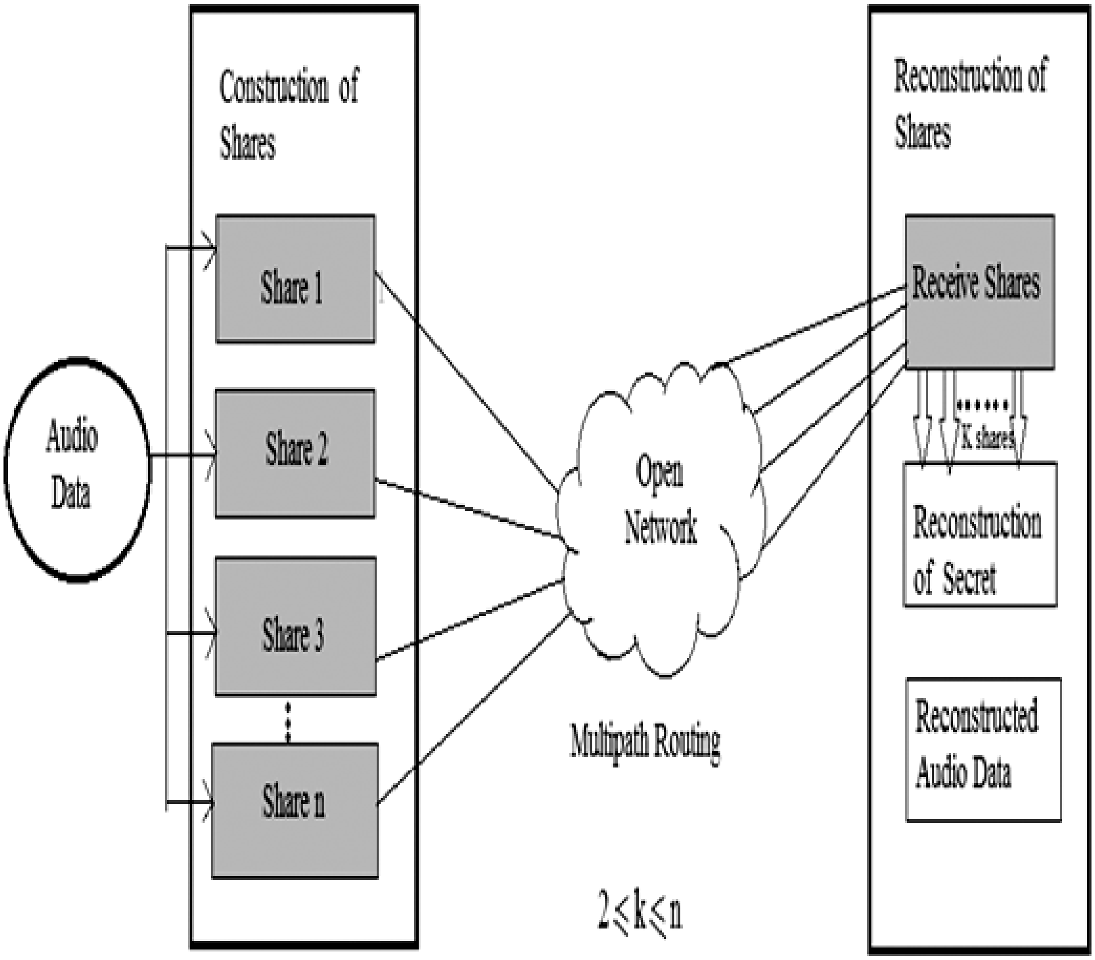

Figure 3: Secret Sharing with Multipath Routing

Step 1: Input the secure vocal data which needs to be transmitted.

Step 2: Convert these audio file into the matrix of 0's and 1's.

Step 3: Then create the n number of shares and n number of masks for these shares using AND operationtechnique as given in graphical masking scheme.

Step 4: Convert these shares back in audio files.

Step 5: Transmit these shares over the network through multiple paths.

Recreation of original data from Shares:

Step 1: Receive the shares coming from multiple paths.

Step 2: Take any k shares where 2<=k<=n.

Step 3: Apply the OR operation of graphical masking scheme on the K shares to generate the original audio message.

4. COMPARATIVE STUDY

The implemented scheme is providing high accuracy as the original and reconstructed files are giving same audio information. The proposed scheme is compared with few techniques used for vocal data sharing based on some parameters. It is shown in below table:

Table 1
Comparative Analysis

Paper	*Technique used*	*Comput-ational Comple-xity*	*Reliability*	*Security*	*Resistance to Attacks*
[2]	Simple (k,n) Threshold Scheme (Polynomial interpolation)	High	No	Low	Low
[3]	Graphical Masking	Low	No Due to single path	Low	Low
[4]	Shamir's Secret Sharing(Polynomial interpolation) with multipath routing	High	YesDue to multiple paths	High	High
Proposed technique	Graphical Masking	Low	YesDue to multiple paths	High	High

5. CONCLUSION

The secret sharing scheme provides encryption of data .The multi-path routing technique provides security while transmission of packets over the open network. The combination of secret sharing along with multipath routing technique provides the high reliability. Security increases with this system for confidential data transfer. Proposed technique promises to provide efficient and reliable communication over network. It can be used to enhance quality and security applications.

REFERENCES

[1] Sonali Patil, Tejal Chavan, Priyanka Sangwan,Vinay Shastri, Akash Sunthwal, "Contemplating Audio Secret Sharing Schemes", International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 11, November 2014.

[2] A. Shamir, "How to Share a Secret ?", Comm Acm, 22 (11): 612-613, 1979.

[3] Prabir Kr. Naskar, Hari Narayan Khan, Ujjal Roy, Ayanchaudhuri, Atal Chaudhuri, "Shared Cryptography with Embedded Session Key For Secret Audio", International Journal of Computer Applications (0975–8887) Volume 26–No. 8, July 2011.

[4] Ryouichi Nishimura, Shun-ichiro Abe, Norihiro Fujita & Yoiti Suzuki "Reinforcement of Voip Security With Multipath Routing and Secret Sharing Scheme" Journal of Information Hiding and Multimedia Signal Processing, July 2010.

[5] Amresh Nikam, Poonam Kapade, Sonali Patil, "Audio Cryptography: A (2, 2) Secret Sharing For Wave File" International Journal of Computer Science and Application Issue 2010.

[6] Sonali Patil, P. R. Deshmukh, Tejal Chavan, Priyanka Sangwan, Vinay Shastri, Akash Sunthwal, "Reduced Share Size Audio Secret Sharing", International Conference on Pervasive Computing (Icpc) 2015.

[7] K. Maheswari and Dr. M. Punithavalli "Secured Secret Sharing Over Single Path in Voip With Consistent Data Transfer" Ijcsi International Journal of Computer Science Issues, Vol. 9, Issue 1, No. 3, January 2012.

[8] Shaofeng Zou, Student Member, Ieee, Yingbin Liang, Member, Ieee, Lifeng Lai, Member, Ieee, and Shlomo Shamai (Shitz), Fellow, Ieee, "An Information Theoretic Approach to Secret Sharing", Ieee Transactions on Information Theory, Vol. 61, No. 6, June 2011.

[9] Youliang Tian, Jianfeng Ma,Changgen Peng,Qi Jiang, "Fair(t, N) Threshold Secret Sharing Scheme", Iet Information Security, 2012.

[10] Yan-xiao Liu, Zhi-xiao Wang,Wen-yao Yan, "Linear (K, N) Secret Sharing Scheme with Cheating Detection", 2015 Ieee International Conference on Computer and Information Technology.