# Securing VoIP Transmission Against Eavesdropping Attack

Hamid Bashir, Professor Ron Ruhl, Dr. Fatemeh Kazemeyni, Dr. Dale Lindskog
Information Systems Security Management
Concordia University College of Alberta, Edmonton, T5B 4E4, Canada
bhamid@student.concordia.ab.ca, {ron.ruhl, dale.lindskog}@concordia.ab.ca, kazemeyni@gmail.com

*Abstract— VoIP technology is rapidly gaining adoption because of its advantage in providing voice services on IP networks. Therefore, it also gains attention of hackers and crackers. In this work, a security issue namely eavesdropping and phrase spotting is handled using a new technique. The proposed technique add noise to the signal and encrypt the signal using AES to prevent it from eavesdropping during transmission. This developed algorithm will prove to be effective in preventing eavesdropping and phrase spotting attacks.*

***Keywords— AES, encryption, IP, SIP, RTP, network layer, VoIP, transport layer, eavesdropping, phrase spotting, voice, security***

## I. Introduction

Voice over Internet Protocol (VoIP) is the transmission of voice using web/internet protocol (IP) using internet or in closed private networks. VoIP in its simplest form can be understood as the routing of voice signals over the internet or in any IP based network. VoIP based applications are used extensively in many areas such as utilizing voice over IP protocol for phone calls over the public network (internet/web). The advantages of VoIP applications include cost savings on long distance calls, toll bypass, network consolidation and convergence of service. In traditional telephone system the cost of calling a user located in long distance area is high. However making voice calls using the internet provide the much needed cost reduction in communications. One simple example of using VoIP applications is the Skype software. Industry estimates predict the use of VoIP will continue to grow as the deployment rate is increasing day by day.

In VoIP a voice signal from a phone is converted into a digital signal and will travel over the internet. If the dialed number is a telephone number, the signal gets converted back into analog voice signal at the receiver's end. Based on the type of VoIP service, a call can be created using a computer, a VoIP phone or a standard phone with or without VoIP adapter. Further VoIP service can also be used in wireless networks which is a benefit for mobile users. However, this depends on the service provider. If the VoIP service provider assigns a telephone number to a user, the user can receive calls from a traditional telephone without the need of any special hardware. The entire system works similar to a normal telephone. For VoIP applications to run on a computer, the user would require broad band internet connection and a special VoIP phone or a normal phone with VoIP adapter or an application. In VoIP voice calls can be made using broadband connections that are similar to traditional telephone calls. Because of its seamless interoperability with existing telephony infrastructure, the new features, speed of deployment, VoIP protocols also contain many vulnerabilities [1], [2], [3]. In spite of all the benefits and advantages securing VoIP systems and applications is highly crucial. This is the main motivation behind doing this research.

Securing VoIP system is quite challenging and even more problematic than securing data networks. It is important to note that all the security issues associated with LAN, WAN and wireless infrastructure also applies to VoIP system. VoIP does not have any dominant standards for security and prevention of attacks. These systems use many of the proprietary protocols in their working and hence the chances of attacks and security issues cannot be over-ruled. The most common vulnerabilities in VoIP systems are provided by VoIP Security Alliance (VoIPSA), an independent organization that is made up by VoIP vendors, individuals and researchers. According to VoIPSA, the threat landscape is provided as a taxonomy having many key elements namely: social threats, eavesdropping, interception and modification threats, denial of service (DoS) threats, service abuse threats, physical access threats, interruption of services threats and so on [4]. The discussions in this research is focused on providing a robust mechanism by which VoIP packets when sent over the internet is highly secure against any type of attack.

The performance of VoIP is based largely on network software and hardware with VoIP components that are supplemented with the existing network infrastructure. However in VoIP, the security tools to safeguard computer networks such as firewalls, network address translation (NAT), encryption, etc do not work similar to ways as they work in a network. In order for a VoIP network to stay secure the procedures related to VoIP working has to be understood first. VoIP networks are subject to different type of security issues namely eavesdropping of telephone conversation, man in the middle attacks, data integrity, and unauthorized access

attack and so on. Fortunately a number of counter measures are also available and used effectively.

In this paper, an innovative method is experimented to secure voice data using cryptography and encryption algorithms. In this work, the data transmitted over the internet shall remain secure without any degradation in performance and provide good QoS. The algorithm used in this paper is advanced encryption standard (AES). In this algorithm, the information that is transmitted is secured through the channel. The security is ensured by using advanced cryptography techniques. In conventional cryptography the data is encoded, but in this case, noise or a random data block is added to the signal to make it impossible to read by an attacker. The flow of voice in VoIP setup is shown in figure 1.

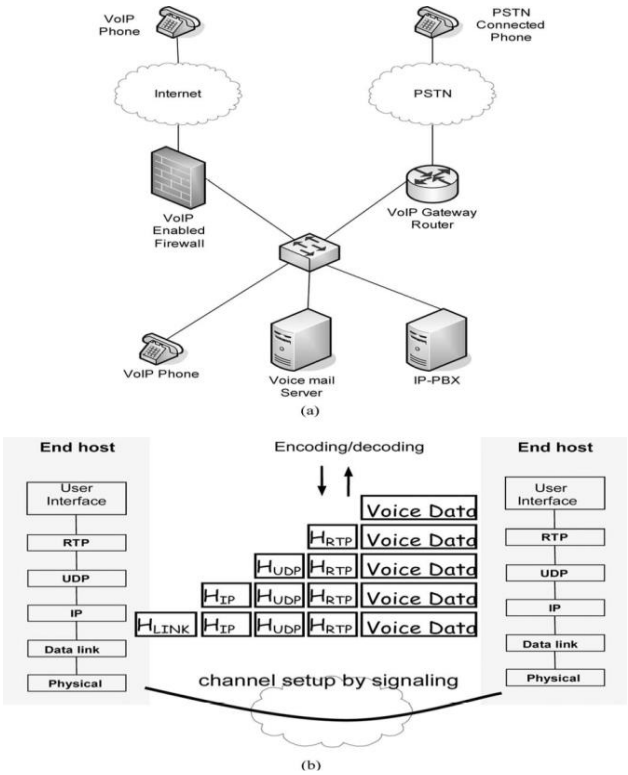


Figure 1: Flow of voice data in VoIP setup

The method presented in this research will take an input voice signal. In our method the indexes of low bit rate using threshold scheme is found and encrypted. We call this signal as A. A random noise signal is added to the location indexes and this signal is called as B. A noise signal is generated so that signal B zeroes signal A. This signal is sent through the channel. At the destination the stream of zeroes are received and signals A and B are received subsequently. Signal A is decrypted, signal B is denoised by using the threshold at noisy indexes. This will retrieve the original voice signal at destination. This entire activity is simulated in MATLAB.

In this paper a new method is explained to secure VoIP signal in IP networks. In sections I and II we introduced the technology of VoIP and the background of this research. Section III provides summaries of related work done by other researchers in this area of VoIP security. Section IV explains the proposed algorithm and the methodology of this research and experimental research. Section V provides the results and provides details on the effectiveness of the proposed method. Finally the paper concludes by understanding this technique will enhance security measures in VoIP.

# II. Aims and Objectives

### *A. Aims*

The aim of this research is to transmit audio signal securely over a channel using AES encryption techniques.

### *B. Objectives*

- The study of different encryption and decryption schemes
- The application of AES algorithms to provide security
- Verifying security of the system, etc
- Add noise to the original audio
- Encrypt the positions of additive noise
- Transmit the data
- Recover original audio after removing the noise at destination

### *C. Background*

In this paper, VoIP signals are secured using advanced encryption standard (AES) to ensure QoS is maintained at the destination. This is done by reading an audio file and identifying the index with low bit rate using threshold schema. The indexes are saved for the signal where threshold is done. A random noise (block of data) is inserted to the threshold index. This noise is a constant bit rate signal which is transferred along with the voice signal. AES is applied to the indexes which are the threshold data. This encrypted signal is transferred through the channel to the destination. At the destination the AES signal is decoded using appropriate keys. The information obtained from decoded signal is used to remove the noise signal to finally obtain the original audio packet at the receiver side.

# III. Related work

Voice over IP is adopted and used widely by private businesses, educational institutions, governments, and so on. In VoIP a user may use a DSL, ISDN or wireless communications network on IT infrastructure. The use of IP networks eliminates the need for public switched telephone network (PSTN). In this section the earlier work related to VoIP systems, security and encryption methods, the protocols used in VoIP are explained. Further the security issues in VoIP systems, mainly the methods or techniques in securing the data in transit for improved performance of voice communication are explored. The most popular VoIP technology and currently in wide use is the SIP (session initiation protocol).

### *A. Overview of SIP*

Session Initiation Protocol (SIP) [5] is widely deployed and most of the research is focused on this area. This protocol is standardized by IETF and is designed to support bi-directional communication this is not limited to VoIP. SIP is a signaling protocol and relies on real time transport protocol (RTP) [6] for media transfer. Support for encryption and integrity is provided by another profile named secure RTP or (SRTP) but not used widely. A number of transport protocols allow SIP operation. These protocols include TCP [7], UDP [8] and SCTP [9]. The main entities of SIP are the endpoints such as physical devices or soft phones, a proxy server, registrar, a redirect server and location server. During a call setup one of the endpoint communicates with the proxy server. The proxy server uses the location server to route the call. It is important to note that another end point can be in the same network or another proxy server in another network. SIP does the negotiation of the actual session parameters. The parameters are CODECs, RTP ports, etc that uses the session description protocol (SDP) [10]. The taxonomy of literature related to security aspects of VoIP are explained by Angelos D. Keromytis in [4]. The threats as explained by VoIPSA are also reviewed in this section.

### *B. Threats Classified by VoIPSA*

Social threats in VoIP focuses on reputation and behaviour based approaches. Many researchers focus on Spam over internet Telephony (SPIT) which is a detection and prevention method. Reputation, behaviour and identity are described by Srivastava and Schulzrinne [11]. In their method they developed a system for blocking SPIT calls and their method is named DAPES. Similarly Dantu and Kolan in [12] demonstrated a possible mechanism for high-volume SPIT using the first and second order derivative of the number of incoming calls from a source (user), host or domain. This method can also prevent certain DoS attacks in VoIP. A statistical algorithm for SPIT was proposed by MacIntosh and Vonokrov in [13]. An overview of SPIT threats and defense mechanisms is provided by Baumann et al in [14].

Considerable amount of work has been done to protect the attacks in VoIP data and signaling. In order to identify and quantify different methods of leaked out data from a user's system or from an enterprise network Takashi and Lee in [15] examined the problem of secret channels in VoIP protocols. They developed the method to hide the true signal from an eavesdropper to conclude possible counter measures and detection methods. An overview of security measures in RTP was provided by Weiser et al in [16]. In their method the security considerations in RTP and media transfer protocol were used in SIP and H.323. They provided results by analyzing six different implementations for confidentiality, integrity and availability. In another method Wright et al [17] applied techniques in machine language in VoIP conversation. They explained by using a variable bit rate (VBR) voice codec used based on the length of encrypted voice frame. They also proposed the technique of block ciphers for encrypting voice. In their continued work in [18] they used Hidden Markov models to identify certain phrases in the encrypted voice signal. They were able to obtain 50% accuracy for phrase identification and for certain phrases they were able to achieve 90% accuracy. Man-in-the-middle attacks are possible by attacker even if they are not present in the direct communication path. This is done by exploiting DNS and VoIP implementation vulnerabilities. Zhang et al, in [19] demonstrated this by showing that such attacks is possible if the attacker only knows the phone number and the IP address of the remote system. It is possible for such attacks to eavesdrop and hijack VoIP calls. Such attacks can be prevented by using media protection, or develop a lightweight VoIP intrusion detection system to be deployed on the VoIP phone.

Research has also been carried out in working out defenses for VoIP systems. Guo et al, in [20] proposed a new scheme that provides strong confidentiality for protecting voice content streaming. In their method they allowed for voice degradation during packet loss, but this scheme is proved to be insecure by Li et al in [21]. The use of cryptography in generating SIP uniform resource identifiers (URIs) to protect the integrity of content in peer-to-peer VoIP was proposed by Seedorf in [22]. Additional security by means of encryption and integrity protection to a lightweight VoIP protocol for mobile devices is proposed by Talevski et al [23]. Passive traffic analysis attacks on VoIP attacks are discussed by Zhang and Berthold in [23]. In their research they also discussed mitigation methods from some of the passive attacks. The privacy of VoIP signals for their protection was discussed by Zhang and Fischer-Hubner in [24] and by Melchor et al in [25]. Srivatsa et al in [27] analysed the problem on-demand construction of QoS sensitive routes in anonymous networks. As a lightweight confidentiality mechanism the use of tiny encryption algorithm (TEA) was proposed by Elbayoumy and Shepherd in [28]. In their method they used an adaptive scheme where the selection of encryption algorithm is used in protecting network traffic. In order to protect from flood based application and transport layer DoS, Reynolds and Ghosal in [29] proposed a multi layer protection scheme. There are many more research works available to develop techniques for handling threats classified by VoIPSA.

### *C. A Brief on Signalling Protocols in VoIP*

Signaling protocols in VoIP establish the features and functionalities and on how the VoIP solution components interact with each other. Some of the common protocols [30] include,

- H.323, this is the ITU standard for establishing VoIP connections
- SIP (Session Initiation Protocol) is the standard for establishing connections in VoIP
- MGCP (Media Gateway Control Protocol) is the protocol developed by IETF to signal the controlling of information between VoIP components

The H.323 is a protocol suit defined by ITU and is intended to provide transmission of voice over packet switched networks of multimedia signals. H.323 defines gatekeepers, which is an additional component that does address resolution and bandwidth control. A control unit named multi-point is used to facilitate multipoint conferencing and other communications between two end points [31].
SIP does the job of creating, managing and terminating sessions in the IP network. A session could be anything such as a voice telephone call, collaborative online conference, etc. This protocol makes it possible to implement many such services and the most preferred protocol used in VoIP related applications recently. It uses the standards explained in RFC 3261 developed by IETF and is still evolving as technology expands. It is important to note that SIP is limited to setup and control the sessions. Other details such as data exchange within the session, encoding or codec, etc is not controlled by SIP and these are done by other protocols [32]. MGCP is the media gateway controllers for VoIP. MGCP manages data by signaling between media gateways and network components such as H.323 gatekeepers or SIP servers. MGCP acts to compliment SIP and H.323 by performing the conversion of audio signals to data packets and further transported over the internet packet networks [33].

The signaling scheme along with encoding scheme is done by H.323 or SIP. These two protocols are implemented in different ways but they offer the same service [34]. The VoIP system in order to establish voice or video to IP networks use many CODECs (Coder-Decoders) to convert analog to digital audio. The CODECs are: G.711, G.722, G.723.1, G.728 and G.729. Video signals use H.611 CODEC. In VoIP another protocol namely real time protocol (RTP) is used to ensure end-to-end delivery of audio or video. Along with RTP the real time transport protocol (RTCP) provides feedback on the quality of connection. RTP runs on top of UDP (user datagram protocol) to offer end to end delivery of services for real time media. The media is encoded as chunks along with the RTP header forms the packet which is encapsulated in a UDP network segment [34].

### *D. Security issues in VoIP*

VoIP systems are required to provide confidentiality, service availability and integrity for their effectiveness. There are many threats that challenge these three service parameters. Xin in [35] explains there are many threats related to confidentiality. Confidentiality refers to data or information that is not accessed by unauthorized users. Information such as financial transactions, personal details, password, etc is termed as confidential information for a user. Similarly confidential information for a network system includes IP addresses, operating systems, user records, etc. Any leak in such information is quite easy for attackers.
Eavesdropping is another threat that is quite common even in conventional telephone (PSTN networks), where the attacker taps a line physically, or penetrates a switch. The numbers of eavesdroppers increase considerably with VoIP because of the large number of nodes involved in VoIP data flow. The attacker can gain access to any one system or IP to monitor and access signals flowing through that node. Further, using freely available network analyzers the attacker can convert the VoIP signals into wave files. The conversations thus gathered can be saved into another computer for playback. One such tool is the Voice over Mis-configured Internet Telephone (VoMIT) [36].

There are also methods to record SIP packets and later retrieve the voice message contained in them. There is another one attack type named as the unauthorized attack. Attackers use this attack type to gain access to resources on the network using open ports or undocumented ports in VoIP phones [37].

There are many subtle differences in security issues in VoIP and in traditional networks. There is a need to understand unique constraints of transmitting voice over IP along with the characteristics of data networks that transmit VoIP signals. IP networks are based on configurable parameters such as IP and MAC (Physical) address of voice terminals and the address of routers and firewalls. Specialized software is used by VoIP systems to make calls and to route them. Network parameters are generated dynamically whenever a VoIP system is restarted or added into the network. Since many of the nodes operate on dynamically configurable parameters, wide array of vulnerable points of attack are available for intruders. Hence VoIP systems have wider implications on security attacks and breaches [38].

### *E. Quality of Service (QoS) in VoIP*

QoS is fundamental to network performance and operations. Normally, VoIP applications are more sensitive to delays than data transfer in traditional networks. It is estimated that delays of 150 milliseconds can turn a clear VoIP signal into garbled signal and this is called the problem of latency [39]. It is important to note that such latency problems are exploited by adversaries. Further the tools to secure firewall protection and network are not effective and in fact they contribute to significant delay. Hence latency is not only a QoS issue, but also a security issue in VoIP systems. A DoS attack may be intended to create latency in the network thus affecting overall network performance. There is another issue in QoS called jitter which refers to delays that are non-uniform. Real time transport protocols (RTP) are used in transporting voice media based on UDP. This leads to packets getting received out of order and cannot be reassembled at the transport level, but reassembled at application layer. This introduces a significant overhead on the network, which is another QoS issue.
Jitter cause packets to arrive in spurts even when packets are coming in a proper order. Jitter can be controlled by using buffers and network elements that allow VoIP packets to travel when larger packets are scheduled ahead of them. The buffers use several strategies such as when to release the voice data and several such schemes [40]. QoS issues result in packet loss. This is a critical concern because data packet loss in normal networks can be managed, but loss of VoIP packets

is useless at the destination. This is because of latency and jitter. Enterprise infrastructure should support QoS to ensure VoIP packets are sent and received fully at high speed. QoS issues are covered in more depth in [41].

Phrase spotting technique and eavesdropping issues were handled using DES and noise blocks by Sahni and Shukla in [43]. In their work, they used random noise block and encryption is done by DES. In this work, I have attempted to continue their work further using one signal along and by using AES. The proposed algorithm is an enhancement to the work in [43]. There are more research literature related to VoIP technologies and security issues covered in [4]. For the purposes of this research we limit our review of related work and focus more on the working of proposed algorithm.

## IV. The Proposed Algorithm

The use of VoIP tehnologies is gaining momentum with millions of users use the internet for voice communications. However most of them are not aware their communication can be overheard or eavesdropped by an attacker. In PSTN networks eavesdopping is quite common, however in VoIP channel attackers can listen to a conversation using phrase spotting. In this technique it is easy to recover data using many specific phrases that are used during a conversation. This phrase spotting technique is used by attackers to gain personal information of users and harmful for privacy [44]. As mentioned in the previous section there are many research reports available that explain the use of encryption and cryptography in securing the VoIP signal from eavesdropping. In our research we shall apply advanced encryption standard (AES) algorithm in securing VoIP signals from many possible attacks.

The use of cryptography is to fulfill objectives in securing information. The objectives include confidentiality, authentication, integrity, non-repudiation, access control and availability [35]. Eavesdropping is done by attackers to impact on confidentiality. This attack type gives an attacker the ability to listen and to record a conversation. Phrase spotting is the method used by attackers to eavesdrop the conversation. The network eavesdropping is illustrated in figure 2.

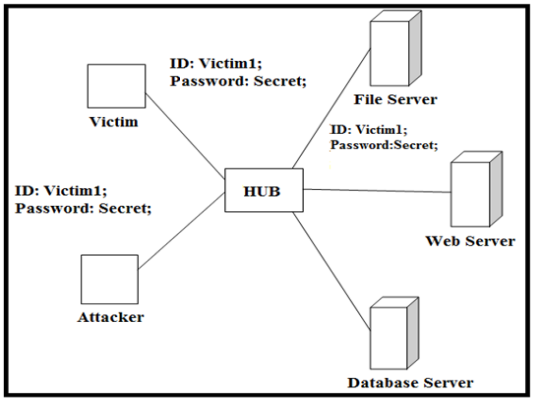


Figure 2: An illustration of Eavesdropping attack [43]

From the figure it can be seen the attack is carried out in the network layer. The attack involves capturing packets from the network which are sent by other computers. A hub is shown in the figure. This device works on the network layer and also repeats data in one port to all the other ports which makes it easy for the attacker to monitor traffic in the network such as capturing passwords. The attacker has to physically gain access to the network in order to eavesdrop. Telnet can be used to further gain access to the network between the source and destination [43].

Logic behind phrase spotting technique is used to gather data on the entire conversation. The attacker checks to find if there are specific phrases used in a VoIP conversation. In VoIP the voice signals are not secure which makes it easy for an attacker to spot a phrase and gain information in the conversation. Normally voice signals use code-excited linear prediction (CELP) technique. The CELP algorithm is based on speech codecs that are standardized. Extensive use of prediction in CELP makes it vulnerable to packet loss. CELP uses a codebook to map a speech sample to the closest original speech pattern. The codebook entry is placed in the VoIP packet which is encoded and sent over the network. Eavesdropping attack is possible and easy in CELP code [42]. The proposed algorithm shall overcome the possibility of such attacks and the proposed work is an improvement to the work done in [43].

The work done in [43] is similar in many respects to the proposed methods for reducing possibilities of attacks in VoIP signals. In paper [43] explains the use of low bit rate indexes and the packets are added with constant bit rate. Random noise is inserted at the threshold indexes with minimum amplitude of the highest bit rate. DES is applied to all indexes that were thresholded. Two signals are obtained from this process and are transferred over the network. At the receiving end, decoding is done using appropriate keys and noise is removed to obtain the final audio. In this way VoIP signals are secured over the network. This work is simulated in MATLAB [43].

The work in this research is intended to protect VoIP signals from attacks using a new algorithm and the steps followed in this algorithm include,

1. Input a VoIP audio signal
2. Determine the indexes of low bit rate using threshold scheme and encrypt them using AES, name this as A
3. In those indexes add noise to get a noisy signal and name them as B
4. Make signals A and B as one single signal such that B zeroes A
5. Send this signal through the network
6. At the destination, check for the stream of zeroes and receive both the signals A and B
7. Decrypt A to get the indexes form where noise will be removed

8. Using the decrypted A, remove noise from B by putting the threshold at noisy indexes
9. The original voice signal is obtained

The method given in the steps is the defense approach for eavesdropping attack. In this research, the AES algorithm is used to encrypt the signal and this signal is transmitted through the network as it is more secure than DES and has very similar network performance [46] making this implementation much more secure than that in [43] . The padding of each packet to different value is done to prevent the attacker to differentiate between low and high bit rate. However constant bit rate is used for transmission in the channel.

In VoIP the conversation is divided into two parts: the sender and the receiver [45]. The sender first reads an audio file to find out the indexes with low bit rate. In order to secure the conversation, the indexes are padded with low bit rate. A random noise is added at threshold indexes with maximum amplitude and highest bit rate. The block which is added at the end of the packet to show location of bits is also an enhancement over the work done in [43]. AES is applied to indexes for encryption and decryption using a previously shared key. The noisy signal is also encrypted and indexed where the noise is added. The key for encryption and decryption is symmetric. The algorithm shares the same key for encryption and decryption. In the destination side, the noisy signal is decoded and the noise is removed first. The original voice signal is obtained. This method is proposed to minimize the attack and the attacker can no longer be able to decode the voice signal before removing the noise block. Hence, this shall prove to be a more robust method of securing VoIP signals. The process steps at the transmitter and receiver are given below:

**Transmitter**

- An audio signal is read
- The indexes are determined with low bit rate using threshold schema
- The indexes of signal where threshold is done are saved
- Random noise block is inserted at threshold indexes with maximum amplitude of highest bit rate
- This is the signal for transfer and let this be A. It is important to note this signal is of constant bit rate
- AES is applied to all indexes which were thresholded. This signal is named as B.
- This signal (A and B) is transferred through the channel.

**Receiver**

- The receiving node receives the encrypted signal with index and noise
- The AES signal will be decoded using the appropriate key
- The decoded information are the indexes that contain keys to remove the noisy signal
- Using these indexes, the noise block is removed from the noisy signal
- The final audio is received by the receiver

The above steps are illustrated in waveforms obtained from MATLAB.

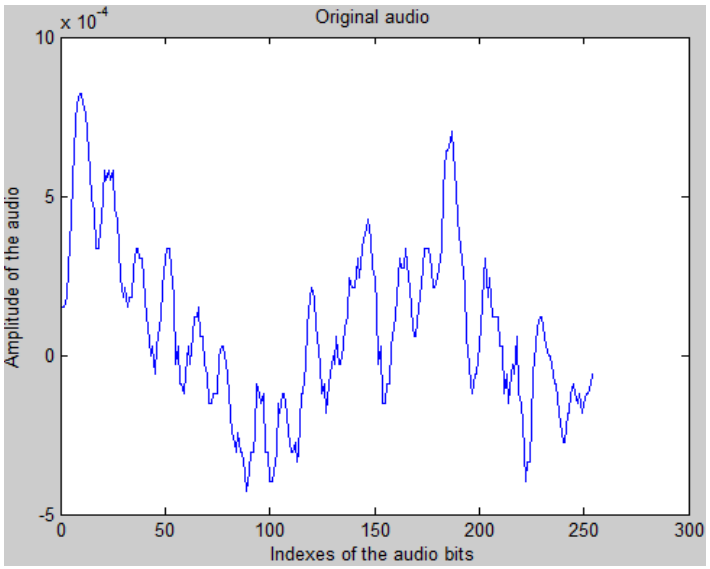


Figure 3: The original audio signal

The audio bits are indexed in the original signal. The indexes are determined with low bit rate using threshold schema and are saved. Noise is inserted at the packet to show location of bits which is illustrated in figure 4.

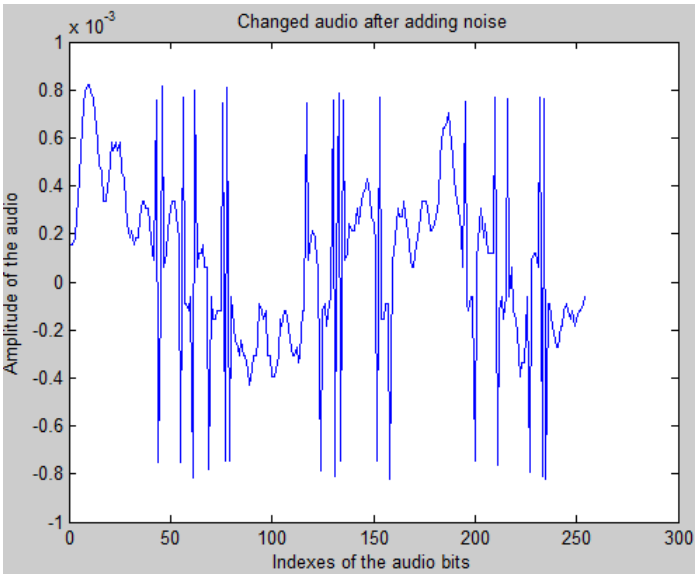


Figure 4: Changed audio with noise

The audio signal is added with noise in figure 4. The changed signal with encryption at the end of the block is shown in figure 5.

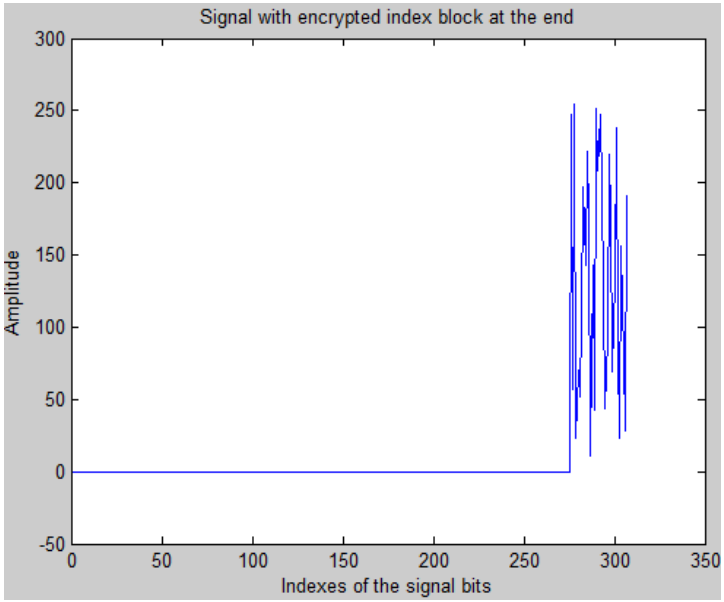


Figure 5: Signal with encryption at end of block

In figure 5, though the waveform output appear as a straight line, they are audio bits. The straight line appearance is because the value of audio bits is very small and the encrypted index values are large. Hence they appear as a line.

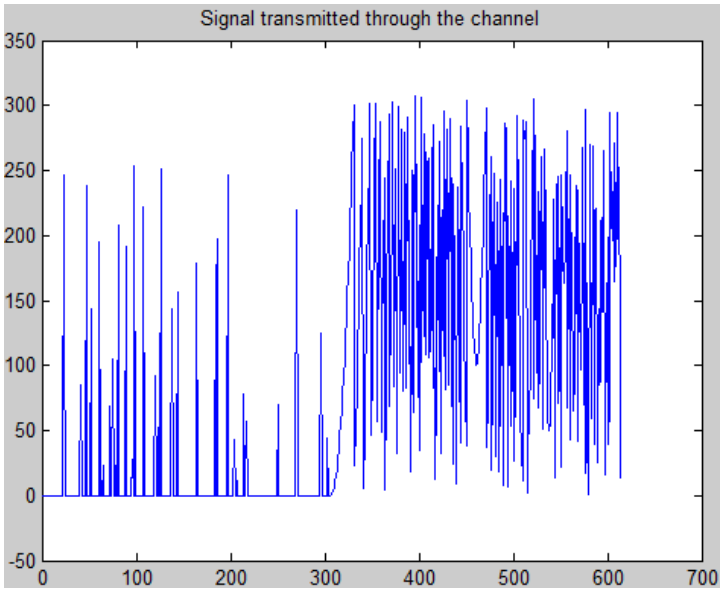


Figure 6: Signal with encryption of whole audio signal

The signal shown in figure 6 is sent across the network. This is the signal which is again encrypted as a whole to make sure that the attacker does not get any piece of information by analyzing the signal.

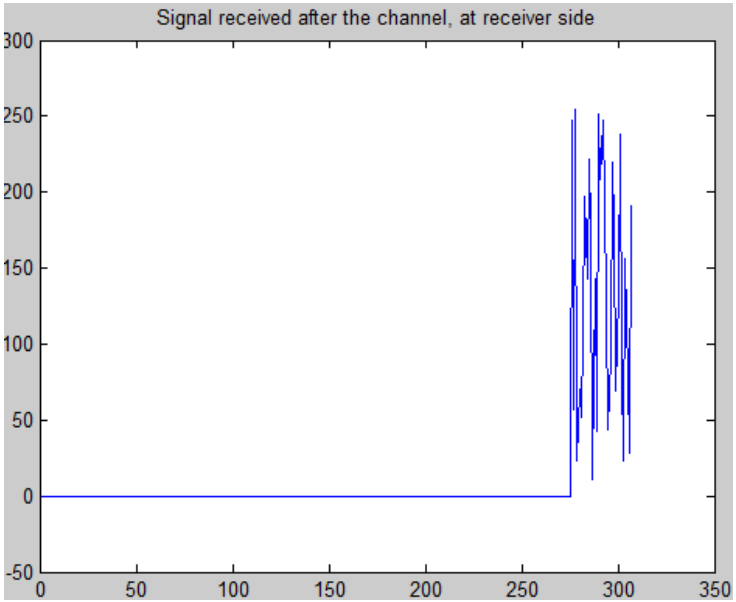


Figure 7: The signal received after channel at reciever side

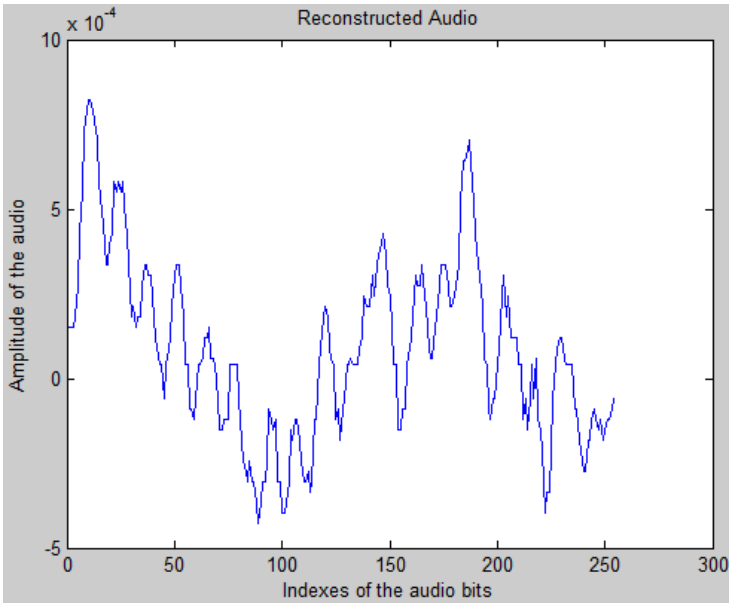


Figure 8: The reconstructed signal after decryption

The above waveforms were obtained by simulation in MATLAB to demonstrate the working of the new security mechanism for VoIP. We can clearly see that the reconstructed audio is similar to the original audio without affecting the performance and jitter in the signal being transmitted over the network.

## V. Results

The results of the simulation are also obtained graphically as wave forms to further explain the effectiveness of the algorithm. Figure 4 shows the wave forms generated in MATLAB. In the above figures the x-axis represents the

indexes of the audio bit and the y-axis denotes the amplitude of the audio signal. It may be seen the original audio and the re-constructed audio signals are similar and this is possible through the algorithm proposed in this research. However the signal changes when we add a noise block thus making it impossible for an attacker to eavesdrop as can be seen in figure 5. Further, we also encrypted the audio signal as a whole as could be seen in figure 6. The amplitude and the frequency of both the audio waves before and after removal of noise are the same and signal quality is also maintained. In this research paper, the use of AES encryption provides many advantages such as providing security in a variety of hardware settings and implementations. Further brute-force attacks are not possible in AES encryption. Moreover, it is more efficient than DES and we did not get any QoS issues as can be seen in the results.

The algorithm uses a set of resource rounds applied to transform cipher text back to the original signal using the same encryption key. This working is seen in getting back the original audio signal at the receiver end in the VoIP system. This developed algorithm may serve the purpose of mitigating threats such as eavesdropping and also prevents audio signals from phrase spotting attacks. Hence the algorithm shall prove to provide robust security in the area of VoIP security.

# VI. Conclusion

In this paper a new technique for handling security attacks in VoIP is explained. An algorithm is presented which shall prove an effective method to prevent attacks such as eavesdropping and phrase spotting technique. In this algorithm a voice signal is encrypted and a noise block is added at source to protect the signal from attacks. The method determines the indexes of low bit rate using threshold scheme and further encrypted using AES. The signal received at the destination is decrypted using the index value, the noise is removed to re-construct the original signal. This is simulated in MATLAB and the wave forms are presented in results. It can be seen the method is effective because the wave forms of the original signal and reconstructed signal have the same value in terms of signal strength and QoS. Further we use AES encryption which is an advanced encryption standard with many benefits. The work presented in this paper will prove to be effective in avoiding attacks such as eavesdropping and phrase spotting.

**References**


[1] A. D. Keromytis, “Voice over IP: Risks, Threats and Vulnerabilities,” in *Proceedings of the Cyber Infrastructure Protection (CIP) Conference*, June 2009.

[2] A. D. Keromytis, “A Look at VoIP Vulnerabilities,” *USENIX login: Magazine*, vol. 35, pp. 41–50, February 2010.

[3] A. D. Keromytis, “Voice over IP Security: Research and Practice,” *IEEE Security & Privacy Magazine*, vol. 8, pp. 76–78, March/April 2010.

[4] Angelos D. Keromytis, ”A Survey of Voice over IP Security Research”, *IEEE Communications Surveys & Tutorials.* pp. 1-17, March 2011.

[5] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, “SIP: Session Initiation Protocol.” RFC 3261 (Proposed Standard), June 2002. Updated by RFCs 3265, 3853, 4320, 4916, 5393.

[6] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacobson, “RTP: A Transport Protocol for Real-Time Applications”, *RFC 3550 (Standard)*, July 2003. Updated by RFC 5506.

[7] J. Postel, “Transmission Control Protocol.” RFC 793 (Standard), Sept. 1981. Updated by RFCs 1122, 3168.

[8] J. Postel, “User Datagram Protocol.” *RFC 768 (Standard)*, Aug. 1980.

[9] L. Ong and J. Yoakum, “An Introduction to the Stream Control Transmission Protocol (SCTP).” *RFC 3286 (Informational)*, May 2002.

[10] M. Handley, V. Jacobson, and C. Perkins, “SDP: Session Description Protocol.” *RFC 4566 (Proposed Standard)*, July 2006.

[11] K. Srivastava and H. Schulzrinne, “Preventing Spam For SIP-based Instant Messages and Sessions,” *Technical Report CUCS-042-04, Columbia University, Department of Computer Science*, October 2004.

[12] R. Dantu and P. Kolan, “Preventing Voice Spamming,” in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM), Workshop on VoIP Security Challenges and Solutions*, December 2004.

[13] R. MacIntosh and D. Vinokurov, “Detection and Mitigation of Spam in IP Telephony Networks Using Signaling Protocol Analysis,” in *Proceedings of the IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication*, pp. 49–52, April 2005.

[14] R. Baumann, S. Cavin, and S. Schmid, “Voice Over IP - Security and SPIT,” KryptDet Report FU Br 41, Swiss Army, August/September 2006.

[15] T. Takahashi and W. Lee, “An Assessment of VoIP Covert Channel Threats,” in *Proceedings off the* 3rd *International Conference on Security and Privacy in Communications Networks (SecureComm)*, pp. 371–380, September 2007.

[16] C. Wieser, J. R¨oning, and A. Takanen, “Security analysis and experiments for Voice over IP RTP media streams,” in *Proceedings of the* 8th *International Symposium on Systems and Information Security (SSI)*, November 2006.

[17] C. V. Wright, L. Ballard, F. N. Monrose, and G. M. Masson, “Language Identification of Encrypted VoIP Traffic: Alejandra y Roberto or Alice and Bob?,” in *Proceedings of* 16th *USENIX Security Symposium*, pp. 1–12, August 2007.

[18] C. V. Wright, L. Ballard, S. Coulls, F. N. Monrose, and G. M. Masson, “Spot Me If You Can: Recovering Spoken Phrases in Encrypted VoIP

Conversations," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 35–49, May 2008.

[19] R. Zhang, X. Wang, R. Farley, X. Yang, and X. Jiang, "On the Feasibility of Launching the Man-In-The-Middle Attacks on VoIP from Remote Attackers," in *Proceedings of the* 4th *International ACM Symposium on Information, Computer, and Communications Security (ASIACCS)*, pp. 61–69, March 2009.

[20] J.-I. Guo, J.-C. Yen, and H.-F. Pai, "New Voice over Internet Protocol Technique with Hierarchical Data Security Protection," *IEE Proceedings — Vision, Image and Signal Processing*, vol. 149, pp. 237–243, August 2002.

[21] C. Li, S. Li, D. Zhang, and G. Chen, "Cryptanalysis of a Data Security Protection Scheme for VoIP," *IEE Proceedings—Vision, Image and Signal Processing*, vol. 153, pp. 1–10, February 2006.

[22] J. Seedorf, "Using Cryptographically Generated SIP-URIs to Protect the Integrity of Content in P2P-SIP," in *Proceedings of the* 3rd *Workshop on Securing Voice over IP*, June 2006.

[23] A. Talevski, E. Chang, and T. Dillon, "Secure Mobile VoIP," in *Proceedings of the International Conference on Convergence Information Technology*, pp. 2108–2113, November 2007.

[24] G. Zhang and S. Berthold, "Hidden VoIP Calling Records from Networking Intermediaries," in *Proceedings of the* 4th *Annual ACM Conference on Principles, Systems and Applications of IP Telecommunications(IPTCOMM)*, pp. 15–24, August 2010.

[25] G. Zhang and S. Fischer-Hu¨bner, "Peer-to-Peer VoIP Communications Using Anonymisation of Overlay Networks," in *Proceedings of the* 11th *Conference on Communications and Multimedia Security (CMS)*, May/June 2010.

[26] C. A. Melchor, Y. Deswarte, and J. Iguchi-Cartigny, "Closed-circuit Unobservable Voice over IP," in *Proceedings of the* 23rd *Annual Computer Security Applications Conference (ACSAC)*, pp. 119–128, December 2007.

[27] M. Srivatsa, L. Liu, and A. Iyengar, "Preserving Caller Anonymity in Voice-over-IP Networks," in *Proceedings of the IEEE Symposium onSecurity and Privacy (S&P)*, pp. 50–63, May 2008.

[28] A. D. Elbayoumy and S. Shepherd, "A High Grade Secure VoIP System Using the Tiny Encryption Algorithm," in *Proceedings of the* 7th *Annual International Symposium on Advanced Radio Technologies*, pp. 342–350, March 2005.

[29] B. Reynolds and D. Ghosal, "Secure IP Telephony using Multi-layered Protection," in *Proceedings of the ISOC Symposium on Network and Distributed Systems Security (NDSS)*, February 2003.

[30] Juniper Networks, "Voice over IP 101: Understanding the Basic Networking Functions, Components and Signalling Protocols in VoIP Networks". *Whitepaper by Juniper Networks Inc*. May 2007.

[31] Westman, Thomas, Kerim Bergstrom, D. and Therese Berge IT, "Voice over IP: Computer Communication and Distributed Systems". *Report*, April, 2006.

[32] Banerjee, K. "*SIP (Session Initiation Protocol) Introduction",* [ONLINE] Available at: http://www.siptutorial.net/SIP/background.html. [Last Accessed 29-Jan-2014], 2005.

[33] Kuhn, D. Richard, Thomas J. Walsh and Steffen Fries, "Security Considerations for Voice over IP Systems". *National Institute of Standards and Technology, NIST Special Publication 800-58*, January 2005.

[34] Taylor, Steve and Larry Hettick, "*H.323 vs SIP"*. [ONLINE] Available at: http://www.networkworld.com/newsletters/converg/2002/01416213.html. [Last Accessed 29-Jan-2014], March 2002.

[35] Xin, Jianqiang, "Security Issues and Countermeasures for VOIP", *SANS Institute*, 2007.

[36] Provos, Niels, "*VoMIT - voice over mis-configured internet telephones"*. [ONLINE] Available at: http://vomit.xtdnet.nl/. [Last Accessed 02-Feb-2014], 2004.

[37] Shawn Merdinger, " *ACT P202S VoIP wireless phone multiple undocumented ports/services",* [ONLINE] Available at: http://lists.grok.org.uk/pipermail/full-disclosure/2006-January/041434.html. [Last Accessed 02-Feb-2014], 2006.

[38] Thomas Walsh J. and Richard Kuhn, "Challenges in Securing Voice over IP", *IEEE Security & Privacy.* pp.44-50, 2005.

[39] ITU-T, "G.114, One Way Transmission Time", *International Telecommunications Union*, 1998.

[40] A. Kos, B. Klepec, and S. Tomazic, "Techniques for Performance Improvement of VoIP Applications", *IEEE Mediterranean Electro-technical Conference, IEEE Press.* pp.250-254, 2002.

[41] V. Fineberg, "Building a QoS Enabled IP Network: A Practical Architecture for Implementing End-to-End QoS in an IP Network", *IEEE Communications*, pp. 122-130, 2002.

[42] Jyoti Shukla, Bhavana Sahni, "A Survey on VoIP Security Attacks and their Proposed Solutions", *IJAIEM*, volume 2, issue 3, March 2013.

[43] Bhavana Sahni, Jyoti Shukla, "Defence Approach for Eavesdropping Attack on VoIP Conversation", *International Journal of Advanced Research in Computer Science and Software Engineering*", vol. 3, pp. 740-746. August 2013.

[44] Vaisly Prokopov, Olekii Chykov, "Eavesdropping on encrypted VoIP conversation: phase spotting attack and defense approaches", 2011.

[45] David Butcher, Jinhua Guo, "Security Challenge and Defense in VoIP infrastructures", *IEEE Transactions*

*on Systems, Man, And Cybernetics—Part C: Applications and Reviews*, vol. 37, No.6, November 2007.

[46] Abdel Karim Al Tamimi, "*Performance Analysis of Data Encryption Algorithms*" Available at http://www.cs.wustl. edu/ ~jain/cse567-06/ftp/encryption_perf/
[Last Accessed 07-April-2014]