REAL-WORLD ATTACKS ON ZRTP WITH RSA ALGORITHM USING NEURAL NETWORK CLASSIFIER

R. Shankar[1] **and S. Duraisamy**[2]
[1]Assistant Professor, Dept. of Computer Science, Chikkanna Government Arts College, Tirupur, Tamilnadu
[2]Assistant Professor, Dept. of Computer Science, Chikkanna Government Arts College, Tirupur, Tamilnadu

ABSTRACT: Voice over Internet Protocol (VoIP) is a trend of applications catching up on the internet in the recent times. The usage of cryptographic methods allows the users to communicate securely, but the computed throughput in addition to the QoS parameters are influenced by the algorithm used. In the technical work studied earlier, Diffie-Hellmann (DH) key exchange algorithm is employed, but it is not quite efficient to tackle against the attacks of malicious intruders. But, it is the only technique available for safeguarding the data from the offenders. In the newly introduced work, the ZRTP security mechanism yields a secure channel for VoIP along with Ron Rivest, Adi Shamir and Leonard Adleman (RSA) algorithm to defend against the intruder threats. It is found that the weakness of ZRTP protocol with RSA algorithm is due to the isolation between the platform state verification process and the key exchange process. End-to-end security is necessary for protecting against wiretapping made on voice calls. The ZRTP key-agreement protocol with the Neural Network (NN) Classifier is used for such communication in real-time. Classifier is utilized for the identification of the dangers from intruders. This comprehensive evaluation reveals a severe vulnerability, which permits wiretapping even when Short Authentication Strings are compared with precision. It explains about the error handling mechanisms of the clients and design of security indicators strongly resulting invulnerable connections. The performance analysis metrics include Recall, Precision, Accuracy and F-Measure result.

KEY WORDS: Voice over Internet Protocol (VoIP), Ron Rivest, Adi Shamir and Leonard Adleman (RSA), Diffie-Hellmann (DH), intruders, and Z and Real-time Transport Protocol (ZRTP).

1. INTRODUCTION

Voice over Internet Protocol (VoIP) is a type of transmission, which lets any individual to call from phone using a broadband internet connection. VoIP access generally permits the user to make calls to others who can also receive calls over the internet. Moreover, VoIP can be explained as a unique solution that facilitates transmitting voice signals over internet connection instead of the conventional telephone line [1].

In the recent VoIP implementations, the voice analog signals are sampled and then encoded employing codec. It is enclosed within an IP packet and transmitted over data cables or the internet facility similar to the manner in which the data packets are transmitted [2]. In the earlier times, VoIP needed a headset to be connected to the computer, and the speaker and receiver can only talk with others with a similar kind of arrangement. It was necessary that the parties had to be informed in prior about the call, so as to intimate the user waiting at the other end of the call and also the time of call [3].

VoIP systems depend on a data network that implies there are possibilities of security vulnerabilities and the kinds of attacks tagged with any data network. For instance, in a traditional telephone system, physical accessing the telephone lines or a get-around of the office private branch exchange (PBX) is needed to carry out activities like wiretapping. However for VoIP, voice is transformed into IP packets, which may be carried through several network access points. Hence the data is endangered to several more probable points of attack, which can be exploited for interruption by malicious attackers.

Truly, every security risk related with IP, like computer viruses, Denial of Service (DoS) and man in the middle attacks can also prove to be damaging to VoIP systems. Hijackers have also attempted using the VoIP technology to usurp identities and take away money [4]. This type of attack is identical to an email-based phishing attack, and therefore it is termed as “vishing”. A victim will get an email or be reached through a phone call, which guides him or her to a customer service number where they are passed through multiple voices cued menus, trying to steal account numbers, Personal Identification Number (PINs), and other crucial data.

Communication with security in VoIP networks is a huge challenge owing to its packet loss rate, absence of authentication and eavesdropping. Therefore, a protected secret sharing approach along with single path routing attains a robust secure communication employing enhanced secret sharing algorithm in VoIP networks. Secret shared security exploited in the VoIP network will avoid dangerous attacks. In order to yield security, the infrastructure is developed with the aim of satisfying the below aspects including solid authentication, access control strategies, and key control.

In the technical work proposed, the ZRTP security approach yields a secure channel for VoIP employing Ron Rivest, Adi Shamir and Leonard Adleman (RSA) algorithm to safeguard against the malicious attacks. It is found that the weakness of ZRTP

protocol with RSA algorithm is due to the isolation between the platform state verification process and the key exchange process.

2. LITERATURE REVIEW

In [5] is introduced an organized security evaluation of the VoIP protocol stack that comprises of signaling (SIP), session description (SDP), key establishment (SDES, MIKEY, and ZRTP) and secure media transport (SRTP) protocols. The most critical attack includes the replay attack on SDES that makes the SRTP to reiterate the key stream utilized for media encryption, thereby destroying the transport-layer security entirely. At last, it is revealed that the key derivation process utilized in MIKEY cannot be utilized for proving the security aspect of the key derived in the standard cryptographic model used for secure key exchange.

In [6] is introduced an encryption approach for Voice Calls. It assists the user in encrypting the voice call prior to its transmission on the mobile network. The concept behind the newly introduced system is the encryption of the voice calls with no usage of any secure servers or any kind of intermediate systems between the mobile device and the Global System for Mobile communications (GSM) network. The process of encryption happens before it reaches the mobile device. In order to keep up the strong security, an encryption algorithm dependent on RSA encryption is utilized. In addition, it makes use of a public key that is known to all the users and a private key, a secret and limited key known to each particular user.

In [7] stated that the VoIP defined the transmission and receipt of voice and video data over networks using the "Internet Protocol" (IP) to be the transport protocol. The frequently-used name "internet telephony" defines the transport medium used for VoIP that will be the Internet here. Depending on the ubiquitous accessibility to broadband Internet access, VoIP is emerging to be more a cheaper alternate to traditional telephone networks. This concept paves the way for the idea of developing VoIP communication software that provides safe and sensitive communication.

In [8] introduced a solution employing dedicated Virtual Private Network (VPN)-based local area firewalls. These firewalls yield more degree of security compared to a border router by keeping the voice information less vulnerable to attacks from an insider presenting the network. Also, they can conveniently and trust ably deal with and safeguard various categories of clients in small office environments, regulate access confining the traffic incoming to the network and encrypt the Internet Protocol (IP) voice packets employing IPSec tunneling prior to the voice packets being sent to the access switch.

In [9] provided an overview regarding the VoIP systems and its security challenges. Firstly, it gives a brief description on the fundamental VoIP architecture and its basic differences in comparison with PSTN. Second, the elementary VoIP protocols utilized for signaling and media transport, in addition to defense strategies are explained. At last, the present and probable VoIP attacks in addition to the techniques, which have been used for defending against the attacks, are studied.

In [10] discussed about the organized security analysis carried out on the VoIP protocol stack that comprises of signaling (SIP), Session Description (SDP), key establishment (SDES, MIKEY, and ZRTP) and secure media transport (SRTP) protocols. At last, it indicates that the key derivation process utilized in MIKEY cannot be exploited for proving the security provided by the derived key in the standard cryptographic model used for secure key exchange.

In [11] introduced the key exchange protocols such as MIKEY, ZRTP and SDES. The research area focused in VoIP is associated with the Security and Quality of Service (QoS) of the Voice information. There exists a necessity for solid key management protocols that will protect the voice data from every kind of attack and also yields a practical key exchange strategy. Every one of these three key management protocols is analyzed and also its resistance against Man-In-The Middle Attack has also been evaluated.

In [12] the solution proposed relies on the Multilayer Perceptron Neural Network (MLPNN). The introduced solution MLPNN in the technical work is exploited in the form of a classifier of attacks happening in a distributed monitoring network consisting of autonomous honeypot probes. A well-prepared set of honeypots monitor different aspects of the recent VoIP infrastructure that gets precious data regarding the activity of the hacker without endangering to the system-in use. The research work discusses about the intrinsic structure of neural network used and also the information regarding this network's implementation. The trained neural network has the capability of classifying the most generally observed VoIP attacks. Using the given technique, malicious activities in various parts of networks that are logically or geographically partitioned, can be detected, and the information obtained from one network can be used for strengthening harden security in the rest of the networks.

In [13] solution proposed is associated with automated attack detection systems. Then the gathered data analyze aggregation server with artificial neural network (ANN). The detection of the source data is carried out by a distributed network consisting of detection nodes. Every node comprises of a honeypot application and traffic monitoring strategy. The aggregated data from every node becomes the input for neural networks. The automated classification performed on a central server having a lesser false positive detection rate minimizes the expense incurred with the resources involving attack detection. The detection system makes use of modular design for a convenient implementation in the output infrastructure. The central server gathers and processes the traffic detected. It also helps in the maintenance of all the detection nodes.

3. PROPOSED METHODOLOGY

ZRTP security approach yields a secure channel for VoIP employing Ron Rivest, Adi Shamir and Leonard

Adleman (RSA) algorithm for safeguarding from malicious attacks. It is found that the weakness of ZRTP protocol with RSA algorithm is due to the isolation between the platform state verification process and the key exchange process. End-to-end security is necessary for safeguarding against the wiretapping performed on voice calls. In such kind of communication happening in real-time, the ZRTP key-agreement protocol is used with the Neural Network Classifier. The classifier is utilized for detecting the malicious attacks.

3.1. ZRTP FUNDAMENTALS

The ZRTP key agreement protocol has been formed as standard in RFC 6189 [14] and makes use of SASs for detecting the MitM attacks. This agreement is then transmitted over a Real-Time Transport Protocol (RTP) communication channel, which has earlier been created with the help of a signaling protocol, like SIP. The SASs are obtained from the RSA shared secrets and exhibited on the screens of the end users. Their comparison has to be done orally by reading them aloud and then verifying that the SAS of the peer is a match with the one that is displayed. If a MitM attack happens, the participants wind up with various shared secrets and therefore diverse SAS. The SASs are very short in length, e.g., 'bz4f' (B32 encoding) or 'spearhead Yucatan' [15, 16]), when still rendering sufficient security owing to the use of a hash commitment [17]. These confines a MitM to just one try to predict the right key for creating the same SAS.

It yields an overview of ZRTP adhering to the notation pertaining to RFC 6189 [14]. It highlights on the portions of the protocol with relevance to the analysis carried out in this research work. While the data exchange is in progress, one participant becomes the Initiator and the other participant to be the Responder. As the errors of 16 bit UDP checksums cannot be differentiated from active MitM attacks, all the ZRTP packets have an extra Cyclic Redundancy Check (CRC) for error detection. In addition, two exponential backoff retransmission timers are used: one for sending Hello messages, the other for every message that is transmitted after HelloAck. After the completion of the ZRTP handshake, the SASs and keys for a SRTP session are obtained and the SRTP session is created. Then the SAS has to be compared orally to be assured that there was no MitM existing between the endpoints. In case, anything goes a miss while the exchange is going on, an Error message is transmitted with a certain error code with encoding on what has been behind the failure of the handshake.

3.1.1. ENCRYPTING VOICE IP CALLS

VOIP transforms voice, which is in the form analog signal into digitized signal and then performs its compression. The voice in the form of digitized data is partitioned or split into packets. The packets are sent across the internet over the IP protocol. Everything that is transmitted across the internet can easily undergo interference. This leads to a problem, particularly if the information is sensitive, such as credit card numbers or corporate information. One more concern is the clear identification of the sender and recipient of the data [18]. A variety of ways have been designed with the intent of resolving these issues, inclusive of encryption, modification of the information software from one to another. Even in the case of it being received by another, it will be observed unusual and does not mean anything. Prior to the recipient receiving the information, the decryption changes the message back to its actual format [19].

3.1.2. RSA ALGORITHM

RSA algorithm is developed by Ron Rivest, Adi Shamir and Leonard Adleman. In the form of an asymmetric cryptography that is responsible for the generation of a public key and private key, everybody is aware of the public key and it can be utilized for the encryption of the messages when the private key is a secret and known only to the user. The generation of the public and private keys can be done in this manner [20]:

- Selecting an arbitrary large number p and q
- n=pq, (n refers to the modulus for the private and the public keys)
- $\emptyset(n) = (p-1)(q-1)$
- Selecting an integer such that as $1 < e < \emptyset(n)$, and e is coprime to $\emptyset(n)$, ((e) is established as the public key exponent)
- Get d so that 1=d.e mod $\emptyset(n)$, ((d) is established as the private key exponent).
- Public key is (e,n)
- Private key is (d,n)
- The encryption of $m=m^e \bmod n$
- The decryption of $c=c^d \bmod n$

RSA is extensively employed for protecting the message communications by means of encryption and decryption. It offers more security compared to DES and others. It offers resistance against attacks from external sources.

3.2. WIRETAPPING VOIP CALLS

It is inspired by the significance of end-to-end encryption and authentication support provided in VoIP clients by exhibiting how simple it is for an immorality operator to wiretap calls by, i.e., someone with access to the primary elements of the VoIP network. This implementation is developed to be non-intrusive to the maximum extent possible regarding to the original SIP flow between the caller Alice and callee Bob. Here, it doesn't try to damage or get through ZRTP.

3.2.1. Design

In order to maintain the interference and changes to a minimal extent possible, it was determined to realize the MitM by securing the SIP flow. An attack probability is

expressed through the modification of the incoming messages so as to forward the calls to a MitM client that allows recording. This ends in a tunnel through the MitM rather than a direct connection made between Alice and Bob. It is taken care by the modification that the header of the messages always have the actually called SIP address(es) to conceal for the attack. A specialized MitM SIP client automatically accepts any incoming call, begins a second call to the actual callee Bob, and then connects the inward data stream from Alice with the new outward stream to Bob. So, everything functions as per the protocol but using a MitM that records the multimedia stream, i.e., the conversation happening. The Figure 1 shown below demonstrates how wiretapping works in these steps:

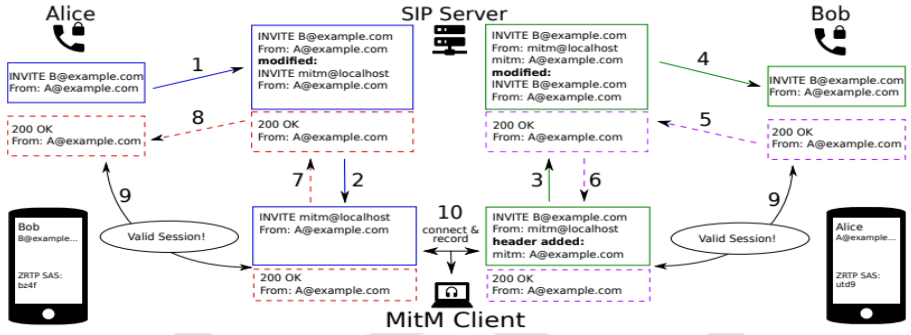

Fig. 1. Flow of minimally intrusive wiretapping: The SIP server re-routes INVITE messages to a MitM client that connects the multimedia streams and records the conversation between Alice and Bob. In between the MitM client and the SIP server a 'mitm' header is presented to pass-through the actual 'From' header. As anticipated, the SASs displayed are different.

1. Alice initializes a call to Bob.
2. The server modifies the INVITE message so that it gets forwarded to the MitM client at 'mitm@localhost'. The information that the message must have been forwarded to Bob does not get lost during the manipulation, as the 'To' header has not been modified.
3. The MitM client initiates a second call to Bob, prior to accepting the call that is incoming. A new 'mitm' header is then added to the outward call having the actual 'From' address from the incoming one.
4. The server modifies the INVITE message from the MitM client so that it seems like it is from Alice.
5. Bob accepts and then acknowledges the INVITE message.
6. This acknowledgment is then forwarded normally to the MitM client, as the MitM is the actual caller.
7. The MitM client automatically receives Alice's call.
8. This acceptance is thereafter forwarded to be normal to Alice, as she is the caller.
9. At present, two valid connections have been created. Preferentially securing these with ZRTP would now result in different SASs.
10. The MitM client connects both the multimedia channels and records all that goes through.

It is an extension of Kamailio [21] with the defined capabilities MitM. This patch forwards the calls to a MitM client employing PJSIP [22] and ZRTP4PJ [23]. Messages are manipulatedon the basis of their kind, e.g., INVITE, BYE, or OK. Multimedia streams are then connected together employing PJSIP's conference bridge framework. The entire call is recorded utilizing the PJSIP's recorder class.

3.3. NEURAL NETWORK CLASSIFIER

Neural networks attempt modelling the information processing abilities of the nervous system in mammals. This nervous system comprises of millions of interlinked cells in a sophisticated setup. The artificial neural network seeks to prototype this design and it is also implemented for various prediction applications in telecommunication systems [24]. The functionalities of a single neuron is known to everyone and acts as a model for an artificial one. Even when there is no complete understanding about the complexity and comprehensive hierarchical networking of the brain, and its remarkable processing rate, artificial neural network manage complicated issues by employing various topologies. Several versions of these topologies are being use in the recent times, each with its own pros and cons. The feed-forward Multilayer Perceptron Network (MLP) neural network was utilized for the classifications of VoIP attack. It comprises of various layers, with each one comprising of a particular number of neurons known as perceptron. These perceptrons present in one layer are then interconnected to one another in the next layer (this connection could be also referred to as a synapse) [25]. The Fig. 2 illustrates the intrinsic structure of the MLP network used. The MLP network solution utilized for classification contains two hidden layers, along with one input and one output layer.

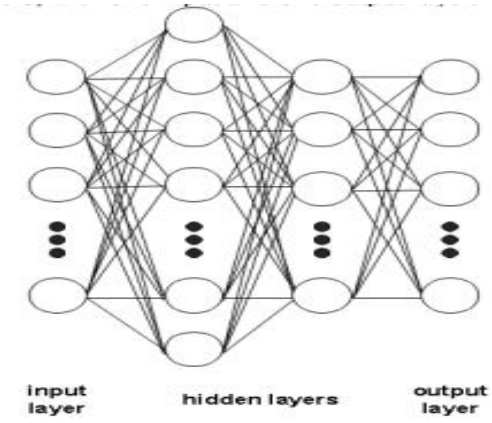

Fig. 2 MLP neural network topology

Each neuron present in the input layer is assigned a value depending on the input parameters. This layer contains the same number of neurons like the number of parameters present in the input set. The input layer is followed by two hidden layers and output layer. The output layer contains the same number of neurons similar to the number of attack classes; therefore every neuron is a single class of an attack learned. The number of neurons present inside the hidden layers is based on the neural network infrastructure and is generally greater than the number of neurons present in input or output layers.

PERCEPTRON

The perceptron is a more generic computational model compared to McCulloch-Pitts units. The important novelty lies in the inclusion of numerical weights for the connections and a specialized pattern of interconnection. The activation function for neuron – sigmoid has an effect over the ultimate strength of a neuron. This resultant strength is then transferred through the connections to neurons present in the next subsequent layer when afflicted by the connection weight of each one. These weights act as a memory for the neural network. The inputs for the activation function are obtained from original inputs $x_1, x_2,\ldots, x_n$ from the earlier layer, with the corresponding connection weights $w_1, w_2,\ldots, w_n$. The output from a neuron ranges between 0 and 1, where 0 implies inhibition and 1 indicates excitation. The ultimate value of the output of neuron (y) is based on its activation function. Like it was stated earlier, this function is a true sigmoid function (1) and (2).

$$S_c: \Re \rightarrow (0,1) \qquad (1)$$

$$y = S_c(z) = \frac{1}{1+e^{-cz}} \qquad (2)$$

The expression (3) depicts parameter z, the sum of the output acquired from the earlier layer neuron x and multiplies by respective connection weight w. Parameter c denotes a skewness of the sigmoid function (generally it equals to 1.0). Greater values of parameter c get the skewness of a sigmoid function nearer to the step function [26], [27].

$$Z = \sum_{i=1}^{n} w_i x_i \qquad (3)$$

BACKPROPAGATION ALGORITHM

As it was stated earlier, the memory of the neural network is maintained in connection weights. The neural network learning approach – backpropagation is utilized to get these values. During the classification, the neural network is in feed-forward mode and information is sent from the input layer to the output layer. Backpropagation function is in the form of a reverse strategy to feed-forward, with the particular set of data known as training set. The format of the training set is the same as the attack inputs used for neural networks but also contains the ultimate result of classification (or the class of the particular attack). The key behind a backpropagation algorithm and the neural network learning includes the weight adaptation process. It is performed on the training set consisting of inputs with outputs that are known. The solution acquired from the learning problem is an integration of weights with the minimalized error function.

$$\delta_j = \sum_{k=1}^{n} \delta_k y_k (1 - y_k) c w_{jk} \qquad (4)$$

The equation (4) reveals the computation of backpropagation error (δ) for connection weight in one layer (marked as j). It is taken as a multiplication of higher layer (marked as k) backpropagation error, real output, anticipated output and the original weight of the connection. Parameter y denotes the neuron output, x indicates its inputs always. Parameter c refers to the anticipated output and w stands for the connection weight. Then the backpropagation error is utilized in weight adaptation equations (5) and (6).

$$\Delta w_{ij} = \eta \delta_j y_i \qquad (5)$$

$$w_{ij} = w_{ij} + \Delta w_{ij} \qquad (6)$$

Learn rate parameter (η) impacts the connection weight correction, utilized for reducing the value of the error function (13). The learn rate parameter (η) helps in setting a correct step of correction in one iteration of back propagation [18], [19]. One iteration of back propagation learning makes use of all the records obtained from the training set. The last parameter w_{ij} refers to the connection weight from the earlier layer (i) to the original layer (j)

4. EXPERIMENTAL RESULTS

In this research work, the result assessment is carried out with the Packet Delivery Ratio (PDR) and Packet Loss Ratio (PLR), the metrics of analysis that include Recall, Precision, Accuracy and F-Measure are utilized for the below existing ZRTP technique and proposed ZRTP+RSA technique. For the purpose of analysis, typical ZRTP-capable VoIP clients are selected. The selection criteria are listed as below.

1. It must be capable of executing these test cases:

- When the client provides support to federated SIP and does not work in a closed network, it can be tested by performing a call to a special

Jitsi client, which has been manipulated to execute the test cases against the calling client.

- When the client is working in a closed network, it has to realize these test cases directly on this client. This needs the source code of the client.

2. The client must possess relevance:

- The client has to be actively utilized, i.e., with a user base installations of close to100,000.
- The realization has to be actively developed, i.e., the release of new versions have been done in 2016.

Packet Delivery Ratio (PDR):

The ratio of the number of packets that are received at the destination end to the number of packets transmitted by source is known as the packet delivery ratio (PDR). Bigger value of this metric denotes a considerable improvement in performance.

$$PDR = \frac{\sum packets\ received\ by\ destination}{\sum packets\ sent by\ source} \times 100 (7)$$

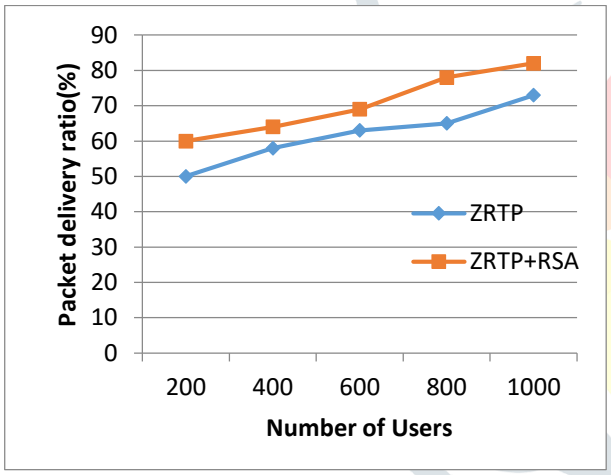

Figure 3. Packet delivery ratio with ZRTP and ZRTP+RSA

Figure 3 graphically represents the Packet delivery ratio obtained with ZRTP and ZRTP+RSA for the data transmission carried out on the networks over VoIP protocol, and the experimental analysis reveals the result that is deemed superior.

Packet Loss Ratio (PLR):

Packet loss ratio is defined as the ratio of data packets that are lost against the number of data packets transmitted during simulation. The metric must have a lesser value for an network with greater efficiency.

$$PLR = \frac{\sum Data\ packets\ dropped}{\sum Data\ packets\ sent} \times 100 (8)$$

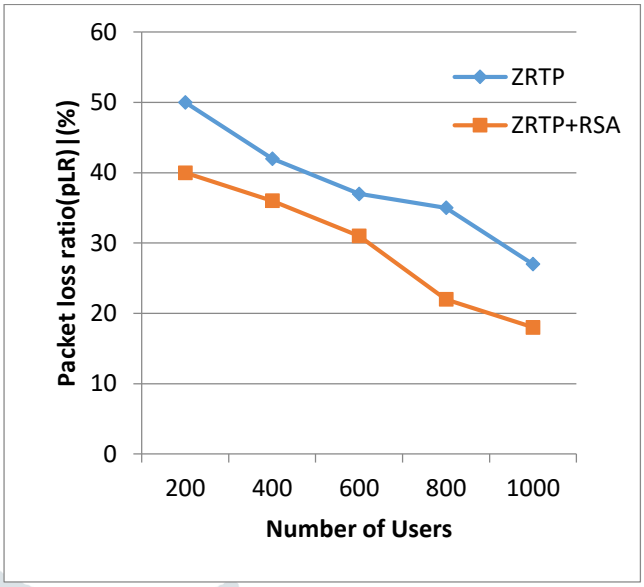

Figure 4. Packet Loss ratio with ZRTP and ZRTP+RSA

Figure 4 graphically represents the Packet Loss ratio obtained with ZRTP and ZRTP+RSA during the data transmission occurring on the networks over VoIP protocol, and the experimental evaluation indicates the loss of the packets in comparison with the delivery packets.

Recall

The recall is computed as below,

$$Recall = \frac{T_p}{T_p + F_n} \times 100 \quad (9)$$

Where T_p is referred to as True positive and F_n is called as false negative.

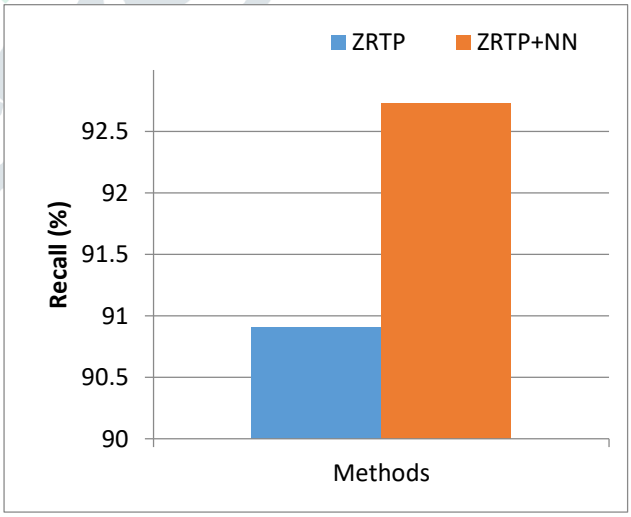

Figure 5. Recall metrics with ZRTP and ZRTP+RSA

Figure 5 graphically shows the Recall metrics obtained with ZRTP and ZRTP+RSA techniques. The experimental outcomes reveal the comparison analysis done with the available and proposed techniques.

Precision

The precision is computed as below,

$$\text{Precision} = \frac{T_p}{T_p+F_p} \quad (10)$$

Where T_p is referred to as True positive and F_p is called as false positive.

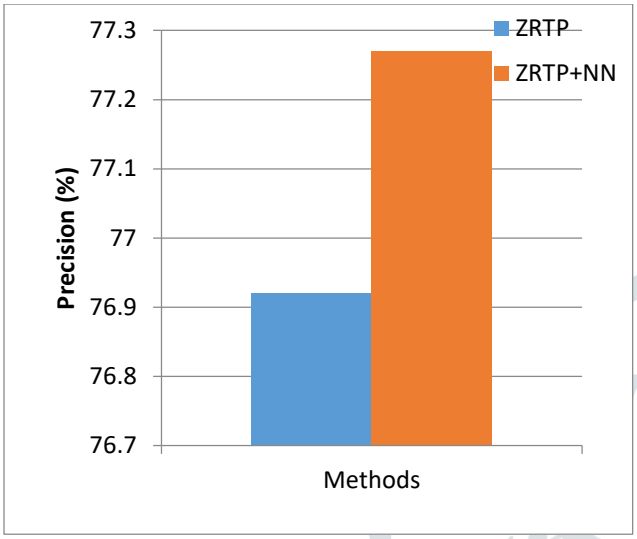

Figure 6. Precision metrics with ZRTP and ZRTP+RSA

Figure 6 graphically represents the Precision metrics using ZRTP and ZRTP+RSA techniques. The experimental outcomes reveal the comparison results obtained with the available and proposed techniques.

Accuracy

The accuracy is computed as below,

$$\text{Accuracy} = \frac{T_P+T_n}{T_P+F_p+T_n+F_n} \times 100 \quad (11)$$

Where T_p is referred to as True positive, T_n is called as True negative, F_n is referred to as false negative andF_p is called as false positive.

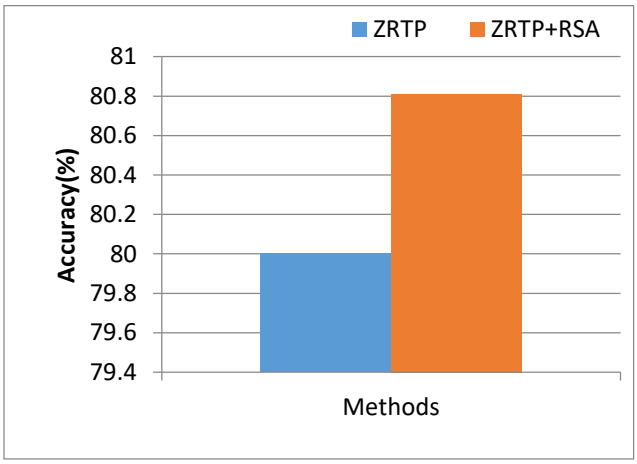

Figure 7. Accuracy metrics with ZRTP and ZRTP+RSA

Figure 7 provides the graphical demonstration of the accuracy metrics using ZRTP and ZRTP+RSA techniques. The experimental outcomes reveal the comparison analysis carried out with the available and proposed techniques.

F-measure

It provides the measure of the test's accuracy. It considers both the Precision(P) and the Recall (R) of the test into account for the score computation.

$$F - Measure = 2.\frac{P.R}{P+R} \quad (12)$$

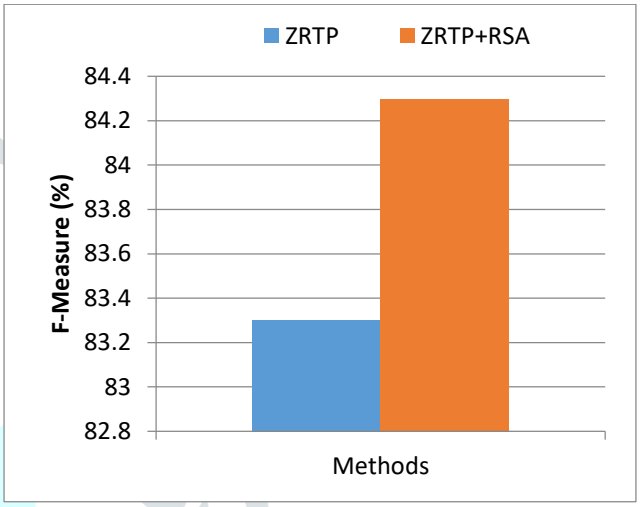

Figure 8. F-Measure metrics with ZRTP and ZRTP+RSA

Figure 8 graphically represents the **F-Measure** metrics obtained with ZRTP and ZRTP+RSA techniques. The experimental outcomes reveal the comparison analysis obtained with the available and proposed techniques.

5. CONCLUSION

Secured communication in VoIP networks is a huge challenge owing to its packet loss rate, absence of authentication and eavesdropping. Therefore, a secured secret sharing approach with single path routing accomplishes a robust secure communication employing enhanced secret sharing algorithm to be used in VoIP networks. Secured secret sharing exploited in the VoIP network will avoid attacks from intruders. In order to yield security, the architecture is developed with the aim of satisfying the concerns including solid authentication, access control techniques, key control. The ZRTP security mechanism renders a secure channel for VoIP along with Ron Rivest, Adi Shamir and Leonard Adleman (RSA) algorithm to safeguard from malicious attacks. It is found that the susceptibility of ZRTP protocol combined with RSA algorithm is due to the isolation between the platform state verification and the key exchange process. End-to-end security is necessary for protection against wiretapping of voice calls. For such communication in real-time, the ZRTP key-agreement protocol is used with the Neural Network Classifier. The classifier is employed for detecting the attacks due to intruders. This

comprehensive evaluation unravelled a crucial danger, which lets wiretapping even when Short Authentication Strings are compared accurately. This technique exhibits superior performance compared to the algorithms available.

REFERENCES

1. Sanjay Kumar Sonkar, Rahul Singh, Ritu Chauhan, Ajay Pal Singh "A Review Paper: Security on Voice over Internet Protocol from Spoofing attacks", International Journal of Advanced Research in Computer and Communication Engineering Vol. 1, Issue 3, May 2012.

2. Phithakkitnukoon, Santi; Dantu, Ram and Baatarjava, Enkh-Amgalan (2008). "VoIP security – attacks and solutions", Information Security Journal: A Global Perspective.

3. Henning Sanneck, Nguyen Tuong Long Le, Martin Haardt and Werner Mohr "Selective Packet Prioritization forWireless Voice over IP", Siemens AG, Information and Communication MobileNetworks.

4. Anderson, R.J., 2010. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.

5. P. Gupta and V. Shmatikov, "Security Analysis of Voice-over-IP Protocols," *20th IEEE Computer Security Foundations Symposium (CSF'07)*, Venice, 2007, pp. 49-63.

6. El Bakry, H.M., El Deen, A.E.T. and El Tengy, A.H., 2016. Implementation of an Encryption Scheme for Voice Calls. *International Journal of Computer Applications*, *144*(2).

7. Dunte, M. and Ruland, C., 2007. Secure Voice-over-IP. *Journal of Computer Science*, *7*, pp.63-68.

8. Chacon, S., Benhaddou, D. and Gurkan, D., 2006, April. Secure voice over Internet Protocol (voIP) using virtual private networks (VPN) and Internet Protocol Security (IPSec). In *Region 5 Conference, 2006 IEEE* (pp. 218-222). IEEE.

9. Phithakkitnukoon, S., Dantu, R. and Baatarjav, E.A., 2008. VoIP Security—Attacks and Solutions. *Information Security Journal: A Global Perspective*, *17*(3), pp.114-123.

10. Gupta, P. and Shmatikov, V., 2007, July. Security analysis of voice-over-IP protocols. In *Computer Security Foundations Symposium, 2007. CSF'07. 20th IEEE* (pp. 49-63). IEEE.

11. Aghila, G. and Chandirasekaran, D., 2011. An Analysis of VoIP Secure Key Exchange Protocols Against Man-In-The-Middle Attack. *the International Journal of Computer Applications*, *34*(7), pp.46-52.

12. Voznak, M., Safarik, J. and Slachta, J., 2014. A neural network based system for classification of attacks in ip telephony. *International Journal of Circuits, Systems and Signal Processing*, *8*, pp.368-375.

13. Safarik, J. and Slachta, J., 2015, May. VoIP attacks detection engine based on neural network. In *Independent Component Analyses, Compressive Sampling, Large Data Analyses (LDA), Neural Networks, Biosystems, and Nanoengineering XIII* (Vol. 9496, p. 94960J). International Society for Optics and Photonics.

14. P. Zimmermann, A. Johnston, and J. Callas. ZRTP: Media Path Key Agreement for Unicast Secure RTP. RFC 6189 (Informational), April 2011.

15. Patrick Juola. Isolated-Word Confusion Metrics and the PGPfone Alphabet. In *International Conference on New Methods in Natural Language Processing*, 1996.

16. Patrick Juola. Whole-word phonetic distances and the PGPfone alphabet. In *Fourth International Conference on Spoken Language (ICSLP 96)*, volume 1, pages 98–101 vol.1, October 1996.

17. Wikipedia. Commitment scheme. http://en.wikipedia.org/ wiki/Commitment_scheme. (Accessed: 10/2016).

18. Saruchi Kukkar, "Encrypted IP Voice Call Communication on Android through Sip Server on 3G GPRS" International Journal of Engineering and Technology Volume 2 No. 2, February, 2012.

19. Ferguson, N., Schneier, B. and Kohno, "Cryptography Engineering: Design Principles and Practical Applications", T. Indianapolis: Wiley Publishing, Inc. 2010.

20. Arfan Shaikh, "Audio Steganography And Security Using Cryptography", International Journal of Emerging Technology and Advanced Engineering, Volume 4, Issue 2, February 2014.

21. Kamailio. Kamailio SIP-Server. https://www.kamailio.org. (Accessed: 10/2016).

22. PjProject. PjProject. http://pjsip.org/, 2015. (Accessed: 10/2016).

23. Werner Dittmann. ZRTP4PJ README. https://github. com/wernerd/ZRTP4PJ/tree/develop, 2015. (Accessed: 10/2016).

24. P. Fazio, F. De Rango, I. Selvaggi, "A novel bandwidth reservation algorithm based on neural networks path prediction in wireless environments", Int.Symposium on Perf. Evaluation of Computer and Telecommunication Systems (SPECTS '10), Jul 2010, Ottawa.

25. R. Rojas, Neural Networks, Springer-Verlag, 1996, ISBN 978- 3540605058.

26. J. Heaton, Introduction to Neural Networks for JAVA, 2nd Edition", Heaton Research, 2008, ISBN 978-1604390087.

27. J. Safarik, P. Partila, F. Rezac, L. Macura, M. Voznak, "Automatic Classification of Attacks on IP Telephony", Advances in Electrical and Electronic Engineering, Vol. 11, Issue 6, 2013, pp. 481-486, ISSN 1336-1376.