Received: June 25, 2017

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Ant Colony Optimization Based Handoff Scheme and Verifiable Secret Sharing Security with M-M Scheme for VoIP

Shankar Ramasamy[1*] **Karthikeyan Eswaramoorthy**[2]

[1]*Computer Science, Chikkanna Govermment Arts College, Tirupu, India*
[2]*Computer Science, Government Arts College, Udumalpet, India*
* Corresponding author's Email: shankarcgac@gmail.com

Abstract: Voice over Inter Protocol (VoIP) empowers in the integration of voice data over IP networks, minimizing the cost of network transmission for helping users of IP protocol. Robust and effective procedure of handoff is introduced for increasing the quality and the dependability of the networks. Ant Colony Optimization (ACO) is presented for the handoff mechanism and Mean Opinion Score (MOS) is observed to be the fitness value for obtained measurements of the assessment of voice quality. In this research, the scheme of Multiplex-Multicast (M-M) is proposed that will improve the capability of VoIP in WLAN to 100% in the form of an infrastructure Basic Service Set (BSS). This research work deals with the security features of VoIP in order to enhance the quality making use of Verifiable Secret Sharing (VSS) with the help of M-M scheme. The M-M scheme will eliminate the downlink VoIP traffic ineffectiveness through the multiplexing of the packets from different VoIP streams into one multicast packet for transmitting over the WLAN. The results from simulation indicate the advancements in the security enhancements making use of the proposed schemes. The average Round Trip Time (RTT) results of the proposed VSS with M-M are 0.30436 milliseconds, whereas average RTT is 0.3598 milliseconds and 0.43604 milliseconds for VSS and Shamir SS methods respectively. It concludes that the proposed VSS with M-M takes lesser RTT results when compared to existing methods.

Keywords: Verifiable secret sharing (VSS), Round complexity, Multiplex-multicast (MM) scheme, Homomorphism, Ant colony optimization (ACO), Seamless vertical handover, VoIP security and network simulator 2 (NS-2).

1. Introduction

Voice over Inter Protocol (VoIP) mechanisms are seeing an increased adoption for usage by consumers, enterprises, and telecoms operators because of their power for greater flexibility, rich feature set, and minimized expenses with respect to their counterparts of Public Switched Telephony Network (PSTN). With the advancement in the technology, VoIP can yield a greater quality and phone service that is still more affordable compared to PSTN.

Due to the requirement for interoperating seamlessly with the already available VoIP telephony infrastructure and the rapidity of development and implementation, VoIP protocols and their products have been observed to have several vulnerabilities many number of times [1] which have been brought into better use. In case an attacker does the sniffing on the network between any two end-users who are in communication, the attacker can observe nearly each piece of data transmitted over the wire. The attacker can also do the insertion of its own malicious packets into the wire disallowing the victim from utilizing the network resources. Among the different problems which are required to be dealt with during the deployment of this scheme, security is one among the most crucial one [2].

Butcher et al [2] provided an overview over the security problems and techniques for VoIP systems that focus on operational practices that are security-oriented used by VoIP providers and operators. Anwar et al [3] identified few areas in which the NIST report is still not complete: counter-intuitive

outcomes corresponding to the relative performance of the encryption and hash algorithms, the non-usage of the standard Mean Opinion Score (MOS) for evaluating the call quality, and the absence of expectation of RTP-based denial of service.

Already available methods have made use of Shamir's secret scheme [4]. In [5] two Shamir's secret sharing scheme modifications are introduced. In the first modification, every shareholder maintains both the x-coordinate and y-coordinate of a polynomial in the form of private share. In the second modification, dealer makes use of polynomial with a degree greater than the threshold value t for generating the shares for (t; n) threshold scheme. But, the effort is not a balanced for the mechanism of handoff; hence a very much reduced effort is put on some problem fields that greatly deserve it.

The major objective of the proposed system is to increase the security of VoIP and the handoff issue is solved by using Ant Colony Optimization (ACO) that measures the quality of the VoIP. Security issue is resolved by making use of Verifiable Secret Sharing (VSS) with Synchronous and Asynchronous Communicational Model [6]. The major organization of the paper is organized as follows: In the section 2 review the details of the existing security algorithms for VoIP protocol. In the section 3 overall methodologies for proposed work is discussed briefly. The simulation results of the proposed VSS-M-M and existing security protocols results are measured using RTT, jitter and Packet Delay Variation (PDV) is discussed in section 4. At finally concludes the paper in the section 5 and scope of the future work also discussed at end of the work.

2. Literature review

Sengar et al [7] illustrated about the threats pertaining to security in the integrated signaling environment and also the evolving PSTN and VoIP networks. The important challenge of this work is that the networks in the neighborhood are vulnerable to attacks. Walsh & Kuhn [8] described the VoIP security threats and the procedures for securing the organization of VoIP network. It renders economic cost and larger flexibility for an enterprise, though it also introduces considerable security issues. Unluckily, firewalls introduced to a VoIP network make different aspects of VoIP to be complex.

Sisalem et al [9] studied about the challenges with consideration to the DoS attacks of VoIP servers. Talevski et al [10] tried to offer for the issues related with the mobility and security in VoIP by integrating the reliable features of security and lightweight VoIP protocol. This protocol will render end-to-end security without the use of special hardware.

Rong and Qian [11] exhibited the SIP for VoIP applications and examined the issues in VoIP systems and presented a design for improved SIP server. Wu et al [12] introduced the Intrusion Detection System (IDS) in VoIP networks. They provide the expansion of the design of a single-component interruption recognition scheme referred to as SCIDIVE for the dispersed and correlation-based interruption recognition system. Passive attacks Detection cannot be performed making use of Space dive.

Yeun and Al-Marzouqi [13] proposed the IDS in VoIP networks. At last, the security evaluation of this implementation is given and various protocols that are involved in securing VoIP more through the prevention from Man in the Middle attack by making use of a novel MIKEY protocol is analyzed. The measurement of the key generation performance is done by only the Initiator hence no provision of a thorough forward secrecy is carried out.

Angrisani et al [14] introduced the design and the deployment of a reconfigurable test bed for the purpose of real time measurements on VoIP systems that facilitate the Telecommunication Engineer with ways for planning the required modifications in the network/VoIP platform, gradually attaining a greater degree of security. The important problem of the work is the non-availability of policy for the control of reservation.

Pecori [15] demonstrated a novel protocol for the establishment of a security association between the two peers that desire setting up a VoIP or multimedia communication by means of the standardized SIP protocol. The technique proposed has been also realized and then integrated in an open source SIP UA. It is costly and it cannot be encrypted for long distance communication.

Sachin &Tamrakar [16] introduces a new efficient technique for identifying the IP and MAC spoofed attacks. Chan and Lin [17] designed a new seamless handoff scheme for IEEE 802.11 networks by installing Access Points (APs) along with multiple Wireless Network Interface Cards (WNICs), one among which is set to function for normal transmission and rest of the others listen or receive STAtion(STA) packets for the signal measurements. Niswar et al [18] introduced Vertical Handover Management (VHM) for VoIP session which concentrates on the initiation of HO and the strategy of decision based on the condition of the

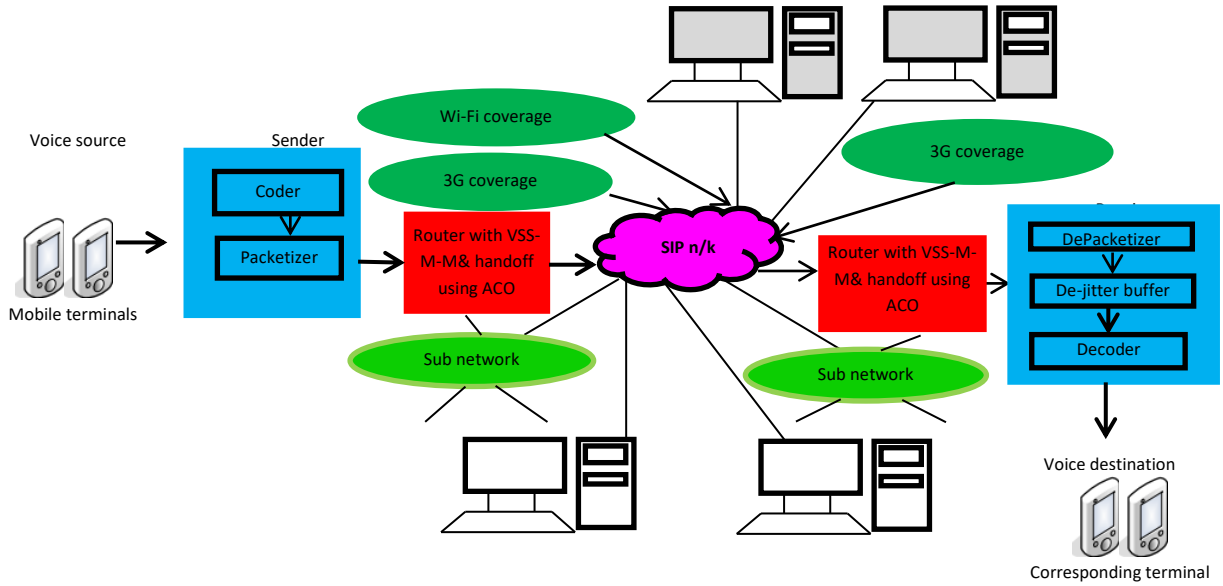

Figure. 1 Proposed Secure VoIP based on a VSS-M-M Scheme

wireless link and the state of congestion of wireless networks. The simulation outcomes indicate that the VHM proposed can maintain the VoIP session quality at the time of such HOs.

But all of these techniques may not resolve handoff issue in VoIP security, as incase the handoff issue is resolved it improves the system efficiency easily by resolving the problem of collision. Few techniques have also been introduced in the work carried out recently for resolving the handoff problem in VoIP without caring for security. But in these schemes security is not an essential factor, but this research work takes both QoS and security.

3. Proposed methodology

In this research, a solution is described for the security and handover mechanism. Security issue is resolved by making use of synchronous and asynchronous communicational model which were utilized in VSS. Figure 1, the security of VoIP is carried out by employing VSS scheme. M-M scheme is proposed for eliminating the huge overload of VoIP over WLAN. In order to resolve the handoff issue, this research work introduces an ACO approach [19-20]. In this research paper, the ACS variant is followed for developing the ACO approach for resolving the handoff issue. Figure 1 IP networks; there are also possibilities for using paths more than two for communicating between a pair of terminals employing an overlay routing mechanism [21].

Vertical Handover Mechanism: In this research paper design of new prototype implementation, and demonstrate the usefulness of this approach for seamless handoffs in Wi-MAX. In Wi-MAX, clients connect to the Internet via APs. In order to maintain continuous connectivity during this period, the mobile client has to switch between APs, in a process known as a handoff. Implementing the handover with the CT might lead to high delays, for this reason, numerous explanations have been proposed to solve this problem by introducing temporary anchor points [21-22]. In the proposed solution the anchor point is not temporary, however permanent. In fact, an enduring media communicate in the path is not an effectual and striking solution; therefore this novel relay is not supplemented with this way out.

A supposition is prepared that the Session Border Controllers (SBCs) will be in the trail previously. Consequently, the mobility anchor point anticipated is included with the ability of SIP dispensation and media communicate specified by SBCs. Extending its network interface capacities to support the vertical handoff is a direct step. For constructing the IP addresses on the MT interfaces, the existing Dynamic Host Configuration Protocol (DHCP) on Purchasing Power Parity (PPP) and the WLAN on the 3G interface has been used to handoff mechanism. When the numerous interfaces are in a lively situation, the MMC necessitates deciding the enviable boundary for transmitting/receiving the media streams or for the switch over of Session Initiation Protocol (SIP) protocol [23]. SIP based solution is used for mobility management aiming to provide seamless voice service in VoIP mechanism. The novelty of the solution is that it depends on the SBCs which are currently used in commercial SIP telephony solutions to deal with NAT traversal. This proposed solution has been experimented in a test

bed where the IEEE 802.11 and 3G technologies have been used correspondingly as typical Wi-MAX and cellular access networks. The assortment of the interface performed out by MMC may rely on the feature of cost and/or on QoS anxiety such as perceived packet loss, Received Signal Strength (RSS), and/or delay and so on.

Delay: Delay can be defined as the total time taken from the time a person, who is communicating with another person, speaks some words and hears them at the other end. End-To-End delay is one amongst the important parameter impacting QoS and encompass to be smaller than 150 ms for a high-quality network association as distinct by ITU G.114 whereas delay lower than 100 ms is defined by the European Telecommunications Standard Institute (ETSI). Delay is chiefly caused by congestion in the network that results in a slower delivery of packets [24-25].

Delay at the mobile terminal: The delay of the complete method carried out at the mobile terminal side previous to the broadcast of the voice packet in excess of the network consequences from diverse components: codec, packetization and process [26]. Codec functions present few delays while doing the processing of the analogue-to-digital conversion.

Delay at the corresponding terminal: The reverse procedure which is demeanor at the MT at the recipient attaches more delay: decoding delay and process delay that comprises decompressing delay.

Network delay: Network delay in the WLAN surroundings and broadcast are the new components encompassing network delays. The propagation delay points to the delay in the corporeal medium of the network, while transmission delay is comprehensive of the MAC retransmission delay and router's delay.

Jitter: IP network does not ensure the delivery time of the packets that brings in changes in transmission delay. This variation is referred to as jitter [27] and it has more of adverse effects on the voice quality [28], as the voice packets in the same flow are not received at the same instant. Many adaptive buffer algorithms [29], are proposed for improving the quality of VoIP.

Packet loss: Packets that are propagated over IP network may get lost in the network or they can arrive being corrupted or late. Hence packet loss is the total loss that occurs because of congestion in the network and late arrival [30]. Moreover, VoIP system can bear the packet loss to some extent such as 1% or less is also acceptable for the roll quality whereas for the case of business, quality of 3% or less can be accepted [31]. Additionally, Forward Error Correction (FEC) is a mathematical strategy which assists the receiver in reconstructing the lost packets from earlier sent packets.

Throughput: This factor is anxious with the utmost number of bits that are reached out of the entire count of bits which are distributed during a scrupulous interval of time. In IEEE 802.11 networks, the bit rate of every standard is defined like IEEE 802.11b transmits at the rate of 1 Mbps, 2Mbps, 5.5 Mbps and 11 Mbps. The throughput accomplished ranges from 50% to 70% of the broadcast rate which is small in contrast with the Ethernet throughput that is accomplished from 80% to 90% of the transmission rate.

PSQM: In the recommendation P.861 Perceptual Speech Quality Measurement (PQSM) has been standardized and their original model of MOS score is improved. The range of a score is [0 - 6.5]. 0 indicates an alignment in perfection between the reference and distorted output signal and means an excellent quality. Based on the scope of P.861, PSQM is preferred for the assessment of speech codec's quality [32].

E-model: E-model is introduced by ITU-T Recommendation G.107 that integrates PQSM and PAMS. E-model is a combination of a different impairment factor for predicting QoS to be *R*-value in Eq.(1).

$$R = R_0 - I_s - I_d - I_e + A(1) \quad (1)$$

$R \rightarrow$ resulting voice quality (from 0 to 100), R_0 is signal to noise ratio, I_s identifies the simultaneous impairment feature similar to load speech level [33], I_d indicates the mouth-to-ear delay, I_e refers to the equipment impairment factor, and A stands for advantage of access.

Received Signal Strength Indicator (RSSI) measures the power level that is being received by an antenna. The higher is the RSSI value, the stronger becomes the signal strength. The relationship between the values and network impairments like packets loss rate is analyzed, it was demonstrated that the poor RSSI values results in higher packets loss rate. Packet losses were only seen from RSSI value that is less than −75 dBm.

Mapping of RSSI to QoE: The MOS model introduced [34] for the QoE measure in AMR codec. It is indicates that the RSSI values greater than −74 dBm yield a very good VoIP quality with 4.2 MOS value. The values with respect to Delay, Packet loss, Throughput, PQSM and RSSI are decided making use of ACO.

Ant Colony Optimization (ACO) for Handoff Mechanism : This research work follows an ACS variant for developing the ACO approach for the handoff issue considered. The important features of the ACS are based on two aspects. First, during the procedure solution construction, the ACS uses a pseudorandom proportional selection rule that follows an aggressive bias in choosing the components having the maximal pheromone and heuristic values. Secondly, in the procedure of pheromone management, ACS comprises two policies of pheromone modernized, that are the local updating and the global updating. The global updating regulation conveys the mechanism particular to the best-so-far solution to be more powerful. The order of the mobile terminal is assumed and given by $MT=(mt_1,.., mt_n)$ which meets the precedence QoS parameters as defined above. Initially, the pheromone and the heuristic for building of the mobile terminal register are definite. After that the process for an ant for construction a mobile terminal register will be given in details elaborately.

Pheromone: To construct a mobile terminal list, an ant has to decide over the order of the senders or the voices. The first kind is the absolute position prototype which defines the pheromone regarding putting the mobile terminals MT_j to the k[th] position of the mobile terminal list to be $\tau_t(j,k)$. The QoS for a mobile terminal MT_j that is represented as QOS_j can be estimated as below:

Step a: Estimate the highest QoS of every mobile terminal. For estimating the highest QoS of MT_j , choose the to be $MaxQoS_j$ the most proficient QoS of MT_j. Here $MaxQoS_j$ refers to the maximum QoS for MT_j which can be assessed by constraints that are mentioned above.

Step b: As per the highest QoS of every mobile terminal, the heuristic for mobile terminal MT_j is expressed by Eq.(2)

$$\eta_t(j) = MaxQoS_j \tag{2}$$

Construction procedure: In order to construct a practical mobile terminal list, every ant keeps a record of an eligible mobile terminal list consisting of the mobile terminal nodes which satisfy the QoS constraint. The construction comprises of the following steps:

Step a: Place the mobile terminals which can be realized at the start of the transmission into the eligible MTSet.

Step b: For *k=1 to n* repeatedly process the following sub steps b-1 and b-2.

Step b-1: Selecting the least one amongst the mobile terminal from suitable MTSet and situate the mobile terminal to the k[th] place of the task register. In the selection rule, at start, a random number q distributed uniformly in [0; 1] is then generated and a comparison is made with a parameter qt. When $< q_t$, then the mobile terminal MT_j from the eligible MTSet having the highest value is selected to be put to the k[th] position. Else, the mobile terminal is chosen making use of the roulette wheel selection scheme. The probability $Pr(j,k)$ of choosing the mobile terminal MT_j to the k[th] position in the roulette wheel selection is expressed by Eq.(3)

$$\Pr(j,k) = \begin{cases} \dfrac{\sum_{l=1}^{k} \tau_t(j,l)\eta_t(j)}{\sum_{mt_u \in eligibleMTSet} \sum_{l=1}^{k} \tau_t(u,l)\eta_t(u)} & if mt_j \in eligibleMTSet \\ 0 & otherwise \end{cases} \tag{3}$$

Step b-2: Update the eligible MTSet by eliminating the chosen mobile terminals from the eligible MTSet and adding the new feasible mobile terminals which meet the precedence QoS constraint into the eligible MTSet. During the building of the mobile terminal list and the QoS allocation matrix, just immediate after a choice is made, the local pheromone updating rule is then applied to minimize the respective pheromone values such that the following ants can have better chances of choosing the other probable selections. In this manner, the algorithm takes care of maintaining the diversity. Suppose that the mobile terminal MT_j is selected for the k[th] location of the mobile terminal list then the relevant pheromone is reorganized by Eq.(4)

$$\tau_t(j,k) = (1-\rho)\,\tau_t(j,k) + \rho.\tau_{initial} \tag{4}$$

Where ρ → parameter. The standards of Pheromone which is linked with the best-so-far arrangement are reorganized by Eq.(5)

$$\tau_t(j,k) = (1-\rho)\,\tau_t(j,k) + \rho.\Delta_\tau \tag{5}$$

where $\Delta_\tau = 1/f$ → reciprocal of the objective function value of the plan. On the basis of these definitions, since the denominator in Eq.(5) is an upper-bound estimation, $\tau_{initial}$ indicates the lower-bound of all the pheromone values. With the development of the algorithm, the cost of the best-so-far plan that is found by the algorithm gets lesser and lesser. This way, the value of $\tau_{initial}$ gets to

become higher. Otherwise said, more amount of pheromone will be added to the constituents of the best so- far plan to give them more attraction for the ants in the iterations that follows. From this step, the identification of a better handoff mechanism is done, and thereafter an M-M scheme is carried on by limiting the block that is formed at the AP making use of this scheme.

M-M Scheme in VoIP Networks : The M-M scheme will have the AP prioritized by means of the Multicast Inter frame Spacing (MIFS), a new inter frame spacing interval. By employing this MIFS, there is no collision between the terminals and the AP since it widens the medium access prior to another station and will directly transmit. Each time, the multiplexed packet will be provided by the multiplexer. The inter packet interval will differ from codec to codec. The VoIP traffic will begin from multiple sources and gathered through the gateway. The multiplexer will substitute the UDP, IP and RTP header of each voice packet. Utilizing the IP address, the packets multiplexed are multi casted through the access point 'W'. The networking environment is then set up with 8 nodes that comprises of a VoIP flow that is established between the two schemes. This research deploys the M-M scheme for synchronous and asynchronous communication in VSS is explained as below.

VSS Protocol Adversary Model: Consider a VoIP network model having 'n' Mobile Terminals (MTs) MT=(mt_1,..,mt_n) in which a popular MT works in the role of a dealer. Considering a scenario wherein adversary 'A' is t-bounded [6] and it can create compromise and coordinate actions of up to 't' out of 'n' MTs. It is also assumed that the adversary is adaptive; it may corrupt any MT at any time at the time of execution of a protocol until the count of corruptions is limited by 't'. A MT is known to be honest, if it is not under the control of any adversary.

Sharing: At first, D has an input s in its hold, known as the secret, and every mobile terminal may have an autonomous random input r_i. The sharing phase may comprise of multiple rounds of interaction between the parties. At the sharing phase's end, every honest mobile terminal mt_i has a notion v_i that may be necessary for reconstructing the secret of the dealer at a later time.

Reconstruction: In this phase, every mobile terminal mt_i announces its whole view v_i from the sharing phase, and then a reconstruction function rec $(v_{1,\ldots,} v_n)$ is employed and is considered to be the protocol's output. An n-party VSS protocol, having t-bounded adversary A, is called an (n,t)-VSS protocol if it meets the conditions that follows:

Secrecy: When D is honest then the intruder's view at the time of the sharing phase exposes no information regarding s.

Correctness: In case D is honest, then the honest parties provide the secret s as the output during the reconstruction phase's end.

Commitment: Lest D is deceitful, then at the end of the allocation phase there is an assessment $S^* \in F^P U\{\perp\}$such a means that all the direct parties' yield S* at the last part of the reconstruction stage. A cryptographic commitment mechanism is a two-phase cryptographic protocol observed between a committer and a verifier.

Commit Phase: Provided a message m, a committer runs C(m,D)=Commit(m) and then announces C to be a commitment which binds it to a certain message m without exposing it. The function may then provide an opening value as the output d.

Open Phase: The committer opens the commitment C by exposing (m, D) to a verifier. The verifier can thereafter check whether the message has consistency commitment i.e. $m \stackrel{?}{=} Open(C,m,D)$

VSS Protocol for Synchronous Communication Model: In the synchronous model [35], in a sequential order of rounds the distributed protocols are worked out. During each round, some local computation is carried out by a party and the messages are transmitted to the dealer employing the authenticated private link and then some information is broadcasted over the broadcast channel. At the end of the round, every message broadcasted or sent is then received by the other parties in the same round. This works in a synchronous model combined with adaptive and t-bounded in order to let the adversary to rush in every round communication such that it can hear or wait for the message from the honest parties prior to transmitting its own message. Even though, it is feasible to hold more than one round at the time of reconstruction phase [36],every one of the protocols request for single round during the time of reconstruction.

VSS Protocol for Asynchronous Communication Model: In VoIP, the VSS focused on asynchronous settings, since it is feasible to $n \geq 3t+1$ [36]. The communication replica of an asynchronous network encompasses n mobile terminals MT=(mt_1,…,mt_n) is pursued in such a means that every pair of parties is linked byways of an authentic, concealed communication link. In the asynchronous communication surroundings, it is more unspecified that the opponent has to organize the network and might delay the messages broad casted among some of two honest mobile terminals.

Liveness: When the dealer D is honest during the sharing phase, then all of the honest mobile terminals are finished with the sharing phase.

Agreement: In case some of the honest mobile terminal finishes the sharing phase, then all the honest mobile terminals will also gradually end the sharing phase. When all the honest mobile terminals subsequently begin the reconstruction phase, then all the honest mobile terminals will end the reconstruction phase.

Packet Multiplexing and Multicasting: The M-M method will unite the data from numerous downlink rivulets into a one particular superior packet. The different VoIP overheads packets are minimized to one overhead packet. For the transmission of the multiplexed packet, the multicast is employed so that all the stations will receive by a single transmission. Specifically, the VoIP downlink traffic will transmit at first in the voice gateway through a MUX. The MUX will then keep the UDP, IP and RTP header of each voice packet down with the compressed small header that combines the numerous packets into a solitary multiplexed packet, and after that the multiplexed packets are multicast keen on to the WLAN utilizing a multicast IP address transversely the AP. In sort to obtain the packets, each VoIP station is locates such that it is able on this multicast channel. For the identification of the session, the payload will provide the identification. The identification is utilized by the VoIP packet of the receiver for retrieving the packet from the packet that is multiplexed. For each t ms, the multiplexer will yield the multiplexed packet. The inter packet interval will differ from codec to codec. The traffic of VoIP will begin from multiple sources and then gathered across the gateway. The multiplexer will substitute the UDP, IP and RTP header of each voice packet. Making use of the IP address, the multiplexed packets are multi casted through the access point. The normal uni-casting is utilized by all the stations for the transmission of the uplink streams. The upstream packets are then delivered by AP and then it is received on the other BSS, once finished, the voice gateway of other BSS will send the packets to their destination by means of the multiplexing scheme. The MUX then broadcasts a multiplexed packet in each T ms that is equal to or smaller than the VoIP bury packet interval. For the case of GSM 6.10, the inter packet interval is set to 20 ms. Larger values can enhance the efficiency of the bandwidth, as more packets could be multiplexed, though the incurred delay will also be greater. By unstable 'T', one can adjust the exchange among the bandwidth competence and delay. There are several free sharewares therefore one could easily make use of the sniffer for the packets collection in the WLAN. In order to prevent this security issue, the HTSS is employed in this in addition to the M-M scheme.

Table1. Experimental conditions

Listeners	Four graduate students in their twenties
Speech signals	80 excerpts from the set of 1000 syllabic balanced sentences
Repetition	20
Sound level	60 dB

4. Experimental results

The experiment illustrates the VSS scheme along with an M-M scheme employing NS-2. Adoption of a secret sharing scheme leads to an increase in the network traffic. G.711 [37] bypass the audio signals in the variety of 300–3400 Hz and subsequently performs their sampling at the rate of 8,000 samples per second, besides the lenience on the rate of 50 divisions per million (pm). The conditions for the experiments are shown in Table 1. Four graduate students who are in their twenties with normal hearing ability took part in the experiments. With respect to source signals, 80 sentences extracted from the set of 1000 syllabic-balanced sentences, having a sampling rate of 44.1 kHz and a resolution of 16 bits, were utilized. These speech signals were transformed into 64-kbps PCM to be fed to an ADPCM encoder and thereafter processed to generate the test stimuli.

The Mobile Wi-MAX (IEEE 802.16e) has severely gained a concentration as resources of given that wireless broadband access to mobile users in a large domain, and it gives QoS for different types of applications. In order to improve wireless link quality and to solve congestion problem in heterogeneous wireless surroundings, implement a Vertical Handover Management (VHM). For the period of HO, the new VHM focus to maintain VoIP quality. Therefore, the VoIP applications must compete with different kinds of applications for acquiring transmission chance in IEEE 802.16e. Three different types of applications are used namely Skype VoIP Telephony, File Transfer Protocol (FTP) and Video Conferencing to give the service to the customer. These include VoIP server with an application of Skype VoIP Telephony (PCM quality), Video Server with an application of Video Conferencing (Light) and finally FTP Server with an application of FTP (Light). These servers are applicable to VoIP handsets. They also have two subnets which are Router Subnet and Wi-MAX

Subnet. The router subnet gives a route to the packets from the servers to reach the customers. The Wi-MAX subnets give the entire distribution of Wi-MAX customer in a cell based structure [38].

The majority of VoIP server with Skype VoIP Telephony uses a proprietary and closed protocol. For example cisco uses the Signalling Connection Control Part (SCCP) protocol, Avaya uses the extension of H.323 protocol, Nortel uses the Unistim protocol, and other vendors use some other proprietary protocols. In VoIP system, handsets call setups are secured through Transport Layer Security (TLS). Once call established, a call control is initiated so that encryption and media channel information can be discussed. Encryption is performed by using VSS within the RTP packet by third party hardware, or at the network layer. Table 3 displays the system parameters for 802.16e at the simulation. The performance of the VSS-M-M scheme technique proposed was evaluated by using NS2 simulator .The test conditions are summarized in Table 2.

The Mobile Node (MN) applied in a single IP address with various types of IP subnet. The MNs has double Ifs associated to two points such as BS and AP. The MNs implement the VoIP call with the CN. The new NHM working in a multi-homing is similar to [39-40] with respect to improve the VoIP session conservation among the MN and CN, it must be correctly switched among the single-casting and bi-casting modes in reply to wireless network rules. Single-casting mode known as the MN communicates with a CN using only one IF. Bi-casting is helpful for eliminating packet loss and examine both the 802.11g and 802.16e Ifs rules while an MN alter its IF for the period of communication. Therefore, it accomplishes more reliable VoIP communication for the period of HO.

Table 2. Summary of test configuration

Secret sharing	Shamir , Verifiable Secret Sharing (VSS), VSS with M-M
Speech codec	Pulse Code Modulation (PCM)
Speech duration	3 min and 45 s
Measure	QoS
Buffer size	80 ms, 330 ms
No of nodes	100
Distance area	100 x100 m
Locations of routers	1. One on wired network and other on wireless network 2. Both on wired network 3. Both on wireless network

Table 3. Simulation parameter for 802.16e

Parameters	Description
Simulation time	15 mins
Frequecny band	2.4 GHz
Dulpex mode	TDD
Channel Mode	10 MHZ
PHY profile type	OFDM
BS MAC address	Distance based routing
Standard	IEEE 802.16e standard
Trasmit time gap, Receive time gap	10 micro seconds
Base Station(BS) transmission power	30 dBm
Mobile Node(MN) transmission power	22 dBm
Fading model	Rayleigh
Applications	IP Telephony, Video Conferencing and FTP
Servers	VoIP server, Video Server and FTP Server

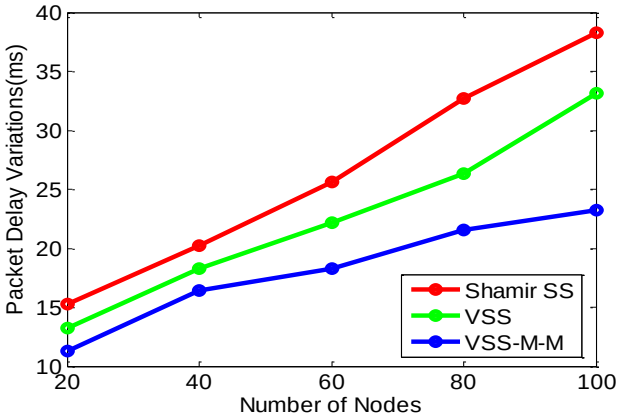

Figure 2. Packet Delay Variations Vs Number of Nodes in VoIP

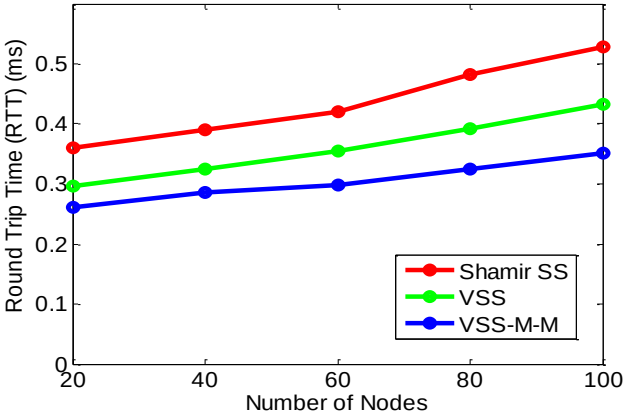

Figure. 3 Round Trip Time (RTT) Vs Number of Nodes in VoIP

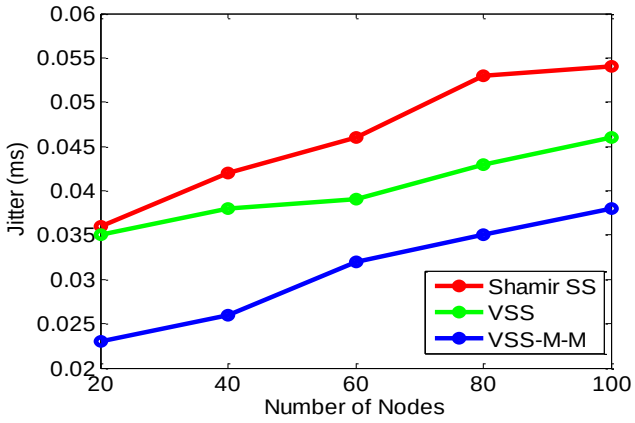

Figure. 4 Jitter Vs Number of Nodes in VoIP

Packet Delay Variations(PDV) is illustrated in figure 2 among the various secret sharing methodologies such as Shamir Secret Sharing (SS) [41], Verifiable Secret Sharing (VSS)[41], VSS with Multiplex-Multicast (M-M) (VSS-M-M). In the proposed method, the average PDV is 18.15 seconds which is 4.486 seconds and 8.26 seconds lesser when compared to VSS and Shamir SS methods respectively.

Round Trip Time (RTT) is the time required for a packet to travel from a specific source to a specific destination and back again. As it may be observed from the Figure 3, RTT of the proposed VSS-M-M is 0.304 milliseconds is an average. However the RTT of VSS is average of 0.3598 milliseconds average of 0.43604 milliseconds for Shamir SS.

Figure 4 is plotted which demonstrates the comparison of voice jitter and the number of nodes in VoIP. In VSS-M-M method has the average jitter value of 0.0308 ms which are 0.009 ms and 0.015ms less when compared to VSS and Shamir SS methodologies.

5. Conclusion and future work

Voice over Internet protocol (VoIP) is a widely known multimedia application in the recent times. For the Mobile Nodes (MNs) utilizing VoIP services in the wireless networks, the handoff concerns require attention. In order to solve handoff issue problem ACO algorithm is proposed for mobile Stream Control Transmission Protocol (SCTP) for transfer in VoIP request is investigate. The mobility of the user stuck between the base stations of the similar technology by exacting methods of the admission network specified and IP re-configuration is not essential. The M-M scheme will do the multiplexing of the downlink traffic of packets of VoIP into bigger multicast packets for decreasing the WLAN overheads. In addition, the VSS scheme is combined with M-M scheme are also proposed for security. In the proposed method, the average PDV is 18.15 seconds which is 4.486 seconds and 8.26 seconds lesser when compared to VSS and Shamir SS methods respectively. The results indicate that the proposed VSS with M-M scheme has achieves higher security than other methods. The future work will analysis and comparison of application layered protocol H.323 and SIP protocols with respect to security attacks and then it can be extend for mobility nodes in VoIP based MANET architecture.

References

[1] D. Keromytis, "Voice over IP: Risks, Threats and Vulnerabilities", In: *Proc. of the Conf. on Cyber Infrastructure Protection*, pp. 223-240, 2009.

[2] D. Butcher, X. Li, and J. Guo, "Security challenges and defense in VoIP infrastructures", *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, Vol.37, No.6, pp. 1152-1162, 2007.

[3] Z. Anwar, W. Yurcik, R.E. Johnson, M. Hafiz, and R.H. Campbell, "Multiple Design Patterns for Voice over IP (VoIP) Security", In: *Proc. of 25th IEEE Conf. on International Performance Computing and Communications*, Phoenix, AZ, USA, pp. 8, 2006.

[4] K. Maheswari and M. Punithavalli, "An Implementation of Security in VoIP using Modified Shamir's Secret Sharing Algorithm", *Networking and Communication Engineering*, Vol.3, No.13, pp.864-868, 2011.

[5] D.S. Kumar and N. Ananthi, "Enhancement of Security in VoIP using Modified Shamir's Secret Sharing and Multipath Routing", *Wireless Communication*, Vol.3, No.16, pp.1110-1115, 2011.

[6] M. Backes, A. Datta, and A. Kate, "Asynchronous computational VSS with reduced communication complexity", In: *Topics in Cryptology–CT-RSA*, Springer Berlin Heidelberg, pp.259-276, 2013.

[7] H. Sengar, R. Dantu, and D. Wijesekera, "Securing VoIP and PSTN from integrated signaling network vulnerabilities", In*: Proc. of the first IEEE Workshop on VoIP Management and Security*, Vancouver, BC, Canada, Canada, pp.1-7, 2006.

[8] T.J. Walsh and D.R. Kuhn, "Challenges in securing voice over IP", *IEEE Security & Privacy*, Vol.3, pp.44-49, 2005.

[9] D. Sisalem, J. Kuthan, and S. Ehlert, "Denial of service attacks targeting a SIP VoIP

infrastructure: attack scenarios and prevention mechanisms", *IEEE Network*, Vol.20, No.5, pp. 26-31, 2006.

[10] A. Talevski, E. Chang, and T. Dillon, "Secure and mobile VoIP", In: *Proc. of the International Conf. on Convergence Information Technology*, Gyeongju, South Korea, pp.2108-2113, 2007.

[11] B. Rong and Y. Qian, "An enhanced SIP proxy server for wireless VoIP in wireless mesh networks", *Communications Magazine*, Vol.46, No.1, pp.108-113, 2008.

[12] Y.S. Wu, V. Apte, S. Bagchi, S. Garg, and N. Singh, "Intrusion detection in voice over IP environments", *International Journal of Information Security*, Vol.8, No.3, pp.153-172, 2009.

[13] C.Y. Yeun and S.M. Al-Marzouqi, "Practical Implementations for Securing VoIP Enabled Mobile Devices", In: *Proc. of the Third International Conf. on Network and System Security* 2009, Gold Coast, Queensland, Australia, Australia , pp.409-414, 2009.

[14] L. Angrisani, M.D. Lelio, P.Morabito, R.S.L. Moriello, and M. Vadursi, "Security in VoIP systems: towards the design and implementation of a reconfigurable test bed for real-time measurements", In: *Proc. of the IEEE International Workshop on Measurements and Networking Proceedings*, Anacapri, Italy, pp.22-26, 2011.

[15] R. Pecori, "A PKI-free key agreement protocol for P2P VoIP applications", In: *Proc. of the IEEE International Conf. On Communications*, Ottawa, ON, Canada, pp.6748-6752, 2012.

[16] P.T. Sachin and S. Tamrakar, "VoIP and data storage in wireless GSM modem over MANET area", In: *Proc. of the International Conf. on Emerging Trends in Computing, Communication and Nanotechnology*, Tirunelveli, India, pp.31-36, 2013.

[17] Y.C. Chan and D.J. Lin, "The Design of an AP-Based Handoff Scheme for IEEE 802.11 WLANs", *International Journal of e-Education, e-Business, e-Management and e-Learning*, Vol.4, No.1, pp.72, 2014.

[18] M. Niswar, S. Kashihara, and S. Yamaguchi, "Vertical Handover Management for VoIP Session over Broadband Wireless Networks", *International Journal of Communications, Network and System Sciences*, Vol.6, No.6, pp.289, 2013.

[19] M. Dorigo and C. Blum, "Ant colony optimization theory: A survey", *Theoretical computer science*, Vol.344, No.2, pp.243-278, 2005.

[20] R. Pitakaso, C. Almeder, K.F. Doerner, and R.F. Hartl, "A MAX-MIN ant system for unconstrained multi-level lot-sizing problems", *Computers & operations research*, Vol.34, No.9, pp.2533-2552, 2007.

[21] J.C. Bermond, D. Coudert, G. D'Angelo and, F.Z. Moataz, "Finding disjoint paths in networks with star shared risk link groups", *Theoretical Computer Science*, Vol.579, pp.74-87, 2015.

[22] A. Dutta, S. Madhani, W. Chen, O. Altintas, and H. Schulzrinne, "Fast-handoff schemes for application layer mobility management", In: *Proc. of the 15th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, Barcelona, Spain ,Vol.3, pp.1527-1532, 2004.

[23] S. Salsano, L. Veltri, G. Martiniello, and A. Polidoro, "Seamless vertical handover of VoIP calls based on SIP Session Border Controllers", In: *Prof. of the IEEE International Conf. on Communications*, Vol.5, pp.2040-2047, 2006.

[24] P.C. Ng, S.C. Liew, and C. Lin, "Voice over wireless LAN via IIEE 802.16 wireless MAN and IEEE 802.11 wireless distribution system", In: *Proc. of the International Conf. on Wireless Networks, Communications and Mobile Computing*, Maui, HI, USA ,Vol.1, pp.504-509, 2005.

[25] H. Kazemitabar, S. Ahmed, K. Nisar, A.B. Said and H.B. Hasbullah, "A survey on voice over IP over wireless LANS", *World Academy of Science, Engineering and Technology*, Vol.71, pp.352-358, 2010.

[26] A.M. Amin, "VoIP Performance measurement using QoS parameters", In: *Proc. of the Second International Conf. on Innovations in Information Technology*, pp.1-10, 2005.

[27] M. Habib and N. Bulusu, "Improving QoS of VoIP over WLAN (IQ-VW)", Project Research Paper, for CS522 Computer Communications, University of Colorado at Colorado Springs, 2002.

[28] C. Lin, X. Yang, S. Xuemin, and W.M. Jon. "VoIP over WLAN: Voice capacity, admission control QoS, and MAC", *International Journal of Communication Systems*, Vol.19, No.4, pp.491-508, 2006.

[29] J. Liu, and Z. Niu, "An adaptive receiver buffer adjust algorithm for VoIP applications considering voice characters", In*: Proc. of the 5th International Symposium on Communications, Multi-Dimensional Mobile Communications*, Vol.2, pp.597-601, 2004.

[30] K.M. McNeill, M. Liu, and J.J. Rodriguez, "An Adaptive Jitter Buffer Play Out Scheme to Improve VoIP Quality in Wireless Networks", In: *Proc. of the IEEE Conf. on BAE Systems Network Enabled Solutions*, Washington, 1-5, 2006.

[31] S. Karapantazis, and F.P. Stylianos, "VoIP: A comprehensive survey on a promising technology", *Computer Networks*. Vol.53, pp.2050-2090, 2009.

[32] ITU-T Rec. P.861, Objective quality measurement of telephone-band (300-3400 Hz) speech codecs, 1998.

[33] F. De Rango, M. Tropea, P. Fazio, and S. Marano, "Overview on VoIP: Subjective and objective measurement methods", *International Journal of Computer Science and Network Security*, Vol.6, No.1, pp.140-153, 2006.

[34] L. Sun, and E. Ifeachor, "Voice quality prediction models and their application in VoIP networks", *IEEE Transactions on Multimedia*, Vol.8, No.4, pp.809–820, 2006.

[35] M. Backes, A. Kate, and A. Patra, "Computational verifiable secret sharing revisited", *In Advances in Cryptology–ASIACRYPT*, Springer Berlin Heidelberg, pp.590-609, 2011.

[36] A. Patra, A. Choudhary, T. Rabin, and C. Pandu Rangan, "The round complexity of verifiable secret sharing revisited", *In Advances in Cryptology*, pp.487–504, 2009.

[37] ITU-T (2008) G.711.1 : Wideband embedded extension for G.711 pulse code modulation Retrieved on 2009-06-19

[38] R.K. Jha, I.Z. Bholebawa, U.D. Dalal, and A.V. Wankhede, "Detection and fortification analysis of WIMAX network: With misbehavior node attack", *International Journal of Communications, Network and System Sciences*, Vol.5, No.6, pp.353-367, 2012.

[39] M. Niswar, S. Kashihara, K. Tsukamoto, Y. Kadobayashi, and S. Yamaguchi, "Handover management for VoWLAN based on estimation of AP queue length and frame retries", *IEICE Transactions on Information and Systems*, Vol.92, No.10, pp.1847-1856, 2009.

[40] S. Kashihara, and Y. Oie, "Handover Management Based on the Number of Data Frame Retransmissions for VoWLAN", *Elsevier Computer Communications*, Vol.30, No.17, pp.3257-3269, 2007.

[41] R.Shankar and Dr.E.Karthikeyan, "A VoIP security assessment using verifiable secret sharing", *Indian Journal of Engineering*, Vol.12, No.30, pp. 326-334, 2015.