Impact Factor Value 4.046 **e-ISSN: 2456-3463**
National Conference on **"Emerging Trends In Engineering & Technology"**
Organized by **Manoharbhai PatelInstitute Of Engineering& Technology Shahpur, Bhandara**
International Journal of Innovations in Engineering and Science, Vol. 4, No.5, 2019
www.ijies.net

An Approach to Efficient Communication over VoIP

Ms. Shraddha Agnihotri, Ms. Bawneet Kaur Plaha, Ms. Devyani Nikhare

[1]AssitantProfessor, [2-3]Students
Dept. of Computer Engineering, M.I.E.T, Shahpur, BHANDARA-441904

Abstact-*Now a days ,Information and Communication technologies plays an important role in communication over the Internet. Voice over Internet protocol (VoIP) is a new way of communicating. It is a technology that allows users to make calls over an IP network. This paper will describe Voice over Internet Protocol (VoIP) to a level that allows business concerns of implementing VoIP, components of a VoIP system. Internet is one of the most important communications intermediate in the world .Recently, VoIP (Voice over Internet Protocol) is also a popularly increased communications technology which recently having an exponential evolution of usage Internet .Existing solutions used several techniques such as Hybrid network ,Peer- to-Peer network to provide decent QoSas well as Privacy. But, some vulnerability occurs between Security and QoS. To overcome these issues propose novel Client-Server Network in which AES algorithm used for encryption /decryption process. Also, SHA-1 will used to provide authentication mechanism to the users of proposed system. Proposed system will give better results over the existing system.*

Keywords—*VoIP, Authentication, AES,QoS, SHA-1,TCP/IP.*

I- INTRODUCTION

Today, one of the most dominant technology in the communication world is Voice Over Internet Protocol (VoIP).It is the easiest way to make a call through internet by sending packets through packet switched based network. Recently, Internet provide slot of various applications with the help of that we can interconnect with each other through Internet Protocol (IP).Voice over Internet Protocol (VoIP) is one of the applications of Internet which allows people to make phone calls through the Internet instead of using the Traditional Public Switched Telephone Network (PSTN). VoIP is an internet telephony which deals extensive range of benefits to talk with each other freely at low rates which Permits for the calls ,long distance, local and international over the Internet. VoIP can accomplish a greater efficiency since the data packets in the network are engaged to their destination by diverse outstand sharing the same facilities extreme incompetently. VoIP are lower in cost since IP systems will offer amore cost-effective means for providing communication connections which is one of the sources of concern. VoIP technology converts the analog telephone communication signals into digital communication signals and transfersthroughtheInternettothedestinationwhereitagain converted back from digital to analog sound which can be overheard using speakers or headphone [3]. Voice over Internet Protocol (VoIP) is a form of communication that allows you to make phone calls over a broadband internet connection. Basic VoIP access usually allows you to call others who are also receiving calls over the internet. Interconnected VoIP services also allow you to make and receive calls to and from traditional landline numbers, usually for a service fee [6]. The problem of security is also major in VoIP. Thus, the user does not get a good guarantee from the VoIP service provider. There fore major aim of VoIP application is to achieve quality of service (QoS) and the security of network. Generally, unify network used

in VoIP to provide good security for high latency communication by routing network traffic through a number of nodes with random routes and random delay but it exist tradeoff between anonymity level and performance efficiency of Quality of services. No de or link failures occur due to software error or hardware. Ideally ,the routing system discovers link failures. Then, routing system reconfigures routing tables to send the packet to some other alternative path. The traffic is also avoided through failed link. Re configuration of routing table takes more time in a network. Therefore, network becomes unbalanced. Secure Hash Algorithm (SHA) is used to generate hash code of the string which is provided in input. SHA-1 produces a message digest based on principles similar to those used by Ronald L. Rivets of MIT in the design of the MD4 and MD5message digest algorithms, but has a more conservative design. SHA-1 differs from SHA-0 only by a single bitwise rotation in the message schedule of its compression function; this was done, according to the NSA, to correct a flaw in the original algorithm which reduced its cryptographic security. SHA-1 forms part of several widely used security applications and protocols [7].

II. RELATED WORK

Several techniques have been proposed for improving the performance of real-time applications while on communication. However, only a few techniques focused on mitigating the delay of MANETs. Since, from source to destination end, the packets must be handled carefully. Some of the literatures are discussed in the following section with respect to VoIP delay.

Wireless LAN (WLAN) is the essentially organized wireless technologies all over the world. The architecture of WLAN is the same as Local Area Network (LAN) except that the transmission happens via Infrared(IR) or radio frequency (RF) and not through physical wires. The main characteristics of the WLAN technologies are scalability, mobility ,simplicity and cost effectiveness. WLAN delivers connections to the IP networks and VoIP applications are already running over Internet Protocol(IP) networks. Subsequently, the setwonew technologies are fused to incorporate VoIP over WLANs (Vo WLAN).[2].

Khushboo et al., [8] compared the AODV, OLSR and TORA routing protocols, and its performances about voice services in MANET environment. For this, they used the OPNET simulator to identify the QoS factors of those protocols. Calduwel et al., [9] proposed a new technique for increasing the admission of real-time users and along with that packet per second also increased. In order to achieve this, they used Analytic Hierarchy Process (AHP) which arranges the available users in an alphabetical order. It ultimately enhances the Quality of Service (QoS) in Mobile Networks.

Mohamed et al., [10] analyzed the performance of voice codec's in WiMAX networks and proved that G.723 offers richer services than the other codecs in terms of delay and throughput along with the speech quality. It is estimated using Mean Opinion Score (MOS) method. OPNET simulator was used here for analyzing the results.

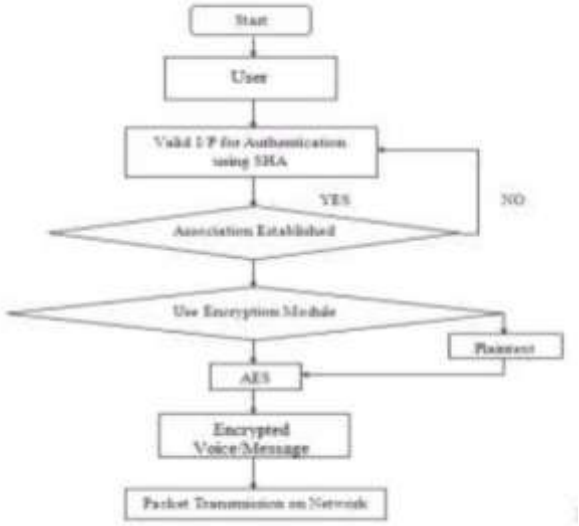
VoIP uses the two main protocols i.e. Route Setup Protocol and Real-Time Transport Protocol(RTP). Firstly, route setup proto coils use for call setup and termination. Besides ,real-time transport protocol isuse for media delivery. In order to satisfy QoS requirement, VoIP uses a route set up protocol which is support to sets up the shortest route from a caller srctoareceiverdst in peer-to-peer network. Also ,RTP support to carry voice traffic among caller and receiver along an established bidirectional voice circuit [

+d Server. Thus, more chances to vulner able network due to any node acts like malicious node. Therefore, this network is vulnerable with respect to privacy. Authentication is necessary in any service-oriented networks to identify and reject any unauthorized network access. Authentication protocol such as IEEE802.11iand802.11s requires centralized authentication server. Centralized server acts as third party [9].

IncomparativestudyrelatedtoAES,DESandRC4.AESi s more effective thanDESandRC4intermsofPacket loss, DelayandThroughput.VOIPtechnology convertstheanalog signalsinto digitalsignals.So,that AES can easily and rapidly encryptandde crypt this signal. Remaining two techniques will not give good performance as compare to AES.[10].

The SHA-1 algorithm accepts as input a message with a maximum length of 264 -1 and produces a 160-

bit message digest as output. The message is processed by the compression function in 512-bit block. Each block is divided further into sixteen 32-bit words denoted by Mt for t = 0, 1, ... , 15. The compression function consists of four rounds; each round is made up of a sequence of twenty steps. A complete SHA-1 round consists of eighty steps where a block length of 512 bits is used together with a 160-bit chaining variable to finally produce a 160-bit hash value[11].



Authentication is the important is phenomenon in any service associated network which respites to distinguish and remove any dishonest network accessory. So that first of all execute authentication process, in which VoIP client want to connect with server. Therefore, it provides server IP as well as its own ID to the server. If this information is correct then server again asks to the client for its password. Then client send its password. And if the client's password is correct then server provides association with it. If the sending information by client is incorrect then server again requires correct information from the client side. Until providing correct information server doesn't provide association between them. This Authentication process is performed using Secure Hash Algorithm (SHA-1) algorithm. After getting association communication will be start and this communication is encrypted using Advanced Encryption Standard (AES) algorithm. AES is a symmetric key algorithm which provides highest security to the data. This conversational data is unbreakable. Finally, this conversational data is transmitted over the network using Transmission Control Protocol (TCP).Secure Hash Algorithm (SHA-1)is nothing but the cryptographic algorithm. It delivers authentication as well as data integrity. SHA-1 is a deterministic hash function approach that continues arbitrary length of input data or message and breeds a stationary size length message which is called as message digest or hash value of the original conversation message. This algorithm is works for a message of size < 2^{64} bits. And it creates a 160-bit (20 byte) output message.

AES is a symmetric key algorithm. Therefore it refers similar key for both encryption and decryption procedure. It operates on fixed size of data i.e. 128 bits. But, in AES key sizes are varying i.e. 128, 192 and 256 bit which is depends on how many rounds are cover under AES. The data is delivered through N stages for encryption. And these stages are shuffle as per the key size. Fort 10 stages key size is 128 bit. If the stages are 12 and 14 then key sizes are 192 and 256 separately. These all rounds or stages are administrated via four modifications i.e. SubByte, ShiftRows, MixColumn and AddRoundkey.

IV. CONCLUSION

Since, VoIP over Wireless LAN(WLAN)network faces voluminous challenges, due to the loose nature of wireless network and security issues .Besides, real time applications require noble Voice quality. Also appropriate balance between the QoSand Security to the data is the key to the successofanyVoIPdeployment.AES algorithm enables voice to be transmitted in encrypted form to ensure the secure transmission and SHA-1 helps to strengthen the authentication mechanism. Further this work can be extended for multiple users are connected with server and they want to secure communication with each other.

REFERENCES

[1] *M.V.Sreeraj,T.SatyaSavitri,"SCTPandFEC basedLoss Recovery Technique for VoIP," International Journal of Innovative Research in Electrical,Electronics,InstrumentationandControlEngineeringVol.2,Issue1,January2014.*

[2] *Haniyeh Kazemitabar, Sameha Ahmed, Kashif Nisar, Abas B Said and Halabi B Hasbullah, "A comprehensive review on VoIP over Wireless LAN*

networks," 2009-2012 All rights reserved. ISSR Journal 2010.

[3] *Mrs. K. Maheswari, Dr. M. Punithavalli, "Receiver Based Packet Loss Replacement Technique for High Quality VoIP Streams," 978-1-4244-5612-3/09/$26.00, 2009 IEEE.*

[4] *Preetinder Singh and Ravneet Kaur, "VOIP Over Wimax: A Comprehensive Review," International Journal of Computer Science and Information Technologies, Vol. 5 (4), 2014, 5533-5535.*

[5] *Haniyeh Kazemitabar, Sameha Ahmed, Kashif Nisar, Abas B Said and Halabi B Hasbullah, "A comprehensive review on VoIP over Wireless LAN networks," 2009-2012 All rights reserved. ISSR Journal 2010.*

[6] *Rahul Singh , Ritu Chauhan," A Review Paper: Voice over Internet Protocol", International Journal of Enhanced Research in Management & Computer Applications, pp:15-23, ISSN: 2319-7471 Vol. 3 Issue 1 , , January-2014.*

[7] *Priyanka Vadhera , Bhumika Lall," Review Paper on Secure Hashing Algorithm and Its Variants", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064),pp no.629-632.*

[8] *Khushboo Mittal and Preeti Sharma, "Performance Evaluation of MANET Routing Protocols for VOIP Applications", International Journal of Science, Engineering and Technology Research,Vol.4,Issue 6,2015,pp.1977-1981.*

[9] *P. Calduwel Newton and K.Ramkumar, Taca: Throughput Aware Call Admission Control Algorithm for VoIP Users in Mobile Networks, proceedings of 2016 International Conference on Computer, Communication & Computational Sciences, Springer Ajmer, Rajastan, India, pp.116-121.*

[10] *M.A. Mohamed, F.W. Zaki and A.M. Elfeki, "Performance Analysis of VoIP Codecs over WiMAX Networks", International Journal of Computer Science Issues, Vol. 9, Issue 6, No.3, 2012, pp. 253-259.*

[11] *X. &. L. G. Chan, Discussion of One Improved Hash Algorithm Based on MD5 and SHA1, San Francisco, USA: World Congress on Engineering and Computer Science (WCECS), 2007.*