TECH-CHRONICLE
AN INTERNATIONAL E-JOURNAL ON
EMERGING TRENDS IN SCIENCE, TECHNOLOGY AND MANAGEMENT

Preserving Anonymity and Quality of service For VoIP Applications over Hybrid Networks

Priyanka Kanoje
PG student
Department of Information Technology,
Tulsiramji Gaikwad-Patil College of Engg. & Tech.,
Nagpur, Maharashtra, India
priyanka.kanoje65@gmail.com

Mukul Pande
Assistant Professor
Department of Information Technology,
Tulsiramji Gaikwad-Patil College of Engg. & Tech.,
Nagpur, Maharashtra, India
Mukulpande2002@gmail.com

Abstract— Now a days, Information and Communication technology plays vital role to communicate over the Internet. Internet is one of the most important communications intermediate in the world. Mostly, PSTN (Public Switch Telephone Network) is used for communication but PSTN is not well suited for real time multimedia applications. Recently, VoIP (Voice over Internet Protocol) is also a popularly increased communications technology which recently having an exponential evolution of usage Internet. In this VoIP is focused on Wireless LAN (WLAN) network for real time multimedia application. But, VoIP over WLAN faces many challenges, due to the loose nature of wireless network. In addition, to maintain QoS, Security are the key concern in VoIP network. Existing solutions used several techniques such as Hybrid network, Peer-to-Peer network to provide decent QoS as 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, network is based on SCTP protocol which is responsible for reliable and secure packet transmission over Internet. So, by using novel network analyzes the performance of QoS and Security concerns in VoIP.

Keywords— ***VoIP, Authentication, Security, QoS, jitter, throughput, delay,*** SHA.

I. INTRODUCTION

Recently, Internet provides lot 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 routes and sharing the same facilities extreme incompetently. VoIP are lower in cost since IP systems will offer a more 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 transfers through the Internet to the destination where it again converted back from digital to analog sound which can be overheard using speakers or headphone [3] [16]. But, the sound quality is not good in VoIP as compare to a conventional telephone. Also the problem of security is also major in VoIP. Thus, the user does not get a good guarantee from the VoIP service provider. Therefore 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.

Node 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. Reconfiguration of routing table takes more time in a network. Therefore, network becomes unbalanced. This unbalancing situation can be avoided through multipath dispersion [5]. Also, low latency applications on unify networks may be vulnerable to timing analysis attacks. Because, timing analysis attack reveal the identity of client.

Authentication is also essential in any service-oriented communication networks to identify and reject any unauthorized network access [11] [6]. The use of VoIP has made it much easier to achieve anonymity in voice

communications, especially when VoIP calls are made between computers. This is because VoIP calls between peer computers have no phone numbers associated with them, and they could easily be protected by end to end encryption and routed through low latency secure networks [16]. The encryption must be as fast as possible for proper streaming. If before successful encryption of one block, the next block arrives there are possibilities of loss of packets over the network which might make the voice content invalid or not understand [12].

II. LITERATURE REVIEW

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 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, these two new technologies are fused to incorporate VoIP over WLANs (VoWLAN).

VoIP is the technology used to transmit voice conversations over a data network using IP. VoIP access frequently permits you to call others who are also receiving calls over the Internet. VoIP offers reasonable long distance and international calling. Also, it is cheaper for end-users to make an Internet telephone call than a circuit-switched call. The major issues in VoIP are Security and preserve Quality of Services (QoS). Commonly, Hybrid Environment is used for providing security in VoIP. Therefore, Pr2P2PSIP is used as a hybrid networks [1]. So that, unify networks is suitable for provide good anonymity for high latency communications by routing network traffic over a number of nodes with random routes and random delay. But, it does not provide QoS. Also, user playing a role of routers in Pr2P2PSIP network which breaks the concept of dividing works on the different components of the network and complicates the design of system. Besides, low latency applications on unify networks may be vulnerable to timing analysis attacks.

A. Timing Analysis Attacks

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. Timing analysis attacks exclusively focus on the execution times of different stages in the route set up protocol. When this protocol meets QoS requirement due to setting up shortest path, it is vulnerable and reveal the identity of the caller. Therefore, different phenomenon likes K-Anonymity Algorithm (anonymity aware route set up protocol (AARSP).).

K-anonymity algorithm is used for providing the anonymous network. Consequently the hackers could not recognize the stream of packets over the network. Let us consider the caller as source S and the receiver as a destination R. The voice packets want to exchange through the personal network. This personal network consists of proxy nodes. The hacker can hack the voice simply from the proxy node which is present next to the caller or at the proxy node which is existent before the destination R. At this stage, the k-anonymity algorithm which will support to hide the proxy nodes which is next to the caller and which is present earlier the receiver. Random Walk Search Algorithm are also used. The random walk algorithm is not vulnerable to shortest path which is based on timing analysis attacks. Mostly, a random walk algorithm does not essentially navigate the shortest path between any two nodes. [11] [9] [3] [4].

B. Authentication

VoIP uses the two main protocols i.e. Route Setup Protocol and Real-Time Transport Protocol (RTP). Firstly, route setup protocol is use for call setup and termination. Besides, real-time transport protocol is use for media delivery. In order to satisfy QoS requirement, VoIP uses a route setup protocol which is support to sets up the shortest route from a caller src to a receiver dst in peer-to-peer network. Also, RTP support to carry voice traffic among caller and receiver along an established bidirectional voice circuit [9].

Similarly, in peer-to-peer network each node acts as a Client and Server. Thus, more chances to vulnerable 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 IEEE 802.11i and 802.11s requires centralized authentication server. Centralized server acts as third party [6]. Multi-hope routing between Authentication server and access point in wireless network would result in low reliability, long delay and thus potential service interruption is occurs.

Also, center server obstructs distributed operations and thus affects scalability. Therefore, to overcome this problem Ticket-based authentication protocols is implemented using Kerberos and a Kerberos-assisted authentication scheme. This does not required centralized server and specially used in Wireless Mesh Network (WMN) [6].

C. Transmission Technology of VoIP

In comparative study related to AES, DES and RC4. AES is more effective than DES and RC4 in terms of Packet loss, Delay and Throughput. VOIP technology converts the analog signals into digital signals. So, that AES can easily and rapidly encrypt and decrypt this signal [3] [1].

Remaining two techniques will not give good performance as compare to AES. Also, the caller's voice is digitized and this digitized voice is compressed and then separated into packets. The streaming of audio content over the

Internet is a challenging task for real time media transmission [10]. A Stream Control Transmission Protocol (SCTP) is suitable for transmission of real time data.

III. PROPOSE WORK

Since, Internet is diffident and it is underlying network for VoIP, some threats and risks inherited from the loosely network to VoIP. The limitation given in existing system, propose system implements Client–Server Network.

In this, SCTP protocol intended to make it easier to accomplish connections over a wireless network and to manage the transmission of multimedia data [12]. It supports multihoming in which connected endpoint can have alternate IP addresses linked with it in order to fluctuating condition or route around network failure. SCTP endpoints swap IP addresses during initiation of the transmission [13] [5].

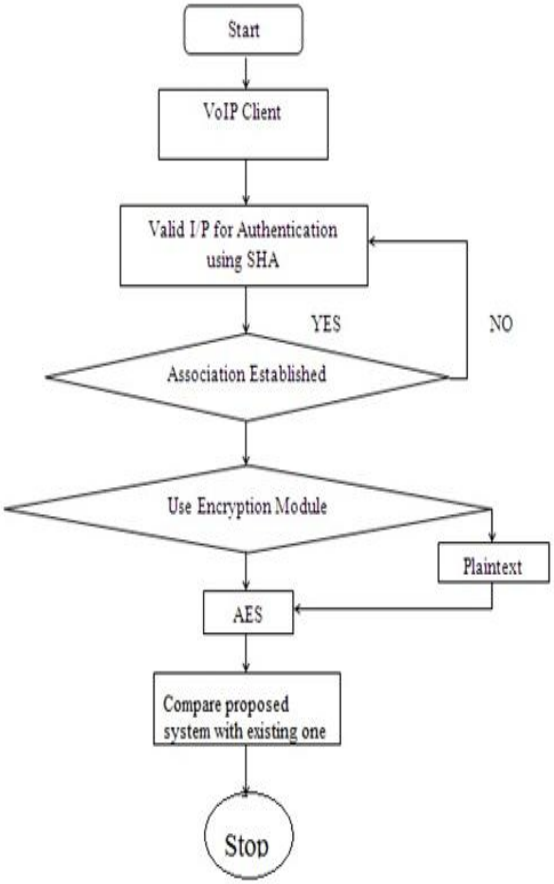

Figure: Flow of proposed work

A single port number is used through the entire address list at an endpoint for a specific session. Also, Authentication will provide to the reject any unauthorized network access. Besides, AES algorithm will use to encrypt and decrypt transmitting data over the internet.

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 QoS and Security to the data is the key to the success of any VoIP deployment. Several techniques used to improve the performance of Voice quality as well as Security issues in VoIP. But, some vulnerability occurs to make proper balance between QoS and Security. Therefore, to remove these issues proposed Client-Server Network in which AES and SCTP protocols will great deal for improving QoS and Security in VoIP. The permutation of these two protocols will help to remove tradeoffs between QoS and Security in VoIP. Using this propose network will improve the performance of VoIP system.

REFERENCES

[1] Zahraa Sabra and Hassan Artail, "Preserving Anonymity and Quality of Service for VoIP Applications over Hybrid Networks," 17th IEEEMediterranean Electrotechnical Conference, Beirut, Lebanon, 13-16 April 2014.

[2] M.V.Sreeraj, T. Satya Savitri, "SCTP and FEC based Loss Recovery Technique for VoIP," International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering Vol. 2, Issue 1, January 2014.

[3] Abdi Wahab, Rizal Broer Bahaweres, Mudrik Alaydrus, Muhaemin, Riyanarto Sarno, "Performance Analysis of VoIP Client with Integrated Encryption Module," 978-1-4673-2821-0/13/$31.00 ©2013 IEEE.

[4] K. Bharathkumar, R. Premalatha Kanikannan, Dr.Rajeswari Mukesh, M.

[5] Kasiselvi, T. Kumanan, "Privacy Preserving of VoIP against Peer-to-Peer Network Attacks and Defense," International Journal of Computer Network and Security (IJCNS) Vol 4. No 1. Jan-Mar 2012 ISSN: 0975-8283.

[6] J. Faritha Banu, V.Ramchandran, "Efficient Bandwidth Estimation Management for VoIP Concurrent Multipath Transfer," International Journal of Internet Computing ISSN No: 2231-6965, VOL-1, ISS-3 2012.

[7] Celia Li and Uyen Trang Nguyen, "Fast- Authentication for Mobile Clients in Wireless Mesh Networks," 978-1-4244-5377-1/10/$26.00 ©2010 IEEE.

[8] Prithula Dhungel, Moritz Steiner ,Ivica Rimac, Volker Hilt, Keith W. Ross, "Waiting for Anonymity:Understanding Delays in the Tor Overlay," IEEE Communications Society subject matter experts for publication in the IEEE P2P 2010 proceedings.

[9] Xiaoliang Wang, Xingming Sun, Guang Sun, Dong Luo, "CST: P2P Anonymous Authentication System based on Collaboration Signature," 978-1-4244-6949-9/10/$26.00 ©2010 IEEE.

[10] Mudhakar Srivatsa, Arun Iyengar, Ling Liu and Hongbo Jiang, "Privacy in VoIP Networks:Flow Analysis Attacks and Defense," IEEE INFOCOM 2009.

[11] 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.

[12] Mudhakar Srivatsa, Ling Liu and Arun Iyengar, "Preserving Caller Anonymity in Voice-over-IP Networks," 978-0-7695-3168-7 /08 $25.00 ©2008 IEEE.

[13] Subashri .T, Sivaram L, Arunprasad .S, Deepak Ranjan .S, VaidehiV,"Reduction in Computational Complexity of a Fast Encryption Algorithm for Application in Voice Oriented System," IEEE-International Conference on Signal processing, Communications

and Networking Madras Institute of Technology, Anna University Chennai India, Jan 4-6, 2008. Pp97-101.

[14] Wei-Cheng Wang, Chih-Hung Hsu, Yung-Mu Chen, and Tein-Yaw Chung, "SCTP-based Handover for VoIP over IEEE802.11 WLAN Using Device Virtualization," ISBN 978-89-5519-131-8 93560 - 1073 - Feb. 12-14, 2007 ICACT 2007.

[15] Jian Wang, Changyong Niu and Ruimin Shen, "Bus-based Anonymous Multicast in Peer-to-Peer Overlay," 2007 IFIP International Conference on Network and Parallel Computing Workshops.

[16] Ginger Perng, Michael K. Reiter and Chenxi Wang, "M2: Multicasting Mixes for Efficient and Anonymous Communication," Proceedings of the 26th IEEE International Conference on Distributed Computing Systems (ICDCS'06)2006.

[17] Xinyuan Wang, Shiping Chen, Sushil Jajodia, "Tracking Anonymous Peer-to-Peer VoIP Calls on the Internet," CCS'05, November 7–11, 2005, Alexandra,Virginia,USA.