IJSAA International Journal of Systems , Algorithms & Applications

Network Factors and Security of VoIP Traffic in 802.11 WLAN

[1]Raju Lakkars, [2]Nisar Ahmed
[1]Assistant Professor,
[1]Department of Computer Science, [2]Department of Computer Networks and Communication
[1]Vaagdevi College of Engineering, Warangal, India
[2]College of Computer Science, King Khalid University, ABHA, KSA
e-mail: raju_01it@yahoo.co.in[1], nahmaad@kku.edu.sa[2]

***Abstract* - The convergence of land-line, wireless, and Internet communications has stimulated the development of new applications and services which have revolutionized communications in the recent technological advancement era. VoIP refers to the transmission of telephone conversations over a packet-switched IP network. . The interconnection between PSTN (Public Switch Telephone Network) and IP (Internet Protocol) networks is referred to as the Next Generation Network (NGN). The security and reliability of VoIP communications are an important requirement for commercial organizations in many sectors, including financial, pharmaceutical, insurance, and energy. We discuss about the network factors such as delay, jitter and packet loss and security concerns in the implementation of VoIP traffic in 802.11 WLAN. The simulation results are obtained from ns-2 simulator.**

Keywords: *VoIP, Delay, Jitter, Packet loss, Security, SIP, 802.11 WLAN*

I. INTRODUCTION

The idea of VoIP, or voice over the Internet or IP telephony, has been discussed since at least the early 1970s when the idea and technology were developed.

The transition from legacy Public Switched Telephone Network (PSTN) into communications using IP-based networks has sparked the development of real-time multimedia applications with many sophisticated features at a lower cost. VoIP is one of the applications that provide global interconnectivity at a low cost.

Voice over IP – the transmission of voice over packet-switched IP networks – is one of the most important emerging trends in telecommunications.

Voice over Internet Protocol technology offers the opportunity to use or return the voice to distance learning in synchronous and asynchronous communication forms, which allows instructors and students greater social presence. Voice over Internet Protocol technology provides cost-effective telephone -based conversations in the learning environment. Voice over Internet Protocol technology increases the simplicity and accessibility of the distance learning

Quality of Service (QoS) is fundamental to the operation of a VOIP network that meets users' quality expectations. However, the implementation of various security measures can cause a marked deterioration in QoS.

As the integration of voice and data takes place in a single network, establishing a secure VoIP and data network is a complex process that requires greater effort than that required for data-only networks. The general guidelines are

1. Develop appropriate network architecture.
2. Ensure that the organization has examined and can acceptably manage and mitigate the risks to their information, system operations, and continuity of essential operations when deploying VoIP systems.
3. Special consideration should be given to E-911 emergency services communications, because E-911 automatic location service is not available with VoIP in some cases.
4. Agencies should be aware that physical controls are especially important in a VoIP environment and deploy them accordingly.
5. Evaluate costs for additional power backup systems that may be required to ensure continued operation during power outages.
6. VoIP-ready firewalls and other appropriate protection mechanisms should be employed. Agencies must enable, use, and routinely test the security features that are included in VoIP systems.
7. If practical, "softphone" systems, which implement VoIP using an ordinary PC with a headset and special software, should not be used where security or privacy are a concern.
8. If mobile units are to be integrated with the VoIP system, use products implementing WiFi Protected Access (WPA), rather than 802.11 Wired Equivalent Privacy (WEP).
9. Carefully review statutory requirements regarding privacy and record retention with competent legal advisors.

II. OVERVIEW

VoIP environment consists of the concepts such as TDM DSN/PSTN . VoIP networks must perform all of the tasks that these systems perform in addition to performing data and signaling gateway functions between these systems and IP networks. VoIP components that must exist for the technology to function properly. The important components of VoIP are[15]

- The IP network
- Call processor/controllers
- Media/signaling gateways
- Subscriber terminal.

a) The IP Network

A network supporting VoIP technology can be viewed as one logical voice switch in distribute form (rather than a single switch frame) with the IP network providing connectivity to the distributed elements in the network. This IP infrastructure must ensure smooth delivery of voice and signaling packets to the VoIP elements. Due to their dissimilarities, the IP network must treat voice and data traffic differently, primarily because latency in voice transmission is more noticeable to the end user than latency in data transmission. If an IP network is to carry both voice and data traffic, it must be able to prioritize the different traffic types.

b) Call Processor/Controller

Call processor/controllers employ system software that sets up and monitors calls, maintains the dial plan, performs phone number translations, authorizes users, coordinates some or all of the call signaling, delivers basic telephony features, and may control the bandwidth utilization on each link. In addition, processor/controllers provide the signaling and control services that coordinate the media gateway functions. A call processor/controller can also be known as a soft switch, call agent, call manager, or gatekeeper depending on its specific function in the VoIP network or specific vendor implementation. The amount of functionality provided by a call processor/ controller is based on the particular VoIP product being deployed.

c) Media/Signaling Gateways
VoIP Gateways are responsible for interfacing IP network based voice communications with the traditional circuit-switched network. They provide call origination, detection, analog-to-digital conversion of voice, and creation of voice packets. In addition, media gateways may provide optional features, such as voice compression, echo cancellation, silence suppression, and statistics gathering. Gateways can exist in several physical forms including discrete device, a physical board or blade found in a dedicated telecommunications frame, or a common Personal Computer (PC) running VoIP software. The features and services provided by Media and Signaling Gateway's can span a wide spectrum.

A VoIP Gateway (or PSTN Gateway) is a device which converts telephony traffic into IP for transmission over a data network.

There are 2 ways:
1. To convert incoming PSTN/telephone lines to VoIP/SIP
In this manner the VoIP gateway allows calls to be received & placed on the regular telephony network. In many business cases, it is preferable to continue to use traditional phone lines because one can guarantee a higher call quality and availability.

2. To connect a traditional PBX/Phone system to the IP network
In this manner the VoIP gateway allows calls to be made via VoI. Calls can then are placed via a VoIP service provider, or in the case of a company with multiple offices, inter office calls costs can be reduced by routing the calls via the Internet. VoIP gateways are available as external units or as PCI cards. The vast majority of devices are external units. A VoIP gateway will have a connector for the IP network and one or more ports to connect the phone lines to it.

d) Subscriber Terminal
It may be an analog telephone or IP terminal.

e) Voice Data Processing in VoIP System
Figure 2 illustrates the basic flow of voice data in a VoIP system. Once the called party answers, voice must be transmitted by converting the voice into digitized form, then segmenting the voice signal into a stream of packets. The first step in this process is converting analog voice signals to digital, using an analog-digital converter. Since digitized voice requires a large number of bits, a compression algorithm can be used to reduce the volume of data to be transmitted. Next, voice samples are inserted into data packets to be carried on the Internet. The protocol for the voice packets is typically the Real-time Transport Protocol, RTP (RFC 3550). RTP packets have special header fields that hold data needed to correctly reassemble the packets into a voice signal on the other end. But voice packets will be carried as payload by UDP protocols that are also used for ordinary data transmission. In other words, the RTP packets are carried as data by the UDP datagram, which can then be processed by ordinary network nodes throughout the Internet. At the other end, the process is reversed: the packets are disassembled and put into the proper order, digitized voice data extracted from the packets and uncompressed, then the digitized voice is processed by a digital-to-analog converter to render it into analog signals for the called party's handset speaker.

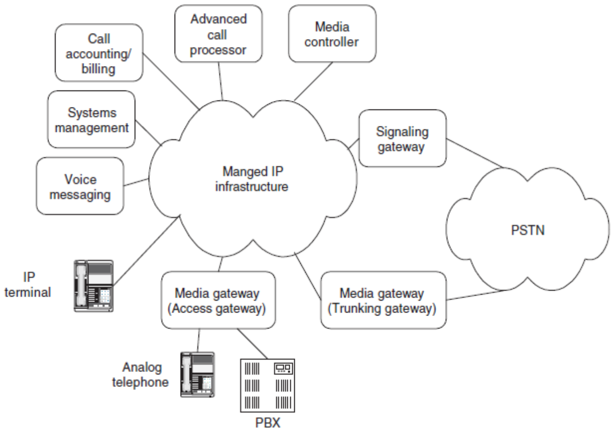

Fig.1. Components of VoIP

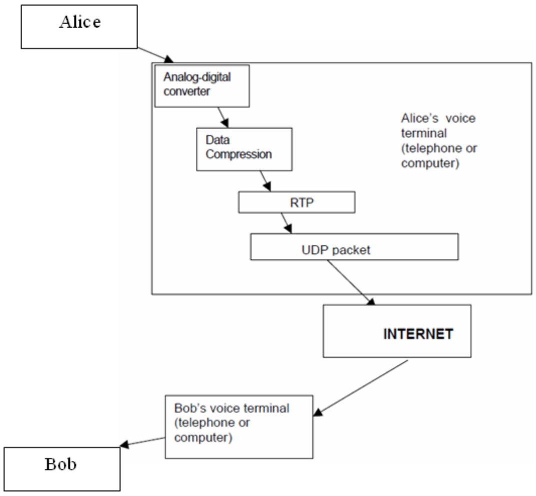
Alice
Analog-digital converter
Data Compression
Alice's voice terminal (telephone or computer)
RTP
UDP packet
INTERNET
Bob's voice terminal (telephone or computer)
Bob

Fig.2. Voice Data Processing in VoIP System

III. NETWORK FACTORS

There exists many network factors that affect the performance of VoIP. We discuss about three of them Delay, Jitter and Packet Loss. The four parameters of ITU-T P.59 are

1. *Talkspurt* : It represents the talking duration with either of the communicators
2. *Pause:* No voice communication
3. *Double Talk:* Both are sending their voices
4. *Mutual Silence:* Both are silent

a) Delay
Delay is caused when packets of data (voice) take more time than expected to reach their destination. This causes some disruption is the voice quality. Its affect can be minimized using the proper methodologies. The delayed packet may come late or may not come at all, in case it is lost. QoS (Quality of Service) considerations for voice are relatively tolerant towards packet loss, as compared to text. When a packet is delayed, we will hear the voice later than we should. If the delay is not big and is constant, our conversation can be acceptable.

VoIP *delay* or *latency* is characterized as the amount of time it takes for speech to exit the speaker's mouth and reach the listener's ear. Three types of delay are inherent in today's telephony networks propagation *delay*, *serialization delay*, *handling delay*. Propagation delay is caused by the length a signal must travel via light in fiber or electrical impulse in copper-based networks. Handling delay—also called processing delay—defines many different causes of delay (actual packetization, compression, and packet switching) and is caused by devices that forward the frame through the network. Serialization delay is the amount of time it takes to actually place a bit or byte onto an interface.

The end-to-end delay time is calculated as follows by the sum of the elapsed times on all of the nodes and links which the packets go through.

E2E Delay = Serialization Delay + Propagation Delay + Switching Delay.

The delay times except for the switching delay are the fixed values or directly (or inversely) proportional to the specific factors.

When packets are held in a queue because of congestion on an outbound interface, the result is *queuing delay*. Queuing delay occurs when more packets are sent out than the interface can handle at a given interval.

b) Jitter

Jitter is the variation of packet inter arrival time. Jitter is one issue that exists only in packet-based networks. . While in a packet voice environment, the sender is expected to reliably transmit voice packets at a regular interval (for example, send one frame every 20 ms). These voice packets can be delayed throughout the packet network and not arrive at that same regular interval at the receiving station (for example, they might not be received every 20 ms). The difference between when the packet is expected and when it is actually received is jitter. Mathematically it can be written as

Jitter = {Exact time required to reach the destination} – {Expected time required to reach the destination}

c) Packet Loss

Packet loss in data networks is both common and expected. When putting critical traffic on data networks, it is important to control the amount of packet loss in that network. When putting voice on data networks, it is important to build a network that can successfully transport voice in a reliable and timely manner. Also, it is helpful when you can use a mechanism to make the voice somewhat resistant to periodic packet loss.

Mathematically,
Packet Loss = {Number of packets sent at sender} – {Number of packets received at receiver}

IV. SECURITY OF VOIP TRAFFIC

The security process should be designed to incorporate controls that can address the following:

1. Identify applicable threats
2. Identify avenues of attack and minimize the opportunity for an attack
3. Minimize the impact of an attack if it occurs
4. Manage and mitigate a successful attack in a timely fashion

A fundamental element for a secure VoIP deployment is a well-defined architecture. The VoIP architecture should incorporate requirements for reliability, availability, confidentiality, authorization, and integrity. To support these objectives, we need to identify, prioritize, and categorize the types of data and information that are exchanged through the VoIP network (for example, secret, confidential, public).

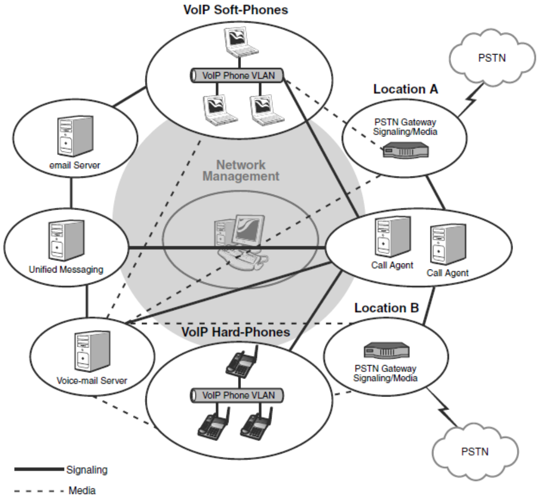

Fig.3. End to End Delay in Time Units

We propose to introduce the network segmentation and private addressing to cope with the security issues.

a) Network Segmentation

In this architecture, all the critical components are logically isolated. Traffic filtering can be enforced by the supporting network elements such as routers and switches or the use of VoIP firewalls or session border controllers (SBCs).

b) Private Addressing

Private addressing is used as another mechanism to protect against external attacks. The exponential growth of the Internet in the early 1990s signaled the rapid depletion of globally unique IP addresses. The IETF published RFC 1918 [16] in an effort to encourage organizations to use non routable IP addresses for systems that were not intended to be directly connected to the Internet. By configuring the internal hosts of an organization with one set of IP addresses and using only a small set of IP addresses to route Internet traffic, the depletion of Internet-routable IP addresses was decelerated. An internal host will send all its traffic through a component that is responsible for routing traffic to the Internet and also perform Network Address Translation (NAT).

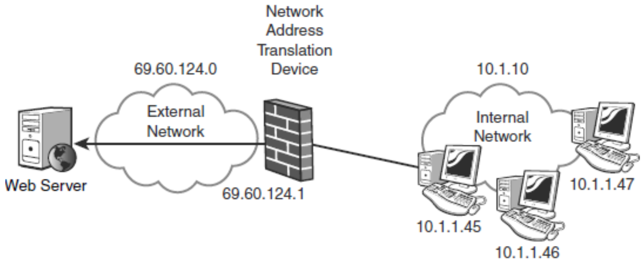

Fig.4. Private Addressing

The NAT device maintains a table that associates the IP address and ports of internal hosts with the IP address and ports of external hosts (source and destination). This option provides an added benefit to the security of the organization's internal network. Any external malicious traffic targeting internal systems is dropped unless the NAT has established an association in its state table. Therefore, it is encouraged to use private addressing in VoIP deployments to provide another layer of protection.

V. SIMULATION

We have used ns -2 simulator [1] for our analysis. The table # 1 represents the parameters as per G.711

Table # 1 parameters of G.711

Parameters	Value
Voice CODEC	64 kb/s
Packet size	160B
Packetization interval	20ms
Transport layer	UDP
PHY data rate	UDP
RTS/CTS	No

a) End to End Delay

The accuracy of using the delay distribution from a single node and applying convolution to find the end-to-end delay. Results obtained above, compare the theoretical end-to-end delay results with results from simulation and are shown in Fig 6

b) Queuing Delay

Figure 7 compares the waiting time distribution for a multiplex of traditional voice (on/off) source models and Data sources at a single buffer using FIFO scheduling. This is a result of a simulation in which both data and VoIP packets were 48 bytes long, and data traffic was not simulated as TCP traffic. These bursty sources are potentially the most difficult for networks to cope with.

Result in Fig.7 shows that data sources suffer greater delays in a multiplexed buffer because of their burstiness. In this paper we extend this experiment by observing a more realistic Internet data model, with packet sizes of 1000 bytes for data, while the on-off values remain constant.

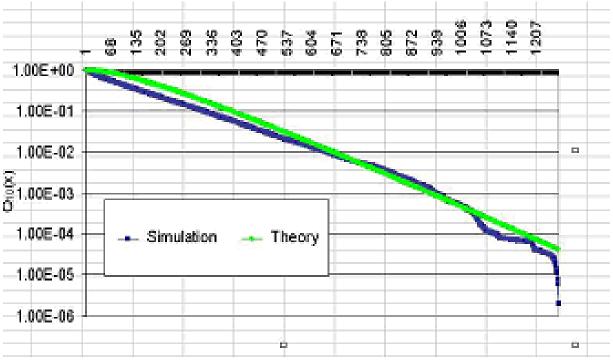

Fig.5. End to End Delay in Time Units

c) Jitter

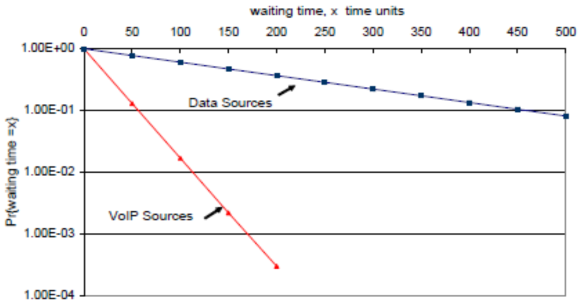

Fig.6. Queuing Delay

we will get the jitter of initial records is 0. This is because there is only CBR traffic flow, no other background traffic flow. After FTP flow starts, we can trace the data.

VI. CONCLUSION

The network factors obtained in the simulation are closely related to the theoretical values. . It is also observed that we need to reduce the switching delay. We also discussed about the theoretical concepts related to security and proposed the possible solutions. This research further can be extended to implement in respect to the security.

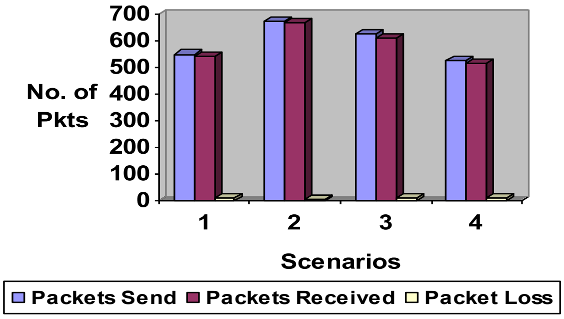

Fig.7. Packet Loss in various scenarios

REFERENCES

[1] NS – 2 for beginners.

[2] M. Veeraraghavan, N. Cocker, and T. Moors, “Support of Voice Services in IEEE 802.11 Wireless LANs,” Proc. IEEE INFOCOM, vol. 1, pp. 488-497, 2001.

[3] D. Chen, S. Garg, M. Kappes, and K.S. Trivedi, “Supporting VoIP Traffic in IEEE 802.11 WLAN with Enhanced Medium Access Control (MAC) for Quality of Service,” technical report, Avaya Labs Research, 2002.

[4] S. Garg and M. Kappes, “An Experimental Study of Throughput for UDP and VoIP Traffic in IEEE 802.11b Networks,” Proc. IEEE Wireless Comm. and Networking Conf. (WCNC ’03), vol. 3, pp. 1748- 1753, 2003.

[5] T. Kodama and Y. Katsube, “Voice Performance in WLAN Networks—An Experimental Study,” Proc. Global Telecomm. Conf. (GLOBECOM ’03), pp. 3504-3508, 2003.

[6] K. Medepalli, P. Gopalakrishnan, D. Famolari, and T. Kodama, “Voice Capacity of IEEE 802.11b, 802.11a and 802.11g Wireless LANs,” Proc. Global Telecomm. Conf. (GLOBECOM ’04), Nov. 2004.

[7] N.T. Dao, X. Wei, and R.A. Malaney, “The Voice Capacity of WiFi for Best Effort and Prioritized Traffic,” Proc. Auswireless Conf., Aug. 2006.

[8] T.J. Patel, V.A. Ogale, N.C.S. Baek, and R. Parkm, “Channel Capacity Estimation in VOIP Channels over Wireless Networks,” http://users.ece.utexas.edu/wireless/EE381K11_Spring03 projects/11.1.pdf, 2003.

[9] F. Anjum, M. Elaoud, D. Famolari, A. Ghosh, R. Vaidyanathan, A. Dutta, and P. Agrawa, “Voice Performance in WLAN Networks. An Experimental Study,” Proc. Global Telecomm. Conf. (GLOBECOM ’03), Dec. 2003.

[10] A. Lakas and M. Boulmalf, “Experimental Analysis of VoIP over Wireless Local Area Networks,” J. Comm., vol. 2, pp. 3-9, June 2007.

[11] I. Dangerfield, D. Malone, and D.J. Leith, “Experimental Evaluation of 802.11e EDCA for Enhanced Voice over WLAN Performance,” Proc. Int’l Symp. Modeling and Optimization in Mobile, AdHoc and Wireless Networks (WiOpt ’06), Apr. 2006.

[12] P. Brady, “A Model for Generating On-Off Speech Patterns in Two-Way Conversation,” Bell Systems Technical J., vol. 48, no. 7, pp. 2245-2272, Sept. 1969.

[13] IEEE Std. 802.11e, Wireless LAN Medium Access Control (MAC) and Physical (PHY) Specifications: Medium Access Control (MAC) Quality of Service Enhancements, IEEE, Nov. 2005.

[14] L. Cai, X.S. Shen, J.W. Mark, L. Cai, and Y. Xiao, “Voice Capacity Analysis of WLAN with Unbalanced Traffic,” Proc. Int’l Conf. Quality of Service in Heterogeneous Wired/Wireless Networks (QSHINE ’05), Aug. 2005.

[15] D. Hole and F. Tobagi, “Capacity of an IEEE 802.11b wireless LAN supporting VoIP,” in *In Proceedings of IEEE ICC*, 2004.

[16] The IETF published RFC 1918 , “Address Allocation for Private Internets”