International Journal of Engineering &Technology, 7 (4) (2018) 6373-6376

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET
doi: 10.14419/ijet.v7i4.15132
Research paper

Performance analysis on high -speed network for secure big data streaming of detecting VoIP calls

Rajinikanth E [1] *, Jayashri S [2]

[1] Research scholar, Sathyabama Institute of Science and Technology, Chennai, India
[2] Director, Adiparasakthi Engineering College, Melmaruvathur, India
**Corresponding author E-mail: rajinikanth4@gmail.com*

Abstract

In this fast growing world, Internet-based Call transferring facilities are most popular and all the telecommunication industries are showing more interest in developing interesting key features and providing better solutions to the users. The detection of transmission and monitoring voice data causes lots of security issues and results in lacking over users to use the VoIP messages instead, of voice calls without an internet. Although there are many VoIP detecting techniques, they are not accurate and not efficient. This can be resolved by using AES algorithm which helps to transfer media files from one end to another end securely. In this approach, Big Data schemes are handled because of media-oriented handlings. This entire system deals with successful and intelligent communication over Internet-based Voice Call transmission. Some of the parameters used are transmission bit rate, speed, packet size, and intervals. Intelligent Media Packet transfer scheme is used for network analysis and route establishment. The proposed system outperforms the graphical representation of throughput, delay, and packet transmission speed. The main objective of this system is to efficiently process high-speed real-time network traffic, which proves that our approach of Intelligent Media Transfer (IMT) outperforms the existing systems with the ability to work in real-time and high-speed Big Data environment.

Keywords: *Intelligent Media Transfer; OWD (One Way Delay); VoIP; WLAN.*

1. Introduction

Voice over internet protocol is a method to transfer voice and media over Internet protocol with the network such as the internet. The Signaling features of VoIP are signaling and media channel setup. Signaling is used to set up a connection in a telephone network. The quality of internet connection determines the quality of the calls. Call signaling includes authentication, authorization and communication security. Signaling protocol for call setup is Session Initiation Protocol (SIP).Media channel response is responsible for transmission between two communication parties and the protocol used is Real-Time Transport Protocol. VoIP is a Layer 3 network protocol that uses various Layer 2 point-to-point or link-layer protocols such as PPP, Frame Relay, or ATM for its transport. VoIP implementations may face problems with latency, packet loss, and jitter.

The security arrangement of VoIP is like any web associated gadget. This implies programmer who thinks about these VoIP uses can initiate dissent of-benefit assaults, gather client information, record discussions and bargain phone message messages. VoIP telephone benefit likewise won't work if there is control blackout and when the web association is down. The crisis focus will most likely be unable to decide your area in view of your virtual telephone number. Traded off VoIP client record or session qualifications may empower an assailant to cause generous charges from outsider administrations, for example, long-separation or worldwide phone calling.

In the literature, four types of VoIP detection techniques are provided namely port based, Signature-based, pattern-based, and statistical analysis based methods.[1] Big data is a term for massive data sets having large, more varied and complex structure with the difficulties of storing, analyzing and visualizing for further processes or results.[2] Flow level behavior is proposed to deduce VoIP using packet size and inter-arrival time.[3] More and more VoIP applications have emerged with the development of network and multimedia coding techniques. Their traffic identification is meaningful to for network management and application optimization. [4]Detecting VoIP calls either to block illegal commercial VoIP or prioritize the paid users VoIP calls.[5] Peer-to-peer (P2P) voice over IP (VoIP) applications (e.g. Skype or Google Talk) commonly use Web TCP ports (80 or 443) as a fallback mechanism to delude restrictive firewalls.[6]

Develop an analytical model of a full duplex MAC protocol for VoWLANs, and study its capacity.[7] MAC scheme for VoIP over WLANs referred to as PAMA (Prioritized Adaptive Multiple Access). [8] The average value of the jitter of the VoIP traffic traversing through the WiFi-WiMAX network was observed to be higher than that of utilizing WiFi alone at some points in time. [9] A comparison of data traffic scheduling techniques, which are Priority Queuing (PQ), First-In-First-Out (FIFO) and Weighted Fair Queuing (WFQ). [10] The average jitter of VoIP transiting the WiFi-UMTS network has been found to be lower than that of either solely through the WiFi and the UMTS networks. The existing system fails to meet the basic requirements to be efficient and independent. Also, they are not capable of providing a high-speed network at the real time [12]. The existing method Lacks in Security, Data Noise occurs or data loss occurs over communication and Data Size problems occurs.

2. Existing system

In past approaches lots of lacking such as failure in Internet-based VoIP calls, security issues and many more. One of the big challenges in VoIP calls detection is the advancement in communication technologies, which increases the amount and velocity of data generated over the internet. In 2008, the number of UK houses connected to the internet is increased to 65%. Also, in 2012, the number is reached to 80% and the amount of data generated by computers was recorded as 2.27 zeta bytes. Therefore, a system is needed that handles high velocity of data during monitoring and analysing network traffic in a real-time. Such enormous amount data at a high velocity at different variety is leading us toward the concept of Big Data. In the existing approach, the lacking have noticed that past statistical techniques fail to meet the basic requirements to be generic, efficient, and independent from VoIP application and protocols. Also, they are not capable of processing ultra-high- speed traffic at the real time.

3. Proposed system

In the proposed approach, we introduce a new mechanism to handle the above-quoted problems in past scenario, by means of Intelligent Media Transfer (IMT) Scheme. This mechanism is to efficiently process high-speed real-time network traffic and has an ability to work in real-time as well as high-speed Big Data environment. The proposed solution is generic, efficient and accurate by considering real-time scenarios and is able to detect encrypted as well as tunnelled VoIP. Furthermore, the proposed scheme is independent of any VoIP application protocol, security mechanisms, or tunnelling mechanism.

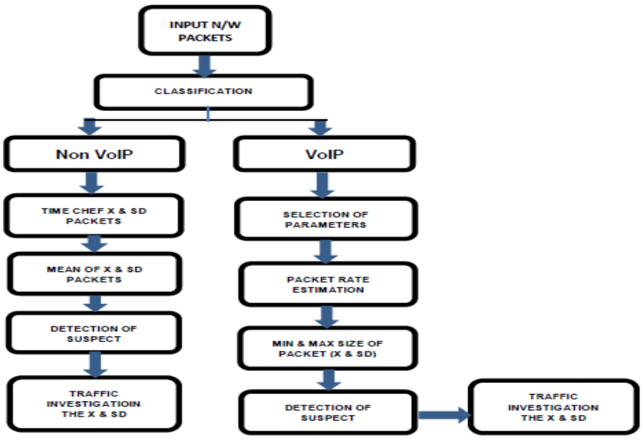

Fig. 1: Block Diagram of IMT.

Table 1: Input Parameters

PARAMETERS	DATA
Initial node energy level	10-50 packets
Node maximum energy level	51-100 packets
Average coverage range	30-250 m
Packet transmission speed	30-70 bps
Channel data rate(Threshold Value)	10-20Mbps
Packet Dropping Rate(Threshold Value)	10-20 bps
Average Transmission Delay(Time Interval)	5 – 10 s
Traffic agent type	CBR

CBR Traffic Creation:

```
set cbr [new Application/Traffic/CBR]
$cbr attach-agent $udp
$cbr set packetSize_ $pkt; #sub packet size
$cbr set interval_ $int
#Attach CBR Caller to sink;
$ns_ at 0.9 "VoIP_Flow_Detection $int 0 1"
```

After the underlying position data, the hubs are determined by their development goal and speed.

From that point onward, the underlying separation (bounce tallies) data are checked by a GOD. As of now, the god question is utilized just to store a variety of the briefest number of bounces required to reach from one hub to another. The god question does not compute this on the fly amid re-enactment runs since it can be very tedious. The data is stacked into the god protest from the development design document (this record).

At that point, the hubs will move amid this 900-second recreation situation. Amid this, the separation (jump tallies) data will change, hence, the accompanying lines will demonstrate this current change. Note that the separation is ascertained in light of an ostensible radio change as "250" meters. The god data ought not to be accessible to any of the hub. Subsequently, for a steering convention, it needs to find the separation without anyone else's input with some instrument.

It's conceivable that a hub achieves its goal before the reenactment clock closes. Along these lines, it needs to re-determine another heading and speed for it. Additionally, the normal delay time is a parameter to permit a hub stop to move toward a goal before moving once more. At last, there are a few measurements about this development record. Amid the recreation, a few hubs get segregated from every single other hub which comes about one check of "goal inaccessible". Likewise, all course changes and connection changes are computed.

4. Simulation analysis

4.1. Bandwidth analysis

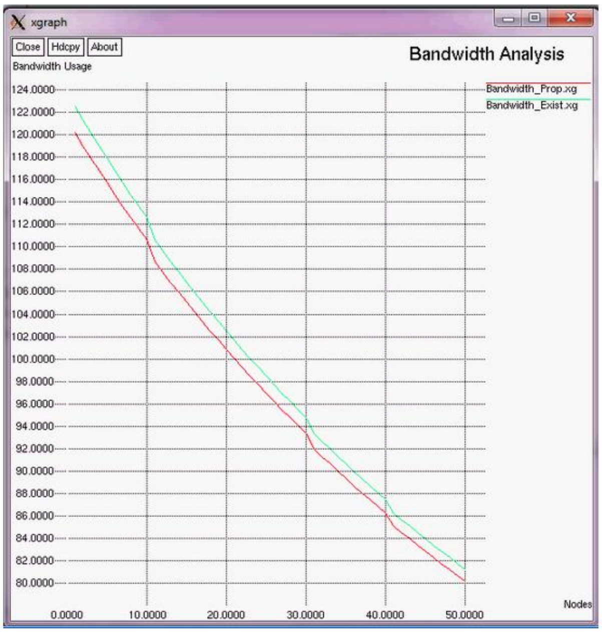

Fig. 2: Bandwidth Analysis.

Transfer speed is characterized as a range inside a band of frequencies or wavelengths. Transfer speed is additionally characterized as the measure of information that can be transmitted in a settled measure of time. For computerized gadgets, the transmission capacity is normally communicated in bits per second (bps) or bytes every second. For simple gadgets, the data transfer capacity is communicated in cycles every second, or Hertz (Hz).

```
Set xe [expr int($sq3*$sq5+$sq6)/($sq4+1.5+$i)]                    (1)
```

The data transmission is especially imperative for I/O gadgets. For instance, a quick circle drive can be hampered by a transport with a low data transfer capacity. This is the principle reason that new transports, for example, AGP, have been produced for the PC.

4.2. Control overhead analysis

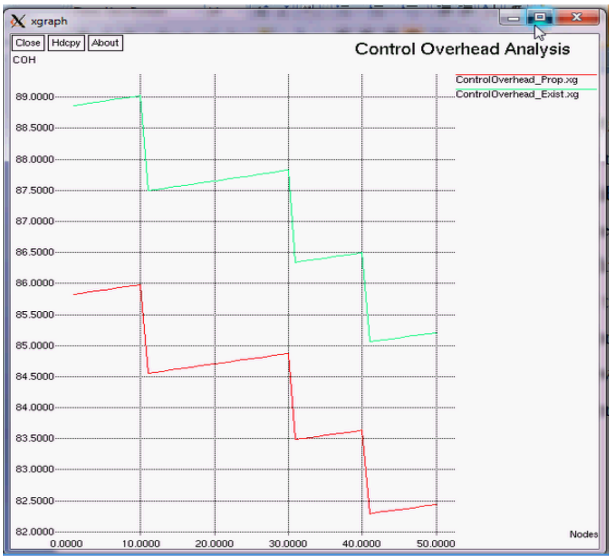

Fig. 3: Overhead Analysis.

Set xe [expr int($sq3*$sq4+$i+$sq7)/($sq6+5.5)] (2)

It is the proportion of the control data sent to the real information got at every hub I the network. It likewise alludes to the preparing time required to transmit information by a hub which incorporates all the supporting capacities like hub disclosure, interface support, network latency and transmission. It is clear from the above graph that there is a vital decrease in the overheads which helps in decreasing the delay in the network.

4.3. End to end delay

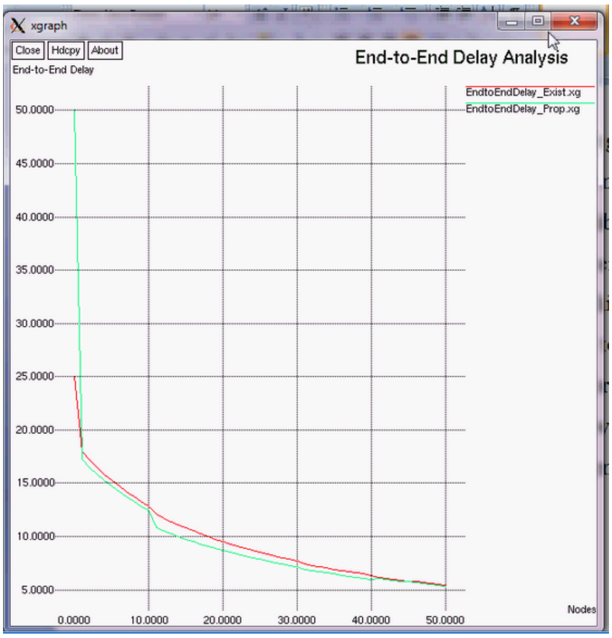

Fig. 4: End to End Delay.

End-to-end defers or one-way delay (OWD) alludes to the time taken for a packet to be transmitted over a system from source to goal. It is a typical term in IP arranges to check, and contrasts from round-trip time (RTT) in that one way in the one bearing from source to goal are estimated.

Set xe [expr int($sq4+$sq6+$sq5)/($sq7+5.5+$i)] (3)

The ping utility measures the RTT, that is, an ideal opportunity to go and return to a host. A large portion of the RTT is frequently utilized as a guess of OWD; however, this accepts the forward and back ways are the same regarding clog, number of bounces, or nature of administration (QoS).

4.4. Packet loss analysis

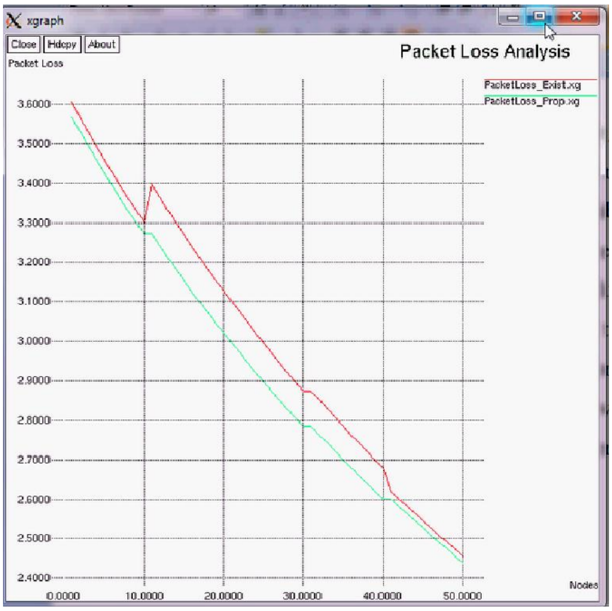

Fig. 5: Packet Loss Analysis.

We assess the connection quality between arrange hubs in light of the connection parcel misfortune and not on the got flag quality marker (RSSI). Our appraisal depends on in field estimations got utilizing the IRIS Crossbow WSN. The estimations are utilized to demonstrate the effect of parcel misfortune in a known steering convention for WSNs, LEACH. We propose a system statement stage where all hubs accumulate data about the connection bundle misfortune from all neighbors.

Set xe [expr int($sq3+$sq6+$sq5)/($sq4-1.5+$i)] (4)

Utilizing this data every hub will pick the going to bunch head (CH) in light of the littlest bundle misfortune instead of on the most noteworthy RSSI. Matlab recreations demonstrate that considering misfortune in picking the best correspondence way significantly affects lessening the vitality utilization of the system and additionally expanding system throughput.
In comparison with the existing system the loss of packets are reduced by maintaining the hub with lesser number of overheads and less packet retransmission so that the end to end delay is considerably reduced.

4.5. Throughput analysis

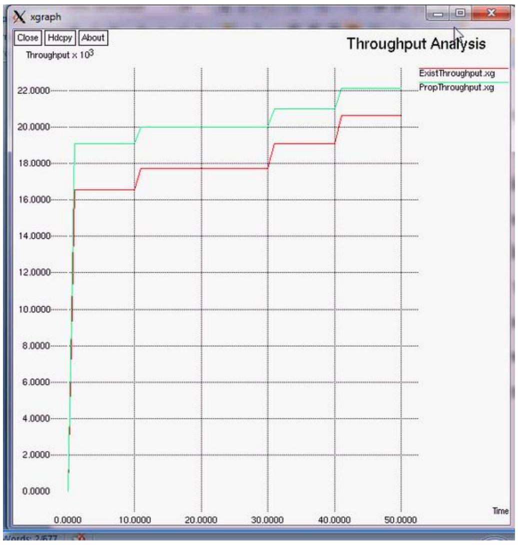

Fig. 6: Throughput Analysis.

Set xe [expr int($sq3*$sq4*$sq5)/($sq6+10.5)] (5)

It alludes to the ratio of number of packets reach the destination at a particular time period. It is observed that there is 10 – 15 % increase in the throughput.

5. Conclusion

The proposed framework introduced in this paper is non-specific, does not rely upon any VoIP application, convention, codec, and security system, can recognize scrambled burrowed VoIP, and implementable at it is possible that restricted or two-way arrange interface. It addresses the issue of any association to identify VoIP streams to either organize or piece. We test our answer on numerous hints of in excess of 10 VoIP applications. The correlations and results demonstrate that our system is the best among all the current methods. It is the better decision for media transmission specialists and ISPs to identify VoIP brings in fast huge Data condition.

References

[1] Vegard Engen, "Machine learning for the network-based intrusion," Ph.D. dissertation, Bournemouth Univ., Poole, UK, 2010.

[2] S. Sagiroglu and D. Sinanc, "Big Data: a review," 2013 International Conference on Collaboration Technologies and Systems (CTS), pp. 42- 47, IEEE, 2013. https://doi.org/10.1109/CTS.2013.6567202.

[3] M. M. U. Rathore and T. Mehmood, "Research on VoIP traffic detection," 2012 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), Genoa, 2012, pp. 1-5.

[4] Bing Li, Shigang Jin, and Moade Ma, "VoIP Traffic Identification Based on Host and Flow Behavior Analysis," Journal of Network and Systems Management, Volume 19, 2010. https://doi.org/10.1007/s10922-010-9184-7.

[5]] Fauzia Idrees and Uzma Aslam Khan,"A Generic Technique for Voice over Internet Protocol (VoIP) Traffic Detection," IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.2, pp 52- 59, 2008.

[6] Emanuel P. Freire, Artur Ziviani, and Ronaldo M. Salles, "Detecting VoIP Call Hidden in Web Traffic," IEEE transaction on network and service management, Vol no. 5, pp- 210-214, 2008 https://doi.org/10.1109/TNSM.2009.041102.

[7] Riyad Alshammari and Nur Zincir-Heywood, "can encrypted traffic be identified without port numbers, IP addresses, and payload inspection?" ELSEVIER: Computer Networks, vol. 55, pp 1326-1350, 2011. https://doi.org/10.1016/j.comnet.2010.12.002.

[8] T. Okabe, T. Kitamura, and T. Shizuno, "Statistical Traffic Identification Method Based on Flow-Level Behavior for Fair VoIP service," Proceedings of IEEE Workshop on VoIP Management and Security, pp. 35-40, 2006. https://doi.org/10.1109/VOIPMS.2006.1638120.

[9] Taner Yildirim and Dr. PJ Radcliffe, "VoIP Traffic Classification in IPsec Tunnels," 2010 International Conference on Electronics and Information Engineering (ICEIE), Koyoto, Japan, pp VI-151-VI-157, 2010. https://doi.org/10.1109/ICEIE.2010.5559900.

[10] P. Branch and J. But, "Rapid and Generalized Identification of Packetized Packetized Voice Traffic Flows," 37th IEEE Conference on Local Computer Networks (LCN12), Clearwater, Florida, October 2012. https://doi.org/10.1109/LCN.2012.6423690.

[11] http://tstat.tlc.polito.it/traces-skype.shtml.

[12] F. Fusco and L. Deri, "High-Speed Network Traffic Analysis with Commodity Multi-core Systems," ACM IMC 2010, Nov. 2010. [13] Hadoop library to read packet capture (PCAP) files. "Available online:https://github.com/RIPE-NCC/hadoop-pcap," Accessed on 1 April 2016.