IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

VoIP Intrusion Detection for secure transmission using PLRT (Packet Level Restraining Technique) under DDOS Attack

Humma Shoket[1], Jagdeep Singh Aulakh[2]

M.Tech Scholar, Electronics & Communication, Amritsar College of Engineering & Technology, Amritsar, Punjab[1]

Asst Professor Electronics & Communication, Amritsar College of Engineering & Technology , College, Amritsar, Punjab India [2]

Abstract: Voice over Internet Protocol (VoIP) shares the network resources with the regular Internet traffic, and is susceptible to the existing security holes of the Internet. Moreover, given that voice communication is time sensitive and uses a suite of inter-acting protocols, VoIP exposes new forms of vulnerabilities to malicious attacks The VOIP services in developed countries because of the existence of technologies i.e. 3G, 4G and LTE. VOIP is the main issue in developing countries because of the absence of these technologies as several main telecommunication companies are stressing on combining their system with VOIP technologies for providing the enjoyment of these less expensive services to the users. The PLRT technique is proposed for DDos Attack Detection and prevention

Keywords: VoIP, PSJA, PLRT.

I. INTRODUCTION

Voice over Internet Protocol (VoIP) which is also called Internet telephony is a technology that sends a voice signal in real time using Internet Protocol (IP) on the public web or private data. [1] it converts a sound signal that is similar to a digital reference in your phone before it is compressed and coded into long strings of IP packets to be transported better than the IP network to the receiver. At the receiving end, the IP packets are reassembled in order before decompressed and processed using a digital/Analog converter (DAC) to create the initial sent signal. [2] Its being is essentially based on two basic technologies, telephone and Internet. [3] The participation of existing infrastructure (convergence) between data and voice applications has been identified as some of the benefits of VoIP through reducing implementation, management and support. IP Telephony insurance is a difficult method. This means not only the ability to have a secure conversation between two contact parts, but also the security of signal messages used to make this call possible to all. The need to provide a certain quality of the parameters (quality of service) often leads to insufficient or not sufficient mechanisms for the VoIP service. This is mainly because the security mechanisms can be responsible for the increase in latency. If the latency is too high, these may be the most suppressed restrictions that limit the quality of VoIP calls. Therefore, today we are often faced with the need for barter between security and low latency for real-time service.

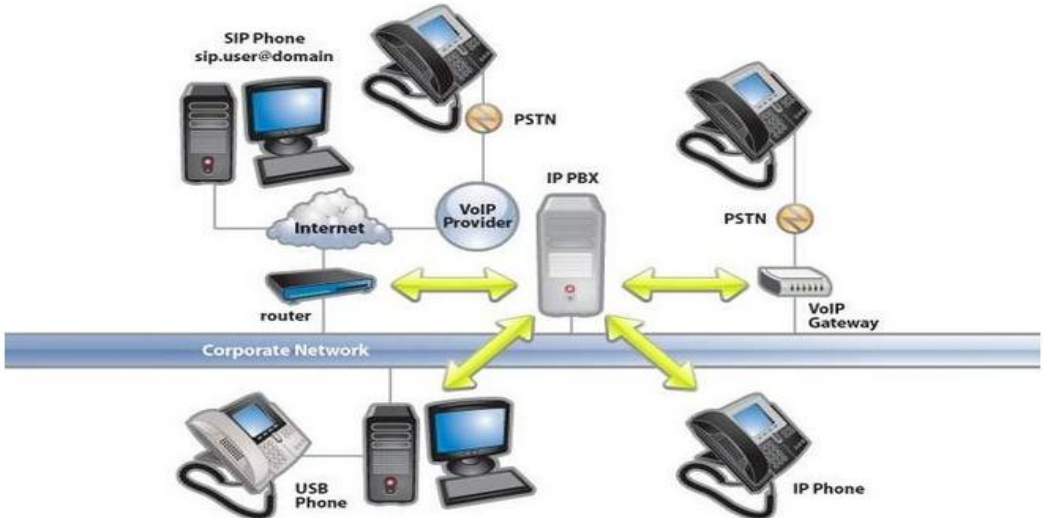

Fig 1: VoIP Structure

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

VoIP (Voice over IP) is a expertise for voice communication with Internet or any IP. This means that it sends the voice signal to the digital model in packets relatively than being sent in digital format or analog circuits using a mobile phone company or a conventional PSTN

II. VoIP SECURITY SERVICES

VoIP systems employ several protocols to monitor calls and deliver data. For example, in SIP-based IP telephony, the SIP Protocol is used [4] to control the installation and dismantling of calls, while the real-time Transfer Protocol (RTP) [5] is intended for media distribution. The VoIP system is spread network, consisting of IP phones, SIP agents, and many other servers. The defence against malicious insects on such a disparate and distributed environment is far from trivial. Recently, Wu and others suggested [6] a intrusion detection structure for VoIP, effective and shared, which is extracted from the protocol-based information from multiple packets and the assembled states are used in the corresponding engine of the rules. Different from its approach, In particular, instead of collecting and deriving the Protocol's call status and information from packets, our approach uses the state transitions that have been made in the State protocol to detect infiltration..The security services for information protection in the system are: certification, reliability, permission (logical access Control), confidentiality and non-repudiation/non-denial. However, taking into account the security of IP telephony systems, the three most major safety services are: verification, reliability and secrecy. The first two can be supplied with the use of watermark techniques. The third should be guaranteed in a different way, for example, with the use of security (encryption) mechanisms from the set for each VoIP standard.[7]

The security services provided are as follows:

I. **Authentication of the data source** (one can be sure of the caller's identification),

II. **Authentication of signalling communication**

III. **Reference to the integrity of communications** (it is known that signalling messages have not been altered during transmission via the communication channel)

IV. **Data certification – Integrity** (it is possible to ensure that the sound comes from the caller and is not tampered with).

III.SECURITY THREATS

A. SIP based Attacks

SIP attacks are located on your desktop, laptops, VoIP phones, mobile phones, and wireless devices. SIP is a SIM-Limit protocol, but it is effective in controlling calls that involve many multimedia and trust relationships between different aspects. Some devices trust each other, while others do not. In the takers, they have a set of targeted devices, starting with the final devices for routers, switches, signal phrases, media gateway controllers, and SIP agents [8,9]

B. **Distributed denial of service (DDos)** attacks are a subclass of denial of service (Dos) attacks. The Dos attack includes many devices connected to the Internet, collectively known as BOTAS, which are used to overwhelm the target site with fake traffic.

Unlike other types of electronic attacks, trampling attacks do not attempt to penetrate your security perimeter. as a replacement for, they plan to make your website and servers unavailable to legitimate users. External control services can also be used as smoke screens for other malicious activities, for the taking of safety devices, and to penetrate the security perimeter of the target.

A successful Dos attack is an extremely noticeable event that affects the entire user base on the Internet. This makes it a popular weapon to choose from . Cyber vandals, and extortionist and any other person who is looking to make a point or a champion of the matter.

Dos attacks often persist for days and weeks, even months at a time, making them extremely destructive to any online organization. Among other things, Dos attacks can lead to a loss of income, erosion of consumer confidence, and the power of businesses to spend wealth in damage and cause long-term damage to reputation.

C. ***Denial of Service (DoS)****:Denial of Service (Dos):* According to in DOS, an attacker is able to disable normal services on the phone system. The results may be unable to make or receive calls across the entire network, or in some cases a specific set of phone numbers can be targeted. The back affects availability and may include resulting latency, physical intrusion, loss of external energy supplies and depletion of resources on the network.[10]

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

D. **Toll fraud**:The attacker connects to the VoIP network for the international illegal or intercontinental calling mode. These effects can be demoralized on the reliability of weak data and passwords and user names by hackers

E. **Signal protocol tampering**: This attack is focused on the call preparation process. It means that the attacker was able to monitor and capture packets during the call that was placed. Through this process, an attacker can change data flow fields. This will allow it to put VoIP phone calls without VoIP. Coulibaly and Liu explained in [7] that this malicious user might also be able to put expensive calls that IP

a. PBX (Internet Protocol Private Branch Exchange) can connect to another user.

b. *Repudiation attacks*: in this attack, a conversation between two parties can be denied by one party.

IV. RELATED WORK

Niherika Singh et.al. [2016]The existing security mechanism is based on the self-adjusting mechanism, which has a decentralized approach to the selective jamming of 4g/TE networks. Selective attack interference is a form of denial-of-service attacks, which is used to cause the resources available for a particular purpose. The Auto-fit in the title means that each knot is individually capable of selective cracking interference attack on its own. The proposed model applies exactly to the 4 G/networks that operate in multi-purpose communications (part-time access) and effective against refusal to attack distributed services. The proposed scheme is intended to work in the MAC layer. The proposed project also aims to solve the problem of energy consumption. The new chart is created in the sheet to put a lower impact on energy consumption and help the 4g/TE networks to establish a stronger connection

Dayung Hyun et.al 2016[12] framework for VoIP security services and sound over the business Network integrated (voltages) in trade networks using specific software (DS) and virtual network functionality (FV). VoIP/Volt services are exposed to several security threats such as denial of service (Dos) attack, sniffer network, access to unauthorized service. Traditional security services for VoIP/voltages suffer from a lack of flexible installation security rules and the updating of dynamic security rules. The security services Framework for VoIP/voltages on the basis of the local Development network and the National Gender Security Fund the framework can flexibly install new rules and dynamically update these rules. Based on the Yang data form to configure the remote network device, we have implemented basic configuration functions for the security services infrastructure for VoIP/voltages. To illustrate the usefulness of the proposed framework, we have used the visual light of our implementation, which can provide effective security services to VoIP/volts providers.

Jakob Spooner et al. [2016] [13] The defined software networking is a paradigm still at its emerging stages in the field of networks at the production scale. New level of dependability by central functioning for administrators and network programmers. safety measures is a enormous factor contributing to the resistance of consumers to the implementation of the SDN architecture. Without addressing the issue inherent in the centralized AIEP nature, the benefits of network configuration performance and flexibility cannot be exploited.

Rafael Horvath et. [2015] [14] network technologies have always been a crucial element of success for technologies such as cloud computing. However, because of the slow development of scalable infrastructure, it can lead to problems of competitiveness. The Knowledge networking software (SDN) Next can address these problems by giving new functionality to the entire network topology. With SDN, administrators have the ability to just basic network infrastructure for applications and Web services. The document highlights the main findings of the systematic review of documentation on the challenges and implications of the network. It shows that most documents deal with the implementation of networked networking programmers, which are defined as a challenge, including factors such as the insurance of the introduction and the overall risks of changing the traditional networks. Concentration is also being given to security issues emanate from specific software networks and the high permanent demand for end-users associated with the fear of shifting conventional networks. Issues relating to specialized know-how have been identified as another category of challenges. The effects of the network are discussed by identifying the unique features of the grid, such as the lack of coupling of the hardware and the overall display of the entire web structure. It also affects network management, including changes in policy dissemination, programming potential and network maintenance.

V. PROPOSED WORK

The proposed work mainly focus on increasing the security of VOLTE-VOIP network the various technique have been proposed for network security but integrity and privacy are always remain serious issues which still require scope of enhancement .the network system is prone to attacks. the weakness of network system are illegitimately used by attackers to exploit the network system for decreasing its working efficiency. There are various attacks in current

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

network system but the Denial-of-Service attack is one among various attacks .DDos attack is strong attack and it can appear any time in network .the main aim of this attack is to stop client from using efficient and continuous service of network by flooding large number of illegible packets in network .the DDos attack use malicious nodes for sending fake packet in network which decreases network bandwidth and working efficiency. with the help of DDos attack the attackers can control large numbers of clients resources by using weakness of system and control them remotely. the DDos attack is very dangerous attack since number of clients machines are involved in this attack so it is very difficult to find from which client machine the attack is originated. in DDos attack the fake IP address are used for sending illegal packet so it is not possible to identify DDos on the basis of client IP address
To increase the working efficiency of network it is important to remove the effect of DDos attack from network .the Packet level restraining algorithm is used for removal of DDos attack for enhancing the working efficiency of network.

The proposed algorithm keeps track of flooded packets in transmission. The proposed algorithm work in three steps

Step1: The DDos attack occurs if the no of packets sent by client machine are more than processing capacity of server. The proposed technique initially calculate drop packets in the network and response time of incoming node requests using packet Level Restraining algorithm

Step2: In DDos Flooding attack the message are flooded with fake IP from client machine. Due to which it is difficult to identify the source of flooding attack. In our proposed technique the origin of DDos attack is Identified by taking unique key with IP address in nodes while transmission. The unique key and IP address of node are compared. If they don't match then node will be considered as DDos node and that node will be neglected while transmission and network will be updated that these nodes are fake node and further transmission will not be done by these nodes

Step3 in third step packet filtering is done to identify the legitimacy of packet on TTL basis. In proposed technique packet processing request of server is considered with value (N) if frequency of the requested message is more than the packet processing request level of server (N) .then the packet is not processed and excluded from transmission if node keeps on flooding message to server more than the packet processing request level than the node is excluded from network and considered as malicious and whole network is updated with the IP address of these nodes .so that these malicious nodes should not be consider while transmissions in future

The Packet Level Restraining Algorithm helps to control the flow of incoming packets into the Base Station such that the Base Station is not flooded with requests. But, this only helps in congestion control at this stage, so, to check validity of an incoming packet we have performed packet filtering on the basis of TTL values of each incoming packet

Algorithm
PF: Packet frequency

SPPRL: Server Packet Processing Request level

MN: Malicious Nodes

CID: Client ID

1: for time=1 to simulation time

2: for i=1: N, where N the number of nodes that placed in the network

3: if PF>SPPRL for CID message request to server)

4: Add (CID); store information of malicious node in route path update network with CID as malicious node

5Else: simple node in route path efficient node for transmission

6: Find CID number of malicious node excluded from network

7: end if
8: end
9: end
10: end

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

VI. SIMULATION RESULTS

1. Throughput: the throughput is defined as a number of bits transmitted in second. The kbps is the metric measure used to measure throughput. The evaluation result between Proposed technique and network under DDOS attack are shown in fig2 and table 1 .the results show that due to IP spoofing and fake message flooding throughput under DDOS attack is less as compared to proposed technique PLRT(Packet Level Restraining Technique) technique which shows that our proposed technique works fine under DDOS attack. the results shows that under DDOS attack PLRT(Packet Level Restraining Technique) has better than PSJA technique

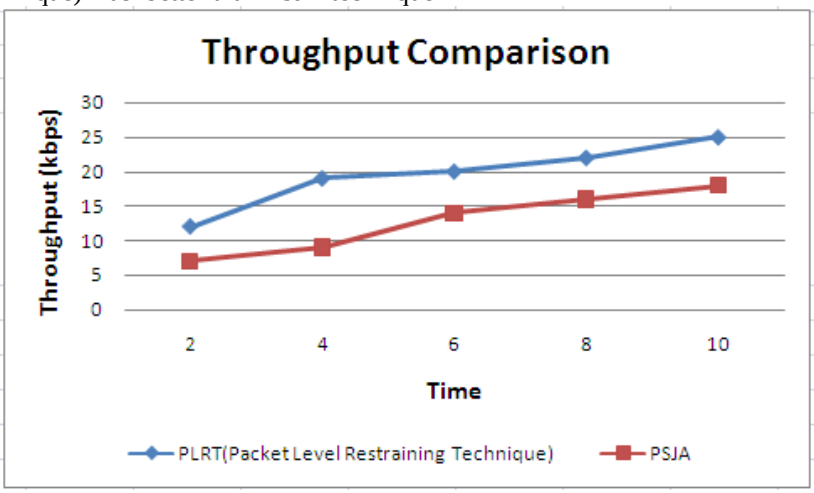

Fig2 Throughput Comparison

Time	PLRT(Packet Level Restraining Technique)	PSJA
2	12	7
4	19	9
6	20	14
8	22	16
10	25	18

Table1 Throughput Comparison

2. Packet Delivery Ratio: the total number of Packet transmitted from sender node to receiver node is called (PDR) "packet delivery ratio". The Fig3 and Table 2 shows comparative analysis graph results based on data transmission after DDOS attack and by applying proposed technique PLRT(Packet Level Restraining Technique)the evolution result shows that proposed technique performing better under dummy packet transmission and IP spoofing for secure and reliable transmission, in particular, VOIP network the results shows that under DDOS attack PLRT(Packet Level Restraining Technique) has better than PSJA technique

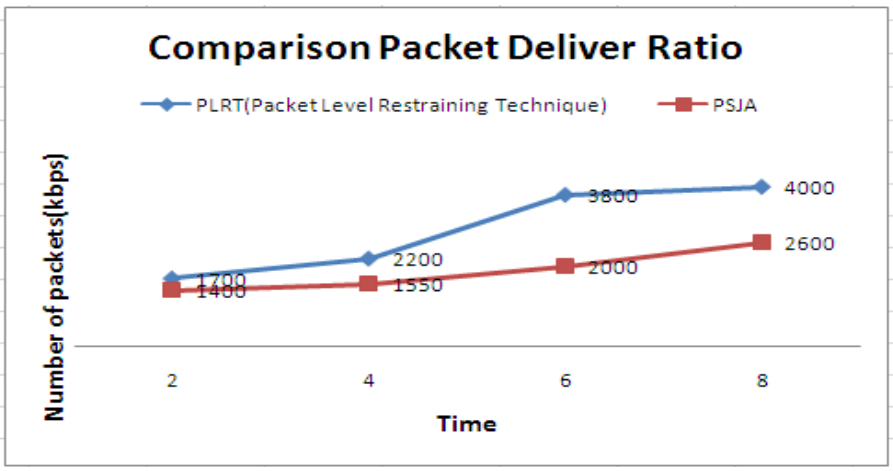

Fig3 Packet Deliver Ratio Comparison

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

Time	PLRT(Packet Level Restraining Technique)	PSJA
2	1700	1400
4	2200	1550
6	3800	2000
8	4000	2600

Table2 Packet Deliver Ratio Comparison

3.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. the comparison of proposed technique and previous technique shows that .the result of proposed technique PLRT(Packet Level Restraining Technique) are better than previous technique(PSJA)

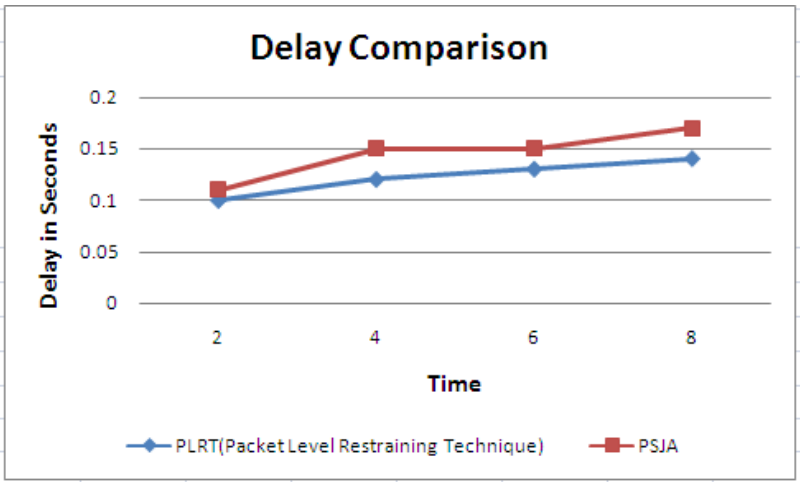

Fig4 Delay Comparison

Time	PLRT(Packet Level Restraining Technique)	PSJA
2	0.1	0.11
4	0.12	0.15
6	0.13	0.15
8	0.14	0.17

Table 3 Delay Comparison

VII. CONCLUSION

IP Voice offers sole and economical service Internet users. It provides quality improvements, Interoperability and videoconferencing .but by providing high speed router and high speed for better and fast services arises various threats while communication. The characteristics of VoIP technology must be precise applicable to the conventional capacity The proposed technique PLRT(Packet Level Restraining Technique) is applied while DDOS attack arises in VOIP network .the proposed technique help in reducing network working and increases the throughput and packet delivery ratio. the PLRT(Packet Level Restraining Technique) technique solution against IP Spoofing in network proposed technique work on finding origin of DDOS attack help network in avoiding transmission with attackers nodes .our proposed technique

REFERENCES

[1] Anita Singh and Dr. Deepti Sharma, "A Review on Voice over Internet Protocol (VOIP) over LTE Networks", International Journal of Science, Engineering and Technology Research (IJSETR) Volume 5, ISSN: 2278 – 7798, 2016, pp.1527-1531

[2] Jakob Spoone and Dr Shao Ying Zhu, "A Review of Solutions for SDN-Exclusive Security Issues", International Journal of Advanced Computer Science and Applications, vol. 7 , 2016, pp. 113-122.

[3] Jinyong Kim, Mahdi Daghmehchi Firoozjaei, Jaehoon (Paul) Jeong, Hyoungshick Kim, and Jung-Soo Park, "SDN-based Security Services using Interface to Network Security Functions", Electronics and Telecommunications Research Institute, Republic of Korea, ISBN :978-1-4673-7116-2, 2015, pp.526-529

[4] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. RFC 3261, IETF Network Working Group, 2002.
[5] H. Schulzrinne, S. Casner, R. Frederick, and V. Jacob-son. RTP: A Transport Protocol for Real-Time Applications. RFC 1889, IETF Network Working Group, 1996
[6] Y. Wu, S. Bagchi, S. Garg, N. Singh, and T. Tsai. SCIDIVE: A Stateful and Cross Protocol Intrusion Detection Architec-ture for Voice-over-IP Environments. In *IEEE Dependable Systems and Networks Conference (DSN 2004)*, June 2004.
[7] ISO 7498. International Standards Organisation (ISO). Information processing systems - Open systems interconnection - Basic reference model - Part 2: Security architecture (ISO/IEC 7498-2). 1989.
[8] O. Arkin. Why E.T. Can't Phone Home? - Security Risk Factors with IP Telephony. Presentation, AusCERT Aus-tralia, 2004.
[9] A. Niemi. Authentication of SIP calls. In *Tik-110.501 Sem-inar on Network Security*, 2000
[10] D. Sisalem, J. Kuthan and S. Ehlert, "Denial of service attacks targeting a SIP VoIP infrastructure: attack scenarios and prevention mechanisms," *Network, IEEE*, vol. 20,pp.26-31, 2006.
[11] E. Coulibaly and Lian Hao Liu, "Security of voip networks," in *Computer Engineering and Technology (ICCET), 2010 2nd International Conference on*, 2010, pp. V3-104-V3-108
[12] Daeyoung Hyun∗, Jinyoug Kim†, Jaehoon (Paul) Jeong" SDN-Based Network Security Functions for VoIP and VoLTE Services" conference ©2016 IEEE 978-1-5090-1325-8
[13] Jakob Spoone and Dr Shao Ying Zhu, "A Review of Solutions for SDN-Exclusive Security Issues", International Journal of Advanced Computer Science and Applications, vol. 7 , 2016, pp. 113-122.
[14] Raphael Horvatha, Dietmar Nedbala and Mark Stieningera, "A Literature Review on Challenges and Effects of Software Defined Networking", 2015 , pp.552-561.