International Journal of Mathematical Archive-2(12), 2011, Page: 2712-2720
Available online through www.ijma.info ISSN 2229 – 5046

Novel Survey on Detection of DDoS Attack Using Traceback Technique in VoIP Networks

R. Thandeeswaran, Asha A. and N. Jeyanthi*

School of Information Technology & Engineering, VIT University, Vellore - 632014, Tamilnadu, India
E-mail: rthandeeswaran@vit.ac.in, ashaanithadevi@gmail.com

(Received on: 12-11-11; Accepted on: 30-11-11)

ABSTRACT

D*DoS attack in internet and Voice-over-IP network can be detected using IP traceback mechanism. VoIP is the technology to transport voice communication over IP network. Such as internet which is capable of making telephone calls over packet switching network. It exploits advance voice compression technique and bandwidth sharing in packet switching network. VoIP works on IP backbone hence it also vulnerable to all types of attacks and internet is susceptible with.*

Among these, DDoS plays a vital role and has major impact on its performance. The goal of IP traceback is to trace the path of an IP packet to its origin. DDoS is a distributed collaborative large scale dos attack which attack on a wide range of subtle. It's very easy to implement and difficult to prevent and trace.

The goal of distributed denial of service attack is to deny legitimate users access to a particular resource. This is done by exploitation system weakness or adding computational system overload or by misusing a protocol. Proper network configuration made DoS attack difficult to accomplish. This paper presents a survey on the existing mechanisms and an analysis on their merits and demerits.

Keywords: *VoIP, DDoS, Traceback*

Introduction:

Voice over Internet Protocol is a family of technologies for the transmission of voice over the internet. Voice is converted into digital signals and is transmitted as data packets. The conversion of analog voice to digital signals is done by the analog to digital converter. Voice over IP is a technology in which transmission of voice using IP technology over packet switching network. VoIP is a subnet of IP telephony which is used for transport telephone calls. So internet telephony is its main application.

Skype is one of its product which reduce communication and infrastructure cost. Main advantage is that more telephone calls are possible over a single bandwidth. But it is not free of attacks. In this paper I focus on DDoS attack which can easily change the source address of an IP packet and cause memory less feature of internet. DoS attack can prevent outgoing traffics or incoming traffic to network services. They utilize the weakness of computer or TCP/IP protocol.

In this paper we are also discussing about different type of DoS attacks and traceback mechanism to detect attacks. To defending against IP spoofing in which identity of sender is fake. Reconstructing the attacked path by tracing the packet back to source. Packet logging and packet marking algorithms are used for this purpose. VoIP can support file sharing, calendaring, sending fax, collaborative editing, and video. It supports dual mode telephone conversation between cellular service and Wi-Fi network, internet to PSDN network bridging, P2P calling in Skype.

Architecture and DDoS attacks:

VoIP has two type of architecture based on H.323 and SIP. H.323 is a set of protocols for data conferencing, voice and video over packet switching network. SIP (Session Initiation Protocol) is an IETF protocol for VoIP and other multimedia. SIP is an application layer protocol for creating, modifying and terminating sessions. SIP being a more flexible and simple protocol, it is quite easy to add features in SIP. The fundamental architecture of H.323 and SIP consist of three logical components: gateway, signalling server and terminal. They differ in call management, transporting using protocols, voice coding, call management and gateway control.

***Corresponding author:** N. Jeyanthi*, **E-mail:** njeyanthi@vit.ac.in*

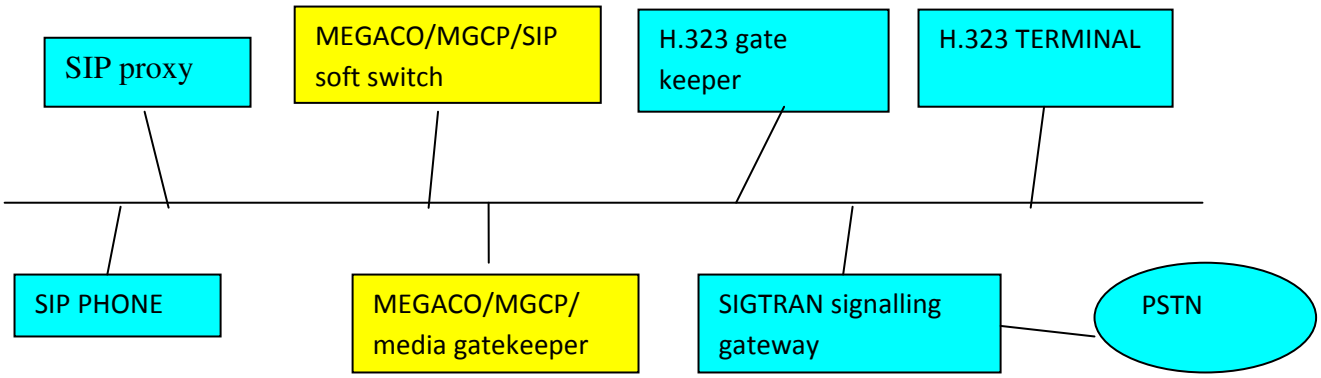

Figure-1: VoIP Architecture

DDoS attacks rely on weakness in TCP/IP protocol. TCP/ IP network are made of packets VoIP use it to go across the networks. Different types of DoS attack include flood attack, ping of death attack, SYN attack, teardrop attack, smurf attack.

Flood attack attacker sends more traffic to server more than it can handle. It is difficult to prevent and the attacker have more speed than target machine.

Ping of death attack the attacker send IP datagram of larger size which exceeds the standards that is sending a ping of 65,535 byte to target.

SYN attack occurs in handshake mode of connection taking place using SYN and ACK messages. The attacker floods the receiving station with SYN messages which appears to be come from unreachable internet address and fill the SYN buffer. The target can't send ACK messages and thus prevent other system communicate with target machine.

Teardrop attack which confuses the target machine or hang it. Here corrupted packets are sent to target machine using packet fragmentation algorithm.

Smurf attack which a broadcast address of third party is used. The attacker sent ping request to third party which is a spoofed IP address appears to be come from target machine. So the every system in the third party will send ping response to target machine.

In DDoS attacks in make compromised systems using Trojan horse or worm or hacked. And these compromised systems are controlled by client server software like tribe flood network, Trinoo, shaft.

How VoIP works:

VoIP works by sending packed digital data over internet. TCP/IP network are made of header and payload. Header is used to control communication and payload used to transport information. The voice at sender which is analog signal is digitized with the help of analog to digital converter (ADC). After encoding and Packetization it is transmitted as IP packet over switched network.

In destination it receives the IP packets containing voice information then decoded and convert the digital signal back to analog signal using digital to analog converter (DAC). VoIP digitize the voice in data packet and send it to the receiver and in receiver reconstruct it back to voice.

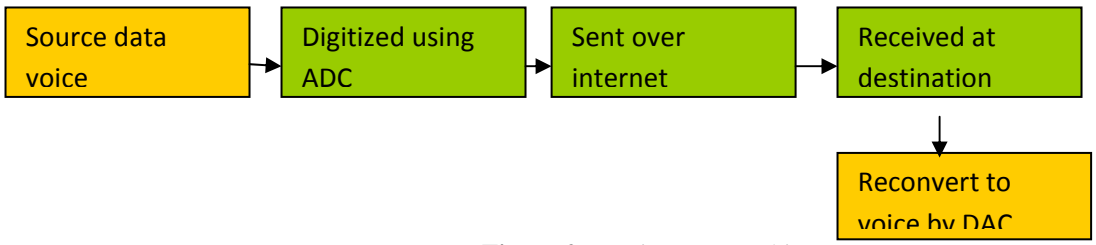

Figure 2: Basic VoIP working

VoIP protocol overview:

Evolution of VoIP in market is due to toll free or low cost phone calls, unified messaging and merging of voice infrastructure. VoIP support different protocol like media gateway control protocol (MGCP), session initiation protocol (SIP), skinny client control protocol (SCCP), session description protocol (SDP), simple gateway control protocol (SGCP) and session announcement protocol (SAPv2).

SIP is a protocol defined in RFC2543 of the MMUSIC working group of internet engineering task force (IETF). Researchers are focused in SIP because of its wide use and open source implementation. It is a stateful protocol supports bidirectional communication and interaction with multiple users. SIP is a client server base protocol which provides call forwarding, cal lee and caller number identification and authentication, invite multicast conference and personal modification.

VoIP networks, flooding attack is the most severe threat. The SIP proxies are flooded up with thousands of INVITE request simultaneously pr within a short period of time. The servers have to maintain the state of each INVITE message while it is waiting for the OK message. In case of severe attacks, the resources of the proxies are exhausted. Registration process also makes bed for DDoS attack as there is no authentication of REGISTER messages. Attackers can make numerous REGISTER requests and thereby flood the Registrar and Location Servers.

SIP is used with other IETF protocols like real time transport protocol (RTP) to provide QoS feedback and transporting data packets. With media gateway control protocol (MEGACO) for controlling the gateway to public switched telephone network (PSTN). And with session description protocol (SDP) for defining the session.SIP works on IPv4 & IPv6.

SIP in IP telephony. All the caller and cal lees in VoIP network is identified by SIP addresses. While making a SIP call, the main operation is invitation in which the caller locates the server and send request. The request is then redirected. Users can register with SIP servers. SIP addresses or URL is embedded in web pages so you can enable it by clicking.

- **Media gateway control protocol** is a master slave protocol used to control telephony gateways from external call control elements. The external call control elements called media gateway controller or call agents. A telephony gateway allows communication between audio signals carrying telephone network to data packet carrying internet using switched network.

In call controlled architecture the media gateway controller handle the call control intelligence outside the gateway. Under the control of this protocol call agents are synchronised to send commands to gateway and the gateway execute it.

- **Skinny client control protocol**used to communicate H.323 proxy with skinny client. Skinny client is Ethernet phone uses TCP/IP for transmitting and receiving the calls. For audio signal it uses UDP or RTP to form skinny client or H.323 terminal. Skinny message are transmitted using port 2000 and TCP.

- **Simple gateway control protocol** is same as media gateway control protocol. It set a simple gateway control interface for transaction. The transactions consist of commands and a response. Commands are create connection, modify connection, delete connection, notification request and notify.

- **Session description protocol** is used for communication with existing system and to transfers information to enabled participants in session. Multicast backbone is a session directory tool. This protocol describes the purpose of session.

- **Session announcement protocol** is used by session directory clients. It multicast announcement packets to server address and port. Announcement describes the permitting constraints.

Threats and traceback mechanisms:

Denial of service threads in VoIP: the main aim is to deny the legitimated user in accessing the VoIP network or connectivity. DoS attacks in VoIP occur by flooding the target machine with unnecessary SIP call which degrades the service. The call processing may drop or halts. The main aim of attacker is to get the remote control of the system.

Spamming over internet telephony as we know the spam messages carry viruses or spywares. Each VoIP account has its own IP address. The spammer sends hundreds of voicemail to IP address and it gets clogged. It is a social threat.

Eavesdropping, modification threats in VoIP: by stealing the credentials like password or username a third party gain a third party gain control over the voicemail and all the information of victim. Hackers listen the signalling or contention of that session. The attacker can also modify the session.

Call tempering in which the attacker can intentionally tamper the call by adding noise packets in communication stream which degrade the quality of service. Vishing by VoIP is called voice phishing in which fake third parties try to get identity of victim. Physical threats affecting VoIP include the unauthorized physical access to VoIP equipment, performance degradation and power loss due to weather cause inaccessible VoIP services.

IP traceback mechanisms include Ingress filtering includes blocking the packet from attacker by configuring the router. The router has capacity to distinguish the legitimate user and illegitimate user by examining the source address of every packet. Link testing is traceback techniques which examine the upstream router from the router closet to victim till the router carrying the attacker traffic are found. Link testing includes input debugging and controlled flooding.

Logging technique which helps in determining the path traversed by the packet using data mining technique. lt is easy method to find the attacker but drawback is that it add enormous resources requirement. ICMP traceback techniques which use internet control message protocol are used to trace out the attack path. Every packet enable edge sampling algorithm with low probability and generate ICMP traceback message which consist of next and previous hops and time field.

Advanced marking and authenticating marking as fragmented marking scheme proposed by savage et al[]. This approach has low network and router overhead. It supports an efficient authentication of routers marking. It reconstructs the attack path efficiently with low false positive.

Packet marking algorithm: Here the mark is the signature or identity of a router. In addition to forwarding it also insert a mark. Deterministic packet marking (DPM) the router mark the entire packet using IP address of router. So the victim can reconstruct the attack path using it. Drawback is that due to additional functionality the router will slow down.

Probabilistic packet marking (PPM) is proposed for achieving traceback of DOS attack. DOS attack can be prevented if the spoofed source IP address is trace back to origin to find the attacker. But in PPM only some packets are marked by the router so the attacker can mislead by marking their original packet.

Hash based IP traceback mechanism is also called source path isolation engine (SPIE). After examining the single packet the router can create queries to reconstruct its path. But the attacker can attack the queries and response communication and thus affect its performance.

Flexible deterministic packet marking (FDPM) is a version of DPM. It is more efficient than DPM and adds flexible features to traceback mechanism. In TOPO based traceback mechanism bloom filter utilize the immediate predecessors topology information to traceback. It is single packet IP traceback mechanisms which reduce unnecessary queries.

Topology based packet marking (TBMP) is an approach against anti IP spoofing technique. It focuses on the path traversed by the packet and strengthens packet marking principle.

Table 1: Comparison of Detection of DDoS Attack Using Traceback Technique in VoIP Networks

Traceback technique	Reference	Advantages	Disadvantages	Technique used	Performance evaluation
An IP traceback technique against DoS attack	[4]	■Advanced and authenticating marking scheme. ■Upstream router map for speeding up attack path reconstruction. ■Low network overhead. ■Low router overhead ■Efficient perform IP traceback in multiple attacks.	■Marked information are not authenticated. ■Compromised router may tamper information marked by upstream router & make victim reconstruct	Reflective algebraic marking scheme contains 3 algorithm marking, reflection, reconstruction algorithm	■Efficient for multiple attack

			wrong path. ■Database is needed to store each packet.		
A resource efficient IP traceback technique for mobile Ad-hoc networks based on time tagged bloom filter.	[16]	■Compatibility with existing protocol stack it doesn't require protocol stack modification. ■Minimum number of traceback packet. ■Minimum traceback load. ■Minimum network load. ■No additional network traffic	■Re-initialization is needed when entry is remarked. ■Duration of filter increases collision rate increase so copy of content is filter regularly. ■Bloom filters collision rate is kept down .07% for efficient working.	Modified bloom filter with time tag (log based).	Low overload
IP traceback based attacker tracking: a probabilistic technique for detecting internet attack using the concept f hidden Marko models.	[3]	■No increasing the overhead on router & packet. ■No intervention to internet service provider. ■Sampling solves problems encountered by packet marking. ■Extended edge sampling solve problem of space & fragmentation.	■Data records are collected in a format in enhanced PPM. ■HMM hidden state denotes routers or system of attacker, victim &legitimate user. ■Only one event is defined at a state for every transition in data records. ■Training phase the HMM parameter are re-estimated by EM algorithms.	Concept used Hidden Markov Models(HMM).(edge sampling)	Solved the problem of space and fragmentation
IP trackbacking based on intelligent packet filtering	[1]	■Protocol independent DDoS defense scheme. ■Victim able to statistically distinguish legitimate traffic from DDoS traffic. ■Marked packet of infected edges is filtered out.	■Need router fully in line with operation of IP traceback.	■Bloom filter	Throughput of legitimate traffic can be increased by 3 or 7 times.
IP traceback for wireless Ad-hoc network.	[10]	■Only one packet is need to reconstruct the attack path.(SPIE)		■Source path isolation engine(SPIE),PPM ■,ICMP	
IP traceback based on packet marking and	[5]	■Have advantages of packet marking &packet logging. ■Reduce storage overhead since partial path information is	■Ability to track a single packet as in hash based.	■Hybrid IP traceback	Storage overhead is reduced to half and access time

logging		forwarded by router. ■Reduce access time required for recording packet.	■Each packet commit marking & logging operation		increased by a factor of no. of neighboring router
Hash based IP traceback	[2]	■Ability to identify the source of any data sent across network. ■Packet encapsulation –new packet is generated with original packet as payload. ■Packet generation -1 or more packet is generated as a result of action by router.	■New packets want to be forwarded & processed independently. ■Packet size shouldn't grow but some protocol cause packet to increase overhead.	■SPIE	System is effective & space efficiency approximately.5 % of link capacity per unit time in storage
QuIT: quantitative IP trackbacking	[15]	■QuIT can fight against DDoS attack power vary from 56k modem dial to 10M broadband access. ■QuIT transfer digest along traffic to target so victim can easily find source without communication with other router. It works on distribution of packet from each source, help to know power of attack.	■Accuracy is less because packet are random selected.	■Traceback both forward and backward.	Traffic generated by QuIT is less than .12%& computation complexity affordable.
Traceback of single IP packet using SPIE	[8]	■SPIE doesn't increase network vulnerability eavesdropping. ■SPIE also trace packet across transform where packet change between router as part of forwarding. ■SPIE support packet logging auditing at network router to support traceback of single packet.	■SPIE support inversion of first packet fragmentation only. ■Attack can't control which fragment are received by viticm.	■SPIE	SPIE reduce memory requirement down to .5%of link BW per unit time.
Detection and tracing DDoS attack by intelligent decision prototyping		■PMD makes IDP more efficient &effective than other packet marking schemas.	■Functional overhead.	■Pre-Marking decision(PMD)evaluate a packet before packet is used for trace backing.	IDP can successfully traceback 75-80% of packet.
A stateless traceback technique to identify the origin of attacks from a single packet		■Locates origin of attack with constant accuracy regardless of no. of attack.	■System doesn't rely on multiple received packets to reconstruct path.		■Constant accuracy
Network support for IP traceback	[7]	■Introduce post mortem capability. ■Encode path information in router and host. ■It doesn't require interaction	■Doesn't address implementation in IPv6. ■Difficulty in	■PPM	Post mortem capability

		co-operation with ISP's	correctly grouping fragments together. ■Backward compatibility		
32 bit as a number based IP traceback	[9]	■Avoid recording the packet unnecessary. ■No.of packet for detection is less. ■We can calculate optimum portability from topology. ■Combine internet topology &PPM.	■Take more time	■Modifying PPM(AS method)	Optimum portability of packet marking of .092 is obtained
A method for IP traceback for DoS	[1]	■Low computation easy to implement. ■Introduced AMN to solve problem of traceback in different network. ■Low network & router overhead. ■Supports incremental deployment. ■No change to existing protocol.	■Some defects in dealing with flooding style DoS. ■Impossible to trace attacks caused by single packet. ■Not effective when many routers are subverted.	■Probabilistic packet logging in internet.	Implementation easy
A novel traceback approach for direct & reflected ICMP attacks.	[12]	■Against both reflective & direct attack. ■Based on behavior of ICMP protocol. ■Only few packet are needed.	■Marking system no limit evasion of attack.	■Novel traceback approach to trace ICMP attack.	Efficient against direct & indirect attack.
A defensive mechanism against DDoS/DoS attack by IP traceback with DPM	[11]	■Module division marking eliminate need for logging. ■No communication overhead. ■It requires no support from IPS	■Difficulty in implementing the system. ■Impose additional burden to router.	■Modulo technique for interface marking(MTIM)	Less overhead
Advanced and authenticated marking scheme for IP traceback.	[6]	■Low network & router overhead. ■Supports incremental deployment. ■No communication overhead. Higher precision & lower computation overhead.	■Take more time for computation	■Advanced marking scheme &authenticated marking scheme.	Accurate for attack path reconstruction.
Scalable packet digesting schemes for IP traceback	[9]	■Hybrid deployment & scalable IP traceback architecture. ■Transformation lookup with flow signature to get advantage of packet aggregation. ■Provide more security.	■Memory requirement under high link capacity.	■Packet digesting	More scalable
Dynamic probabilistic packet for efficient IP	[16]	■Improved the effectiveness of PPM. ■DPPM support incremental deployment.	■Traveling distance of packet is calculated by	■DPPM(dynamic probabilistic packet marking)	Improved than PPM

traceback		■DPPM completely removed uncertainty & help victim to pinpoint origin of attack.	TTL value to calculate marking probability. ■DPPM cost is more than PPM.		
An implementation of a hierarchical IP traceback architecture	[14]	■Decompose internet wide traceback into intradomain&interdomaintraceback. ■Independent of single IP traceback. ■Domain decomposition depends on existing operational model of internet.	■Implementation cost	■Hierarchical IP traceback architecture.	eIPtraceback capable of finding attack path in 30 minute.

CONCLUSION:

In this paper, surveys of various IP traceback techniques which are applicable to VoIP networks were presented. Since the VoIP network not free from DoS attacks, IP traceback mechanism like link testing, packet logging, packet marking, ICMP traceback, advanced marking and authenticated marking, packet marking algorithm, deterministic packet marking, probabilistic packet marking and hash based IP traceback are applicable to VoIP. In future we are trying to implement advanced marking and authenticated marking scheme in VoIP which help to prevent more attacks with less network and router overhead.

REFERENCES:

[1] A John, T Sivakumar "DDoS: survey of traceback mechanism", 2009 academy publisher, International Journal of Recent Trends in Engineering, Vol. 1, No. 2, May 2009.

[2] Alex C. Snoeren, Craig Partridge, Luis A. Sanchez, Christine E. Jones, Fabrice Tchakountio, Stephen T. Kent, and W. Timothy Strayer "hash based IP traceback".

[3] Angeles D. Keromytis "A Comprehensive Survey of Voice over IP Security Research" IEEE communications surveys & tutorials.

[4] Zhaole Chen, Moon-Chuen Lee "An IP Traceback Technique against Denial-of-Service Attacks" computer security application conference, 2003.

[5] Chao Gong, SaracK "IP traceback based on packet marking and logging". IEEE international conference, 2005.

[6] Dawn Xiaodong Song and Adrian Perrig, "Advanced and authenticated marking scheme for IP traceback", IEEE INFOCOM 2001

[7] Stefan Savage, David Wetherill, Anna Karl in, and Tom Anderson, "Network Support for IP Traceback", IEEE transactions on networking, vol. 9, June 2001.

[8] Wang yu, Li yiChou, Zhang xiao. shong, Zengjiazhi, "A Method of IP Traceback for DOS" IEEE 2003.

[9] Tsern-Huei Lee, Wei-Kai Wu, Tze-Yau William Huang. "Scalable Packet Digesting Schemes for IP Traceback"2004 IEEE.

[10] Vrizlynn L. L. Thing, Henry C. J. Lee, "IP Traceback for Wireless Ad-hoc Networks", IEEE, 2004

[11] S. Malliga, Dr. A. Tamilarasi, "A defensive mechanism to defend against DoS/DDoS attacks by IP traceback with DPM.

[12] HachemGuerid, Ahmed Serhrouchni, Mohammed Achemlal and KarelMittig, "A Novel Traceback Approach for Direct and Reflected ICMP Attacks" 2011 IEEE

[13] Mohammed Alenezi, Dr.Martin J Reed, "IPTraceback methodologies", IEEE, 2011.

[14] Masafumi OE, Youki KADOBAYASHI, Suguru YAMAGUCHI, "An implementation of a hierarchical IP traceback architecture"

[15] Shidong Dai, Xing Li "QuIT: quantitative IP trackbacking" 2009 IEEE

[16] Il Yong Kim; Ki Chang Kim "A resource efficient IP traceback technique for mobile Ad-hoc networks based on time tagged bloom filter."2008.

****

