INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 2)
Available online at: www.ijariit.com

Implementation of TTL based packet marking for IPV4

Kolipakula Yuvanaga Venkata Manishankar
k.manishankar44@gmail.com
Vellore Institute of Technology, Vellore, Tamil Nadu

Samayamanthula Navyasainarayana Datta
samayamantula.saidatta@gmail.com
Vellore Institute of Technology, Vellore, Tamil Nadu

D. Nagasai Shanmuka Sreenivas
nagasaishanmukasreenivas@gmail.com
Vellore Institute of Technology, Vellore, Tamil Nadu

K. Manikandan
kmanikandan@vit.ac.in
Vellore Institute of Technology, Vellore, Tamil Nadu

ABSTRACT

There are more chances nowadays for a network to be attacked the common attacks are DoS and DDoS attacks. They are mainly responsible for causing disturbances for the network. There are so many mechanisms in preventing these attacks like packet marking. This packet marking is mainly used to find the source of an attack. While solving this process, the main problem is to minimize the number of IP packets used in the tracing of the attacks. The number of packets that are beginning from the individual sources is not adequate to trace back the aggressors and consequently, a proficient bundle checking plan is required in this unique circumstance. This paper focusses on finding the source of the attack using the less number of hops counts. For implementing this project we are mainly using NS2 and prove that it is more efficient than existing algorithms of finding the attacker.

Keywords— *Denial of Service (DoS), Distributed Denial of Service (DDoS), Probabilistic Packet Marking (PPM), Deterministic Packet Marking (DPM)*

1. INTRODUCTION

The growth of internet technologies increases the network from getting attacked. The common attacks are DoS and DDoS attacks. They are mainly responsible for causing disturbances for the network. This name itself indicates that it makes the networks in such a way that, the service is unavailable. The most common of this attack is flooding the target by sending more packets causing traffic to be high and make the communication slow.

There have been a lot of incidents in the technology field where this kind of attacks happens like Yahoo, Google etc. Identifying the attacker is the key issue nowadays. For this IP packet tracing is used, this helps in finding the attacker. The DDoS attacks are distributed in nature, they flood the victim by sending the packets continuously to the victim. The effectiveness of an IP traceback mechanism mainly depends on a number of packets involved in finding the attacker.

2. EXISTING METHODS

2.1 Edge sampling

In Node Sampling methodology it is seen that only a single router marks the packet with a probability in the path of its travel from source to destination. It is difficult for the victim to determine how far the marking router is. Edge Sampling overcomes this problem. In this packet marking technique, two routers mark a packet forming an edge. A packet participating in a network employing Edge Sampling should be able to accommodate two 32 bits space, i.e., 64 bits to store the routers' addresses and also an additional 8-bit space to store the distance between the marking routers.

In this technique every router that receives a packet it chooses a random number among 0 and 1. If the selected number is less than the marking probability, then the router inserts its 32-bit address into the first address space and sets the distance field value to 0. If the selected value is greater than the marking probability and the distance field equals to 0, then the router understands that the packet was marked by the previous router and inserts its 32-bit address into the second address space forming an edge between the previous router and the current router. If the router decides not to mark the packet, it increments the distance field value. The distance field provides the distance between the victim and the edge marking in the packet.

$$E(X) <= ln\ (d)/p\ (1-p)^{d-1}$$

Where d is the number of routers the packet has to pass into the destination from the source and p is the probability of the packet at each router which is marked.

2.2 Probabilistic Packet Marking (PPM)

It is an extension to the Edge Sampling method. There is not enough space available in a packet header to store the address of a router, which is of 32 bits. Instead, the address is fragmented and stored into the packet headers. The forwarding mechanism of routers probabilistically marks the packets with fragments of its identification. The marked packets contain only partial information of the path. This reduces the storage

overhead in the packets. The receiver has to receive enough number of packets to construct the path, as each packet contains only partial information of the path.

The minimum number of packets required to construct the path can be obtained using

$$E(X) <= k\ (ln\ (KD)/p\ (1-p)^{d-1}$$

Where,

k is the number of fragments is fragmented into the address of the router

d is the number of hops or nodes the packet has taken to pass into the destination from the source

p is the probability of packet which is marked

2.3 Node append

It is one of the least difficult packet marking methods. In this method, the total course gone by the packet is recorded. Each node the packet travels through annexes its location to the packet. This data causes the intruder to develop the way to the intruder.

This method for packet marking is strong in nature. The sufferer requires only one packet to follow the sender of the packet. Be that as it may, this technique has certain constraints. Since each and each node annexes its location to the packet, this builds the overhead at each node in the network. The separation from the source so there is a destination not known, as the way of movement for a packet may change during the course because of different network conditions. Hence it is beyond the realm of imagination to reserve enough space on the packet to suit the movement way of the packet to the destination. The intruder may fill the space with misleading data regardless of whether enough space is guaranteed in the packet.

2.4 Node sampling

It was introduced all together with decrease the router overhead and likewise the space in a packet to record the location of each switch it goes through. In this technique, each packet contains enough space to store the address of a single router. As a rule, the size of a router address is 32 bits if there should arise an occurrence of an IPv4 organize. Each node or a router in a network contains the packet marking algorithm, which depends on a likelihood to check the packet or not.

The likelihood is picked randomly by the node. In the event that the likelihood of the algorithm is to check the packet, at that point, the node embeds its 32-bit location into the packet and advances it to the following node in the network. A packet which is once set apart by a hub isn't checked again by some other node in the network.

After sufficiently accepting a number of packets, the receiver can develop the way dependent on the markings on the packets received. So as to develop the way to the sender, the receiver should gather packets set apart by every single diverse hub in the way to the sender. As the movement way of the packet isn't predefined, it winds up hard to locate the definite number of nodes in the way reconstruction. Another confinement of this packet checking marking is that the likelihood of marking is either 0 or 1, which implies the likelihood of marking is 0.5.

Thus it progresses toward becoming hard to accept that the node denotes the packet at cases. The sender should also send enough number of packets required to develop the way. The assumption of a single course for the packets to cross is certainly not a good assumption to actualize this method.

2.5 Deterministic packet marking

Deterministic Packet Marking is a packet marking technique. In DPM the edge routers which are nearer to the source of the packets are utilized to check the packets. In this component, the edge routers are considered as interfaces. These interfaces can distinguish among approaching and active packets. At the point when a packet is sent onto the network through this interface, it is considered as an approaching packet. When an approaching packet touches base at an interface, the interface address is put away in the parcel. For the most part, an interface address is of 32 bits length. A single packet can't convey all the 32 bits of information, which over-burdens the packet header, so the marking information must be fragmented. It requires 16 bit of packet header space and 1-bit space to store the flag value. Accordingly, it requires 17 bits of the room altogether to store the interface data.

The location of the interface is isolated into two sections, each comprising of 16 bits, i.e., 0 - 15 bits also, 16 - 31 bits. When a packet lands at the interface one of these two sections is put away into the packet header. The piece of location to be put away is picked deterministically. The flag piece is set to 0 in the event that the 0 – 15 bits of the location is put away into the packet, else the flag piece is set to 1 if the 16 – 31 bits of the location is put away into the packet. When these two packets land at the goal, the IP address of the interface is recovered by reassembling the location parts dependent on the banner bits of every packet.

3. METHODOLOGY

The Internet is a vast network of an interconnected network serving a large number of clients. On a normal, the greater part of the packets on the internet takes at most 25 hops to achieve the goal.This has been affirmed by a few tests performed in Appendix A. Therefore, this value is viewed as the edge an incentive for the Hop-Based packet marking algorithm which assumes a vital job.

The usefulness of a router implementing the packet marking method appears in Figure1. Each router in the network executes this packet marking algorithm after getting the packet also, marks the packet or passes it, in view of the yield of the algorithm. The receiver may require just packets with one of the kind markings of all the got packets to developing the way to the source or intruder. This may be equivalent to the all-out number of hops between the source and the destination.

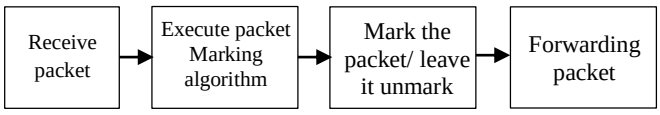


Fig. 1: Packet marking method

3.1 TTL based packet marking algorithm

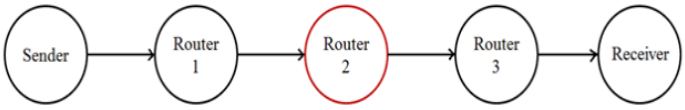
The framework for TTL-Based packet marking algorithm has been adapted from the paper It uses the Identification field of the packet header in an IPv4 datagram shown in Figure 4 to store the identification data of the routers. The stored information is known as the marked data. The length of the Identification field is 16 bits. It is split into two parts to store the stored node's identification data (SRK) and the Packet Hop Count (PHC). The Packet Hop Count (PHC) is used to determine the number of hops between the marking router and the destination. Time to Live (TTL) value depicts the life of the packet on a network in terms of hops. It is known that every router decrements the TTL value of the packet before forwarding the packet to the next router.

3.2 IPV4 Packet Header

Initially, the PHC is set equal to the Time to Live (TTL) value of the packet by the source. Stored node (SRK) field is used to store the information of the marking router. In order to understand the behaviour of the fields PHC, MRK and TTL, consider a scenario of a source, sending a packet to a receiver which passes through intermediate routers Router 1, Router 2 and Router 3 as shown in below. Let Router 2 be the router which marks the packet.

Table 1: IPV4 header format

Version	Header length	Type of Service (TOS)	Total length	
Identification			Flags	Fragment Offset
TTL	Protocol		Header checksum	
Source address				
Destination address				



TTL=20	TTL=19	TTL=18	TTL=17	TTL=16
PHC = 20	PHC=20	PHC = 0	PHC=1	PHC=2
SRK= -1	SRK=-1	SRK=2	SRK=2	SRK=2

Fig. 2: Behavior of the fields PHC, SRK and TTL

3.3 Behavior of the fields PHC, SRK and TTL

- The values of the fields SRK and PHC of a packet will not change until the packet is marked through the value of TTL decrements for every node or hop.
- The Router 2 that marks the packet by inserting its identification data into SRK field, sets the value of PHC to 0 and the value of TTL decrements as usual for every hop.
- After the packet is marked by Router 2, the value of PHC is incremented by 1 unit and the value of TTL is decremented by 1 unit for every hop, while the value of SRK is not altered.

From the above figure 1, the receiver can identify that the router with identification value 2 (SRK = 2) has marked the packet is 2 hops away (PHC = 2). If the packet is not marked by Router 2 the values of PHC and SRK remain constant all the way. The receiver can identify the hop distance between the sender and the receiver from the difference of PHC and TTL of the unmarked packet.

An intermediate router upon receiving the packet checks if the packet has been marked or not. If the packet has not been marked then the router selects a random number 'x' between 1 and 20 (threshold value). The value 20 is considered maximum for the random number selection as most of the packets on internet reach destination in 20 hops.

The packet ID is a unique ID assigned to the packet by the source. A modulus operation is performed on the packet ID with 'x'. Hop count of the packet at the current router is obtained, which is the difference between the Marked Hop Count (PHC) and Time to Live (TTL). If the hop count is equal to the result of (the modulus operation) + 1, then the packet is marked. Here the value of modulus operation is incremented by 1 as the hop count can never be equal to zero.

Consider the values TTL = 20, PHC = 20 and packet ID = 66 of a packet received by a router. Let the random number generated be x = 10, so the result of the operation (packet ID % x) + 1 is 7, which is equal to the hop count (PHC – TTL). As the marking criterion is satisfied the packet is marked by inserting the router's address into the SRK field of the packet and sets the Packet Hop Count (PHC) value to 0. If the hop count is not equal to the result of (the modulus operation) + 1, then the router forwards the packet to the next router. Consider the values TTL = 16, PHC = 20 and packet ID = 163 of a packet received by a router. Let the random number generated be x = 15 and the result of the operation (packet ID % x) + 1 is 14, which is not equal to the value of the hop count (PHC – TTL) = 4. So the packet is not marked and forwarded to the next router in the path. If the packet has already been marked, then the router increments the Packet Hop Count (PHC) value of the packet by one unit and forwards it to the next router in the path.

3.4 Algorithm

```
if the packet is not marked
select random number 'x' between 1 and 20
            hop count=PHC-TTL
if ((packet ID %x)+1==hop count)
  insert router address into the packet header
     set PHC=0
       end if
else
      increment PHC
end if
```

The receiver can distinguish between marked packets and unmarked packets from the information available in the SRK field of the packet. The address of the router that has marked the packet and the Packet Hop Count (PHC) can be obtained from the marked packets. The PHC values of the marked packets depict the number of hops between the router that has marked the packet and the receiver. Based on the values of SRK and PHC fields of the packets received path to the source can be constructed.

4. IMPLEMENTATION

This procedure was actualized and tried on a reenacted system utilizing Network Simulator prominently known as NS-2.

NS-2 is an event-driven simulator used to contemplate continuous systems. It is utilized in the vast majority of the systems administration looks into. It underpins recreation of different conventions over a wide assortment of systems, for example, wired, remote, satellite, and so forth.

NS-2 comprises of two languages to be specific C++ and Object-oriented Tool Command language (OTcl). C++ is the backend, while OTcl is the front end. The frontend, backend is connected together utilizing TclCL. The client's program is written in Tcl and it is given to the test system utilizing the direction 'ns' followed by the content name. The file content is read by the simulator and simulates a network related to real events provided in the code.

Now NS-2 generates a file after the completion of all the events of the simulation. This file makes the user to better understand the scenario involved in the simulation. NS-2 underpins a network animator called NAM. This gives a clear graphical picture of the file. For showing the packet markings on the file, the file format is modified as shown in fig. The network animation is shown on the display which provides a clear view for the user with some buttons likes forward, play, rewind, stop etc.

The results from the file can be obtained using script language called as AWK. The result can also be obtained by using some Linux commands called "grep".

NS-2 can be installed on a windows environment as well as on UNIX environment. But in windows, the user has to use a UNIX emulator called "Cygwin".

5.1 Simulation

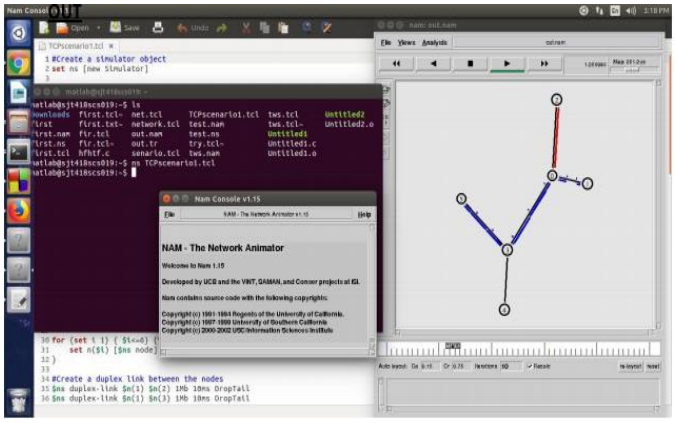


Fig. 3: A simulated network with 6 nodes

The implementation of the algorithm in a simulated network shown in figure 3. The simulated network has 6 nodes interconnected to each other. Here in this fig node 0 acts as a source of the packets and node 5 are the destination in the simulation. This network is related to the real-time environment. Every intermediate node acts as a router.

Each and every node present in the network is related with the packet marking algorithm. If a node receives a packet a code executes before forwarding the packet to the next intermediate router.

The algorithm is included in the ns-2 simulator. So all the nodes present in the simulated network execute the technique. We can start the simulation by clicking the play button in the menu bar in ns-2. After starting the simulation, the node 0 tries to send the packets to its next intermediate nodes and this process continues until the packet reaches to its desired destination. The blue colour in the simulation indicates the flow of packets from one node to another node.

4.2 Mechanism to trace the packets

The markings present on the packet helps the receiver to trace the path how and from where to where the packets are transmitting. Now after completion of simulation, all the data will be recorded into the trace file. By analyzing the trace file the receiver can construct the path from source to destination. Each and every packet consists of a unique packet marking. We included a term called Packet Hop Count (PHC). This represents the number of hops or routers present in between the marked packet router and the destination.

4.3 Sample trace file

r 0.321 24 25 cbr 500 ---------- 1 0.0 25.0 2 692 20 PRK : 0 PHC : 19
r 0.424 24 25 cbr 500 ---------- 1 0.0 25.0 5 729 20 PRK : 4 PHC : 14
r 0.512 24 25 cbr 500 ---------- 1 0.0 25.0 6 772 20 PRK : 6 PHC : 8
r 0.558 24 25 cbr 500 ---------- 1 0.0 25.0 10 802 20 PRK : 11 PHC : 10
r 0.642 24 25 cbr 500 ---------- 1 0.0 25.0 14 843 20 PRK : 8 PHC : 6
r 0.756 24 25 cbr 500 ---------- 1 0.0 25.0 26 895 20 PRK : 13 PHC : 4

Here 692, 729, ---- indicates the unique id of the packet, 20 – indicates the TTL value

Here TTL value is 20 PHC is 19 it indicates that 7 hops are away from the destination. At last with the available information, the receiver can construct the path to the source.

6. CONCLUSION

- Most of the existing packet marking techniques requires a huge number of packets to trace back the source. They also have drawbacks such as router overhead, packet header overload, network overhead, etc.
- This project is to reduce the number of packets involved across the efficient traceback using Hop-based packet marking technique.
- Our paper ensures that the receiver requires packets marked with unique data
- Equal to the number of intermediate routers between the source and the destination.
- The algorithm can be enhanced in terms of security constraints, such that an attacker cannot modify any marked information on the packet.
- The algorithm should be extended to IPv6 packet, as today IPv6 is widely in use.

7. REFERENCES

[1] [NS Manual] The ns Manual Available: http://www.isi.edu/nsnam/ns/doc/index.html Last Accessed: June 5, 2012
[2] M.T. Goodrich Probabilistic packet marking for large-scale IP Traceback IEEE/ACM Trans Network, 16 (2008), pp. 1524
[3] D. Dean, M. Franklin, A. Stubblefield, An algebraic approach to IP Traceback. ACM Transactions on Information and System Security, 2002; 5: 119–137.
[4] S. Yu, W. Zhou, S. Guo, M. Guo, A feasible IP traceback framework through dynamic deterministic packet marking. IEEE Transactions on Computers, 2016; 65: 1418–1427."CERT Advisory CA-2000-01: Denial-of-Service Developments," Computer Emergency Response Team, http://www.cert.org/-advisories/-CA-2000-01.html, 2006."CERT Advisory CA-2000-01: Denial-of-Service Developments," Computer Emergency Response Team, http://www.cert.org/-advisories/-CA-2000-01.html, 2006."CERT Advisory CA-2000-01: Denial-of-Service Developments," Computer Emergency Response Team, http://www.cert.org/-advisories/-CA-2000-01.html, 2006.
[5] K. Park and H. Lee, "On the Effectiveness of Route-Based Packet Filtering for Distributed DoS Attack Prevention in Power-Law Internets," Proc. ACM SIGCOMM "01, pp. 15-26, 2001.

