Journal of Theoretical and Applied Information Technology
10th November 2014. Vol. 69 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

DDOS AND DOS PARALLEL ATTACK TRACEBACK BY SPATIAL MARKING TECHNIQUE

[1]PERIYASAMY.S, [2]DURAISWAMY.K

[1]Assistant Professor, Department of IT, K.S.R. college of Engineering

[2]Dean, K.S.Rangasamy College of Technology

E-Mail: [1]yesperiyasamy@gmail.com, [2]deanac@ksrct.ac.in

ABSTRACT

The usage of internet is increased day by day when compared to past days. Because of this increased internet usage, the possibility of loss of data and cause for providing security to the information in the system is increased. It leads to the blocking of services results in Distributed Denial of Service (DDoS) attack. It is identified as the very harmful threat to internet user and information server. But the router and routing mechanism available in the network makes the trace back process very difficult. Till now, no paper deals with efficient trace back of source of attack for DDoS attack. In this paper, we propose a spatial marking trace back scheme for finding DDoS intruders based on geographical landscape identification information. The information's identified are utilized for the efficient routing of the packets. Also, a comparison with existing trace back methodology like Geographical Divisional Traceback and Directed Geographical Traceback is also proposed.

Keywords: *DDoS, Spatial marking, Network Security, IP Traceback, Divide and Conquer.*

1. INTRODUCTION

In the present running world, there are lot of problems arises in the security issues and trustworthiness. It is very difficult for an ordinary person to differentiate with the trust and trustless people. To get the accessibility, every user must prove them as a legal user and provide proper authentication.

Denial of Service is the problem of legal user and the hackers to prove themselves as a trusted client in the network in order to access to the information server. The Server gets confused in finding out the valuable user and differentiates them from the attackers whom are the victims for the Denial of Service (DOS) attack. DOS is an attack by intruder who is ambitious to make the server very slow in respond to the intended user's request from the single system. Being in this internet world, it is extremely difficult to get away from Distributed Denial of Service (DDoS), where attack is by number of zombies across different part of the network termed as Distributed Denial of Service (DDoS).

Also it is necessary to trace back the source for DDoS attack to prevent the further attack from the same source again in future. DDoS attacker generates an ample number of requests through zombies in a wise way to damage the victim. Due to this multiple links of attack, the IP address of intruders is critical to identify. There are parallel researches on DDoS prevention, DDoS filtering and DDoS detection have been in progress, but less effort is made to trace the IP address of the DDoS attacker.

In this study, we come up with the approach of inserting information in the bits along with the packet which is send from each client browser to the router. For the identification of IP address of intruders who attempt for DDoS attack, our proposed method is used. To trace back the IP address for DDoS defense methodology, Spatial Marking Technique (SMT) approach is proposed. In this, the entire world can be divided into continental division, a separate region, which is a required strategy to mark some information into the individual packets while up streaming it to the router. This technique announces Area Indication Pointer (AIP) to identify the location of DDoS attack. It easily traces back the source of attack which is responsible for the DDoS attack. AIP parameter is taken with the help of DDoS defense methodology. By this, IP spoofing can be detected and the origin for DDoS attack can be easily identified. In this approach, trace back of DDoS attack IP address is proposed. This proposal contains various advantages over the easy trace back of intruders and enhanced features with the time efficiency and prevents next DDoS attack from the same machine again in future.

The few bits are injected in to the packet which is uploaded from each router to make the trace back of intruders with effectiveness and in next coming paragraph which gives the detailed description about the DDoS attack and the current scenario in which it happens. Also the technique involved in trace back the number of bits injected to the packet and about the method adopted to solve the IP trace back issues and capable to find out the concurrent attack from various part of huge network. The method which is used for the AIP and the factor that is used to trace back the DDoS attackers IP in the minimized time and its method to implement the mechanism of our approached method for the parallel and concurrent trace back.

The remaining part of this paper discusses about the inter-level work of DDoS attacks and the comparison factors for the IP trace back and how this DDoS attack has made the service delay and its parameter to trace back the intruder by the packet send by them and basic methodology and technique used in trace back of attackers machine.

2. BASIC ATTACK MECHANISMS AND THE METHODS USED

2.1 DDoS Attacks

DDoS attack which is severe in the modernized internet world. The increase in usage of internet cause more traffic to get the services quick than few years before though using high speed network. DDoS attacks are targeted on the victim's fame and on their resources to reduce the bandwidth of victim's network, to waste computer power and efficiency and to increase the delaying time. The attack which is severe threat to large organizations, the client and the user had greatly increased. Because of this, the delay to provide service has increased. Also the preventive mechanism to overcome this attack is very difficult because of increased traffic and the new latest technology has adopted for data transmission in the large network. To do a DDoS attack, the attacker(s) first has to setup a network(s) of computers that is used to generate the enormous amount of packets that is send to deny the service of the victim and their actual user. To launch this attach on the victims, the attackers should find vulnerable host. Vulnerable hosts are the machine that has no antivirus, firewall programs or the antivirus without updated or system with any proper protection. And these are found out by the attacker and they install an application (tools for attack) on the compromised host to attack the large server. This host machine that has the "attack application" is called Zombies and they are used to attack the targeted server under the control of who injected the "attacking application" in the host machine as depicted in Figure 1. The large amount of Zombies together called botnet.

In this DDoS attacks, the attack of the victim is done by either the attacker who orders the zombies to run the attacking application which sends huge volume of packet to victim machine and makes delay in providing the service. Figure 2 shows the attacking of the victim machine induced by the attacker with the help of zombies.

When thousands of request are received from hundreds of zombies, or by master(attacker) send the packet which request for service of victim to its zombies with destination IP as victims IP which in turn send vast number of request to victims machine and attack by denial of services to legitimate users of the service.

2.2 Methods used in the Approach

Understanding the DDoS attack is very critical to find and to overcome. This proposed method will do four basic works against the attacks namely: detection of injected packets, isolation of those packets, Trace back of attacker and prevention of further attacks from the same attacker again. Mainly researches were undergone in the area of DDoS attack trace back but this study is completely based on the IP address of the attackers who had generated the DDoS attacks from the zombies. This paper not only deals with the IP trace back of master (attacker) but also provide mechanism to prevent further attack from the same intruder again. It should be necessary to hunt the IP address of the attackers and zombies. The summary of present DDoS trace back methods are discussed but not the efficient way to trace back the IP of the zombies and attackers

Approaches for DDoS attack mitigation and detection are Directed Geographical Trace back (DGT) which contain subfields that is to denote geographical direction and it takes more amount of bits to represents the location and the router needs to inject these bits in the packets that are from the client. If the attack is detected through the injected address of the victim machine, we can effortlessly locate the attacker by the direction of the attack through the direction field.

Another method is Geographical Division Trace back (GDT) which also inject few bits in the packets that are send via router. It divides the earth in to 4 parts and each part is sub-divided in to 4 again and repeats this until single router and corresponding part which has the 2 bit binary value and that is injected to the each packet by the router.

The main drawback of GDT and DGT are, it takes more bit in the packet which is send a router and it takes more time to trace back the infected packet and also cannot work for router which contain more than 8 interfaces because of only two bits available in the packet and it cannot be used for spoofed marking, but Spatial Making Traceback (SMT) which is for concurrent and parallel trace back in which only less bits are injected to the packets and for packet making and spoofed making packets to identify the infected packets takes less than 15 seconds in approximation.

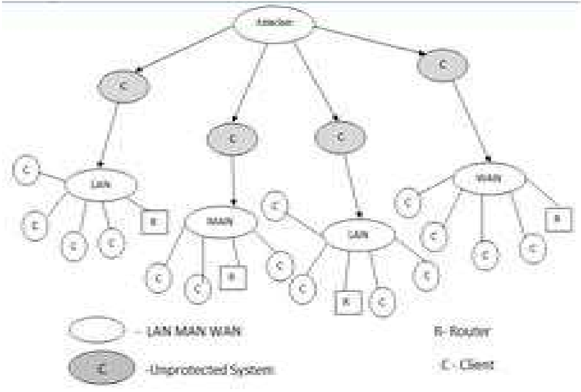


Figure 1: Sample network which is attacked by attackers by inject on "Attacking Application"

In packet making, the packets are marked with the routers IP address information's which mark the information of the local routers and if the packet is traced which is difficult to trace back the actual attackers or zombies by the reconstructed path of the attackers packet which is shown in figs and it takes more space to construct the attack tree by its algorithm. Also by the way attackers can choose spoofed marking technique. The information to the victim goes wrong by this spoofed making and this paper deals with the efficient trace back which is done in the very less time and to preventing the same attacks again from the founded attackers.

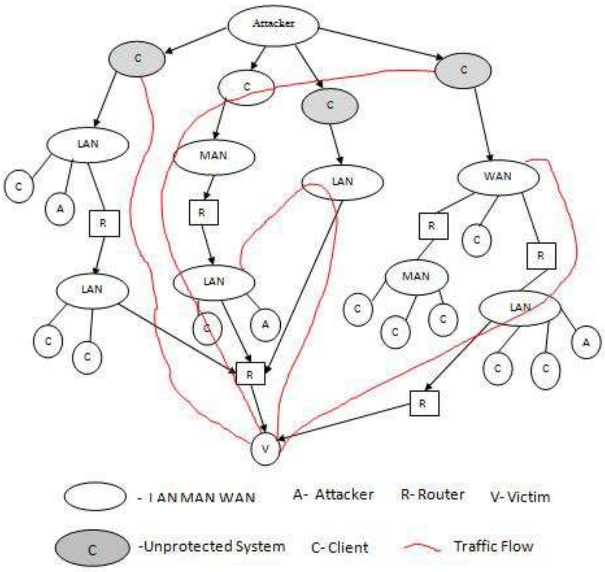


Figure 2: A Sample DDoS attack induced by attackers to attack victim through zombies.

Probability based packet marking method is introduced in which it add the address of each node at the end of the packet from the attackers to the victims which when the DDoS attack is detected. Long tree is used to found the source of attack and which has unused space in original packet and in randomize and link approach[22] for trace back of IP address based on probabilistic packet marking mechanism and many packet marking technique to trace back but not the efficient way to trace back the IP address of the source attacker.

2.3 DGT and its problem:

"Diagnosis of Attack" (DOA) and Parallel Attack Traceback (PAT) are the technique used in this paper for having the efficient trace back of the attacks from different machine by the parallel trace back mechanism.

0	4	8	16	19	31
Version	IHL	ToS	Total Length		
Identification				Flags	Fragments
			Header Checksum		
Source IP address					
Destination IP address					
Option field (if any)					
IP Data					

Figure 3: IP Header Utilized in DGT

In Directed Geographical Traceback (DGT) [2], mitigating the DDoS attack and the detection is proposed. It needs an additional field to mention the direction of the source for attacks. It has to include possible geographical direction information and the path length through which the injected packet travels which takes more than 32 bits. The bit availability for the Spatial Marking technique is shown in the Figure 3.But by DGT we need 40 bits to represent each direction and it takes more time to trace back the source IP and if the source IP is spoofed, victim can find relative location by the direction field when the packet arrives nearer. The main limitation is it will not work well when the router has more than 8 interfaces. Also spoofed marking cannot handle well and it has the major concerns over the trackback by DGT.

2.4 GDT and it s problem:

Geographical Division Traceback (GDT) uses 25 bits for storing GDT information of the each packet which is send by the attackers or zombies through the router and it is injected by the first router in the packet while transmitting from intruders to router. The world is divided in to 4 equal parts and each large part is subdivided in to 4 equal small parts and this division is done till the earth area is available under the traceable area and the bits to represent the India is given in Figure 4.

0	1	1	0	0	1	-	-	-	-	-	-	-	-

Figure 4: Bit indication by GDT

The main disadvantage of using GDT is that in which the India is not completely represented by 011011 also the above part which takes 011001 which also have few north parts of India, by the bits we cannot locate the entire parts of the country. We can only locate the place through particular router and it takes more time than the existing system. Also it takes more number of bits to represent the value for the GDT information and the memory in the packet is wasted.

2.5 Description of Spatial Marking Technique:

The adapted method which are facing the layer problem in mitigating and trace back of the IP by the various discussed techniques [1] [2]. But our proposed spatial marking technique uses the method of allocating the number to the each continent. There are 7 continents in the world which in turn it takes only 3 bits to represent each of the continent by the corresponding binary bit value from 000 to represent the first continent, 001 to represent 2nd continent and so on upto 110 to represent 7th continent shown in the Figure 5. Each continent has many countries in it and the maximum of 56 countries present in the continent, which in turn takes 6 bits to represent it such that 2^6 leads to 64 values for representation is depicted in Figure 6. If the country is identified, the states which can be found by providing another 6 bits, the maximum of 58 states in the country is represented by 2^6=64 representing by giving the value to state by 6 bits and thereby giving 6 bits to found the inner district within the each state. 2^6=64 bits which is used to represent each district presented in a state as shown in the Figure 8. With the help of location information, the attacker who sends the infected packet to the victim is identified.

Figure 5: Numbering continent by Binary value.

Only 20 bits are needed to represent the attacker's information injected by the first router from which the packet is transferred from the zombies or attackers machine in to the network. Only with the help of small number of bits, we can able to trace back the zombies who is very efficient to send the injected packet in the network and the information injected to each and every packet which is transferred by the router in the network.

This information helps to find out the exact location information of the victim which is responsible for the entire network processing delay. The information retrieved from the router helps to trace back to the victim machine located in the different network.

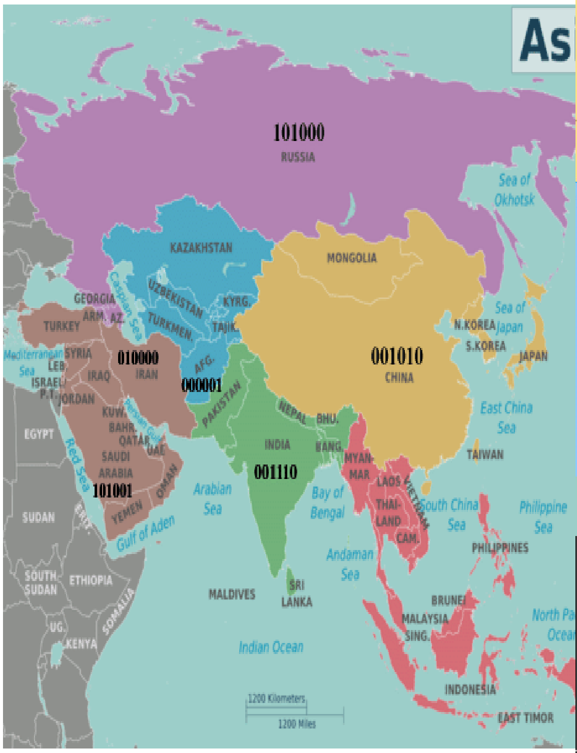
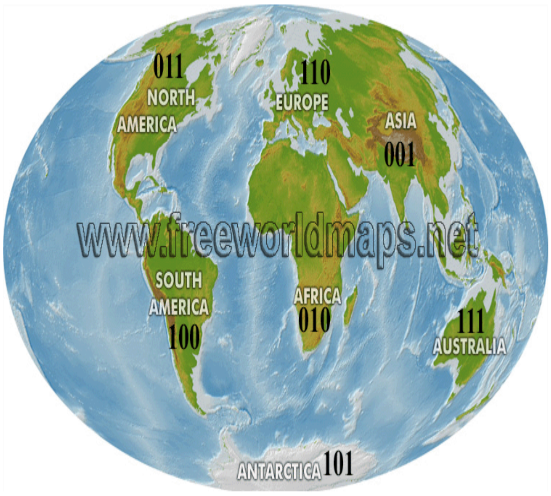


Figure 6: Numbering country of Asia by Binary value.

The time taken by the victim which when diagnosis the attacks by the intruders and the zombies takes only less than 15 seconds (approximately) to trace back the attackers machine. Based on the minimum time, if takes 7 seconds (minimum) to locate the attackers machine, we can stop the further attacks from the same attacker at the minimum amount of time. Also this proposed system which contains the capability to locate the attacks from the parallel and concurrent attackers. Because of the injected packet, once the attack is diagnosed, then the source runs the efficient method of SMT to trace back all the attackers within 15 seconds (approximately) in hitting the source.



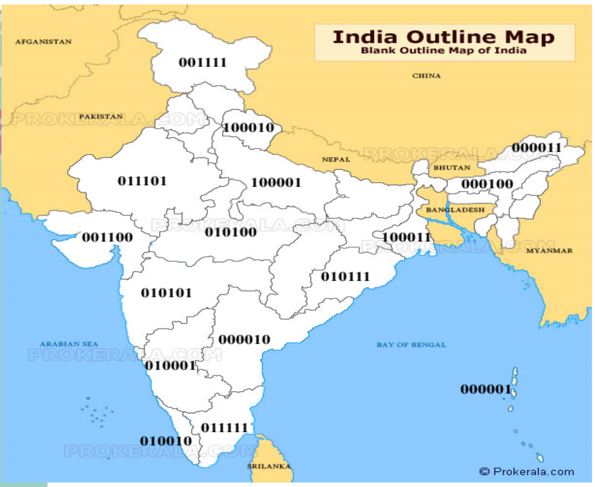


Figure 7: Numbering States of India by Binary value.

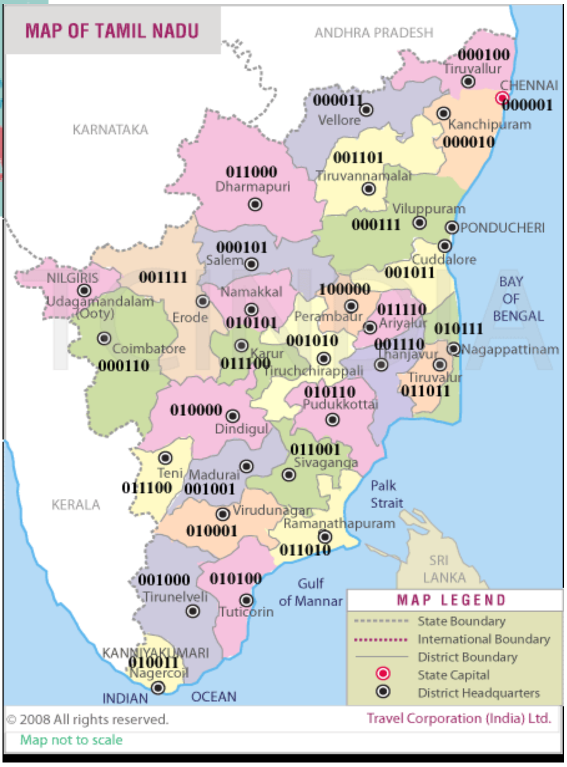


Figure 8: Numbering Districts of Tamil Nadu.

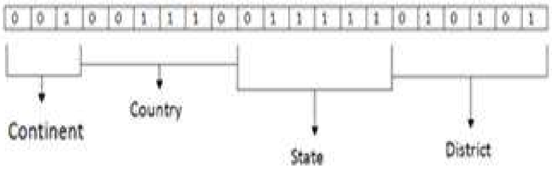


Figure 9: Bit Representation in header memory for effective traceback of zombies by SMT

3. MODELING USED IN THE SPATIAL MARKING TECHNIQUE

3.1 SMT Principle:

Directed Geographical Trace back (DGT), Geographical Division Trace back (GDT) and AD attack diagnosis and Parallel Attack Diagnosis (PAD) paves the way to give the new scheme of Spatial Marking Trace back (SMT). As per SMT, the packet which is having the malicious program to generate the DDoS attack is identified by using Attack Diagnosis (AD) and PAD techniques [4] and that are used to trace back, once it is found. IP address from which this request had sent, need to be traced by the victim. To trace back the address of the attackers, the victim need not to use source IP address so that the victims IP address can be spoofed, it can generally trace back by our proposed mechanism and the steps which is involved in our proposed trace back methodology are

1. In earth, each continent is provided with binary number for its identification.
2. Assign the identification for each continents, country, states, and districts.
3. Each space which has unique binary value.
4. Based on all the information bits, the place from which malicious send of packet is identified.

The network and the traffic are to be in the below order to name the spatial marking techniques. They are

1. A single attacker may produce any number of malicious packets.
2. The malicious packet from the attackers may be small.
3. Routing behavior should be stable.
4. Attackers may conscious that they can be tracked.
5. They provide no information about them into the security mechanism.

This trace back is for providing the security to prevent the attacks from the same attackers again. This is to consider the entire network which has only the fixed routers and we can assign the value to the each router by spatial marking technique and their Area Identification Pointer (AIP). Each packet which is send from the router is injected with AIP. To trace back the infected packet, this gives the default numbering to all the continents' in the earth. Each continent takes the individual bit from 000, 001,010,.....110 and the 3 bits in addition to represent the continents and the next 6 bits which are used to represent the country in the continent.

Example: 001 001110 011111 010101.

1st 3 bit 001 which represent Asia. 2nd 6 bit 001110 represents India. 3rd 6 bit 011111 represents Tamil Nadu. Last 5 bit 010101 represents Namakkal.

3.2 Bit representation for SMT:

Each bit represents the individual location in the earth, through by which the routers are needed to inject the bits based on their location in which less than 20 bits are sufficiently needed to locate the accurate location and their exact place from which the attack have been initiated to attack the victim. The sufficient trace back technique which takes only fewer bits to be injected from the router to the packets from machine which sends packets.

Table 1: Bit representation of continents.

S.no	Bit Value	Continent Name
1	001	Asia
2	010	Africa
3	011	North America
4	100	South America
5	101	Antarctica
6	110	Europe
7	111	Australia

Table 2: Bit value for country in Asia continent.

S.no	Bit Value	Country Name
1	000001	Afghanistan
2	000010	Armenia
3	000011	Bahrain
4	000100	Bangladesh
5	000101	Bhutan
6	001101	Hong Kong
7	001110	India
8	001111	Indonesia
9	010000	Iran
10	101000	Russia
11	101001	Saudi Arabia
12	101010	Singapore
13	110111	Vietnam
14	111000	Yemen

AIP will be encoded in the IP header when the packet enters the first router from the attackers or zombie's machine. Area Identification Pointer (AIP) is nothing but a bit which is assigned to each continent country and the state.

Table 3: Bit value for District in Tamil Nadu state.

S.No	Bit value	District name
1	000001	Chennai
2	000010	Kancheepuram
3	000011	Vellore
4	000100	Thirivallur
5	011101	Karur
6	011110	Ariyalur
7	011111	The Nilgris
8	100000	Perambalur

Each assigned bit is constant for the router by which the informations about those routers are traced with less of time. Few amount of space is needed in the IP header which is used to trace back the intruder in less time of 7 sec (minimum) because it is only for the fixed routers. AIP stored in the system is just mapped with the location of attackers and are easily found with the information which is injected in the each packet by the first router.

3.3 Time for Attack Detection:

The time which in needed to detect the location is only considerable because the each of the spatial location is stored in the entire server which is targeted to prey for DDoS attack. The server compare the stored data in it with the AIP in the packets send by the source of attackers. Once the victim IP address is recognized that is it being for DDoS attack, it compares the AIP with the stored spatial marking data. It takes first 3 bit to identify the continent from which the packet was send once it identified the continent, from the next 6 bits, server will identify the country by that recognized continent information.

If the country also hit then based on the next 6 bit, the state in that country which is found and next 5 bits are used to find the district. If that is found and the server which do found the router and important thing is to find the machine from which the malicious packet had been send to make DDoS attack.

This takes lesser time of 7 seconds (minimum) if the server is not busy in offering its service. If server is hectic to hit victim machine with the attackers machine takes 15 seconds (maximum) and that is found based on the mechanism and it stop the further DDoS attack from the same machine through the algorithms that is given to the router to ignore such type of request again from the same machine. Also the victim who is capable of hitting the parallel attacks and to found the source for all the parallel attacks is simple by using spatial marking technique.

3.4 Algorithm to Trace back Source

In the proposed method, the entire world is divided into continent by the bits in the first iteration .Once the continent is identified then that the in next iteration based on the continent code, the country in the continent are found by having the 6 bit value, once if country is hit and based on next 6 bit value the state of that particular country is encountered and this iteration and the looping steps which is repeated continuously till the router from which the source of the attacks has made which sends the request to do attacks. The following table represents the tracking of the intruders' location by the above algorithm.

Table 4: The Location is found by bits in zombie's packet

Continent	0		0		1	
Country	0	0	1	1	1	0
State	0	1	1	1	1	1
District	0	1	0	1	0	1

.

3.5 Performance Analysis

In this section, we evaluate the performance of the spatial marking technique (SMT) and the effectiveness and efficiency when the attacker's packets are traced by this mechanism. First in to show how our proposed system is better than the existing systems.

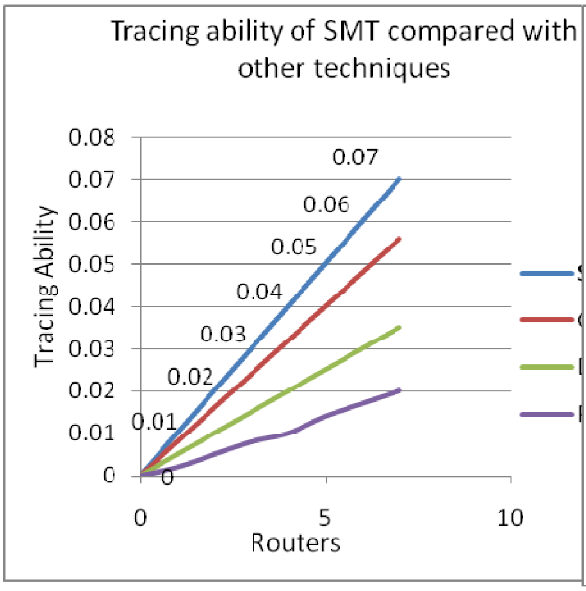


Figure 10: Comparison of SMT with other existing Techniques

Spatial Marking Technique can able to withstand at higher level when the number of routers in the country, states, and district are increased and it is based on efficiency mechanism to offer optimized results.

SMT technique helps to prevent Denial of Service attack even though having less packet memory. The extra additional memory is used to transmit the actual information and data of user and for other usage which reduces cost. The amount of bits that is needed by following SMT is less when that in following the other techniques likes PPM, DGT, and GDT. In all the existing techniques which needs to inject the minimum of 40,32,25 bits in the IP header to trace back the attackers source, but in our proposed SMT we need only 20 bits to be injected to the IP header to efficient trace back of source of the attacker with efficiency and reduced time.

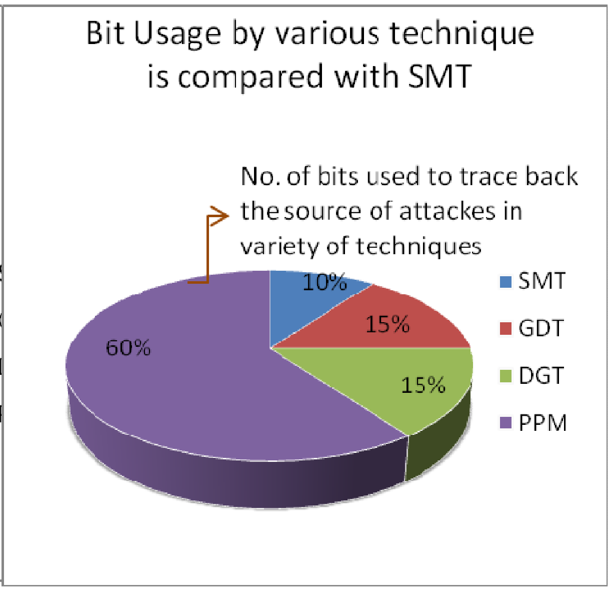


Figure 11: Comparison of bit usage of SMT with other techniques

Based on the time factor, SMT it can able to trace back in very less time than all the proposed technique of minimum 7 seconds to trace the intruders and zombies' machine.

Also finally Spatial Marking Technique which is compared with other performance like scalability, reliability, etc. And SMT is compared to trace back of other different techniques such as PPM, DGT, and GDT shown in the Figure 11. Thus the graph is shown below depicts the performance evaluations of SMT with other trace back techniques.

S.No.	**Technique**	**Scalable**	**Capability to mitigate effect of attack**	**Time**
1	PPM	Good	Poor	Very Low
2	DGT	Good	Good	Low
3	GDT	Good	Best	Medium
4	**SMT**	**Good**	**Best**	**Fast**

Figure 15: Performance Evaluation of SMT compared with other Techniques.

4. CONCLUSION AND FURURE WORK

In this paper, our proposed technique which is efficient and effective way to trace back the IP address of the attacker's methodology against the DoS and DDoS attack based on the Spatial Marking Technique and the Area Identification Pointer (AIP). It is one of the different trace back mechanisms of the fixed routers from currently using packet marking strategies. Many of the research work on IP trace back which only depend on the Packet Marking, Spoofed Marking, Probabilistic Packets Marking (PPM) or Deterministic Packet Marking (DPM). But in this internet world and of vulnerable internet, the packet marking technique which has major disadvantages such as less scalable challenges on storage space. But our proposed method has no such problem, only few bits in the IP header which is enough to inject the location of the attackers' computer.

The study of Spatial Marking Technique is the mechanism to defend an attack from thousand of hundred zombies from the entire part of the world with in a large network. The "divide and conquer" technique is used to detect the malicious request and to defense the victim again from the same attackers again.

SMT and AIP principle is capable to handle and with stand the large scale attacks from entire world are as follow:

1. Defect and trace back the attackers' source.
2. Easy to calculate AIP value.
3. No complex calculations.
4. Time taken is minimum than all existing methodology.

The future work involves the reduction of DDoS attack which makes the victim machine free from the identification of the attacker. Also helps the routers to route the harmless packets to it without affecting the efficiency and time taken.

REFERENCES

[1] Al-Duwairi, B. and M. Govindarasu, "Novel hybrid schemes employing packet marking and logging for IP traceback", IEEE Transaction on Parallel Distributed Systems, 17: 2006, pp.403-418.

[2] Al-Duwairi, B., "Novel hybrid schemes employing packet marking and logging for IP traceback", IEEE Trans. Parallel Distribution System, 2006, pp.403-418.

[3] Burch, H. and B. Cheswick, "Tracing anonymous packets to their approximate source", Carnegie Mellon University.

[4] Chen, R., J.M. Park and R. Marchany, "A divideand-conquer strategy for thwarting distributed denial-of-service attacks", IEEE Trans. Parallel Distribution System, 2007, pp. 577-588.

[5] Gao, Z. and N. Ansari, "Directed geographical traceback", Proceedings of the 3rd International Conference on Information Technology, Research and Education, June, 27-30, IEEE Xplore Press, Newark, NJ, USA, 2005, pp: 221-224.

[6] Ghazali, K.W.M. and R. Hassan, "Flooding distributed denial of service attacks-a review", Journal of . Computer Science, 7: 2011, pp. 1218-1223.

[7] Keromytis, A.D., K.V. Misra and D. Rubenstein, "SOS: Secure overlay services", Proceedings of the Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, (ATAPCC'02), ACM New York, NY, USA., 2002, pp: 61-72.

[8] Snoeren, A.C., C. Partridge, L.A. Sanchez, C.E. Jonesn and F. Tchakountio *et al.*,"Hash-Based IP traceback", Proceedings of the Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, (ATAPCC' 01), ACM New York, NY, USA, 2001, pp: 3-14.

[9] Xiang, Y., W. Zhou and M. Guo,"Flexible deterministic packet marking: An IP traceback system to find the real source of attacks", IEEE Trans. Parall Distribut. Syst., 20,2008, pp.567-580.