

Adaptive IP Traceback Mechanism for Detecting Low Rate DDoS Attacks

Department of Information Technology
R.M.K College of Engineering & Technology
Chennai, India
baashkarinfo@yahoo.co.in

Department of Information Technology
R.M.K Institutions
Chennai, India
t.gnanasekaran@gmail.com

Department of Computer Science & Engineering
R.M.K College of Engineering & Technology
Chennai, India
saran.mecse@gmail.com

Index Terms – *Internet, Distributed Denial of Service, trace back mechanism, low rate attacks, Network Security*

The Internet could be a large repository of data that has convenience, support and worth to its users. However one in every of the issues related to web is that its wide accessibility makes it extremely vulnerable to the users whose intention is to disrupt the flow of data or to use it for their personal gain. The tools for interference are unit readily accessible to the attackers, mistreatment that they exploit such vulnerabilities. A typical kind of attack is Denial of Service (DoS) attack that consumes the resources of a number or a network, thereby denying the desired service to legitimate users. Typically, the adversaries conduct DoS attacks by flooding the target network with an oversized quantity of traffic from one and within the case it's referred to as distributed DoS (DDoS) attack. Such attacks are unit among the toughest to deal with as a result of their straightforward to implement, onerous to forestall, and troublesome to trace. IP traceback strategies facilitate the network directors to spot the address of actuality supply of the packets inflicting the attack. Therefore IP traceback is significant for restoring traditional network practicality, preventing reoccurrences, and so holding the attackers responsible. Identification of the machines and networks that generate attack traffic may appear sort of a

pushover; however the essential clues that it provides will facilitate to tell apart the particular wrongdoer. Many efforts are unit below thanks to develop attacker identification technologies on the internet. There are unit two general kinds of DoS attacks like the attacks those crash services and attacks those flood services. A DoS attack might embrace execution of malware supposed to exhaust the CPU's usage, preventing any work from occurring, trigger errors within the firmware of the machine, trigger errors within the sequencing of directions, therefore on force the computer into associate unstable state or lock up or exploits the errors within the software system to cause resource starvation.

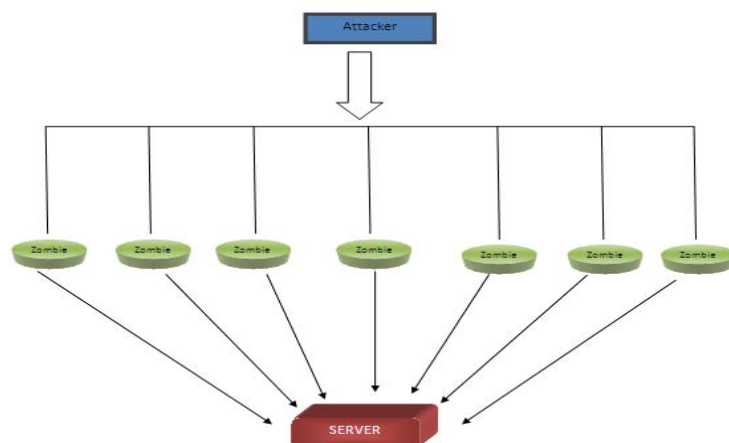


Fig. 1 DDoS attack

DDoS attacks attempt to exhaust the victim's resources. These resources may be network information measure, computing power, or software package knowledge structures. To launch a DDoS attack, malicious user's initial build a network of computers that they'll use to supply the amount of traffic required to deny services to computer users. to form this attack network, attackers discover vulnerable sites or hosts on the network. Vulnerable hosts are typically those who are either running no antivirus code or out of date antivirus code, or those who haven't been properly patched. Vulnerable hosts square measure then exploited by attackers who use their vulnerability to achieve access to those hosts. Figure 1 explains however DDoS

attack takes place during a network. Ensuing step for the trespasser is to put in new programs referred to as attack tools on the compromised hosts of the attack network. The hosts that are running these attack tools are referred to as zombies and that they will perform any attack underneath the management of the aggressor. Several zombies along kind a military, though this preparation stage of the attack is incredibly crucial, discovering vulnerable hosts and putting in attack tools on them became a really simple method. there's no would like for the trespasser to pay time in making the attack tools as a result of there are already prepared programs that mechanically realize vulnerable systems, break into these systems, and so install the required programs for the attack. After that, the systems that are infected by the malicious code search for alternative vulnerable computers and install on them constant malicious code. due to that widespread scanning to spot victim systems, it's possible that enormous attack networks may be designed very quickly. The results of this automated process are that the creation of a DDoS attack network that consists of handler, master and agent machines. DDoS attacks became associate progressively frequent disturbance of the global internet. They are terribly onerous to defend against as a result of they are doing not target specific vulnerabilities of systems of the internet. Information processing traceback means that the aptitude of distinctive the particular supply of any packet sent across the internet. Due to the vulnerability of the initial style of the internet, we have a tendency to may not be able to realize the particular hackers at the present. In fact, information processing traceback schemes are thought of roaring if they will establish the zombies from that the DDoS attack packets entered the internet.

II. RELATED WORK

In general, the trace back methods are supported packet marking. Packet marking ways embody the PPM and also the DPM. The PPM mechanism tries to mark packets with the router's ip address information by probability on the native router, and also the victim will reconstruct the ways that the attack packets went through. The PPM technique is liable to attackers as attackers will send spoofed marking information to the victim to mislead the victim. The accuracy of PPM is another drawback as a result of the marked messages by the routers who are nearer to the leaves, which implies distant from the victim can be overwritten by the downstream routers on the attack tree [7]. At constant time, most of the PPM algorithms suffer from the space for storing drawback to store great amount of marked packets for reconstructing the attack tree. Moreover, PPM needs all the net routers to be concerned in marking.

Based on the PPM mechanism, Law et al. tried to traceback the attacker's mistreatment traffic rates of packets that were targeted on the victim [12]. The model bears a awfully robust assumption: the pattern has got to adapt the distribution, that isn't continually true within the web.

Moreover, it inherits the disadvantages of the PPM mechanism: great amount of marked packets square measure expected to reconstruct the attack diagram, centralized process on the victim, and its simple be fooled by attackers mistreatment packet pollution.

The settled packet marking mechanism tries to mark the spare house of a packet with the packet's initial router's data, e.g., IP address. Therefore, the receiver will establish the supply location of the packets once it's comfortable data of the marks. The main drawback of DPM is that it involves modifications of the present routing computer code, and it's going to need terribly great amount of marks for packet reconstruction. Moreover, the same as PPM, the DPM mechanism cannot avoid pollution from attackers. Savage et al. [6] 1st introduced the chance primarily based packet marking technique, node appending, that appends every node's address to the top of the packet because it travels from the attack supply to the victim. Obviously, it's unworkable once the trail is long or there's poor unused house within the original packet.

Dean et al. [2] planned a deterministic packet marking strategy for ip traceback. each ingress router writes its own ip address into the outgoing ip packet header, and there's no a lot of marking for the packet. They used associate degree algebraical approach, originally developed for coding theory and learning theory, for cryptography traceback information. Their plan is that for any polynomial $f(x)$ of degree d within the prime field $GF(p)$, $f(x)$ may be recovered given $f(x)$ evaluated at $d+1$ unique point.

Belenky and Ansari [5] noticed that the PPM mechanism will solely solve large flooding attacks, and it's not applicable for attacks consisted of a small variety of packets. Moreover, PPM is vulnerable if hackers inject marked packets into the network. Therefore, the paper planned a deterministic packet marking technique for ip traceback. The essential plan is that at the initial router for associate degree information source, the router embeds its ip address into the packet by chopping the router's ip into 2 segments with seventeen bits each. As a result, the victim will trace that router the packets came from

Jin and rule [4] improved the ID writing of the deterministic packet marking scheme using redundant decomposition of the initial router ip address. For associate degree ip address, they divided them into 3 redundant segments, 0-13 bits, 9-22 bits, and 18-31 bits, and so 5 totally different hash functions are applied on the 3 segments to make 5 results. The ensuing eight segments are recorded within the outgoing packets indiscriminately. The victim will reassemble the source router ip using the packets it's received.

Chao Gong, et al., [1] focuses on tracing ip packets back to their origins in defensive the net against denial of service attacks. Tracing the ways of ip packets back to their origin, referred to as ip traceback, is a vital step in defensive

against DoS attacks using ip spoofing. Their approach makes associate degree intelligent use of packet marking to assist improve the quantifiability of log primarily based ip traceback. The key plan of the approach is to record network path information partially at routers and partially in packets. Whereas a packet is traversing the network, the most recent portion of the network path is recorded within the packet, and therefore the upstream portion of the path is recorded at some intermediate routers. Within the approach, looking on the availability of free space within the marking field of the forwarded packets, routers decide wherever to record network path information. If there's free space available within the marking field, routers write their identification information into the packets; otherwise, routers compute and record the packet digests and then clear the marking field. based on this concept, a concrete single-packet ip traceback approach is developed. Compared to SPIE, this approach (1) reduces the storage overhead of packet digests to at least one 0.5 and (2) reduces the access time requirement for recording packet digests by an element of $2n$, wherever n stands for the amount of neighboring routers. the disadvantage of this approach is that it will increase the memory space.

Kejie Lu, et al., [10] have mentioned the ways that to defend against DDoS attacks. The host primarily based approach will facilitate defend the server system; however it should not be able to protect legitimate access to the server, as a result of high volume attack traffic might congest the incoming link to the server. This work proposes the framework that makes use of spatial and temporal correlation of DDoS attack traffic. a fringe primarily based anti DDoS system is intended, during which traffic is analyzed only at the sting routers of a web service supplier network. The framework is capable of detecting any source address spoofed DDoS attack, in spite of whether or not it's a low volume attack or a high volume attack. The novelties of the framework square measure (1) temporal correlation based feature extraction and (2) spatial correlation based detection. With these techniques, the theme will accurately find DDoS attacks and determine attack packets while not modifying existing ip forwarding mechanisms at routers. The most disadvantage of the approach is that new legitimate users won't be allowed, i.e., packets from new legitimate users are going to be born, that could be a limitation of this psychoanalytic process.

Yoonhwan Kim, et al., [8] have mentioned the traffic analysis and control in DDoS attack. This work focuses on the look and analysis of the machine-controlled attack characterization, selective packet discarding and overload management portion of the planned design. they need provided an summary of the complete Packet Score DDoS defense design. they need planned hardware implementation of advanced knowledge stream process techniques, as well as one pass operations of iceberg style histograms and quintile (CDF) computations, to modify scalable, high speed fine grain traffic identification and per packet marking. Such theme will tackle DDoS attack varieties by providing a applied mathematics primarily based adjustive differentiation between

offensive and legit packets to drive selective packet discarding and overload control at high-speed. Their plan is to order packets supported a per packet score that estimates the legitimacy of a packet given the attribute values it carries. Once the score of a packet is computed, score-based selective packet discarding is performed wherever the dropping threshold is dynamically adjusted supported (1) the score distribution of recent incoming packets and (2) this level of overload of the system. Packet Score isn't appropriate for core network operation during a distributed manner. Packet Score doesn't work well with low volume attacks.

III. AADS ARCHITECTURE

Here we describe the architecture and the components of the Adaptive Attack Detection System.

A. Overview of AADS

We use entropy variation to measure changes of randomness of flows at a router for a given quantity. we have a tendency to notice that entropy variation is only one of the possible metrics. Chen and Hwang used a applied mathematics feature, change point of flows, to identify the abnormality of DDoS attacks [3]; but, attackers might cheat this feature by increasing attack strength slowly. we are able to additionally use different statistic metrics to measure the randomness, like normal variation or high order moments of flows. We elect entropy variation instead of others during this paper due to the low computing work for entropy variations.

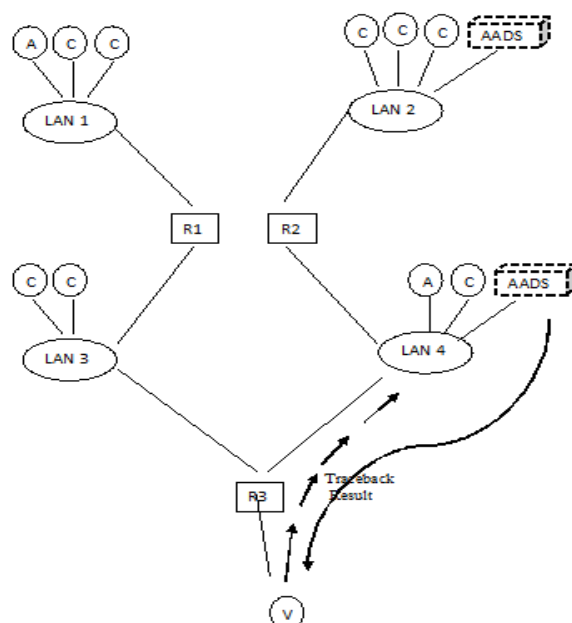


Fig.2 Architecture of AADS

Figure 2 describes however the method of tracing the supply is completed. Routers R1, R3 can notice the dramatic changes but, the routers that aren't within the attack ways, like R2 won't be able to sense the variations. Therefore, once the victim realizes an in progress attack, it will push back

to the LANs, that caused the changes supported the data of flow entropy variations, and thus, we are able to determine the locations of attackers. The algorithms used in AADS are described below

B. The local flow monitoring algorithm

The steps involved in local flow monitoring algorithm are listed below.

Step 1: Initialize the local threshold parameter, C, δ and sampling interval ΔT ;

Step 2: Identify flows f_1, f_2, \dots, f_n and set count number of each flow to zero, $x_1 = x_2 = \dots = x_n = 0$;

Step 3: When ΔT is over, calculate the probability distribution and entropy variation as follows.

$$p_i = x_i / (\sum x)^{-1}, H(F) = -\sum p_i \log p_i;$$

Step 4: Save x_1, x_2, \dots, x_n and $H(F)$;

Step 5: If there is no dramatic change of the entropy variation $H(F)$, namely, $|H(F) - C| \leq \delta$

progress the mean

$$C[t] = \sum \alpha_i C[t-i], \sum \alpha_i = 1, \text{ and}$$

the standard variation

$$\delta[t] = \sum \beta_i \Delta[t-i], \sum \beta_i = 1$$

Step 6: Goto step 2.

C. IP traceback algorithm

The steps involved in IP traceback algorithm are listed below.

Step1: Initialize set $A = \emptyset$, and obtain local parameter of C and δ ;

Step2: Let $U = \{u_i\}$, $i \in I$ be a set of upstream routers, $D = \{d_i\}$, $i \in I$ be a set of destinations of the packets and V be the victim.

Step 3: Define attack flows $f_i = \langle u_j, v \rangle$, $i = 1, 2, \dots, n, u_j \in U$, and sort the attack flow in the descent order and we have f_1, f_2, \dots, f_n

Step 4: For $i = 1$ to n

```
{
  calculate  $H(F; f_i)$ 
  if ( $|H(F) - C| > \delta$ ) then append the responding
    upstream router of  $f_i$  to set  $A$ 
  else break;
  end if;
end for;
}
```

Step5: Submit traceback requests to the routers in set A respectively and deliver the confirmed zombies information, set A , to the victim. Whenever the attack strength is less than seven times of the normal flow, low rate detection algorithm is used to detect the attack.

D. The low rate detection algorithm

Step 1: Compare $TS_{Traffic}$ and $TS_{ATraffic}$;

if ($TS_{Traffic} > ((1+\beta) * TS_{ATraffic})$) then

goto step 2

else

goto step 4

Step 2: Compare TS_{To} with T_{Con} and TS_{Tn} with $Th_{Discard}$;

if ($(TS_{To} \geq 2 * TS_{Con})$ and ($TS_{Tn} > Th_{Discard}$)) then

goto step 3

else

goto step 4

Step 3: Compare T_{IA} with T_{AIA} ;

if ($(T_{IA} \leq \gamma * T_{AIA})$) then

conclude low rate DoS attack and not congestion.

else

goto step 4

Step 4: Suspend thread processing till the end of current time slot interval.

IV. SYSTEM MODEL AND EXPERIMENTATION

The major elements of the experimental setup concerned in detecting DDoS attacks using our hybrid AADS is delineate below. The primary parts deployed are flow monitor, source tracker and attack detection agent

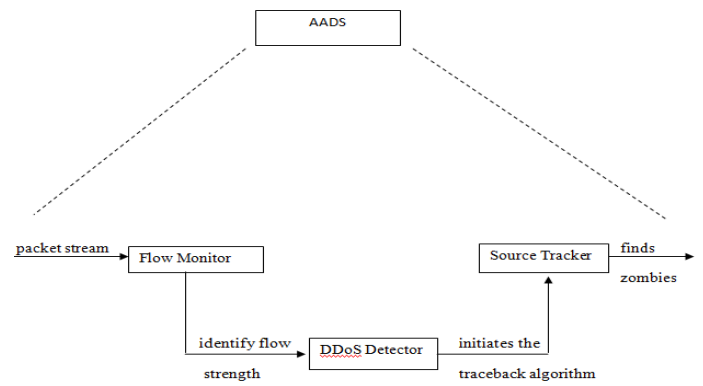


Fig.3 AADS-Internal architecture

Figure 3 describes the interior design of AADS. The flow monitor is employed to identify the strength of the flow by carefully examining the incoming packet stream. The DDoS detection agent is employed to visualize if there's an attack within the system. It also classifies the attack into high rate and low rate attack and therefore the corresponding traceback algorithm is initiated. Finally the source tracker is employed find the supply of the attack.

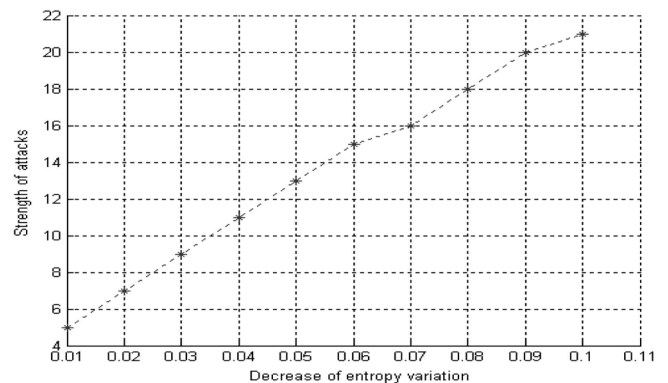


Fig.4. Entropy variation vs Strength of attacks

Figure 4 describes however entropy variation changes drops linearly once the attack strength will increase. It indicates that the decrease of entropy variation is 0.02 once the attack strength is seven times of the conventional flow, in different words, we will solely discriminate DDoS attack flows once its attack strength is regarding seven times of the conventional flow; and that we extend our traceback procedure for detecting low rate once the attack strength isn't robust, say but seven times of the legitimate flows. Our mechanism is appropriate for each robust and weak attack. Therefore, the planned traceback methodology will touch upon the bulk of DDoS attacks, e.g., packet flooding attacks. Another accuracy issue for our methodology is that the false positive, as an example, flash crowds can produce false positive if we tend to begin the traceback procedure at the victim website. We tend to currently think about the whole attack tree and investigate the convergence of entropy variation once a DDoS attack is in progress. Assume that there are 1,024 zombies within that and that they are distributed uniformly in terms of hops from the victim. Assume that, we tend to ignore the hops with no zombies, and therefore the most remote zombie's square measure ten hops aloof from the victim, namely, every hop has around a hundred zombies. We tend to examine the convergence of the entropy variation with completely different attack tree structures, e.g. two-branch tree and three-branch tree. For every simulation, we tend to examine 3 cases, 100 flows, 500 flows, and 1,000 flows, severally. Since this methodology doesn't traceback to zombies whose attack strength is a smaller amount than seven times the legitimate flows, we tend to use software based low rate detection rule to seek out the zombies.

V. CONCLUSION AND FUTURE ENHANCEMENTS

We planned an efficient and efficient ip traceback scheme against DDoS attacks supported entropy variations. it's a essentially completely different traceback mechanism from the presently adopted packet marking methods. several of the on the market work on ip traceback rely on packet marking, either PPM or DPM. owing to the vulnerability of the web, the packet marking mechanism suffers variety of great drawbacks: lack of scalability; vulnerability to packet pollution from hackers and extraordinary challenge on space for storing at victims or intermediate routers. On the opposite hand, the planned methodology wants no marking on packets, and so, avoids the inherent shortcomings of packet marking mechanisms. It employs the options that are out of the management of hackers to conduct ip traceback. we tend to observe and store short term info of flow entropy variations at routers. Once a DDoS attack has been known by the victim via detection algorithms, the victim then initiates the pushback tracing procedure. The traceback rule initial identifies its upstream routers wherever the attack flows came from, and so submits the traceback requests to the connected upstream routers. This procedure continues till the most remote zombies are known or once it reaches the discrimination limitation of DDoS attack flows. Whenever the flow strength is low, it

initiates the low rate detection rule to trace out the zombies. The work planned during this paper could additional be extended by considering the differentiation of the DDoS attacks and flash crowds. The planned methodology could treat flash crowd as a DDoS attack, and hence hence mechanism could also be explore.

REFERENCES

- [1] C. Gong and K. Sarac, "A More Practical Approach for Single-Packet IP Traceback Using Packet Logging and Marking," *IEEE Trans. Parallel and Distributed Systems*, vol. 19, no. 10, pp. 1310-1324, Oct. 2008.
- [2] D. Dean, M. Franlin, and A. Stubblefield, "An Algebraic Approach to IP Traceback," *ACM Trans. Information and System Security*, vol. 5, no. 2, pp. 119-137, May 2006.
- [3] Y. Chen and K. Hwang, "Collaborative Detection and Filtering of Shrew DDoS Attacks Using Spectral Analysis," *J. Parallel and Distributed Computing*, vol. 66, pp. 1137-1151, 2006.
- [4] G. Jin and J. Yang, "Deterministic Packet Marking Based on Redundant Decomposition for IP Traceback," *IEEE Comm. Letters*, vol. 10, no. 3, pp. 204-206, Mar. 2006.
- [5] A. Belenky and N. Ansari, "IP Traceback with Deterministic Packet Marking," *IEEE Comm. Letters*, vol. 7, no. 4, pp. 162-164, Apr. 2003.
- [6] S. Savage, "Network Support for IP Traceback," *IEEE/ACM Trans. Networking*, vol. 9, no. 3, pp. 226-237, June 2001.
- [7] B. Al-Duwairi and M. Govindarasu, "Novel Hybrid Schemes Employing Packet Marking and Logging for IP Traceback," *IEEE Trans. Parallel and Distributed Systems*, vol. 17, no. 5, pp. 403-418, May 2006.
- [8] Y. Kim et al., "PacketScore: A Statistics-Based Packet Filtering Scheme against Distributed Denial-of-Service Attacks," *IEEE Trans. Dependable and Secure Computing*, vol. 3, no. 2, pp. 141-155, Apr.-June 2006.
- [9] M.T. Goodrich, "Probabilistic Packet Marking for Large-Scale IP Traceback," *IEEE/ACM Trans. Networking*, vol. 16, no. 1, pp. 15-24, Feb. 2008.
- [10] K. Lu et al., "Robust and Efficient Detection of DDoS Attacks for Large-Scale Internet," *Computer Networks*, vol. 51, no. 9, pp. 5036-5056, 2007.Apr.-June 2006.
- [11] A.C. Snoeren et al., "Single-Packet IP Traceback," *IEEE/ACM Trans. Networking*, vol. 10, no. 6, pp. 721-734, Dec. 2002.
- [12] T.K.T. Law, J.C.S. Lui, and D.K.Y. Yau, "You Can Run, But You Can't Hide: An Effective Statistical Methodology to Traceback DDoS Attackers," *IEEE Trans. Parallel and Distributed Systems*, vol. 16, no. 9, pp. 799-813, Sept. 2005.
- [13] Shui Yu and Wanlei Zhou, "Traceback of DDoS Attacks Using Entropy Variations," *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no. 3, March 2011.