academicJournals

Vol. 8(20), pp. 1074-1079, 30 May, 2013
DOI: 10.5897/IJPS12.639
ISSN 1992 - 1950 © 2013 Academic Journals
http://www.academicjournals.org/IJPS

International Journal of Physical Sciences

Full Length Research Paper

Triangular fuzzy based classification of IP request to detect spoofing request in data network

Narayanan Arumugam[1]* and Chakrapani Venkatesh[2]

1Anna University, Chennai, India.
[2]Faculty of Engineering, EBET Group of Institutions,Kankayam, Tamilnadu, India, Member IEEE, India.

Accepted 15 April, 2013

In data nework data packets are normally forwarded from one router to another through networks until it gets to reach its destination node. According to the internet architecture routers in the internet do not perform any security verification of the source IP address contained in the IP packets. The lack of such a verification opens the door for variety of network security vulnerabilities like Denial-of-Service (DoS) attacks, man-in-the-middle attacks. One of the major threats to the Internet is source IP address spoofing. Different types of IP spoofing detection and prevention approaches are proposed by the research community. In this paper an ant algorithm based traceback approach is proposed to identify the spoofed request origin. In the proposed traceback approach flow level information of each network path is used to identify the origin of the spoofing attack. The significant characteristics of ant algorithm such as quick convergence and heuristic are adopted in the proposed method to find out the origin of the attack.

Key words: IP spoofing, hop count, ant algorithm, pheromone intensity, fuzzification.

INTRODUCTION

Packet forwarding in the Internet is based only on the destination IP address contained in the IP packet. This permits forging of the source IP address, commonly referred to as IP spoofing (Beverly and Bauer, 2005). IP spoofing is a boon for miscreants. Perhaps the most well-known misuse of IP spoofing is in launching Denial-of-Service (DoS) attacks on critical infrastructure such as Web and DNS servers, as evidenced by backscatter analysis (Moore et al., 2001, 2006). Another avenue made possible by spoofing is that of illegal content distribution. UDP-based peer-to-peer (p2p) applications that exploit IP spoofing to mask the identity of the sender already exist. Present approaches to curb IP spoofing researchers have taken two distinct approaches: router-based and victim-based. The router-based approach makes improvements to the routing infrastructure, while the victim based approach enhances the resilience of Internet servers against attacks. The router-based approach performs either off-line analysis of flooding traffic or on-line filtering of DDoS traffic inside routers. But the victim-based prevention methods, which detects and discards spoofed traffic without any router support. Compared to the router-based approach, the victim based approach has the advantage of being immediately deployable. More importantly, a potential victim has a much stronger incentive to deploy defense mechanisms than network service providers. The current victim-based approach protects Internet servers using sophisticated

*Corresponding author. E-mail: nanptc@gmail.com.

resource management schemes. These schemes provide more accurate resource accounting and fine-grained service isolation and differentiation (Wang, 2007).

Spoofed packets detection methods

A variety of methods are deployed in determining whether a received packet has spoofed source IP address or not. In Internet, when a node receiving a packet can determine whether the packet is spoofed by either an active or passive ways. The term active mean the host must perform some network action but the passive method does not require such action. However, an active method may be used to validate cases where the passive method indicates the packet was spoofed. Among different methods this study considers both IP trace back and hop count based detection method. Since the late 1999 research on IP trace back has been active to detection of DDOS attacks. Several approaches have been proposed to trace IP packets to their origins. IP trace back is usually performed at the network layer, with the help of routers and gateways. The traceback techniques can trace packet paths and help in identifying the perpetrators of the DoS attacks with a high probability. These can be useful forensic tools in law enforcement but do nothing to prevent the occurrence of IP spoofing (Bellovin et al., 2001).

Traceback techniques

IP traceback is a name given to any method for reliably determining the origin of a packet on the Internet by Goodrich (2002). It is a critical ability for identifying sources of attacks and instituting protection measures for the Internet. Probabilistic marking method suggested by Savage et al. (2000) probabilistically marking packets as they traverse routers through the Internet. They propose that the router mark the packet with either the router's IP address or the edges of the path that the packet traversed to reach the router. Deterministic packet marking scheme outlined by Belenky and Ansari (2007) is a more realistic topology for the Internet Snoeren et al. (2001) propose marking details within the router that is to generate a fingerprint is generated with each of the packet. Another method denoted as ant-based traceback approach is proposed to identify the DoS attack origin by Gu Hsin Lai et al. (2008).

Time-To-Live (TTL) methods

When IP packets are routed across the Internet, the Time-To-Live (TTL) field is decremented. This field in the IP packet header is used to prevent packets from being routed endlessly when the destination host cannot be located in a fixed number of hops. It is also used by some networked devices to prevent packets from being sent beyond a host's network subnet. The TTL is a useful value for detecting spoofed packets. Its use is based on several assumptions, which, from our network observations, appear to be true. When a packet is sent between two hosts, as long as the same route is taken, the number of hops will be the same. This means that the initial TTL will be decremented by the same amount. Packets sent near in time to each other will take the same route to the destination. Routes change infrequently. When routes change, they do not result in a significant change in the number of hops (Steven and Templeton, 2003).

The objective of this study is to find out the DOS attack origin (spoofing request) on the network. For the detection process this article uses both the concepts of traceback and hop count of the packet while routing from source to destination on Internet. The IP traceback approach is used to finding out the origin of the spoofing attack using the network data packets traffic flow information on each path. Furthermore, to strengthen the spoofing prevention hop count value of the packet between the source and destination are also validated. An ant-based traceback algorithm is using for finding the traffic flow information as the trace for ants finding the attack path. The hop-count information is indirectly reflected in the TTL field of the IP header, since each intermediate router decrements the TTL value by one before forwarding a packet to the next hop (Stevens and Wright, 1995). The difference between the initial TTL (at the source) and the final TTL value (at the destination) is the hop-count between the source and the destination.

MATERIALS AND METHODS

This study proposes an optimistic method that validates incoming request before it reach the destination without using any cryptographic methodology. The fundamental idea is to utilize inherent network information that each packet carries. The inherent network information this study use here is the flow information and the number of hops of a packet takes to reach its destination. This proposed method uses an ant-based traceback algorithm to find the traffic flow information and hop count value, Since an attacker can forge any field in the IP header, he cannot forged the number of hops an IP packet takes to reach its destination, which is solely determined by the Internet routing infrastructure. The hop-count information is indirectly reflected in the TTL field of the IP header, since each intermediate router decrements the TTL value by one before forwarding a packet to the next hop.

Ant algorithm

Ethnologists states that animals like ants could manage to establish shortest route paths from their colony to feeding sources and back. It was found that the medium used to communicate information among individuals regarding paths and used to decide where to go, consists of pheromone trails. A moving ant lays some pheromone (in varying quantities) on the ground, thus marking

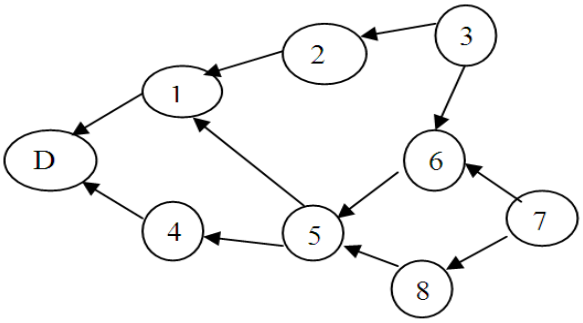

Figure 1. IP trace back of all possible paths.

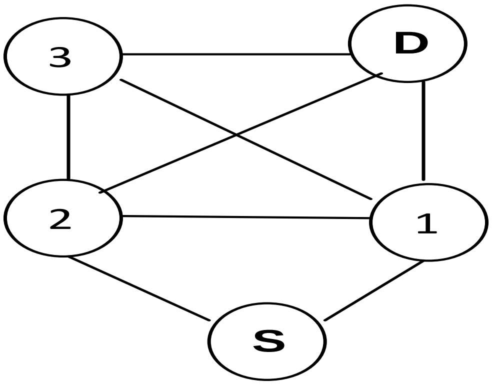

Figure 2. Experimental topology with 5 nodes. S = Source node, D = Destination node.

the path by a trail of this substance. While an isolated ant moves essentially at random, an ant encountering a previously laid trail can detect it and decide with high probability to follow it, thus reinforcing the trail with its own pheromone. The collective behavior that emerges is a form of autocatalytic behavior 1 where the more the ants following a trail, the more attractive that trail becomes for being followed. The process is thus characterized by a positive feedback loop, where the probability with which an ant chooses a path increases with the number of ants that previously chose the same path (Dorigo et al., 1996). The idea is that if at a given point an ant has to choose among different paths, those which were heavily chosen by preceding ants (that is, those with a high trail level) are chosen with higher probability. Furthermore, high trail levels are the same with shortest paths.

Ant based IP traceback

Basically, the attack path reconstruction process involves interrogating the routing packets received at the victim in order to find the immediate upstream node and then systematically repeating the interrogation process at each intermediate upstream node until the attack source is reached. The path reconstruction problem could be solved using the ant-based IP traceback. Figure 1 shows the IP trace back of all possible paths from the source node 3 to the destination node D. Basically the ants lay a pheromone trail along the route they select between the source node (the food source) and the destination (e.g., paths 3-2-1, 3-6-5-4 and 3-6-5-1 in Figure 1) and the relative probability of each path being the actual path is given by the intensity of the pheromone along the corresponding trail.

As in nature, the isolated ants in the ant algorithm scheme move essentially at random. However, upon encountering a previously laid trail, the ants decide with a high probability to trace it. As a result, the pheromone intensity of this path progressively increases and thus the likelihood of the path representing the actual path also increases. The proposed solution could take the victim host as the starting point and perform IP traceback. It is assumed that the legitimate request might reach the victim node in a shortest path (Lai et al., 2008). The description of the ant-based IP trace back is as follows:

Step 1: Construct network topology,
Step 2: Determine all possible paths between two network nodes (source node to destination node),
Step 3: Find out the shortest path,

The shortest path searching process is done with the exploitation policy as in the Equation (1) chooses the arc with the greatest pheromone intensity and visibility, while the exploration policy as in the Equation (2) is a random decision rule. Thus, an ant located at node i choose the next node j in accordance with the following rule:

$$j = \begin{cases} \arg\max\left\{\left\lfloor t_{ij}(t)^{a} \right\rfloor \left\lfloor \eta_{ij}(t)^{\beta} \right\rfloor\right\} \text{if } q \le q^{o} \\ S \text{ otherwise} \end{cases} \qquad (1)$$

$$S = p_{ij}(t) = \begin{cases} \dfrac{\left[\tau_{ij}(\tau)\right]^{\alpha}\left[\eta_{ij}(\tau)\right]^{\beta}}{\sum\left[\tau_{i\,j}(\tau)\right]^{\alpha}\left[\eta_{ij}(\tau)\right]^{\beta}} \\ 0 \qquad \text{otherwise} \end{cases} \qquad (2)$$

where, $\tau_{ij}(t)$ the pheromone intensity of trail between router i and router j at time $\eta_{ij}(t)$ = the number of routing packets between router i and router j between time (t-1) and time (t) α is the weighting factor of pheromone, β is the weighting factor of visibility.
Ant colony updates the probability density function of feasible attack paths and chooses the right one.

RESULTS

The suggested method have tested using a PC with a specification of Intel Dual core CPU, 3.0G DDR2, 1G of RAM and the MS Windows XP operating system. The experimental topology constructed with 5 nodes as shown in the Figure 2. Where node S considered as a source node and the node D as s destination, the possible path between the node S and D where identified using an algorithm. According to the ant system optimization by a colony of cooperating agent, ants follow a path between the source to destination with all possible paths with equal probability. This process continues until all of the ants will eventually choose the shortest path.

The idea is that at a given point an isolated ant can choose a path among different paths, but according to the ant algorithm, those which were heavily chosen by preceding ants are chosen with higher probability based on with a high trail level. Furthermore, high trail levels are synonymous with shortest paths. It is

Table 1. Experimental value for 5 nodes.

S/N	Possible path	Hop count	Pheromone intensity
1.	s-> 1->d	1	2.129463
2.	s->1->d	1	2.129463
3.	s->1->2->d	2	2.063101
4.	s->1->3->d	2	1.631010
5.	s->2->1->d	2	2.211162
6.	s->1->3->d	2	1.911162
7.	s->1->2->3->d	3	1.327916
8.	s->1->3->2->d	3	1.309615
9.	s->2->1->3->d	3	1.309615
10.	s->2->3->1->d	3	1.512709

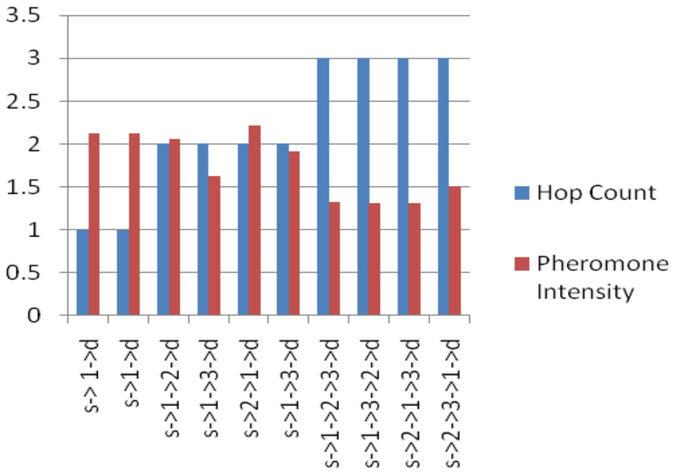

Figure 3. Possible path between sources to destination.

understood that the isolated ant would reach the destination in a shortest way. The shortest path is identified by the isolated ant based on the maximum pheromone intensity. Hence, it is clear that the shortest path may not have fake request. Experimental values are tabulated as in the Table 1 with possible path, hop count and pheromone intensity. From the tabulation it is understood that the legitimate request has minimum hop value and maximum pheromone intensity value. Figure 3 shows the possible path among source and destination with pheromone intensity.

DISCUSSION

From the experimental result this paper classify the IP request either spoofed or legitimate. Fuzzification techniques is used to classify the spoofing request among all possible IP request. Fuzzification is the process of changing a real scalar value into a fuzzy value. This is achieved with the Trapezoidal fuzzifiers. Intuition is used to fuzzify this scalar quantity into the fuzzy or linguistic variables as spoofed request, partially spoofed and legitimate request. The membership function associated with each scalar quantity as defined by intuition is as follows:

$$\mu_{leg} = \begin{cases} 1 & if \quad p \le 1.4 \\ \dfrac{1.6 - p}{0.2} & if \quad 1.4 < p < 1.6 \\ 0 & if \quad p \ge 1.6 \end{cases} \tag{3}$$

$$\mu_{par} = \begin{cases} 1 & if \quad p \le 1.9 (or) p \ge 1.6 \\ \dfrac{p - 1.9}{0.2} & if \quad 1.9 < p < 2.1 \\ \dfrac{1.6 - p}{0.2} & if \quad 1.4 < p < 1.6 \end{cases} \tag{4}$$

$$\mu_{s} = \begin{cases} 0 & if \quad p \le 1.9 \\ \dfrac{p - 1.9}{0.2} & if \quad 1.9 < p < 2.0 \\ 1 & if \quad p \ge 2.1 \end{cases} \tag{5}$$

where *p* is the pheromone intensity, and subscript $\boldsymbol{\mu}_{\text{leg}}$ denotes legitimate request, $\boldsymbol{\mu}_{\text{par}}$ denotes partially spoofed request and $\boldsymbol{\mu}_{\text{s}}$ denotes spoofed request. From the fuzzification condition stated as in Equations (3), (4) and (5) it is understood that the pheromone intensity p below 1.4 is assumed as legitimate request, between 1.6 to 1.9 as partially spoofed request and above 1.9 as spoofed request. A graphical representation of the membership function of IP request is shown in Figure 4.

Table 2 gives the pheromone intensity of all possible shortest paths among the source to destination with the membership function associated with each fuzzy variable, that is, spoofed request, partially spoofed request and legitimate request for each path. For example consider a specific path s->2->1->d and the membership value of each fuzzy set for this path is calculated from Equations (3), (4), and (5) as: $\boldsymbol{\mu}_{\text{leg}}$ =0, $\boldsymbol{\mu}_{\text{par}}$ =0, $\boldsymbol{\mu}_{\text{s}}$ =1. It can be bring

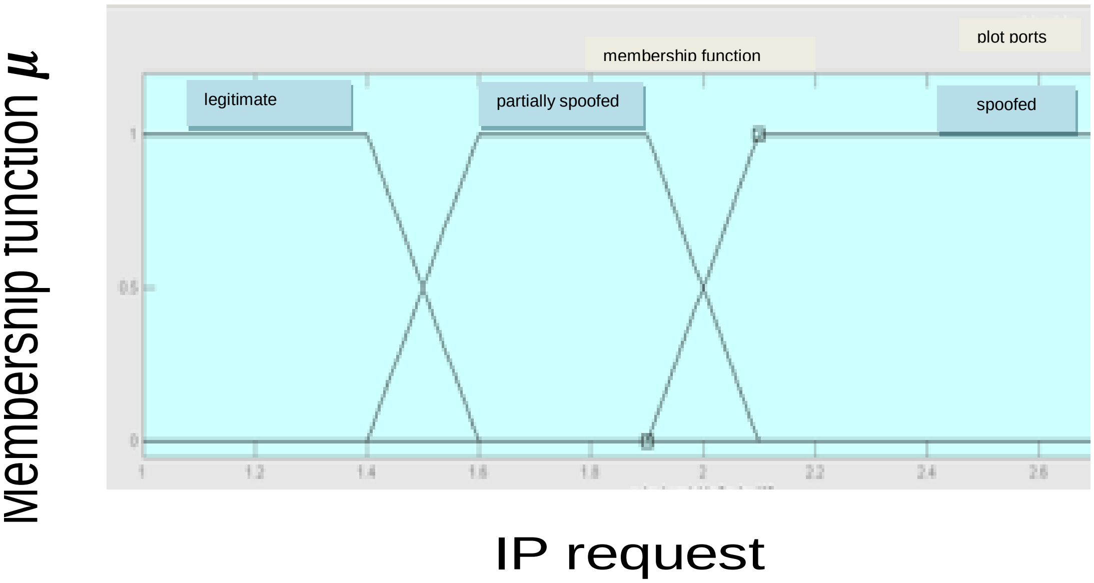

Figure 4. Membership function of IP request.

Table 2. Experimental value for 5 nodes.

S/N	Possible Path	Hop	Pheromone Intensity	μ_l	μ_p	μ_s
1	s-> 1->d	1	2.129463			1
2	s->1->2->d	2	2.063101		0.5	
3	s->2->1->d	2	2.211162			1
4	s->1->2->3->d	3	1.327916	1		
5	s->1->3->2->d	3	1.309615	1		
6	s->2->1->3->d	3	1.309615	1		
7	s->2->3->1->d	3	1.512709		0.5	

to a close from above result that the path request(s->2->1->d) is spoofed by 100%, partially spoofed by 0%, and legitimate request by 0%. In this article the fuzzification techniques is used to classified each request as legitimate, partially spoofed and spoofed. These types of request classification may easy for prevention of spoofed request.

Conclusion

Internet security is a fashionable and fast-moving field at the same time network-based attacks are inevitable. Identifying the source of attack origin is mandatory to protect the network resources. Among different IP spoofing detection method classification of each request is mandatory. The proposed ant algorithm based IP trace back method is identified the attack source effectively and also the spoofing request is classified using triangular fuzzification. This method examined all possible way to reach destination node and classified the most spoofed request from partially spoofed request.

REFERENCES

Belenky A, Nirwan A (2007). "On deterministic packet marking," Computer Networks: The International Journal of Computer and Telecommunications Networking.

Bellovin S, Leech M, Taylor T (2001). On design and evaluation of intention-driven ICMP traceback. Proceedings of the Tenth International Conference on Computer Communications and Networks, IEEE Xplore Press, Scottsdale, AZ, pp. 159-165. DOI: 10.1109/ICCCN.2001.956234.

Beverly R, Bauer S (2005). The spoofer project: Inferring the extent of Internet source address filtering on the Internet. Proceedings of the Steps to Reducing Unwanted Traffic on the Internet on Steps to Reducing Unwanted Traffic on the Internet Workshop, (TIW '05), USENIX Association Berkeley, CA, USA. pp. 8-8.

Dorigo M, Maniezzo V, Colorni A (1996). The ant system: Optimization by a colony of cooperating agents. IEEE/ACM Trans. Syst. pp. 1-13.

Goodrich MT (2002). Efficient packet marking for large-scale IP traceback. Proceedings of the 9th ACM Conference on Computer and Communications Security, (CCS' 02) ACM New York, NY, USA.

Lai GH, Chen CM, Jeng BC, Chao W (2008). Department of Information Management, National Sun Yat-Sen University, Taiwan,” Ant-based IP traceback”, Elsevier, pp. 3071-3080.

Moore D, Voelker G, Savage S (2001). Inferring internet denial-of service activity. USENIX Secur. Symp. 24(2):115-139.

Moore D, Shannon C, Brown D, Voelker GM, Savage S (2006). Inferring internet denial-of-service activity. ACM Tran. Comp. Sys. 24:115-139. DOI: 10.1145/1132026.1132027.

Savage S, Wetherall D, Karlin A, Anderson T (2000). Practical network support for IP traceback. Proceedings of the Conference on Applications, Technologies, Architectures and Protocols for Computer Communication, (PCC’ 00) ACM New York, NY, USA. pp. 295-306. DOI: 10.1145/347059.347560.

Snoeren AC, Partridge C, Sanchez LA, Jones CE, Tchakountio F (2001). Hash-based IP trace back. Proceedings of the 2001 Conference on Applications, Technologies, Architectures and Protocols for Computer Communications, (PCC’ 01) ACM New York, NY, USA., pp. 3-14. DOI: 10.1145/383059.383060.

Steven and Templeton (2003). Detecting Spoofed Packets, http://seclab.cs.ucdavis.edu/papers/DetectingSpoofed-DISCEX.pdf.

Stevens WR, Wright GR (1995). TCP/IP Illustrated: The Implementation. 1st Edn., Addison-Wesley Professional, Reading, Mass, ISBN: 020163354X, P. 1174.

Wang H (2007). Defense against spoofed ip traffic using hop-count filtering. IEEE/ACM, DOI: 10.1109/TNET.2006.890133 Tran. Netw. 15:40-53.