Detection of Spoofing Using Packet Marking Algorithm

B.Balasankari[1], M.G. MathanKumar[2].
[1](Computer Science and Engineering, Oxford Engineering College, India)
[2](Computer Science and Engineering, Oxford Engineering College, India)

ABSTRACT: Wireless networks are vulnerable to spoofing attacks, which allows for many other forms of attacks on the networks. However the localization infrastructure can be subjected to non cryptographic attacks, such as signal attenuation and amplification that cannot be addressed by traditional security services. An interruption in an authorized users access to a computer network, typically one caused with malicious intent (DDOS). Although the means to carry out motives for and targets of a DOS attack may vary, it generally consists of efforts to indefinitely interrupt services of a host connected to the Internet (DDOS). EPPM significantly reduces the number of IP (Internet protocol) or IP packets required to convey the relevant information, when compared to the prior best known scheme. Compared with the hash-based approach, our approach incurs less storage overhead and less access time overhead at routers. Specifically, the storage overhead is reduced to roughly one half, and the access time requirement is decreased by a factor of the number of neighbour routers.

Keywords: **Network Analysis, Spoofing attack detection EPPM, Attack detection, Localization**

1. INTRODUCTION

Obtaining the Distributed denial-of-service attack (DDOS service Attack) is an attempt to make a network resource unavailable to its intended users. Although the means to carry out motives for and targets of a DOS (Denial of service) attack may vary, it generally consists of efforts to indefinitely interrupt services of a host connected to the internet. The main problem with current intrusion detection systems is high rate of false alarms. The design and implementation of a load balancing between the traffic coming from clients and traffic originated from the attackers is not implemented. In the proposed System novel scheme for detecting and preventing the most harmful and difficult to detect Distributed Denial of Service (DDOS) Attacks those that use IP (Internet Protocol) address spoofing to disguise the attack flow an IP (Internet protocol) trace back approach based on both and packet logging. Compared with the probabilistic packet marking algorithm (PPM) approach and approach is able to track individual packet and hash-based approach and approach of incurs less storage overhead and less access time overhead at routers. Specifically, the storage overhead is reduced to roughly one half, and the access time requirement is decreased by a factor of the number of neighbour routers and also in the proposed system our modified probabilistic algorithms (PM) called efficient probabilistic packet marking (EPPM) algorithm. To conclude, our algorithm, EPPM marking algorithm is an effective means of improving the reliability of original probabilistic packet marking (PPM) algorithm.

2. RELATED WORKS

In this paper, define EPPM, an efficient general probabilistic packet marking scheme with a wide range of potential applications of which locating Internet bottlenecks, IP trace back are investigated as

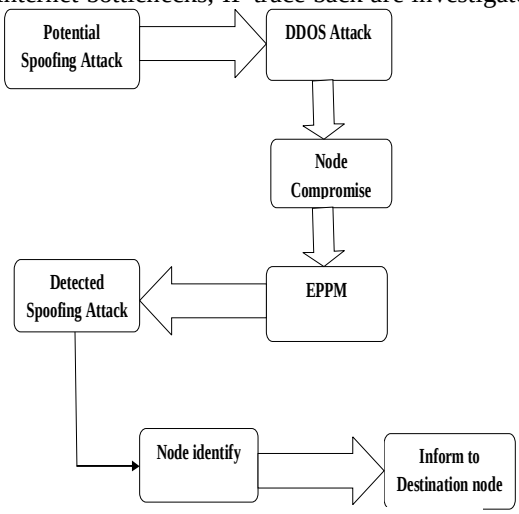

Fig .1. Detect the DDOS Attack and EPPM

two representative examples to demonstrate its effectiveness. Our proposed scheme imposes only a single-bit overhead in the IP packet headers. More importantly, it significantly reduces the number of IP protocol packets required to convey the relevant information, when compared to the prior best known scheme. In the modified probabilistic algorithm called EPPM algorithm and overcome this problem. To conclude, our algorithm Efficient Probabilistic Packet Marking algorithm (EPPM) is an effective means of improving the reliability of original PPM algorithm. In the algorithm EPPM is a modified version of PPM algorithm. So EPPM inherits the defects of the PPM algorithm. In the proposed system various algorithm implemented to detect the DDOS

attack, efficient probabilistic packet marking algorithm, Cracking Algorithm.

3. EPPM AND MARKING PROCEDURE AT ROUTER R

The routers encode the information in three marking fields of an attack packet: (start, end, distance). The start and end fields store the IP addresses of the two routers at the end points of the marked edge. The distance field records the number of hops between the marked edge and the victim site. In the PPM a packet stores the information of an edge in the IP (Internet protocol) header. The pseudo code of the procedure is given in for reference. The router determines how the packet can be processed depending on the random number generated. If x is smaller than the predefined marking probability pm, the router chooses to start encoding an edge. The router sets the start field of the incoming packet to the routers address and resets the distance field to zero. If x is greater than pm, the router chooses to end encoding an edge by setting the router's address in the end field. An extra field named as flag which takes either 0 or 1. The flag value at first is made 0. If the end field is set then the flag is made 1. Now, the start field is encoded only when the flag is 0. If the flag is 1 it implies that the start and end fields together encoded an edge of the attack graph.

4. CRACKING ALGORITHM

In this paper a new cracking algorithm is implemented to stop that Distributed Denial of Service service attacks. In this algorithmic design a practical DDOS (Distributed denial of service attack) defence system that can protect the availability of web services during severe DDOS service attacks. The proposed system identifies whether the number of entries of client exceeds more than five times to the same sever, then the client will be saved as a attacker in blocked list and service could not be provided. So this algorithm protects legitimate traffic from a huge volume of DDOS service attack traffic when an attack occurs. New Cracking algorithm Start the Process H=Maintain the IP address History; U=User enter into the website; I=Store the Each Client IP (Internet Protocol) address; Check each time U in server, When the new user enters into the site continuously, new cracking algorithm to determine whether the user is DDOS service attacker. At the same time our experimental result obtains without any DDOS service prevention. In that situation, what is sate of web server is calculated and also when the attacker is allowed to access the website, the status of the web server also calculated, the attacker list is maintained and checked the user with the list [7]. If the attacker is found, the access is denied by New cracking Algorithm. In this situation, the web server status also calculated and very useful for the users to determine the efficiency of our proposed algorithm named as New Cracking Algorithm**.** In this algorithm to use the Distributed denial of service (DDOS) attack to prevent the server from accessing the server and interruption of the performance in server is distribute successfully in this system.

5. MAC GENERATOR

Certain bits from this IP address and the port number pair will serve as the Message Authentication code (MAC) for the client's IP address. MAC is a symmetric authentication scheme that allows a party A, which shares a secret key k with another party A, which shares a secret key k with another party B, to authenticate a message M sent to B with a signature MAC (M, k) has the property that, with overwhelming probability, no one can forge it without knowing the secret key k. We are verifying the secret key to prevent attackers who are using genuine address or spoofed address. Since a legitimate client uses its real IP address to communicate with the server, it will receive the HTTP (Hypertext transfer protocol) redirect message. So, all its future packets will have the correct MACs inside their destination IP addresses and thus be protected. DDOS service traffic with spoofed IP addresses, on the other hand, will be filtered because the attackers will not receive the (Media Access Control) MAC. This technique effectively separates legitimate traffic from DDOS service traffic with spoofed IP (Internet protocol) addresses.

6. PREVIOUS MAC ALGORITHM

MAC layers Denial of service (DOS) attacks are launched due to the unencrypted management frames and they disrupt the network access completely [1]. The selected Denial of service (DOS) attacks is made on the individual stations not on the whole network. The MAC (Media access control) layer DOS (Denial of service) attacks are classified into three type's namely masquerading; resource flooding and media access Denial of service (DOS) attacks.

7. MASQUERADING (DOS) ATTACKS

Denial of service (DOS) attacks free tools using the identities of the client or AP, the intruder traces the MAC (Media access control) address and brings the network under control. Deauthentication and disassociation and power saving attacks are based on the masquerading attack types.

7.1. Deauthentication attacks

The client and AP mutually request deauthentication by sending a request message [11]. But these messages are not authenticated itself by any keying procedures. This vulnerability makes the

intruder to exploit the client or (Access Point) and launch the deauthentication attack. In response to the attack, the client or AP refuses to access the packets until they reauthenticate [12].

7.2. Resource Flooding DOS attacks

The most important DOS service attack vulnerability is flooding attacks which are named as Resource depletion or flooding DOS service attacks which targets the shared resources such as AP and uses all its memory and processing so that it cannot continue services to its legitimated clients. The resource depletion attacks are categorized as probe request flood, association request flood, authentication request flood and deauthentication/disassociation request flood.

7.3. Media Access Attacks

The unauthenticated management and control frames contain a duration field which is used by the virtual carrier sense mechanism that is used for solving the hidden terminal problems. The media access attacks are caused by affecting the legitimate transmission by asserting a large duration field to ensure the value of Network Allocation Vector (NAV) value for each node is greater than zero.

8. BEHAVIOUR MONITORING AND DETECTION ALGORITHM

DDOS attacks are a critical threat to the Internet. Recently, there are an increasing number of DDOS attacks against online services and Web applications. These attacks are targeting the application level. Detecting application layer DDOS attack is not an easy task. A more sophisticated mechanism is required to distinguish the malicious flow from the legitimate ones. This paper proposes a detection scheme based on the information theory based metrics. The proposed scheme has two phases: Behaviour monitoring and Detection. In the first phase, the Web user browsing behaviour is captured from the system log during non attack cases. Based on the observation, Entropy of requests per session and the trust score for each user is calculated. In the detection phase, the suspicious requests are identified based on the variation in entropy and a rate limiter is introduced to downgrade services to malicious users.

8.1. MONITORING ALGORITHM

The system log Extract the request arrivals for all sessions, page viewing time and the sequence of requested objects for each user from the system log. Compute the entropy of the requests per session using the formula: $H(R) = -\sum_J Pj(rj) \log Pj(rj)$ and Compute the trust score for each and every user based on their viewing time and accessing behaviour.

8.2. DETECTION ALGORITHM

The predefined entropy of requests per session and the trust score for each user. Define the threshold related with the trust score (T_{ts}) Define the threshold for allowable deviation (T_d) for each session waiting for detection Extract the requests arrivals. Compute the entropy for each session using $Hnew(R) = -\sum jPj(rj) \log Pj(rj)$. Compute the degree of deviation: $D = |H\ new(R)| - |H(R)|$ If the degree of deviation is less than the allowable threshold (Td), and user's trust score is greater than the threshold (Tts), then, Allow the session to get service from the web server.

9. FLOODING

It is a simple routing algorithm in which every incoming packet is sent through every outgoing link except the one it arrived on. Flooding is used in bridging and in systems such as Usenet and peer-to-peer file sharing and as part of some routing protocols, including OSPF,DVMRP, and those used in ad-hoc wireless networks.

9.1. Problems on Flooding

Flooding can be costly in terms of wasted bandwidth. While a message may only have one destination it has to be sent to every host. In the case of a ping flood or a denial of service attack, it can be harmful to the reliability of a computer network. Messages can become duplicated in the network further increasing the load on the networks bandwidth as well as requiring an increase in processing complexity to disregard duplicate messages. Duplicate packets may circulate forever, unless certain precautions are taken: Use a hop count or a time to live count and include it with each packet. This value should take into account the number of nodes that a packet may have to pass through on the way to its destination. Have each node keep track of every packet seen and only forward each packet once and enforce a network topology without loops.

10. FALSE ALARM

Although an intelligent intrusion and detection strategies are used to detect any false alarms within network critical segments of network infrastructures, reducing false positives are still being a major challenges. Up to this moment, these strategies focus on either detection, but often lack of having both features together. Without considering those features together, intrusion detection systems are probably cannot highly detect on low false alarm rates. The role of the constant false alarm rate circuit is to determine the power threshold above which any return can be considered to probably originate from a target. If this threshold is too low, then more targets will be detected at the expense of increased numbers of false alarms. Conversely, if the threshold is too high, then fewer targets will be detected, but the number of false alarms will also be low. In most radar detectors, the threshold is set in order to achieve a required probability of false. If the background against which targets are to be detected is constant with time and space, then a fixed threshold level can be chosen that provides a specified probability of false alarm, governed by the probability density function of the noise, which is usually assumed to be Gaussian. The probability of detection is then a function of the signal-to-noise ratio of the target return. However, in most fielded systems, unwanted clutter and interference sources mean that the noise level changes both spatially and temporally. In this case, a changing threshold can be used, where the threshold level is raised and lowered to maintain a constant probability of false alarm. This is known as CFAR detection. In order to reduce the network attacks are becoming more and more difficult to identify the need for better and more efficient intrusion detection systems .In the proposed system introduce the algorithm as Packet marking methods include the probabilistic packet marking and the DPM. The PPM mechanism tries to mark packets with the router's IP address information by probability on the local router, and the victim can reconstruct the paths that the attack packets went through. The PPM method is vulnerable to attackers, as pointed out in , as attackers can send spoofed marking information to the victim to mislead the victim. The accuracy of PPM is another problem because the marked messages by the routers who are closer to the leaves could be overwritten by the downstream routers on the attack tree. At the same time, most of the PPM algorithms suffer from the storage space problem to store large amount of marked packets for reconstructing the attack tree. Moreover, PPM requires all the Internet routers to be involved in marking. They broke the 16-bits marking space into three parts: 1 bit for distance, 2 bits for fragmentation index, and a hash fragmentation of 13 bits. By this modification, the proposed FIT algorithm can trace back the attack paths with high probability after receiving only tens of packets. The FIT algorithm also performed well even in the presence of legacy routers and it is a scalable algorithm for thousands of attack sources.PPM is vulnerable if hackers inject marked packets into the network. Therefore, the paper proposed a deterministic packet marking method for IP trace back. The basic idea is that at the initial router for an information source, the outer embeds its IP address into the packet by chopping the router's IP into two segments with 17 bits each .As a result, the victim can trace which router the packets.

11. CONCULSION

In this paper, we proposed an effective and efficient IP trace back scheme against DDOS attacks based on entropy It is a fundamentally different trace back mechanism from the currently adopted packet marking strategies. Many of the available work on IP trace back depend on packet marking, either probabilistic packet marking or deterministic packet marking and also reduce the overhead.

12. REFERENCES

[1]. J. Mirkovic, G. Prier, and P. Reiher, "Attacking DDOS at the source," in Proceedings of the IEEE International Conference on Network Protocols, pp. 312-321, Nov. 2002.

[2] K. Park and H. Lee, "On the effectiveness of route- based packet filtering for distributed Denial of service attack (DDOS) prevention in power-law internets," in Proceedings of ACM SIGCOMM'01, Aug. 2001.

[3] T. Peng, C. Leckie, and K. Ramamohanarao, "Adjusted probabilistic packet marking for IP trace- back," in Networking 2002, pp. 697-708, May 2002.

[4] J.Ioannidis and S. M. Bellovin, "Implementing push- back: router-based defense against DDOS attacks," in Proceedings of the Network and Distributed System Security Symposium (NDSS'02), pp. 6-8, Feb. 2002.

[5] H. Burch and B, Cheswick, "Tracing anonymous packets to their approximate source," in Proceedings of the 14th Systems Administration Conference (LISA'00), pp. 319-327, Dec. 2000.

[6]. T. Peng, C. Leckie, and K. Ramamohanarao, "Adjusted probabilistic packet marking for IP trace- back," in Networking 2002, pp. 697-708, May 2002.

[7] An effective prevention of attacks using gi Time frequency algorithm under DDOS attack by Dr.K.Kuppusamy, S.Malathi, International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011

[8] Exploiting P2P Systems for DDOS Attacks by Naoum Naoumov and Keith Ross, Department of Computer and Information Science Polytechnic University, Brooklyn, NY 11201.

[9] Trends in Denial of Service Attack Technology CERT® Coordination Center Kevin J. Houle, CERT/CC George M. Weaver, CERT/CC In collaboration with: Neil Long Rob Thomas v1.0 - October 2001.

[10] K. Park and H. Lee. On the effectiveness of route based packet filtering for distributed DOS prevention in power-law internets. In Proc.ACM SIGCOMM, San Diego, CA, August 2001.