www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -02 February, 2016 Page No. 15714-15718

Defence Mechanism to Mitigate DDoS Attack For Wireless LAN

Anushree[1], Priyanka Baviskar, Pooja Dalimbe[3], Sneha Dhaswadikar[4], S V Athawale[5]

[1]Student (UG), Department of Computer Engineering,
A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India
anushree1293@gmail.com@gmail.com

[2]Student (UG), Department of Computer Engineering,
A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India
priyankabaviskar94@gmail.com

[3]Student (UG), Department of Computer Engineering,
A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India
puja.vandu@gmail.com

[4]Student (UG), Department of Computer Engineering,
A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India
sneha.hd28@gmail.com

[5]*Assistant Professor, Department of Computer Engineering,*
A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India
sv_athawale@rediffmail.com

Abstract: ***In today's world one of the major challenge to defense against Distributed Denial of Service (DDoS) Attack. We cannot completely avoid DDoS attack but we can reduce the DDoS attack. In IP traceback schemes, the victim can identify the sources of an attack and can block them. However, these methods react to the attack once it is completed. This means the critical resource of the victim already have been consumed by the attacker and reached the goal of blocking the access to the victim. To overcome this problem of existing IP traceback scheme, defense mechanism against DDoS flooding attacks have been proposed based on existing Deterministic Flow Marking (DFM) IP traceback method. The fundamental issue worried with discovery frameworks is IP spoofing. This paper proposes a bundle marking plan which checks the data into IP header field of the packet to beat the issue of IP spoofing. The marked data is utilized to remake the IP location of the entrance router joined with the attack source at the distinguishing end. The work is sent in the programmable router progressively and the attack source recognition systems are completed. It will improve the performance of the legitimate traffic.***

Keywords: DDoS attack, packet marking, Deterministic Flow Marking, IP Traceback, packet filtering.

1. Introduction

In the field of correspondence and information stockpiling over the web, security has been the key focus of numerous analysts throughout the years. The Denial of Service (DoS) and Distributed Denial of Service (DDoS) are the types of attacks which have changed the point of view of system security. By these sorts of attacks even superior limit servers can be pounded. Because of the trusting way of IP, the source location of a packet is never validated hence it is troublesome for the victim to recognize the wellspring of DoS/DDoS attack. This prompts the need of some method to discover the wellspring of the transmitted packet. Consequently diverse IP traceback approaches have been examined and assessed [1]. The two primary downsides with the concentrated on methodologies are: First, because of the impressive computational overhead, it is wasteful to utilize bounce by-jump way recreation. Besides, changes are should have been be done in the center steering structure, for the way remaking. This is not productive by any means. As needs be, the current methodologies can be grouped by diverse perspectives [2] [3]. Another deterministic packet checking approach, called DDPM, was proposed [4]. Its prime center was on the DoS and DDoS attack. They effectively found the deploying so as to wellspring of DoS and DDoS attack just edge routers in the web. The base for this calculation was the dynamic marking, which will be meant to complete at the edge router or closest router from the source. The disadvantage of the calculation was space overhead. Be that as it may, as of late, the routers are outfitted with expansive measure of physical memory. This makes the disadvantage ignorable. The paper additionally gave the validated marking framework. This practice just uses one cryptographic MAC (Message Authentication Code) figuring per checking, which is requests of greatness more able to register and can be adjusted so it just requires the 16-bit over-burden IP recognizable proof field for capacity. The recognizable proof information should be gone to the destination for every current. The acknowledgment information is isolated into a few parts. In this manner, the imprint contains the recognizable proof information and a few bits required to distinguish a section. It additionally distinguishes marked and unmarked bundles in a stream. Every destination keeps up a table coordinating the stream ID and conceivable imprint pieces. At the point when a packet has a place with an inconspicuous stream touches base at the objective, the objective makes another table section in the recreation table. At that point, it will separate the marking bits of this stream from the checked packets, and thinks of them in the relating fields. After all sections comparing to a stream achieve the objective, the beginning source for the given stream gets to be unmistakable to the objective. Utilizing Deterministic Flow Marking, the objective can separate the movement of diverse systems behind an edge router. In validation checking system [5], both sides share a mystery key. The source annexes the message with MAC (Message Authentication Code) of message utilizing the key. Collector can check the legitimacy of MAC. This strategy likewise gives the router validation, yet it is illogical as every router needs to impart the mystery key to every potential victim. Hence, the need of system to validate the stream marking was excited. Source can send packets alongside the marking information to the objectives. Since a traded off router does not distinguish the mystery keys of edge routers, it can't fashion stream markings. At the point when the destination gets the marked stream, it utilizes the dispatcher's open key to accept the sender. On the off chance that both sides concur, the destination realizes that the creator of the imprint was in control of the edge router's private key, and that the imprint is truth be told legitimate, or else it would dismiss the stream.

Other than these, [6] [7] Deterministic Flow Marking (DFM) plan was acquainted for vast distributed attacks with the sender's system situated in the LAN behind the edge routers. The deterministic system is picked over the probabilistic strategy is because of the higher traceback exactness. Same is the explanation behind the use of deterministic checking for cutting edge security administrations. Deterministic Flow Marking likewise gave a technique to validate the marking data to fathom the issue of imprint satirizing by manufactured routers. One point of interest of the proposed verified stream marking strategy is that it is discretionary for the destination to remove and accept the mark for each stream while it doesn't get attacking streams. In circumstances when the victim is under attacks, it might utilize the mark to verify the imprint to discover the attacker system. Thus the objective is not authorized to dependably expend its CPU and memory assets to check Elliptic Curve Digital Signature Algorithm (ECDSA) signature as clarified [8] [9].

Literature Survey

Numerous traceback approaches have been proposed yet. By the traceback methodologies are ordered in various classifications such as Basic Principle, Processing Mode, and Location.

2.1 Basic Principle

On the off chance that arranged with Basic rule, the offered traceback techniques are segregated into Marking and Logging bunches. In marking systems [10], the voyaging bundles are included with specific data by some or all routers in the way. Utilizing this data, regardless of the probability that the IP is satirize, the attacker can be followed down. In logging technique [11], the routers keep some data related to the voyaging packet. This data can be later on used to traceback to the sender from which the packet has been started. Necessity of extensive measure of memory and CPU utilization at routers of the attacked way makes a fundamental issue for logging strategy, as it stores data about every last bundle went through the router [12].

2.2 Processing Mode

Taking into account the preparing mode, traceback plans are recognized in two gatherings, deterministic and probabilistic. In deterministic technique, the bundle ought to be honed at source and in addition at focus, in spite of marking or logging. Despite the fact that this system gives prevalent precision, it requires more administration overhead at both source and the objective, in evaluation to the probabilistic technique. Probabilistic strategies are to some degree undifferentiated from the deterministic systems; just the required handling time and transfer speed is relatively less. The vast majority of the current traceback techniques are probabilistic.

2.3 Location

From the part of characterization by areas, exhibited traceback strategies can be separated into two gatherings. One that sends data through the edge routers by the source is called source bunch. Second, in the system through some or all routers in the strike way called system bunch. The greater part of the present traceback strategies have a place with the system bunch. The essential motivation behind the gathering is to distinguish attack way totally or modestly [13]. These techniques require consideration of all routers and profoundly expend assets, for example, preparing time and memory. Source bunch strategy goes for distinguishing the attack source and not the attack way [14] [15]. Light, adaptable, secure DPM is suitable for some sorts of attacks [14]. A basic adjustment was expected to the fundamental way to deal with handle the circumstance for the way that assailant can continue changing the IP source address amid the attack. In spite of the fact that the imprints in DPM can't be parodied, the way that successive spoofing of IP source address with different qualities by the attacker, might diminish the DPM's viability. The destination could make to depend on the imprints, which can't be satirizing to take care of this issue. The destination can confirm that two parts of the entrance address do has a place with the same entrance address, without depending on the source location of the bundle, by utilizing an all-around known hash capacity. This arrangement requires sending extra checks with hash esteem. In any case, the quantity of packets expected to remake the entrance location will be expanded. Deterministic Edge Router Marking (DERM) for safeguard against DDOS attack was proposed to highlight remaking approach. The recreation was finished by client in two stages. To be specific, a sifting stage and an assailant distinguishing proof stage. The separating stage included a setting of banner in the table bolstered on imprints, in arriving bundles for ID of attacking activity and use of these imprints to channel the attack movement. The assailant recognizable proof stage included taking note of down of the IP location of entrance bundle and to check them against the channel table sections. The quantity of bundles required for the recognizable proof of an attacker is additionally little.

H. Dong et.al [12], author proposed a conceptual framework is designed for a semantic focused crawler to accomplish the goal of annotation, automatic service discovery and classification in the Digital Ecosystems environment. A semantic focused crawler integrates the speciality of the strength of metadata abstraction from the metadata abstraction crawlers. After experiments, author drawn two-fold conclusions that is 1)increase of the threshold value can diminish the amount of associated and non-associated metadata and 2) the higher threshold values can benefit the overall performance of the crawler.

2. IP Traceback Approaches

3.1 Probabilistic Packet Marking (PPM)

In view of methodologies of IP traceback plan examined above PPM goes under Basic Principle: Marking, Processing Mode: Probabilistic, Location: Network Group. Figure1 outlines the PPM approach for IP traceback

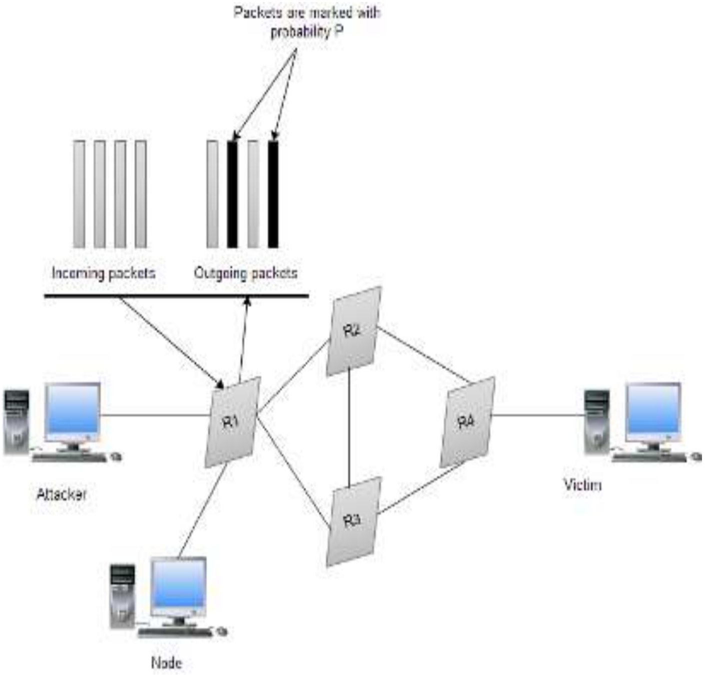

Figure 1: PPM approach for IP Traceback

In PPM [10], it is expected that attacking bundles are substantially more regular than ordinary packets. It denotes the bundles probabilistically with some way data and permits the victim to revamp the way in view of checked packets. Yet, packets are marked arbitrarily taking into account some likelihood along these lines it is hard to recreate the way. It requires high computational work when there are numerous sources. Numerous sources could bring about false positive rate [10]. To defeat this issue, progress and validated PPM was proposed [5], which could follow more assets at one time and tackled the issue of spoofed marking. To decrease the issue of remaking [10] another methodology is exhibited which lessened computational time and false positive rate. Time and route setup time and these are main advantage of proposed protocol. While performing route setup blue wave protocol captures the features of Bluetooth technology.

3.2 Deterministic Packet Marking (DPM)

Taking into account methodologies of IP traceback plan talked about above DPM goes under Basic Principle: Marking, Processing Mode: Deterministic at bundle level, Location: Source Group. Figure 2 shows the DPM approach for IP traceback.

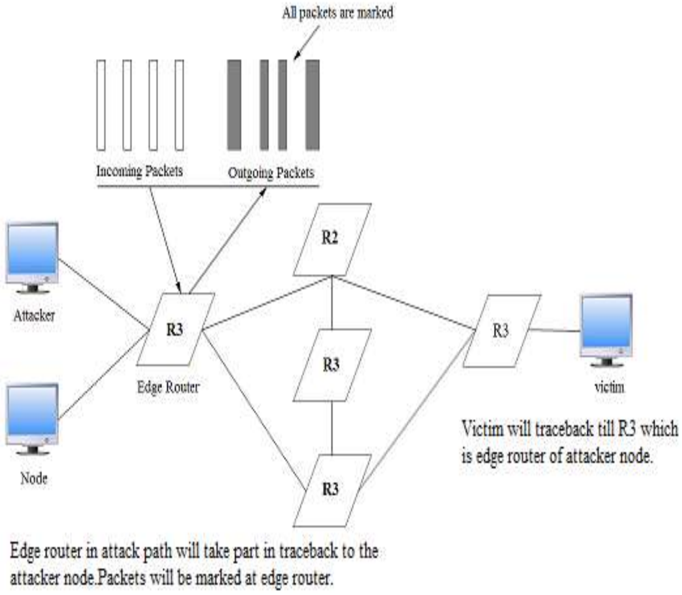
All packets are marked
Incoming Packets
Outgoing Packets
Attacker
Node
R3
Edge Router
R2
R3
R3
R3
victim
Victim will traceback till R3 which is edge router of attacker node.
Edge router in attack path will take part in traceback to the attacker node.Packets will be marked at edge router.

Figure 2: DPM approach for IP Traceback

At the DPM empowered router, each packet navigated is marked in Deterministic Packet Marking. It implies that each bundle that experiences a router is recorded with some included data about the router interface. The strategy depends on two key presumptions: First, any given packet might be created by the Attacker and second, routers have constrained CPU and memory.

The prime centre was on security against the mysterious attacks [15]. In this approach, the character of attacker(s) is not immediately accessible for the victim. Since the source IP location is spoofed. Thusly, a strong system to traceback the right IP was required and the deterministic bundle marking was at first proposed [15]. The deterministic bundle marking (DPM) strategy depends on checking packets with the partial location data of entrance interface forlorn. The victim can recover the whole address data in the wake of getting a few packets from a specific attacking have or has. The whole way is not by any means required for the traceback, as it would be distinctive for diverse bundles in light of the fact that, the course is haphazardly trailed by diverse packets. This methodology is adaptable, simple to actualize; likewise it presents no vast transfer speed and makes no extra preparing overhead on the system types of gear, similar to routers. It can follow a great many attackers at the same time amid a Distributed Denial of Service (DDOS) attack. All handling is done at the victim side. Internet Service Provider (ISPs) association in these procedures is exceptionally restricted. Least changes are should have been be done to the foundation and negligible operations are required to introduce the Deterministic Packet Marking. The fancied nature of any traceback plan is not to uncover the inner topology of supplier's system, which is accomplished by the Deterministic Packet Marking.

3.3 Comparison Parameters

Base on comparative parameters, correlation of handling modes PPM, DPM and DFM is compressed in taking after Table 1.

Parameters	PPM	DPM	DFM
Computational Overhead	Moderate	Low	Very Low
Maximum Traceback Ability	Edge Router	Upto ingress interface of edge router	Upto attacker node
Flow Marking	No	No	Yes
No of packet marked at ingress interface of edge router	Random number of packets	Each packet of every flow	Few packets of every flow
Minimum Packets required to trace IP	More than DPM	More than DFM	Minimum 4

Table1: Comparison of IP Traceback Approaches.

3. CONCLUSION

With expanding number of web clients, issue of following the wellspring of Denial of Service (DoS) attack is looked into. In this paper, a wide study has been done to recognize and group the current IP traceback plans. Selecting the best system for packet marking is the key point in following the source IP. Difficulties of past IP traceback strategies was, remaking the attack way proficiently and following precise assailant hub covered up by a NAT or intermediary server. These difficulties are overcome by DFM IP traceback approach. What is more it gives discretionary confirmation strategy. Deterministic Flow Marking (DFM) gives higher traceback precision and confirmation, yet victim assets in connect way are expended even before the traceback is finished. Along these lines, a need emerges to give a component to save the assets in connect way even before the IP traceback. To achieve this, attack recognition, counteractive action and traceback with novel approach can fortify complete security stage to safeguard the assets in attack way even before traceback.

With increasing number of internet users, issue of tracing the source of Denial of Service (DoS) attack is reviewed. In this paper, a wide survey has been carried out to recognize and classify the existing IP traceback schemes. Selecting the best method for packet marking is the key point in tracing the source IP. Challenges of previous IP traceback methods was, reconstructing the attack path efficiently and tracing exact attacker node hidden by a NAT or proxy server. These challenges are overcome by Deterministic Flow Marking IP traceback approach. In addition it provides optional authentication method. Deterministic Flow Marking provides higher traceback accuracy and authentication, but victim resources in attach path are consumed even before the traceback is completed. Therefore, a need arises to provide a mechanism to preserve the resources in attach path even before the IP traceback. To accomplish this, attack detection, prevention and traceback with novel approach can reinforce complete security platform to preserve the resources in attack path even before traceback.

References

[1] V. Aghaei-Foroushani and N. Zincir-Heywood, “Deterministic and Authenticated Flow Marking for IP Traceback”, The 27th IEEE International Conference on Advanced Information Networking and Applications (AINA-2013), March 2013.

[2] T. Subbulakshmi, I. A. A. Guru and S. M. Shalinie, “Attack Source Identification at Router Level in Real Time using marking Algorithm Deployed in Programmable Routers”, ICRTIT, 2011.

[3] Z. Gao, N. Ansari, “Tracing Cyber Attacks from the Practical Perspective”, IEEE Communications Magazine, 2005.

[4] R. Shokri, A. Varshovi, H. Mohammadi, N. Yazdani, B. Sadeghian, “DDPM: Dynamic Deterministic Packet Marking for IP Traceback”, 2006.

[5] D. X. Song, A. Perrig, “Advanced and Authenticated Marking Schemes for IP Traceback,” INFOCOM, 2001

[6] V. Kuznetsov, H. SandStrom, A, Simkin, “An Evaluation of Different IP traceback Approaches”, Information and Communications technology, 2002.

[7] S V Athawale, D N Chaudhari, “Towards effective client-server based advent intrusion prevention system for WLAN”, Conference International Conference on Computer, Communication and Control (IC4), IEEE, 2015(1-5).

[8] S V Athawale, “International Journal of Advanced Research in Computer Science and Software Engineering”, International Journal of Advanced Research in Computer Science and Software Engineering 2013(280-283).

[9] D. Johnson, A. Menezes and S. Vanstone, “The Elliptic Curve Digital Signature Algorithm (ECDSA)”, Certicom Corporation, 2009.

[10] S. Savage, D. Wetherall, A. Karlin and T. Anderson, “Network Support for IP Traceback,” IEEE/ACM Transactions on Networking, 2001.

[11] S. Matsuda et al., “Design and Implementation of Unauthorized Access Tracing System,” SAINT 2002.

[12] B. Gong., K. Sarac, “IP Traceback based on Packet Marking and Packet Logging”, University of Texas at Dallas, 2005.

[13] A. Yaar, A. Perrig, D. Song, “Pi: A Path Identification Mechanism to Defend Against DDOS Attacks” Proc. Symposium on Security and Privacy, 2003.

[14] M. T. Goodrich, “Efficient Packet Marking for Large-Scale IP Trace back,” Proc. Ninth ACM Conference of Computer and Communication Security, 2002.

[15] Ansari, Belenky, N. “Deterministic Packet Marking”, New Jersey Institute of Technology, 2005.

Author Profile

Anushree, pursuing Bachelor’s degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India.

Priyanka Baviskar, pursuing Bachelor’s degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India.

Pooja Dalimbe, pursuing Bachelor’s degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering, Pune, Maharashtra, India.

Sneha Dhaswadikar, pursuing Bachelor’s degree from Savitribai Phule Pune University in A.I.S.S.M.S College of Engineering,Pune, Maharashtra, India.

S V Athawale, Assistant Professor, completed M.Tech from BVP Pune, Maharashtra, India. 10 papers have been published and presented in various National and International Conferences as of now.