IPHV7I10023X
International Journal Of Advanced Research and Innovation -Vol.7, Issue .I
ISSN Online: 2319 – 9253
Print: 2319 – 9245

Probe Packet Security For Wireless and Mobile Ad-hoc Networks

B. Krishna Mohan[#1], B.Srilakshmi[#2] and DT Subba Reddy[#3]

[#] *Department of Computer Science &Engineering,Guntur Engineering college, Guntur, AP, India.*

Abstract: — **Wireless Mobile Ad-hoc networks are protected from various treats by means of Antivirus, firewalls, Intrusion Detection system and security software's. Due to the various changes in the security level, open environment and lack of centralized security, the open wireless communication system is critical to communicate due to the presence of the attackers. In the existing systems are not sufficient and effective in preventing the attacks from the attackers. So that the effective detection system is required to monitors the network defects, detects misbehavior or anomalies and in order to prevent the attacks the networks. So that in this paper, we propose a new technique of Intrusion Detection System against DDOS attack in Wireless Mobile Ad-hoc Networks using probe packets. This approach will resist the malicious attacks of DDOS in the Wireless Mobile Ad-hoc Network (MANET) effectively.**

Keywords— *Mobile ad-hoc network (MANET), Security, algorithms, distributed denial of service (DDOS), intrusion detection system (IDS).*

I. INTRODUCTION

Mobile ad hoc network (MANET) is the rising technology, is used for wireless communication between the two or more devices or nodes or terminals. There are many security services for the wireless mobile networks but for MANETs are authentication, confidentiality, integrity, non repudiation and availability are very important. It has high strength to communicate or send data in critical situation like battlefields and commercial purpose also. It communicate by nodes itself, though it communicate well through the nodes it has no centralized system and security level is low. Attackers easily attack the data. The Intrusion attack in the wireless networks is easily acquired compared to the wired networks. So that DDOS (Distributed Denial of Service) in the Mobile Ad-hoc networks was easily attacks the networks. DDOS are a large scale coordinated attack by sending the huge amount of packets to the target node. So that in the victim side consumes the larger bandwidth and not allows the important packets to the target or destination.

To overcome the issues happened due to the DDOS attacks in the wireless mobile network, we introduce the secure Intrusion Detection System (IDS) in the mobile networks. IDS system was described by two types. They are: first is signature based IDS and secondly Anomaly based IDS. In the signature based intrusion detection, it has previously saved patron or signature in the database of the IDS. If there is any disturbance found in the network, IDS compares the signature or patron with the previously saved one. If IDS found the same means it will found the attacks. In these IDS updating the signature is very compulsory. However it found the attacks, signature is not in the database of IDS means it will not find the attacks of DDOS. In the anomaly intrusion detection, it makes the normal profile of the network and then the normal profile consider as the base profile. Finally base profile of the network gets compared with monitored network profile. This technique of the IDS can easily detect the DDOS in the wireless mobile ad-hoc networks.

II. RELATED WORKS

The DDOS attacks not only the wireless networks and also plague the internet, cloud computing, websites and so on. This is related to the DDOS attacks and its security level. The DDOS attacks various level of the different application. e.g. if DDOS attacks on the application layer means it will limits resources, curtails revenue and leads to the customer dissatisfaction.

Abraham Yaar, Adrian Perrig and Dawn Song[1], proposes a scheme of a path identification mechanism against the DDOS attacks by introducing the PI(path identifier). Distributed Denial of Service (DDOS) attacks continue to plague the Internet. Defense against these attacks is complicated by spoofed source IP addresses, which make it difficult to determine a packet's true origin. We propose Pi (short for Path Identifier), a new packet marking approach in which a path fingerprint is embedded in each packet, enabling a victim to identify packets traversing the same paths through the Internet on a per packet basis, regardless of source IP address spoofing.

Jelena Mirkovic, Janice Martin and Peter Reihe[2], This paper proposes a taxonomy of distributed denial-of service attacks and a taxonomy of the defense mechanisms that strive to counter these attacks. The attack taxonomy is illustrated using both known and potential attack mechanisms. Along with this classification we discuss important features of each attack category that in turn define the challenges involved in combating these threats. The defense system taxonomy is illustrated using only the currently known approaches. The goal of the paper is to impose some order into the multitude of existing attack and defense mechanisms that would lead to a better understanding of challenges in the distributed denial-of-service field.

Li-chiou chen and Kathleen M Carley [3] proposes a method to defense against the DDOS attack on website by developing the computational testbed and its associated technology.

Sanjay B Ankali and Dr. D V Ashoka [4] proposed a scheme to prevent the internet from the DDOS attacks by using the HTTP and FTP architecture. This paper designs two independent architectures for HTTP and FTP which uses an extended hidden semi-Markov model is proposed to describe the browsing habits of web searchers.

Wei-Shen Lai et al [5] proposes the Denial of service attacks occur when the attacks are from a single host, whereas distributed denial of service attacks occur when multiple affected systems flood the bandwidth or resources of a targeted system. Although it is not possible to exempt entirely from denial of service or distributed denial of service attacks, we can limit the malicious user by controlling the traffic flow. In the paper, we propose to monitor the traffic pattern in order to alleviate distributed denial of service attacks. A bandwidth allocation policy will be adopted to assign normal users to a high priority queue and suspected attackers to a low priority queue.

.

Shabana Mehfuz1 et al [6] have proposed a ant routing algorithm (SPA-ARA) for mobile ad hoc networks that is inspired from ant colony optimization (ACO) algorithms technique used to prevent the DDOS attacks. In this paper, we have proposed a new secure power-aware ant routing algorithm (SPA-ARA) for mobile ad hoc networks that is inspired from ant colony optimization (ACO) algorithms which are a swarm intelligent technique. In this algorithm, we have introduced a new metric, next-hop availability, which is a combination of two metrics. It maximizes path availability and minimizes travel time of packets, and therefore it offers a good balance between selection of fast paths and a better use of network resources. The protocol also incorporates a trust model which helps in detection of unauthorized and compromised nodes in MANETs.

Giriraj Chauhan and Sukumar Nandi [7] introduce a QoS aware on demand routing protocol that uses signal stability as the routing criteria along with other QoS metrics. The proposed QoS Aware Stable path Routing (QASR) is designed over Signal Stability based Adaptive routing (SSA) and aims to select stable QoS routes that can survive for longer period of time. Using the NS-2 simulator, we have conducted an extensive set of simulations to verify the effectiveness of QASR with a wide variety of mobility patterns and network loads. A comprehensive performance analysis of QASR and comparison with other QoS aware routing for MANET is also presented in the paper.

Xiapu Luo et al [8] have presented the important problem of detecting pulsing denial of service (PDoS) attacks which send a sequence of attack pulses to reduce TCP throughput. This paper addresses the important problem of detecting pulsing denial of service (PDoS) attacks which send a sequence of attack pulses to reduce TCP throughput. Unlike previous works which focused on a restricted form of attacks, we consider a very broad class of attacks. In particular, our attack model admits any attack interval between two adjacent pulses, whether deterministic or not. It also includes the traditional flooding-based attacks as a limiting case (i.e., zero attack interval). Our main contribution is Vanguard, a new anomaly-based detection scheme for this class of PDoS attacks. The Vanguard detection is based on three traffic anomalies induced by the attacks, and it detects them using a CUSUM algorithm.

Xiaoxin Wu et al [9] propose a DoS mitigation technique that uses digital signatures to verify legitimate packets, and drop packets that do not pass the verification. Since nodes are selfish, they may not perform the verification so that they can avoid paying the overhead. A bad packet that escapes verification along the whole network path will bring a penalty to all its for- warders. A network game can be formulated in which nodes along a network path, in optimizing their own benefits, are encouraged to act collectively to filter out bad packets

S.A.Arunmozhi and Y.Venkataramani [10] proposed a defense scheme to improve the performance of the ad hoc networks. Our proposed defense mechanism uses the medium access control (MAC) layer information to detect the attackers. The status values from MAC layer that can be used for detection are Frequency of receiving RTS/CTS packets, Frequency of sensing a busy channel and the number of RTS/DATA retransmissions. Once the attackers are identified, all the packets from those nodes will be blocked. The network resources are made available to the legitimate users.

Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim [11] propose the entropy-based detection mechanism against DDoS attacks in order to guarantee the transmission of normal traffic and prevent the flood of abnormal traffic. The OPNET simulation results show that our ideas can provide enough services in DDoS attack.

Qi Chen, Wenmin Lin, Wanchun Dou, Shui Yu [12] proposed a Confidence-Based Filtering method (CBF) to detect DDoS attack in cloud computing environment. in this paper. Concretely speaking, the method is deployed by two periods, i.e., non-attack period and attack period. More specially, legitimate packets are collected at non-attack period, for extracting attribute pairs to generate a nominal profile. With the nominal profile, the CBF method is promoted by calculating the score of a particular packet at attack period, to determine whether to discard it or not. At last, extensive simulations are conducted to evaluate the feasibility of the CBF method. The result shows that CBF has a high scoring speed, a small storage requirement and an acceptable filtering accuracy, making it suitable for real-time filtering in cloud environment.

III.PROPOSED WORK

In a wireless mobile Ad-hoc network (MANET) has a main problem of DDOS attacks, not only in the MANET networks it attacks the wireless sensor networks too. To overcome the above issues we introduce the Intrusion Detection System with two parameters: one is packet reception rate (PRR) and the other is inter arrival time (IAT). These parameters are not solve all problems is in the MANET network and wireless sensor networks. So that we also introduce the another parameter to solve this problem, which is created by DDOS attacks in the MANET network. In this paper we proposed the ADOV routing protocol and IDS (Intrusion Detection System). In order to prevent the DDOS attacks in the MANET, whereas the communication between the two or more devices by intermediate nodes itself without any centralized system so that attacks can be achieved easily in the network. To overcome this attack we simulate the three different conditions: first is normal time second is Attack time and finally IDS module time and these three conditions simulated.

IV. ALGORITHM

In the algorithm first we create the IDS node and set the ADOV as a routing protocol.

After that IDS node checks for the network configuration and capture the nodes is in the radio range and also the capture the information of all nodes or else out of range or destination unreachable. From the information the IDS nodes creates the normal profile that contains the information of packets, time of packet send and receive and threshold. After creating the normal profile, the threshold checking is done in the network. i.e. if network load is smaller than or equal to maximum limit and new profile is smaller than or equal to maximum threshold and new profile is greater than or equal to minimum threshold then there is no any kind of attack present. Else there is an attack in the network and find the attack. For doing it compare normal profile with each new trace value i.e. check packet type, count unknown packet type, arrival time of packet, sender of packet, receiver of packet. And after detection of any anomaly in that parameters then block that packet sender node (attacker node).

```
Create node =ids;
Set routing = AODV;
If ((node in radio range) && (next hop! =Null)
{
Capture load (all_node)
Create normal_profile (rreq, rrep, tsend, trecv, tdrop)
{pkt_type; // AODV, TCP, CBR, UDP
Time;
Tsend, trecv, tdrop, rrep, rreq
}
Threshold_parameter ()
If ((load<=max_limit) && (new_profile<=max_threshold) && (new_profile>=min_threshold))
{
No any attack;
}
Else {
Attack in network;
Find_attack_info ();
}
Else {
"Node out of range or destination unreachable"
}
Find_attack_info ()
{
Compare normal_profile into each trace value
If (normal_profile! = new trace_value)
{
Check pkt_type;
Count unknown pkt_type;
Arrival time;
Sender_node;
Receiver_node;
Block_Sender_node(); //sender node as attacker
}
```

V. SIMULATION WORKS/RESULTS

We have simulated our system in DOT NET. We implemented and tested with a system configuration on Intel Dual Core processor, Windows XP and using VISUAL STUDIO 2008. We have used the following modules in our implementation part. The details of each module for this system are as follows:

Network Creation and Socket Connection

In this module, we first create the simulation environment by creating the network as three entities viz: Source node, Router Node and Destination Node. The source node is created with the properties of sending the files using socket connection using IP Address provided by the user. Then the router node and destination node is created with the socket connection of using their properties.

Normal Case

In this module, we design the system using the normal case scenario that is: We set number of sender and receiver nodes and transport layer mechanism as TCP and UDP with routing protocol as AODV (ad-hoc on demand distance vector) routing. After setting all parameter simulate the result through our simulator.

Attack Case

In Attack module we create one node as attacker node whose set the some parameter like scan port , scan time , infection rate , and infection parameter , attacker node send probing packet to all other neighbour node whose belongs to in radio range, if any node as week node with nearby or in the radio range on attacker node agree with communication through attacker node, so that probing packet receive by the attack node and infect through infection, after infection this infected node launch the DDOS (distributed denial of service) attack and infect to next other node that case our overall network has been infected.

IDS Case

In IDS (Intrusion detection system) we set one node as IDS node, that node watch the all radio range mobile nodes if any abnormal behaviour comes to our network, first check the symptoms of the attack and find out the attacker node , after finding attacker node, IDS block the attacker node and remove from the DDOS attack. In our simulation result we performed some analysis in terms of routing load , UDP analysis , TCP congestion window, Throughput Analysis and overall summery.

Simulation Results Analysis

In this module we analyze the results, in our simulations we use several performance metrics to compare the proposed AODV protocol with the existing one [20]. The following metrics were considered for the comparison were

a) Throughput: Number of packets sends in per unit of time.

b) Packet delivery fraction *(PDF):* The ratio between the numbers of packets sends by source nodes to the number of packets correctly received by the corresponding destination nodes.

VI. Conclusion

The proposed mechanism eliminates the need for a centralized trusted authority which is not practical in ad-hoc network due to their self organizing nature. The results demonstrate that the presence of a DDOS increases the packet loss in the network considerably. The proposed mechanism protects the network through a self organized, fully distributed and localized procedure. The additional certificate publishing happens only for a short duration of time during which almost all nodes in the network get certified by their neighbours. After a period of time each node has a directory of certificates and hence the routing load incurred in this process is reasonable with a good network performance in terms of security as compare with attack case. We believe that this is an acceptable performance, given that the attack prevented has a much larger impact on the performance of the protocol. The proposed mechanism can also be applied for securing the network from other routing attacks by changing the security parameters in accordance with the nature of the attacks.

VII. References

[1]. Abraham Yaar Adrian Perrig Dawn Song Carnegie Mellon University fayaar, perrig, dawnsongg@cmu.edu Pi: A Path Identification Mechanism to Defend against DDoS Attacks

[2]. Jelena Mirkovic, Janice Martin and Peter Reiher A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms Computer Science Department University of California, Los Angeles Technical report #020018

[3]. Li-chiou chen and Kathleen M Carley Modelling Distributed Denial Of Service Attacks and Defenses

[4]. Sanjay B Ankali Department of Information Science & Engg, SJBIT, Bangalore, India Email: sanjay.ankali@yahoo.com Dr. D V Ashoka, Professor & Head, Department of Information Science & Engg, SJBIT, Bangalore, India Email: dr.ashok_research@hotmail.com Detection Architecture of Application Layer DDoS Attack for Internet Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:984-990 (2011)

[5]. F. Anjum, D. Subhadrabandhu and S. Sarkar. Signaturebased intrusion detection for wireless Ad-hoc networks," Proceedings of Vehicular Technology Conference, vol. 3, pp. 2152-2156, USA, Oct. 2003.

[6]. D. E. Denning, An Intrusion Detection Model," IEEE Transactions in Software Engineering, vol. 13, no. 2, pp. 222-232, USA, 1987.

[7]. Wei-Shen Lai, Chu-Hsing Lin , Jung-Chun Liu , Hsun-Chi Huang, Tsung-Che Yang: Using Adaptive Bandwidth Allocation Approach to Defend DDoS Attacks, International Journal of Software Engineering and Its Applications, Vol. 2, No. 4, pp. 61-72 (2008)

[8]. ShabanaMehfuz, Doja,M.N.: Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs", Journal of Artificial Evolution and Applications (2008)

[9]. Giriraj Chauhan,Sukumar Nandi: QoS Aware Stable path Routing (QASR) Protocol for MANETs, in First International Conference on Emerging Trends in Engineering and Technology,pp. 202-207 (2008).

[10]. Xiapu Luo, Edmond W.W.Chan,Rocky K.C.Chang: Detecting Pulsing Denial-of-Service Attacks with Nondeterministic Attack Intervals, EURASIP Journal on Advances in Signal Processing (2009)

[11]. Xiaoxin Wu, David,K.Y.Yau, Mitigating Denial-of-Service Attacks in MANET by Distributed Packet Filtering: A Game theoretic Approach, in Proceedings of the 2nd ACM symposium on Information, computer and communication security, pp 365-367 (2006)

[12]. S.A.Arunmozhi, Y.Venkataramani "DDoS Attack and Defense Scheme in Wireless Ad hoc Networks" International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.3, May 2011, DOI: 10.5121/ijnsa.2011.3312.

[13]. Jae-Hyun Jun, Hyunju Oh, and Sung-Ho Kim "DDoS flooding attack detection through a step-by-step investigation" 2011 IEEE 2nd International Conference on Networked Embedded Systems for Enterprise Applications, ISBN: 978-1-4673-0495-5,2011

[14]. Qi Chen , Wenmin Lin , Wanchun Dou , Shui Yu " CBF: A Packet Filtering Method for DDoS Attack Defence in Cloud Environment", 2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing. ISBN: 978-0-7695-4612-4.2011

[15]. Yih-Chun Hu, Adrian Perrig, and David B. Johnson., "Packet Leashes A Defense against Wormhole Attacks in Wireless Ad Hoc Networks" In Proceedings of the Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003), April 2003

[16]. Patroklos g. Argyroudis and donal o'mahony, "Secure Routingfor Mobile Ad hoc Networks", IEEE Communications Surveys & Tutorials Third Quarter 2005.

[17]. K. Balakrishnan, J. Deng, and P.K. Varshney, "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks" Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.

[18]. Mohammad Al-Shurman and Seong-Moo Yoo, Seungjin Park, "Black Hole Attack in Mobile Ad Hoc Networks" ACMSE'04, April 2-3, 2004, Huntsville, AL, USA.

[19]. Yih-Chun Hu, Adrian Perrig, David B. Johnson, "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols" WiSe 2003, September 19, 2003, San Diego, California, USA.

Author's Profile:

[1] B.Krishna Mohan pursuing M.Tech (C.S.E) at Guntur Engineering College,Guntur.His intersted research area is wireless Networks.

[2] B.Srilakshmi Received M.Tech(C.S.E) JNTUK .Her Interested area is Wireless Networks and MANETS.

[3] DT.Subba Reddy Received his M.E (C.S.E) from Satyabhama university, Chennai. He is working as Head of the Department of CSE at Guntur Engineering College, Guntur. He guided many projects in the area of Networks for CSE & IT Students.