International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 06 | June - 2022 Impact Factor: 7.185 ISSN: 2582-3930

A SECURE INTRUSION DETECTION SYSTEM AGAINST DDOSATTACK IN WIRELESS MOBILE AD1

Mrs.V.Manimegalai , M.E – II[nd] year, CSE, P.S.V. College Of Engineering & Technology, Krishnagiri.

Dr.S.Chandra Sekeran, Professor, Department of Computer Science and Engineering, P.S.V.College of Engineering & Technology, Krishnagiri.

ABSTRACT:

Wireless Mobile ad-hoc network (MANET) is an emerging technology and have great strength to be applied in critical situations like battlefields and commercial applications such as building, traffic surveillance, MANET is infrastructure less, with no any centralized controller exist and also each node contain routing capability, Each device in a MANET is independently free to move in any direction, and will therefore change its connections to other devices frequently. So one of the major challenges wireless mobile ad-hoc networks face today is security, because no central controller exists. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a link layer ad hoc network. Ad hoc also contains wireless sensor network so the problems is facing by sensor network is also faced by MANET. While developing the sensor nodes in unattended environment increases the chances of various attacks. There are many security attacks in MANET and DDoS (Distributed denial of service) is one of them. Our main aim is seeing the effect of DDoS in routing load, packet drop rate, end to end delay, i.e. maximizing due to attack on network. And with these parameters and many more also we build secure IDS to detect this kind of attack and block it. In this paper we discussed some attacks on MANET and DDOS also and provide the security against the DDOS attack.

1. INTRODUCTION

Mobile ad hoc network (MANET) is a group of two or more devices or nodes or terminals with a capability of wireless communications and networking which makes them able to communicate with each other without the aid of any centralized system. This is an autonomous system in which nodes are connected by wireless links and send data to each other. As we know that there is no any centralized system so routing is done by node itself. Due to its mobility and self-routing capability nature, there are many weaknesses in its security. To solve

the security issues we need an Intrusion detection system, which can be categorized into two models: Signature-based intrusion detection and anomaly-based intrusion detection. In Signature-based intrusion detection there are some previously detected patron or signature are stored into the data base of the IDS if any disturbance is found in the network by IDS it matches it with the previously saved signature and if it is matched than IDS found attack. But if there is an attack and its signature is not in IDS database then IDS cannot be able to detect attack. For this periodically updating of database is compulsory.

To solve this problem anomaly based IDS is invented, in which firstly the IDS makes the normal profile of the network and put this normal profile as a base profile compare it with the monitored network profile. The benefit of this IDS technique is that it can be able to detect attack without prior knowledge of attack. Intrusion attack is very easy in wireless network as compare to wired network. One of the serious attacks to be considered in ad hoc network is DDoS attack. A DDoS attack is a large scale, coordinated attack on the availability of services at a victim system or network resource. The DDoS attack is launched by sending huge amount of packets to the target node through the co-ordination of large amount of hosts which are distributed all over in the network.

2. LITERATURE SURVEY

2.1 SIGNATURE BASED INTRUSION DETECTION FOR WIRELESS AD-HOCNETWORKS

AUTHORS: F. Anjum, D. Subhadrabandhu and S. Sarkar.

In this paper, particularly focusing on intrusion detection in wireless networks. The intrusion detection community has been concentrating mainly on wired networks. Techniques geared towards wire line networks would not suffice for an environment consisting of multi hop wireless links because of the various differences such as lack of fixed infrastructure, mobility, the ease of listening to wireless transmissions, lack of clear separation between normal and abnormal behavior in ad hoc networks. In this paper, consider the signature detection technique and investigate the ability of various routing protocols to facilitate intrusion detection when the attack signatures are completely known. Reactive ad-hoc routing protocols suffer from a serious problem due to which it might be difficult to detect intrusions even in the absence of mobility.

Mobility makes the problem of detecting intruders harder. Investigation of a relationship between the probability of detecting an intrusion and the number of nodes that must participate in the process of detecting intrusions.

2.2 AN INTRUSION DETECTION MODEL AUTHORS: D. E.

Denning

A model of a real-time intrusion-detection expert system capable of detecting break-ins, penetrations, and other forms of computer abuse is described. The model is based on the hypothesis that security violations can be detected by monitoring a system's audit records for abnormal patterns of system usage. The model includes profiles for representing the behavior of subjects with respect to objects in terms of metrics and statistical models, and rules for acquiring knowledge about this behavior from audit records and for detecting anomalous behavior. The model is independent of any particular system, application environment, system vulnerability, or type of intrusion, thereby providing a framework for a general-purpose intrusion-detection expertsystem.

2.3 USING ADAPTIVE BANDWIDTH ALLOCATION APPROACH TO DEFEND DDOSATTACKS

AUTHORS: Wei-Shen Lai, Chu-Hsing Lin, Jung-Chun Liu, Hsun-Chi Huang, Tsung-Che Yang

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 orresources of a targeted system. Although it is not possible to exempt entirely from denial of service or distributed denial of service attacks, but it is possible to limit the malicious user by controlling the traffic flow. A bandwidth allocation policy will be adopted to assign normal users to a high priority queue and suspected attackers to a low priority queue. Simulations conducted in network simulator of a proposed system is a priority queue-based scheme shows its effectiveness in blocking and attacking the traffic while maintaining constant flows for legitimate traffic.

2.4 SWARM INTELLIGENT POWER-AWARE DETECTION OF UNAUTHORIZEDAND COMPROMISED NODES IN MANETS

AUTHORS: ShabanaMehfuz, Doja,M.N

Characteristics of mobile ad hoc networks (MANETs) such as lack of central coordination, mobility of hosts, and limited availability of resources make quality of service (QoS) provisioning very challenging. Limited resource availability such as battery power and insecure medium is one of the major QoS issues to be dealt with. In the proposed project, 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, introducing 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.

2.5 QOS AWARE STABLE PATH ROUTING (QASR) PROTOCOL FOR MANETSAUTHORS: Giriraj Chauhan,Sukumar Nandi

Dynamic topology and limited bandwidth of mobile ad hoc networks (MANETs) make end-to-end QoS support an inherently complex and difficult task. Most of the current QoS routing protocols propose routing based on two QoS metrics. This paper introduces 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, conducting 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.

2.6 DETECTION OF PULSING DOS ATTACKS AT THEIR SOURCE NETWORKSAUTHORS: Ming Yu , Xiong-wei Li

Pulsing Denial of Service (PDoS) is a type of DoS attack. Its attacking behavior is intermittent rather than constant, which helps it avoid being detected. In this paper, an adaptive detection method is proposed for source-end detection of PDoS attacks. It has three distinctive features: (i) its detection statistic is based on the discrepancy in the aggregated outbound and inbound packets; (ii) a self-adaptive detection threshold adapts it quickly to the variations of network traffic and the latest detection result; (iii) random abnormalities in the normal network traffic can be filtered by consecutive accumulation of threshold violations. Experimental results show the minimum attack traffic that can be detected is less than 35% of the background traffic, under the requirements that probability of false alarms is less than 10-6, probability of a miss during an attack is less than 10-2 and detection delay is within 7 sampling periods.

2.7 MITIGATING DENIAL-OF-SERVICE ATTACKS IN MANET BY DISTRIBUTED PACKET FILTERING: A GAME-THEORETIC APPROACH AUTHORS: Xiaoxin Wu and David K. Y. Yau

Defending against denial-of-service (DoS) in a mobile ad hoc network (MANET) is challenging because the network topology is dynamic and nodes are selfish. In this paper, we 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 forwarders. 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. Analytical results show that Nash equilibrium can be attained for players in the proposed game, in which significant benefits can beprovided to forwarders such that many of the bad packets will be eliminated by verification.

2.8 CBF: A PACKET FILTERING METHOD FOR DDOS ATTACK DEFENSE INCLOUD ENVIRONMENT

AUTHORS : Qi Chen,Wenmin Lin,Wanchun Dou And Shui Yu

Distributed Denial-of-Service attack (DDoS) is a major threat for cloud environment.Traditional defending approaches cannot be easily applied in cloud security due to their

relatively low efficiency, large storage, to name a few. In view of this challenge, a Confidence- Based Filtering method, named CBF, is investigated for 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.

3. SYSTEM STUDY

3. 1 EXISTING SYSTEM

In existing system, Mobile ad-hoc networks devices or nodes or terminals with a capability of wireless communications and networking which makes them able to communicate with each other without the aid of any centralized system. This is an autonomous system in which nodes are connected by wireless links and send data to each other. There is no any centralized system so routing is done by node itself. Due to its mobility and self- routing capability nature, there are many weaknesses in its security. One of the serious attacks to be considered in ad hoc network is DDoS attack. A DDoS attack is launched by sending huge amount of packets to the target node through the co-ordination of large amount of hosts which are distributed all over in the network. At the victim side this large traffic consumes the bandwidth and not allows any other important packet reached to the victim.

3.1.1 DRAWBACKS OF EXISTING SYSTEM

- Performance degradation while data transfer from server to client.
- Quality loss while receiving the data's.
- DDOS attack occurs when transmitting the data's through the router.
- This kind of attack may destroy the data's.
- Easily intruders attack the client.
- Increasing operational costs.

- Data reliability is too low.
- No proper deduction of attackers in client server computing.

3.2 PROPOSED SYSTEM

DDOS attack is the main problem in all ad hoc scenario i.e. in MANAT and as well as in wireless sensor networks. In this paper has an intrusion detection system in wireless sensor network which uses the anomaly intrusion detection system in which IDS uses two intrusion detection parameters, packet reception rate (PRR) and inter arrival time (IAT).But only these two parameters are not completely sufficient for intrusion detection in wireless sensor network and aswell as in MANET. If we also add other parameters into it to make it works more accurately. So in our proposal we use different intrusion detection parameters in mobile Ad hoc networks. We assume that a mobile ad hoc network contains two or more than two mobile devices that are communicate from each other through intermediate nodes, each node contain routing table , in our proposal we use AODV routing protocol in all normal module attack module and Intrusion Detection System (IDS) for prevention through attack. In this paper we simulate the three different condition results normal time, Attack time and IDS module time through simulation modules.

3.2.1 ADVANTAGES OF THE PROPOSED SYSTEM

- This proposed method was implemented by used IDS methodology.
- IDS provide sub techniques for contributing the data transfer in efficient manner.
- Those techniques are PRR and SRR, it is very useful for transmitting the data in clientserver systems.
- Provides solutions less computationally and minimize the data loss.
- It is good methodology for identifying the intruders.
- In this system give suggestion to transfer the secured data to the client by using IDS.

3.3 MODULES DESCRIPTION

1. Network Creation and Socket Connection module
2. Normal Case module
3. Attack Case module

1. **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 theuser.

Then the router node and destination node is created with the socket connection of using their properties. In this module is mainly used to creating the new destination with t network id for sending the data's from source to destination with the use of valid socket connection.

2. **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.

In our proposal use AODV routing protocol in all normal module attack module and IDS (intrusion detection system) for prevention through attack. In this module it simulate the results as a form of normal time receiving the data's from the server by using TCP and UDP protocols.

3. **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 neighbor node whose belongs to in radio range, if any node as week node with nearbyor 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.

A DDoS attack is a form of DoS attack but difference is that DoS attack is performed by only one node and DDoS is performed by the combination of many nodes. All nodes simultaneously attack on the victim node or network by sending them huge packets, this will

totally consume the victim bandwidth and this will not allow victim to receive the important data from the network.

4. CONCLUSION

The proposed mechanism eliminates the need for a centralized trusted authority which is not practical in ADHOC network due to their self-organizing nature. The results demonstrate thatthe 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 neighbors.

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. I 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.

In this project “ENHANCED FIREWALL USING DDOS ATTACK” was developed successfully with the use of IDS method. This method gave the good solution for prevent the attackers from various networks. It neutralized damaged data’s in efficient manner. This project will useful for all companies for protecting the data’s.

REFERENCES

[1] H. Yetgin, K. T. K. Cheung, M. El-Hajjar, and L. H. Hanzo, ``A survey of network lifetime maximization techniques in wireless sensor networks,"IEEE Commun. Surveys Tutr., vol. 19, no. 2, pp. 828_854, 2nd Quart., 2017.

[2] A. B. Noel, A. Abdaoui, T. Elfouly, M. H. Ahmed, A. Badawy, and M. S. Shehata, ``Structural health monitoring using wireless sensor networks: A comprehensive survey," IEEE Commun. Surveys Tutr., vol. 19, no. 3, pp. 1403_1423, 3rd Quart., 2017.

[3] J. Zhang, J. Tang, T. B. Wang, and F. Chen, ``Energy-efficient data gathering rendezvous algorithms with mobile sinks for wireless sensor networks," Int. J. Sensor Netw., vol. 23, no. 4, pp. 248_257, Apr. 2017.

[4] Q. Jiang, S. Zeadally, J. Ma, and D. He, ``Lightweight three-factor authentication and key agreement protocol for Internet-integrated wireless sensor networks," IEEE Access, vol. 5, pp. 3376_3392, 2017.

[5] M. H. Anisi, G. Abdul-Salaam, M. Y. I. Idris, A. W. A. Wahab, and I. Ahmedy, ``Energy harvesting and battery power based routing in wireless sensor networks," Wireless Netw., vol. 23, no. 1, pp. 249_266, Jan. 2017.

[6] J. Wang, J. Cao, S. Ji, and J. H. Park, ``Energy-efficient cluster based dynamic routes adjustment approach for wireless sensor networks with mobile sinks," J. Supercomput., vol. 73, no. 7, pp. 3277_3290, Jul. 2017.

[7] K. Dantu, M. Rahimi, H. Shah, S. Babel, A. Dhariwal, and G. S. Sukhatme, ``Robomote: Enabling mobility in sensor networks," in Proc. 4th Int. Symp. Inf. Process. Sensor Netw., Apr. 2005, pp. 404_409.

[8] I. Din, B.-S. Kim, S. Hassan, M. Guizani, M. Atiquzzaman, and J. Rodrigues, ``Information- centric network-based vehicular communications: Overview and research opportunities," Sensors, vol. 18, no. 11,p. 3957, 2018.

[9] Y. Yang, M. I. Fonoage, and M. Cardei, ``Improving network lifetime with mobile wireless sensor networks," Comput. Commun., vol. 33, no. 4,pp. 409_419, 2010.

[10] H. A. Khattak, H. Farman, B. Jan, and I. U. Din, ``Toward integrating vehicular clouds with IoT for smart city services," IEEE Netw., vol. 33,no. 2, pp. 65_71, Mar./Apr. 2019.

[11] I. U. Din, H. Asmat, and M. Guizani, ``A review of information centric network-based Internet of things: Communication architectures, design issues, and research opportunities," Multimedia Tools Appl., vol. 78, no. 21, pp. 30241_30256, 2019.