International Journal of Scientific Research in Computer Science and Engineering **Research Paper**
Vol.7, Issue.6, pp.43-45, December (2019) **E-ISSN:** 2320-7639

Securing MWSNs using Game Theory and Multiple Evidence Approach

Bindushree V.

Department of Computer Science and Engineering, BGSIT, ACU, Mandya, India

Author: bindushree11v@gmail.com, Tel.: 9964981481

Available online at: www.isroset.org

Received: 18/Nov/2019, Accepted: 12/Dec/2019, Online: 31/Dec/2019

***Abstract*—** Mobile wireless sensor network can be distinct as a wireless sensor association in which the nodes are mobile. There are many applications which make use of wireless sensor network so protection of nodes in the network is very important. These nodes are limited in terms of their processing units and power. Each sensor node is vulnerable to malicious attacks, so ensuring proper network operation is essential to protect these nodes from the attacks. In MWSNs, denial of service attack is more damaging the network by sending unnecessary packets to the victim node to drain resources offered to the fatality node. Denial of service attack is exceedingly complicated to detect using traditional invasion recognition systems. The proposed method, adopts a combination of game theory and multiple evidence combination. Game theoretic approach is a diversion between the nodes, attacker and intrusion detection system. The game will be performed at any moment a target node encounters a packet at the same time as a DDoS assail after an unambiguous sill in mobile wireless sensor network. Multiple evidence combination finds out internal attacks, by collecting evidences from the neighbour nodes and detects misbehaving nodes and isolates it. In order to estimate the concert of anticipated form, the optimized link state routing protocol was replicated in NS-2 simulator. The proposed model attack's detection yields greater packet delivery ratio and reduced average end to end delay and packet loss.

***Keywords*—** Denial of Service Attack, Network Simulator, malicious, Mobile wireless sensor network, Game theoretic

I. INTRODUCTION

Mobile wireless sensor network (MWSN) is a compilation of movable nodes organized in to a cooperative network. It provides diverse applications such as martial use, disaster response, scrutiny and systematic investigation of destructive environments. There are many applications which make use of wireless antenna system, so protection of nodes in the set of connections is very important. Wireless sensor arrangement consists of a collection of minute devices called feeler nodes. Each node composed of processing capability, memory, transceiver, power source. Sensor nodes are distributed across an area and communicate among themselves. These are restricted in provisions of their power and dispensation units.

Apart from these nodes, sensor network also contain sink nodes which is responsible for processing and storing the information collected by the network. Wireless sensor network generally follows rooted topology, which is an arrangement of nodes, links in the network. It also has computing devices called base station. Sink node sends the processed data collected from the network in the direction of the pedestal location. Support position has more authority and longer life time when compared to a sensor node. Operations performed by base station are initialization of network, dissemination of information, activation of node and revocation of tasks. It also helps in interfacing with other sensor networks. Each sensor node is vulnerable to wicked storming that may be launched by means of the opponent group commencing also inside or exterior the system. Employment of these nodes over superior locale makes them even supplementary susceptible to many incursion. So ensuring proper and uninterrupted network operation is indispensable to look after these nodes from ambush. In radio signal transducer complex Distributed Denial of Service (DDoS) violation is more damaging which tries to fatigue assets presented to the victim node via conveyance superfluous avoidable packets. Proposed method detects flooding attack and internal routing attacks.

To deal with DDoS attack and routing attacks in mobile wireless sensor network, cooperative game theory and multiple evidence combination methods are used. The game theoretic approach for wireless sensor networks security helps in preventing Distributed Denial of Service (DDoS) bombards, intermission exposure, and amplification protection along with to exist together with transducer connection point. Routing table records all node movements which is beneficial for finding future points of attack in advance.

II. RELATED WORK

Repeating the game infinite number of times gives more accuracy because all the attack patterns are stored in the base station. Node is assigned with a rank by monitoring process. This process collects information about each node to calculate reputation. But this is not realistic. If there is more number of malicious nodes then the system performance disgraces. This is suitable reality so as to apiece player tries to capitalize on its profit that is IDS improves its profitability by bringing down the tempo of counterfeit positives and negatives revealing, finally fails to detect more spiteful nodes. Advantage of this approach is finding selfish nodes and disadvantage is isolation leads to separation in the network [1].

Performing sampling in real time environment is very expensive, bound on the sampling rate is to be set. Vault indicates utmost rate at which nodes in the network for intruder exposure can course packets in factual time. This is called as two-player and zero-sum competition, where intruder's and service provider's payoff are sum up to zero.

Packets are transmitted by selecting path from source to destination, attacker may choose any path to transmit its malicious packets but at most on any links it will be detected due to min-max solution. But this method requires sampling of each and every packet which is time consuming. If service provider could sample every packet, attackers always fail to Inject attack packets to reach target node and service provider always win against attacker. In the real world there would not be enough resources to sample all packets [2].

DDoS detection in casualty router is moderately effortless for the reason that elevated pace of resources conservation. To secure legitimate user resources, this method is most practically applicable, but the disadvantage of this approach is that, during denial of service attacks, legitimate user resources such as bandwidth, often gets overwhelmed and also it takes defence action only after attacker reaching the target but it is waste as the legitimate users are already denied [3].

III. METHODOLOGY

The game based detection and resistance mechanism is used to notice DDoS attacks, it consists of number of decision makers called players, players are users controlling their devices. Here nodes, IDS and attacker are considered as players. Node and IDS chooses good strategy to detect an attack. IDPS can be able to regulate its wisdom parameters to make out outlook attacks. When a node performs useful action, it will get positive reward. Based on the reward value acquired by the node IDS decides which nodes are under attack.

IV. RESULTS AND DISCUSSION

1. Packet Delivery Ratio:
PDR is the quantity of packets sent starting the source node to the amount of packets acknowledged at end node. The OLSR protocol performed principally fine, delivering more than 98% of the records packets even when there is node mobility when compared to existing method.

Table 1: Packet delivery ratio of proposed method

Number of nodes	Packet delivery ratio
10	97.76
20	97.94
30	98.15

Standard instance waits for information packets from the starting place to the end node. The average interruption of packet delivery was less. It additionally includes delay caused by itinerary detection method as a result the queue in data packet diffusion. Solely information packets which are effectively delivered to destination were counted. Since Number of nodes Packet delivery ratio

2. Average end to end delay
Securing MWSNs using game theory and multiple evidence approach two hop routes are stored by MPR selector, it will provide to corresponding node whenever it needs to send packets. So resulted in less delay, hence performance of the protocol was high.

Table 2: Average end to end delay of proposed method

Number of nodes	Average end to end delay
10	1.0137
20	1.0130
30	1.0168

V. CONCLUSION AND FUTURE SCOPE

The proposed system ensures efficient end-to-end delivery of messages and it is working as anticipated, successfully minimize packet failure inside the system. In this thesis, the communication relating the nodes, attackers and intrusion detection system was premeditated by means of cooperative game theoretic approach. An incoming attack was detected by this method that may cause flooding packets in mobile wireless sensor network. Multiple evidence combination method is used to detect internal attacks in the network, and also adds confidence value and establishes reputation in tracking an attack.

REFERENCES

[1]. A. Agah and S. K. Das, “Preventing DoS attacks in wireless sensor networks: A repeated game theory approach,” *International Journal of Network Security*, vol.5, pp. 145–153, **Sept. 2007.**

[2]. M. Kodialam and T. V. Lakshman, “Detecting network intrusions via sampling: A game theoretic approach,” *Proc. Annual Joint Conference of the IEEE Computer and Communications* (INFOCOM 2003), vol. **3**, pp. 1880-1889, **2003.**

[3]. Thomas, R., Mark, B., Johnson, T., and Croall, J. NetBouncer: Clientlegitimacy- based highperformance DDoS filtering. *Proceedings of the 3rd DARPA Information Survivability Conference and Exposition*, Washington, DC, 22-24 April, pp. 111–113. IEEE CS, USA, **2003.**

Authors Profile

Mrs. Bindushree V pursed Bachelor of Science from MIT, Mysore in 2012 and Master of Science from MIT in year 2015. I’m a member of IAENG Publications, I have published 3 research papers.

.