Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 715 – 721

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

DoS attack prevention technique in Wireless Sensor Networks

Shital Patil[a], Sangita Chaudhari[b,*]

[a]*A. C.Patil College of Engineering, Mumbai University, Kharghar, Navi Mumbai, 410210, India*
[b]*A. C.Patil College of Engineering, Mumbai University, Kharghar, Navi Mumbai, 410210, India*

Abstract

Wireless Sensor Networks (WSN) has wide applications in data gathering and data transmission via wireless networks. Due to the weaknesses in the WSN, the sensor nodes are vulnerable to most of the security threats. Denial-of-Service (DoS) attack is most popular attack on these sensor nodes. Some attack prevention techniques must be used against DoS attacks. There are different techniques to prevent DoS attack in wireless sensor network. In this paper, an immune system is proposed for the DoS attack on WSN which will improve the accuracy rate of attack prevention, reduce the false alarm rate and able to recognize different Dos attack.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Dos attack, attack prevention, prevention in WSN;

1. Introduction

The WSN are flexible, easy to implement and straight forward. They are growing because of low cost and effective. It has wide applications in military, health care to gather data and data transmission. Due to security issues and limited resource energy, they are vulnerable to security attack. So there is a need to provide effective security mechanisms. The DoS attack is considered as one of the major attack on WSN. The main aim of DoS is the disruption of services by attempting to limit the access to a machine or service instead of subverting the service itself. This kind of attack aims at rendering a network incapable of providing normal service by targeting either the network's bandwidth or its connectivity. These attacks achieve their goal by sending at a victim a stream of packets that swamps his network or processing capacity denying access to his regular clients[1]. Most of the attack prevention

* Corresponding author. Tel.: +91-932-420-4088;
E-mail address: sschaudhari@acpce.ac.in

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.094

techniques are based on soft computing, game theory, artificial intelligence and multi-agent approaches. Soft computing based approaches uses the fuzzy Q-learning algorithm, Decision tree. In game theory, a strategy is de fined for all possible situations and Nash equilibrium is the solution. Artificial intelligence uses the danger theory, dendritic cells. In multi-agent immune system, each agent has defined duties and goals[2].

The game theory framework based on Utility based Dynamic Source Routing (UDSR) is used as secure routing protocol which is derived from Dynamic Source Routing (DSR) and Watch-list is used to identify malicious node. Utility value is used to choose secure route. Cooperation and reputation are used to calculate node misbehavior. UDSR loses fewer fractions of packets due to malicious nodes, whereas regular DSR faces loss of more packets. UDSR is facing less loss comparing to DSR because DSR doesn't react to the bad behavior of nodes but UDSR and Watch-list isolate the node by labeling that node as malicious node. So that node in the network can be ignored and it won't be able to harm the network. The major problems are how to avoid the false labeling and how to set threshold values[3].

Auction theory is used to detect non-cooperative nodes. This approach uses UDSR protocol. Instead of utility value bid price is used to choose secure route. This protocol is named as Secure Auction-based Routing (SAR). To recognize malicious node timeout timer is used by destination. If the timer expires and before reaching packet to the destination, then bad route message to base station and all nodes will be placed into watch-list. If nodes comes more than a predefined number of times then base station will put that node into ignore list and it will broadcast that list. In SAR the average number of dropped packets stays steady, because nodes with bad reputation will be ignored by the majority. SAR loses fewer fractions of packets due to malicious nodes because it reacts to the bad behavior. It has same problems as UDSR, false labeling and threshold values[4].

The repeated game theory approach is based on game theory which recognizes the presence of nodes that agree to forward packets but fail to do so. It categorizes different nodes based upon their dynamically measured behavior. This framework enforces cooperation among nodes and provides punishment for non-cooperative behavior. Sensor nodes trust each other based on the reputation. To increase the reputation in the network, each node will participate fairly in packet transfer. Otherwise IDS will recognize the malicious nodes and isolates them from participating in network functions which will have less reputation. The benefit of this framework is that, the base station has a history of the previous games and when a node is malicious it gets a negative reputation when the total reputation accumulates, a path consisting of less number malicious nodes is chosen to be the winning path. This results in isolation of malicious nodes. To lower the rate of false positives and false negatives detection, it misses more malicious nodes[5].

A LEACH protocol is secured by using a Bayesian game which is called as S-LEACH. S-LEACH has different rounds, each starts with setup phase, and continues with a steady state phase. In setup phase cluster heads (CHs) are selected. For second phase, the cluster heads assign the time on which the sensor nodes belong to their cluster, can send data to them, based on a TDMA (Time Division Multiple Access) approach. The local intrusion detection system (IDS) would notify central IDS about malicious nodes. Then central IDS informs about malicious nodes to whole network. So local IDSs would be alerted to not assign any time for selfish nodes, and prevent wastage of system resources. The number of packets dropped is less than non-secured network. Throughput is high because CHs can check their member nodes more in their all located transmission times and recognize the type of them[6].

The AODV-HFDP (Ad-hoc On demand Distance Routing with Hello flood Detection cum Prevention) routing protocol is used to detect node that generates hello flood attack. Hello flood attack is an attack on the network layer. A hello message is used to indicate presence of node. On receiving a hello message, each node updates its neighbor table, to indicate route towards the base station node. To distinguish between a friend and a stranger a technique based on simple test packet is applied. The Hello message receiving node sends simple test packet to hello sending node, if the reply comes in allotted time threshold then hello sending node is considered as a friend, if not then it is classified as a stranger. After declaring the node as malicious, the information of hello sending node is deleted from the routing table and this information is broadcast throughout the network. All nodes in the network delete malicious node information from routing table. As compared to AODV, AODV-HFDP gives higher packet delivery ratio. But it works for homogeneous sensors, fixed signal strength[7].

An ant-based framework exploits the significance of stateless and stateful signatures and hence preserving the legitimate packets only, thereby discarding the contaminated packets. The Ant-Based Routing Algorithm is used. The attack is detected by DDA (DDOS Detecting Ants), if reliability changes or buffer size exceeds the threshold