Detecting Wormhole Attack on Data Aggregation in Hierarchical WSN

Mukesh Kumar, National Institute of Technology, Hamirpur, India
Kamlesh Dutta, National Institute of Technology, Hamirpur, India

ABSTRACT

Wireless networks are used by everyone for their convenience for transferring packets from one node to another without having a static infrastructure. In WSN, there are some nodes which are light weight, small in size, having low computation overhead, and low cost known as sensor nodes. In literature, there exists many secure data aggregation protocols available but they are not sufficient to detect the malicious node. The authors require a better security mechanism or a technique to secure the network. Data aggregation is an essential paradigm in WSN. The idea is to combine data coming from different source nodes in order to achieve energy efficiency. In this paper, the authors proposed a protocol for worm hole attack detection during data aggregation in WSN. Main focus is on wormhole attack detection and its countermeasures.

KEYWORDS
Data Aggregation, Location ID, Nodes, Sensor, Wormhole Attack

1. INTRODUCTION

Wireless Sensor Networks (WSNs) generally consists of highly distributed network of small-size, lightweight wireless nodes. Wireless sensor network provides a bridge between the real physical and virtual world. Sensor network refers to as the heterogeneous system which is primarily design for real-time collection. The sensors all together provide global views of the environments that offer more information than those local views provided by independently operating sensors. There are numerous potential applications of WSNs in various areas such as residence, industry, military, transportation, civil infrastructure, communication, security and many others (Feng, Leonidas, 2004). Elements of WSN are the base stations and the sensor nodes. Base station acts as a gateway between the wireless network and the external world. There are one or more several base stations in a network which receive report from the sensor nodes, when they detect any misbehavior occurred in that network by any sensor node. Then it shows there is an adversary node which destroys the packets. Sensor nodes are used to monitor the physical or environmental attributes like temperature, humidity, pressure, sound, etc. (Sharma et al, 2012)

Among the designs of WSNs, security is one of the most important aspects that deserve great attention, considering the tremendous application opportunities (Padmavathi, & Shanmugapriya, 2009). In wireless networks, there is much more threat of attacks than in wired networks. The main characteristics of a WSN includes power consumption constraints, ability to cope with node failures, scalability of network, ability to withstand in harsh or disastrous environmental conditions, communication failures, etc. Security in sensor networks is complicated by the constrained capabilities of sensor node hardware and the properties of the deployment (Murugaboopathi et al., 2013).
Data aggregation is basically a process in which we aggregate or combine the data and pass it to the aggregator node which is close to the sink node or base station in the network. In WSN, each node forwards data to its neighbouring node which is nearer to the sink (Patil Nandini, & Patil, 2010). This scheme is not energy efficient. Therefore, we need a data aggregation approach. There are many approaches used in data aggregation. These are grid or centralized approach, cluster based approach, tree based approach, in-network based approach. Efficient data aggregation does not only provide energy constraint but also remove data redundancy and hence provide useful data only in the network (Rajagopalan et al., 2008)

There are two network in wireless sensor network i.e., flat and hierarchical network. In flat WSN, each sensor nodes have the same level to transmit the data. It uses the multi-hop path. The overhead is more but we get an optimal data. In hierarchical WSN, we consider a tree based topology in which root node act as a sink which takes all the aggregated data from the below level nodes and then transfer the data to above level of the tree. We need hierarchical WSN to get the energy efficiency and scalability. It involves data fusion at intermediate nodes; it reduces transmitted packets in the network. Results are propagated level by level in a tree. As we know, tree techniques or approach are not efficient in the network. If there is any failure of nodes, then the entire setup is failed. Therefore, we combine both tree and cluster approach to get a new approach. It provides simple routing but not necessarily optimal routing. We focus on data aggregation in energy constraint sensor network. The main goal of data aggregation is to collect and aggregate all the data in an energy efficient manner so that the lifetime of the network is enhanced (Krishnamachari et al., 2002). The overall cost of the WSN should be as low as possible. The goal of security is to provide security services to defend against all the kinds of threats.

In this paper, we propose an algorithm which detects the wormhole attack by using scenarios. There are two algorithms, secure data transmission (SDT) and neighbour table (NT). In SDT, we use two scenarios and find which one is legal or adversary node and then forward the data to the aggregator node. We create an aggregator node by getting the minimum distance from all nodes. Then make an aggregator node which aggregates and send the data to the base station in a secure way.

2. RELATED WORK

In this section, we show the previous work to introduce wormhole attack and its countermeasures. As we know security is the main concern in the WSN. All the techniques/schemes which are used in WSN to detect or defend wormhole attack which is not sufficient and some of them are costly or time consuming. In wormhole attack, the adversary or the attacker carry packets, route, routing information, ACK, etc. through a link from the legitimate node by making a tunnel between one adversary to other adversary and send packet to the legitimate node with a high speed then the original path or replays them in a different part (Karlof, & Wagner, 2003). An attacker disrupts or intrudes forwarding messages that originated by senders, copies a portion or a whole packet and sending the copied packet through the tunnel with a low latency so that it reaches before the original packet which traverses through the original route.

An attacker mostly situated near the base station, so it may easily interrupt the routing by creating a well-placed wormhole (Chaudhari, & Kadam, 2011). Attacker convinces the legitimate nodes those have multiple hop from a base station, which are close to the wormhole. Sometimes it only copies the data of the packet and used as an eaves dropping attack. It can be used in the combination with the selective forwarding or eavesdropping. Detection of wormhole attack is difficult when it conducted with a sybil attack. Wormhole attacks are difficult to detect as they use a private out-of-band channel invisible to the underlying sensor network (Karlof, & Wagner, 2003) by broadcasting in the network. Detecting wormhole attacks requires tight time synchronization among the nodes, which is infeasible in practical environment (Chaudhari, & Kadam, 2011).
Flood Risk Awareness: An Experiment Using School Students to Inform Families and Friends
[www.igi-global.com/article/flood-risk-awareness/65731?camid=4v1a](www.igi-global.com/article/flood-risk-awareness/65731?camid=4v1a)

Toward What End?: Three Classical Theories
[www.igi-global.com/chapter/toward-end-three-classical-theories/46339?camid=4v1a](www.igi-global.com/chapter/toward-end-three-classical-theories/46339?camid=4v1a)