Improved Cross-Layer Detection and Prevention of Sinkhole Attack in WSN

Ambika N.
https://orcid.org/0000-0003-4452-5514
Department of Computer Application, SSMRV College, Bangalore, India

INTRODUCTION

Wireless sensor network (Chen, Makki, Yen, & Pissinou, 2009) (I.Akyildiz, Su, & Sankarasubramaniam, 2002) is an assembly of tiny devices which self-configure and communicate in the unsupervised environment. These devices are used in many applications (Xu, 2002). Military surveillance (Lee, Lee, Song, & Lee, 2009), agriculture monitoring (Baggio, 2005), habitat monitoring (Polastre, Szewczyk, Mainwaring, Culler, & Anderson, 2004), smart homes (N.K.Suryadevara & Mukhopadhyay, 2012), hospital surveillance (López, Custodio, & Moreno, 2010) are some of the applications where these devices play a major role in accumulating data without human intervention.

Transmitting confidential information is one of the responsibilities of these devices. While doing so, these devices are liable to get compromised due to their limitations. As these devices are not monitored, the illegitimate nodes and their activities will remain undiscovered. Hence to bring the guilty into light better security measures have to be accommodated. The methodology adopted has to minimize the occurrence of the same by alerting the legitimate nodes of their activity.

Sinkhole attack (Ngai, Liu, & Lyu, 2006) (Rehman, Rehman, & Raheem, 2019) is one such attack where the compromised nodes advertise themselves. They broadcast false hop count to the normal nodes in their vicinity. The attack is launched by the illegitimate node advertising itself as the most favourable path to the base station. Their activity not only attracts the traffic towards itself but also utilizes the network resources. The guilty node after obtaining the trust of its surrounding nodes attracts all the traffic and is liable to launch different kinds of attacks. In the proposed work the solution is provided to minimize sinkhole attack in the network. The proposed work is improving cross-layer design suggested in (S & S, 2017), where Media Access control layer (MAC) and network layer is provided with algorithms to perform. The proposed work is divided into five sections. A detailed literature survey is provided in section 2. The proposed work is explained with detail analysis in section 3. Future research directions are suggested in section 4. The work is concluded in section 5.

BACKGROUND

The proposed work provides solution to tackles and minimizes the occurrences of Sinkhole attack in the network. Many authors have provided their suggestions to tackle the same. This section provides a brief history of the same.

In (Ngai, Liu, & Lyu, 2006) network flow graph is utilized to detect sinkhole attack. The selective forwarding activity is considered to make the detection of the attack. The nodes are monitored to find the missing data from the region. A statistical methodology is adopted to accomplish the task. Using the

DOI: 10.4018/978-1-7998-3479-3.ch037

mean of the data sent and amount of data collected using sliding window a measure is calculated. This calculated value is compared against the threshold to measure the suspicious activity in the respective area. The base station gauges the suspected area. After detecting the affected area the base station forwards a request message to the area. The message contains the IDs of all the affected nodes and is made to move from hop to hop. A timestamp is included in the message to avoid replay of the messages. The respective nodes sign the message with its private key. After receiving the message from the nodes, the receiving reply with the base station with its message. The message contains details of IDs, ID of the next hop and estimated cost [hop-count, data rate]. The base station constructs the tree using the information from the received message. The area under sinkhole attack follows a pattern where all the packets move towards the invaded node. Using this methodology the adversary can be detected.

The authors in (Krontiris, Dimitriou, Giannetsos, & Marios, 2007) have constructed a routing tree to tackle sinkhole attack. The system follows distributed architecture. Identical IDS clients are embedded in the nodes deployed in the network. The IDS agent is responsible for network monitoring, intrusion detection and decision making. The client listens to the network traffic, captures the individual packets and examines the same. The packets in vicinity are scrutinized for legitimacy. A specification based approach is followed by the supervising nodes. A deviation from the normal user defined rules is considered in the detection procedure. The system has to provide appropriate rules to detect suspicious behaviour. Two rules are used in the proposed work. In both the rules the sender field is verified to know its identity. The node ID has to be one of the neighbours and not the examining node. A cooperative mutual conclusion approach is followed to conclude the behaviour of the guilty nodes. Each watchdog in the neighbouring list broadcast the alert message and arrives at the conclusion. On affirmation, the nodes involve themselves in regenerating the cryptographic materials and distributing the same among the trusted nodes. The base station is notified of the illegitimate node.

In (S & S, 2017) cross layer approach is adopted. The paper tackles sinkhole attack. LEACH protocol is used in the work. Two assumptions are considered in the work. It is assumed that cluster heads cannot be compromised. The nodes are availed flexibility to vary their transmitting power. Rectangular clustering approach is adopted. The network is divided into rectangular clusters of equal area. The average location of nodes is calculated using Dijkstra's algorithm. The MAC layer sends link information to the network layer. The information is evaluated considering re-transmissions. Using the estimations an optimal routing scheme is provided. Considering Packet-delivery ratio sinkhole attack is evaluated. The work considers only retransmission to locate sinkhole attack.

The authors have proposed a different way to detect sinkhole attack in (Krontiris, Giannetsos, & Dimitriou, 2008). Two scenarios are considered in the work. Mintroute protocol (Rassam, Zainal, Maarof, & Al-Shaboti., 2012) is considered where the routing tree is built considering the link quality estimates. Packet error rate is considered. Periodically an update packet is transmitted to check the packet loss based on the number of packets received by the neighbouring nodes. The data of the same is updated in all the nodes with the respective sender node Ids. The nodes under sinkhole attack persuade the other legitimate nodes to change their route and choose the adversary as its next hop. Once the message is received by the legitimate node, the same checks the received message. If the node is not the one of the legitimate node in its list, it rejects the offer. Second scenario considered in the work is Multihop Link Quality Indicator Protocol (MultiHopLQI) (Gupta, Sharma, Marot, & Becker, 2010). The nodes calculate the link quality based on its own hardware. A beacon message is broadcasted by the nodes. The receiver uses its hardware to calculate LQI. Link quality indicator provides the cost of the corresponding link. The payload is the summation of cost of all links that make the given path. The nodes in this environment check the advertised path cost of the node and makes a comparison with the path cost