International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 12 | Dec 2020 www.irjet.net p-ISSN: 2395-0072

Review on Detecting Malicious Packet Dropping in Wireless Sensor Networks

Namratha B S[1], Chinnaswamy C.N[2], Dr.T.H.Sreenivas[3]

[1-3]PG Student, CNE, Associate Professor, Professor Dept. of CS&E, "Vidyavardhaka college of Engineering", Mysore, India

---

***Abstract**: A wireless sensor network (WSN) becomes popular on all aspects due to the rapid growth in technology. It has equal frequency of risks towards the different types of attacks. It compromises a large number of sensor nodes along with a base station.*

Base station is also known as the gateway to other networks. Sinkhole is a type of attack in which approaches are used for security problems. It is a type of attack that degrades the performance of a network.

Malicious node is a node used for denial of service (DoS) to the other nodes. They actually spoof their identity and location. Packet dropping is a type of DoS attack that is used to drop packets and make the packets and destination disconnected for path quality.

Keywords: Wireless sensor networks, Sinkhole, Malicious node, Packet dropping, Route discovery.

Introduction: Wireless Sensor Networks (WSN) is formed by a number of small sensor nodes. These nodes are generally composed of four main components such as processor and memory (microprocessor), sender and receiver (transceiver), power supply and sensors with digital to analog converter. There are several applications ranging from different technologies. These are typically used out in open, uncontrolled environment. The data is generated from the source node and it is propagated to destination nodes. This process continues until all the nodes die. The destination nodes are also called sink nodes. The sink nodes aggregate data for presentation.

Wireless sensor networks have the resource simplicity constrained nodes that make them vulnerable extremely to many of the different types of attack.

Among these packet dropping and modifying packets are the most common ones.

i.e.: compromised nodes may drop or modify the data packets that they are supposed to forward. These are actually composed of large number of sensor nodes and a base station. This base station is a gateway to all other networks. It is a powerful data processing or storage centre or a separate access point for human interfaces.

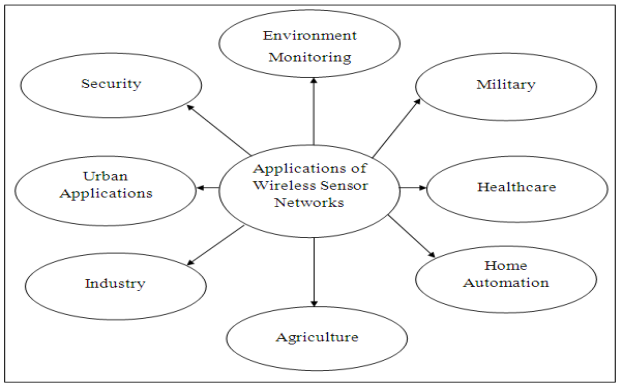

Fig 1:Applications of WSN

Sinkhole Attacks:

A sinkhole attacker node will first advertise the best possible route (with less hop-distance route) to reach the destination (BS) and to attract its neighbours so that they may fall into the category of attraction to utilize the advertised route more frequently. In a sinkhole attack an intruder compromises of a node or introduces a counterfeit node to travel inside the network and uses it to launch an attack. Based on the communication flow in the wireless networks the sinkhole attack does not need to target all the nodes in the network but only those close to the base station. The sinkhole attack allows a malicious node, called the sinkhole node, to advertise the best possible path to reach the base station (BS).

This misguides its neighbours to utilize that path more frequently. The sinkhole node gets the opportunity to tamper with the data, it also performs the modifications in messages or it drops messages or it produces unnecessary delay before forwarding them to the BS. There are basically three types of malicious nodes in a wireless sensor networks: sinkhole message modification node (SMD), sinkhole message dropping node (SDP), and sinkhole message delay node (SDL).

Sinkhole message modification nodes (SMD): Sinkhole attacker nodes will make sure about the modification of the messages before forwarding them to the next node.

Sinkhole message dropping nodes (SDP): Sinkhole attacker nodes will drop the messages, or even sometimes selectively.

Sinkhole message delay nodes (SDL): Sinkhole attacker nodes may cause delay to the messages that are being forwarded.

In the presence of the sinkhole attacker nodes, messages sent or received may be modified or delayed or dropped. A neighbour of the compromised node selects the forgotten route for data communications. The compromised node sends the fake route information with highest sequence number and the least hop count for the destination node when it receives the route request from the source node.

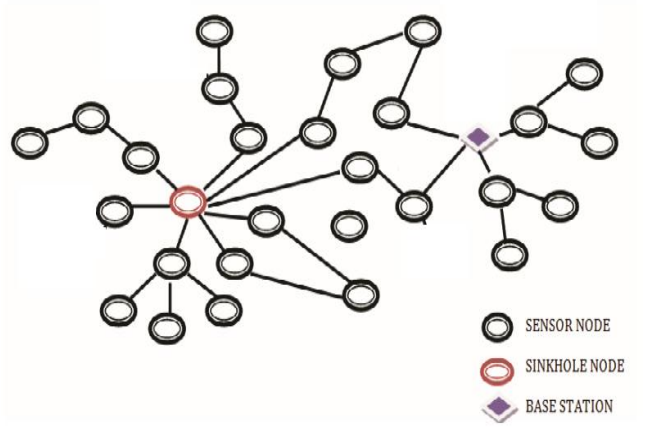

Fig 2: Sinkhole Attack

Related work:

WSN has many prone on the following packet dropping attacks: Sinkhole attack

Here, the compromised node will advertise itself to possess an excellent link to the base station that misleads the neighbouring nodes of the compromised node to choose and use the best route to reach the destination node 'n' number of times. In order to attract the network traffic surrounding to it they try to make it appear with a good possessing link to the base station.

At this time the compromised node will modify the routing packet to advertise fake routing information. Every neighbouring node of the sinkhole node will identify this node to forward the data packet to the base station. The compromised node will send the fake route information that has highest sequence number and with least hop count for the destination node at the time it will receive route request from the source node. Once all the route replies are received, the source node will agree the forged malicious route because of its minimum hop count when compared to the other available routes. On successful route selection, the victim node uses the forged route to send the data. During data distribution the compromised node drops the data packet based on some statistical predetermined probability distribution.

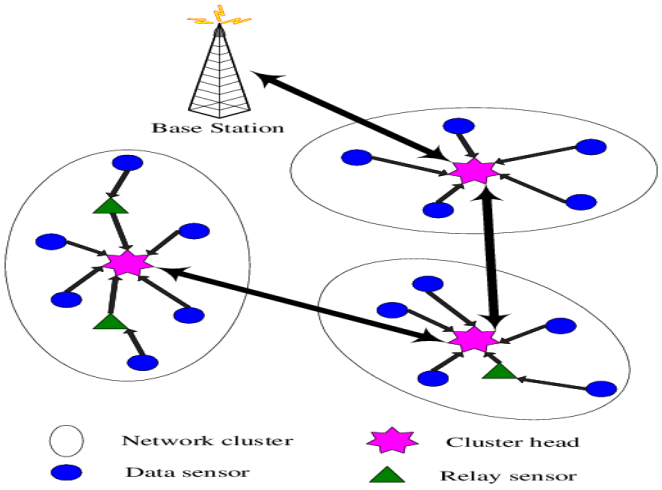

Fig 3:Infrastructure of WSN

The main objective of this attack is to attract the network traffic along with fake routing information and to have a proper distribution of network flow. To detect this packet dropping attack various technique are used. Anomaly based intruder detection system (IDS) is used to identify the packet dropping behavior of wireless networks. Here IDS gathers the information of the network from each node. Next with the help of this network information the packet dropping probability (PD) will be calculated. The obtained dropping probability (PD) is further compared with a predefined threshold value if not it will be declared as a compromised node(Lesser threshold value).The drop probability(PD) depends on the following parameters i.e. the probability of the control packet to be lost due to collision(PCLOST),the probability of the packet loss due to broken links (PPLOST) and the probability of data packet forwarded (PFORWARD).Here the disadvantage is that the initial computation cost for finding the drop probability (PD) for each node is high.[1]A specific table is used to store all the incoming route replies for all the requested routes .i.e. source ID, destination ID, destination sequence number(DSN) etc is used by the source node to store all the received routing details at that particular time.

The table will be calculated and updated until a route selection is done. Before a route is established the DSN will compare the route replies with the threshold value. If the destination sequence number of the route reply is greater than the threshold value then the route information is generated by sinkhole attack. Otherwise the source node will select a feasible route for data distribution. Limitation is that each and every node should run or travel across to identify the fake route. For this limitation [2] used a code sequence packet and packet response was used to detect the sinkhole attack. Here the technique used by the code sequence packet is that it contains the sender details with the sender sequence ID and the response sequence packet contains the receiver details with appropriate destination sequence ID. The route request takes place within the communication range i.e. when a particular node needs to send data packet

to the intended destination node.

The node is identified to be malicious if the receiver sequence ID is much larger than the sender sequence ID. Finally, IDS blocks the respective node by broadcasting a BLOCK message.

Krishnamurthy [3] proposed a modified dynamic source routing [DSR] approach for the recognition and elimination of the selective black hole attack. In modified DSR approach, the data packets are sent to the destination with the help of shortest path. It makes sure that the quantity of data packet to be sent in a block to the target by using different routes. The destination node will calculate the probability of the packet that is to be acknowledged. If the probability of the packet acknowledged at the destination is greater than the threshold value of the packet loss then the target node sends an ALARM packet to the neighbours of the IDS node. An ID detects the malicious node by checking the number of packets identified by all the nodes from the source node to two-hop distance (Shortest path).

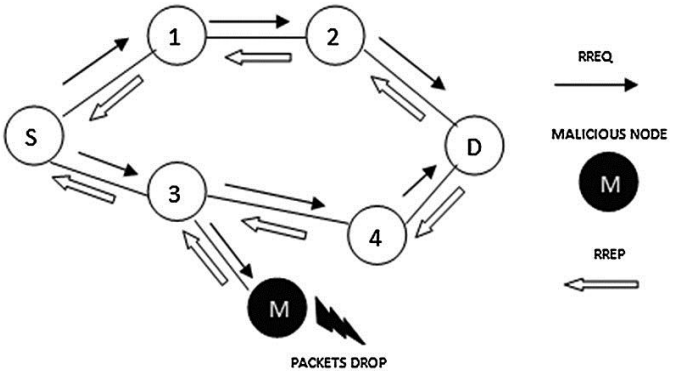

Fig 4: modified dynamic source routing [DSR] approach for the recognition and elimination of the selective black hole attack

Balakrishnan [4] proposed TWINEACK technique to detect malicious node in the network. Here, a network layer acknowledgement method is used to detect the malicious node. In this method while forwarding a packet a two hop acknowledgement is sent to other nodes to confirm the node cooperation. The major difference is that the TWINACK method does not use any authentication method to avoid tampering of data packets.

It suffers with message overhead due to TWINACK message for every data packet. In this method an authentication mechanism takes place to prevent tampering of data as it is acknowledged packet and it also takes care of message overhead to reduce with SINGLEACK.

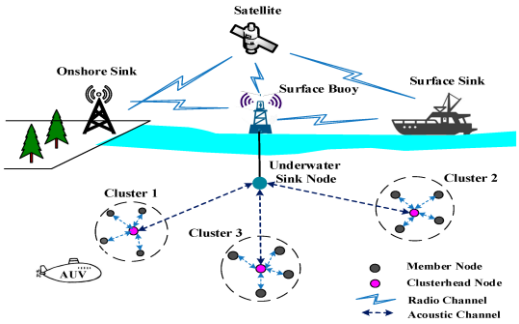

Fig 5: authentication method to avoid tampering of data packets

Haidari and Yoo [5] use another approach called PIGACK at the MAC layer to detect the misbehavior of the nodes in WSN. In this method each node has to maintain a table to store the malicious flag and reporter node details. Each node when sends a data packet it receives a PIGACK packet that must be saved in to the next node confirmation and sends back the confirmation for the next packet transformation. If in case a node fails to send PIGACK twice then it will be marked as a misbehaving node and then the interaction will be stopped with other nodes.

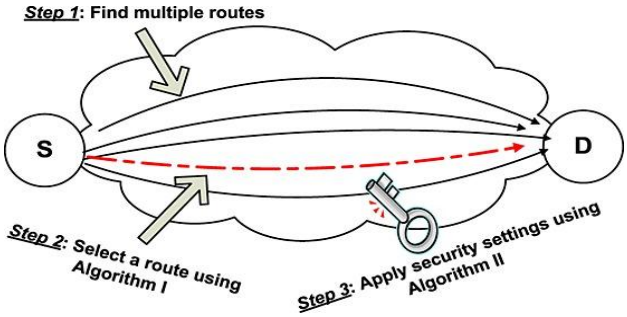

Fig 6: Flow control of WSN with security

Note: different techniques to detect malicious packet drop or the techniques for packet drop detection methods.

i) Network model and system Theory:

The network is designed with mainly sensor nodes and monitor nodes. The work of the sensor is to sense the data and forward it to the destination node and the sensor nodes are monitored under the region and it identifies the compromised nodes in the network. Here each sensor node has a unique identifier, random function (F) and a key (K).

ii) Single hops next door detection:

Each sensor node discovers one hop neighbors by broadcasting HELLO message. Reply confirmation is received from each and every node that accepts the HELLO message. Each node receives a single node and accepts the HELLO message from its neighbors. Based on this the neighbor list is constructed.

iii) Early path discovery:

In this process the source node will direct the data packets to the intended destination node or to the base station by selecting the shortest path. When the route reply is received from the neighbor the source node will select the shortest path for further data distribution.

iv) Data Circulation:

After a successful route discovery the source node directs the data packets to the destination node or to the respective base station for the selection of shortest path. Now the data that is being used for circulation can be detected by using one of the types of packet dropping attack known as the "Caution Notification Token" (CNT) approach.

v) Caution Notification Token:

In CNT method each monitor node will maintain a monitor table. This table contains two fields namely node ID and caution count (CC).Here the source node will select the shortest path and then directs the data packet to the destination through the chosen path. Once the data packet reaches the destination a ACK will be sent back for the best shortest path.

Otherwise, If ACK is not received from the destination node after sending the data packet from the selected shortest route then the source node will pop a warning message to the monitor node about the advertiser node.

When the monitor node receives the warning message it will update the caution count of the particular node in the monitor table.

This approach is explained in two ways:

i) Approach for sinkhole: Node J is a sinkhole node and it advertises that it offers a good quality link. This fake advertisement is received by node I, K, L, M, N and O. These are the neighbouring nodes of node J. Nodes I, K, L, M, N and O sends data packets to node J. If in case this node does not receive ACK from the base station then they will send warning message to the monitor node about the advertiser node J. Otherwise if ACK is received successfully then continuous data circulation will be done through node J. When the warning message is received, the monitor node will increase the counter count of node J.

ii) Approach for black hole: Suppose source node (I) broadcasts route request packet to establish a route to the destination node (Z). The black hole node (X) will send a route reply along with large sequence number and fewer hop count to the source node. When this fake route reply is received the source node (I) will select the best path for data circulation. The malicious node detection depends on the threshold value. The selection of threshold value plays a vital role in the malicious node detection.

vi) Reliable path realization against malicious node:

A compromised node list is sent to the entire sensor node in a particular region by the monitor node. The neighbour node list is then compared with the malicious node list. If the node contains malicious node as its neighbour then it will be removed from the neighbour node list. It again reconstructs its neighbour list by triggering neighbour discovery process.

vii) Cost Analysis:

Let's consider "N" to be the number of sensor nodes and "N_{avg}" be the average neighbours for the sensor nodes. Then, $N_{avg} < N$. i.e. the total time complexity proposed by Caution notification taken method is linear to the number of sensors in the wireless network.

Conclusion:

An unconventional way of acknowledgement based caution notification token is being proposed that makes use of network layer acknowledgement to identify the packet dropping attacks in wireless networks. In most of the present ACK based approaches the nodes suffers due to the computation overhead. i.e. every time the node should travel a complete path to identify the malicious node. But, in our proposed survey study by using CNT method the monitor node will collect the response from each and every node and then detect the malicious node. The CNT method is tested against two types of attacks namely sinkhole and black hole attacks. The end results of the survey for this technique shows the correctness and efficiency in malicious node detection.

References:

1. Kumar, V., & Kumar, R. (2015). An adaptive approach for detection of black hole attack in mobile ad hoc network. Procedia Computer Science, 48, 472-479.

2. Dhaka, A., Nandal, A., & Dhaka, R. S. (2015). Gray and black hole attack identification using control packets in MANETs. Procedia Computer Science, 54, 83-91.

3. Mohanapriya, M., & Krishnamurthy, I. (2014). Modified DSR protocol for detection and removal of selective black hole attack in MANET. Computers & Electrical Engineering, 40(2), 530-538.

4. Balakrishnan, K., Deng, J., & Varshney, V. K. (2005, March). TWOACK: preventing selfishness in mobile ad hoc networks. In IEEE Wireless Communications and Networking Conference, 2005 (Vol. 4, pp. 2137-2142). IEEE.

5. Heydari, V., & Yoo, S. M. (2015). Lightweight Acknowledgement-Based Method to Detect Misbehavior in MANETs. KSII Transactions on Internet & Information Systems, 9(12).