4.8 Block Hole Attack and its Countermeasures

- Black Hole attack occurs under Dos (Denial of service) attack in the network layer of OSI Model. In this kind of attacks the malicious node forgery other nodes by announcing a shortest false route to the destination then attracts additional traffic and drops continually the packets.

- During data transmission the source node sends a Route REQuest (RREQ) message to all the nodes including malicious node. Given that a malicious node may become active by receiving RREQ message and replies using Route REPly (RREP) message.

- It attracts additional traffic by falsely claiming the shortest route to the destination. This causes blocking and increasing the energy consumption in each node, leading to the formation of routing holes which disturb or stop the network functionality.

- The Fig. 4.3 illustrates the Black hole attack: while the source node A broadcasts an RREQ messages to discover the route for sending packets to destination node C. An RREQ broadcast from node A is received by neighbouring nodes B, D and the malicious node E. The RREP message sent by the malicious attacker node E is the first message reaching the source node. This last updates its routing table for the new route to the intended node destination, discarding any RREP message from other neighbouring nodes including the actual node destination and starts sending the buffered data packets immediately. In the same time the Black hole node drops all coming data packets rather than forwarding.

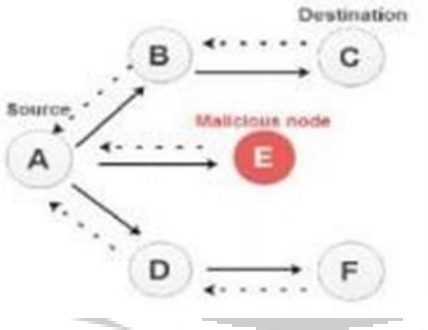

Figure 4.2 Black hole Attack schematic illustration using RREQ and RREP Packet

Source : Protocol and Architecture for Wireless Sensor Networks by Holger Karl , Andreas willig

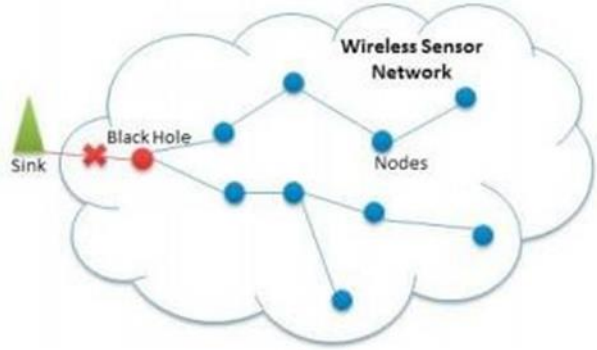

Figure 4.3 Black Hole Attaack
Source : Protocol and Architecture for Wireless Sensor Networks by Holger Karl , Andreas willig

Countermeasures

Routing Access Restriction

- Routing may be one of the most attractive attack targets in WSNs. If we can exclude attackers from participating in the routing process, i.e. restrict them from accessing routing, a large number of attacks in the network layer will be prevented or alleviated.
- Multi-path routing is one of the methods to reduce the effectiveness of attacks launched by attackers on routing paths. In these schemes, packets are routed through multiple paths. Even if the attacker on one of the paths breaks down the path, the routing is not necessarily broken as other paths still exist.
- This alleviates the impact of routing attacks, although does not prevent these attacks. A general way is to use authentication methods. With authentication, it can be easily determined whether a sensor can participate in routing or not.
- Authentication can be either end-to-end or hop-to-hop. In end-to-end authentication, the source and destination share some secret and can thus verify each other. When a node receives a routing update, it always verify the sender of the update before accepting the update.
- In hop-to-hop authentication, each message in transmission is authenticated hop by hop. Therefore, the trust between the source and the destination is built upon the trust on all the intermediate nodes in the path.
- Data are authenticated hop by hop between associated nodes until they reach the base station. Hop-to-hop authentication can be combined with multi-path routing. This paths can be physical, meaning that messages are routed through multiple physically different communication paths.

False Routing Information Detection

- Sometimes attackers do have chances to send false routing information into the network, e.g. during route discovery stages. If the false information does not lead to network failure such as broken routes, we really cannot do much about it. Otherwise, we can apply the idea of misbehaviour detection method.
- For example, watchdog or IDS (Intrusion Detection System) may find that some node fails to route messages along the routing path due to the wrong information it keeps. This anomaly of route failure may trigger out an alarm.
- Nodes can start to trace the source of false routing information. The Reputation can also be maintained, depending on whether nodes are providing valid routing information.

4.9 Flooding Attack and its Countermeasures

- Many protocols require nodes to broadcast HELLO packets to announce themselves to their neighbors, and a node receiving such a packet may assume that it is within (normal) radio range of the sender (Figure 4.4).
- This assumption may be false: a laptop-class attacker broadcasting routing or other information with large enough transmission power could convince every node in the network that the adversary is its neighbour.
- For example, an adversary advertising a very high-quality route to the base station to every node in the network could cause a large number of nodes to attempt to use this route, but those nodes sufficiently far away from the adversary would be sending packets into oblivion. The network is left in a state of confusion.

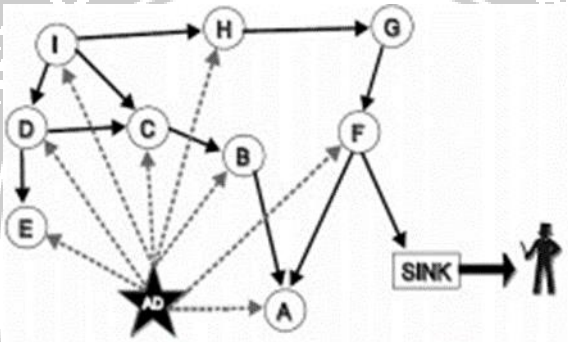

Figure 4.4 Flooding Attacks

Source : Protocol and Architecture for Wireless Sensor Networks by Holger Karl , Andreas willig

Countermeasures

Using Secret Keys Method

- In multi-path multi-base station data forwarding technique, each sensor node maintains number of different secrets (keys) in a multiple tree.
- Sensor node can forward its sensed data to multiple routes by using these secrets. There are multiple base stations in the network that have control over specific number of nodes and also, there are common means of communication among base stations.
- Each base station has all the secrets that are shared by all the sensor nodes, covered by it, according to the key assignment protocol.

Using Threshold Method

- A threshold based solution is used to defend against flooding attacks in WSN.
- The mobile nodes use a threshold value to check whether its neighbors are intruders or not.

- When the number of route request packets broadcasted by a node exceeds the predefined threshold value, it is treated as an intruder and the node stops providing its services to the intruder.