Selective Forwarding attack in wireless sensor networks

In this type of Selective Forwarding attack, malicious nodes reject the request to facilitate some information packets and ensure that they are not forwarded any further.

Attackers can selectively or randomly drop packets and try to increase the rate of packet loss in the network.

Two ways to attack Selective Forwarding

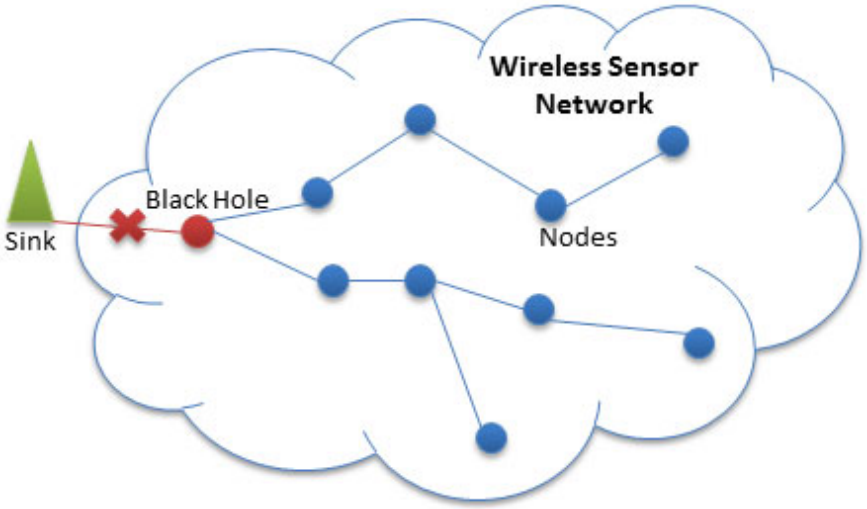
Two ways bad guys can attack a network are:

1. Attack from within

Authorized sensor node authentication can be compromised or bad guys can steal some keys or information from the nodes and attack the entire network. It is very difficult to detect such an attack.

1. Attack from the outside

This is done by jamming the routing between legitimate nodes.



Types of Selective Forwarding Attacks

There are several types of Selective Forwarding attacks:

The malicious node prohibits the flow of information from the authorized nodes to the base station, thus leading to a DoS denial of service attack, which can be turned into a Black Hole attack by attacking the entire network and term Process the flow of information from every node to the sink (the node is responsible for interacting with the sensor nodes).

Unauthorized nodes skip forwarding information and randomly drop them off. Instead, the unauthorized node sends their own packets of information to other nodes. One such attack is called Neglect and Greed.

Another form of attack is when unauthorized nodes delay the messages passing through them to falsify routing data between nodes.

- The last type is the Blind Letter attack. When a packet is forwarded from a legitimate node to a malicious one, it ensures to the legitimate node that the information is forwarded to the next node and eventually discard the packet without being detected. This scheme can attack various multistep routing protocols such as Geographic routing, TinyOS beaconing, etc.

Detect and prevent Selective Forwarding attacks

Detection and containment are classified according to an implementation plan or on the basis of a defense plan:

I. On the basis of the nature of the implementation plan, it is divided into two sub-parts: Centralized and distributed.

In centralized plans, the head or sink part of the sensor nodes is responsible for detecting and preventing this attack. In distributed plans, both the base station and the cluster head are responsible for preventing such an attack.

II. On the basis of a defense plan, they are divided into the following 2 parts: detection and prevention

The prevention plans are not able to detect the attack or the faulty nodes, instead, they ignore the faulty nodes and remove them from the network. Detect type is capable enough to detect an attack or a faulty node or even both.

How to resist a Selective Forwarding attack

There are different plans to combat such attacks:

A security plan that detects the attack and pushes the alarm level up, using multi-step validation from different sensor nodes in the network. In this plan, both the source node and the base station can detect the attack and make the right decision even if one of them is compromised.

This follows a distributed approach and can detect if any malicious node tries to drop the packet, instead of forwarding it to the next node. The accuracy of this method is claimed up to 95% in detecting Selective Forwarding attacks.

Intrusion detection system (IDS) can detect any loophole exploited by an attacker and warn the network about the malicious nodes involved. IDS system is designed based on detection capabilities based on specification.

This technique uses a Watchdog approach, in which the neighboring nodes can monitor the node's activity and see if it forwards the actual packet to other nodes. If it ignores the actual packet, the counter increases and generates an alarm when this value reaches a certain limit. If multiple watchdog nodes generate an alarm, the base station is notified and the compromised node is discarded.

A distributed containment plan that uses multi-step confirmation to counter Selective Forwarding attacks. In this scheme, it is assumed that all sensor nodes know their location and the number of faulty nodes, the energy level of the network is known or estimated.

All data paths are inferred by an indeterminate logic taking into account energy restriction and faulty nodes will be present. In cases where the multipath routing protocol cannot provide authentication information, the propagation restriction method will be used.

- Another plan uses hexagonal mesh topology. The routing algorithm is applied to find the best packet path. Nodes near the routing path check the communication of neighboring nodes, locate the attacker, and resend these ignored packets to where it is supposed to be reachable.

This method clearly shows the Selective Forwarding attack, which in turn warns neighboring nodes about the attacker's location and ignores the attacker's node in forwarding other messages. This method ensures authentic data is provided, while also consuming less energy and space.