51260 Muhammad Raza

A Hidden Routing Path Model for Reducing PDoS Attacks in Wireless Sensor Network

Abstract

Sensor networks have now become popular for monitoring of defense installations, traffic signals, and environmental changes such as monitoring of gases like CO2. Sensor networks face various problems and attacks. Problems faced include fading, signal attenuation, and path loss. Attacks include jamming style or Path based Denial of Service (PDoS) attacks. A PDoS attack causes an increase in MTTR of the sensor network and hence leads to energy and data losses. This research addresses PDoS attacks in sensor networks. I have proposed a novel architecture named HRPM (Hidden Routing Path Model) that reduces the effect of PDoS attacks, which in turn keeps the MTTR down and thus saves data and energy of the sensors. It not only stops the DoS attacks but also stops the attacker by identifying it through IDS (Intrusion Detection System) and counter-attacks the attacker through jamming style DoS attack to prevent it from making further attacks.

In this model, I assume that the network is centralized because the network is dedicated to single special purpose task and needs to store data and process it directly at a single place. The network is being used for a single special purpose. The nodes and server are homogeneous due to compatibility issues. All the nodes have full information about the task and resources present on the server. The server knows about the nodes and their location. Nodes and server both are interconnected with each other.

It is also assumed that the server and all the nodes support both WiFi and WiMax technology for which each keeps two transceivers: One for regular use employing WiFi technology (IEEE standard of 802.11b/g 2.400 GHz to 2.487 GHz) and another for the hidden route employing WiMax technology (IEEE standard 802.16 10 to 66 GHz range). The hidden route transceiver (WiMax) is kicked in to substitute the regular path when an attack is detected and is being repaired.

Suppose that a node wants to store data on the server but the storage media is unavailable due to Path based Denial of Service (PDoS) attack. When the server suspects that the node is sending garbage due to collisions from an attacker, it asks the node to switch its transmission from WiFi to WiMax and get on to the alternate path.

It is the responsibility of the hidden resource present on the server to manage and identify the attack, correct it and send positive acknowledgment if the path is repaired. In the mean time, the node communicates using the hidden transceiver and continues to performs its operations using the hidden route until the regular path is repaired and a positive acknowledgment is received by the node through the regular path (WiFi) of communication. Then, the node stops the communication through the hidden transceiver (WiMax) and resumes communication through the regular path (WiFi).

When the transmission of data is cut off on the regular route, (WiFi) then the server starts receiving packets coming from the attacker in their original form, as they are no longer garbled due to collisions. These packets have the MAC address of the intruder, which enables the server to identify the intruder with the help of IDS (Intrusion Detection System), and enables it to mount a counter-attack on the intruder through Jamming style DoS attack. The Jamming style DoS attack results in repairing of the path and the jamming of the intruder prevents it from repeating its attacks.

The simulation shows satisfactory results in decreasing the MTTR, energy and data losses. This research plays an important role in sensor network's area to improve the quality and the performance of the sensor nodes.