Availing security in a wireless sensor network requires more than user authentication with passwords or digital certificates and confidentiality in data transmission. The openness of wireless sensor network model makes it vulnerable and prone to sophisticated intrusion attacks like Denial of Service (DDOS) and side channel attacks. To handle large scale network access traffic and administrative control of data and application in wireless sensor network, a Multiple Sensing Intrusion Detection model has been proposed. Our proposed Multiple Sensing Intrusion Detection model handles large flow of data packets, analyze them and generate reports efficiently by finding the probability of network being attacked by an intruder. The intrusion distance, the minimum coverage of an area where the intruder can be sensed is found.
and multiple (sensing) detectors are situated there to detect the intruder once it enters or establishes its effect in the network.

References


Index Terms

Computer Science  Wireless Sensor Networks

Keywords
Wireless Sensor Networks  Multiple Sensing  Heterogeneous/homogeneous  Intrusion Detection System

Attacks

Packet Filtration

Packet Generation