Abstract

Wireless Sensor Networks (WSNs) are currently being used in a wide range of applications including military areas that demand high security requirements. WSNs are susceptible to various types of attacks as they are unsupervised in nature. Since sensor network is highly resource constrained, providing security to data transmission becomes a challenging issue. Attacks must be detected and eliminated from the network as early as possible to enhance the rate of successful transmissions. In this paper, an energy efficient algorithm is proposed to eliminate Black Hole and False Data Injection Attack (BHnFDIA) to overcome black hole attack in WSNs using a new acknowledgement based scheme with less overhead. Every intermediate node check the authenticity and integrity of the received packet. The authentic packets will be forwarded and malicious packets will be discarded immediately. The proposed
scheme can eliminate false data injection by outside malicious nodes and Black hole attack by compromised insider nodes. Simulation results show that the scheme can successfully identify and eliminate 100% black hole nodes. Malicious packets are immediately removed with 100% filtering efficiency. The scheme ensures more than 99% packet delivery with increased network traffic.

References


**Index Terms**

Computer Science Security

**Keywords**

ACK SINK (Sink Acknowledgement) Black hole attack False data injection Packet delivery rate

Security in WSN