Abstract

Wireless sensor network is a highly distributed network of small lightweight wireless sensor nodes, deployed in large numbers to monitor the environment or system. These sensor networks have limitations of system resources like battery power, radio range and processing capability. Low processing power and wireless connectivity make such networks vulnerable to various attacks like sink hole, black hole, Sybil attacks, selective forwarding, worm hole, hello flood etc. Among these hello flood attack is an important attack on the network layer, in which an adversary, which is not a legal node in the network, can flood hello request to any legitimate node using high transmission power and break the security of WSNs. The current solutions for this type of attack are mainly cryptographic, which suffer from heavy computational complexity. Hence these are less suitable in terms of memory and battery power. In this paper a method has been proposed to detect and prevent hello flood attack using signal strength of received Hello messages. Nodes have been classified as friend and stranger based on the signal strength of Hello messages sent by them. Nodes classified as stranger are further validated by sending a simple test packet; if the reply of test packet comes back in a predefined time then it is treated as valid otherwise it is treated as malicious. The algorithm is implemented in ns-2 by
modifying the AODV-routing protocol. The performance of algorithm has been tested under different network scenarios. The simulation results show improved performance of the new algorithm in terms of number of packet delivery ratio as compare to AODV with hello flood attack.

References

- A. Khetrapal, "Routing Techniques for Mobile Ad Hoc Networks Classification and Qualitative/Quantitative Analysis," Department of Computer Engineering, Delhi College of Engineering University AK-ACWN, 2006

**Index Terms**

Computer Science

Wireless

**Keywords**

WSN Keywords Hello Flood