Abstract

Wireless Sensor Networks (WSNs) operates with an open network topology without well-established infrastructure. Due to the absence of a centralized administration in network management, WSNs are highly vulnerable to various malicious attacks. The introductory of such a malicious node in a network may lead the network to security breaches, miscommunication, starvation and finally decay. In this paper, the authors attempt to reduce the vulnerability of a WSN node communicating with a malicious node by establishing a TRUST based authentication and filtering routing mechanism. The authors aim to detect and prevent potential attacks such as DoS attacks and Blackhole attacks, thus providing the associated security needed in order to build up relationships among each other to communicate.

The authors have used the existing AODV routing protocol and modified to perform a heuristic based TRUST metric calculation. In a situation of a suspected malicious node, the TRUST based security protocol detects and isolate the attacker as the communication channels proceed. The TRUST based AODV protocol has been implemented and evaluated with the
NS-2 simulator and simulation results are compared with the existing protocols.

References


Index Terms

Computer Science  Wireless

Keywords

WSN, AODV, TRUST, Security Protocol