Dynamic window secured implicit geographic forwarding for wireless sensor network.

ABSTRACT

Routing security is a major concerned in Wireless Sensor Network since a large scale of unattended nodes is deployed in ad hoc fashion with no possibility of a global addressing due to a limitation of node's memory and the node have to be self organizing when the systems require a connection with the other nodes. It becomes more challenging when the nodes have to act as the router and tightly constrained on energy and computational capabilities where any existing security mechanisms are not allowed to be fitted directly. These reasons thus increasing vulnerabilities to the network layer particularly and to the whole network, generally. In this paper, a Dynamic Window Secured Implicit Geographic Forwarding (DWSIGF) routing is presented where a dynamic time is used for collection window to collect Clear to Send (CTS) control packet in order to find an appropriate hoping node. The DWIGF is expected to minimize a chance to select an attacker as the hoping node that caused by a blackhole attack that happen because of the CTS rushing attack, which promise a good network performance with high packet delivery ratios.

Keyword: Sensor; Security; Routing; Attack; Random.