

The impact of window's size in DWSIGF routing protocol.

ABSTRACT

In this study, different collection window's size is been analyzed to investigate the impact on network performance: packet delivery ratio, message overhead and end to end delay on the Dynamic Window Secured Implicit Geographic Forwarding (DWIGF) routing protocol where this protocol is based on a dynamic collection window approached. Its method on using dynamic window's size has minimized the probability of selecting attackers and guaranteed high packet delivery ratios when there is a blackhole attack in the communication link. The DWSIGF is then compared with the best chosen window's size to analyze the network performance with and without attacker in the communication line, respectively. The DWIGF is able to minimize a Clear To Send (CTS) rushing attack that leads to a blackhole and selectively forwarding attack with a guaranteed of high packet delivery ratios where a selection of a failed trade and all attacker is minimized, respectively. As a result, this routing protocol is promising a dynamic and secured communication without inserting any existing security mechanism inside.

Keyword: Dynamic window; Secured routing; Sensor network; Routing attacks; Lazy binding; Geographic routing.