Impact of blackhole and Sybil attacks on dynamic windows secured implicit geographic forwarding routing protocol

ABSTRACT

Dynamic windows implicit geographic forwarding (DWSIGF) routing protocol promises a minimal selection on attacker as a hop node. However, it was tested only on blackhole attack with a single optimal attacker. Thus, a thorough investigation was performed to examine whether the protocol is secure against other routing attacks. This study presents a comprehensive analysis of an impact of blackhole and Sybil attacks on the DWSIGF. The analyses on blackhole attack were carried out on a single and multiple attackers using priority selection, random selection, an optimal relay, non-optimal relay, with and without clear to send (CTS) rushing attack. While on the other hand, the Sybil attack's analyses were investigated on the impact of single attacker using optimal and non-optimal relay over increasing traffic loads and growing number of Sybil attackers. The study showed that the DWSIGF promised a superior protection against blackhole/selective forwarding and Sybil attacks with minimum attacker selection and high performance in packet delivery ratio even without inserting any security mechanism in the routing protocol.