Implementation of Temporal Attacks in Vehicular Ad Hoc Networks

Abstract

Vehicular Ad Hoc Network (VANET) is vulnerable to temporal attacks in which a malicious node either impedes or delays the forwarding of critical safety messages received from neighboring nodes. It can also perform replay attack by sending the information of events occurred earlier. VANET applications are based on periodic exchange of safety packets. It is
very important that all the safety packets are sent on time so that proper action should be taken. It is the responsibility of each node in VANET to forward the received safety packet to its neighboring nodes. Attacker node exploits VANET vulnerabilities and performs these attacks. We discuss these attacks in brief and analyze their impact on VANET performance through NCTUuns-6.0 simulations. We also propose counter measures for these attacks.

Reference


Index Terms

Computer Science Information Technology
Key words

VANET
Packet Replay
Packet
Delay
Packet Suppression
attack
simulation