Abstract

Vehicular Ad-Hoc Network (VANET) is inherently insecure, primarily due to the broadcast nature of the wireless medium as well as the need for an infrastructureless architecture. This can be an opportunity for malicious nodes to attack against the routing protocol. The attacks can not only disrupt the normal routing process but also adversely affect the protocol network performance or even disable it. So, security solutions are needed in the development of a routing protocol, to protect the communication between the nodes which build the VANET network from malicious nodes attacks.

Reactive routing protocol SAODV, are used to address vulnerability from attacks on VANET. Integrity and authentication are security goals are implemented in the SAODV routing protocol. By using a model of asymmetric key cryptography, SAODV do security by using hash and digital signature mechanisms. This routing protocol will be simulated in VANET network and with or without RREQ disruption and blackhole attacks. These conditions will be included in the scenario with the change in the number of nodes as much as 10, 16 and 20, as well as change the nodes speed of 15m/s, 20m/s and 25m/s, which simulated by network simulator 2 (NS2). That would seem the obvious impact of the attacks from malicious nodes on the performance of routing protocol SAODV.

Performance evualuation of routing protocol SAODV is in terms of parameters : packet delivery ratio, packet loss ratio, convergence time, routing overhead dan normalized routing load. Packet delivery ratio and packet loss ratio indicates the impact of attacks against packet delivery from the source node to the destination node. Meanwhile, convergence time, routing overhead and normalized routing load indicates performance of SAODV routing protocol which uses reasonable amount of routing packets in the communication process, though SAODV uses security mechanisms.

Keywords: *VANET, reactive routing protocol, SAODV, integrity, authentication, packet delivery ratio, packet loss ratio, convergence time, routing overhead, normalized routing load, and NS2.*