ABSTRACT

Vehicular Ad-Hoc Networks (VANET) is a network technology in which the vehicle is used as a mobile noded to form a communications network. Communicate between vehicles use a routing protocol to finding the shortest routes for sending data packets to the destination. In the process of communication, routing protocols that are used will be very vulnerable to an attack that can interrupt search process routes or even disable the performance as a whole. Routing protocols SAODV and ARAN used to address vulnerability to attacks on VANET. To secure against communications and route search process is implemented in the routing protocols SAODV and ARAN. This research aims to analyze the influence of blackhole attacks against performance routing protocols SAODV and ARAN in VANET network. Scenario simulation in accordance with input programs and then implemented blackhole attacks on one of the nodes and using only one model of the topology, the topology model based on a system of communication Vehicle to Vehicle (V2V). Scenario simulated with the network simulator 2 (NS2) with the change of the number of nodes as 10, 20, 30, and change the nodes speed of 15 m/s, 18 m/s, 20 m/s. To analyze the performance, use some test parameters, such as packet delivery ratio (PDR), average end-to-end delay, packet loss ratio, routing overhead, convergence time, and normalized routing load. By looking at the results of a simulation of the six such parameters obtained by routing protocol that SAODV superior almost in every parameters. Routing protocols SAODV superior are characterized by greater PDR when dynamic topology, with better the average end-to-end delay, smaller packet loss ratio, more efficient on convergence time, normalized routing load less than ARAN routing protocol, then the routing protocol that is more suitable to be applied to the test scenarios is protocols routing SAODV.

Keywords: VANET, ARAN, S-AODV, Blackhole, V2V.