Evaluasi kinerja protokol routing AODV, AODV-UU, dan AODV dalam mode serangan malicious pada vehicular Ad-hoc network = Performance evaluation of AODV,AODV-UU, and AODV with malicious attack mode on vehicular Ad-hoc network

Revient Noor Ode, author

Abstrak

Traffic is a major problem in large cities which requires wireless infrastructure that controls traffic density. Vehiculer Ad-hoc Network (VANET) which becomes communication among vehicles can solve the main problem of traffic congestion. VANET requires dynamic routing protocols such as AODV routing protocol and its extensions such as AODV-UU. Manhattan map is used in this simulation because it represents the condition of a big city. VANET network simulation with AODV routing protocol uses network simulator 2 (NS2) with the scenario of traffic density addition. We simulate routing protocol is AODV, AODV-UU, and AODV with malicious node attacks on Manhattan mobility model.
The simulation results show that VANET is more effective and efficient using AODV-UU than other routing protocol, because AODV-UU routing protocol has fast computation in transferring data. The results of VANET simulation experiments with AODV-UU routing protocol generated average delay of 16.56 ms, average packetloss of 0.228%, and average throughput of 159.64 ms. In the VANET network simulation using AODV routing protocol with malicious nodes attack mode, packetloss values generated in very large values from 30% to 50%. This results shows that a malicious hacker attacks on VANET network using AODV routing protocol will decrease the Quality of Service (QoS) performance.