Abstract

The requirement of secure communication is very crucial part in network due to presence of unwanted attackers. The SDSR is identified the packet dropping but only due to presence of attacker. If an intrusion is detected quickly enough, the intruder can be identified and turned out from the network before any harmful action is done or any data are compromised. Moreover, proposed SDSR have served as prevention, acting to prevent intrusions. Proposed scheme enables the collection of information about intrusion techniques that can be used to reinforce the intrusion prevention facility. The performance of previous scheme is better and secure network from calculating the trust value of values and the trust value calculation is dependent on the packets forwarding of nodes in network. The performance of normal routing, with presence of Balckhole attack (BAODV), Old-Prevention (SAODV) and Proposed SDSR prevention performance is evaluated. The performance of proposed security system is better because at receiver end identified the packets dropping and set the threshold of dropping and also identified the attacker infection existence in network that shows the attacker effect and also affected the routing performance of network. The proposed SDSR performance is measured
through performance metrics and a result shows the improvement in performance.

References

16. https://www.isi.edu/nsnam/ns/
Index Terms

Computer Science  Security

Keywords

VANET, SDSR, Security, Routing, RSU, SAODV, Attacker.