Abstract

Sybil attacker is the routing layer active attacker that replies with multiple identification number (ID's) to nodes that forward request to attacker in a different time instant and drop the data forwarded to attacker after link establishment. The proposed research work is provides the novel secure Intrusion Detection System (IDS) against routing misbehavior of Sybil attack in MANET. The IDS are not determining whether the losses are caused by link errors. It determines the loss due to malicious nodes. In the especially interested in the insider Sybil attack case, whereby malicious nodes that are part of the route exploit their data of the communication context to drop an amount of packets critical to the network performance. The basic idea behind this method is that even though malicious dropping may result in a packet loss rate that is not comparable to normal channel losses. The attacker loss is more than the loss of channel. The proposed IDS is detecting attacker node that reply with multiple ID’s and broadcast the particular attacker original ID’s that generate fake ID’s. Therefore, by detecting the malicious or attacker loss % is decided whether the packet loss is purely due to a combined effect of fake ID’s for malicious drop. The routing performance is measured through
performance metrics and detection through TPR and FPR. The simulation of attacker and proposed IDS is done in ns-2 simulator.

References

8. R. Vintoh kumar, Mr. P. Ramesh,Dr. H. Abdul Rauf, "Cluster Based Enhanced Sybil Attack Detection in MANET through Integration of RSSI and CRL", IEEE International Conference on Recent Trends in Information Technology, pp. 1-7, 10-12 April 2014.
15. www.isi.edu/nsnam/ns/
Index Terms

Computer Science 
Networks

Keywords

Sybil attacker, MANET, IDS, Routing, Multiple Identities, performance metrics, ns-2