Abstract

Wireless networking is becoming one of the most important technologies nowadays, allowing users to get services and access information regardless of their location and allows users to communicate with each other wirelessly without depending on any fixed infrastructure. However, MANET works under an assumption that all nodes in the network are collaborating to forward packets which in fact isn't true as there are selfish nodes which refuse to forward the packets to reserve its energy and other resources, also there are misbehaving nodes (attack nodes) which drop packet to harm the network. So, with the presence of the selfish nodes and dropping attack nodes the sureness of the data packet delivery to the destination is absent, therefore, the importance of an intrusion detection system arises to prevent those kinds of nodes from harming the network and make sure that data packet arrives at the destination node. As the importance of the MANET increases, it became a point of interest to the researchers to secure it, so many schemes like Watchdog and Pathrater; Ex-Watchdog; TWOACK; AACK and A3ACK were introduced to achieve this goal. The reference to all techniques is the watchdog technique but it has six weaknesses which are it fails to detect
malicious misbehaviors with the presence of the following: (i) partial dropping; (ii) collusion; (iii) false misbehavior report; (iv) limited transmission power; (v) receiver collisions, and (vi) ambiguous collisions. The ACK based techniques were proven to detect malicious misbehaviors with the presence of collaborative attacks, receiver collisions, and limited transmission power. This paper introduces a study of the ability of the ACK based techniques to overcome a major disability in watchdog technique (using omnet++ simulator) which is used to detect malicious misbehaviors with the presence of partial dropping 50%. The importance of choosing partial dropping comes from simulating a real attack scenario, also it is more difficult for the intrusion detection system to detect attackers with partial dropping so, in some way using a partial dropping attack is an evaluation of the strength of the intrusion detection system technique. From this research, it is proven that the ACK based techniques can actually overcome this disability but only with low speed as with low speed the performance is acceptable but with high speed and the presence of collaborative attacks the ACK based techniques have low performance.

References


Index Terms

Computer Science

Networks

Keywords

Mobile Ad hoc Network (MANETS), Ack-based Intrusion Detection System, Dropping attack, Partial dropping, OMNET++