Mobile Ad-Hoc network (MANET) is a temporary infrastructure less network. This network is formed by combining some set of wireless mobile hosts [1] [5]. The host is called as a node which dynamically establishes their own network. Intrusion detection in MANETs, however, is challenging for a number of reasons. These networks change their topologies dynamically due to node mobility; lack concentration points where traffic can be analyzed for intrusions; utilize self-configuring multi-party infrastructure protocols that are susceptible to malicious manipulation; and rely on wireless communications channels that provide limited bandwidth. To overcome these constraints, researchers have proposed a number of intrusion detection approaches specifically for MANETs. Intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources. In this IDS architecture multilayer specification based detection engine is used along with Random Walker Detector (RWD) [1] [16]. It randomly traverses a network and finds out that on which node which attack is occurred. If there is attacks it performs re-routing.
References


Index Terms

Computer Science Wireless

Keywords

Attacks, Intrusion Detection System (IDS), and Mobile Ad-Hoc network (MANET), Random Walker Detector (RWD).