ABSTRACT

Networks are protected using many firewalls and security software. Several of them are not sufficient and effective. Many intrusion detection systems for mobile ad hoc networks are focusing on either routing protocols or their efficiency, but they do not address the security problems. A number of nodes may be selfish meaning that by not forwarding the packets to the target, thereby cutting back the battery power. Some others may act malevolent by commencement of security attacks similar to denial of service or hack the data. The ultimate aim of the protection solutions for wireless networks is to offer security services, for instance confidentiality, authentication, accessibility, integrity, and secrecy to mobile users. This thesis proposes a multitier intrusion detection system. Here three tiers are application, routing and trust. The data transfer takes place between different nodes. First a trusted connection is established between different nodes. Second the routing policy is conformed for all nodes. Finally at the application layer data is routed on the type of application. The node not following trust or routing policy is considered a malicious node. In this research work simulation different types of attacks was done. Then the performance of these attacks against the proposed algorithm has been calculated and result is displayed.