Abstract

Mobile Ad-hoc network is a temporary network of mobile nodes where mobile nodes communicate with each other through wireless links with no fixed infrastructure & no centralized control. Each mobile node in such a scenario acts as both a router & host. Nodes within each other’s radio range communicate directly, while those other nodes that are far apart used as relays. Thus the nodes find a path to the destination node using routing protocols. Minimal configuration & quick deployment make them suitable for emergency situations like war, emergency medical situations etc. Since Mobile Ad-hoc networks lack an infrastructure, they are exposed to a lot of vulnerabilities. In this paper, we present a survey on the protocol stack based security vulnerabilities in MANETs. All these vulnerabilities attempt to affect the overall performance and throughput of the network. The intent of this paper is to classify and explain the security vulnerabilities in the MANET protocol stack.

References

- Vikrant Gokhale, S. K. Gosh, and Arobinda Gupta, &quot;Classification of Attacks on Wireless Mobile Ad Hoc Networks and Vehicular Ad Hoc Networks a Survey&quot;.
Protocol Stack based Security Vulnerabilities in MANETs

- Mohammad Ilyas, “The Handbook of Ad Hoc Wireless Networks”.
- Hoang Lan and Uyen Trang Nguyen, “Study of Different Types of Attacks on Multicast in Mobile Ad hoc Networks”. Proceedings of ICNICONSMCL06, 0-7695-2552-0/06 @ 2006 IEEE.
- Sonja Buchegger and Jean-Yves Le Boudec, “Cooperative Routing in Mobile Ad hoc Networks: Current Efforts Against Malice and Selfishness”. In Lecture Notes on Informatics, Mobile Internet Workshop, Germany, October 2002. Springer.

Index Terms
Keywords
MANETs  DoS  Ad-hoc  Security