Abstract

MANETs (Mobile Adhoc Networks) are used to build up dynamic wireless networks which have no strictly defined infrastructure and no fixed topology with lucrative flexibilities to be used in various applications. Nodes with malicious intent or misleading behavior can join the adhoc network together with trustworthy nodes easily due to inherent characteristics of MANETs which makes them more prone to several attacks than wired networks. Conventional security policies and mechanisms designed for wired networks are mostly considered inadequate and ineffective for these highly dynamic and resource-constrained Adhoc networks. To design and develop security models for MANETs we must first be intriguing about the possible security attacks that may pounce upon different adhoc network scenarios. This paperwork focusses our attention on a comprehensive review to the various security threats and attacks prevalent in MANETs with the classification being done by taking into account the layered architecture of TCP/IP protocol suite underneath it.

Index Terms

Computer Science Wireless

Keywords

Internal attacks, External attacks, Active attacks, Passive attacks, Blackhole attack, Wormhole attack, Byzantine attack, Flooding attack, Colluding Misrelay attack.