Abstract

A wireless mesh network is a kind of multi-hop network and can be used as synonym for an ad-hoc network. It is a network having many to many connections with the capability of dynamically healing the network topology. Security is a challenging application of a wireless mesh network. The self configurable self organized nature makes a wireless mesh network more vulnerable to various types of attacks. Exploitation of a WMN can cause a large scale degradation of network performance. In this paper we have discussed some attacks that are performed on various layers of TCP/IP model. And we performed a comparative study for a specific network layer attack: grey hole attack. A grey hole attack is often difficult to detect and recover. There are different techniques for its detection which have their advantages and shortcomings. We have discussed some of them in this paper.
A Survey on Grey Hole Attack in Wireless mesh Networks


- S. Banergee, “Detection/Removal of cooperative black and gray hole attack in mobile ad-hoc networks”; in 2008 WCECS.
A Survey on Grey Hole Attack in Wireless mesh Networks

- J. Eriksson, M. Faloutsos, and S. V. Krishnamurthy, "Routing amid colluding Attackers;" in Proc. 2007 ICNP, pp. 184-193

Index Terms

Computer Science

Wireless
Keywords
Grey hole attack  Wireless mesh networks  Ad-hoc networks  Routing layer.