Abstract

Mobile ad hoc networks (MANET) are widely used in places where there is little or no infrastructure. A number of people with mobile devices may connect together to form a large group. Later on they may split into smaller groups. This dynamically changing network topology of MANETs makes it vulnerable for a wide range of attack. In this paper we propose a complete protocol for detection & removal of networking Black/Gray Holes.

Reference

- "Security Issues in Mobile Ad Hoc Networks- A Survey" Wenjia Li and Anupam Joshi, Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County.
- Sanjay Ramaswamy, Huirong Fu, Manohar Sreekantaradhya, John Dixon, and Kendall Nygard, "Prevention of Cooperative Black Hole Attack in Wireless Ad Hoc Networks”. In Proceedings of 2003 International Conference on Wireless Networks (ICWN'03), Las Vegas,
Detection and Removal of Cooperative Black/Gray hole attack in Mobile AdHoc Networks

- Sudath Indrasinghe, Rubem Pereira, John Haggerty, "Conflict Free Address Allocation Mechanism for Mobile Ad Hoc Networks", 21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)
- Mansoor Mohsin and Ravi Prakash, "IP Address Assignment in a mobile ad hoc network", The University of Texas at Dallas Richardson, TX Kaixin Xu, Xiaoyan Hong, Mario Gerla Computer Science Department at UCLA, Los Angeles, CA 90095 project under contract N00014-01-C-0016

Index Terms

Computer Science          Communication

Key words

Mobile Ad-hoc Networks

Black Holes

Gray Holes

Routing

AODV

Routing Table