Detection and Removal of Co-Operative Black Hole Attack in Manet

Abstract

Advancement in the research field has witnessed a rapid development in Mobile Ad-hoc Networks. The distributive nature and the infrastructure less structure make it an easy prey to security related threats. In this paper, we propose a secure routing protocol for DSR called as BDSR (Baited Black Hole Attack) for the detection and the removal of Black Hole and Co-operative Black Hole attack in MANET. A black hole is a malicious node which replies the route requests that it has a fresh route to destination and drops all the receiving packets. The damage will be serious when they work as a group. This type of attack is called cooperative black hole attack. The BDSR scheme merges the proactive and reactive defense architecture. In the initial stage it uses a proactive architecture, i.e., uses a Bait id concept for the detection of malicious nodes present in the network. Upon the completion of initial stage it switches to reactive defense strategy. The secure routing protocol resulted in increased packet delivery ratio and reduced overhead ratio. The extended defense routing protocol worked efficiently for the malicious node detection and removal in case of Co-operative Black Hole attack resulting in increased network performance.

References

- Po-Chun TSOU, Jian-Ming CHANG, Yi-Hsuan LIN, Han-Chieh CHAO, Jiann-Liang CHEN
"Developing a BDSR Scheme to Avoid Black Hole Attack Based on Proactive and Reactive Architecture in MANETs" ICACT2011.
- Irshad Ullah and Shoaib Ur Rehman, "Analysis of Black Hole Attack on MANETs Using Different MANET Routing Protocols," 2010

Index Terms
Computer Science Wireless

Keywords
Black Hole  Co-operative Black Hole  Dsr  Manet