

Performance Analysis of OLSR Protocol under MPR Attack in Progressive Size Grid MANET

Submitted by aekwall on Tue, 05/26/2020 - 11:04am

Title Performance Analysis of OLSR Protocol under MPR Attack in Progressive Size Grid MANET

Publication Type Conference Paper

Year of Publication 2019

Authors [Soualfi, Abderrahim Hajji](#), [Agoujil, Said](#), [Qaraai, Youssef](#)

Conference Name 2019 International Conference on Wireless Networks and Mobile Communications (WINCOM)

Date Published oct

Keywords [1-hop neighbor nodes](#), [battery life](#), [central administration](#), [compositionality](#), [control messages](#), [effective routing protocol](#), [efficient OLSR attacks](#), [grid MANET](#), [hello messages](#), [low level applications](#), [MANET](#), [MANET security](#), [Metrics](#), [mobile ad hoc network](#), [mobile ad hoc networks](#), [mobile ad-hoc network](#), [mobile devices](#), [MPR attack](#), [OLSR](#), [OLSR protocol](#), [Performance analysis](#), [predefined infrastructures](#), [proactive routing protocol](#), [progressive size grid MANET](#), [pubcrawl](#), [relay networks \(telecommunication\)](#), [Resiliency](#), [Routing protocols](#), [security](#), [telecommunication network topology](#), [topological information](#)

Abstract

Mobile Ad-hoc NETWORK (MANET) is a collection of mobile devices which interchange information without the use of predefined infrastructures or central administration. It is employed in many domains such as military and commercial sectors, data and sensors networks, low level applications, etc. The important constraints in this network are the limitation of bandwidth, processing capabilities and battery life. The choice of an effective routing protocol is primordial. From many routing protocols developed for MANET, OLSR protocol is a widely-used proactive routing protocol which diffuses topological information periodically. Thus, every node has a global vision of the entire network. The protocol assumes, like the other protocols, that the nodes cooperate in a trusted environment. So, all control messages are transmitted (HELLO messages) to all 1-hop neighbor nodes or broadcasted (TC and MID messages) to the entire network in clear. However, a node, which listens to OLSR control messages, can exploit this property to lead an attack. In this paper, we investigate on MultiPoint Relay (MPR) attack considered like one of the efficient OLSR attacks by using a simulation in progressive size gridMANET.

DOI [10.1109/WINCOM47513.2019.8942557](https://doi.org/10.1109/WINCOM47513.2019.8942557)

Citation Key soualfi_performance_2019



[security](#) [Resiliency](#) [pubcrawl](#) [Routing protocols](#) [Metrics](#) [MANET](#) [mobile ad hoc networks](#) [mobile ad-hoc network](#) [telecommunication network topology](#) [mobile devices](#) [Compositionality](#) [relay networks \(telecommunication\)](#) [battery life](#) [MANET](#) [security](#) [Performance analysis](#) [1-hop neighbor nodes](#) [central administration](#) [control messages](#) [effective routing protocol](#) [efficient](#) [OLSR attacks](#) [grid](#) [MANET](#) [hello messages](#) [low level applications](#) [mobile ad hoc network](#) [MPR attack](#) [OLSR](#) [OLSR protocol](#) [predefined infrastructures](#) [proactive routing protocol](#) [progressive size](#) [grid](#) [MANET](#) [topological information](#)
