# Evaluation of Detection Method to Mitigate DoS Attacks in MANETs



| | |
|---|---|
| Title | Evaluation of Detection Method to Mitigate DoS Attacks in MANETs |
| Publication Type | Conference Paper |
| Year of Publication | 2018 |
| Authors | Alsumayt, A., Haggerty, J., Lotfi, A. |
| Conference Name | 2018 1st International Conference on Computer Applications Information Security (ICCAIS) |
| Date Published | apr |
| Keywords | Ad hoc networks, composability, DoS, Filtering, Firewalls (computing), MANET Attack Detection, MANETs, Metrics, mobile computing, Monitoring, MrDR, pubcrawl, Resiliency, Routing, Routing protocols |


Abstract

A Mobile ad hoc Network (MANET) is a self-configure, dynamic, and non-fixed infrastructure that consists of many nodes. These nodes communicate with each other without an administrative point. However, due to its nature MANET becomes prone to many attacks such as DoS attacks. DoS attack is a severe as it prevents legitimate users from accessing to their authorised services. Monitoring, Detection, and rehabilitation (MrDR) method is proposed to detect DoS attacks. MrDR method is based on calculating different trust values as nodes can be trusted or not. In this paper, we evaluate the MrDR method which detect DoS attacks in MANET and compare it with existing method Trust Enhanced Anonymous on-demand routing Protocol (TEAP) which is also based on trust concept. We consider two factors to compare the performance of the proposed method to TEAP method: packet delivery ratio and network overhead. The results confirm that the MrDR method performs better in network performance compared to TEAP method.


| | |
|---|---|
| URL | https://ieeexplore.ieee.org/document/8441952 |
| DOI | 10.1109/CAIS.2018.8441952 |
| Citation Key | alsumayt_evaluation_2018 |

Ad hoc networks composability DoS Filtering Firewalls (computing) MANET Attack Detection MANETs Metrics mobile computing Monitoring MrDR pubcrawl Resiliency Routing Routing protocols