Performance Evaluation of Attack Detection Algorithms in Delay Tolerant Networks

International Journal of Computer Applications
Foundation of Computer Science (FCS), NY, USA

Volume 171
Number 4

Year of Publication: 2017

Authors:
Chaudhari Rajashri M., Patil Manesh P.

10.5120/ijca2017915008

Abstract

DTN (Delay Tolerant Network) is a new kind of wireless technologies which includes Radio Frequency (RF) and acoustic (sonar) technologies. DTN developed for interplanetary use where the speed of light is slow. DTN is a new kind of network derived from deep space communication. DTN is characterized as long delay and intermittent connectivity. The Delay Tolerant Network (DTN) is more vulnerable to different kinds of attacks like blackhole and greyhole attacks, due to limited connectivity. There is no end to end connectivity between source & destination in DTN. So that it uses store, carry and forward mechanism to transfer the data from one node to other node. Delay tolerant networks (DTNs) are characterized by delay and intermittent connectivity, due to this, malicious nodes drops all or a part of the received messages. This dropping behavior is known as blackhole and greyhole attacks respectively. Existing research scheme can detect individual attackers well but they cannot handle the case where attackers cooperate to avoid the detection. So that SDBG scheme implements an algorithm to detect individual attacks with collusion attack. The simulation result shows the protocol reduces the delivery delay using RAPID protocol by detecting collusion attacks that is
simulated using the ONE simulator.

References


Index Terms

Computer Science Wireless
Keywords

Delay Tolerant Network, Blackhole attack, Greyhole attack, Collusion, Detection Accuracy, and Delivery Delay.