Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol

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

Volume 125

Number 4

Year of Publication: 2015

Authors:
Shruti Bhalodiya, Krunal Vaghela

10.5120/ijca2015905878

Abstract

Mobile ad-hoc network (MANET) is a self-deliberate data network, where all nodes behave like host or router. MANET is a collection of number of mobile nodes or devices that randomly generate a temporary network. Security is the fundamental requirement in MANET due to its behavior of changing topology, open medium and lack of centralized authentication. This leads to various security attacks in mobile ad hoc network and violate the criteria of routing mechanism. Mobile Ad-hoc network doesn’t need backbone infrastructure support and it is very reliable and also contains the routable networking environment. In this paper, the effect of flooding attack in AODV based network is explained. The network parameters like Throughput, Packet Delivery Fraction (PDF) and End to End Delay are compared with normal network (without flooding attack) and a network with one or more flooder nodes. The performance of network parameters is compared in all the three scenarios. We have proposed a scheme which is finds single or number of malicious nodes in the network and drops fake packets.

References
Enhanced Detection and Recovery from Flooding Attack in MANETs using AODV Routing Protocol


Index Terms
Computer Science Networks
Keywords

MANET, AODV routing protocol, Flooding attack, NS-2.35