Improving Security Issues in MANET AODV Routing Protocol

Mahsa Gharehkoolchian[1], A.M. Afshin Hemmatyar[2], and Mohammad Izadi[2]

[1] School of Science and Engineering, Sharif University of Technology, International Campus, Kish Island, Iran
Gharehkoolchian@gmail.com
[2] Department of Computer Engineering, Sharif University of Technology, Tehran, Iran
{Hemmatyar,Izadi}@sharif.edu

Abstract. Mobile Ad-hoc Networks (MANETs) are forming dynamically by joining or leaving the nodes into/from the network without any fix infrastructure. It is also possible that each mobile node act as a host or router. This kind of wireless network is prone to various security threats or attacks due to its unique characteristics like dynamic topology, open medium, lack of central monitoring, etc. So security is a vital scope in MANET to protect communication between mobile nodes. Ad-hoc On-demand Distance Vector (AODV) is one of the on-demand reactive routing protocols in MANET that initially was improved without considering security protection. Significant attempts have been done to secure AODV routing protocol in MANET but there are still critical challenges to overcome. In the present study, after reviewing secured protocols of some previous researches, an improved protocol is proposed to enhance the security of AODV routing protocol against black hole attack. For this purpose, we used a different level of trust for MANET nodes and imposed the limitations based on the nodes' trust level, in order to detect the compromised nodes and malicious behaviors inside MANET; which leads to the low delay and high performance in the network. Finally, we simulated the proposed protocol with NS-2 simulator as a means to validate it and evaluate the results. In fact, the results, demonstrate the efficiency of the presented protocol and its resistance to the black hole attack in comparison to AODV routing protocol.

Keywords: AODV protocol, Black hole attack, MANET, Secure routing, Trust-based technique.

1 Introduction

Accessing network resources from any location makes the wireless networks the most popular networks all over the word. On the other hand, this key feature can increase many problems regarding data security. By increasing the number of mobile hardware and devices, wireless networks' security becomes a big concern issue. MANET is a class of wireless networks that include mobile users which are connected by wireless

N. Mitton et al. (Eds.): AdHocNets 2015, LNICST 155, pp. 237–250, 2015.
DOI: 10.1007/978-3-319-25067-0_19

links with no fixed infrastructure (access point) and are formed on ad-hoc basis. Lack of fixed structures makes MANET more vulnerable to different kinds of attacks in comparison with other types of networks.

MANET does not have typical routers for routing in the network. Instead, each node in the system should function as a router for the other nodes. As a result, malicious behavior from any node can destroy network's function.

One of the most well-known routing protocols in MANET is Ad-hoc On-demand Distance Vector (AODV) protocol, a class of the reactive protocols that finds a route on demand by flooding the network with Route Request packets. This protocol is vulnerable to security threats and attacks. Overall, significant attempts have been done regarding security in MANETs but security issues in a wireless networks still exist.

In this article, first we are going to discuss different security threats and vulnerabilities in MANET and AODV. In next subsections different type of attacks, security attributes and MANET routing protocols are described. Then, the related works, the proposed protocol and achieved results are mentioned.

2 Routing Attacks and Threats in MANET

2.1 Some Attacks against MANET

Networks usually threat by the attackers, different types of attacks are known as flooding attack, gray-hole attack**,** Denial of Service (DoS) attack, impersonation attack, black hole attack, modification attack, etc. At the following section some of them are explained [1], [2]:

1) Wormhole attack: This attack creates a tunnel by attackers who placed themselves in the strategic position of the network; declaring the tunnel as a shortest path of transmission in order to record the traffic or ongoing packets.
2) Black Hole attack: A malicious node realizes a neighbor initiates to send a RREQ packet, it RREP the fake packet with the highest value of sequence number and lowest hop count. Consequently, neighbor node assumes that this malicious node has the best route to the destination. Thus, the source node discards all other RREPs; malicious node drops all the packets as well. In other words, it stops forwarding packets to the right destination [3], [4].
3) Flooding attack: The attacker set up a path between network's nodes to disseminate its unpleasant packets and congest the network.
4) Gray Hole attack: attacker acts as a both malicious and normal node in the network with aim of misleading network, being detected hardly and preventing them to reach the destination [5].
5) Modification attack: both Impersonation and misrouting attacks are including modification attacks.
6) Denial of Service (DoS) attack: a malicious node with the increase of fake RREQs, floods the network. Subsequently, non-malicious nodes cannot work well in the