International Journal of Computing Science and Information Technology, 2018
ISSN: 2278-9669, April 2018 (http://ijcsit.org)

Various Network Security Attacks And Prevention Of Attacks

Dr. K.R. Viswa Jhananie [1].
Seshadripuram Academy of Business Studies,
Bangalore, India;
viswajhananie.kr@gmail.com

Dr. S. Deepa [2].
Presidency College,
Bangalore, India,
sdeepa369@gmail.com

Received January 2018

Abstract

In the world of technology, network is used everywhere in today's life. As the amount of internet communication increases, the number of attacks also increases in parallel, which becomes a challenge to secure the data. Especially, securing data in Mobile Ad-hoc Networks (MANET) are challenging, because, they are infrastructure less, self-organizing and due to multi-hop network. This paper presents various attacks in network and provides a solution for securing the data.

Keywords: MANET, attacks, security, data packet

1. Introduction

Ad-hoc networks are easy to set up as they work without any fixed infrastructure [1]. Central administration is not required while forwarding the data packets, instead every node will be in-charge of sending and receiving the data packets. Mobile ad-hoc network is useful even when there is no proper communication infrastructure. MANETs are useful in real time business applications. They can also be used in sensor network which is composed of very large number of small sensors.

MANETs are vulnerable to many attacks, because of its dynamic nature [2]. The various routing attacks that MANETs come across are wormhole attack, black hole attack, gray hole attack, jamming, eavesdropping. The main aim of this paper is to find some major attacks that MANETs are susceptible. The related work is discussed in section-2. Different security attacks are addressed in section-3. A solution is proposed in section-4. Finally, conclusion and future work are given in section-5.

2. Related Work

Shivangi et al [3] has used neighbor list detection approach to detect wormhole attack. Anamika et al [4] has compared MAC with IP address for detecting Sybil attack. Aashima et al [5] has used Security Aware Routing (SAR) in detecting sinkhole attack. The trustworthiness of a node is verified at the time of receiving route request from its neighbor node itself using trust hierarchy. Abhishek et al [6] has used Knowledge Based Intelligent Node (KBIN) to reduce sleep deprivation attack in MANETs.

3. Security Attacks

Attacks in network can broadly be classified as internal attacks and external attacks. In internal attack, any node that is present in the network can attack the other nodes by creating link between them [7]. In external attack, nodes from outside cause congestion in network by giving wrong routing information. The external attacks can be classified as active attacks and passive attacks. In active attack, the attacker snoops the data without altering it. This mainly targets confidentiality of data. Passive attack is used to get the information about the network. Attacker will alter the data and even can disrupt the normal functioning of the network. The various attacks that affect routing in MANET are

a. Black hole attack:

In black hole attack, the malicious node act as a trustworthy node by using a routing protocol and advertises itself as having a short route to the destination node. An attacker sends a fake RREQ message in order to form a black hole attack [8].

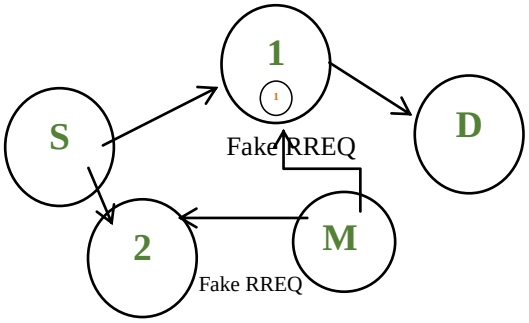

Fig-1 Black hole formation by fake RREQ

S→ Source node, D→ Destination node, M→Malicious node, 1,2→ nodes in the network

The source node after receiving the RREQ from all the routes, decides to choose the shortest path for further communication. Since the malicious node advertises to have the shortest route to the destination node, the source node chooses this route ignoring all the other routes. Thus the malicious node easily drops all the data packets that come from the source node.

b. Wormhole attack:

In wormhole attack, the attackers will not act as a real node in the network, instead they form a tunnel from source node to destination node. Thus the malicious node over hear the transmissions that takes place within the network and gets the complete access of the entire network [9].

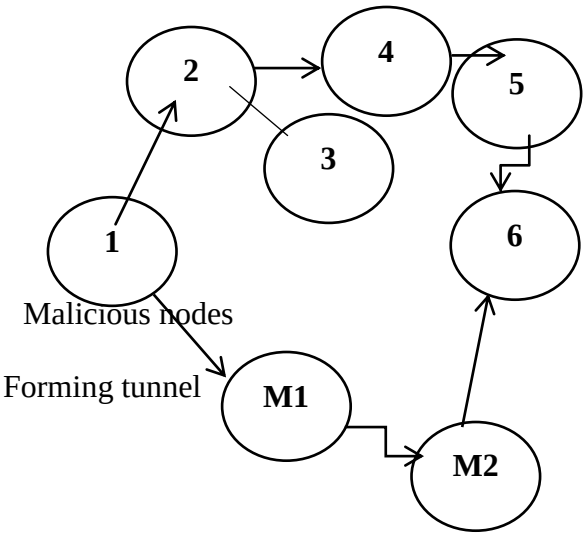

Fig-2 Tunnel formation by malicious node in wormhole attack

1→Source node, 2,3,4,5→ nodes in the network, 6→ Destination node, M1,M2→ Malicious nodes.

c. Rushing attack:

In MANET, the source node will send a RREQ message to the neighboring nodes in order to find the shortest path to the destination node. The attacker node sends RREP message to the source node. Since, the source node receives this RREP first, this route is chosen for future communication, thus getting disconnected with the real route [10].

d. Sybil attack:

In this attack, the malicious node uses multiple identities at a particular time that leads to lot of miscommunication among the nodes in the network. By doing so, the malicious node might use the identity of a trustworthy node's identity also [11]. Thus, the entire network gets disturbed by the malicious node.

4. Proposed Solution:

A table is maintained in which the source node number, neighbor node number, hop count, sequence number, threshold value and destination node number are available.

When a source node sends route request message to its neighbor node, the sequence number of the neighbor node and the time taken by the node to receive the data is recorded. Then it is compared with the threshold value, which is common for every node. A specific time interval is set for every node within which the data packet should be received. If the time exceeds the given specific time and the sequence number does not match, then the node is identified as a malicious node. Then, this route is discarded by the source node and the same procedure begins for the other route. Thus the data packets can be transmitted safely from source to destination.

Simulation parameters:

Parameters used	Values
Area	1000 X 1000
Radio propagation model	Two way propagation
Network interface type	Wireless physical
MAC type	802_11
Maximum packet in the queue	50
Number of mobile nodes	30
Routing protocol	AODV
Topological area	800 X 600 sq.m
Simulation period	50ms

Table-1 parameters

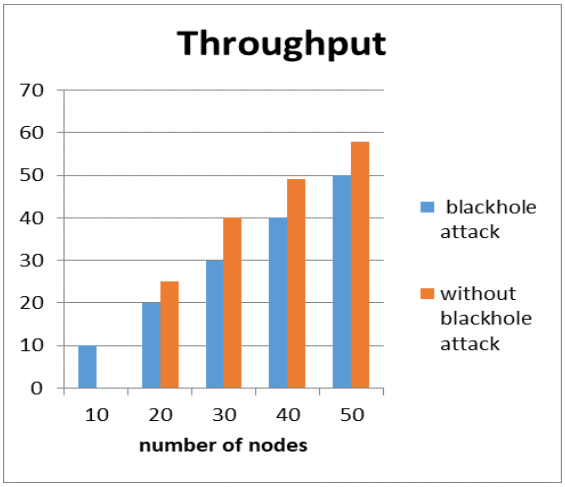

Fig-3 Throughput rates

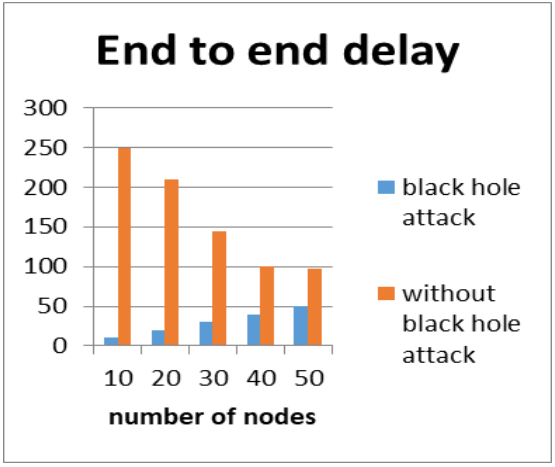

Fig-4 End to end Delay

The above figure-4 shows a high throughput rate with the proposed solution. Figure-5 shows that, the delay is very much reduced in the proposed solution.

5. Conclusion and Future work

MANETs are vulnerable to many attacks. In this paper, a solution is proposed to overcome black hole attack, which is a serious attack in MANET. The above results show high throughput ratio and reduced delay. It can be extended to different routing protocols and various mobility models.

REFERENCES:

1. D. Helen and D. Arivazhagan, "Applications, Advantages and Challenges of Ad-hoc Networks", JAIR, Vol-2, Issue-8, Jan 2014.

[2]. Umesh Kumar Singh, Kailash Phuleria, Shailja Sharma and D.N. Goswami, "An Analysis of security attacks found in Mobile Ad-hoc Network".

[3]. Shivangi Dwivedi and Priyanka Tripathi, "An Efficient Approach for Detection of Wormhole Attack in Mobile Ad-hoc Network", IJCA,Vol-104, No-7, Oct 2014.

[4]. Anamika Pareek and Mayank Sharma, " Detection and Prevention of Sybil Attack in MANET using MAC address", IJCA, Vol-122-No-21, July 2015.

[5]. Aashima and Gagandeep, "Study on Sinkhole Attacks in Wireless Ad-hoc Networks", IJCSE, vol-4, No-6, June 2012.

[6]. Abhishek Ranjan, Venu Madhav Kuthadi, Rajalakshmi Selvaraj and Tshilidzi Marwala, "Detection and Avoidance of Routing Attack in Mobile Ad-Hoc Network Using Intelligent Node", ITCSE – 2013.

[7]. Gagandeep, Aashima and Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", IJEAT, Vol-1, Issue-5, June 2012.

[8]. Nishant Sitapara and Sandeep B. Vanjale, "Detection and Prevention of Black hole Attack in Mobile Ad-Hoc Networks", ICETE, Feb 2010.

[9]. Anshika Garg and Shwetha Sharma, " A study on wormhole attack in MANET", IJSRET, Vol-3, Issue-2, May 2014.

[10]. Satyam Shrivastava, "Rushing attack and its prevention Techniques", IJAIEM, Vol-2, Issue-4, April 2013.

[11]. Abdullah Saad Al Shahrani, "Rushing Attacks in Mobile Ad-Hoc Networks", International conference on Intelligent Networking, Dec 2011.