I J C T A, 9(11) 2016, pp. 5103-5110

ADVANCED HIGHLY REPUTED AUTHENTICATED ROUTING PROTOCOL

Harleen Kaur [*] and Gagandeep Singh

Abstract: With the introduction of technology and increasing demand of computers the demand of wireless devices is also increasing. Almost all the people are using wireless devices and networks in their day to day life. As the wireless technology is increasing the attackers are also affecting the security of these systems by new techniques. In this paper we have discussed various security issues in Mobile ad-hoc network and different types of attacks possible on the different layers of mobile ad-hoc networks. Highly reputed authenticated routing protocol is a method used to guarantee an end to end authentication in network and ensures reliable transmission of data using public key cryptography and reputation techniques. The proposed system makes use of reputation value trust, value and then finding the optimized route for transmission of data in mobile adhoc network. Simulation result in of the proposed system is accurately predicted the packet delivery ratio, route throughput and packet loss.

Key Words: MANET, attacks, security issues, HRARAN.

1. INTRODUCTION

Mobile Ad Hoc network (MANET) is the wireless communication network, which helps the users to connect to any network without having any fixed infrastructure. It is a self-configuring network of mobile devices [1]. The ad Hoc network concept is not a new concept, but the demand of user to have portable devices has been resulted in the increasing demand of mobile ad-hoc network. Wireless system operates on with the centralized and access points which help the nodes to get connected to a network. Ad hoc network is the collection of two or more nodes, which don’t have any fixed topology and forms a temporary network.

A node can join or leave the network whenever it wishes. The mobile devices must be in a fixed range in order to communicate with each other. There may be multiple hops between the source node and the destination node. There is no fixed topology for the MANET. Mobile devices have a battery constraint operation.

2. CHARACTERISTICS AND APPLICATIONS OF MANET:

Mobile Ad- hoc networks are different from other networks due to the following characteristics[2]:

- The network doesn’t need any fixed infrastructure
- No fixed topology is required
- Multi-hop network

[*] Lovely School of Computer Science and Engineering, Lovely Professional University, Phagwara, Punjab, India Email: h29.bhullar@gmail.com

Due to these characteristics the use of Ad-hoc devices have been increased in many fields, some of its applications are listed below:

- Military operations
- Emergency/ rescue operations
- Smart sensors
- Robotic pets

3. AD-HOC NETWORK SECURITY ISSUES AND VULNERABILITY:

Mobile ad-hoc network is infrastructure less networks so it is more vulnerable [3]. They have discussed about various security issues and types of attacks.

Security issues in MANET:

- **Confidentiality:** It assures that the information or data is being accessed by an authorized user only, and any unauthorized users don't have the right to access it.
- **Availability:** It means that in order to send or receive the data the nodes must be available in the network.
- **Authentication:** It tells us whether the user is a genuine user or not, whether he has the right to access the network.
- **Integrity:** It tells us that the data is sent by the source should be received as it is to the receiver. There should be no modification of the information sent.
- **Non -repudiation:** It means when any kind of information is sent to the receiver then the user can't deny that he has not sent the particular data. Whenever any information is received by the receiver then it can't deny that he has not received any data.
- **Authorization:** It means to provide a certification or authority to a particular user to access that network.
- **Eavesdropping:** It is when a third person secretly gets to know about the transferred information without letting the sender and receiver know about it.
- **Traffic analysis:** It is when the attacker analyzes or checks the amount of data sent from the sender to the receiver over a network.

Vulnerabilities in MANET:

- **Lack of Boundaries:** Due to lack of fixed infrastructure the MANET nodes can join and leave the network whenever they wish, this make the MANET more vulnerable to attacks.
- **Compromised node:** Due to lack of infrastructure a compromised node can enter the network at any time and can attack with it.
- **Centralized System:** Due to the absence of a central monitoring system, it is very hard to detect the attacking node in the network.

Types of attack in MANET:

- **External Attacks:** Attack which is performed by the external node is external attack. It can be congestion, link spoofing etc.
- **Internal Attack:** Attack in which the node within the network harms the whole network. It can be like a black hole, greyhole, wormhole etc.

- **Denial of Services:** Attack in which the attacker prevents the server from providing any services to the other users.
- **Active Attack:** Attack in which the attacker attacks the network and even modifies its data. It can be jammed, spoofing, modification, replaying etc.
- **Passive Attack:** Attack in which the attacker attacks the network but don't modify the data. It can be eavesdropping, traffic analysis, monitoring etc.

4. ATTACKS ON DIFFERENT LAYERS OF MANET:

Development in the wireless network leads to increase in the number of portable devices worldwide. The wireless network topology is unpredictable and can change at any instance of time. Manet has many features which differentiate it from the wired network. A mobile node can act as server and client whenever it wants. Terminal nodes are responsible for the management and control operation.

Table 1
Attacks on different layers of MANET

Layers	*Type of attacks*
Application	Viruses and worms
Transport	Session hijacking, SYN flooding
Network	Blackhole, Link Spoofing, Replay attack, Greyhole, Wormhole
Data Link Layer	Traffic Analysis
Physical	Eavesdropping, jamming

- **Eavesdropping:** It is the type of attack in which the adversary listens to the conversation between two paired nodes secretly. The attacker's motive is to obtain the confidential information. This attack can be prevented by the encryption techniques.
- **Jamming:** It is the type of attack which the transferred data is interfered which corrupts the message and fails the transmission of data. Signal jamming or data jamming can be done by adding noise to the data.
- **Traffic analysis:** It is they type of attack in which the attacker analyzes the pattern of data being transferred. The attacker keeps a check on the number of packets being sent and received by the users
- **Blackhole attack:** In this attack the node acts as the part of a network and represents itself as the intermediate node to the destination node. The attacker node captures all packets and don't let it to reach to the destination.
- **Greyhole attack:** In this attack attacker consumes the packet, and selectively forwards the few messages to the destination and drops the other packets.
- **Link Spoofing:** In this attack the intermediate node acts as an intermediate node and acts as a fake route and captures the package sent through it.

5. ROUTING PROTOCOLS:

The mobile adhoc network makes use of certain rules which help in the transfer of data, these rules are known as protocols. There are basically three types of protocols used in the MANET proactive protocol, reactive protocol and hybrid protocol [6]. For different type of data transfer different routing protocols are used depending on the type of data and security needed. In Proactive protocols the nodes maintain a routing table of the other nodes and then whenever data are to be sent them by using the value from routing table they send the data. Due to the maintenance of table the proactive protocols are also known as table driven protocols. Dynamic destination sequenced distance vector routing protocol (DSDV), Wireless routing protocol (WRP), Cluster gateway switch routing protocol (CGSR) is table driven protocols. In reactive protocol the route discovery is done whenever there is a need of sending any data, no table is maintained in this, due to this it is referred as on demand routing protocol. Dynamic Source routing (DSR), Adhoc on demand distance vector routing (AODV), Associativity based routing (ABR), Signal Stability based adaptive routing protocol (SSA), Temporary ordered routing algorithm (TORA) are the types of reactive routing protocol. Hybrid routing protocol is the combination of both the reactive and proactive routing protocols. Zone routing protocol (ZRP), Sharp hybrid adaptive routing protocol (SHARP) are a type of hybrid routing.

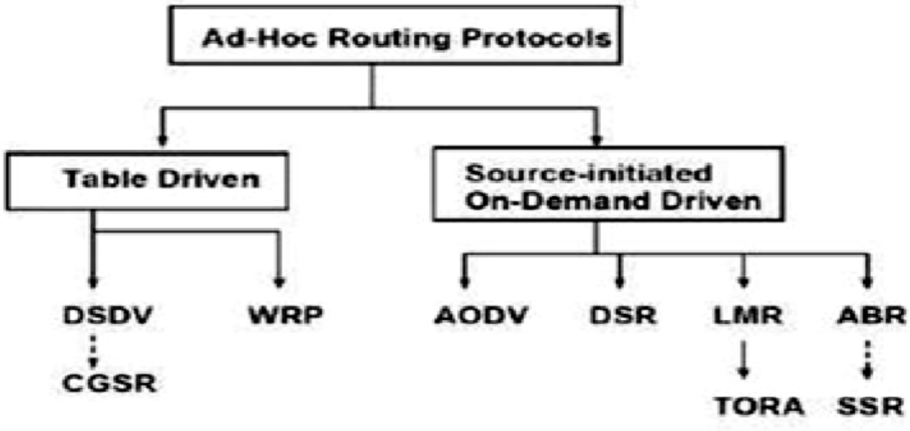

Figure 5.1 Routing Protocols

6. HIGHLY REPUTED AUTHENTICATED ROUTING PROTOCOL

HRARAN [5] protocol makes use of public key cryptography and reputation techniques. It uses the reputation value to find the co-operative and compromised nodes in an ad hoc network. HRARAN has five phases:

- Node Initialization
- Route Discovery Phase
- Reputation value Phase
- Data Transmission Phase
- Performance Evaluation

In Authenticated Node Initialization each node must get a certification before connecting to a network. The certificate has an IP address of client, Public key of client, timestamp of certificate creation and expiry. All these things are together signed by a trusted server. The source broadcast the RREQ to the next hop and when it reaches to the destination the receiver sends the RREP to the trusted server. Route Lookup Phase helps to authenticate the route discovery. When we have to send a packet from source to destination, then the source node broadcast the message to all the nodes and the intermediate nodes interested in the routing the packet broadcast it through the mobile ad hoc network. In Reputation Phase every node finds the reputation value. After getting the routing information the node decides its next hope and finds the shortest way to reach the destination. Reputation value (Repv) is calculated by: (number of routed packets- number of dropped packets) / total number of packets. In Data Transfer Phase the data is transferred from the source to the destination. The source chooses the highly reputed node to send its data to the destination. If any two nodes have the same reputed value the any intermediate node is chosen randomly by the source. When the data is received by the destination, then a data acknowledgment (DACK) is sent to the source by the same route in reverse order.

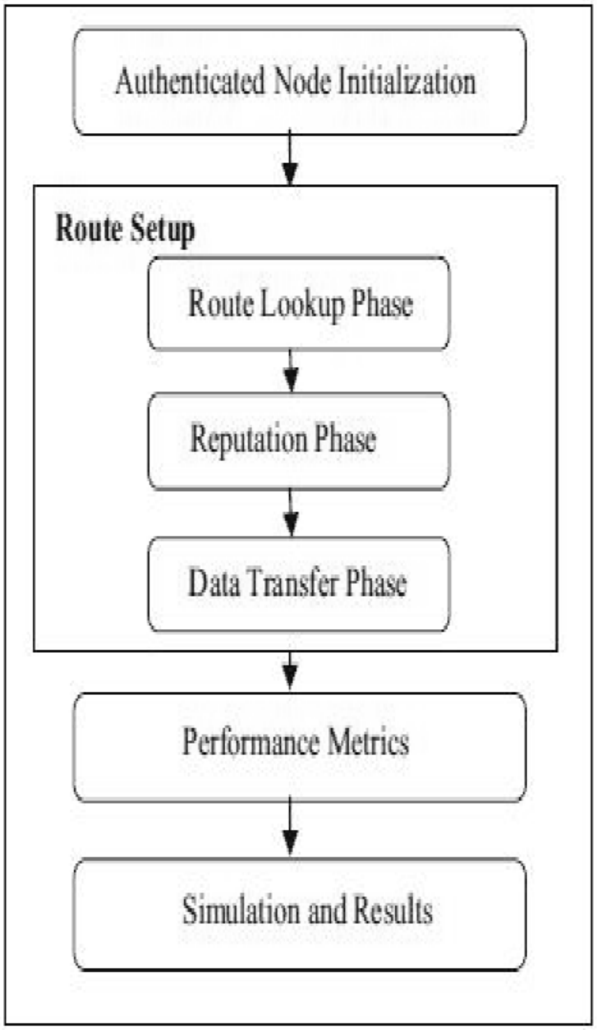

Figure 6.1 Phases of HRARAN

7. ADVANCED HIGHLY REPUTED AUTHENTICATED ROUTING PROTOCOL:

In highly reputed authenticated routing technique the reputation value of the nodes of the network is considered in order to transfer our data. It makes use of public key cryptography for transferring the data reliably. Reputation value helps to find whether the node is co-operative or not. But in this routing technique they have not considered the QoS parameters and denial of service attack was possible in this. So to resolve this problem new method is proposed in which the QoS parameters will be considered and DOS attack will be prevented from considering the trust value of a node.

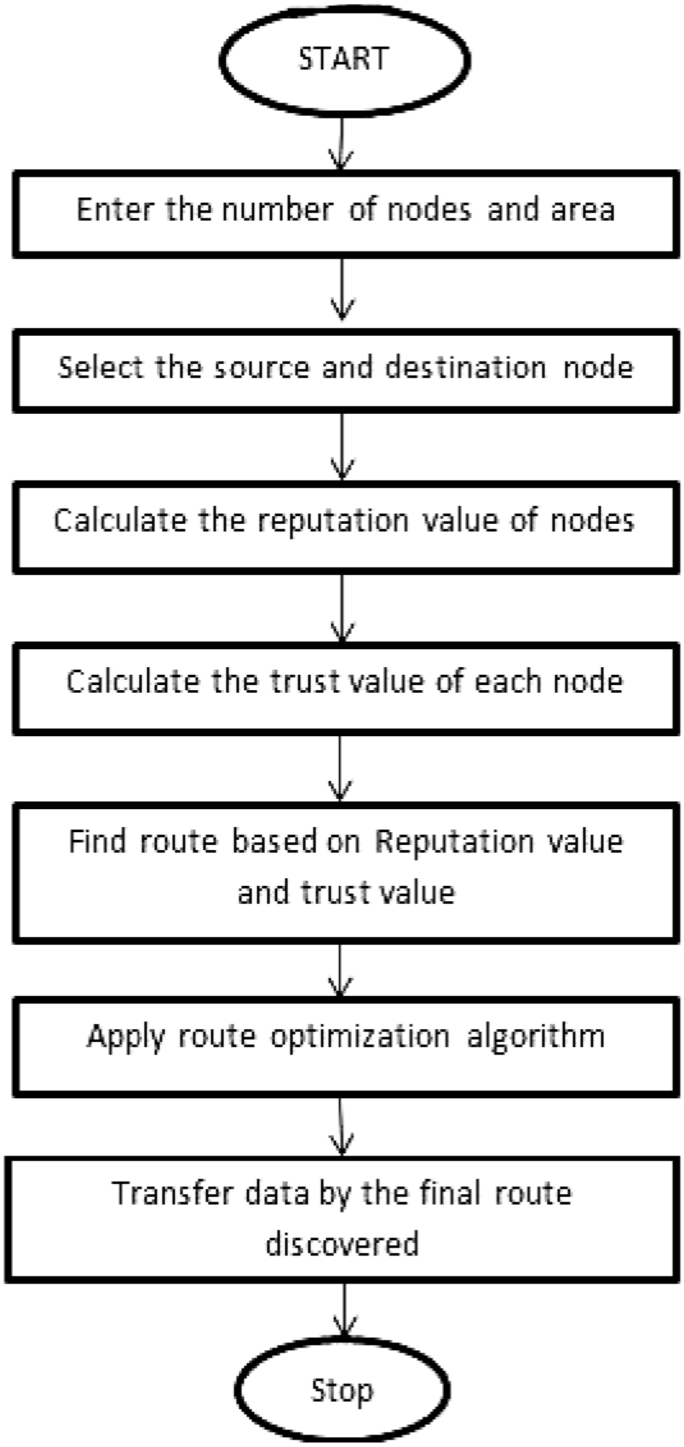
START
Enter the number of nodes and area
Select the source and destination node
Calculate the reputation value of nodes
Calculate the trust value of each node
Find route based on Reputation value and trust value
Apply route optimization algorithm
Transfer data by the final route discovered
Stop

Figure 7.1 Flowchart of Advanced HRARAN

8. SIMULATION AND RESULTS:

Route Throughput: Throughput of s system is defined by the amount of data that can be sent from the source to destination in a given interval of time. In advanced highly reputed authenticated routing protocol the throughput is more as compared to that of HRARAN.

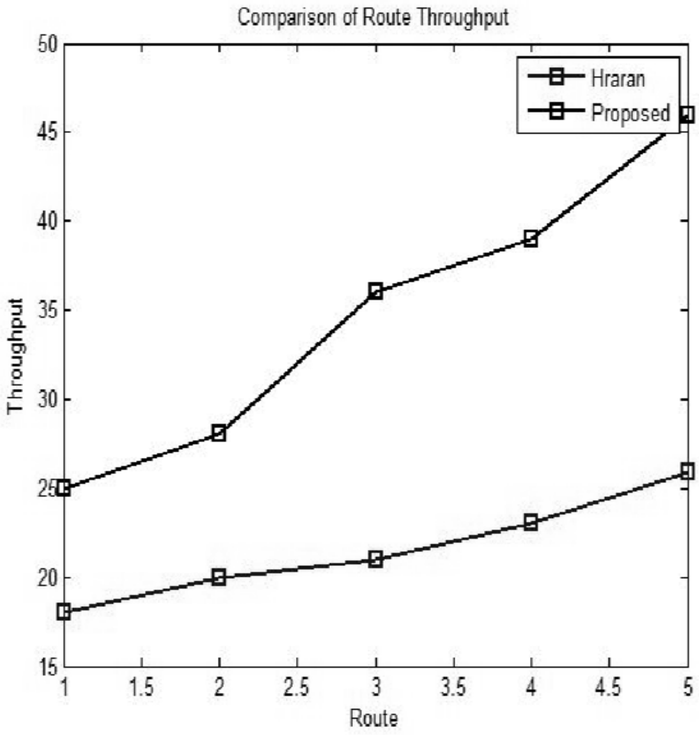

Figure 8.1 Performance Evaluation of Route Throughput

Packet Loss Ratio: Packet loss is when one or more packets don’t reach their intended destination, but they are being sent from the source and are lost during the transmission. In advanced HRARAN the packet loss is less than HRARAN.

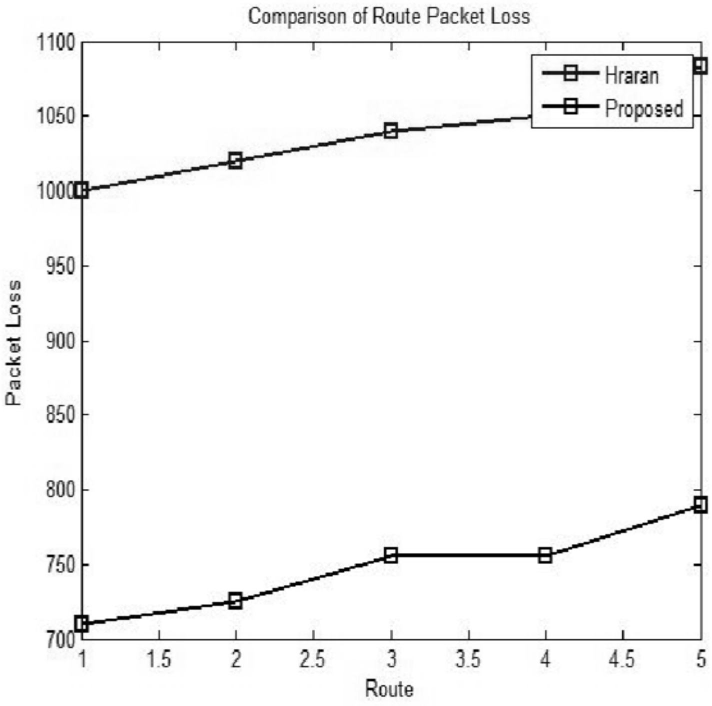

Figure 8.2 Performance Evaluation of Packet Loss

Packet delivery Ratio: It is the ratio of the number of packets sent to the number of packets received in a network. The packet delivery ratio in advanced HRARAN is increased.

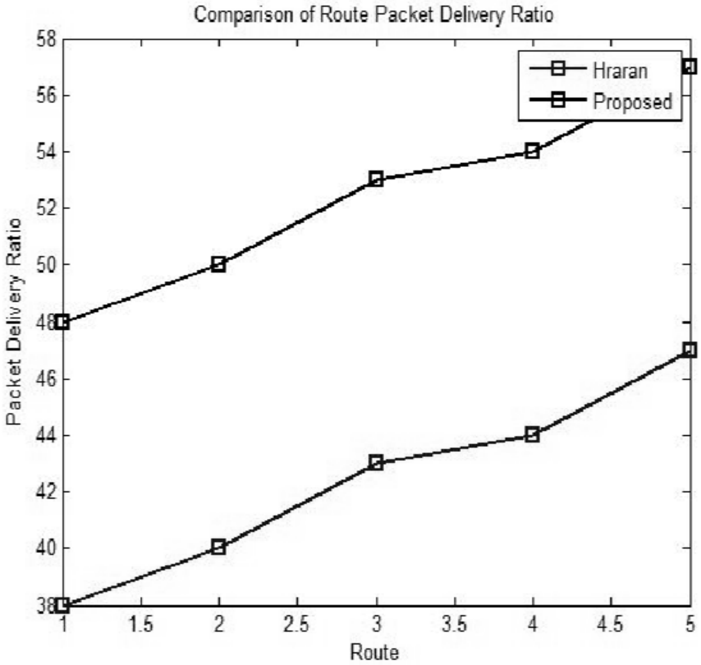

Figure 8.3 Performance Evaluation of Packet Delivery

References

[1] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester "An Overview of Mobile Adhoc Network: Application and Challenges".

[2] Swati Shukla and Sunil Kumar Singh, "A Survey on Mobile Adhoc Network Security and Vulnerabilities", International Journal of Engineering Research and Management Technology, volume 1, issue 2, 2014.

[3] Jyoti Goyat, Bhanu Priya, Swati, "Analysis and prevention of security issue in Manets", International Journal of Engineering Research and Management Technology, volume 4, issue 3, 2014.

[4] K. Sivakumar and Dr. G. Selvaraj, "Analysis of Warm hole attack in Manet and Avoidance using robust, secure routing method", International journal of advanced research in computer sciences and software engineering, volume 3, issue 1, 2013.

[5] P. Annadurai and S. Vijayalakshmi, "Highly reputed Authenticated Routing in MANET (HRARAN)", Wireless Personnel Communication DOI 10.1007/s11277-015-2403-5, Springer publication, 2015.

[6] Dr. S.S. Dhenakaran and A. Parvathavarthini, "An overview of routing protocol in Mobile Adhoc Network" published in International Journal of Advanced Research in Computer Science and Software Engineering, volume 3, issue 2, 2013.

[7] Mieso K. Denko, "Detection and Prevention of Denial of Services (DOS) Attacks in Mobile AdHoc Networks using Reputation-Based Incentive Scheme", Systemics, Cybernetics and Informatics, Volume 3- Number 4, 2005.

[8] Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Clay Shields, Elizabeth M. Belding-Royer, "Authenticated Routing for AdHoc Networks", 2015.