ISSN:2320-0790

An International Journal of Advanced Computer Technology

Safe Trust Alert Routing in MANET

Srikanth Meda[1] , Mabu Bhasha R[2], Asha Aruna Sheela.M[3]
[1]Associate Professor, [2,3]Assistant Professor
[1,2,3]Department of Computer Science& Engineering
[1,2]RVR & JC CE, Chowdavarm, Guntur, AP, India.
[3]Universal College of Engineering, Guntur, AP, India.

Abstract: The main characteristic of the ad-hoc network is dynamic topology. In this, nodes modifications its position usually and these nodes have to be compelled to be compelled to adapt for the topology amendment. Nodes can amendment position quite frequently that mean the standard of the network. For quick info transmission, we'd sort of a routing protocol that adapts to topology changes. For our convenience, we've projected a fast and secure protocol that's proactive and reactive in nature. Proactive nature used for adding the node into list, as a results of it taking a short while to line the selection relating to node. And reactive nature used for locating the path for providing fast transmission.

Keyword: MANET, security, Reactive routing, Proactive routing, hybrid technology.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires [1]. MANET could also be a network that's freelance network. There's MANET technology employed in completely different application, like military and civil applications. As a result of figureless property, network might even be stricken with attackers. To avoid security disadvantage there are many varied researchers fictional several security ways like coding ways. To reinforce security here we've got a bent to practice customary a pair of ways, one is RSA formula and SHA-1 formula. Throughout this project we've got a bent to prompt un-observability by providing protection for the asking and reply. Our proposed system main aim is to provide ultimate security in military application

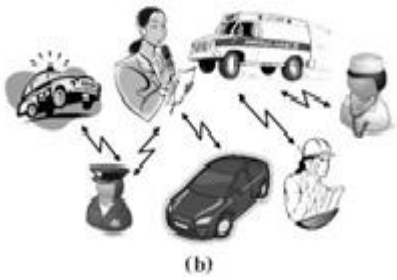

Fig.1 (a) MANET devices in ARMY, (b) MANET in civil application

II. RELATED WORK

In this paper [2], author projected a replacement classification of the defense lines taking into thought the resiliency-oriented approach which we tend to establish survivability properties. Survivability is made public as a result of the network ability to fulfill properly its functions even at intervals the presence of attacks. Survivability permits MANETs to fulfill their goals even in presence of attacks or intrusions. Ancient defense lines are not enough for giant networks, since them gift altogether totally different characteristics and properties that require new approaches.

[3]During this paper, author projected a replacement due to improve the accountable of message transmission is

presented. Inside the open cooperative Edouard MANET atmosphere, any node can maliciously or selfishly disrupt and communication of different nodes. Associate in Nursing SMT protocol provides the way to secure message transmission by dispersing the message among several ways with least redundancy. It provides secure communication even with accumulated vary of adversaries but cryptologic protection can't be effective against network layer attacks notably like Byzantine attacks.

[4]In this paper, author projected a replacement because of improve the irresponsibility of message transmission is given at intervals the open cooperative MANET atmosphere, any node can maliciously or selfishly disrupt and communication of different nodes. Associate degree SMT protocol provides a way to secure message transmission by dispersing the message among several strategies with least redundancy. It provides secure communication even with inflated vary of adversaries but the method and data overhead square measure high.

[5]In this paper author target the impact of quality models on the performance of painter routing protocols, so our a try of observations concerning dialogue the impact of movement quality speed of the nodes to causes the performance of ancient customary proactive routing protocol DSDV from ancient proactive family comparison with the two outstanding On-demand reactive routing protocols AODV and DSR from the reactive family for mobile ad-hoc networks. This paper has conferred a comparison performance of protocols for routing packets between wireless mobile hosts in associate ad-hoc network AODV, DSR associated DSDV with entirely totally different form of movement speed at constant pause time that used AN AODV and DSR from On-Demand protocols compared with DSDV from proactive table-driven routing protocols.

2.1. Existing system:

In previous methodology they're exploitation the various protocols in numerous network sections like pro active and another one is reactive mechanism.

2.2. Disadvantage:

In proactive methodology, once a current node is joined at intervals the network it delays it slow to converge throughout that time if we tend to want to transmit data to sink through that new node directly, it takes it slow to converge then it will transmit the data. One the other hand, routes will unendingly be offered for the asking. Reactive protocols get to line up routes on-demand only.

III. PROPOSED SYSTEM

Planned quick and secure protocol, routing is performed through proactive and reactive mechanism. In routers that use dynamic routing protocols, it is vital to possess quick convergence as a result of routers may build incorrect forwarding choices till the network has totally converged.

Therefore we tend to area unit progressing to propose the idea that is combination of each kind that's Proactive structure, reactive structure and secure mechanism.

3.1. Algorithm for Fast and secure

1. Initialize the nodes: there are the two type of node as follows
   a. Traffic monitor node
   b. Normal node
2. Traffic monitor generates the request in small interval
3. If new node detected
   a. Checks its activity (malicious or not)
      i. If malicious informing to all normal node
      ii. If not malicious
         1. Find the path through the new node by reactive
4. Else transfer the data by proactive

3.2. Checks its activity (malicious or not)

1. Traffic monitor send the request to new node and monitors the activity.
2. If the node is normal node then it forward idle message when it is in idle mode.
3. If not is malicious, then it won't provide any info simply drop the packets.

3.3. Proposed system description

The main characteristic of the ad-hoc network is dynamic topology. In this, nodes changes its position often and these nodes have to adapt for the network topology change. For quick data transmission, we need a routing protocol that adapts to topology changes. For our need of QoS, we have proposed a fast and secure protocol which is proactive and reactive in nature. And also we considered data

transmission with encryption decryption model, which is not considered in our reference research model.

3.4. MODULES

[1]. Network design
- Traffic manager
- Normal node

[2]. Monitoring the traffic

[3]. Route discovery process
- Create trust list
- Check trust list

3.4.1) Network design:

We are going to create a network with number of nodes which is a mobile ad-hoc network and we are going to create the network with the MANET specifications i.e., each node can communicate with any other node directly which are in coverage area of the node. In this network we are forming one leader node which is known as traffic manger which will controls the entire traffic of the network and remaining are normal nodes.

TRAFFIC MANAGER**:** This is the leader node which is going to take care of all other nodes by managing the traffic. It is going to check whether the reply's sending by the nodes are appropriate or not in regular intervals, whenever any new node enter in to the network it will check whether the node is hacking node or not by the reply it sending and inform to all other nodes about the new node for the secure data transmission.

NORMAL NODE: This is the general node which will make the data transmissions whenever it wants to communicate with any other node. It will send the data directly if the node is in its coverage area otherwise it will use intermediate nodes by checking whether that node is hacking node or not from the traffic manager.

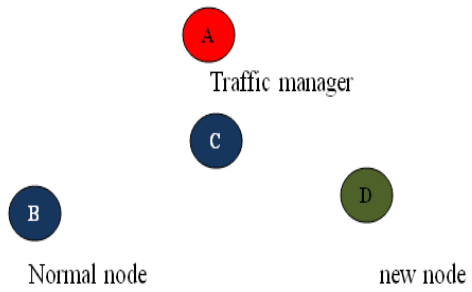

Fig.2 Network model

3.4.2) Monitoring the traffic:

Traffic monitoring will be handled by Traffic manager which is the leader node. It is going to take care of the entire network i.e., it monitors all the nodes and checks which are giving good response based on that it will allow other nodes to communicate with each other.

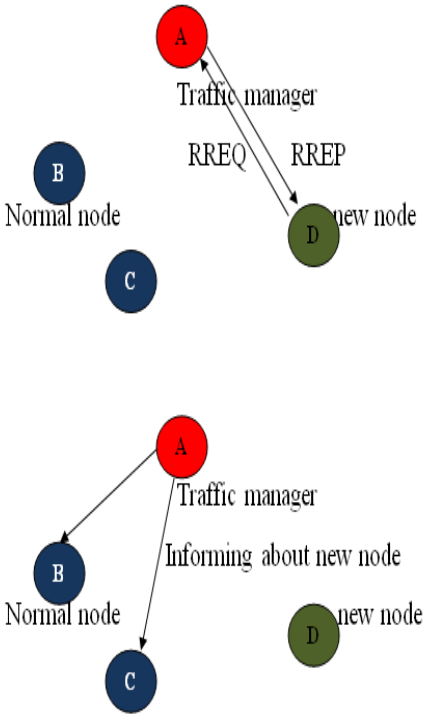

Fig.3. Key sharing

3.4.3) Route discovery process:

Whenever a node want to communicate with other node it have to find the route for forwarding the data. In this route if any new node is entered means there is a chance of that may be a hacking node. So, we have to avoid that hacking nodes for secure data transmission. For this nodes are maintaining a list known as true list, in this nodes are going to store about the other nodes for finding the secure route.

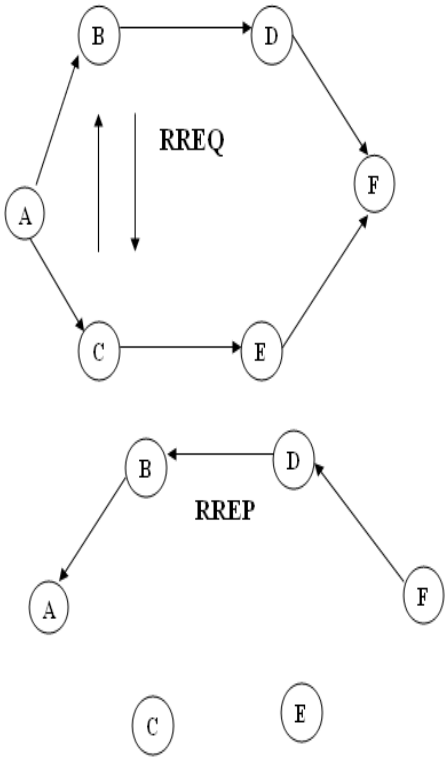

Fig.4. Route discovery process

CREATE TRUST LIST: Nodes are going to create a list known as true list, in this they are going to store about the node information's which given proper response to the traffic manager.

CHECK TRUST LIST: Whenever a node want to send the data it will send route request to other nodes. The node which received the route request packet will checks whether that node is present in the true list or not if presented means it will forward to other nodes and it will repeats until it reaches destination.

IV. PERFORMANCE ANALYSIS

In this paper, we presented our research model testing result, which is shown in Xgraph. Here we analyzed two main parameters. One is convergence time and another one is packet delivery ratio.

Packet delivery function:

Packet delivery function is the defined as number of packets successfully transmitted between source and destination.

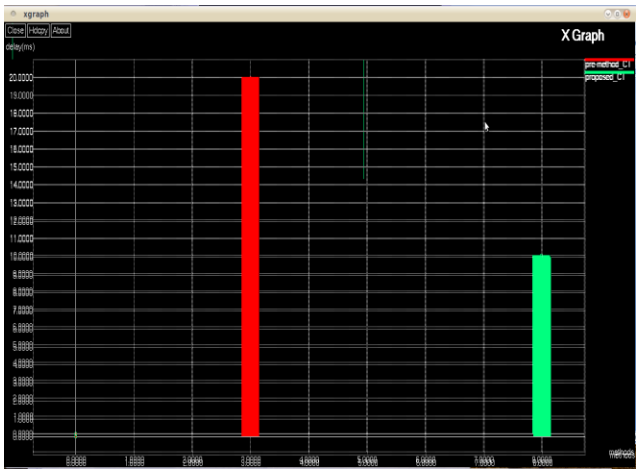

Fig.5. Delay time

Fig5. Shows that the delay of packet transmission, in that green colour bar graph indicates the proposed model and red colour indicates the existing model.

Fig6. Shows that the PDF, in that green colour bar graph indicates the proposed model and red colour indicates the existing model.

Fig6. Packet delivery ratio

V. CONCLUSION

The proposed fast and secure transmit protocol performs fast routing using proactive and reactive mechanism. It also gives security to the network with help of algorithm. The proposed work is simulated in ns2.

REFERENCES

[1].http://en.wikipedia.org/wiki/Mobile_ad_hoc_network

[2].B.Thanikaivel, B. Pranisa **"Fast and Secure data transmission in MANET"** 2012

[3].Michele Nogueira Lima , Aldri Luiz dos Santos ,Guy Pujolle **"A Survey of Survivability in Mobile Ad Hoc Networks**" , 2007.

[4].V. Anitha, Dr. J. Akilandeswari **"Secured Message Transmission in Mobile AD HOC Networks through Identification and Removal of Byzantine Failures**" , 2010

[5]. Jiejun Kong, Xiaoyan Hong,Mario Gerla. "**An Identity-free and On Demand Routing Scheme against Anonymity Threats in Mobile Ad-hoc Networks**" 2007

[6].Yasser Kamal Hassan, Mohamed Hashim Abd El-Aziz, and Ahmed Safwat Abd El-Radi. **"Performance Evaluation of Mobility Speed over MANET Routing Protocols**", 2010.

[7].Ajay Vikram Singh, Prof. M. Afshar Alam and Prof. Bani Singh. **"Mobility Based Proactive and Reactive Routing Algorithm in Mobile Ad hoc Networks (MANETs)**", 2011

[8]. **"Detecting Malicious Nodes For Secure Routing in MANETS Using Reputation Based Mechanism**" Santhosh Krishna B.V, Mrs.Vallikannu A.L.

[9].Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng. "**Anonymous Secure Routing in Mobile Ad-Hoc Networks",2004**

[10]. Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham Flaxman."**SybilGuard: Defending Against Sybil Attacks via Social Networks**" 2008