International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 9, September- 2014

Secure Trust Aware Routing in MANET

T. Subba Reddy
M.Tech in Vignan's lara institute of technology and science, vadlamudi Guntur, Andhra Pradesh, India.

G. Prashanti
Assistant Professor in vignan's lara institute of technology and science, vadlamudi, Guntur, Andhra Pradesh, India.

Abstract: **- The main characteristic of the ad-hoc network is dynamic topology. In this, nodes modifications its position typically and these nodes have to be compelled to adapt for the topology change.**

Nodes will change position quite oftentimes that mean the quality of the network. For fast information transmission, we'd like a routing protocol that adapts to topology changes. For our convenience, we've projected a quick and secure protocol that is proactive and reactive in nature.

Proactive nature used for adding the node into list, as a result of it taking a while to line the choice regarding node. And reactive nature used for locating the trail for providing quick transmission.

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

1) INTRODUCTION:

MANET may be a network that is freelance network. There is MANET technology used in different application, like military and civil applications. As a result of figureless property, network could also be laid low with attackers. To avoid security drawback there are several numerous researchers fictional many security strategies like encoding strategies. To enhance security here we have a tendency to mistreatment standard 2 strategies, one is RSA formula and Sha-1 formula. During this project we have a tendency 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

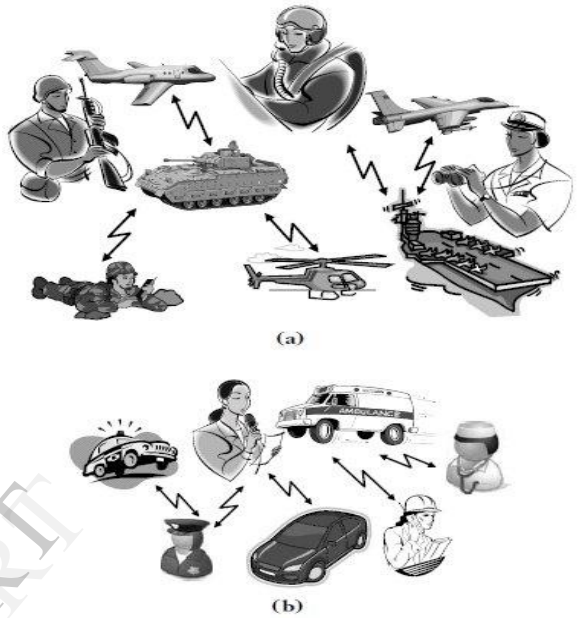

Fig.1a MANET devices in ARMY, b) MANET in civil application

2) RELATED WORK:

In this paper[2], author projected a replacement classification of the defense lines taking into consideration the resiliency-oriented approach and that we establish survivability properties. Survivability is outlined because the network ability to meet properly its functions even within the presence of attacks. Survivability allows MANETs to meet their goals even in presence of attacks or intrusions. Traditional defense lines aren't enough for big networks, since them gift totally different characteristics and properties that need new approaches.

[3]During this paper, author projected a replacement thanks to improve the responsible of message transmission is bestowed. Within the open cooperative MANET atmosphere, any node will maliciously or egotistically disrupt and communication of alternative nodes. AN SMT protocol provides how to secure message transmission by dispersing the message among many methods with least redundancy. It provides secure communication even with increased range of adversaries however cryptographic protection can not be effective against network layer attacks particularly like Byzantine attacks.

[4]In this paper, author projected a replacement thanks to improve the irresponsibleness of message transmission is bestowed. Within the open cooperative MANET atmosphere, any node will maliciously or

egotistically disrupt and communication of alternative nodes. AN SMT protocol provides how to secure message transmission by dispersing the message among many methods with least redundancy. It provides secure communication even with increased range of adversaries however the process and knowledge overhead are high.

[5]In this paper, author proposes a replacement routing approach that mixes the residual information measure, energy and quality of the network nodes. Metrics are designed to address high quality and poor residual energy resources so as to search out best methods that guarantee QoS constraints. A increasing routing metric theory has been wont to realize a metric that selects, throughout the routing method, routes that are a lot of stable (less mobile), that supply a most out-turn which live for an extended time.

The projected metric is predicted to expeditiously support period transmission traffic with totally different QoS needs however the projected approach is verified to OLSR protocol solely we've got to verify it to alternative ad-hoc routing protocols and conjointly to adapt our developed algorithms to Wireless sensing element Network routing protocols.

[6]In this paper author target the impact of quality models on the performance of painter routing protocols, thus our a pair of observations regarding dialogue the impact of movement quality speed of the nodes to causes the performance of ancient standard proactive routing protocol DSDV from traditional proactive family comparison with the 2 outstanding On-demand reactive routing protocols AODV and DSR from the reactive family for mobile ad-hoc networks. This paper has bestowed a comparison performance of protocols for routing packets between wireless mobile hosts in associate ad-hoc network AODV, DSR associated DSDV with totally different variety 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 brand new node is joined within the network it delays your time to converge throughout that point if we wish to transmit information to sink through that new node directly, it takes your time to converge then it'll transmit the info.

One the opposite hand, routes can continuously be offered for the asking. Reactive protocols get to line up routes on-demand solely.

3) 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.

3.4.1.A) 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.

3.4.1.B) 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.

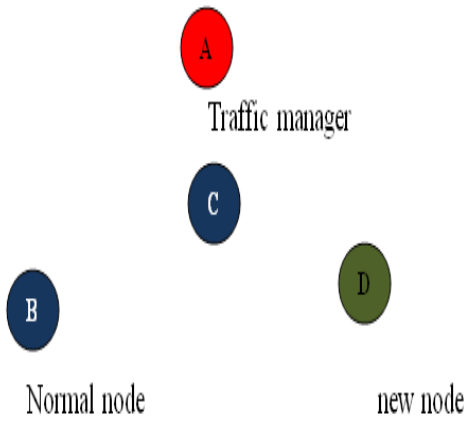

Fig.2 Network model

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.

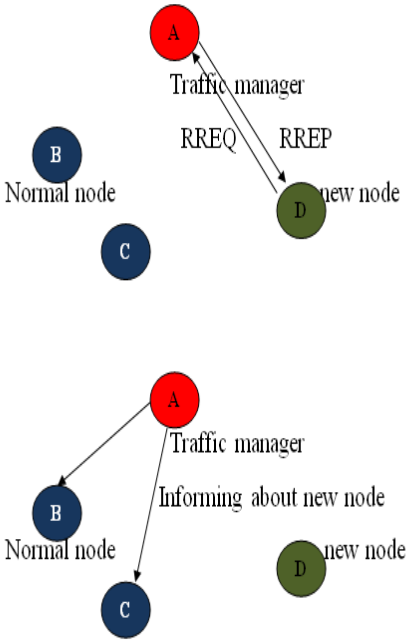

Fig.3. Key sharing

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.

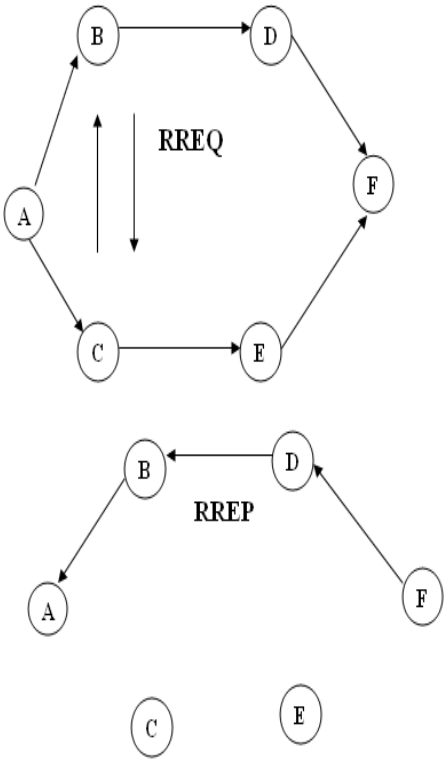

Fig.4. Route discovery process

3.4.3.A) 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.

3.4.3.B) 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.

4) 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.

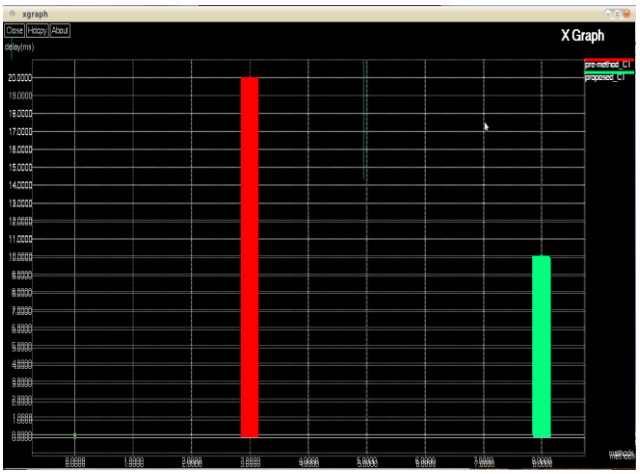

Fig.5. Delay time

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.

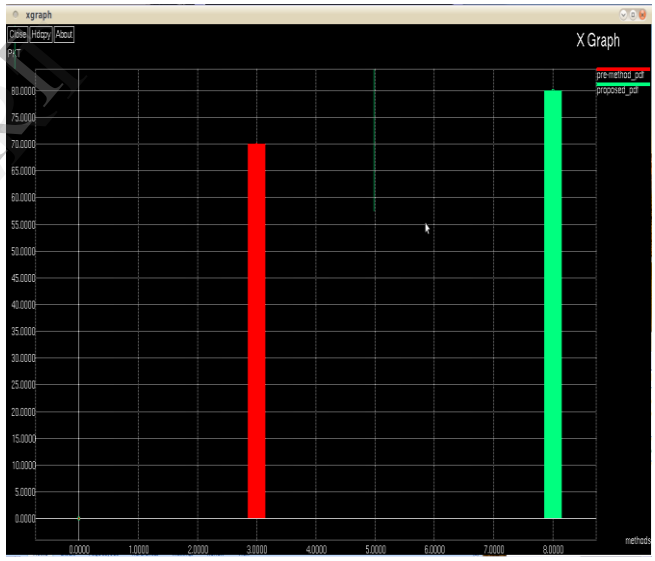

Fig6. Packet delivery ratio

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] B.Thanikaivel, B. Pranisa "Fast and Secure data transmission in MANET" 2012
[2] Michele Nogueira Lima , Aldri Luiz dos Santos ,Guy Pujolle "A Survey of Survivability in Mobile Ad Hoc Networks" , 2007
[3] V. Anitha, Dr. J. Akilandeswari "Secured Message Transmission in Mobile AD HOC Networks through Identification and Removal of Byzantine Failures" , 2010
[4] Jiejun Kong, Xiaoyan Hong,Mario Gerla. "An Identity-free and On Demand Routing Scheme against Anonymity Threats in Mobile Ad-hoc Networks" 2007
[5] kamal oudidi, abdelmajid hajami and mohammedel koutbi. "QoS Routing Using OLSR Protocol" , 2008
[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
[11] Charles E. Perkins, Elizabeth M. Royer. "Ad-hoc On-Demand Distance Vector Routing" 2002