Secure Data Transmission Model in MANET

Priyanka Takalkar
Department of Computer Engineering ,
Smt. Kashibai Navale College of Engineering ,
Off Sinhgad Road,Vadgaon (Bk),Pune- 411041,India.

Aaradhana Deshmukh
Department of Computer Engineering ,
Smt. Kashibai Navale College of Engineering ,
Off Sinhgad Road,Vadgaon(Bk),Pune- 411041, India.

ABSTRACT
MANET is mobile ad-hoc network. It is simply a collection of nodes where each node acts as independent router or host. Mobility is the main characteristics of MANET. Therefore routing protocol is required that adapts whenever topology changes. Secure data transmission is the main issue in MANET. The enhancement in the secure data transmission in MANET using both reactive and proactive routing protocols. Expecting the performance enhancement in Packet delivery ratio, Normalized routing load, End to end packet delay, Throughput, Energy Consumption, Residual Energy of secure data transmission in comparison with existing similar routing protocols for MANET.

General Terms
Routing Protocols, Security Algorithms.

Keywords
MANET, secure data transmission, fast and secure data transmission.

1. INTRODUCTION
MANET is mobile ad-hoc network. It is simply a collection of nodes where each node acts as independent router or host. MANET is a infrastructure less wireless network. Each node can change their position frequently. So mobility is the main characteristics of MANET. Therefore routing protocol is required that adapts whenever topology changes. Two routing protocols i.e. proactive routing protocol and reactive routing protocol are present. The reactive routing protocol does not take initiative for finding a route from source to destination unless until it is required. It discovers routes only on demand by flooding its query in the network. This type of protocols reduces control traffic overhead at the cost of increased latency in finding the route to a destination. On other hand proactive protocols maintains fresh list of destination and their routes by periodically distributing tables throughout the network. Each node has its cpu capacity, battery power and bandwidth. So routing protocol is used to minimize the traffic for packet transmission. If two nodes are not in the same range for transmission then data transmission between those nodes which do not in the same range is done through intermediate nodes. The main objective for routing protocol is to minimize its control traffic overhead. It should be capable of rapidly adapting to link failures. Therefore routing protocol should work in distributed manner & it should be self starting & self organizing. If any node wants to communicate with other node to which it has no route, the routing protocols will establish a route then node can communicate with each other. In open MANET environment practically any node can maliciously or selfishly disturb and deny communication of other nodes.

2. RELATED WORK
In paper [2] proposed an approach for new routing which is combines energy, residual bandwidth, and mobility of new node.
In paper [3] describes the comparisons of all routing protocols.
In paper [4] described challenged node technique. Challenged node technique is used for detection of correct path. Using intermediate nodes, it can forward the packet. In challenged node technique, any intermediate node new route reply verifies with next hop node challenged replay by its mitigating neighborhood nodes. In essence, new route replay verification algorithm describe about how efficiently it detects the malicious node at route discovery process [4].
Source driven self selection [5] is based on mobility for routing discovery through self selection. They enable the intermediate nodes for effective decision regarding participation in route discovery or not. It helps in reduction participation in route request rebroadcast in the network. In this source is responsible for specifying a required utility metric in each RREQ packet [5].
In paper [6], [7] using threshold value detect misbehavior of node using packet forwarding misbehavior algorithm. If node exceeds the threshold value then it is considered as a malicious node and if those below the threshold considered to be correctly behaving.
In paper [8] describes the critical node test. Using this algorithm, it can identify the critical node. The different stages are given in paper for identification for critical node. The node is under test is consider as node under test and the node performing test considered as testing node. First step is change the routing table of testing node and find the alternate path using ping command. When it will get routing table back update that routing table. If alternate link is present means link is not critical. When it will remove that link the network will not be disconnect.
Multipath OLSR (MP-OLSR) [9] is hybrid protocol which combines all the characteristics of reactive and proactive protocol. This algorithm is used for route discovery. It uses multipath dijkstra algorithm for route computation to calculate multipath based on the information obtained from the topology sensing. Multipath is used for parallel data transmission. It contains a flag value for each node. If the flag value is true then it will find valid route from multipath routing table. If it contains a false value then using multipath OLSR algorithm it can find multiple routes and save it into routing table.
Figure 1 shows SMT (Secure Message Transmission) [10] is well known protocol for data transmission. It is used to safeguard the data transmission against arbitrary malicious behavior of network nodes. SMT for secured data communication provides end to end secure and robust feedback mechanism.SMT uses an active path set comprising node disjoint paths, determined and deemed operational at the

source for communication with a specific destination's disperses each outgoing message, adding limited redundancy to the data and dividing the resultant information into N pieces, which are transmitted across routes one piece per route. Even if the message pieces are lost or corrupted, successful reception of M out of N pieces allows the reconstruction of messages at the destination. The ratio r=N/M is termed the redundancy factor and denote a dispersed message with redundancy r as an (M, N) message.

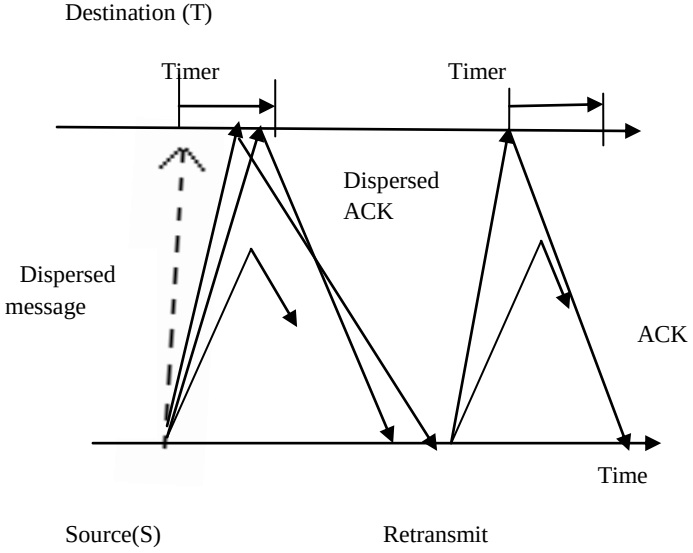

Fig 1: Simple SMT Protocol

3. PROPOSED SYSTEM

In this system proactive and reactive mechanism is used for routing purpose. In proactive protocol when new node is get added into the network it takes more time to converge at that time if want to send data to destination through that node then it will take more time for transmission of data. This problem is avoided by using reactive protocol instead. In this system when new node is added into the network first it will check whether it is malicious or not by using security algorithm. If node is not malicious it will find the path between source and destination using reactive mechanism as well as it will updates its routing table by using proactive mechanism. After path is established data is transferred from source to destination.

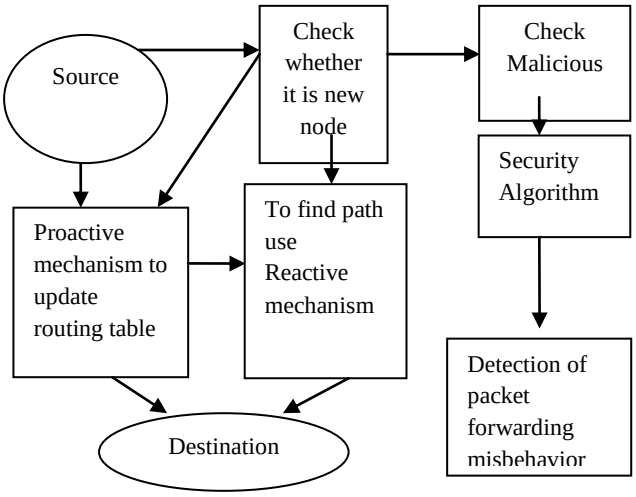

Fig 2: Fast and secure data transmission protocol

Table 1: Comparision of existing protocol with MP-OLSR

Characteristics	**OLSR**	**MP-OLSR**
Nature	Proactive	Hybrid
Path Detection	Unipath	Multipath
Delivery Ratio	Average	Better than OLSR
Delay	More	Shorter
Performance	Average	Better than OLSR
Loop Detection	No	Yes

3.1 Reactive Mechanism to Find Route

Whenever a path is established between source and destination by sending RREQ packet. RREQ packet contains source address, destination address, broadcast id, sequence number and hop count. After receiving RREQ packet by node it will check its routing table. If its routing table contain valid path then it will transmit acknowledge to sender node. This mechanism will take more delay and consume bandwidth that's why this mechanism is proposed. In this mechanism when node is formed and topology is formed. Then each node in the network will send message to other node i.e. it will check that other node is ready to accept data from other node. Then any node want to send data it will check message and then send data along with RREQ directly. Receiver node gives acknowledgement for new data transmission. This mechanism reduces the round trip time and also it will send data without delay. Suppose there are 4 nodes i.e. n1, n2, n3, n4 and topology is formed. Each node in the network will send accept_message to its neighbors node i.e. n1, n2, n3, n4 nodes will send accept_message to each other.

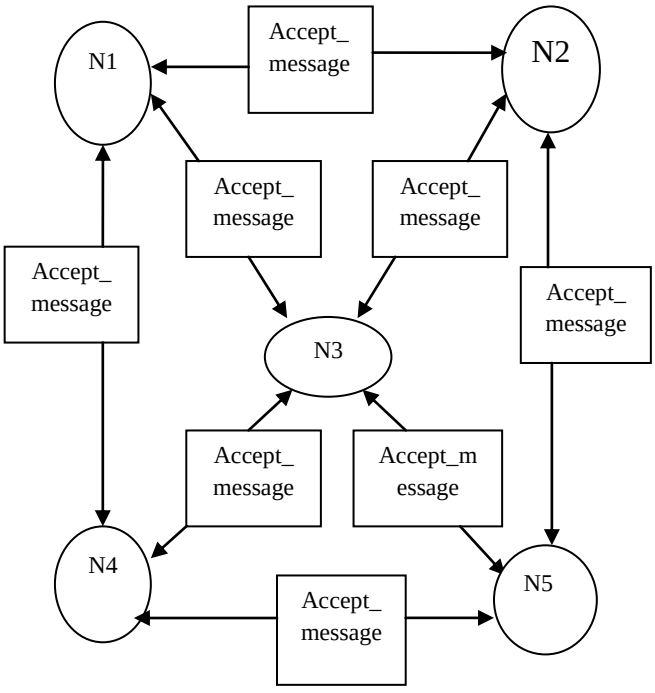

Fig 3: Sending Accept_message to neighbors

If any node is busy i.e. its transmission is going on with other nodes then that node will send busy_message to its all neighbor node and if node is idle then it will send

idle_message. Then any node wants to transmit data it will directly send data to idle node.

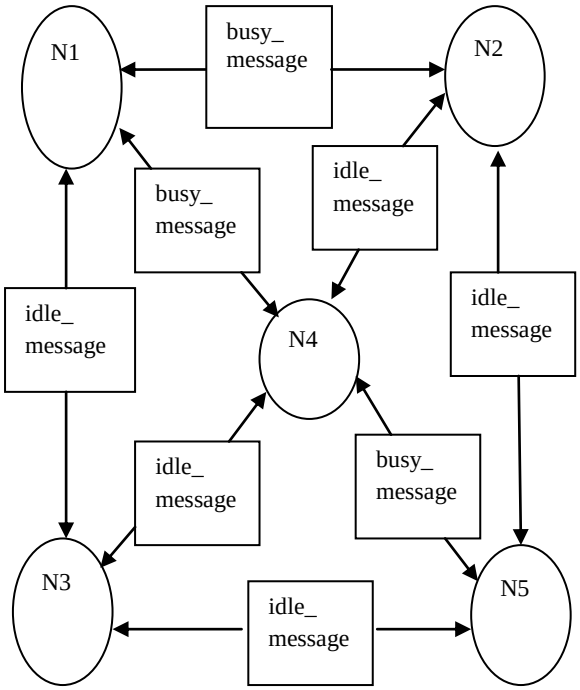

Fig 4: Specification of modes of the node

3.2 Detection of Packet Forwarding Misbehavior

Let V_j be a node such that $V_i \in V$ where $V_j \in V$= {V1, V2, V3 ...VN} is the set of all nodes in the network, N is the total number of nodes in the network, and j= 1, 2, 3 ... N.

Let Uj be the subset of nodes in the network which are neighbors of V_j, i.e. Uj is the neighborhood of vj. It follows that ($V_j \notin$ Uj) and also Uj $\subset$ V.

Let Δt be the period of time elapsed between two points in time to and t1 such that $\Delta t = t_1 - t_o$.

Let Tij be the number of packets that node vi has successfully sent to node vj for vj to forward to a further node vi $\in$ Uj , vj $\in$ Ui , i≠j and Tij (t_o) = 0.

Let Rij be the number of packets that node vi has successfully received from node vj that did not originate at vj; vi $\in$ Uj, vj $\in$ Ui , i≠j and Rij (t_o) = 0. If all nodes vj $\in$ V remain static for a period of time Δt during which no collisions occur in any of the transmissions over an ideal (noiseless) wireless channel, then for a node vj:

$$\sum_{\forall i/vi \in Uj} Rij(t1) = \sum_{\forall i/vi \in Uj} Tij(t1)$$

This equation states the fundamental premise of the flow conservation principle in an ideal static network, and is applied to packets rather than individual bytes. It states that if all neighbors of a node vj are queried for the amount of packet sent to v; to forward and the amount of packets forwarded by vj to them, the total amount of packets sent to and received from vj must be equal. However, a node may exhibit malicious behavior even if it is not purposefully doing so. For example, an overloaded node may temporarily lack the CPU cycles, buffer space or bandwidth to forward packets. In addition, some reactive routing protocols cause buffered packets to be dropped if they go through a path that is even temporarily.

$$(1 - \alpha_{threshold}) \sum_{\forall_i / v_i \in U_j} R_{ij}(t_1) \leq \sum_{\forall_i / v_i \in U_j} T_{ij}(t_1)$$

The $\alpha_{threshold}$ factor can take values between 0 and 1 and as we shall see plays an important role in the detection power in proposed algorithm, i.e. the capability of the algorithm to detect misbehaving nodes. The lower $\alpha_{threshold}$ is the more likely it is that algorithm detects any malicious behavior. However, it also means that the probability of a false detection increases. A false detection occurs when the result of a single evaluation of a node mistakenly determines that the node appears to be misbehaving.

3.3 Security Algorithm

Security is also main issue in the MANET, in open environment in the network any node behaves like trusted node and joins the network and hack the node information to avoid this problem there are 2 mechanisms are present.

3.3.1 Central Agent Monitoring Traffic in The Network

In this, central agent is present. Central agent maintains ids of each node. It gives unique id to each node for identification so that central agent will monitor traffic in the network. It also monitors the misbehavior of nodes so it will detect malicious node. If malicious node is present with duplicate id then it will stop network services and generate more traffic. If malicious node will found it will remove from the network.

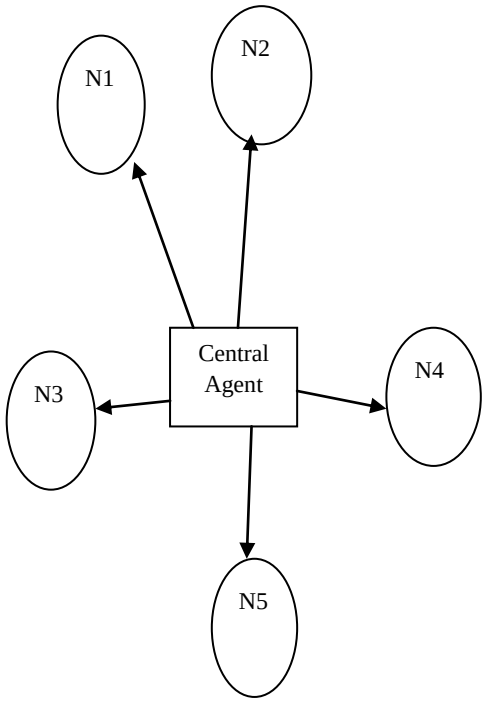

Fig 5: Central Agent Monitoring In The Network

3.3.2 Nodes With Background Process

In this each node has its own background process; background process will monitor the incoming traffic. Malicious node is detected by using process algorithm. This algorithm initiate's background process of each node if node is misbehaving then it will remove from network

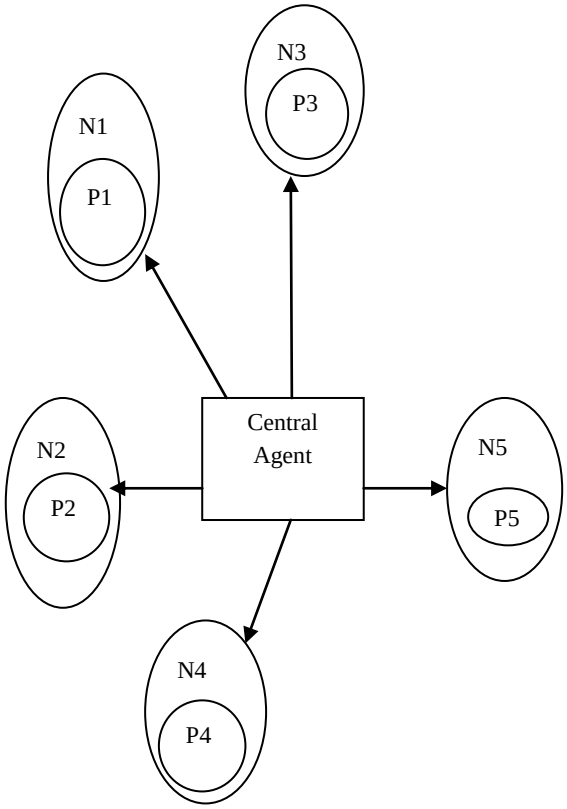

Fig 6: Nodes with Background Process

3.3.3 Algorithm

Step 1: node Xni creates RREQ= {D, hop_count', seq.no}
Xni sends RREQ to Xc
Xc sends RREQ to Xnexthop
Step 2: if Xnexthop= newnode
Check whether it is malicious
Processing Algorithm
Node Vj is misbehaving (Detection)
Else
Node Vj is not misbehaving (Non-detection)
Endif
Step 3: if newnode_malicious
Step 4: then find route using Fast Transmission algorithm

Step 5: if Xnexthop_newnode
Step6: Then perform proactive routing
If node ID matches the routing table
Then it will forward the packet
Step 7: If Xnexthop= new node
Then perform reactive routing (go to step 8)
Step 8: Send the accept message to neighboring node
If node is busy
Send busy_message
If node is idle
Send idle_message
Then send the request and data to the target.
If target receive the data
Then send reply and acknowledgement to sender.

3.4 CONCLUSION AND FUTURE SCOPE

The proposed algorithm performs fast and secure routing with the help of combination of proactive and reactive mechanism also provides security using process algorithm. In future it can be implemented in real time application.

4. REFERENCES

[1] B.Pranisa,B.Thanikaivel,"Fast and Secure Data Transmission in MANET", International Conference on Computer Communication and Informatics(ICCCI)Jan. 10− 12, 2012.

[2] Kamal oudidi, Abdelmajid hajami, Ohammedel koutbi,"Qos Routing Using Olsr Protoco, Latest Trends On Communications"

[3] Yasser Kamal Hassan1, Mohamed HashimAbd El-Aziz, and Ahmed SafwatAbd El-Radi, "Performance Evaluation Of Mobility Speed Over Manet Routing Protocols", International Journal of Network Security, Vol.11, No.3, PP.128(Nov. 2010).

[4] Ganesh Reddy Karri, P.M. Khilar,"RoutingMisbehavior Detection and Reaction In Manets", International Conference on Industrial andInformation Systems, ICIIS 2010.

[5] Ajay VikramSingh , Prof. M. Afshar Alam and Prof. Bani Singh,"Mobility Based Proactive And Reactive Routing Algorithm In Mobile Ad Hoc Networks"(Manet), International Journal of Computer Science and Information Technologies,Vol. 2 (4) , (2011).

[6] Oscar F. Gonzalez, Michael Howarth, GeorgePavlou," An Algorithm To Detect Packet ForwardingMisbehavior In Mobile Ad- Hoc Networks ",IEEE (2007).

[7] Manikandan T, Sathyasheela K B "Detection OfMalicious Nodes in MANET", IEEE(2010)

[8] Nitiket N Mhala and N K Choudhari,"An Approach Determining Conditions for Monitoring of Critical Nodes for MANET Intrusion Detection System",International Journal of Future Generation Communication and Networking Vol. 4, No.1, March 2011.

[9] Jiazi YI, Asmaa ADNANE, Sylvain DAVID,BenoËEÄst PARREIN, "Multipath OptimizedLink State Routing for Mobile ad hoc Networks",published in Ad Hoc Networks 9, 1 (2011).6

[10] Panagiotis Papadimitratos and Zygmunt J. H"Secure Data Transmission in Mobile Ad Hoc Networks" ACM Workshop on Wireless Security September 19, 2003.