Middle-East Journal of Scientific Research 15 (9): 1290-1294, 2013
ISSN 1990-9233
© IDOSI Publications, 2013
DOI: 10.5829/idosi.mejsr.2013.15.9.11514

Fast and Secure Data Transmission by Using Hybrid Protocols in Mobile Ad Hoc Network

Ipsita Panda and Sidharth Dash

Department of CSE, S.I.E.T., Dhenkanal, Odisha, India

Abstract: Mobile ad hoc network (MANET) is a self organized and self configurable network where the mobile nodes move arbitrarily. For faster data transmission, we need a routing protocol that adapts to topology changes. Secure data transmission is the main issue in MANET. The enhancement in the secure data transmission in MANET uses both reactive and proactive routing protocols. In proactive protocol, when a new node is added in the network it takes some time to converge during that time if we want to send data to destination through that new node immediately, it takes some time to converge and then it will transmit the data. To avoid this problem we are going to use reactive protocol instead of proactive. Proactive protocol structure, reduce the packet size and contains only limited field. By this, the total bit size gets reduced. We propose this mechanism to avoid waiting time and to transmit data as early as possible. Also we propose a security mechanism for detecting malicious node by using central agent and process algorithm.

Key words: Algorithm · MANET · Central agent · Proactive · Reactive · Routing Protocols · Secure data transmission

INTRODUCTION

Mobile ad hoc network (MANET) is a self organized and self configurable network where the mobile nodes move arbitrarily. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. 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. Each node should maintain some CPU capacity, storage capacity, battery power and bandwidth. So that routing protocol try to minimize the traffic in packet transmission [1]. But normal routing protocol in fixed network does not show the same performance in MANET. In this, if the two mobile nodes are not in the same transmission range, message communication between the nodes can be done through the intermediate node. This node can also change their position, so that network should adapt to the topology change. Therefore, nodes in such a network expected to cooperatively to establish routes instantly. Routing protocols for MANETs are divided into pro-active, reactive, hybrid types.

Proactive routing protocols attempt to maintain consistent, up-to-date routing information between every pair of nodes in the network by propagating, proactively, route updates at fixed intervals. Representative proactive protocols include: Destination-Sequenced Distance-Vector (DSDV) routing, Clustered Gateway Switch Routing (CGSR), Wireless Routing Protocol (WRP) and Optimized Link State Routing (OLSR). A different approach from table-driven routing is reactive or on-demand routing. Reactive protocols, unlike table-driven ones, establish a route to a destination when there is a demand for it, usually initiated by the source node through discovery process within the network [2]. Representative reactive routing protocols include: Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) routing, Temporally Ordered Routing Algorithm (TORA) and Associativity Based Routing (ABR). Purely proactive or purely reactive protocols perform well in a limited region of network setting. However, the diverse applications of ad hoc networks across a wide range of operational conditions and network configuration pose a challenge for a single protocol to operate efficiently. For example, reactive

Corresponding Author: Ipsita Panda, Department of CSE, S.I.E.T., Dhenkanal, Odisha, India.

routing protocols are well suited for networks where the call-to-mobility ratio is relatively low. Proactive routing protocols, on the other hand, are well suited for networks where this ratio is relatively high. Researchers advocate that the issue of efficient operation over a wide range of conditions can be addressed by a hybrid routing approach, where the proactive and the reactive behaviour is mixed in the amounts that best match these operational conditions. Representative hybrid routing protocols include: Zone Routing Protocol (ZRP) and Zone-based Hierarchal Link state routing protocol (ZHLS) [3].

Mechanism to Find Route: Ajay VikramSingh, Prof. M. Afshar Alam and Prof. Bani Singh presents a Source driven self selection (SDSS) algorithm based on mobility for the route discovery process in [4]. In this algorithm, the source node is mainly responsible which specifies the required utility metric in each RREQ packet. The source node begins by calculating the mobility utility function which selects a value for maximum allowable velocity at each intermediate node during a route discovery phase. It mainly increases the stability of the route over blind flooding and it also reduces the broadcast storm problem due to fewer rebroadcasting modes during route discovery. [5] Describes about Detecting packet forwarding misbehaviour algorithm by considering the threshold value of the node, it detects the misbehaviour of the nodes. It mainly uses the principle of flow conservation in a network. Any node dropping packets in excess of this threshold is deemed a misbehaving node while those below the threshold are considered to be correctly behaving. Challenged node technique mainly detects the correct path for transferring in the routing protocol. In this, Intermediate nodes are mainly responsible for packet forwarding. Any intermediate node new route reply verifies with next hop node challenge replay by its overheard neighbouring nodes. ADCLI algorithm described in it detects malicious nodes in a set of nodes such that each pair of nodes in the set is within the radio range of each other. At the monitor node, the suspected nodes that receive at least a minimum number of votes are finally detected as malicious nodes. Thus instead of giving the sole authority to a single node to decide about the maliciousness of another node, the algorithm works in such a way that a group of nodes together make this decision Critical node test described in [6].In this, identification of critical nodes can be performed by critical node test. There are different stages in this evaluation of critical nodes. First it changes the routing table of the testing node and attempts to find an alternate path using ping command. When the results of the ping are returned, the network routing table is restored during this final step to its initial configuration.

Zone Routing Protocol (ZRP): It is possible to exploit the good features of both reactive and proactive protocols and the Zone routing protocol does that. The proactive part of the protocol is restricted to a small neighbourhood of a node and the reactive part is used for routing across the network. The Zone Routing Protocol (ZRP) is a hybrid routing protocol, where the network is divided into routing zones according to the distances between nodes and the routing zone defines a range (in hops) that each node is required to maintain network connectivity proactively. This reduces latency in route discovery and reduces the number of control messages as well.

In Fig. 1 each node S in the network has a routing zone. This is the proactive zone for S as S collects information about its routing zone in the manner of the DSDV protocol. If the radius of the routing zone is k, each node in the zone can be reached within k hops from S. The minimum distance of a peripheral node from S is k (the radius). All nodes except L are in the routing zone of S with radius 2. But since hierarchical routing is used, the path to a destination may be suboptimal and since each node has higher level topological information, memory requirement is greater [3].

Zone-Based Hierarchical Link State (ZHLS) Routing Protocol: In Zone-based Hierarchical Link State Routing Protocol (ZHLS) the network is divided into non-overlapping zones. Unlike other hierarchical protocols, there is no zone-head. ZHLS defines two levels of topologies - node level and zone level. A node level topology tells how nodes of a zone are connected to each other physically. A virtual link between two zones exists if at least one node of a zone is physically connected to some node of the other zone. Zone level topology tells how zones are connected together. The ZHLS uses proactive routing inside the zone and reactive routing is used outside the zone. ZHLS requires GPS or similar service to identify itself with a certain zone. Zones: coverage of the single node, application scenario, mobility of nodes, network size [7].

There are two types of Link State Packets (LSP) as well - node LSP and zone LSP. A node LSP of a node contains its neighbour node information and is propagated with the zone where as a zone LSP contains the zone information and is propagated globally. So each node has full node connectivity knowledge about the

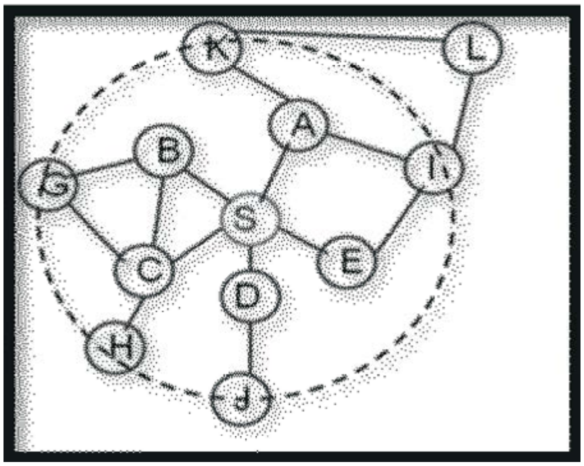
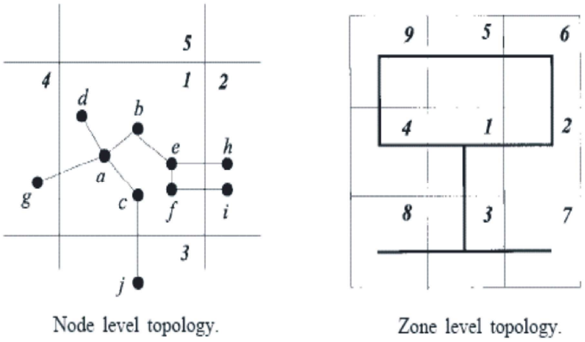


Fig. 1: Zone routing protocol



Node level topology.

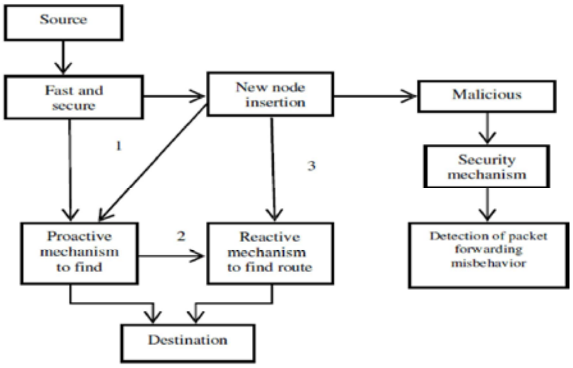
Zone level topology.

Fig. 2: Node level and Zone level topology

nodes in its zone and only zone connectivity information about other zones in the network. So given the zone id and the node id of a destination, the packet is routed based on the zone id till it reaches the correct zone. Then in that zone, it is routed based on node id. A <zone id, node id@gt; of the destination is sufficient for routing so it is adaptable to changing topologies.

The Repair of Broken Links Is as Follows: source is noticed about the link failures; if there are multiple gateways with the required zone, packet if forwarded via one of those; if no multiple gateways, packets are forwarded to other zones and then to the required zone.

Proposed Work: In this proposed fast and secure protocol, routing is performed through proactive and reactive mechanism. In routers that use dynamic routing protocols, it is important to have fast convergence because routers could make incorrect forwarding decisions until the network has fully converged [7]. Fig. 3 shows the architecture model of fast and secure transmit protocol.

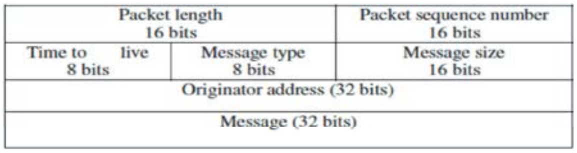

Source
Fast and secure
New node insertion
Malicious
1
3
Security mechanism
Proactive mechanism to find
2
Reactive mechanism to find route
Detection of packet forwarding misbehavior
Destination

1. Take time to convergence to find the route
2. Use reactive mechanism
3. If not malicious

Fig. 3: Architecture of fast and secure transmit protocol

Proactive Routing Protocol Structure: The proposed protocol structure which represented here is similar to OLSR protocol with reduced packet size. It contains packet length which represents the length of entire packet in bytes. Packet sequence number 16 bits which gets incremented when a new message is transmitted by this host. Message sequence number also inserted into this packet sequence number field itself. Time to live field which maintains the maximum number of hops this message can be forwarded. This field contains only 8 bits. Message type, 8 bits, an integer represents the type of message. In this, message type of 0-127 is reserved for specific protocol and 128-255 is considered for private. Message size field 16 bits which maintains the size of the message including header. Originator address field 32 bits which specifies the main address of the originator of this message. In this proposed work, the packet structure contains a total of 128 bits.

Reactive Mechanism to Find Route: Path discovery is done by sending RREQ and RREP packets. RREQ contains source and destination address, sequence number, broadcast id and hop count. Once the node receives the RREQ, it checks its routing table. If it contains a valid route, it sends RREP to source node. RREP packet contains source and destination address, sequence number hop count and life time of the packet. After finding its path, sender sends the data in next transmission. Then the receiver transmits the acknowledgement in next transmission in normal mode data transfer mechanism. It cause more delay in packet transmission and consumes more bandwidth. In the proposed algorithm, when a node is created and topology



Packet length 16 bits		Packet sequence number 16 bits
Time to live 8 bits	Message type 8 bits	Message size 16 bits
Originator address (32 bits)		
Message (32 bits)		

Fig. 4: Proactive routing protocol structure

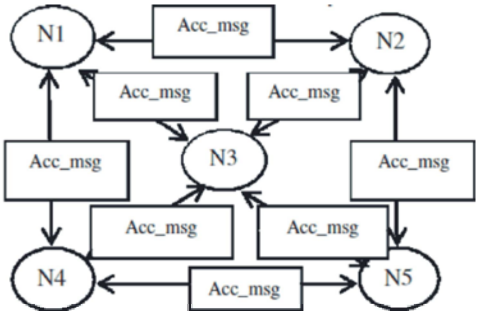


Fig. 5: Sending Acc_ msg to neighbours

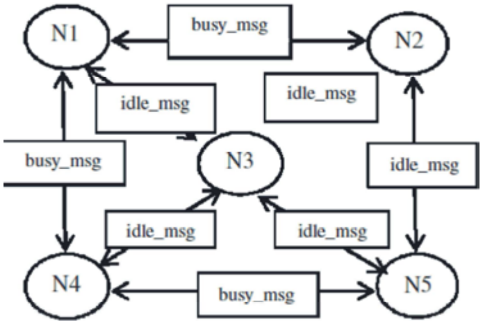


Fig. 6: Specification of modes of the node

is formed, each node will send a message that it can accept the data from the other node. Then any node want to send data will check that message and then send the data along with its route request directly. Receiver sends the acknowledgement for the data in next transmission. By this, we can reduce the round trip time in transmission and we can transmit the data without any delay.

In Fig. 6, for detecting its route, all the nodes in the topology send accept_ message to all its neighbouring nodes. If any node is already performing transmission with other nodes, it sends busy_message to its neighbour node and if the node is idle, then it sends idle_ message to its neighbours. Then it sends the data directly with its route request to the idle node.

When the node detects idle_ message from its neighbours, then it can send the data directly along with its route request to the receiver node in a single transmission and the receiver sends the acknowledgement in the next transmission. After finding its path in initial transmission, sender sends the packet directly to receiver without sending any route request by its previous route.

Security Mechanism: In MANET, each node will communicate with other node using its node information. In this network, the malicious node can join in the network by hacking the node information and can act like a trusted node. Then the malicious node will perform dangerous activities in network like DoS, hacking of packets, etc. To avoid this problem we use the following technique:

- Central Agent Monitoring traffic in Network
- Background process in each node for monitoring incoming traffic.

Central Agent Monitoring Traffic in Network: In this, central agent will maintain the entire node Ids in the network. It also allocates unique id to each node in the network for its identification to monitor the traffic in the network. This central agent monitors the nodes misbehaviour to detect its malicious activity. When a new node is coming with duplicate id or generating more traffic to stop the network services then, it will be detected by that central agent and it will remove it from the network.

Nodes with Background Process: In this mechanism, processing algorithm is used to detect malicious node by initiating the background process at the each node, this background process will monitor the incoming traffic. The process algorithm is initiated by Central agent and then each node will start the process for monitoring the incoming traffic and it will run in the background of the each node.

Algorithm:

```
Step 1: Node X creates RREQ = {D, hop_count, Seq_no}

X sends RREQ to Xc
Xc sends RREQ to Y

Step 2: If Y = 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 is malicious

Then find route using Fast Transmission algorithm.
```

Step 4: If Y is newnode
Then perform proactive routing

Step 5: If node ID matches the routing table
Then it will forward the packet

Step 6: If Y = new node
Then perform reactive routing i.e. go to step 8.

Step 7: Send the accept message to neighbouring 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.

In this algorithm, node X creates a challenged message and sends the request message to challenged node Xc. Then Xc forward that request to Y. If the next hop node is a new node, by the detection of packet forwarding misbehaviour mechanism, it detects that whether it is malicious or not. This mechanism mainly based on the threshold value of the nodes. If it is not malicious, then routing is performed through a reactive mechanism. It performs routing through fast transmission algorithm. In this, all the nodes in the topology first perform communication with its neighbours through accept_message. If any node is already performing transmission with other nodes, it sends busy_ message to its neighbour node and if the node is idle, then it sends idle_message to its neighbours. Then it sends the data directly with its route request to the idle node which performs fast transmission.

CONCLUSION

For secure data transmission in MANET we use both reactive and proactive routing protocols a hybrid protocol where the proactive and the reactive behaviour is mixed. The proposed algorithm performs fast 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 applications.

REFERENCES

1. Thanikaivel, B. and B. Pranisa, 2012. Fast and Secure Data Transmission in MANET, 2012. International Conference on Computer Communication and Informatics, ICCCI -2012, Coimbatore, INDIA.
2. Mobile computing book by Vishnu Sharma and S.P.S. Chauhan. Katson Books.
3. Ipsita P., 2012. and QoS Parameters Analysis to Improve QoS in MANETs Routing Protocol, International Journal of Advanced Research in Computer Science and Electronics Engineering, IJARCSEE, 1(7): 43-49.
4. VikramSingh, A., 2011. Prof. M. Afshar Alam and Prof. Bani Singh Mobility Based Proactive And Reactive Routing Algorithm In Mobile Ad Hoc Networks Manets, International Journal of Computer Science and Information Technologies, 2(4).
5. Oscar F. Gonzalez, Michael Howarth and George Pavlou, 2007. An Algorithm To Detect Packet Forwarding Misbehavior In Mobile Ad- Hoc Networks, IEEE.
6. Takalkar, Priyanka and Aradhana Deshmukh, 2013. Secure Data Transmission Model in MANET. International Journal of Computer Applications, 0975-8887, 67(24).
7. Misra, Padmini Routing Protocols for Ad Hoc Mobile Wireless Networks. Available at http:// www.cse.wustl.edu/~jain/cis78899/ftp/adhoc_routing/#ZHLS.