International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 32423-32431

http://www.ripublication.com

Minimizing Routing Overhead in Topology Concealing Multipath Routing Protocol (TOCOP)

B.SalimBasha[1], M.R.Pavan Kumar[2]

The department of Computer Science and Engineering
Sree vidyanikethan engineering college
Sree Sainath Nagar, A. Rangampet, Tirupati, Andhra Pradesh 517102
India
(Email :{ saleembasha513,sivapavan.mr}@gmail.com)

ABSTRACT

Mobile Ad-Hoc Networks (MANETs) do not need any fixed or supporting infrastructure, in fact offers quick network deployment. The characteristics ofMANETs such as: dynamictopology, node mobility, provides freedom and self-organizing capability that make MANETs completely differentfrom other network. Due to the nature ofMANETs, designing anddevelopment of routing protocols is a challenging task. Multipath Routing Protocols in MANETs has the topology issue with which attackers can make use of topology information and tries to invade the network. So, Topology hiding is a solution to avoid attacks (such as black hole attack, warmhole attack, rushing attack and Sybil attack) in MANETs. But, it causes Routing Overhead because of detecting the unreliable routes before transmitting the packets.In the present it is proposed to designed new technique called Position based Opportunistic Protocol (POR) which inturn reduces the routing overhead and better data transmission by hiding the topology.

Keywords: Multipath Routing, Global Positing System, Topology Hiding, MANET

1. INTRODUCTION

Mobile Ad-Hoc Network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless links. The topology of the MANET may change uncertainly and quickly due to high mobility of theindependent mobile nodes, and because of the network decentralization, each node in the MANET will act as a routerto discover the topology and maintain the network connectivity.In MANET's multipath routing protocols plays a major role. However the existing secure multipath routing protocols have the topology-exposure problem which leads to launch various

attacks like black hole attack [2], wormhole attack [3], rushing attack[4] and sybil attack [5].

To overcome this topology-exposure problem Topology hiding multipath routing (TOHIP) protocol is designed which hides the topology by removing link connectivity information in route messages, exclude the unreliable routes and also find node-disjoint routes. But in TOHIP more routing overhead than secure routing protocols because of detecting the unreliable routes before transmitting the packets.

To reduce the routing overhead, this paper uses the location information by hiding the topology. Which increases the packet delivery ratio and control the Route Request (RREQ) packets.

An integrated Internet and mobile ad hoc network can be subject to many types of attacks

- **Black hole Attack:** Route discovery process in AODV is vulnerable to the black hole attack. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough route, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.
- **Rushing Attack:** Rushing attacks are mainly against the on-demand routing protocols. These types of attacks subvert the route discovery process. On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. When compromised node receives a route request packet from the source node, it floods the packet quickly throughout the network before other nodes, which also receive the same route request packet can react.
- **Wormhole attack:** A typical wormhole attack is launched as follows. Two collaborating attackers first select two central positions in the network to reside such that they are located on many potential routes.Then they build a private tunnel between them and advertise a fake hop count which is smaller than the real hop count between them. The action disrupts the route discovery mechanisms which only use hop count as routing metric since the private channel between the two attackers will always be selected as part of routes considering the smaller hop account.
- **Sybil attack:** A Sybil attacker disrupts route discovery by impersonating multiple legal nodes. To launch this attack, the attacker first obtains the identity of a set of legal nodes and then impersonates some or all of them to participate in multiple route discoveries.

2. TOPOLOGY-EXPOSURE PROBLEM

Consider an example MANET, whose topology is shown in Fig. S is the source node and D is the destination node. There are two routes from node S to node D, which are

S ->C ->F -> D and S ->A ->D, in some multipath routing protocols. Based on the two routes, node D can conclude that S is connected to A and C, C is connected to F, A and F are connected to D. Clearly, the two routes enable node D to obtain the whole network topology. We call this problem as topology-exposure.

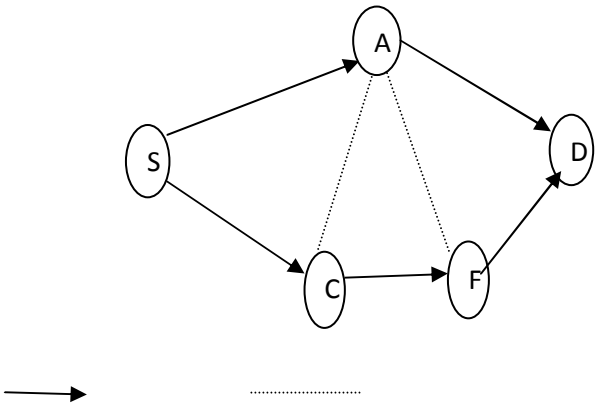

Fig 1: Topology-exposure Problem

Hiding the network topology can avert many regular attacks. Topology Hiding can be defined as follows:

Let N be the set of all nodes in a topology. Let dist(n_i,n_j) be the hop count between a node ni and a node n_j. A routing protocol is topology-hiding only if:

For any $n_i \in$ N and $n_j \in$ N, if dist(n_i, n_j) >2, then node $n_i$cannot know which nodes are connected to node n_j.

3. OVERVIEW AND DATA STRUCTURE

TOCOP has 3 phases: Route Request Phase, Route Reply Phase and Route Probe Phase.

- Route Request Phase: A route request messages is transmitted from the source node (S) to the destination node (D) via broadcasting. To maintain network connectivity, upon receiving a route request message, every intermediate node creates a reverse route, and rebroadcasts the message if it has never received this message before.
- Route Reply Phase: A route reply message is transmitted from the destination node to the source node via broadcasting. Upon receiving such a message, an intermediate node selects the neighbor closest to the source node as the previous hop on the route. It then advertises this selection to all its other neighbors, to ensure no node is selected on multiple routes.
- Route Probe Phase: In this phase the unreliableroutes can be detected and eliminated.

In TOCOP every node have two tables they are Sequence Number Table (SNT) and Routing Table (RT).SNTprevents nodes from rebroadcasting unnecessary route request messages. Eachentry in *SNT* contains the source node which initially requestsroute discovery and the sequence number that the source nodeuses in this route discovery attempt.Each entry in *RT* includes the destination node, the node through which to reach the destination, the location information of destination and the number ofhops to the destination node.

4. RELATED WORKS

Large portions of the current multipath directing conventions have been gotten from Dynamic Source Routing (DSR) [6], Ad hoc On-demand Distance Vector (AODV) [7] and there is another kind of routing protocols, called the geographic routing.

- **Dynamic Source Routing (DSR):**

DSR is an On-demand convention intended to confine the "bandwidth" devoured by control parcels in impromptu remote systems by wiping out the occasional table-driven messages needed in table-driven methodology. Course disclosure contains both course demand and course answer messages.

In course disclosure stage, when a hub wishes to communicate something specific, it first telecasts a course ask for bundle to its neighbors. Each hub inside a show extent adds their hub id to the course ask for parcel and rebroadcasts. Every hub keeps up a course store, it first checks its reserve for course that matches the asked for destination.

Keeping up course hold in every hub diminishes the overhead made by course disclosure stage. In the event that a hub is found in course disclosure store, the hub will give back a course answer message to the source hub as opposed to sending the course demand message further.

The course answer bundle is sent to the source which contains the complete course from source to destination. In the course upkeep stage, course lapse and affirmations bundles are utilized.

- **Ad hoc On-demand Distance Vector (AODV):**

AODV aims to reduce the number of broadcast messages forwarded throughout the network by discovering routes on-demand instead of keeping a complete up-to-date route information. A source node looking to send a data packet to a destination node checks its “route table” to see if it has a valid route to the destination node. If a route exits, it simply forwards the packet to the next hop along the way to the destination. If there is no route in the table, the source node begins a route discovery process.

Every node maintains two separate counters sequence number and broadcast-id. Broadcast-id is incremented whenever the source issues a new RREQ. Route maintenance is required if either the destination or intermediate node moves away and it is performed by sending a “link failure notification” message to each of its upstream neighbors to ensure the deletion of that particular part of the route.

5. PROTOCOL DESIGN

In MANETs existing multipath routing protocols which hide the topology have the routing overhead problem in route discovery mechanism. This routing overhead created during the route discovery phase leads to compromise in QoS (Quality of Service). So, reducing the routing overhead helps for better data traffic.

The main objectives of TOCOP is as follows:

- Hiding the topology to avoid the attacks like black hole attack, wormhole attack, rushing attack and Sybil attack.
- Reducing the routing overhead in route discovery.
- Minimizing end-to-end delay which reflects the average transmission delay from source to destination.

Before we present the Route Request Phase with neighbor authentication [9], we introduce the following notations: S and D represents the source node and the destination node, respectively. A and B represents two intermediate nodes, and N represents a neighbor of the destination, indicates that the message is sent via broadcasting. Assume that every node has a pair of public key PK and private key SK, and it keeps its authentication information IMSG:

- IMSG= [t, ID, SK (t, ID), PK]
- S*A: RREQ = [[S, seq, D, hopCt] SK_S , $IMSG_S$]
- A*B: RREQ = [[S, seq, D, hopCt] SK_A , $IMSG_A$]
- B*D: RREQ = [[S, seq, D, hopCt] SK_B , $IMSG_B$]

After authenticating the nodes Route Request Phase it is started by flooding the RREQ message towards the destination location. Here the Location information used in this protocol may be provided by the Global Positioning System (GPS) [10]. By using GPS we can find the location of mobile node. But in reality the location information provided by GPS includes some amount of error, which is the difference between GPS-calculated coordinates and the real coordinates. Here we assume that each node knows its current location precisely.

Route Request Phase:

The Route Request (RREQ) message contains the following parameters:

- S: Source ID
- D: Destination ID
- seq: sequence number generated by S
- hopCt: hop count
- LOC_S: source location information in two-dimensional plane (Xs, Ys)
- LOC_D: destination location information in two-dimensional plane (Xd, Yd)
- t_0, t_1: timer set by S

At source node S:
Before broadcasting Route Request (RREQ) message the Source node S first checks its Routing Table (RT)to find route to the destination. If not S broadcasts the RREQ < S, D, seq,LOC_D, t_0, t_1> to its neighbors, else simply sends data through that route.

At intermediate nodes y:
Every intermediate node receiving route request message checks <S, seq > in SNT to determine whether this is the first RREQ copy for this route discovery attempt. If yes, they record <S, seq > in SNT, increases hopCt by 1, and then rebroadcast the RREQ message. Instead, they process every received copy and record the reverse route to the source via the sender of this copy.

Algorithm 1: Protocol at node y
A node y receives an RREQ packet from a node x
If (y is not the destination)
If (y is afirst-hop)
y inserts its ID and its geographical location in a firsthoplist
else if (in the Routing Table ofy does not exist a path tothe destination)
if (the same RREQ packet with the same first-hophas already receivedfrom y)
y drops the packet
else
/*y has received the same packet with a different first-hop or y has not yet received the RREQpacket*/
1) y records the ID's neighbour from which it received the RREQ packet
2) y broadcasts the RREQ
else // y is the destination
if (a path already exists)
1) y computes the distance d1 between the first-hop nodes of the two paths (the first path and the path we will build)
2) y computes the distance d2 between the first-hop nodes of the two paths (the first path and the path we will build)
if (d1 >= TR and d2 >= TR)// TR is the transmission range
y sends an RREP packet immediately
else
y sets the WAITING state for x

At destination node D:
When the destination node receives the first RREQ copy,it initiates a timer T_D to collect the following copies.Destination D only accepts the copies that arrive before T_D times out. It processes them in the same way as the intermediate nodes do, but does not rebroadcast.

Request Zone:
Assume that request zone is in rectangular shape. Assume that node S knows that node D was at location (Xd, Yd) at time t0. At time t1, node S initiates a new route

discovery for destination D. We assume that node S also knows the average speed v with which D can move. Using this, node S defines the expected zone at time t1 to be the circle of radius R = v(t1 - t0) centered at location (Xd, Yd).

We define the request zone to be the smallest rectangle that includes current location of S and the expected zone (the circular region defined above), such that the sides of the rectangle are parallel to the X and Y axes. In figure 4(a), the request zone is the rectangle whose corners are S, A, B and C, whereas in figure 4(b), the rectangle has corners at point A, B, C and G – note that, in this figure, current location of node S is denoted as (Xs, Ys).The source node S can, thus, determine the four corners of the request zone. S includes their coordinates with the route request message transmitted when initiating route discovery. When a node receives a route request, it discards the request if the node is not within the rectangle specified by the four corners included in the route request.

If node I receives the route request from another node, node I forwards the request to its neighbors, because I determines that it is within the rectangular request zone. However, when node J receives the route request, node J discards the request, as node J is not within the request zone as shown in figure. When node D receives the route request message, it replies by sending a route reply message.

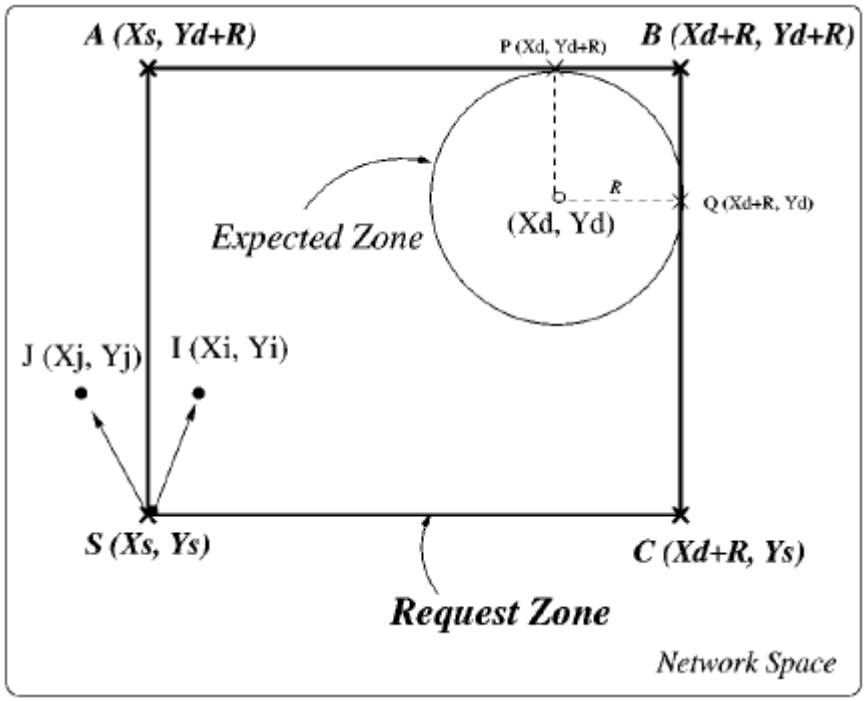

Fig 2: Source node outside the expected zone

6. PERFORMANCE EVALUATION

TOCOP is implemented in NS-2 network simulator. In our protocol routing overhead is decreased by using Position based information than TOHIP. We compare the

results from TOHIP and TOCOP in terms of Packet Delivery Ratio (PDR) and Routing Overhead (RO).

Packet Delivery Ratio (PDR): the ratio of packets successfully delivered to packets generated.

$$PDR = \frac{\sum packet\ received\ by\ the\ destination}{\sum packet\ generated\ by\ the\ source} \times 100\%$$

Routing Overhead (RO): the average number of route messages (in packets) per successfully delivered packet.

$$RO = \frac{\sum route\ message}{\sum data\ packet\ recevied\ by\ the\ destination}$$

Malicious Dropping Ratio (MDR): the number of packets discarded by the malicious nodes by data packets sent by source node.

$$MDR = \frac{\sum data\ packet\ discarded\ by\ the\ malicious\ nodes}{\sum data\ packet\ sent\ by\ the\ source\ node}$$

As shown in the below figure the routing overhead is decreased when compared from existing multipath routing protocols to our protocol.

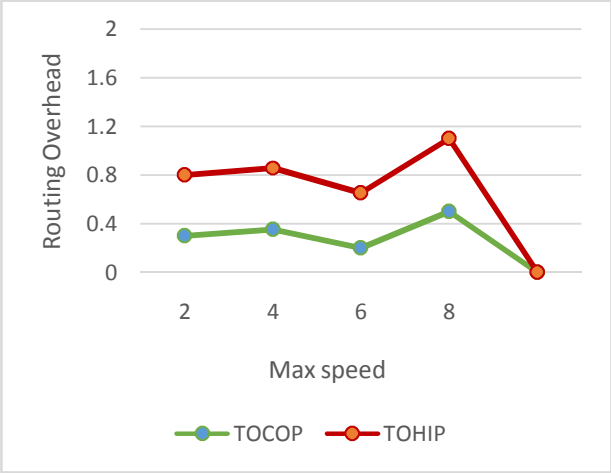

Fig 3: Routing Overhead

`

7. CONCLUSION

In existing multipath routing protocols routing overhead created during the route discovery phase leads to compromise in QoS (Quality of Service). This paper describes how location information may be used to reduce the routing overhead by hiding the topology in ad hoc networks. Performance evaluation shows that TOCOP

has better capability of finding routes and resist attacks at a low routing overhead. As for the future work, we plan to design the data transmission strategy with fault detection mechanism.

8. REFERENCES

[1] L. Abusalah, A. Khokhar, et al., "*A survey of secure mobile ad hoc routing protocols"*, IEEE Commun. Surv. Tut. 10 (4) (2008) 78–93.

[2] E. Gerhards-Padilla, N. Aschenbruck, et al., "*Detecting black hole attacks in tactical MANETs using topology graphs*", in: IEEE Conference on Local Computer Networks (LCN), 2007, pp. 1043–1052.

[3] F.N. Abdesselam, B. Bensaou, et al., "*Detecting and avoiding wormhole attacks in wireless ad hoc networks*", IEEE Commun. Magaz. 46 (4) (2008) 127–133.

[4] Y.C. Hu, A. Perrig, et al., "*Rushing attacks and defense in wireless adhoc routing protocols*", in: ACM Workshop on Wireless Security(WiSe), 2003, pp. 30–40.

[5] J.R. Douceur, "*The Sybil attack, in: International Workshop on Peer-to-Peer Systems (IPTPS)*", 2002, pp. 251–260.

[6] D. Johnson, Y. Hu, et al., "*The dynamic source routing protocol (DSR) for mobile ad hoc networks for IPv4*", IETF RFC 4728, 2007.

[7] Y.B. Yang, H.B. Chen, "*An improved AODV routing protocol for MANETs*", in: International Conference on Wireless Communications,Networking and Mobile Computing (WiCom), 2009, pp. 1–4.

[8] K.E. Defrawy, G. Tsudik, "*ALARM: anonymous location-aided routing in suspicious MANETs*", IEEE Trans. Mob. Comput. 10 (9) (2011)1345–1358.

[9] K. Sanzgiri, B. Dahill, et al., "*Authenticated routing for ad hoc networks*", J. Select. Areas Commun. 23 (3) (2005) 598–610.

[10] G. Dommety and R. Jain, "*Potential networking applications of global positioning systems (GPS)*", Technical report TR-24, The Ohio StateUniversity (1996).