Reliable Prioritize and Topology Hiding in Mobile Ad hoc Networks

Ajay V K[1], Praveen Kumar[2], Yuvaraja Dakka[3]

[1]Dept of IT Networking
VIT University Vellore, Tamil Nadu, India
Ajayvk2@email.com

[2]Dept of IT Networking
VIT University Vellore, Tamil Nadu, India
Praveendasare.123@email.com

[3]Dept of IT Networking
VIT University Vellore, Tamil Nadu, India
Yuvarajaeee59@email.com

Abstract: ***Existing multipath navigating conventions in MANETS overlook the topology-presentation issue. This paper investigates the dangers of topology-presentation and proposes a Topology-Hiding multipath Protocol (TOHIP). TOHIP does not permit packages to convey navigating data so the vindictive hubs can't find system topology and dispatch different assaults based on that. The convention can likewise build numerous hub disjoint courses in a course disclosure endeavor and prohibit problematic courses before transmitting parcels. We formally demonstrate that TOHIP is circle free and does not uncover system topology. Security examination demonstrates that TOHIP can oppose different sorts of assaults effectively and successfully. Reproduction results show that TOHIP has better capacity of discovering courses and can significantly increment the ability of conveying parcels in the situations where there are malignant hubs at the expense of low directing overhead. This paper also eliminates the problem of link disjoint path by eliminating common route node and adds an extra feature of prioritizing the packet by providing shortest path for the prioritized packet.***

Keywords: Topology Hiding, Multi Path, Route Reply, Packet Priority, Topology, Capacity, Routing

1. Introduction

Multipath routing protocols attracts a lot of attentions because they support load balancing and improve the reliability it will be a susceptible target for the malicious node for exploring and causing to launch different attacks for the same reason. However as far as we know none of the current existing secure protocol provides the alternate solution for topology exposure problem which is reliable and adds a priority and this topology exposure is a serious problem which will cause a malicious node to launch different kinds of attacks such as black hole and rushing attacks. Topology-exposure is much more serious in multipath routing protocols than in other routing protocols considering that multipath routing protocols usually carry a lot of routing information in route messages in order to find sufficient routes. In some cases, data packets are also required to carry routing information. For example, Dynamic Routing Protocol (DSR) carries the whole route from source to destination in packet headers[9]. Malicious nodes can deduce part or the whole network topology based on the captured routing information and it is hard to ensure the confidentiality of routing information because of the open media network environment in which any node can capture packets within its transmission range. Once the network is established we will run the topology hiding algorithm for that and we will eliminate the common node which gets a too many requests from the neighbor and well give priority to the packets to travel in a shortest path. Thus no node capture network topology and we can say that it is a loop free w.r.t reliability and security.

2. Literature Survey

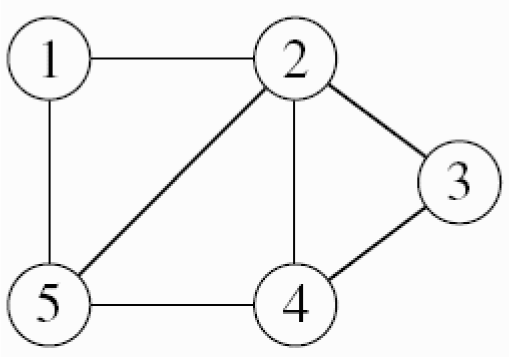


Figure 1: Topology of network

Considering the given figure 2.0 and node 1 as a source node and 3 as the destination node and remaining nodes as the intermediate nodes. Now data packets are sent from source to destination by all the node. First we will simulate the concept of Topology hiding multipath protocol (THOIP) to the given network which will be explained in the proposed algorithm section of this paper. As data passes from all the nodes to reach the destination it can be observed that the node which is having many connected neighbors has high data traffic. After removing the node which has high traffic in the network the path so obtained may or may not be the shortest path .the path so obtained after removing the node which has high traffic will be more reliable. We include the concept of priority packets that has to be transferred to the destination. There will be a priority table and the source node will be aware of the priority of the packet .the shortest path which we have identified in the Topology hiding multipath protocol

(THOIP) will be given to the high priority path to reach the destination.

3. Proposed Method

Topology hiding is defined, if the distance between the node Ni and Nj (which are part of the entire node N) is greater than 2 than node Ni cannot know which nodes are connected to Nj .In other words any node can deduce network topology within 2 hops at most.

3.1. Protocol Design

Three objectives in designing THOIP

1. Link connection is hidden in root message.
2. We will find as many node disjoint path as possible such that load balancing and reliable packet delivery can be improved.
3. It removes malicious node from roots and detect unrealizable roots.
4. THOIP uses the combination of hop count and RTT as a routing matrix

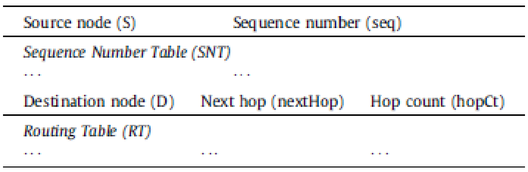
Data structure used: instead of using routing table here each node uses two tables

1. Sequence number table (SNT)
2. Routing table (RT)

   As shown in figure 2.0

   Fig:2.0

Data structures.



Source node (S)	Sequence number (seq)
Sequence Number Table (SNT)	
...	...

Destination node (D)	Next hop (nextHop)	Hop count (hopCt)
Routing Table (RT)		
...	...	...

TOHIP has three phases: Route Request Phase, Route Reply Phase and Route Probe Phase.

3.2. Route Request Phase

Please use a 9-point Times Roman font, or other Roman font with serifs, as close as possible in appearance to Times Roman in which these guidelines have been set. The goal is to have a 9-point text, as you see here. Please use sans-serif or non-proportional fonts only for special purposes, such as distinguishing source code text. If Times Roman is not available, try the font named Computer Modern Roman. On a Macintosh, use the font named Times. Right margins should be justified, not ragged.

3.3. Route Request Phase

It makes converse courses that will be utilized as a part of Route Reply Phase. A course demand messages is transmitted from the source hub to the goal hub through television. To keep up system integration, after accepting a course demand message, each transitional hub makes a converse course, and rebroadcasts the message on the off chance that it has never gotten this message previously.

3.4. Route Reply Phase

It find whatever number hub disjoint courses as could reasonably be expected. A course answer message is transmitted from the goal hub to the source hub by means of television. After getting such a message, a transitional hub chooses the neighbor closest to the source hub as the past bounce on the course. It then promotes this determination to all its different neighbors, to guarantee no hub is chosen on various course

3.5. Route Probe Phase

Distinguishes the temperamental courses before transmitting parcels. To guarantee the courses made in Route Reply Phase are accessible, the source hub sends a course test message through every found course to the objective hub. Thusly, the inconsistent courses can be distinguished and dispensed with. In the three stages above, no steering data is conveyed in course messages. Regarding information structure, each hub keeps two tables. One is Sequence Number Table (SNT) which keeps hubs from rebroadcasting unnecessary course demand messages. Every section in SNT contains the source node which initially requests route discovery and the sequence number that the source node uses in this course revelation endeavor. The other is Routing Table (RT). Every entrance in RT incorporates the objective hub, the hub through which to achieve the end of the line, and the quantity of jumps to the goal hub

3.6. Route Request Phase

S: source ID.
D: destination ID.

Seq: sequence number, set by the source node.(s,seq) uniquely identifies a RREQ message. All RREQ messages with the same (s,seq) belong to a same route discovery.

hopCt: hop count to the source node.

At source node S:At the point when a source hub S needs a course to goal D yet can't find a course in its directing table, S launches Route Request Phase by broadcasting a RREQ(S,D,seq,hopcount) At intermediate nodes: 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

4. Results and Analysis

It concludes that in order to provide high reliability, high security, prioritizing the packets and to overcome the traffic congestion we are going for thesis. All the above objectives we are getting by using topology hiding prioritize the packets. In order to get reliability we are going to hide our network topology to overcome malicious attacks this we will achieve by using topology hiding And also owe are giving security by using hiding topology. By priority indicator present in the source we are going to choose shorter path or longer path. This priority table contains the info regarding the importance of the packets, based on the priority i.e., high priority packet going to choose the shorter path and lower priority packet going to choose longer path.
We have taken the snap shot of two wireless networks and we are going to show the simulation results of those two networks by eliminating one of the node the network still

remains the same i.e. undivided so reliability will be there among senders and receivers

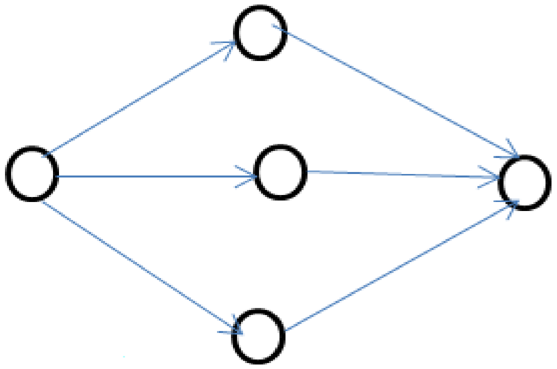


Figure 2: Initial Topology

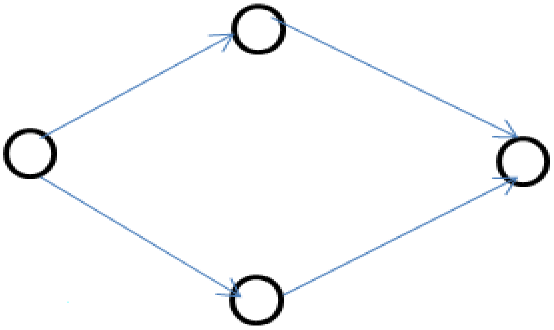


Figure 3: Changed Topology when a node gets un reachable

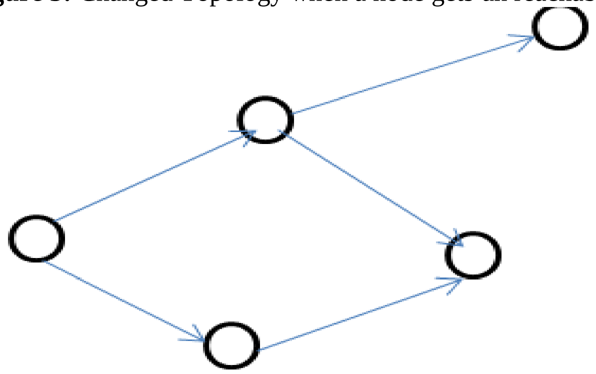
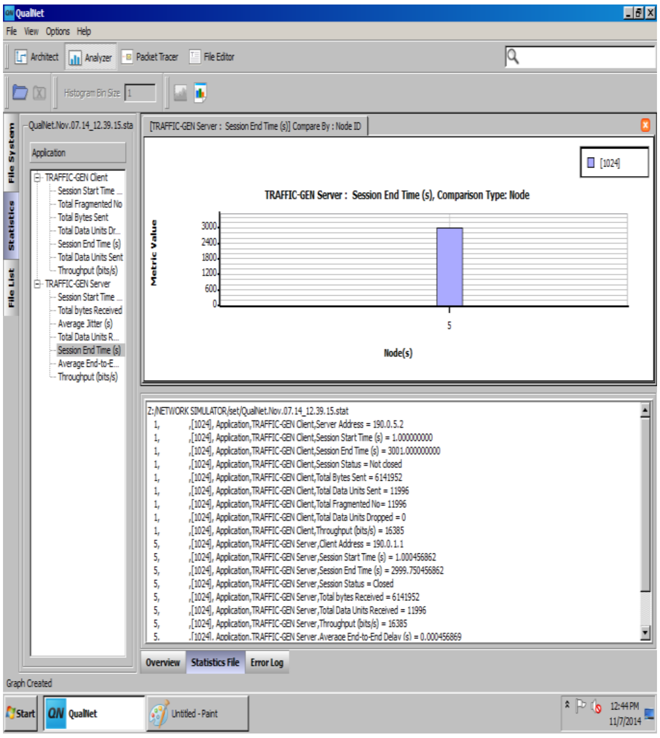
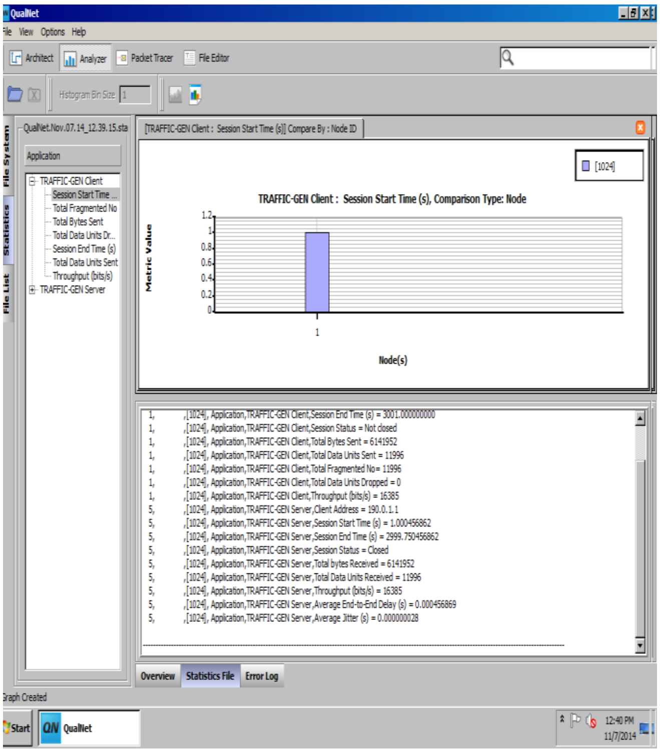


Figure 4: Changed Topology on entrance of new node



```
Z:/NETWORK SIMULATOR/set/QualNet.Nov.07.14_12.39.15.stat
  1,        ,[1024], Application,TRAFFIC-GEN Client,Server Address = 190.0.5.2
  1,        ,[1024], Application,TRAFFIC-GEN Client,Session Start Time (s) = 1.000000000
  1,        ,[1024], Application,TRAFFIC-GEN Client,Session End Time (s) = 3001.000000000
  1,        ,[1024], Application,TRAFFIC-GEN Client,Session Status = Not closed
  1,        ,[1024], Application,TRAFFIC-GEN Client,Total Bytes Sent = 6141952
  1,        ,[1024], Application,TRAFFIC-GEN Client,Total Data Units Sent = 11996
  1,        ,[1024], Application,TRAFFIC-GEN Client,Total Fragmented No= 11996
  1,        ,[1024], Application,TRAFFIC-GEN Client,Total Data Units Dropped = 0
  1,        ,[1024], Application,TRAFFIC-GEN Client,Throughput (bits/s) = 16385
  5,        ,[1024], Application,TRAFFIC-GEN Server,Client Address = 190.0.1.1
  5,        ,[1024], Application,TRAFFIC-GEN Server,Session Start Time (s) = 1.000456862
  5,        ,[1024], Application,TRAFFIC-GEN Server,Session End Time (s) = 2999.750456862
  5,        ,[1024], Application,TRAFFIC-GEN Server,Session Status = Closed
  5,        ,[1024], Application,TRAFFIC-GEN Server,Total bytes Received = 6141952
  5,        ,[1024], Application,TRAFFIC-GEN Server,Total Data Units Received = 11996
  5,        ,[1024], Application,TRAFFIC-GEN Server,Throughput (bits/s) = 16385
  5.        .[1024]. Application.TRAFFIC-GEN Server.Average End-to-End Delay (s) = 0.000456869
```

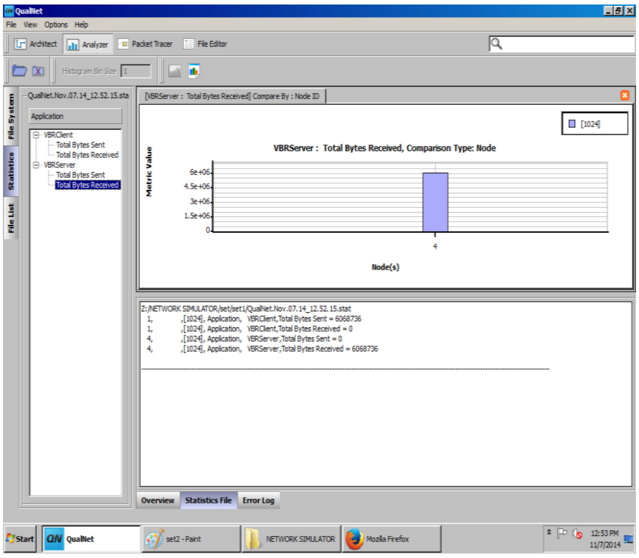
Figure 5: simulation results when a node is intact



```
  1,        ,[1024], Application,TRAFFIC-GEN Client,Session End Time (s) = 3001.000000000
  1,        ,[1024], Application,TRAFFIC-GEN Client,Session Status = Not closed
  1,        ,[1024], Application,TRAFFIC-GEN Client,Total Bytes Sent = 6141952
  1,        ,[1024], Application,TRAFFIC-GEN Client,Total Data Units Sent = 11996
  1,        ,[1024], Application,TRAFFIC-GEN Client,Total Fragmented No= 11996
  1,        ,[1024], Application,TRAFFIC-GEN Client,Total Data Units Dropped = 0
  1,        ,[1024], Application,TRAFFIC-GEN Client,Throughput (bits/s) = 16385
  5,        ,[1024], Application,TRAFFIC-GEN Server,Client Address = 190.0.1.1
  5,        ,[1024], Application,TRAFFIC-GEN Server,Session Start Time (s) = 1.000456862
  5,        ,[1024], Application,TRAFFIC-GEN Server,Session End Time (s) = 2999.750456862
  5,        ,[1024], Application,TRAFFIC-GEN Server,Session Status = Closed
  5,        ,[1024], Application,TRAFFIC-GEN Server,Total bytes Received = 6141952
  5,        ,[1024], Application,TRAFFIC-GEN Server,Total Data Units Received = 11996
  5,        ,[1024], Application,TRAFFIC-GEN Server,Throughput (bits/s) = 16385
  5,        ,[1024], Application,TRAFFIC-GEN Server,Average End-to-End Delay (s) = 0.000456869
  5,        ,[1024], Application,TRAFFIC-GEN Server,Average Jitter (s) = 0.000000028

------------------------------------------------------------------------------------------
```

Figure 6: Simulation results when a node is unreachable



```
Z:/NETWORK SIMULATOR/set/set1/QualNet.Nov.07.14_12.52.15.stat
  1,          ,[1024], Application,   VBRClient,Total Bytes Sent = 6068736
  1,          ,[1024], Application,   VBRClient,Total Bytes Received = 0
  4,          ,[1024], Application,   VBRServer,Total Bytes Sent = 0
  4,          ,[1024], Application,   VBRServer,Total Bytes Received = 6068736

------------------------------------------------------------------------------------------
```

Figure 7: Simulation results when a node is removed

References

[1] M., Balakrishnan, karger., H Walfish, Vutukuru., M and S., Shenker "Dodos defense by offense", it was in SIGCOMM ACM Computer Communication Review ,ACM the Vol.303-314 and Vol.36,(2006)

[2] Agrawal, V., and H. Denesha, In computing Communication and Applications(ICCCA) and "Multi-level authentication technique for accessing cloud services", International Conference on the , IEEE.(2012),1-4

[3] S., Koch and J. Schneider "Handling overload situations without losing of the contact to the user (Httpreject)", in Computer Network Defense(EC2ND), European Conference on, IEEE., at (2010),29-34

[4] Bansidhar, Joshi, Santhana Vijayan .A and Bineet Kumar Joshi on "The Securing Cloud Computing Environment AgainstDDos Attacks".

[5] "G. Aghila., Sivakumar .T., and Tarun Karnwal" performed on the A Comber Approach to Protect Cloud Computing against XML DDoS and HTTP DDoS attack.

[6] "Wentao Liu", performed based on the "Research On Cloud Computing Security Problem and Strategy", Wuhan Polytechnic University.

[7] "Gurudatt Kulkarin, and Jayant Tejswini P,. Amuruta Dongare". Performed on the A Security Aspects in Cloud Computing.

[8] "Akhil Behl & Kanika Behl", Centre of Excellence and Advance Service in Cicso System they performed on the "An Analysis of Cloud Computing Security Issues".

[9] "Naresh Kumar and Shalini Sharama", both from (U.I.E.T.KUK) Research on the "Study Of Intrusion Detection System for DDoS Attacks in Cloud Computing".

[10] "Moses Garruba, Rajni Goel and Anteneh Girma", from Howard university performed both of his ideas on "Cloud Computing Vulnerability:DDoS as its main Security Threat, and Analysis of IDS as a Solution Model".

[11] "Ankit Kumar & Madhavi Sinha", both of them performed on the "Overview On Vehicular Ad Hoc Network and its Security Issues".

Author Profile

Ajay V K received the B.Tech degree in computer science branch in East Point Engineering College in Bangalore during 2009-13 and persuing MTech in Computer Networking at VIT University Vellore. Currently doing research on project which involves management of disasters using wireless sensor networks

Praveen Kumar A Dasare received the B.Tech degree in Information science branch in BVB Engineering College in Hubli (Karnataka) during 2009-13 and persuing MTech in Computer Networking at VIT University Vellore. Currently doing research on project which involves management of ambulance alarm systems.

Yuvaraj Dakka received the B.Tech degree in Electrical and Electronics branch in Vidhya Bharati Institute in Bangalore during 2009-13 and persuing MTech in Computer Networking at VIT University Vellore. Currently doing research on projects in wireless sensor networks