INTERNATIONAL JOURNAL FOR TRENDS IN ENGINEERING & TECHNOLOGY
VOLUME 4 ISSUE 1 – APRIL 2015 - ISSN: 2349 - 9303

Enhancing performance using TOHIP in MANET

Thilagavathy S[1]
[1]M.E Communication and Networking,
National Engineering College, Kovilpatti
julietthilagavathy@gmail.com

Subbulakshmi P[2]
[2]Asst Professor, Department of IT,
National Engineering College, Kovilpatti
Subbu.psk@gmail.com

Abstract— Mobile Ad hoc Network (MANET) is a special self-describing wireless ad hoc network which consists of additional number of nodes that can move randomly and erratically. Due to this infrastructure it enables numerous kinds of attacks and establish topology-exposure problem. Many of the existing multipath protocols may ignore the topology-exposure problem. In this, we proposed a TOpology-HIding multipath routing Protocol (TOHIP) for preventing attacks in topology-exposure. In TOHIP, the link connection information is hidden in route messages, so that the malicious nodes cannot conclude the network topology. In Route Reply phase, the protocol TOHIP can also be used to establish multiple node-disjoint routes and eliminate the unreliable route before transmitting packets in Route Probe phase. With facilitate of a newly designed protocol, security was assured and earned superior capability of finding routes in MANET. The simulation result shows that TOHIP has given recovered performance when compared with Ad hoc On-demand Multipath Distance Vector (AOMDV) routing protocol.

Index Terms— MANET, Multipath routing, Node-disjoint route, Topology hiding, Topology exposure.

1 INTRODUCTION

In MANET, nodes are mobility in nature and it has no fixed infrastructure. Due to the fundamental characteristics [1] of the MANET, the exploration of routing protocol has been one of the majority anxious issues in the MANET. The eminent challenges of MANETs are their vulnerabilities to various security attacks [2] and inability to operate securely while preserving its resources and perform secure routing among nodes. Accordingly it is very much essential to develop an adequate, secure routing protocol to preserve the nodes.

Nowadays, Multipath routing protocol [3] is being considered since it plays a vital role to provide load balancing and reliable route discovery for transmission of packets in the MANET. However, this type of protocol is not simple for a malicious node to lance several kinds of attacks based on the security purpose in route discovery attempt. Therefore, a lot of researchers have been developing the secure routing protocols.

However, none of the already established secure multipath routing protocols accords with the topology-exposure problem. Topology-exposure is a crucial problem in MANET that induces malicious nodes to produce different type of attacks and it is a further severe problem in multipath routing protocol than the other routing protocols. Since, in route messages the multipath routing protocol sustains a lot of routing information to detect enough routes.

To overcome the problem of topology-exposure and provide security to prevent the attacks in the same problem, a novel multipath routing protocol called TOHIP is proposed. The contribution of this paper is summarized as follows:

- Design a TOpology-HIding multipath routing Protocol (TOHIP). It will not hold link connection information in route nodes; subsequently the malicious node cannot assume the network topology. It can also acquire node-disjoint routes and prohibit the unreliable route.
- TOHIP can resist the attacks such as black holes and rushing by using hop count and round-trip time as a routing metric.
- TOHIP can enormously increase the packet delivery ratio and provide an improved facility to finding routes. It achieves a sophisticated performance than the existing protocol AOMDV.

The rest of the paper contains six sections. In Section 2, we have summarized related works and spotlight on the difference between our work and other related works. In Section 3, we have constructed a contemporary protocol in a MANET to hide topology, to find reverse route, node-disjoint route and to exclude unreliable route. In Section 4, we have depicted the security to prevent the attacks allied a black hole and rushing based on TOHIP. In Section 5, we have shown our simulation results to analyze the protocol performance when there is a malicious node as well as when there is no malicious node in the network environment. Finally, Section 6 presents the conclusion.

2 RELATED WORKS

The idea of creating node-disjoint route and overcoming the attacks are captured from various routing protocols. For example, in [3] an Anonymous Location-based and Efficient Routing protocol (ALERT) is proposed to provide high anonymity protection (for sources, destination, and route) with low cost. ALERT can also avoid timing attacks by virtue of its non fixed routing paths for a source destination pair. ALERT is not completely bulletproof to all the attacks. In [4], a risk-aware response mechanism is used to systematically cope with routing attacks in MANET. Due to infrastructure-less architecture of MANET, the risk-aware response system is distributed. On the other hand, the mean latency of risk-aware response is higher while the number of nodes is smaller. In [5], they address a

number of issues arising in suspicious location-based MANET settings by designing and analyzing a privacy-preserving and secure link-state based routing protocol (ALARM). It provides security which includes node/origin authentication and location integrity although not deliberate the topology exposure problem. In [6], a novel route discovery mechanism based on the estimated distance (EstD) is developed in order to reduce the control overhead of routing protocols in MANETs. It can estimate the distance of two nodes augmented accurately without positioning service and avoid RREQ packet to the entire network. However, the packet delivery ratio and the average end-to end delay give negative effect when the node distribution is incredibly sparse.

In [7], they addressed to ensure the safety of the forwarding function by staving off malicious nodes from being involved in routing paths. Nevertheless, if no shared node is identified, subsequently the source node delays or abandons the transmission of the data packets, leading to a severe degradation of the network performance. In [8], an improved AODV (I-AODV) protocol is introduced to conserve energy among the nodes, and a delay reduction mechanism is applied to reduce the average end-to-end delay of the network, although it will not consider the packet delivery ratio. In [9], they focused on the various load metrics and summarizes the principles behind several existing load balanced ad hoc routing protocols.Load Aware Routing in Ad hoc (LARA) and Content Sensitive Load Aware Routing (CSLAR) incur higher complexity in capturing load information. During route maintenance Load Balanced Ad hoc Routing (LBAR) and Associativity Based Routing (ABR) perform load balancing and not achieve load balancing during route discovery. In [10], a new on-demand multipath protocol called ad hoc on-demand multipath distance vector (AOMDV) is projected to ensure that the set of multiple paths are loop-free and the alternate paths at every node are disjoint. Although the relative performance gain with AOMDV reduces since it may not have any mechanism to mitigate congestion at high loads and it incurs additional overhead for each route discovery.

In [11], the secure message transmission (SMT) protocol and the secure single-path (SSP) protocol are designed for malicious disruption of data transmissions. On the contrary, the security and fault-tolerance of the data communication are paramount in the inherently insecure and unreliable ad hoc networking environments. In [12], a novel centralized intrusion detection approach is introduced for detecting routing attacks against the Optimized Link State Routing protocol (OLSR) in tactical MANETs. It tries to detect falsified HELLO messages, but the average probability density function is dropped when the black hole attack is switched on.

In [13], a secure and efficient MANET routing protocol (SAODV) is developed to address the security weakness of the AODV protocol and is capable of withstanding the black hole attack. SAODV can effectively prevent black hole attack in the MANET and maintains a high routing efficiency. On the contrary, it will not reduce the packet loss rate. In [14], a Node-Disjoint Multipath routing Protocol based on AODV (NDMP-AODV) is developed to discover multiple node-disjoint paths with a low routing overhead during a route discovery and maintained control overhead during route maintenance. This protocol improves the packet transmission rate and reduces the end-to-end delay; however it may not consider the topology hiding.

From these works, none of the protocols may focus on the topology-exposure problem. It provides the security which includes confidentiality and availability whereas our work is introduced to resist the attacks in topology-exposure problem by designing a topology hiding protocol.

3 PROTOCOL DESIGN

This section presents a protocol called TOpology-HIding multipath routing Protocol (TOHIP) [16]. There are three major goals in designing the protocol TOHIP. First, TOHIP does not maintain the link connection information consequently the malicious node cannot deduce the network topology. Second, TOHIP can also find node-disjoint route that is once a route is established, it can advertise a set which contains the nodes on routes and prevents a node from an already established route. Therefore, it ensures that all the established routes are node-disjoint.

TOHIP possess three phases: route request phase, route reply phase and route probe phase.

- Route request phase creates a reverse route which is used in route reply phase. In this phase, route request messages are transmitted from source to destination. After receiving a route request message, every intermediate node creates a reverse route and rebroadcast them if the message is not received before.
- Route reply phase finds several node-disjoint routes as possible in route messages. In this phase, route reply messages are transmitted from destination to source node. After receiving a reply message, an intermediate node picks the neighbor, which is close to the source node and thus multiple node-disjoint routes are established.
- Route probe phase detects the unreliable route and excludes it before sending out the packets. The source node sends a route probe message through every exposed route in route reply message to the destination node. By performing this action, the unreliable route is detected and eliminated.

In these three phases, every node maintains two tables. One is Sequence Number Table (SNT) which is used to prevent nodes from unnecessary route messages. The other is a Routing Table (RT) that includes the node through which to reach the destination and determine the number of hops to the destination.

3.1 Route Request Phase

A route request message (RREQ) contains the following fields such as source, destination, sequence number and hop count.

- S: source ID
- D: destination ID
- Seq: sequence number, which is fixed by the source node <s, seq> and exclusively identifies the RREQ message.
- HopCt: hop count to the source node

3.1.1 At source node S

When a source node S needs a route to destination D but cannot find a route in its routing table, S initiates Route Request Phase by broadcasting a route request message which is transmitted from source node to destination node.

3.1.2 At intermediate nodes

After receiving a route request message, every intermediate node checks whether this message is the first RREQ replica. If it is right, then it registers in SNT, adds the hop count by 1 and afterward rebroadcast the route request message. In TOHIP, every intermediate node creates reverse route. Therefore, numerous reverse routes will be created with this protocol though it will be used in route reply phase.

3.1.3 At destination node D

After the destination node receives the first RREQ copy the timer T_D is initiated to gather the other RREQ copies. The destination node only acquires the RREQ copies before the timer T_D times out. It progresses in the same way as that of intermediate node except the retransmission.

3.2 Route Reply Phase

A route reply message (RREP) consists of the consecutive fields.

- S: source ID
- D: destination ID
- HopCt: hop count to the destination node
- Next Node: the RREP message can reach the source node by using the smallest number of hops.
- exNodeSet: consist of a set of nodes which is not representing the intermediate node in the routes.

3.2.1 At destination node D

When the destination node D receives the first RREQ copy, the route reply phase is initiated by broadcasting a route reply message. The route reply message contains the hop count as 0, Next Node is null and exNodeSet have the neighbors of destination node D.

3.2.2 At intermediate nodes

After intermediate node obtains a RREQ copy, it acquires the numerous actions. The first action is to detach the routes when destination node acts as a source node and Next Hop is present in exNodeSet. The next action is to remove all the routes if certain nodes are already present in an established route.

The intermediate node can seize further actions in two cases. In the first case, the Next Node is an intermediate node itself while in another case, Next Node is null. The actions are as follows: First, the intermediate node creates a route to destination by using the RREP sender. Second, the intermediate node discovers the neighbor, which is close to the source node by examining its routing table. At that time, the intermediate node eliminates all the other routes, excluding the one which is close to source S.

The additional action is that the intermediate node modernizes and rebroadcasts the RREP message. After that, the intermediate node sets Next Node to the nearest neighbor, appends it into exNodeSet, raises hop count by 1 and subsequently rebroadcasts the RREP message.

3.2.3 At source node S

Source node receives the first RREP copy and the timer is initiated to obtain the other RREP copies. Source accepts the copies which have arrived before exceeding the timer. The source will not accept the RREP message when it exceeds the timer and finally node-disjoint routes to destination are established.

3.3 Route probe phase

Before broadcast the packets, the source will set off a route probe phase of transmitting the route probe message (RPRO) to destination through every route which is established in route reply phase. If the malicious nodes are dropping packets on a route, afterward the source node could not send the returning probe message. Hence, the unreliable route is identified and excluded.

4 SECURITY ANALYSIS

Since the network topology concealed by TOHIP, the malicious nodes are not able to trigger attacks from the central position of the network. Consequently, the possible harms acquired by malicious nodes are enormously reduced or excluded.

4.1 Black hole attack

Black hole attack is a type of denial of service wherein a malicious node can induce all packets by falsely declaring a fresh route to the destination and will not forward them to the destination. The black hole attacker can interrupt the route detection by faulty discovers a route to the destination. TOHIP can prevent the black hole attack since the intermediate nodes are not allowed to send the route reply messages [16] and to convey the packets through contemporary route when the attacker route is detected as unreliable.

4.2 Rushing attack

When a typical node remains for an arbitrary delay before dispatching a packet to abstain the collision in wireless communication, a rushing attacker will continuously forward packets rapidly. If an attacker is present in the route subsequently the round trip time traced by the route request will be smaller than the true value due to the rush. Thus the route is selected as the shortest route. TOHIP can resist the rushing attack whereas the route reply phase uses hop count as a routing metric [16] and will not forward data immediately.

5 PERFORMANCE EVALUATION

In order to evaluate the performance of the proposed TOHIP protocol, compare it with a few other protocols like AOMDV using the NS-2 simulator. The objectives in conducting this evaluation are appraising the capability of TOHIP in finding routes, testing the effectiveness of TOHIP in delivering packets

and checking the overhead of TOHIP. Performance of the network can be estimated through maximum speed changes in the network and the metrics used in the network. The following performance metrics are used for the evaluation.

- Packet Delivery Ratio (PDR): the ratio of the number of packets successfully delivered to the destination.

$$PDR = \frac{\text{Number of packets received}}{\text{Number of packets transmitted}} * 100\% \quad (1)$$

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

$$RO = \frac{\text{Number of route messages}}{\text{Number of received packets}} \quad (2)$$

- End-to-End Delay (EED): time taken for a packet to reach the destination. The average delay refers to the ratio of total number of packet delay per successfully received packets.

$$EED = \frac{\text{Total number of packet delay}}{\text{Number of received messages}} \quad (3)$$

5.1 Capability of finding routes

Many of the existing multipath routing protocols built the reverse route for the first received RREQ message. On the contrary, the protocol TOHIP may build the reverse route for every received RREQ messages. Therefore, it maintains healthier network connectivity. Once a node is positioned on a route after that the node does not place on any other already established route. So it developed the multiple node-disjoint routes. Thus the capacity of discovering routes is improved than the other existing protocols.

5.2 Non-adversarial scenario

This scenario describes the performance of proposed protocol TOHIP and existing protocol AOMDV when there is no attack in the network environment. Fig 1 shows how the maximum speed of several nodes concerns the performance in terms of packet delivery ratio, routing overhead and end-to-end delay in the non-adversarial scenario when there is no invader.

- From Fig.1 (a), the packet delivery ratio of TOHIP decreases when the maximum speed increases. The Packet Delivery Ratio (PDR) is similar for both TOHIP and AOMDV when there is no attack.
- From Fig.1 (b), the routing overhead of TOHIP increases when the maximum speed rises. TOHIP displays a similar performance when compared with AOMDV.
- From Fig.1 (c), the End-to-End delay of TOHIP was declined when the maximum speed increases. TOHIP produces an analogous performance when compared with AOMDV.

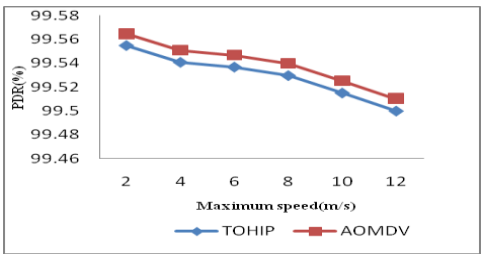

Fig 1(a) Max speed vs. PDR

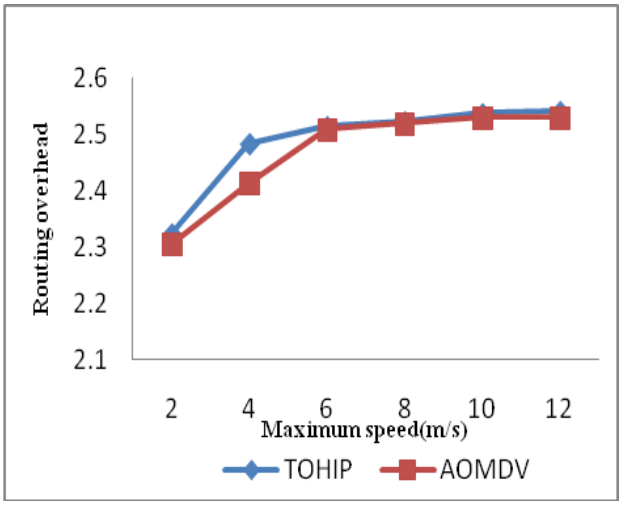

Fig 1(b) Max speed vs. Routing overhead

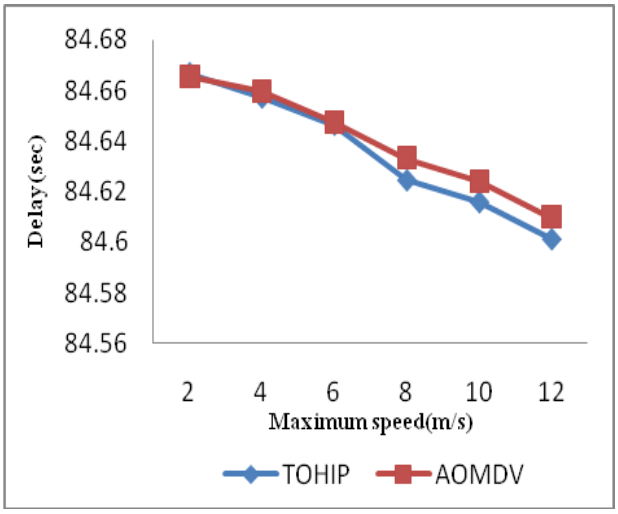

Fig 1(c) Max speed vs. End-to-End Delay

Fig 1 Performances of TOHIP and AOMDV without the attacks

The simulation result of this scenario shows that the protocol TOHIP will not degrade the performance and achieves a similar performance as AOMDV when there is no attack.

5.3 Adversarial scenario

The performance in this scenario will be evaluated when the

malicious nodes perform the black hole attack and rushing attack. It analyzes the performance for the packet delivery ratio, routing overhead and end-to-end delay as the maximum speed increases.

- Fig 2(a) shows that the packet delivery ratio of TOHIP with attack was augmented when the maximum speed enlarged. TOHIP with attack fabricates a superior performance when compared AOMDV with attack.
- Fig 2(b) shows that the routing overhead of TOHIP with attack was increased when the maximum speed enhances. Since TOHIP needs to detect the unreliable route and contains the exNodeSet in RREP messages.
- Fig 2(c) shows that the End-to-End delay of TOHIP with attack was diminished when the maximum speed improved. When comparing with AOMDV, the delay of TOHIP was decreased. Thus, TOHIP provides recovered performance when delay is reduced.

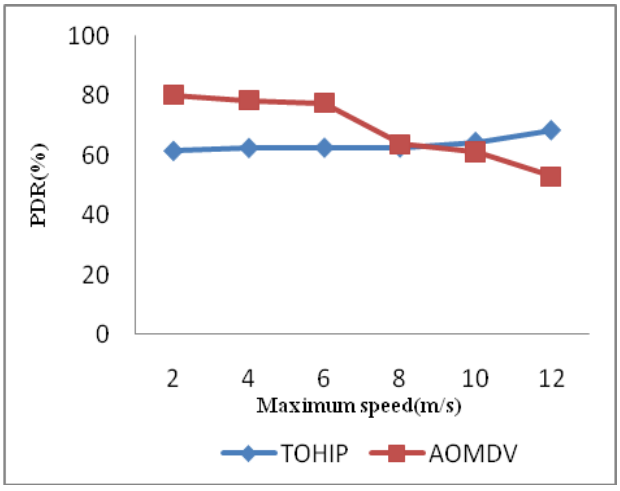

Fig 2(a) Max speed vs. PDR

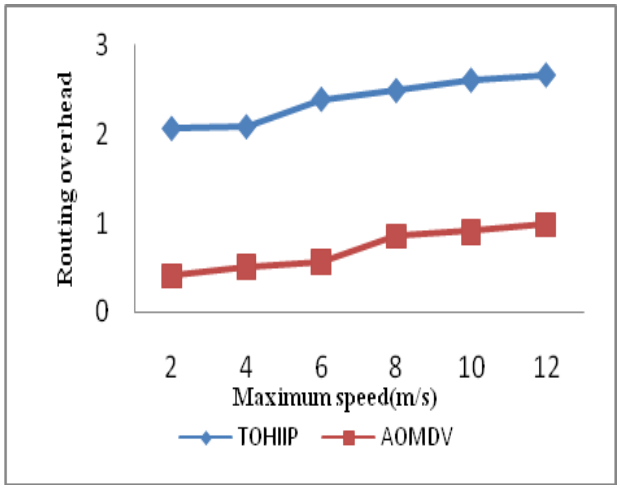

Fig 2(b) Max speed vs. Routing overhead

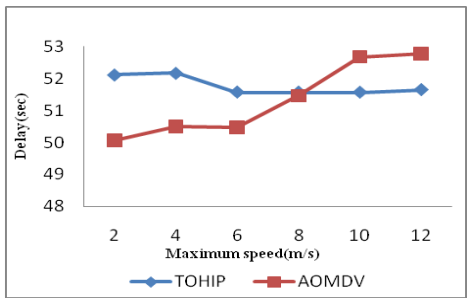

Fig 2(c) Max speed vs. End-to-End delay

Fig 1 Performances of TOHIP and AOMDV with the attacks

While comparing the proposed protocol TOHIP with AOMDV, the performance analysis of this scenario demonstrates the enhanced performance when the black hole attack and rushing attack is present into the network environment.

5 CONCLUSION

The Topology-Hiding multipath routing Protocol (TOHIP) has designed in the network environment. By using this protocol, the black hole attack and rushing attacks are prevented for the purpose of security. The performance evaluation shows that the TOHIP has improved capability of finding routes and additionally it has been shown that the performances of TOHIP will not degrade when there is no attack. If there is an attack in the network environment, TOHIP gives improved performances when compared with the existing protocol (AOMDV).

REFERENCES

[1] Aarti and Dr.S.S Tyagi, "Study of MANET: Characteristics, Challenges, Application and Security Attacks", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE),vol.3, May 2013.

[2] Priyanka Goyal,Vinti parmar and Rahul rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application",International Journalof Computational Engineering and Management (IJCEM), vol.11, Jan 2011

[3] Stephen Mueller, Rose P. Tsang, and Dipak Ghosal, "Multipath Routing in Mobile Ad Hoc Networks:Issues and Challenges", University of California, vol. 2965,(2004), pp 209-234

[4] L.Y. Zhao, H.Y. Shen, "ALERT: an anonymous location-based efficient routing protocol in MANETs", in: International Conference on Parallel Processing (ICPP), (2013), 703–712.

[5] Z.M. Zhao, H.X. Hu, et al., "Risk-aware mitigation for MANET routing attacks", IEEE Trans. Depend. Sec. Comput. 9 (2) (2012) 250–260.

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

[7] X.M. Zhang, E.B. Wang, et al., "An estimated distance-based routing protocol for mobile ad hoc networks", IEEE Trans. Veh. Technol. 60 (7) (2011) 3473–3484.

[8] S. Djahel, F. Nait-abdesselam, et al., "Mitigating packet dropping problem in mobile ad hoc networks: proposals and challenges", IEEE Commun. Surv. Tut. 13 (4) (2011) 658–672.46

[9] C.K. Toh, A.N. Le, et al., "Load balanced routing protocols for ad hoc mobile wireless networks", IEEE Commun. Magaz. 47 (8) (2009) 78–84.

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

[11] M.K. Marina, S.R. Das, "Ad hoc on-demand multipath distance vector routing", Wirel. Commun. Mob. Comput. 6 (7) (2006) 969–988.

[12] P. Papadimitratos, Z.J. Haas, "Secure data communication in mobile ad hoc networks", J. Select. Areas Commun. 24 (2) (2006) 343–356.

[13] E.Gerhards-padills, N.Aschenbrunk et al., "Detecting black hole attacks in MANETs using topology graphs, in IEEE Conference on Local Computers(LCN),2007,pp.1043-1052.

[14] Songbai Lu, Longxuan Li, Kwok-Yan Lam and Lingyan Giya, "SAODV: AMANET routing protocol that can withstand black hole attacks", in International Conference on Computer Intellligence and Security,(2009), 421-425.

[15] Snehal P. Deulkar and Vishwajit K.Barbudhe, "Discovery of path using Node-disjoint multipath routing method based on AODV protocol", International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol2, Feb 2014.

[16] Yujun Zhang,Tan Yan,Jie Tian,Qi Hu,Guiling Wang and Zhongcheng Li, "TOHIP: A topology-hiding multipath routing protocol in mobile ad hoc networks", Ad hoc networks, 21 (2014) 109-122.