ISSN No. 0976-5697

Volume 2, No. 3, May-June 2011

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

A Review on Security Issues in Multipath Routing Protocol in MANET

P.Purniemaa*
School of Computing Science & Engineering
VIT University
Vellore-632014,
Tamilnadu, India
purniemaa@yahoo.co.in

K.Manikandan
School of Computing Science & Engineering
VIT University
Vellore-632014,
Tamilnadu, India
kmanikandan@vit.ac.in

M.A.Saleem Durai
School of computer Science & Engineering
VIT University
Vellore-632014
Tamilnadu, India
masaleemdurai@vit.ac.in

Abtract: A MANET is a multi-hop ad-hoc wireless network where nodes can move arbitrary in the topology. In such networks, the wireless mobile nodes may dynamically enter the network as well as leave the network. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network. Multipath routing allows the establishment of multiple paths between a single source and single destination node. While sending data from source to destination through various paths the security in multipath and in MANET plays a serious concern. The success of mobile ad hoc networks (MANET) strongly depends on people's confidence in its security. So, in this paper we going to deal with review of multipath routing protocols along with secure data transmission related with those protocols.

Keywords: MANET, Routing Protocols, Security, Multipath, AOMDV, MP-OLSR.

I. INTRODUCTION

A Mobile Ad hoc Network is a group of wireless mobile computers in which nodes cooperate by forwarding packets for each other to allow them to communicate beyond direct wireless transmission range. MANETS are more vulnerable to attacks than wired networks due to open medium, dynamically changing network topology, cooperative algorithms, and lack of centralized, monitoring and lack of clear line of defense. During data transmission between these nodes there may be malicious threats, attacks, and penetrations which alters the performance of the system and insecure transmission. Multiple routing protocols have been developed especially for these conditions to find optimized routes that free from attacks from a source to some destination**.** These protocols consist of finding multiple routes between a source and destination node. The multipath routing could offer several benefits: load balancing, fault-tolerance, higher aggregate bandwidth, lower end-to-end delay, effectively alternative congestion and bottlenecks and security. The Security challenges in the MANET arise due to its dynamic topology**.** The communication in mobile ad hoc networks comprises two phases, the route discovery and the data transmission. In an adverse environment, both phases are vulnerable to a variety of attacks. So in multipath environment variety of attack may take place in different paths and also while transmitting data through these multiple paths. Because of the node mobility and topology changing, multipath routing in ad hoc networks presents great challenge. This paper describes we explain overview of what are the security issue related while sending the data in multiple path by using secure data transmission protocol. The rest of the paper will obtain this below. Finally, we will conclude this paper.

II. UNIPATH Vs MULTIPATH

In a multipath routing the packet can be sent via multiple paths [1] between the source and destination. This increases the packet delivery ratio with regard to unipath.

A. Benefits of multipath

Fault tolerance – Multipath routing protocols can provide fault tolerance by having redundant information routed to the destination via alternative paths. ***Load balancing*** – When a link becomes over-utilized and causes congestion, multipath routing protocols can choose to divert traffic through alternate paths to ease the burden of the congested link. ***Bandwidth aggregation*** – By splitting data to the same destination into multiple streams, each routed through a different path, the effective bandwidth can be aggregated. ***Reduced delay*** – The delay is minimized in multipath routing because backup routes are identified during route discovery.

B. Elements of a multipath routing protocol:

There are three elements of multipath routing: path discovery, traffic distribution, and path maintenance.

C. Path Discovery:

Path discovery is the process of determining the available paths for a source-destination pair [2].

Disjoint paths - The most commonly used criterion is the *disjointness* of paths, which are three main types of path, namely *non-disjoint*, *link-disjoint*, and *node-disjoint*.

A set of node-disjoint paths have no common nodes except the source and the destination. Similarly, link disjoint paths have no common links, but may share some common intermediate nodes. And Non-disjoint paths can have links in common. A link failure will only bring down one of multiple paths, whether they are link-disjoint or node disjoint.

D. Traffic Distribution:

There are various strategies of allocating traffic over available paths [3]. Path selection algorithm is used to select a subset of available paths according to certain quality of the paths. *Hop-count* has traditionally been a popular metric to use. If multiple paths are used concurrently to carry traffic, the protocol needs to decide how traffic is split over the paths and how to handle out-of-order packets at the destination. It is also possible to add a degree of redundancy when distributing traffic over multiple paths.

E. Path Maintenance:

Path maintenance is the process of regenerating paths after the initial path discovery. It can be initiated after each path failure, or when all the paths have failed. Over time, paths may fail due to link/node failures or, in ad hoc networks, node mobility. Some multipath protocols use dynamic maintenance algorithms to constantly monitor and maintain the quality or combined QoS metric of available paths.

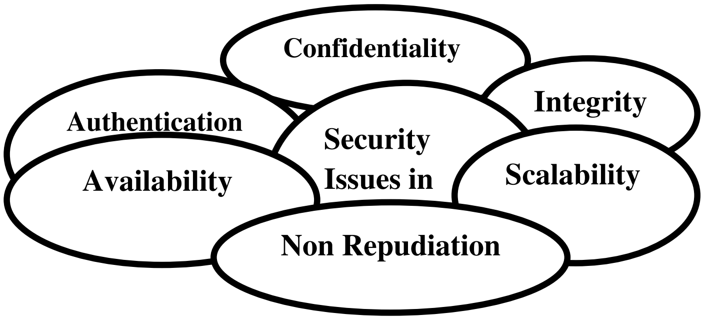
III. MANET'S SECURITY SERVICES

Security means the security mechanism for all protocols involved in this (MANET) service to protect the basic function of MANET during bit transfer from one node to another [4]. The characteristics of MANET pose both challenges and opportunities in achieving security goals, There are mainly five security services:

Authentication: Correct identity is known to the communicating partner. It is concerned with assuring that a communication is authentic. This property assigns different access rights to different types of users. ***Confidentiality:*** Message information is kept secure from unauthorized party. Basically, it protects data from passive attacks. ***Integrity:*** Integrity guarantees that the authorized parties are only allowed to modify the information or messages. Message is unaltered during communication. The altering of message can be malicious or accidental. ***Non Repudiation:*** The origin of the message cannot deny having sent the message. Thus, when a message is sent, the receiver can prove that the message was in fact sent by the alleged sender. On the other hand, after sending a message, the sender can prove that the message was received by the alleged receiver. ***Availability:*** Availability is concerned with the (unauthorized) upholding of resources. The normal service provision in face of all kind of attacks. A denial of service attacks is based to attack this property. **Scalability:** Scalability is not directly related to security but it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

IV. RELATED WORK

Security issues in ad hoc networks have been well enumerated in the literature and there are many proposed protection protocols [5, 6]. In this section, we provide a brief description of previous work on the misbehavior discussed in various papers.



A. *Single Path Security Schemes*:

Various mechanisms to prevent misbehavior on routing and data transmission in ad hoc networks have been proposed. To detect the routing misbehaviors in ad hoc networks, Marti et al. propose a reputation-based scheme composed of two modules called watchdog and path rather. The watchdog overhears the medium to check whether the next hop node faithfully forwards the packet or not and accordingly decide whether to clear a data packet in the buffer or not. Based on the information the watchdog collects, the path rater rates each path and chooses the path with the fewest misbehaving nodes. These single path security schemes are relatively simple. They can detect data dropping conducted by one individual misbehaving node. However, they fail to detect fabricated or colluded misbehavior.

B. *Multipath Security Schemes*:

Several protocols using multiple paths between source and destination to provide secure data transmission in wireless adhoc networks have been studied. Zhou and Haas initially proposed using multiple routes between nodes, just like what diversity coding to defend routing against denial-of service (DOS) attacks. Recently, several studies have been conducted on providing protection on data transmission by using multiple node disjoint paths between the source and the destination. Papadimitratos and Haas present and evaluate the Secure Message Transmission (SMT) protocol, which fights against malicious behavior of intermediate nodes on data transmission in the network. With SMT, it divides each outgoing message into a number of pieces using some message dispersal scheme, which adds limited redundancy to the transmitted data, and sends them into different routes in APS. At the destination, the received pieces are validated and the successfully received ones are acknowledged to the source through a dispersed and cryptographically protected feedback mechanism. Lou et al. [7, 8] propose and investigate a scheme called SPREAD, which provides further protection to the existed data confidentiality service in an ad hoc network using multipath routing. It aims to protect secret message from being compromised. A secret message is transformed into multiple shares using the threshold secret sharing algorithm, which also introduces some redundancy into the system.

V. ROUTING PROTOCOLS IN MANET

Routing protocols have to find routes for packet delivery and make sure the packets are delivered to the correct destinations [7]. Generally speaking, currently known routing protocols for ad hoc networks can be classified in three different classes: pro-active protocols, re-active protocols and the hybrid protocols.

Pro-active protocols (or table-driven protocols) work in a way similar to wired networks: they try to maintain an up-to-date map of the network, [9] by continuously evaluating known routes and attempting to discover new ones. The Distance-Vector protocols fall in the pro-active class. Unlike pro-active protocols, re-active protocols [10] (on-demand protocols) only start a route discovery procedure when needed. When a route from a source to a destination is needed, some sort of global search procedure is started. This does not require the constant updates being sent through the network, as in pro-active protocols. Protocols such as DSR and AODV are members of the re-active protocol class.

Hybrid protocols combine the advantages of both pro-active and re-active routing, by locally using pro-active routing and inter-locally using re-active routing [11]. Most of the multi-path routing protocols are implemented as extensions or modifications of existing single path routing protocols like the proactive protocols: DSDV and OLSR or the reactive on demand protocols: AODV or DSR. Multi-path routing achieves in general better performance than single path routing in dense networks and networks with high traffic load. It's proved that protocol performance is examined with regard to protocol overhead, traffic distribution, and throughput. The results reveal that multi-path routing achieves higher throughput and increases network capaci

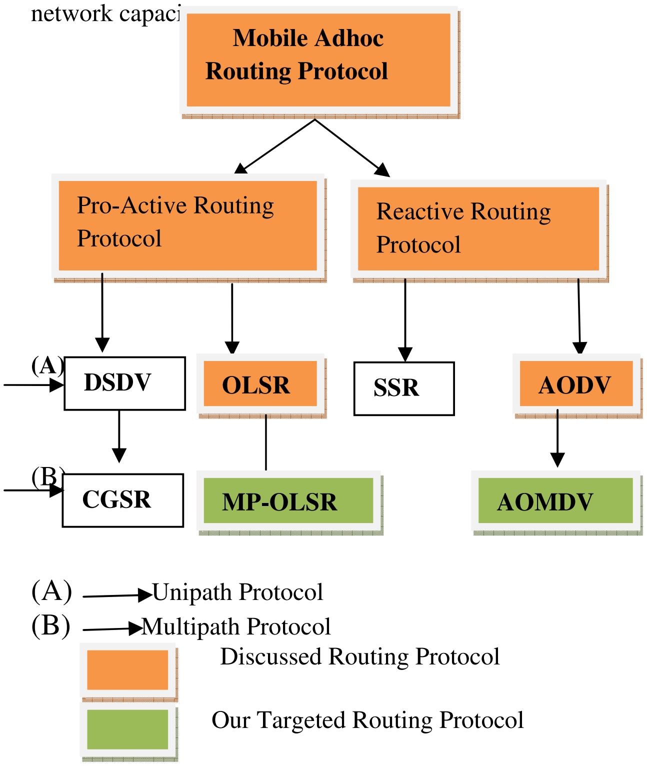

Mobile Adhoc Routing Protocol
Pro-Active Routing Protocol
Reactive Routing Protocol
(A)
DSDV
OLSR
SSR
AODV
(B)
CGSR
MP-OLSR
AOMDV
(A) Unipath Protocol
(B) Multipath Protocol
Discussed Routing Protocol
Our Targeted Routing Protocol

Fig.1 Our Targeted Routing protocol

VI. REVIEW OF TARGETED MULTIPATH ROUTING PROTOCOL

In this section we are going to study the working of multipath routing protocols like MP-OLSR and AODMV protocol.

A. Working of AOMDV Routing protocol:

AOMDV is an extension to the AODV protocol for computing multiple loop-free and link-disjoint paths. The main idea in AOMDV is to compute multiple paths during route discovery. It is designed primarily for highly dynamic ad hoc networks where link failures and route breaks occur frequently [12, 13]. With AOMDV, when a source node S desires to transmit a packet to a destination node D, it broadcasts a RREQ packet. Every node receiving the RREQ replies only if it has a fresh route to D. Otherwise it retransmits the first copy of the RREQ packet that it received after incrementing the hop-count. These intermediate nodes create a reverse route for every copy of the RREQ packet they receive. Like AODV, AOMDV RREQ packet contains a sequence numbers that is used to avoid routing loops. When D, or a forwarding node has a fresh route to D, receives S's RREQ it transmits a RREP packet through the reverse path. Every forwarding node that receives the RREP packet increments the hop count, establishes a route toward D and retransmits the RREP through every reverse route to S. Through this procedure, multiple node disjoint paths can be established between S and every forwarding node. AOMDV establishes multiple node disjoint paths, however packets are sent via unipath transmissions through the shortest paths, other paths are stored and used to avoid a time consuming route discovery procedure when the shortest path is broken.

B. Working of MP-OLSR Protocol:

MP-OLSR is the extension of the Optimized link state Routing protocol (OLSR) is a point to point protocol based on the link state algorithm. In this protocol, topology information is periodically exchanged by using of link state messages [14]. Every node periodically broadcasts its topology information and receives the information of the entire network. The topology sensing is to make the nodes aware of the topology information of the network. This part benefits from MPRs like OLSR. The route computation uses the Multipath Dijkstra Algorithm to calculate the multipath with node-disjoint or path-disjoint properties based on the information obtained from the topology sensing. The topology sensing and route computation make it possible to find multiple paths from source to destination. In the specification of the algorithm, the paths will be available and loop-free. However, in practice, the situation will be much more complicated due to the change of the topology and the instability of the wireless medium. If a link or node failure occurs, the node detecting the failure recomputes the alternative path based on the topology information and then forwards the packet through the new route. So route recovery and loop detection are also proposed as auxiliary functionalities to improve the performance of the protocol. The route recovery can effectively reduce the packet loss, and the loop detection can be used to avoid potential loops in the network. The Multipoint Relays (MPR) is the key idea behind the OLSR protocol to reduce the information exchange overhead. Instead of pure flooding the OLSR uses MPR to reduce the number of the host which broadcasts the information throughout the network. However, as a drawback OLSR protocol needs that each host periodic sends the updated topology information throughout the entire network, this increase the protocols bandwidth usage. But the flooding is minimized by the MPRs, which are only allowed to forward the topological messages.

VII. SECURITY CONSIDERATIONS

Both protocols [12] and [15] state that the protocols do not specify any special security measurements, but while sending data in multiple paths there are recommendations how the security as to enhance in order to overcome from various attacks.

The main points in the AOMDV and MP-OLSR protocols is that the control messages must be protected, that the malicious information sent by some attacking host could not affect the routing processes in the network. Both protocols should use the IPSec authentication headers for the authentication of the hosts. The AOMDV needs less protection of the control messages it is enough to protect the RREP and RRER messages in order for the protocol to be secured. Based on this information it is obvious that the AOMDV is less flexible to security solutions, because not all the AOMDV control messages are in need of the protection, so it can save the resource usage of the AOMDV protocol. The protection of the network from the other hosts can be done by encrypting all messages with some public key cryptography. However, there were not any issues about denial of service attack, because it seems impossible task to implement in such networks. AOMDV also takes the advantage of maintaining multiple alternative paths in the routing tables of nodes. Where as in the MP-OLSR malicious nodes can perform many attacks by these ways as follows:

1. There is no security mechanism for a good node to distinguish an attacker from his neighbors, once an attacker becomes his MPR node, then the attacker can create a black hole which drops all packets from or to the selector, or just drops the packets selectively, or temper the packet contents and then relay it. All of those behaves can cause the good node cannot work normally;
2. An attacker can generate lots of false Topology Control Message to broadcast. Because there is no source authentication, other nodes will accept it and update the global topology information.
3. OLSR doesn't protect the routing packets in networks, so an attacker can easily modify them and won't be detected.
4. OLSR use HELLO packets for neighbor detection, so if an attacker tunnels to B all HELLO packets transmitted by A and tunnels to A all HELLO packets transmitted by B, then A and B will believe that they are neighbors, which would cause the routing protocol to fail to find routes when they aren't actually neighbors. This attack is called wormhole attack.

VIII. PERFORMANCE EVALUATION

The following four important performance metrics are considered for evaluation of these routing protocols.

Throughput - The number of packets delivered to the receiver provides the throughput of the network. From the below figure we can say that throughput is high in MP-OLSR when compared to AOMDV.

Average end-to-end delay - Is the end-to-end delay averaged over all surviving data packets for each source/destination pair. From the below figure we can say that is more in MPOLSR.

AED = Total Delay (TD) / Packet Received (PR)

Bandwidth cost for data: is the total number of data packets all nodes transmitted normalized by the total number of data packets they received. From the below figure we can say that band with increases as the no of node increases

Packet Dropping Rate: It shows the number of data packets which were dropped during their journey to destination. From the below figure we can say that dropping of packet is low in MPOLSR.

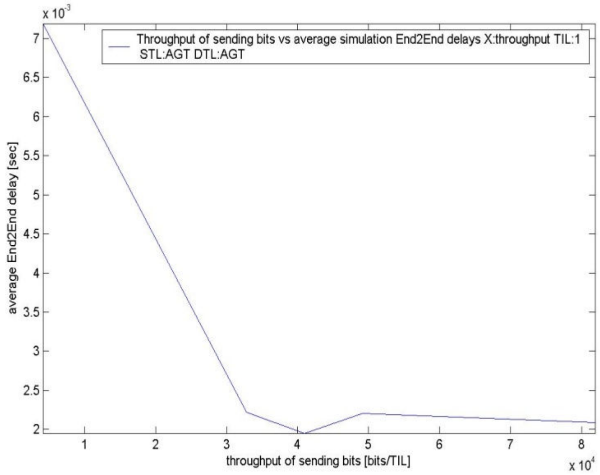


Figure2.Average End to End delay Vs Throughput of sending bits

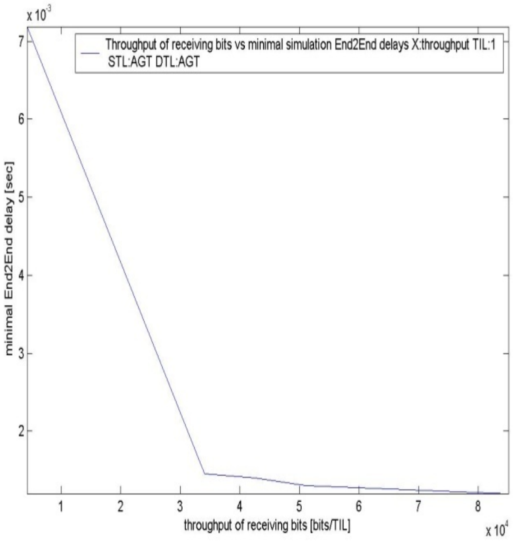


Figure3.End to End delay Vs Throughput receiving bits

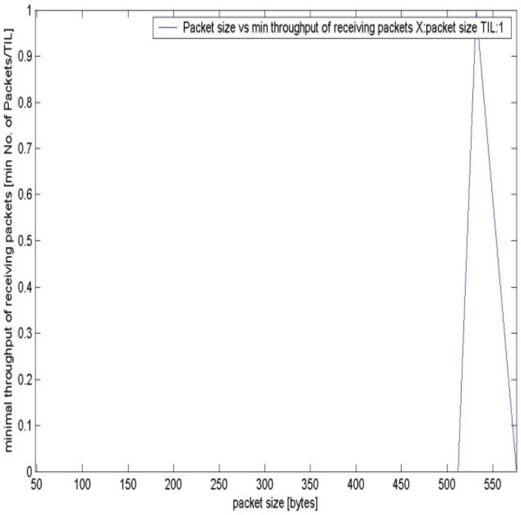


Figure4. Packet Size Vs Receiving Packets Size

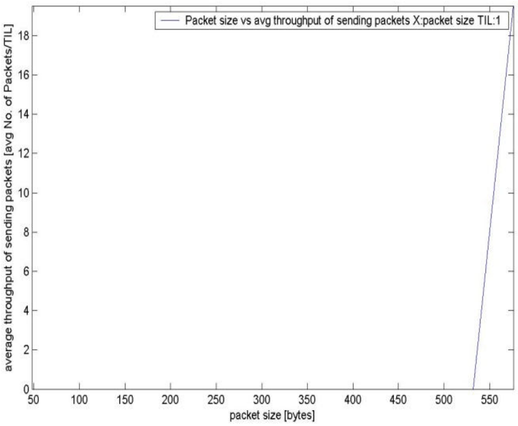


Figure5. Packet Size Vs Sending Packet Size

IX. CONCLUSION AND FUTURE WORK:

In this paper the characteristic of the ad hoc network were introduced and was explained how security issues plays important role because of its dynamic topology and also while sending data in multiple paths when route fails. Multi-path protocol i.e. AOMDV, can also work better than single-path and could offer more stable data transmission compared with single path protocol. The scalability of these protocols is quite good and their performance depends a lot on the network environment. The MP-OLSR protocol is more efficient in networks with high density and highly sporadic traffic. But the best situation is when the between a large number of hosts. The quality metrics are easy to expand to the current protocol. MP-OLSR requires that it continuously have some bandwidth in order to receive the topology updates messages. AOMDV would try to find an alternate path from among the backup routes between the source and the destination node pairs resulting in additional delay to the packet delivery time. Both protocols scalability is restricted due to their proactive or reactive characteristic. In the AOMDV protocol it is the flooding overhead in the high mobility networks. Keeping in view the above findings, we conclude that the link disjoint path option of multi-path routing protocol overall performs better than single-path or node disjoint path option of multi-path routing protocol. As a future work, we planned to provide how data can be transmitted in multiple (MP-OLSR) by using secure message transmission protocol.

X. ACKNOWLEDGMENT

The first author of this paper would like to acknowledge the help of K.Manikandan and M.A.Saleem Durai in this work.

XI. REFERENCES

[1] Jack Tsai and Tim Moors “A Review of Multipath Routing Protocols: From Wireless Ad Hoc to Mesh Networks”

[2] Stephen Mueller, Rose P. Tsang, and Dipak Ghosal “Multipath Routing in Mobile Ad Hoc Networks: Issues and Challenges”

[3] V.C. Patil1, Rajashree. V. Biradar, R. R. Mudholkar and S. R. Sawant,” On-Demand Multipath Routing Protocols for Mobile Ad Hoc Networks Issues and Comparison” International Journal of Wireless Communication and Simulation Volume 2 Number 1 (2010), pp. 21–38

[4] Pradeep Rai and Shubha Singh “A Review of ‘MANET’s Security Aspects and Challenges” IJCA Special Issue on “Mobile Ad-hoc Networks” MANETs, 2010.

[5] Li Zhao and José G. Delgado-Frias,” Multipath Routing Based Secure Data Transmission in Ad Hoc Networks”, 2006

[6] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani “A Survey of Secure Mobile Ad Hoc Routing Protocols” WIRELESS/MOBILE NETWORK SECURITY IEEE Communications Surveys & Tutorial, VOL. 10, 2008

[7] T.V.P. Sundararajan , Karthik , A. Shanmugam “Security and Scalability of MANET Routing Protocols in Homogeneous & Heterogeneous Networks” Proceedings of the International Conference on Man-Machine Systems (ICoMMS) October 2009.

[8] S. Bouam and J. B. Othman. “Data Security in Ad Hoc Networks Using Multi-Path Routing”. Beijing, China, September 2003. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC’03).

[9] YI Jiazi, “Summary of Routing Protocol in Mobile Ad Hoc Networks “Polytechnic de Nantes March, 2007.

[10] Md. Arafatur Rahman and Farhat Anwar Jannatul Naeem and Md. Sharif Minhazul bedin,” A Simulation Based Performance Comparison of Routing Protocol on Mobile Ad-hoc Network” International Conference on Computer and Communication Engineering (ICCCE 2010), 11-13 May 2010

[11] Georgios Parissidis, Vincent Lenders, Martin May, and Bernhard Plattner,” Multi-path Routing Protocols in Wireless Mobile Ad Hoc Networks: A Quantitative Comparison

[12]Yun Ge1, Guojun Wang1, Weijia Jia, Yongming Xie,"Node-Disjoint Multipath Routing with Zoning Method in MANETs", the 10th IEEE International Conference on High Performance Computing and Communications, 2008

[13]Mahesh K.Marina and Samir R.Das,"On-demand Multipath distances Vector Routing in Ad HocNetwork"2001

[14] Mazliza Othman and May Zin Oo "Performance Comparisons of AOMDV and OLSR Routing Protocols for Mobile Ad Hoc Network" Second International Conference on Computer Engineering and Applications, 2010.

[15]Jiazi Yi, Eddy Cizeron, Salima Hamma, Benoît Parrein and Pascal Lesage." Implementation of Multipath and Multiple Description Coding in OLSR" in a proceeding of 4th OLSR Introp/Workshop (Http: //www.sereadmo. org)