DETECTING AND RECOVERING MULTI-TAP FAILURE IN AD-HOC NETWORK USING OPTIMUM LINK STATE ROUTING PROTOCOL

[1]Tejhaskar A, [2]Vigneshwar R
[1]UG Scholar, [2]UG Scholar
[1]Computer Science and Engineering,
[1]Sri Sai Ram Institute of Technology, Chennai, India

Abstract : Ad hoc network is a self organizing neteork connection and it has no infrastructure to form any specific network that can change locations on the fly. Packet losses in network due to link failure in ad hoc network. In this paper, we maintain log at each router to find out where the loss occurred and a special scheme used is Optimum Link State Routing Protocol (OLSR) that uses the effective combination of proactive and reactive routing protocols. This protocol uses intra-zone and inter zone-protocol to route the packet to its destination without any loss.

IndexTerms **– Log record, proactive, reactive, OLSR.**

I. INTRODUCTION

Due to nature of wireless ad hoc network, it had relative congestion which leads to packet buffering and continuously degrades the network performance. In this paper, a new approach used to find out where the loss happen. The idea behind is that detecting packet loss is to find where the packet lost in the network. when broken link is detected in any of nodes, it performs optimized link state routing to find its destination. If not found it initiate border casts routing to find its destination.

II. PROTOCOL

Each and every router maintain log that provides information about each packet that passes through it. Failure occur when actual behavior deviates from the predicted behavior.

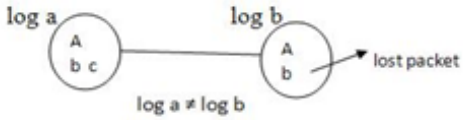

fig.2.1

Condition to be satisfied where the packet has been lost:
If Buffer limit (BL), BL<QP+ps, then the packet P is dropped due to congestion. Each log is evaluated with the previous log before it is forwarded. In our case, if log a ≠ log b, then rb stops forwarding packets further- detect failure.

III. LOG RECORD

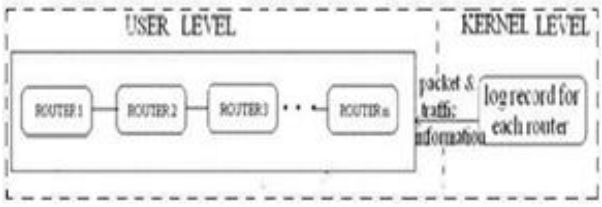

fig.3.1 log record

Log record maintains each router that has information about packets sent and received, packet size(ps), header(h), packet receiving time(t). Packet loss will be detected with help of log record. Each router maintains a queue (Q) and Buffer limit (BL) at each router. If BL< (qh+ps), then the packet P is dropped. When each packet arrives at router r and it forwarded to a destination that will traverse a path segment ending at router x, it then r increments an outbound counter related with router x. Equally, when a packet arrives at router r, it increments its inbound counter related with router x. Periodically, router x validate its outbound counters. Then, router r compare the number of packets arrived to x to have sent to r with the number of packets being received from x, and then it can detect the number of packet lost in networks.

IV. Optimized Link State Routing Protocol

The Optimized Link State Routing Protocol (OLSR) is an IP routing protocol optimized for mobile ad hoc networks, which can also be used on other wireless ad hoc networks. OLSR is a proactive link-state routing protocol, which uses hello and topology control (TC) messages to discover and then disseminate link state information throughout the mobile ad hoc network. Individual nodes use this topology information to compute next hop destinations for all nodes in the network using shortest hop forwarding paths.

V. Contrast Of Proactive vs Reactive

As a reactive, it finds a route On-Demand and it provide low overhead of control message and has disadvantage of higher latency in route discovering. As a proactive, it finds a route in advance because it maintains table at each node about entire network.

VI. Description Of OLSR Protocol

The Optimized Link State Routing (OLSR) is a table-driven, proactive routing protocol developed for MANETs. It is an optimization of pure link state protocols that reduces the size of control packets as well as the number of control packet transmissions required. OLSR reduces the control traffic overhead by using Multipoint Relays (MPR), which is the key idea behind OLSR. An MPR is a nodes one-hop neighbor which has been chosen to forward packets. Instead of pure flooding of the network, packets are forwarded by nodes MPRs. This delimits the network overhead, thus being more efficient than pure link state routing protocols. OLSR is well suited to large and dense mobile networks. Because of the use of MPRs, the larger and more dense a network, the more optimized link state routing is achieved. MPRs help providing the shortest path to a destination. The only requirement is that all MPRs declare the link information for their MPR selectors (i.e the nodes which have chosen them as MPRs). The network topology information is maintained by periodically exchange link state information. If more reactivity to topological changes is required, the time interval for exchanging of link state information can be reduced. Control messages OLSR uses three kinds of control messages: HELLO, Topology Information (TC), and Multiple Interface Declaration (MID). A Hello message is sent periodically to all of nodes neighbors. Hello messages contain information about a nodes neighbors, the nodes it has chosen as MPRs (i.e., the MPR Selector set), and a list of neighbors with whom bidirectional links have not yet been confirmed.

6.1 Multipoint Relays

The Multipoint Relays (MPR) is the key plan following the OLSR protocol to decrease the information replaces transparency. In its position of uncontaminated flooding the OLSR develop MPR to decrease the amount of the host which broadcasts the information throughout the network. The MPR is a host's single hop neighbor which may promote its messages. The MPR set of host is reserved miniature in arrange for the procedure to be competent. In OLSR merely the MPRs are capable to forward the information all through the network. Each host must have the information regarding the symmetric one skip and two skip neighbors in order to compute the finest MPR set. Information about the neighbors is taken from the Hello messages. The two skip neighbors are establishing from the Hello message since every Hello message contains all the hosts' neighbors. Selecting the lowest number of the one skip neighbors which covers all the two skip neighbors is the purpose of the MPR assortment algorithm. Also every host has the Multipoint transmit Selector position, which indicates which hosts has preferred the contemporary host to perform as a MPR When the host gets a innovative transmit message, which is require to be broaden throughout the network and the message's dispatcher boundary address is in the MPR Selector position, then the host must promote the message. Due to the potential changes in the ad hoc network, the MPR Selectors sets are modernized incessantly using Hello messages.

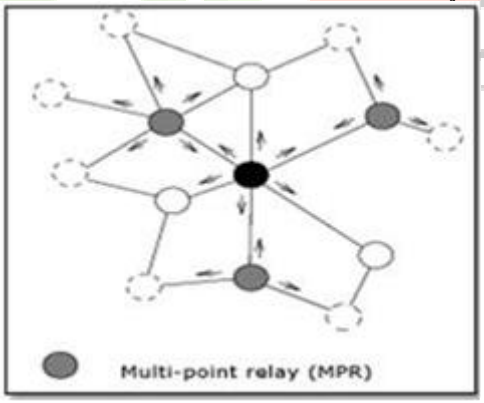

fig.6.1.1 multi-point relay

6.2 Topology Sensing

To get the topology information of the network, the nodes use Topology sensing which includes link sensing, neighbor detection and topology discovery, just like OLSR.

Link sensing populates the local link information base (Link Set). It is exclusively concerned with OLSR interface addresses and the ability to exchange packets between such OLSR inter-faces. Neighbor detection populates the neighborhood information base (Neighbor Set and 2-hop Neighbor Set) and concerns itself with nodes and node main addresses. Both link sensing and neighbor detection are based on the periodic exchange of HELLO messages. Topology Discovery generates the information base which concerns the nodes that are more than two hops away (Topology Set). It is based on the flooding of the TC messages (optimized by selecting the MPR set).

Through topology sensing, each node in the network can get sufficient information of the topology to enable routing. The link state protocol tries to keep the link information of the whole network as mentioned above. By default, the path quality is measured by the number of hops according to. It can also be measured by other metrics such as BER (Bit Error Rate)or the queue length. In our previous work, the BER metric

showed better performance in certain scenarios, but the benefit is not obvious in various situations (such as urban areas). ETX metric is also proposed as a MANET Internet Draft and is bound to become a standard. It has been extensively used in mesh networks around the world.
.

6.3 Routing Table Calculations

The host maintains the routing table, the routing table entries have following information: destination address, next address, number of hops to the destination and local interface address. Next address indicates the next hop host. The information is got from the topological set (from the TC messages) and from the local link information base (from the Hello messages). So if any changes occur in these sets, then the routing table is recalculated. Because this is proactive protocol then the routing table must have routes for all available hosts in the network. The information about broken links or partially known links is not stored in the routing table. The routing table is changed if the changes occur in the following cases: neighbor link appear or disappear, two hops neighbor is created or removed, topological link is appeared or lost or when the multiple interface association information changes. But the update of this information does not lead to the sending of the messages into the network. For finding the routes for the routing table entry the shortest path algorithm is used (eg.Djikstra's algorithm).

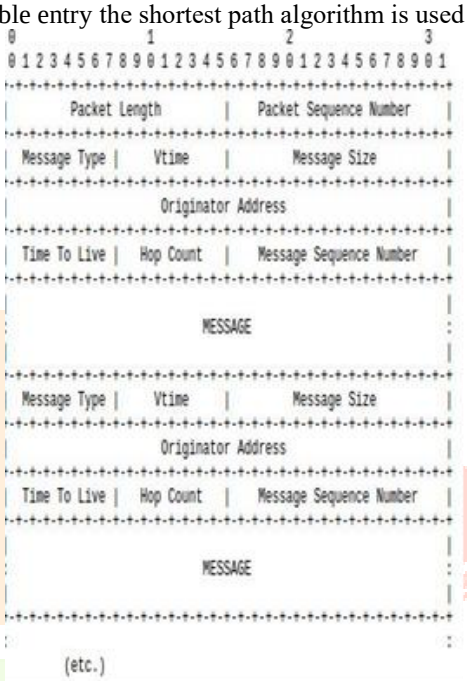

fig.6.3.1 routing table format

6.4 Route Recovery

By using the scheme of the Topology Sensing, we can obtain the topology information of the network with the exchange of HELLO and TC messages. All this information is saved in the topology information base of the local node: link set, neighbor set or topology set. Ideally, the topology information base can be consistent with the real topology of the network. However, in reality, it is hard to achieve, mainly because of the mobility of the ad hoc network.

Firstly, for the HELLO and TC messages, there are certain intervals during each message generation (2s for HELLO and 5s for TC by default). During this period, the topology might change because of the movement of the nodes. Secondly, when the control messages (especially the TC messages) are being transmitted in the network, delay or collision might happen. This will result in the control message being outdated or even lost.

Both of the two reasons mentioned above will result in the inconsistency between the real network topology and the node's topology information base. This means that when a node is computing the multiple paths based on the information base, it might use links that do not exist anymore, and cause the route failure.

Several techniques already exist in the literature to deal with the route failures in source routing. DSR handles route errors using route maintenance, mainly by sending RERR messages, which will increase the end-to-end delay significantly.

For MP-OLSR, we propose Route Recovery to overcome the disadvantage of the source routing. The principle is very simple: before an intermediate node tries to forward a packet to the next hop according to the source route, the node first checks whether the next hop in the source route is one of its neighbors (by checking the neighbor set). If so, the packet is forwarded normally. If not, then it is possible that the "next hop" is not available anymore. Then the node will recompute the route and forward the packet by using the new route.

In Figure 6.4.1 we present an example of route recovery. Node S is trying to send packets to D. The original multiple paths we have are S→A →B→D and S→C→E→G→D. However, node G moves out of the transmission range of node E and makes the second path unavailable. The source node S is not able to detect the link failure immediately (because of the delay and long interval of TC messages) and keeps sending the packets along the path, and all these packets are dropped during this period if only the source routing is used. With Route Recovery, when the

packet arrives, node E will first check if node G is still one of its neighbors, before forwarding the packet according to the source route. If not, node E will recompute the route to node D, and obtain E→F→D. Then the following packets will be sent through the new path.

Because the Route Recovery just checks the topology information saved in the local node, it will not introduce much extra delay. And most importantly, it will effectively improve the packet delivery ratio of the network.

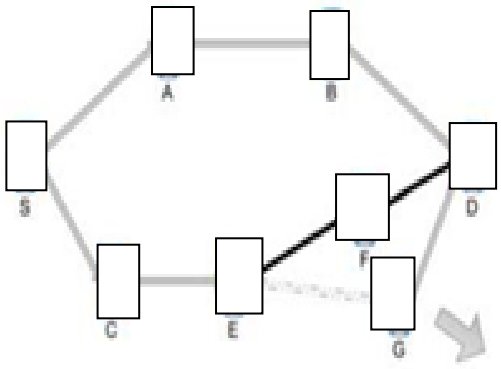

Figure 6.4.1 : An example of route recovery. The movement of node G makes the link E to G unavailable. Then node F is chosen as next hop of node E by using route recovery

6.5 Loop Detection

Loop in the network is always an important issue in routing. It is important to mention the LLN (Link Layer Notification) before taking the problem of the loops of the protocol. LLN is an extended functionality defined. in, and implemented in different OLSR or MP-OLSR simulations and implementations. If link layer information describing connectivity to neighboring nodes is available. In theory, the paths generated by the Dijkstra algorithm in MP-OLSR are loop-free. However, in reality, the LLN and Route Recovery which are used to adapt to the topology changes make the loops possible in the network. With LLN, when a node tries to send a packet over a link but fails in the end, the link layer will send feedback to the routing protocol to notify it of the link loss. This kind of abrupt interruption will result in additional operations on the topology information base rather than just regular HELLO and TC messages. This means that other nodes cannot be aware of these changes immediately. So, LLN might cause some inconsistency of the topology information in different nodes. And with Route Recovery, which might change the path in intermediate nodes, loops can occur temporarily in the network.

In Figure 6.5.1 we give an example of how a loop is generated in the network. Node A is an intermediate node of a path. The packets with source route A→C arrive at node A and need to be forwarded to node C. Then node C moves out of the transmission range of node A and node B, and makes the links A→C, B→C no longer available.

When the new packets arrive at node A, the transmission to node C will be failed. Then in node A, the routing protocol will be acknowledged by LLN, and it will remove the link A→C from node A’s link set. For node A, although it can detect the link failure of A→C by LLN, it is hard to know the failure of B→C immediately. This is because link B→C can only be re-moved when the NEIGHB HOLD TIME (6 seconds by default) expires. In the meantime, Route Recovery will be awaken. A new path A→B→C will be established and the following packets will be forwarded along the new path. Then the packets will be redirected to node B. The same operation will be performed in node B: LLN of the failure of B→C, and Route Recovery. Unfortunately, because node B cannot detect the link failure of A→C immediately, the new path obtained by

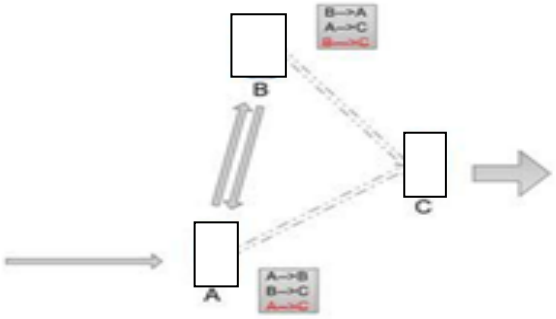

Figure 6.5.1: An example of loop in the network. The movement of node C results in inconsistency of the information bases in node A and B. One transient loop is formed between A and B.

Route Recovery is B→A→C. Thus the packet will be returned to node A, and from node A to B again, creating a loop. This is not a permanent loop, but a transient loop which will exist for several seconds and will disappear when the related link expires. However, this kind of temporary loops will block the links in the loop and congest the related transmission area.

For MP-OLSR, we propose a simple method based on source routing that can effectively detect loops without causing extra cost of memory: after the Route Recovery is performed, a new path will be calculated from the current node to the destination. The algorithm will make use of the new path if there is no loop. Or else it will try to find another path according to the multi-path algorithm. If there is no suitable path, the packet will be discarded.

For the example in Figure 6.5.1, node A will get a path A→B→C by Route Recovery. Then, when the packet arrives at node B, a new path B →A→C will be generated because of link break-age of B→C. Node B will compare the new one with the former source route A→B→C in the packet. We will find that the packet has already crossed node A, and so there might be a loop. So, the algorithm will try to find if there is any other possible path, or else the packet will be discarded.

Compared with LD-Post, which needs to keep a record of all the incoming packets, our loop detection mechanism could effectively detect the possible loops in the network without consuming extra memory space. By reducing the loops in the net-work, the network congestion can be reduced. Thus, the performance of the network can be improved, especially the end-to-end delay.

VII. PERFORMANCE EVALUATION

Performance evaluation has following steps:

7.1 Throughput

The ratio of bits received to the amount of time taken to travel from source to destination.

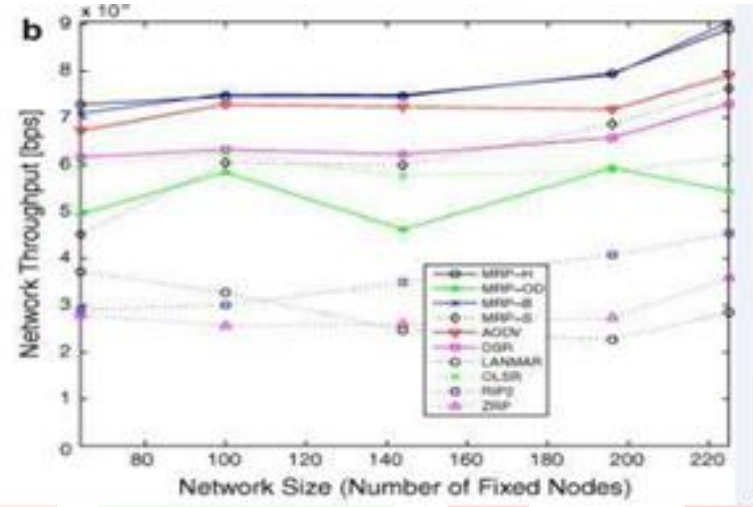

fig.7.1.1 comparison of throughput

7.2 Router Overhead

The average amount of routing protocol control packets in the network.

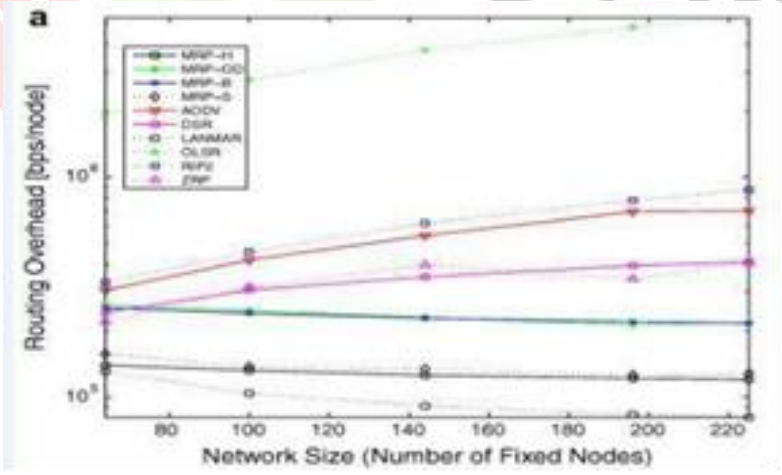

fig 7.2.1 comparison of router overhead

7.3 End-To-End Delay

Time taken for a packet to be transmitted across a network from source to destination.

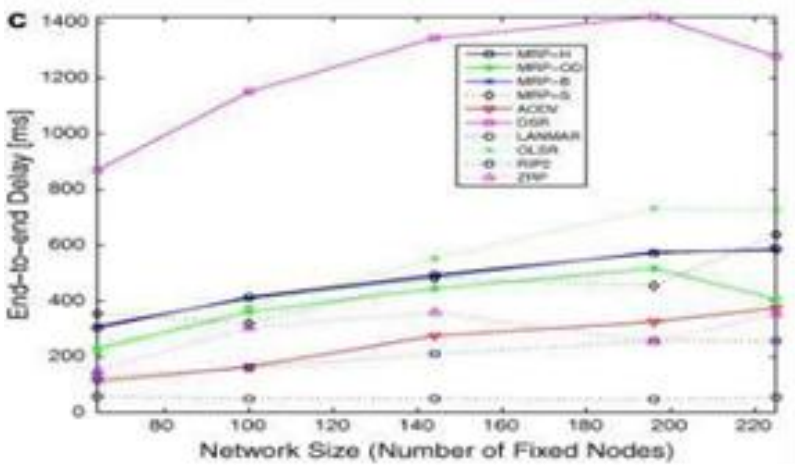

fig 7.3.1 comparison of rate of transmission

X. CONCLUSION

When link failure occur, there is a loss of packet in network, log record used to detecting where the packet loss occurred and it can be recovered by OLSR Routing mechanism, by routing mechanisms and loop detection techniques. The simulation results show that this protocol reduces the control overhead and the periodic flooding of routing information packets in table-driven approaches.

.

References

[1] R. Dube, C. D. Rais, K. Y. Wang, and S. K. Tripathi, "Signal Stability-Based Adaptive Routing for Ad Hoc Mobile Networks,"IEEE Personal Communications Magazine, pp. 36 -45, February 1997.

[2] Ashok, P.; Purushothaman, N.; Elumalai, K., "Detecting and temporarily recovering lost packets in Ad-hoc network by using Bypass routing," Radar, Communication and Computing (ICRCC), 2012 International Conference on , vol., no., pp.264,267, 21-22Dec. 2012.

[3] E. Royer and C.-K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," IEEE Personal Communications, vol. 6, no. 2, pp. 46–55, Apr. 1999.

[4] Levente Buttyán, Jean-Pierre Hubaux "Simulating Cooperation in Adhoc Wireless Network" "Mobile Networks and Applications" October2003.8thvolume

[5] C.E Perkins and E.M Royer, "Ad Hoc On-Demand Distance Vector Routing," Proceeding of IEEE Workshop on Mobile Communication System and Applications 1999, pp. 90-100 Februaru 1999.

[6] V. Padmanabhan and D. Simon. Secure traceroute to detect faulty or malicious routing. In Proc. ACM SIGCOMM HotNets Workshop, Oct. 2002

[7] Kimaya Sanzgiri, Bridget Dahill, Brian Neil Levine, Clay Shields and ElizabethM.Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks", in proc. of 10th International Conference on Network Protocol,November 2002

[8] M. K. Marina and S. R. Das, "On demand multipath distance vector routing in ad hoc networks," in IEEE International Conference of Network Protocols (ICNP), 2001.

[9]http://www.scribd.com/doc/37457740/Detecting-Malicious-Packet-Losses

[10] www.ecse.rpi.edu/ "router overhead "

[11] Hari, K.K.K., "On demand temporary route recovery for frequent link failures in adhoc networks," Trendz in Information Sciences & Computing (TISC), 2010 , vol., no., pp.181,185, 17-19 Dec. 2010 doi: 10.1109/TISC.2010.5714635

[12] Alper T. Mizrak, Stefan Savage and Keith Marzullo, "Detecting Malicious Packet Losses" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 20, NO. 2, FEBRUARY 2009.

[13] Ashok. P, Satheesh .P. S, Karthikeyan. J, "Detecting and Recovering Link-Failure in Ad-hoc Network Using Signal Stability-Oriented Routing Protocol" International Journal of Engineering Research & Technology (IJERT), Vol. 2 Issue 4, p.449-452, April – 2013,

[14] Z. J. Haas, "The Routing Algorithm for the Reconfigurable Wireless Networks," Proceedings of ICUPC 1997, Vol. 2, pp. 562-566, October 1999

[15] Comparsion of proactive and reactive people.cs.vt.edu/~irchen/6204/pdf/lecture4-mobile-ad-hoc-networks.pdf

[16] Arisyah Azizan, Megat F. Zuhairi, Hilmi M.Salleh, Mohd Nazri Ismail"Optimized Link state Routing Protocol TestBed Performance Evaluation", in International Journal Of Computer Science and Network Security(IJCSNS), Vol.16 No.10 October 2016.

[16] N.Nithya, S. Velu Chamy "An Energy Efficient Routing Based On OSLR In Wireless Sensor Networks"in IOSR Journal Of Computer Engineering(IOSR-JCE) e-ISSN:2278-0661,p-ISSN:2278-8727,pp.48-57.

[17]Yi, Jiazi; Adnane, Asma; David, Sylvain; Parrein, Benoit"Multipath optimized link state routing in mobile ad-hoc networks"DOI:10.1016/j.adhoc2010.04.007

[18] Rohit Katoch,Anuj Gupta "Implementation of OLSR protocol in MANET" International Journal Of Advanced Research ,Ideas And Innovations in Technology(IJARIIT)Vol.2,Issue 4

[19] Ayyaswamy Kathirvel and Rengaramanujam Srinivasan "Performance Analysis of Propagation Model using Wireless Mobile Ad Hoc Network Routing Protocols" DOI: WC092009002.