HSR: A New Lightweight Hybrid Source Routing Protocol for Mobile Ad Hoc Networks

Varun Pandey[1], **Somesh Dewangan**[2]

[1]Chattisgarh Swami Vivekanand University Bhilai, MTech Research Scholar CSE Dept, Disha Institute of Management and Technology, Raipur, CG, India

[2] Chattisgarh Swami Vivekanand University Bhilai, Reader CSE Dept ,Disha Institute of Management and Technology, Raipur, CG, India

Abstract*: In Mobile Ad-hoc Networks, routing is the most vital criteria on which the performance of the network depends which can easily be calculated by the parameters like packet delivery fraction, delay, overhead and the number of packets received. Abundant routing protocols have been introduced to enhance the performance under various specific scenarios. In this paper, we pro-pose an innovative technique to improve the data delivery along with effective failure detection mechanism that is lightweight hybrid source routing (HSR) protocol.. The problem of proactive and reactive methods when they are used individually is the main motivation to introduce and implement this novel technique. By this technique we can improve the QoS in MANET as compare to the proactive source routing .Our tests using computer simulation in Network Simulator 2 (ns-2) indicate that the delay in HSR is only a fraction of the delay of these baseline as well as light weight psr protocols, and HSR yields similar or better data transportation performance than these baseline as well as psr protocols.*

Keywords: Differential update, mobile ad hoc networks (MANETs), opportunistic data forwarding, proactive routing, Hybrid routing, routing overhead control, source routing, tree-based routing

1. Introduction

An ad-hoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any stand-alone infrastructure or centralized administration. Mobile Ad-hoc networks are self-organizing and self re-configuring multihop wireless networks where, the structure of the network changes dynamically.This is mainly due to the mobility of the nodes. Nodes in these networks utilize the same random access wireless channel, cooperating in a friendly manner to engaging themselves in multi-hop forwarding. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network [2].

In mobile ad-hoc networks where there is no infrastructure support as is the case with wireless networks, and since a destination node might be out of range of a source node transmitting packets; a routing procedure is always needed to find a path so as to forward the packets appropriately between the source and the destination. Within a cell, a base station can reach all mobile nodes without routing via broadcast in common wireless networks. In the case of ad-hoc networks, each node must be able to forward data for other nodes.This creates additional problems along with the problems of dynamic topology which is unpredictable connectivity changes [6].

MANETS rely on wireless transmission, a secured way of message transmission is important to protect the privacy of the data. An insecure ad-hoc network at the edge of an existing communication infrastructure may potentially cause the entire network to become vulnerable to security breaches. In mobile ad hoc networks, there is no central administration to take care of detection and prevention of anomalies [7]. Mobile devices identities or their intentions cannot be predetermined or verified. Therefore nodes have to cooperate for the integrity of the operation of the network. However, nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources. Various other factors make the task of secure communication in ad hoc wireless networks difficult include the mobility of the nodes, a promiscuous mode of operation, limited processing power, and limited availability of resources such as battery power, bandwidth and memory [2]. Therefore nodes have to cooperate for the integrity of the operation of the network. Nodes may refuse to cooperate by not forwarding packets for others for selfish reasons and not want to exhaust their resources.

MANET has a decentralized network infrastructure. MANET does not require a fixed infrastructure; thus, all nodes are free to move randomly MANET is capable of creating self-configuring and self-maintaining network without the help of a centralized infrastructure, which is often infeasible in critical mission applications like military conflict or emergency recovery. Minimal configuration and quick deployment make MANET ready to be used in emergency circumstances where an infrastructure is unavailable or unfeasible to install in scenarios like natural or human-induced disasters, military conflicts, and medical emergency situations Owing to these unique characteristics, MANET is becoming more and more widely implemented in the industry However, considering the fact that MANET is popular among critical mission applications, network security is of vital importance. Unfortunately, the open medium and remote distribution of MANET make it vulnerable to various types of attacks. For example, due to the nodes' lack of physical protection, malicious attackers can easily capture and compromise nodes to achieve attacks. In particular, considering the fact that most routing protocols in MANETs assume that every node in the network behaves cooperatively with other nodes an presumably not malicious, attackers can easily compromise MANETs by inserting malicious or no cooperative nodes into the network. Furthermore, because of MANET's distributed architecture and changing topology, a traditional centralized monitoring technique is no longer feasible in MANETs. In such case, it is crucial to develop an intrusion-detection system [10].

In present days, mobile communication has increased in usage and popularity. Tasks earlier handled by wired communication can now be performed using wireless devices offering different styles of technologies (such as IEEE 802.11, IEEE 802.16, Bluetooth and so on) that also provide for the user the advantage of the mobility. For some tasks, such as the ones involved during emergency network scenarios, the use of wireless devices is mandatory. Some relevant scenarios include coalition military operation, disaster relief efforts, and on-the-fly team formation for a common mission, such as search and rescue. In these situations, multiple groups and organizations may need to establish a way to communicate and collaborate to achieve a goal. For example, in a disaster relief effort, a military force may need to coordinate its activities with fire fighters, medical team, police force and other entities by sharing information without being concerned with the particular networking technologies that each group uses. Such tasks call for the development of an approach that enables end-to-end communications over those mobile wireless networks (networks containing wireless devices). The fundament of mobile ad-hoc networking is to support efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes, and any device (router or host) that implements the IP [8].

A mobile ad-hoc network (MANET) is a multi-hop ad-hoc wireless network where nodes can move in an arbitrary manner in the topology. Therefore, the network may experience rapid and unpredictable topology changes. Such networks have no given infrastructure; can be set up quickly in any environment and generally are likely composed of nodes with constrained capabilities (power level, processing capacity, and so forth). Moreover, this kind of network could be linked to other infrastructure networks constituting a mesh network. Several MANET routing protocol have been specified by the IETF MANET WG and other entities to achieve an easy deployment of these networks. Those protocols are based on different design philosophies and proposed to cope with certain requirements from different domains. An important scenario yet not fully explored is the deployment of a MANET with heterogeneous technologies with an efficient warranty for the communication of its node [9].

2. Related Work

In our paper, we have proposed the innovative technique to improve the data delivery that is Light Weight Hybrid source routing protocol (HSR). The problem of proactive and reactive methods when they are used individually is the main motivation to implement this novel technique. In our base method we have discussed the details with the benefits of proactive routing over reactive routing. In our base work we have successfully implemented the light weight proactive routing protocol, which reduces the overhead and improves the QOS in MANET. But from our literature work we have learned about proactive routing problems. In proactive routing, the nodes need to get the periodic update from the neighbors. Due to time dependency, the proactive routing will be get fails to build instant route when the link fails [8].

On another hand we have studied the details about on-demand routing protocol for MANET. The common reactive routing protocols takes more delay to build the new route, the reactive routing protocols uses the query and response message to build the routes. And the advantage of reactive routing is instance route formation when the link fails.

In our base work we have tested the proactive routing and we have enhanced the proactive routing protocol, and which can rebuild the route instantly. To improve the performance, we campaign the advantages of both routing techniques.

In our base PSR we have considered source routing, each node can update the details about neighbor node and filter the unnecessary packets. In our enhanced work we have added the link failure detection technique.

To get know the link availability information, we have used the cross layer operation. In that the node can use the basic CSMA/CA protocol to send the data with out collision. To make communication the CSMA/CA protocol uses the RTS/CTS/ACK sharing. For each data transmission, the node need to check the clearance detail from the receiver node by collecting the CTS signal and if the data is delivered in indented receiver then the sender can get proof of data reception by the acknowledgement sharing. In our enhanced method we have connected the MAC layer with the network layer. So the node can monitor the data delivery. If the data is not delivered or there in no clearance information from the neighbor receiver then MAC layer of sender can know the link is broken. Then the MAC layer will share this failure information to the network layer. Once the failure message is received in network layer then the routing information of the neighbor and destination which depends on the broken neighbor will be deleted [12].

Once the routing table is modified then route need to be updated if any packet is waiting in buffer for the indented destination with route.

So the node will checks the destination details with old hop count, if the old hop count is less then half of total route then the intermediate node will start the route searching by broadcasting route request. Due to the proactive nature of our base work, the nodes can get know the destination availability. So the intermediate node can give the reply back to the node which searches the route to destination. Once reply received the node can update new route and then the data sharing will be done.

In case, the node is far away from the destination, then the node will share the route error message to the neighbors about unreachable destination details. And if the error message is received from neighbor then the node will deletes the broken neighbors from the routing table. If the node is source of data packet then the node need to be start the searching process about broken destination [5].

So in our enhanced work we have added the reactive nature with proactive routing protocol to rebuild instant route. By this novel technique we can improve the QoS in MANET compare than the proactive source routing. We have named this innovative technique as Light Weight Hybrid source routing [8].

3. Design of Hybrid Source Routing

Essentially, PSR provides every node with a breadth-first spanning tree (BFST) of the entire network rooted at itself. To do that, nodes periodically broadcast the tree structure to their best knowledge in each iteration. Based on the information collected from neighbors during the most recent iteration, a node can expand and refresh its knowledge about the network topology by constructing a deeper and more recent BFST. This knowledge will be distributed to its neighbors in the next round of operation. On the other hand, when a neighbor is deemed lost, a procedure is triggered to remove its relevant information from the topology repository main-tained by the detecting node. Intuitively, PSR has about the some communication overhead. We go an extra mile to reduce the communication overhead incurred by PSR’s routing agents with the help of some extra mechanism added along with the features of PSR [4].

3.1.1 PSR Properties

The Properties of PSR bestowed in [4] and [1] has also been retained in this new Hybrid Source Routing Protocol. such as:-

a. Route Update
b. Neighborhood Trimming
c. Streamlined Differential Update

These properties helps the HSR in gaining all the advantages that the previous protocols were possessing and then the newer features can futher enhance the performance.

3.1.2 Network info Discovery

In this module, each node constructs the table, which will be used to store the neighbor node information. The table contains the packet generator id, and path detail, and time and hop count. The beacon message used to advertise the availability of node to other nodes. This message will be generated in periodic interval; the beacon message will be generated when the timer is triggered.

3.1.3 Source Routing

The beacon message contains the path to reach the generator. If any node receives the beacon message then the node has to update the details from the beacon packet and as well as it’s need to update the packet from neighbor table. The node can send the data with the total route information, so there is no need of intermediate node route update for the data packet. In, each subsequent iteration nodes exchange their spanning trees with their neighbors. From the perspective of node v, toward the end of each operation interval, it has received a set of routing messages from its neighbors packaging the BFSTs. Note that, in fact, more nodes may be situated within the transmission range of v, but their periodic updates were not received by v due to, for example, bad channel conditions[2].

3.1.4 Filtering

The periodically broadcast routing messages in PSR also double as “hello” messages for a node to identify which other nodes are its neighbors. When a neighbor is deemed lost, its contribution to the network connectivity should be removed; this process is called neighbor Filtering. By using the source routing, the node can update the intermediate node details. Based on the time interval of packet arrival, new packet generation will be cancelled. Piggybacking literally refers to carrying someone on one's back. Same idea is implemented in networking to improve the communication such as the process of sending data along with the acknowledgment is called piggybacking in networking [4].

Filtering is the process of avoiding the unnecessary packet transmission. In this module, after collecting the hello message interval we are comparing controlling packet generation time and hello message transmission time. If both are at same time we are going to delete hello message for avoiding overhead in network, and we are adding the information of hello message into control packets such as RREQ, RERR, and this phenomena is named as piggy backing. Using this extra information we can find the high efficient path for another node communication also, so this method is called as piggy backing with weighted transmission [9].

To improve this communication module, we are enhancing this paper work with the implementation of the event of hello and control packet generation at same time is very rare incident. In our model, message interval with small time variation also taking into account for providing more reliable transmission.

3.1.5 Route discovery

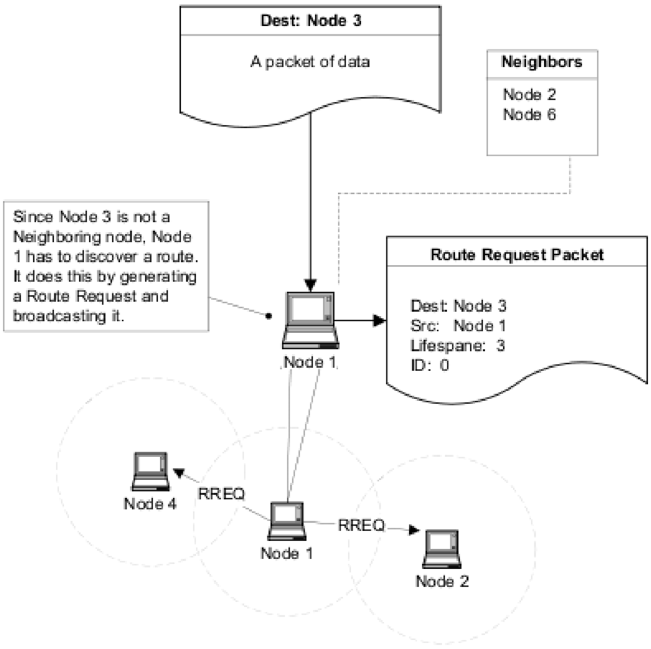
A destination nodes replies to a received RREQ packet with a route reply (RREP) packet in only the following three cases:

a. If the RREQ packet is the first to be received from this source nodes.
b. If the RREQ packet contains a higher source sequence number than the RREQ packet previously responded to by the destination nodes.
c. If the RREQ packet contains the same source sequence number as the RREQ packet previously responded to by the destination nodes, but the new packet indicates that a better quality route is available [3].

In this module, there are the two main processes taken into account.

a. Route request
b. Route reply

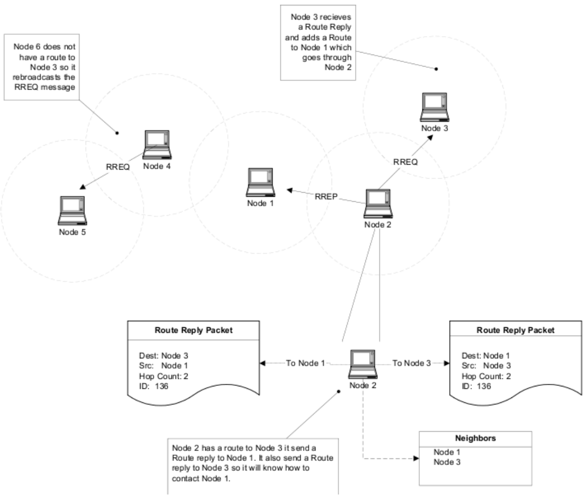
When one node needs to send a message to another node that is not its Neighbor it broadcasts a Route Request (RREQ) message. The RREQ message contains several key bits of information: the source, the destination, the lifespan of the message and a Sequence Number which serves as a unique ID [3].



Since Node 3 is not a Neighboring node, Node 1 has to discover a route. It does this by generating a Route Request and broadcasting it.

Figure 1: RREQ message [3]

In the example, Node 1 wishes to send a message to Node 3. Node 1's Neighbors are Nodes 2 + 4. Since Node 1 can not directly communicate with Node 3, Node 1 sends out a RREQ. The RREQ is heard by Node 4 and Node 2. When Node 1's Neighbors receive the RREQ message they have two choices; if they know a route to the destination or if they are the destination they can send a Route Reply (RREP) message back to Node 1, otherwise they will rebroadcast the RREQ to their set of Neighbors. The message keeps getting rebroadcast until its lifespan is up. If Node 1 does not receive a reply in a set amount of time, it will rebroadcast the request except this time the RREQ message will have a longer lifespan and a new ID number. All of the Nodes use the Sequence Number in the RREQ to insure that they do not rebroadcast a RREQ [3].



Node 6 does not have a route to Node 3 so it rebroadcasts the RREQ message

Node 3 recieves a Route Reply and adds a Route to Node 1 which goes through Node 2

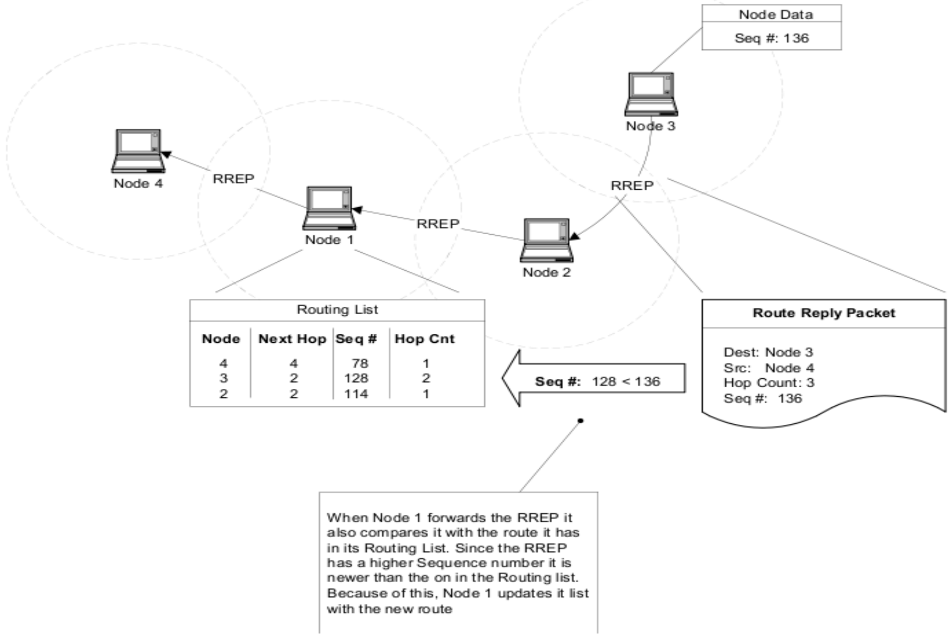
Node 2 has a route to Node 3 it send a Route reply to Node 1. It also send a Route reply to Node 3 so it will know how to contact Node 1.

Figure 2: Communication between node 1 and 3 [3]

In the example, Node 2 has a route to Node 3 and replies to the RREQ by sending out a RREP. Node 4 on the other hand does not have a route to Node 3 so it rebroadcasts the RREQ.

Sequence numbers serve as time stamps. They allow nodes to compare how "fresh" their information on other nodes is. Every time a node sends out any type of message it increases its own Sequence number. Each node records the Sequence number of all the other nodes it talks to. A higher Sequence numbers signifies a fresher route. This it is possible for other nodes to figure out which one has more accurate information.

In the example, Node 1 is forwarding a RREP to Node 4. It notices that the route in the RREP has a better Sequence number than the route in it's Routing List. Node 1 then replaces the route it currently has with the route in the Route Reply.



Routing List

Node	Next Hop	Seq #	Hop Cnt
4	4	78	1
3	2	128	2
2	2	114	1

When Node 1 forwards the RREP it also compares it with the route it has in its Routing List. Since the RREP has a higher Sequence number it is newer than the on in the Routing list. Because of this, Node 1 updates it list with the new route

Figure 3: RREP Message [3]

3.1.6 Algorithm

```
Initialize the Hello timer $H_{tim}$
In $n$ node, If $H_{tim}.Exip = True$
Initialize $Table_{neigh}.dst$
If $Filtering = False$
Create the broadcast packet $Pkt$
$pkt.src = n$
pkt.type= Hello.Norm
 $n \cup pkt.Path$
 Foreach $Nd \in Table_{neigh}$
 If $Nd \nexists pkt.neigh$
 Nd ∪ pkt . neigh
 Broadcast $pkt$
Resched $H_{tim}.Exip = Time_{now} + Rand_{time}$

If $Pkt$ recv in node $n$
        If $pkt.type = Hello.Norm$
         If $pkt$ not duplicate
         Update($Table_{neigh}$ ← pkt. info
         $n \cup pkt.path$
         Set time $filtering$
         Rebroadcast $pkt$
        If $pkt.type = Hello.Routerecov$
         If $Node_{failed} = Node\_active$
         Send $pkt\_reply$
         Else
         $Table_{neigh}$ = $Table_{neigh}$ \ $Node_{failed}$
        If $pkt.type = reply$
         Update($Table_{neigh}$ ← pkt. info
If $link = Failed$
        $Table_{neigh} = Table_{neigh} \setminus Node_{failed}$
        Send $Hello.Routerecov$
```

3.1.7 Route Repair

The major drawback of various routing protocols used in MANETs are their performance in the scenario of frequent link failures and handoffs. Most of the protocols have degrading performances in those circumstances. Inorder to cover those aspects a mechanism should be available which can play the part of route repair in case of link failure. An important and very crucial mechanism is proposed and implemented through HSR in experimental analysis in which the route repair routine is used to establish a connection with very less delay and packet loss between the source and the destination.

3.1.8 New Route

Another alternative that is added to this new protocol is that if the old route is not working due to the link failure or any other reason and repairing of that route is also not in the equations then a new route to the destination is found with the help of this New Route mechanism by the route request to the neighbouring tree structure.

4. Performance Evaluation

We study the performance of HSR using computer simulation with Network Simulator 2 version 2.34 (ns-2). We compare HSR against PSR [7], Simple Proactive Routing , which are three different routing protocols in MANETs, and as the PSR is evaluated in performance with the baseline protocols and is found much better on the prefixed parameters so we have compared our new protocol HSR with the PSR directly with varying network densities and node mobility rates. We measure the data transportation capacity of these protocols supporting the User Datagram Protocol (UDP) with different data flow de-ployment characteristics. Our tests show that the HSR offers much better data delivery performance and has the lower delay than its counterpart but overhead of HSR is indeed only a fraction of that of the baseline protocols with exception that the overhead is slightly on the higher side than that of the PSR. Nevertheless ,as it provides global routing information at link failure and handoffs which is a much vital issue in the real time environment. Here, we first describe how the experiment scenarios are configured and what measurements are collected.

4.1 Experimental Settings

Since many routing protocols performances are well known in the classic two-ray ground reflection propagation model, we select such a model as well in our simulation to present a consistent and comparable result.[1] Without loss of generality, we select a 1-Mb/s nominal data rate at the IEEE 802.11 links to study the relative performance among the selected protocols. With the default physical-layer parameters of the simulator, the transmission range is approximately 250 m, and the carrier sensing range is about 550 m [1].

We compare the performance of HSR with that of PSR and simple Proactive Routing. The reasons that we select these protocols is that they are not so different in nature. On one hand, PSR and Proactive are both proactive routing protocols, and HSR is also in this category but having additional on demand routing mechanism that is a reactive protocol. With PSR, it support source routing, which does not require other nodes to maintain forwarding lookup tables. All three baseline protocols are configured and tested out of the box of ns-2.with PSR and PSR was the better of all of them so here we compare our HSR directly with PSR only. Parameters which are taken for the comparison of the protocols are overall delay, network overhead and the packet data function/fraction. These comparisons are the key parameters through which it can be evaluated that the performance of the previous baseline protocols are superseded by the proposed routing protocol [1].

[1] In paper [8], PSR’s performance is also tested under a more realistic physical model with opportunistic forwarding techniques.

4.1.1 Comparison on Packet Delivery Fraction

On the basis of Packet delivery fraction, the HSR is much better in performance as compared to the PSR and even better than the normal proactive routing protocol. The calculation of the packet delivery fraction is accomplished by the percent of the total number of packets received successfully at the destination.

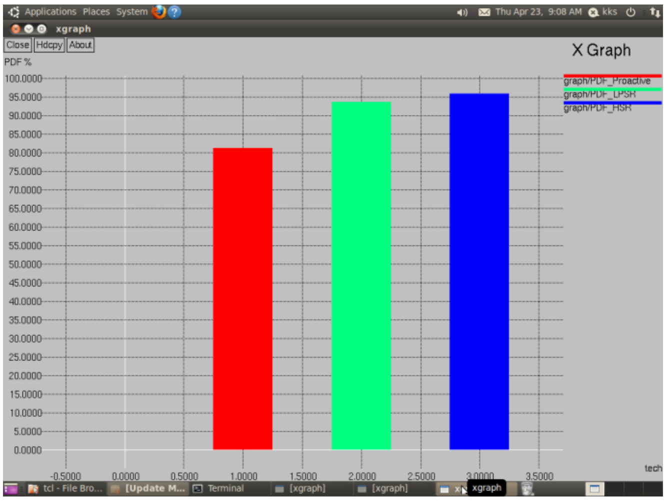


Figure 4: PDF of HSR, PSR and Proactive routing protocol

4.1.2 Comparison on Packet Delay

Packet Delay is one of the most prominent parameter that is used to evaluate the performance of various protocols and also is the tool for proper comparison of the protocols. On the basis of overall Packet Delay, the HSR is much better in performance as compared to the PSR and even better than the normal proactive routing protocol. As the packet delay is calculated by reducing the initial time with the time on which the packet reaches the destination. Calculation of the time is done in the milliseconds. In the consolidated output the results are shown in terms of seconds.

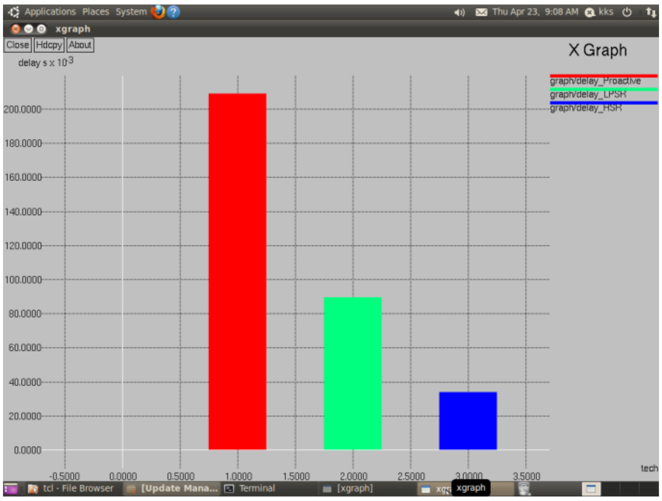


Figure 5: Time Delay of HSR, PSR and Proactive protocol

4.1.3 Comparison on Network Routing Overhead

On the basis of overall Routing Overhead, the HSR is lagging slightly in performance as compared to the PSR as the overhead increases slightly but still remains much better than the normal proactive routing protocol. The reason behind this is that the new route finding and route repair packets increase the control traffic which in turns increase the overhead of the network to a really small extent but this overhead performance more than acceptable on the cost of quick failure detection and recovery because present day real time environment contains frequent link failures and handoffs. So in those circumstances the HSR will perform better than the PSR.

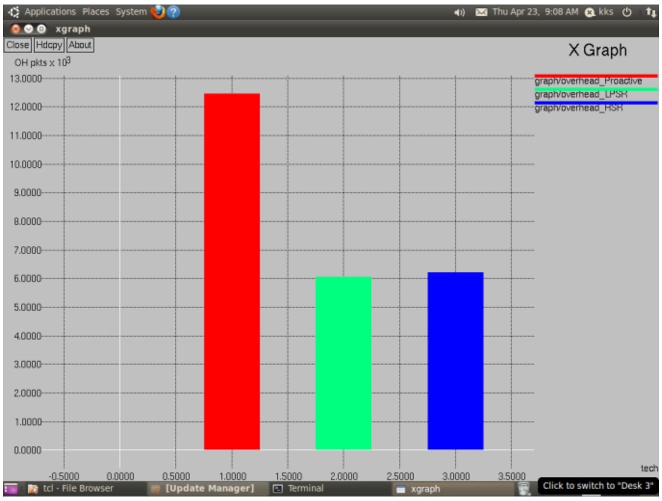
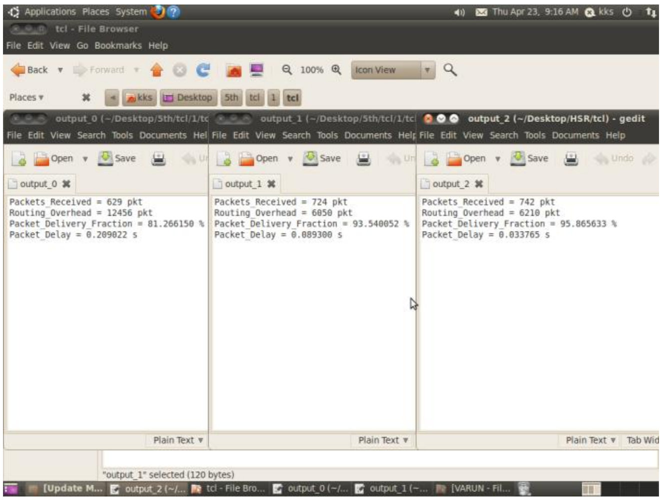


Figure 6: Network Overhead of HSR, PSR and Proactive protocol

4.1.4 Overall Comparison Statistics of the parameters

All the three parameters Network Overhead , Time Delay, and the Packet Data Function choosen for the comparison of the three protocols that is HSR , PSR and Proactive protocol are consolidated in a single statitics with the help of the data collected from the trace file and they are seen with the required and scrutinized format with the help of the AWK programming. The required statistics which proves the better performance of HSR over its ccounterparts are shown below:


tcl - File Browser
File Edit View Go Bookmarks Help
Back
Forward
100%
Icon View
Places
kks
Desktop
5th
tcl
1
tcl
output_0 (~/Desktop/5th/tcl/1/tc
output_1 (~/Desktop/5th/tcl/1/tcl
output_2 (~/Desktop/HSR/tcl) - gedit
File Edit View Search Tools Documents Help
Open
Save
Undo
Plain Text
Tab Wid

output_0
```
Packets_Received = 629 pkt
Routing_Overhead = 12456 pkt
Packet_Delivery_Fraction = 81.266150 %
Packet_Delay = 0.209022 s
```

output_1
```
Packets_Received = 724 pkt
Routing_Overhead = 6050 pkt
Packet_Delivery_Fraction = 93.540052 %
Packet_Delay = 0.089300 s
```

output_2
```
Packets_Received = 742 pkt
Routing_Overhead = 6210 pkt
Packet_Delivery_Fraction = 95.865633 %
Packet_Delay = 0.033765 s
```

"output_1" selected (120 bytes)

Figure 7: Statistics of HSR, PSR and Proactive Protocol

This output can also be represented as the contents of the table for better understanding.

Table 1: Comparison Statistics

Protocol	*Packets Received*	Packet Delivery Fraction	*Packet Delay*	*Routing Overhead*
Proactive	*629*	*81.266150%*	*0.209022 s*	*12456*
PSR	724	93.540052%	0.089300 s	6050
HSR	742	95.865633%	0.033765 s	6210

5. Conclusion

This Paper has been motivated by the need to support the frequent link failures and the handoffs in MANETs. In the simulation in this paper, we used Proactive routing to support traditional IP forwarding for a closer comparison with PSR and HSR, whereas both in the latter still carried source-routed messages. While alleviating forwarding nodes from table lookup, PSR's source routing is particularly vulnerable in rapidly changing networks. The reason for this is that, as a source-routed packet progresses further from its source, the path carried by the packet can become obsolete, forcing an intermediate node that cannot find the next hop of the path to drop the packet. This is fundamentally different from traditional IP forwarding in proactive routing with more built-in adaptivity, where the routing information maintained at nodes closer to the destination is often more updated than the source node.

As with many protocol designs, in many situations working on HSR, we faced tradeoffs of sorts. Striking such balances not only gave us the opportunity to think about our design twice but also made us understand the problem at hand better. In case of the Packet overhead calculation the HSR slightly lags behind as it has more overhead than PSR because of the increase in the control packets to detect and repair the link failures. Out of the scope of this paper it would be interesting if the directional routing (eg. GPS) is used which would even bring the overhead down by reducing the number of those control packets precisely to the needed quantity without compromising the performances of other parameters.

6. Future Scope

In our future work we will try to reduce the overhead.The overhead increased in our enhanced system due to the link rebuild. The link rebuilding is done by broadcasting the request to filter the extra request packet we will use position based routing scheme. With the growing popularity of positioning devices (e.g. GPS) and other localization schemes geographic routing protocols will become an attractive choice for use in mobile ad hoc networks. The underlying principle can used in geo protocols involves selecting the next routing hop from among a node's neighbors, which is geographically closest to the destination. Since the forwarding decision is based entirely on local knowledge, it obviates the need to create and maintain routes for each destination.

References

[1] PSR:A Lightweight Proactive Source Routing Protocol For Mobile Ad Hoc Networks. IEEE Transactions on Vehicular Technology, Vol. 63, No. 2, February 2014
[2] An Overview of MANET: History, Challenges and Applications, Mohit Kumar, Feb-Mar 2012.
[3] Z. Wang, Y. Chen, and C. Li, CORMAN: A novel cooperative oppor-tunistic routing scheme in mobile ad hoc networks, IEEE J. Sel. Areas Commun., vol. 30, no. 2, pp. 289–296, Feb. 2012.
[4] PSR: Proactive Source Routing in Mobile Adhoc Networks, IEEE Globecom 2011, Symposium.
[5] Routing Overhead as A Function of Node Mobility: Modeling Framework and Implications on Proactive Routing, Xianren Wu, Hamid R. Sadjadpour and J.J.Garcia-Luna-Aceves.
[6] Survey of Routing Protocols in Mobile Ad-hoc Network, Kevin C. Lee, Uichin Lee and Mario Gerla.
[7] A Survey on Wireless Mesh Networks, Ian F. Akyildiz, George Institute of Technology, Xudong Wang, Kiyon, Inc.
[8] Distributed Quality-of-Service Routing in Ad Hoc Networks, Shigang Chen and KlaraNahrstedt, Member, IEEE
[9] A Routing Strategy for Mobile Ad-hoc Networ in City Environments Christian Lochert, Hannes Hartenstein, Jing Tian, Holger Füßler Dagmar and Hermann Martin.
[10] Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks.
[11] "Optimized Link State Routing Protocol (OLSR)", Yuanzhu Peter Chen, February 2009.
[12] ExOR: Opportunistic Multi-Hop Routing for Wireless Networks, Sanjit Biswas and Robert Morris, 2005

Author Profile

Varun Pandey Pursuing Mtech degree in Computer Science and Engineering with specialization in Information Security from Disha Institute of Management and Technology, Raipur affiliated by Chattisgarh Swami vivekanand technical university , bhilai and received the B.E. degree in Information Technology Engineering from Government Engineering College, Jagdalpur affiliated by Chattisgarh Swami vivekanand technical university ,bhilai in 2009.

Somesh kumar Dewangan received his M. Tech in Computer Science and Engineering from RCET Bhilai, Chhattisgarh Swami Vivekanand Univerisity Bhilai , in 2009. Before that the MCA.Degree in Computer Application from MPBO University, Bhopal, India, in 2005. He is lecturer, Assistant Professor, associate professor, Disha Institute of Management and Technology, Chhattisgarh Swami Vivekanand Technical University Bhilai, India, in 2005 and 2008 respectively. He was a teaching assistant, lecturer, associate professor, with Department of Computer Science & Engineering, Pragati College, Pt. Ravishankar Shukla University Raipur 2002, 2004 and 2005 respectively. His research interests include digital signal processing and image processing, Natural Language Processing, Neural Network, Artificial Intelligence, Information and Network Security, Mobile Networking and Cryptography and Android based Application.