Volume 3 ▪ Issue 4 ▪ October 2011

Editor-in-Chief
Dr. Min Song

INTERNATIONAL JOURNAL OF COMPUTER NETWORKS (IJCN)

ISSN : 1985-4129
Publication Frequency: 6 Issues / Year

CSC PUBLISHERS
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER NETWORKS (IJCN)

VOLUME 3, ISSUE 4, 2011

EDITED BY
DR. NABEEL TAHIR

ISSN (Online): 1985-4129

International Journal of Computer Networks (IJCN) is published both in traditional paper form and in Internet. This journal is published at the website http://www.cscjournals.org, maintained by Computer Science Journals (CSC Journals), Malaysia.

IJCN Journal is a part of CSC Publishers
Computer Science Journals
http://www.cscjournals.org

INTERNATIONAL JOURNAL OF COMPUTER NETWORKS (IJCN)

Book: Volume 3, Issue 4, October 2011
Publishing Date: 05-10-2011
ISSN (Online): 1985-4129

IJCN Journal is a part of CSC Publishers
http://www.cscjournals.org

Published in Malaysia

Typesetting: Camera-ready by author, data conversation by CSC Publishing Services – CSC Journals, Malaysia

CSC Publishers, 2011

EDITORIAL PREFACE

The International Journal of Computer Networks (IJCN) is an effective medium to interchange high quality theoretical and applied research in the field of computer networks from theoretical research to application development. This is the third issue of volume second of IJCN. The Journal is published bi-monthly, with papers being peer reviewed to high international standards. IJCN emphasizes on efficient and effective image technologies, and provides a central for a deeper understanding in the discipline by encouraging the quantitative comparison and performance evaluation of the emerging components of computer networks. Some of the important topics are ad-hoc wireless networks, congestion and flow control, cooperative networks, delay tolerant networks, mobile satellite networks, multicast and broadcast networks, multimedia networks, network architectures and protocols etc.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 3, 2011, IJCN appears in more focused issues. Besides normal publications, IJCN intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

IJCN give an opportunity to scientists, researchers, engineers and vendors to share the ideas, identify problems, investigate relevant issues, share common interests, explore new approaches, and initiate possible collaborative research and system development. This journal is helpful for the researchers and R&D engineers, scientists all those persons who are involve in computer networks in any shape.

Highly professional scholars give their efforts, valuable time, expertise and motivation to IJCN as Editorial board members. All submissions are evaluated by the International Editorial Board. The International Editorial Board ensures that significant developments in computer networks from around the world are reflected in the IJCN publications.

IJCN editors understand that how much it is important for authors and researchers to have their work published with a minimum delay after submission of their papers. They also strongly believe that the direct communication between the editors and authors are important for the welfare, quality and wellbeing of the journal and its readers. Therefore, all activities from paper submission to paper publication are controlled through electronic systems that include electronic submission, editorial panel and review system that ensures rapid decision with least delays in the publication processes.

To build its international reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCN. We would like to remind you that the success of our journal depends directly on the number of quality articles submitted for review. Accordingly, we would like to request your participation by submitting quality manuscripts for review and encouraging your colleagues to submit quality manuscripts for review. One of the great benefits we can provide to our prospective authors is the mentoring nature of our review process. IJCN provides authors with high quality, helpful reviews that are shaped to assist authors in improving their manuscripts.

Editorial Board Members
International Journal of Computer Networks (IJCN)

TABLE OF CONTENTS

Volume 3, Issue 4, October 2011

Pages

Enhanced Multiple Routing Configurations For Fast IP Network Recovery From Multiple Failures

T. Anji Kumar *anji5678@gmail.com*
Dept. of IT/ UCEV
JNTUK
Vizianagaram, 535003, India

Dr MHM Krishna Prasad *krishnaprasad.mhm@gmail.com*
Dept. of IT/ UCEV
JNTUK
Vizianagaram, 535003, India

Abstract

Now a days, Internet plays a major role in our day to day activities e.g., for online transactions, online shopping, and other network related applications. Internet suffers from slow convergence of routing protocols after a network failure which becomes a growing problem. Multiple Routing Configurations [MRC] recovers network from single node/link failures, but does not support network from multiple node/link failures. In this paper, we propose Enhanced MRC [EMRC], to support multiple node/link failures during data transmission in IP networks without frequent global re-convergence. By recovering these failures, data transmission in network will become fast.

Keywords: Re-convergence, Routing Instability, Proactive Mechanism, Failure Recovery.

1. INTRODUCTION

The demand on the Internet has been increased by transforming it from a special purpose network to a common platform for many online services such as online transactions, entertainment and for other e-commerce applications. Internet suffers from slow convergence of routing protocols after a network failure. The central goal in the Internet is the ability to recover from failures [1]. Generally in IP networks, when a node/link failure occurs, the IGP routing protocols like OSPF are used to update the forwarding information based on the changed topology and the updated information is distributed to all routers in the network domain and each router individually calculates new valid routing tables.

The IGP convergence process is slow, as it is reactive i.e., it reacts to a failure after it has happened, and global i.e., it involves all the routers in the domain. This global IP re-convergence is a time consuming process, and a link/node failure is followed by a period of routing instability which results in packet drop. This phenomenon has been studied in both IGP [2] and BGP context [3], and has an adverse effect on real-time applications [4]. Though the different steps of the convergence of IP routing, i.e., detection, dissemination of information and shortest path calculation has been optimized, the convergence time is still too large for applications with real time demands [5]. Since most network failures are short lived [6], too rapid triggering of the re-convergence process can cause route flapping.

Multiple Routing Configurations [MRC] [7] is a proactive and local protection mechanism that allows fast recovery. When a failure is detected, MRC forwards the packets over pre-configured alternative next-hops immediately. Since no global re-routing is performed, fast failure detection mechanisms like fast hellos or hardware alerts can be used to trigger MRC without compromising network stability [8].The shifting of recovered traffic to the alternative link may lead to congestion and packet loss in parts of the network [9]. Ideally, a proactive recovery scheme should not only guarantee connectivity after a failure, but also do so in a manner that does not cause an

unacceptable load distribution. This requirement has been noted as being one of the principal challenges for pre-calculated IP recovery schemes [10].
MRC is a proactive routing mechanism, and it improves the fastness of the routing but it does not protect network from multiple failures. It can protect only from the single link/node failures. Hence, in this paper, using the time slot mechanism, we propose Enhanced Multiple Routing Configurations [EMRC] for fast multiple nodes/links failure recovery.

2. ENHANCED MULTIPLE ROUTING CONFIGURATIONS

2.1 Motivation

Even though the MRC provides an elegant and powerful hybrid routing framework, it doesn't protect the network from multiple failures and MRC is expensive as it requires more number of backup configurations. Hence, EMRC is designed to support multiple failures by utilizing time slot mechanism and less number of backup configurations.

2.2 Basic idea of EMRC

The basic idea of EMRC is as follows: Each source to destination transmission maintains original route. First shortest path is taken as an original route. These shortest paths are calculated by using the OSPF algorithm. Initially, data packets will be transmitted using this original route.

In this source to destination transmission, any sudden occurrence of node or link failure happens, total transmission is collapsed. At this time EMRC uses the timeslot mechanism. If a failure is occurred we will give the timeslot, means give some time to failure recovery before changing the route. Within the timeslot, if the failure is recovered then data is transmitted by using the original route only and if the failure is not recovered, then the data is transmitted by using the backup route and send the probing for failure recovery. During the backup route transmission, if failure is recovered, then backup route transmission is stopped and again reuses the original route. By reusing the original route we can improve the fastness of routing, since the backup route is longer than the original route.

2.3 EMRC Approach

EMRC is a threefold approach. First, a set of backup configurations are created, such that every network component is excluded from packet forwarding in one configuration. Second, for each configuration, a routing algorithm like OSPF is used to calculate configuration specific shortest paths and create forwarding tables in each router. Third, a forwarding process is designed which uses the backup configurations to provide fast recovery from a component failure.

2.4 Generating Backup Configurations

For generating backup configurations, we adopt an algorithm proposed by Hansen [7]. Our algorithm takes as input the directed graph *G* and the number *n* of backup configurations that is intended created. The algorithm will typically be run once at the initial start-up of the network, and each time a node or link is permanently added or removed. We use the notation shown in TABLE1.EMRC configurations are defined by the network topology, which is the same in all configurations, and the associated link weights, which differ among configurations. We formally represent the network topology as a graph $G = (N, A)$, with a set of nodes *N* and a set of links *A*. In order to guarantee single-fault tolerance, the topology graph *G* must be bi-connected. A configuration is defined by this topology graph and the associated link weight function:
Definition: A configuration C_i is an ordered pair (G,W_i) of the graph *G* and a function $W_i : A \rightarrow \{1, . . . ,W_{max}, W_r, \infty\}$ that assigns an integer weight $W_i(a)$ to each link $a \in A$.

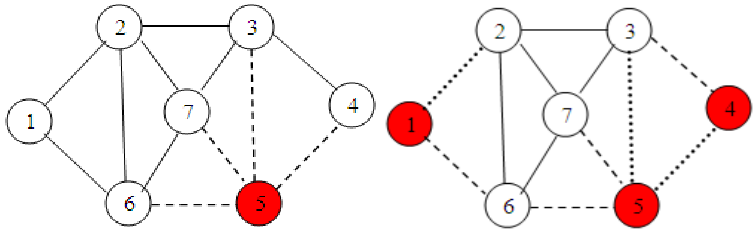
We distinguish between the normal configuration C_0 and the backup configurations C_i, $i > 0$. In the normal configuration C_0, all links have "normal" weights $W_0(a) \in \{1, . . . ,W_{max}\}$. We assume that C_0 is given with finite integer weights. EMRC is agnostic to the setting of the link weights in C_0. In the backup configurations, selected links and nodes must not carry any transit traffic. Still, traffic must be able to depart from and reach all operative nodes. These traffic regulations are imposed by assigning high weights to some links in the backup configurations.

Definition: A link $a \in A$ is isolated in C_i if $W_i(a)=\infty$.
Definition: A link $a \in A$ is restricted in C_i if $W_i(a) = W_r$.

$G = (N,A)$	Graph with set of nodes N and set of links A
C_i	The graph having link weights as in configuration i
S_i	The set of isolated nodes in configuration C_i
B_i	The backbone in configuration C_i
$A(u)$	The set of links from node u
(u,v)	The directed link from node u to node v
$P_i(u,v)$	A given shortest path between nodes u and v in C_i
$N(p)$	The nodes on path p
$A(p)$	The links on path p
$W_i(u,v)$	The weight of the link (u,v) in configuration C_i
$W_i(p)$	The total weight of the links in path p in configuration C_i
W_r	The weight of a restricted link
n	The number of backup configurations to be generated

TABLE 1: Notation

Isolated links do not carry any traffic. Restricted links are used to isolate nodes from traffic forwarding. The restricted link weight W_r must be set to a sufficiently high, finite value to achieve that. Nodes are isolated by assigning at least the restricted link weight to all their attached links. For a node to be reachable, we cannot isolate all links attached to the node in the same configuration. More than one node may be isolated in a configuration. The set of isolated nodes in C_i is denoted S_i, and the set of normal (non-isolated) nodes $S_n = N \setminus S_i$.



a) b)

FIGURE 1: Examples of isolated links and isolated nodes.

The purpose of the restricted links is to isolate a node from routing in a specific backup configuration C_i, such as node 5 in FIGURE 1.a. In many topologies, more than a single node can be isolated simultaneously. In the example in FIGURE 1.b. three nodes and three links are isolated. Restricted and isolated links are always given the same weight in both directions. EMRC guarantees single-fault tolerance by isolating each link and node in exactly one backup configuration. In each configuration, all node pairs must be connected by a finite cost path that does not pass through an isolated node or an isolated link. A configuration that satisfies this requirement is called valid.

Termination: The algorithm runs through all nodes trying to make them isolated in one of the backup configurations and will always terminate with or without success. If a node cannot be isolated in any of the configurations, the algorithm terminates without success. However, the algorithm is designed so that any bi-connected topology will result in a successful termination, if the number of configurations allowed is sufficiently high.

Complexity: The complexity of the proposed algorithm is determined by the loops and the complexity of the connected method. This method performs a procedure similar to determining whether a node is an articulation point in a graph, bound to worst case $O(|N|+|A|)$. Additionally, for each node, we run through all adjacent links, whose number has an upper bound in the maximum node degree Δ. In the worst case, we must run through all n configurations to find a configuration where a node can be isolated. The worst case running time for the complete algorithm is then bound by *O(n∆|N||A|)*.

2.5 Forwarding Procedure for EMRC

When we want to transmit any data from source to destination in the network, first we identify the source node and destination node, after that we look at the shortest path in between them in the original routing table and the data packets are transmitted by using that shortest route. When a data packet reaches a point of failure, the node adjacent to the failure, called the detecting node stops the transmission. At that time, the detecting node gives the timeslot to failure recovery before shifting to the backup route. Within the timeslot, if the failure is recovered then data is transmitted by using the original route only and if the failure is not recovered, then the detecting node is responsible for finding a backup configuration where the failed component is isolated. The detecting node marks the packet as belonging to this configuration, and forwards the packet. From the packet marking, all transit routers identify the packet with the selected backup configuration, and forward it to the egress node avoiding the failed component. Packet marking is most easily done by using specific values in the DSCP field in the IP header. If this is not possible, other packet marking strategies like IPv6 extension headers or using a private address space and tunneling [11] could be used. During the backup route transmission, the detecting node sends the probing signals for failure recovery and if failure is recovered, then backup route transmission is stopped and the data packets are transmitted by reusing the original route. By reusing the original route we can improve the fastness of routing, since the backup route is longer than the original route. If a failure lasts for more than a specified time interval, a normal re-convergence will be triggered. EMRC does not interfere with this convergence process, or make it longer than normal. However, EMRC gives continuous packet forwarding during the convergence, and hence makes it easier to use mechanisms that prevents micro-loops during convergence, at the cost of longer convergence times [12]. If a failure is deemed permanent, new configurations must be generated based on the altered topology.

Failed forwarding in node U towards node V

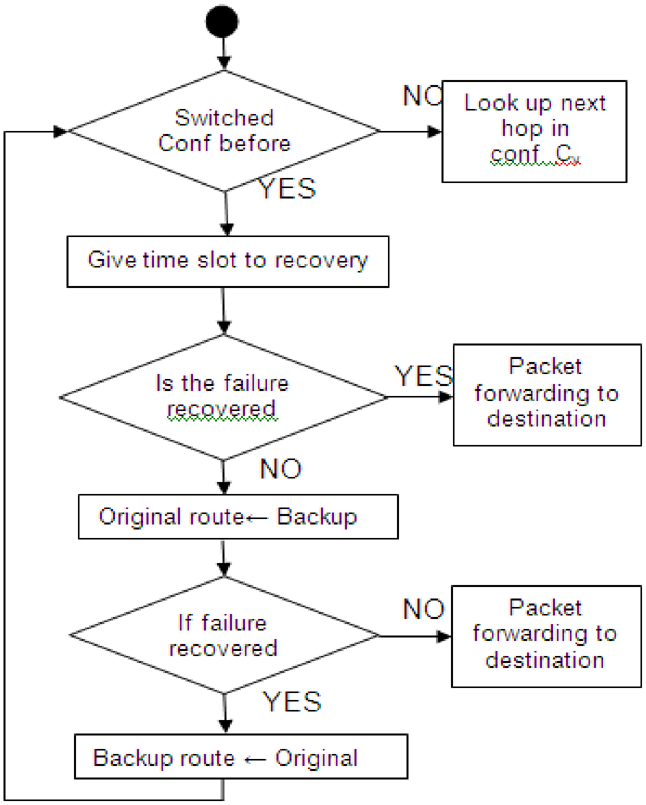


FIGURE 2: Packet forwarding state diagram.

2.6 Comparison of MRC and EMRC

EMRC is developed from MRC. So, all the processes in EMRC such as backup route finding, shortest path finding and forwarding is same as the MRC. These all are explained and compared by using the following in FIGURE 3 and FIGURE 4.

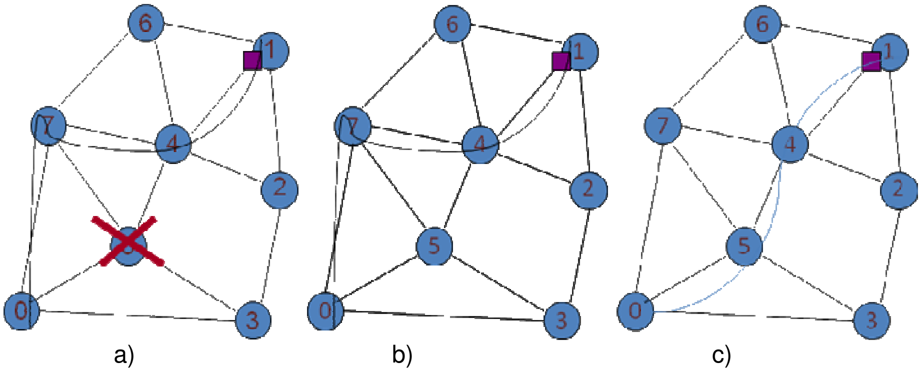
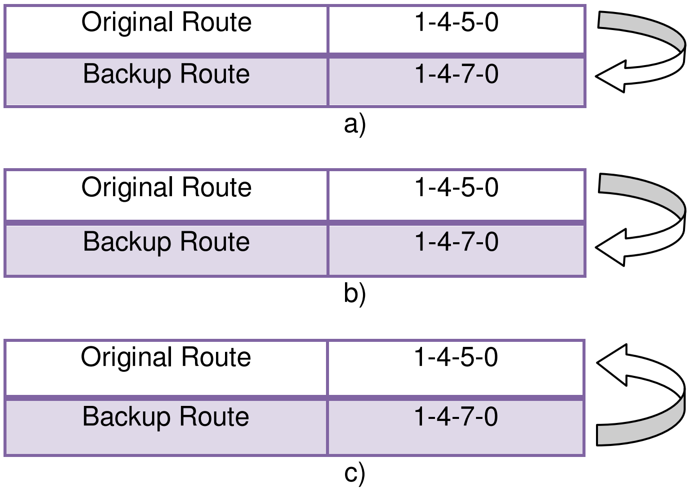


FIGURE 3: Selection of routes in MRC and EMRC a) At the time of failure occurrence in MRC and EMRC b) After the failure recovery in MRC c) After the failure recovery in EMRC.

As shown in FIGURE 3, we want to transmit the data from node 1 to node 0 by using the shortest path. Hence, in FIGURE 3 the source node is 1 and destination node is 0 and the shortest route is 1-4-5-0. 1-4-5-0 route is taken as a original route. Another route i.e. 1-4-7-0 is a backup configuration, where the node 5 is isolated. In original route, at middle of the transmission, any sudden occurrence of failure of node 5, data transmission is stopped at node 4. At that time MRC selects the backup route i.e. 1-4-7-0 and transmit the data to destination. By using the backup route, total transmission time increases and fastness of the routing decreases.



Original Route	1-4-5-0
Backup Route	1-4-7-0

a)

Original Route	1-4-5-0
Backup Route	1-4-7-0

b)

Original Route	1-4-5-0
Backup Route	1-4-7-0

c)

FIGURE 4: Selection of routes in MRC and EMRC a) At the time of Failure occurrence in MRC and EMRC b) After the failure recovery in MRC c) After the failure recovery in EMRC.

Using EMRC, at the time of failure of node 5, it gives the timeslot for failure recovery before shifting to the backup route i.e. 1-4-7-0. Within the timeslot if the failure is recovered, then the data is transmitted by using the original route i.e. 1-4-5-0 only. If the failure is not recovered, then the transmission is shifted to the backup route i.e. 1-4-7-0. During the time of backup route transmission we send the probes for failure recovery to the node 5. If at any time, failure is recovered, we again reuse the original route i.e. 1-4-5-0 and backup route transmission is stopped. In EMRC, by using the timeslot and reusing mechanism, we can improve both i.e. fastness of routing and as well as data transmission.

3. EXPERIMENTAL WORK

The Enhanced Multiple Routing Configurations (EMRC) scheme is implemented in C++ and TCL (Tool Command Language) by using “ns-allinone-2.30” tool and the whole experiment is carried out on the LINUX operating system.

The following FIGURE 5.1 shows the process of simulation in which we have to observe the simulation time as well as the nodes advertising themselves.

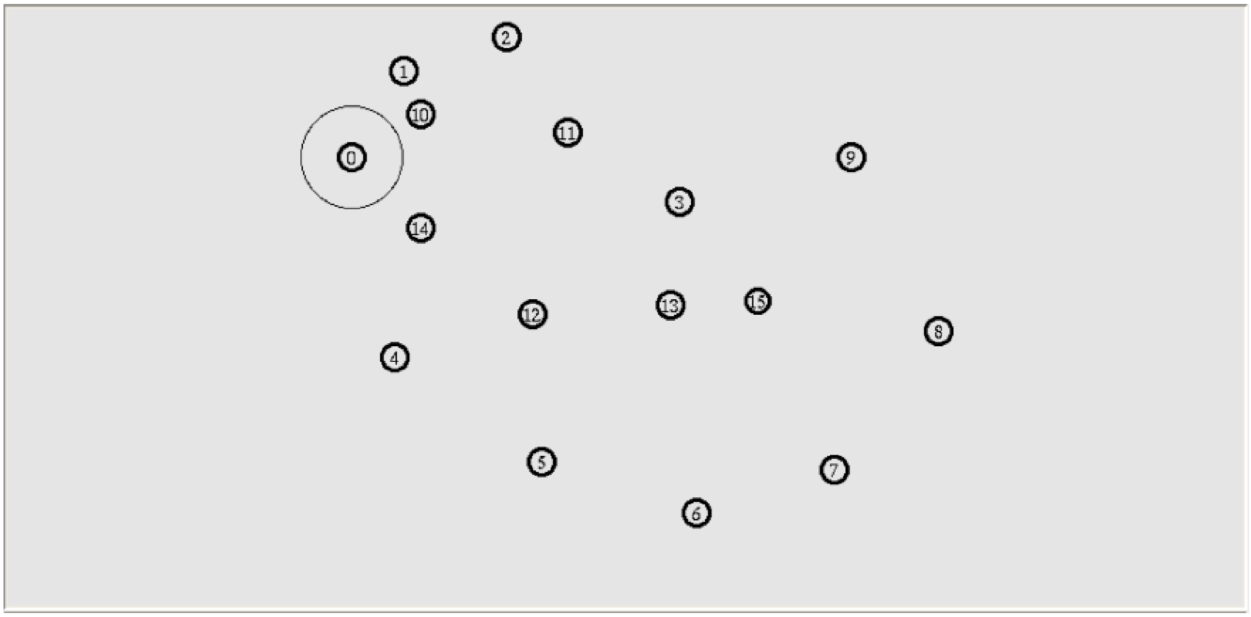


FIGURE 5.1: Screenshot of nodes advertising themselves.

The following FIGURE 5.2 shows the route discovery process to the destination. In this process every node tries to know the nearest neighbours for finding the shortest route.

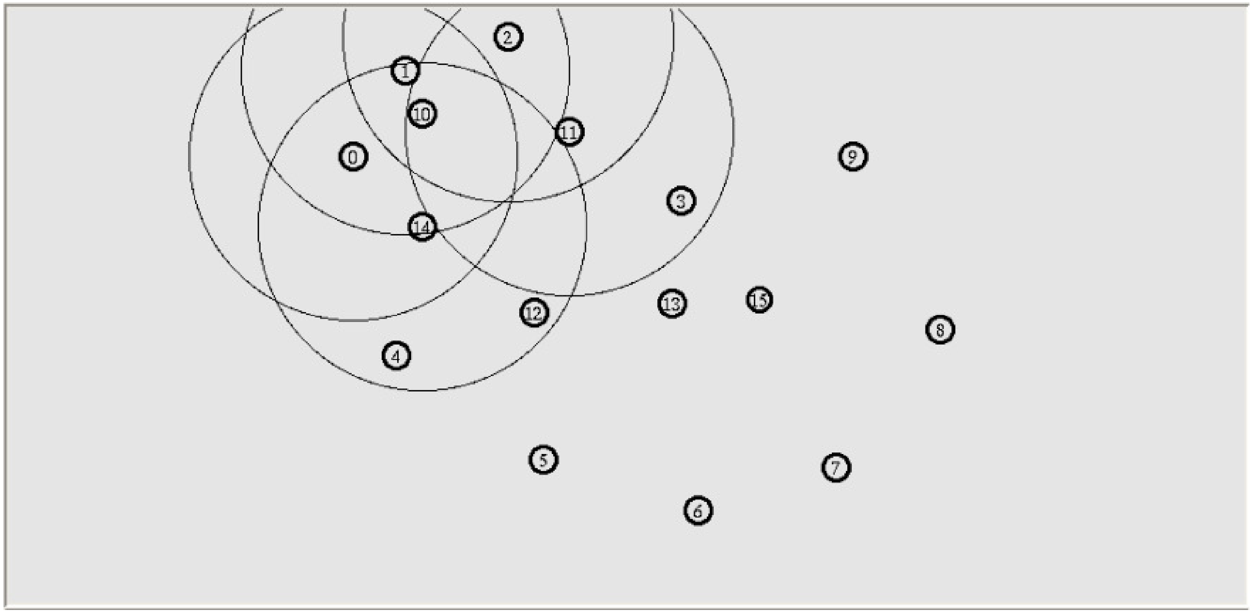


FIGURE 5.2: Screenshot of route discovery process.

The following FIGURE 5.3 represents the process of sending acknowledgements to senders after receiving request or data i.e., node 6 send acknowledgements to node 5 and node 13.

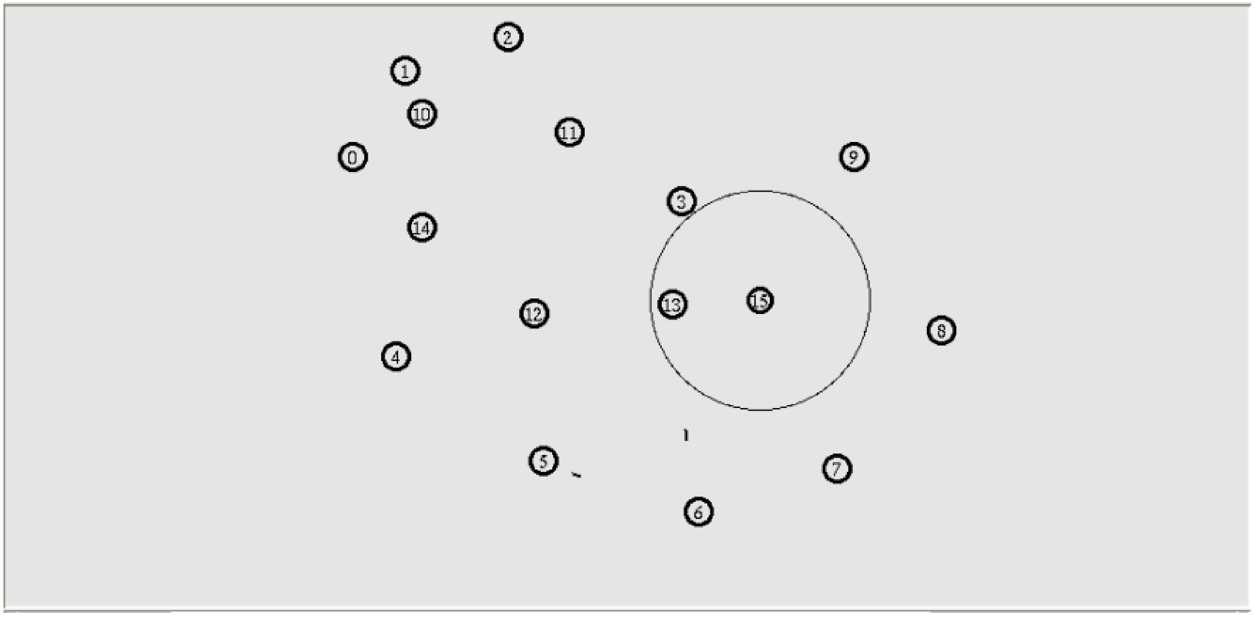


FIGURE 5.3: Destination node sends acknowledgements to the best routes.

The following FIGURE 5.4 represents the node 4 receiving the packet from node 14 and sending the acknowledgement to node 14. After that node 4 send data to node 5.

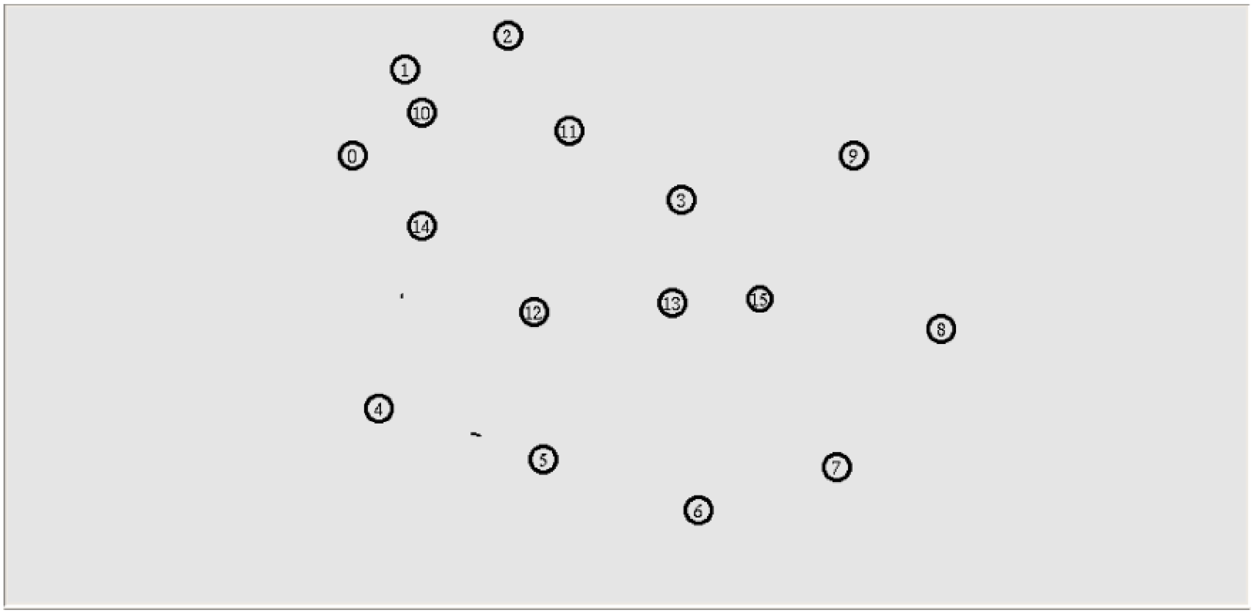


FIGURE 5.4: Receives the packet and send acknowledgement to the source.

From the following FIGURE 5.5, one can observe that the node 4 is out of range from node 14 i.e. node 4 is a failure node. So node 14 gives timeslot for failure recovery.

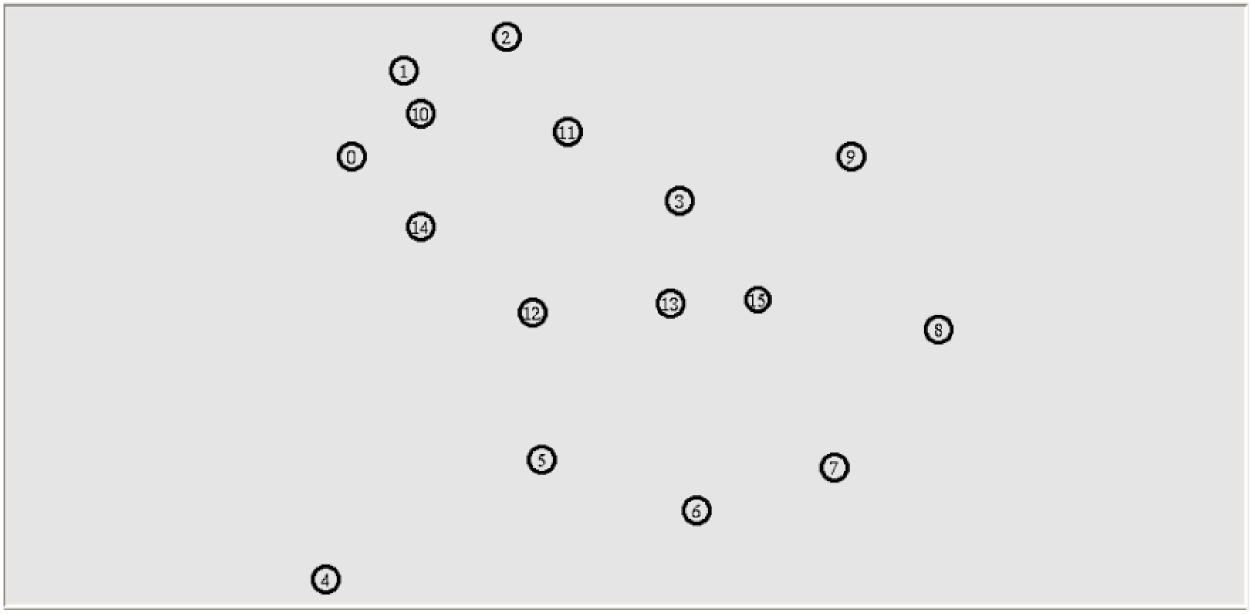


FIGURE 5.5: Movement of node 4 out of range of node14, breakage of best route.

From the following FIGURE 5.6, one can observe that within the timeslot, node 4 is not recovered from failure. So, the node 14 transmits the data by using the backup route and probes for node 4 from failure recovery.

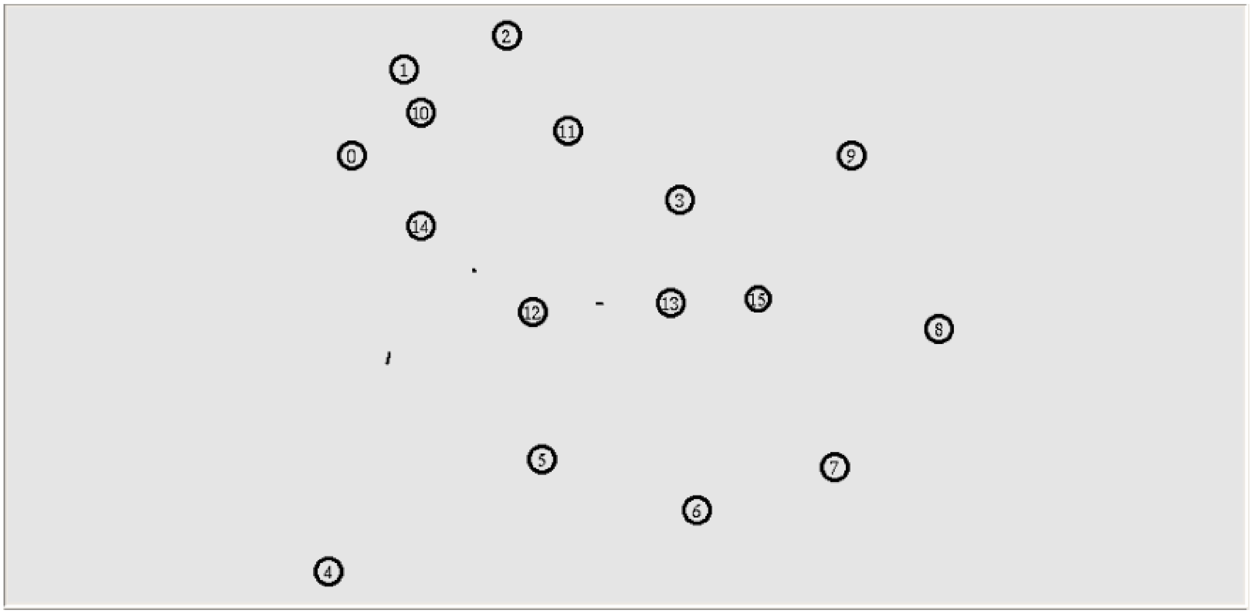
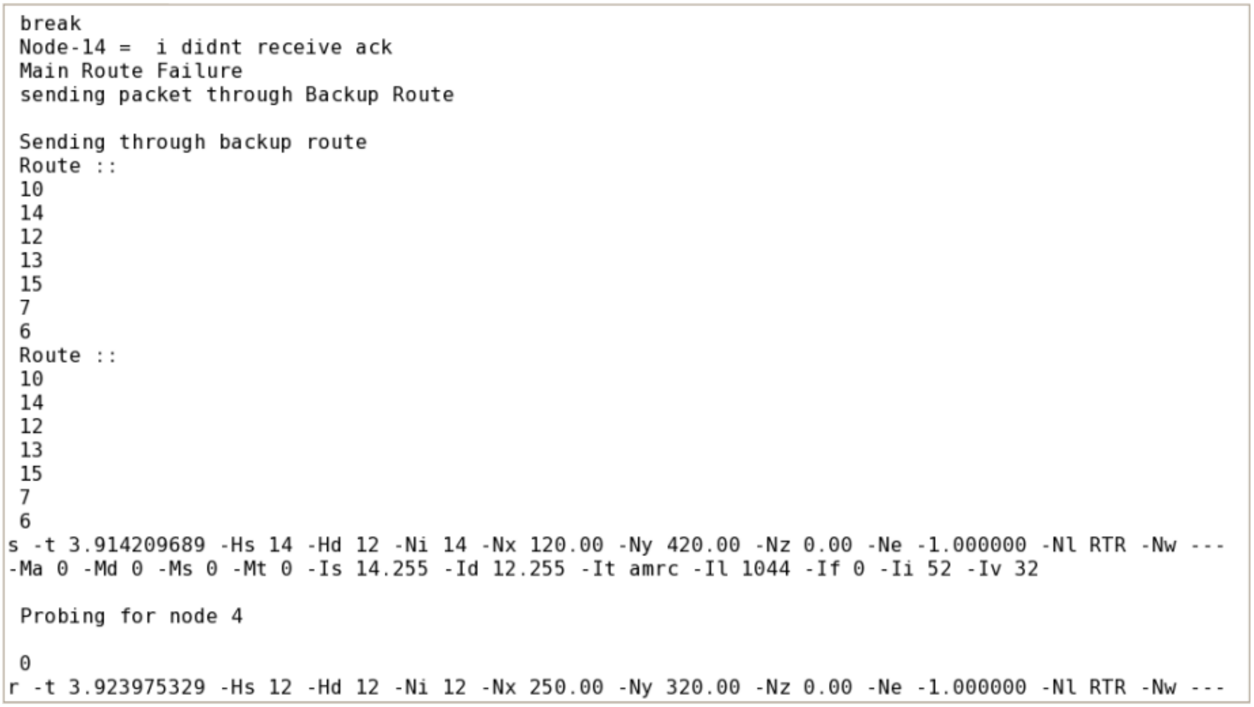


FIGURE 5.6: Selection of backup route and probing for node 4.

The following FIGURE 5.7 shows the selection of backup route in the trace file.



```
 break
 Node-14 =  i didnt receive ack
 Main Route Failure
 sending packet through Backup Route

 Sending through backup route
 Route ::
 10
 14
 12
 13
 15
 7
 6
 Route ::
 10
 14
 12
 13
 15
 7
 6
s -t 3.914209689 -Hs 14 -Hd 12 -Ni 14 -Nx 120.00 -Ny 420.00 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw ---
-Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 14.255 -Id 12.255 -It amrc -Il 1044 -If 0 -Ii 52 -Iv 32

 Probing for node 4

 0
r -t 3.923975329 -Hs 12 -Hd 12 -Ni 12 -Nx 250.00 -Ny 320.00 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw ---
```

FIGURE 5.7: Selection of backup route and probing for node 4, see from the trace file.

The following FIGURE 5.8 shows that after the recovery of node 4 from failure, it sends the reply to the node14 for the probing signal.

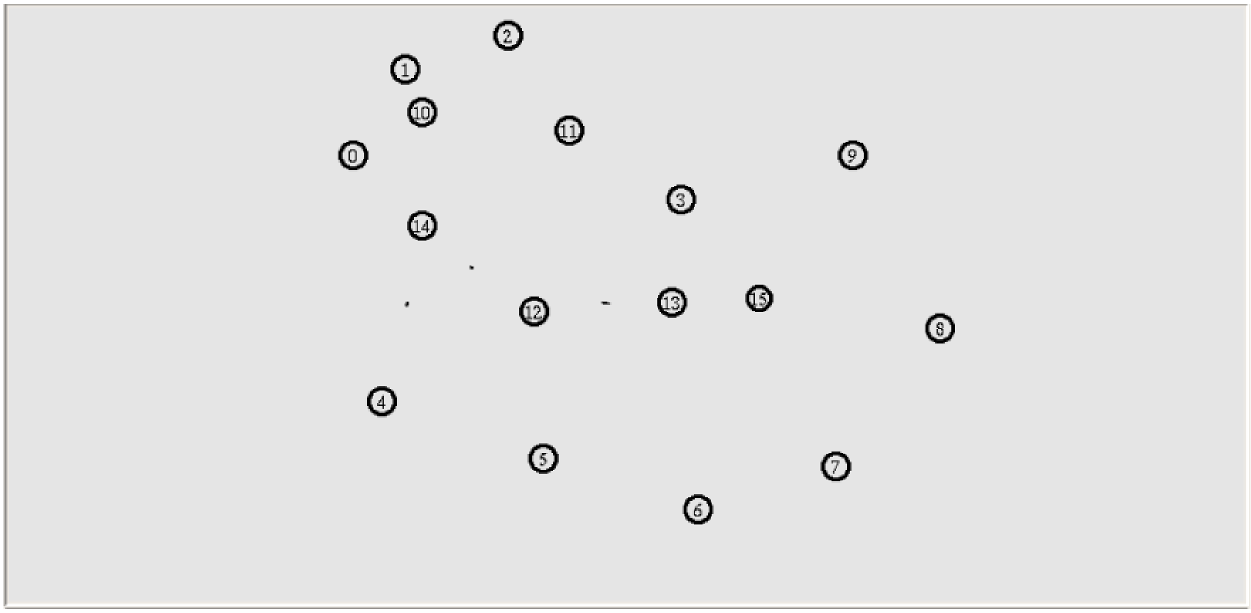


FIGURE 5.8: Sending the reply to node 14 for the probing signal after the node 4 is recovered from failure.

The following FIGURE 5.9 shows the use of recovered original route after the node 4 is recovered from failure.

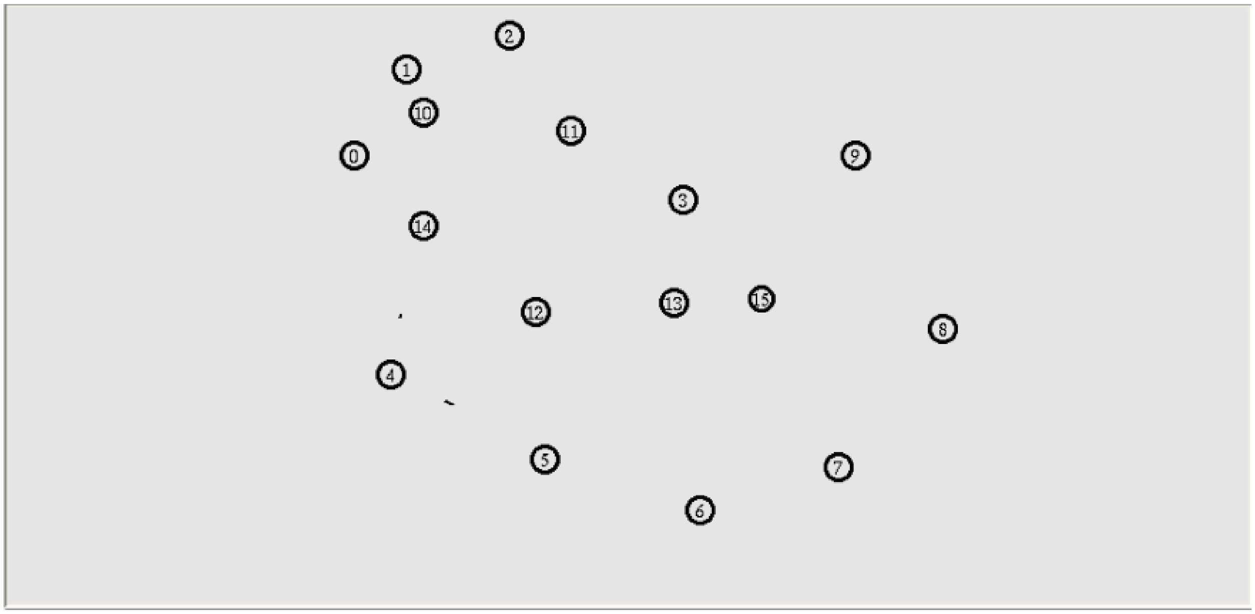
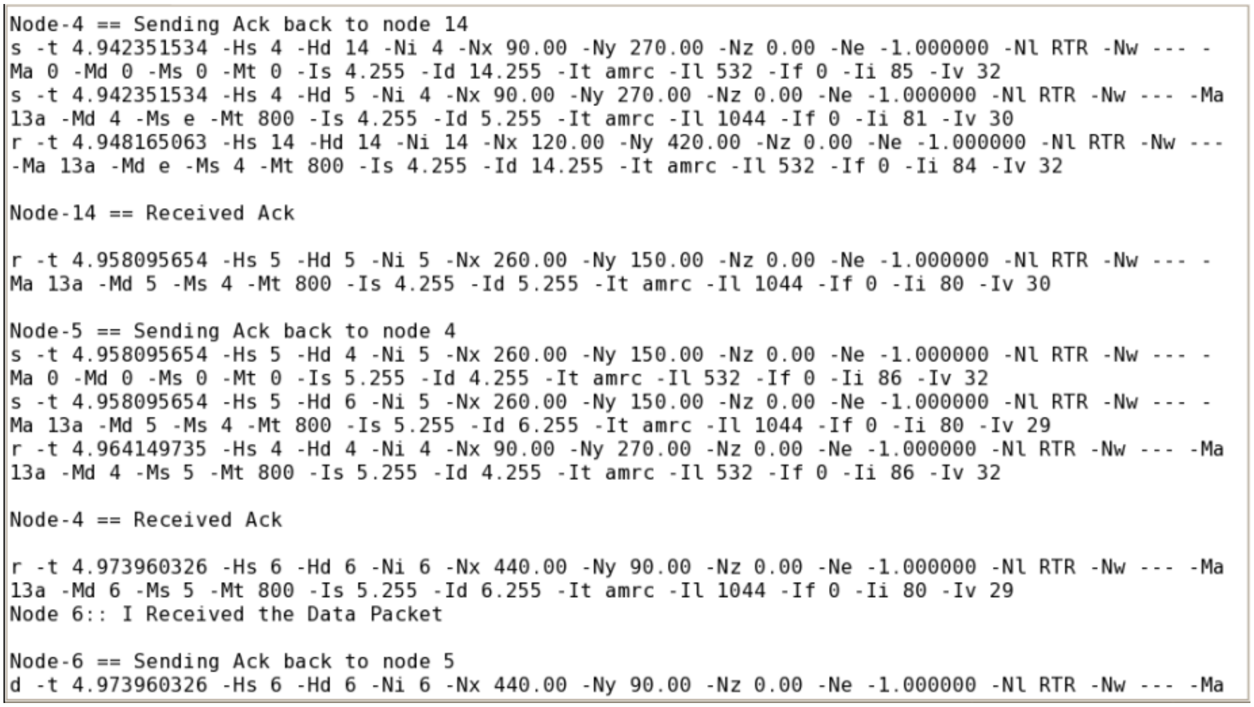


FIGURE 5.9: Reconstruction of the original route.

The following FIGURE 5.10 shows the reconstruction of original route after the node 4 failure recovery in the trace file.



```
Node-4 == Sending Ack back to node 14
s -t 4.942351534 -Hs 4 -Hd 14 -Ni 4 -Nx 90.00 -Ny 270.00 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -
Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 4.255 -Id 14.255 -It amrc -Il 532 -If 0 -Ii 85 -Iv 32
s -t 4.942351534 -Hs 4 -Hd 5 -Ni 4 -Nx 90.00 -Ny 270.00 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma
13a -Md 4 -Ms e -Mt 800 -Is 4.255 -Id 5.255 -It amrc -Il 1044 -If 0 -Ii 81 -Iv 30
r -t 4.948165063 -Hs 14 -Hd 14 -Ni 14 -Nx 120.00 -Ny 420.00 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw ---
-Ma 13a -Md e -Ms 4 -Mt 800 -Is 4.255 -Id 14.255 -It amrc -Il 532 -If 0 -Ii 84 -Iv 32

Node-14 == Received Ack

r -t 4.958095654 -Hs 5 -Hd 5 -Ni 5 -Nx 260.00 -Ny 150.00 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -
Ma 13a -Md 5 -Ms 4 -Mt 800 -Is 4.255 -Id 5.255 -It amrc -Il 1044 -If 0 -Ii 80 -Iv 30

Node-5 == Sending Ack back to node 4
s -t 4.958095654 -Hs 5 -Hd 4 -Ni 5 -Nx 260.00 -Ny 150.00 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -
Ma 0 -Md 0 -Ms 0 -Mt 0 -Is 5.255 -Id 4.255 -It amrc -Il 532 -If 0 -Ii 86 -Iv 32
s -t 4.958095654 -Hs 5 -Hd 6 -Ni 5 -Nx 260.00 -Ny 150.00 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -
Ma 13a -Md 5 -Ms 4 -Mt 800 -Is 5.255 -Id 6.255 -It amrc -Il 1044 -If 0 -Ii 80 -Iv 29
r -t 4.964149735 -Hs 4 -Hd 4 -Ni 4 -Nx 90.00 -Ny 270.00 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma
13a -Md 4 -Ms 5 -Mt 800 -Is 5.255 -Id 4.255 -It amrc -Il 532 -If 0 -Ii 86 -Iv 32

Node-4 == Received Ack

r -t 4.973960326 -Hs 6 -Hd 6 -Ni 6 -Nx 440.00 -Ny 90.00 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma
13a -Md 6 -Ms 5 -Mt 800 -Is 5.255 -Id 6.255 -It amrc -Il 1044 -If 0 -Ii 80 -Iv 29
Node 6:: I Received the Data Packet

Node-6 == Sending Ack back to node 5
d -t 4.973960326 -Hs 6 -Hd 6 -Ni 6 -Nx 440.00 -Ny 90.00 -Nz 0.00 -Ne -1.000000 -Nl RTR -Nw --- -Ma
```

FIGURE 5.10: Reconstruction of the original route, see from the trace file.

From the experimental results we obtained, the following graphs (FIGURE 6.1 and FIGURE 6.2) can be drawn which represents the comparison between MRC and EMRC for the time taken to transmit the data from source to destination.

In this graph, X-axis represents the packets that are transmitted in the network and Y-axis represents the time taken in seconds for transmission of each packet. The graph shows that the packets are transmitted using the backup route (long route) in MRC and original route (short route) in EMRC after link/node failure recovery which shows that the performance of the EMRC scheme is better than the MRC scheme.

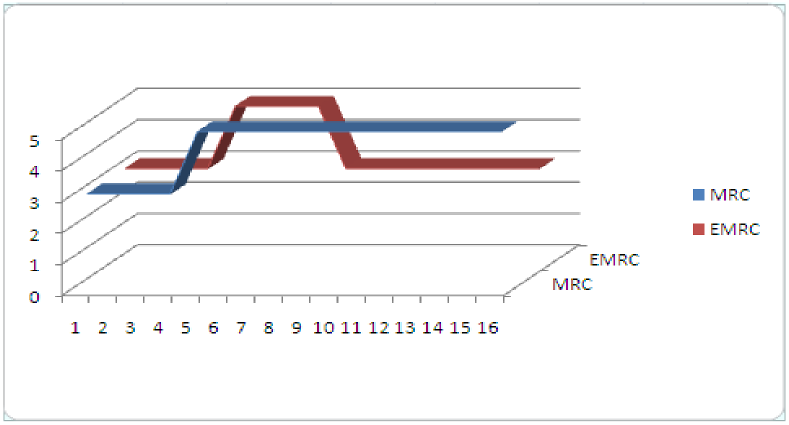


FIGURE 6.1: Time taken for transmission of each packet in MRC and EMRC.

In this graph, X-axis represents the number of packets transmitted in the network and Y-axis represents the average time taken for each packet transmission in seconds. The graph shows that the average time taken for each packet transmission in MRC is more than that of in EMRC which shows that the EMRC scheme is more efficient than the MRC scheme.

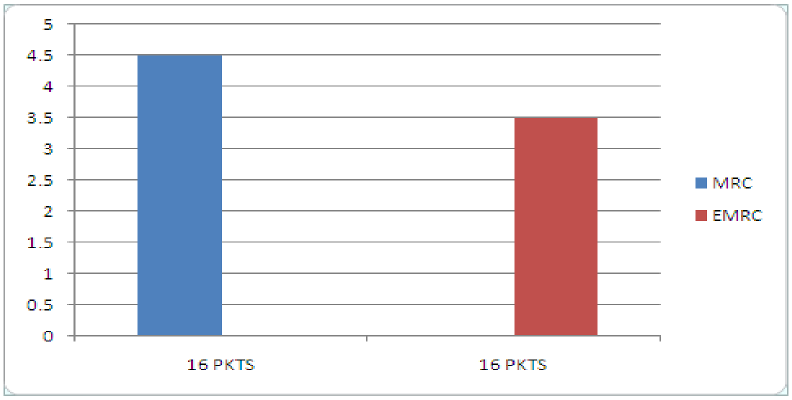


FIGURE 6.2: Average time taken for each packet transmission in MRC and EMRC.

4. CONCLUSIONS

Multiple Routing Configurations [MRC] recovers network from single node and link failures, but does not support for multiple node/link failures. Enhanced Multiple Routing Configurations [EMRC] is an approach to achieve fast recovery from multiple failures in IP Networks by using the timeslot mechanism. EMRC is based on providing the routers with additional routing information, allowing them to forward packets along routes that avoid a failed component. EMRC guarantees recovery from any failures in source to destination transmission, by calculating the alternate backup configurations in advance.

After the occurrence of original route failure, it is not discarded before completion of timeslot. Within the timeslot, if the failure is recovered, data is transmitted by using the original route. If the failure is not recovered; data is transmitted by using the backup route. During this transmission at any time, if the original route is recovered, data transmission using backup route is stopped and again shifted to the original route. By using this configuration one can improve the fastness of failure recovery and data transmission. EMRC thus achieves fast recovery with a very limited performance penalty.

EMRC does not take any measures towards a good load distribution in the network in the period when traffic is routed on the recovery paths. Existing work on load distribution in connectionless IGP networks has either focused on the failure free case or on finding link weights that work well both in the normal case and when the routing protocol has converged after a single link failure. *Hence, EMRC leaves more room for optimization with respect to load balancing*.

In spite of these encouraging results, this configuration is not to explain some of the issues those are like that this configuration can’t develop for some multiple data failures at a time like occurrence of isolated nodes. It is recovered by improving the efficiency of isolated nodes by using the isolated links as restricted links.

5. REFERENCES

[1] D. Clark. “The design philosophy of the DARPA internet protocols.” in Proc. SIGCOMM '88, 1988, pp. 106-114.

[2] A. Basu and J.G. Riecke. “Stability issues in OSPF routing.” in Proc. ACM SIGCOMM, 2001, pp. 225–236.

[3] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian. (2001, June). “Delayed internet routing convergence.” IEEE/ACM Trans. Networking, 9(3), pp. 293–306. Available: http://portal.acm.org/citation.cfm?doid=347059.347428 [Jan. 10, 2011]

[4] C. Boutremans, G. Iannaccone and C. Diot. “Impact of link failures on VoIP performance.” in Proc. Int. Workshop on Network and Operating System Support for Digital Audio and Video, 2002, pp. 63-71.

[5] P. Francois, C. Filsfils, J. Evans and O. Bonaventure. (July 2005). “Achieving sub-second IGP convergence in large IP networks.” SIGCOMM Comput. Commun. Rev. 35(3), pp. 35-44. DOI=10.1145/1070873.1070877. [Mar. 15, 2011]

[6] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.N. Chuah and C. Diot, (August 2008). “Characterization of failures in an IP backbone network,” IEEE/ACM Trans. Netw. 16(4) pp. 749-762. DOI=10.1109/TNET.2007.902727. [Mar. 25, 2011]

[7] A. F. Hansen, T. Cicic, S. Gjessing, A. Kvalbein, and O. Lysne. (April 2009). “Multiple Routing Configurations For Fast IP Network Recovery,” IEEE/ACM Trans. Netw. 17(2), pp. 473-486. DOI=10.1109/TNET.2008.926507. [June. 25, 2010]

[8] S. Nelakuditi, S. Lee, Y. Yu, Z.-L. Zhang, and C.-N. Chuah. (April 2007). “Fast local rerouting for handling transient link failures,” IEEE/ACM Trans. Netw. 15(2), pp. 359-372. DOI=10.1109/TNET.2007.892851. [Aug. 25, 2010]

[9] S. Iyer, S. Bhattacharyya, N. Taft, and C. Diot. “An approach to alleviate link overload as observed on an IP backbone.” in Proc. IEEE INFOCOM, 2003, pp. 406–416.

[10] S. Rai, B. Mukherjee, and O. Deshpande. (Oct. 2005). “IP resilience within an autonomous system: Current approaches, challenges, and future directions.” IEEE Commun. Mag. 43(10), pp. 142–149.

[11] S. Bryant, M. Shand, and S. Previdi. “IP fast reroute using not-via addresses.” Internet Draft (work in progress), draft-ietf-rtgwg-ipfrrnotvia-addresses-01, 2007.

[12] P. Francois, M. Shand, and O. Bonaventure. “Disruption free topology reconfiguration in OSPF networks.” in Proc. IEEE INFOCOM, 2007, pp. 89–97.

Traffic Control System by Incorporating Message Forwarding Approach

K.V.Ramana Ph.D *vamsivihar@gmail.com*
Professor/ CSE Department
Jawaharlal Nehru Technological University
Kakinada, 533003, India
.
Raghu.B.Korrapati Ph.D *raghu.korrapati@waldenu.edu*
Walden University

N. Pattabhi Ram *pattabhiram.nallam@gmail.com*
Jawaharlal Nehru Technological University
Kakinada, 533003,India.

K.Syam Kumari *shyamvarma28@gmail.com*
Jawaharlal Nehru Technological University
Kakinada, 533003,India

Abstract

During the last few years, continuous progresses in wireless communications have opened new research fields in computer networking, aimed at extending data networks connectivity to environments where wired solutions are impracticable. Among these, vehicular traffic is attracting a growing attention from both academia and industry, due to the amount and importance of related distributive applications to mobile entertainment. VANETs are self-organized networks built up from moving vehicles, and are part of the broader class of MANETs. Because of these peculiar characteristics, VANETs require new networking techniques, whose feasibility and performance are usually tested by means of simulation. In order to meet performance goals, it is widely agreed that VANETs must rely heavily on node-to-node communication. In VANET, each vehicle acts as a node and communicates with other vehicles within the range or communicates with base stations. The main idea is to deploy a wireless communication network that has a capability of sending and receiving messages between transmitter and mobile devices in the particular network. Results can be shown using an effective VEINS Simulator. This Simulator can produce detailed vehicular movement traces and can simulate different traffic conditions through fully customizable scenarios. The Framework is expected to be employed using such simulator that makes use of traffic modulator, network simulator and coupling module that integrates the traffic and network.

Keywords: Networking Techniques, VANETs, Node-to-node Communication, Modulator.

1. INTRODUCTION

Road and traffic safety can be improved if drivers have the ability to see further down the road and know if they are approaching a traffic jam. The productivity of vehicles is in greater proportion to the number of roads. Under these circumstances, Researches have been done to improve the road safety like safe driving education, roads expansion and speed management etc., has not made much impact. As the road accidents increasing day by day there is much need to think of new approaches like, if drivers and vehicles communicate with each other and with roadside base stations. It is possible to build a multi-hop network among several vehicles that have communication devices. Communication between vehicles [1] can be used to realize driver support and active safety services like collision warning, up-to-date traffic and weather information or active navigation systems.

Vehicular Ad-hoc Networks (VANETs) represent a rapidly emerging, particularly challenging class of Mobile Ad Hoc Networks (MANETs). VANETs are distributed self-organizing communication networks built up from travelling vehicles, and are thus characterized by: (a) trajectory-based movements with prediction locations and time-varying topology, (b) varying number of vehicles within dependent or correlated speeds, (c) fast time-varying channel (e.g., signal transmissions can be blocked by buildings), (d) lane-constrained mobility patterns (e.g., frequent topology partitioning due to high mobility), and (e) reduced power consumption requirements.

VANETs have very high speed and limited degree of freedom in nodes movement patterns. Such particular features often makes standard network protocols are inefficient in VANETs. Thus there is a huge impact in the deployment of VANET technologies and development of communication protocols in vehicular networks. Hence VANETs leads to the need for new system concepts and information dissemination protocols. In addition, new approaches for data and communication security have to be designed to fit the specific network needs and to guarantee reliable and trustworthy services.

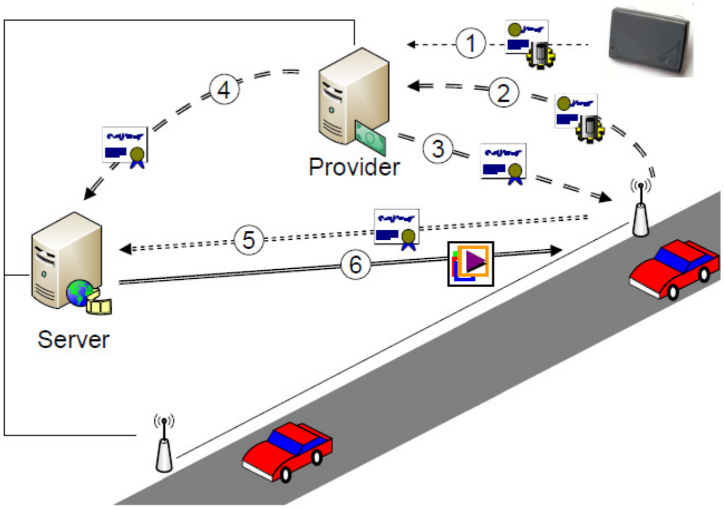


FIGURE 1: Scenario depicts the snapshot of the Vehicular Adhoc Network

(1) User registers device with provider (2) User sends payment/service request
(3) Provider issues temporary credentials
(4) Provider informs server of service purchased and temporary credentials
(5) User requests service using temporary credentials (6) Server delivers content.

Above figure demonstrates the illustration of payment and service requests and temporary credentials. One of the main challenges posed by VANETs simulations is the faithful characterization of vehicular mobility [2][3] at both macroscopic and microscopic levels leading to realistic non-uniform distributions of cars and velocity, and unique connectivity dynamics[4][5][6]. The new approach to solve this problem in the current transportation system is implementing the wireless technology. In VANET the vehicles exchange the information while moving which gives the driver an additional time to react accordingly. The communication in a vehicle is of 2 types: Intra-Vehicle communication and Inter-Vehicle communication. Intra-Vehicle communications references the communication which occurs within vehicle and inter-Vehicle communication represents the communication between the vehicle and roadside units.

In this paper we will focus on implementing the inter-Vehicle communication and analyse the benefits we can bring to the currents transportation system. Security of the VANET is least bothered in the contended methodology. Since, this methodology does not deal with the inner details of the transmitting signals. One way to effectively adapt the security techniques in VANET is by incorporating Certificate Distribution Technique [7] which makes use of the third party to monitor and distribute the certificates. The realistic implementation of VANET is much costly and challenging. Thus, simulation is much practical and cost effective [8],[9]. In this work, a simulator called VENIS (vehicles in network simulation) is used to simulate the real time scenario.

2. RELATED WORK

In traffic applications, we need to simulate the combined performance of wireless protocols and traffic conditions using wireless network simulators and traffic network simulators.

2.1 Vehicular Network Access or Intelligent Vehicular Ad Hoc Networks

InVANET helps in defining safety measures in vehicles, streaming communication between vehicles, infotainment and telematics. InVANET can be used as part of automotive electronics, which has to identify an optimally minimal path for navigation with minimal traffic intensity. The system can also be used as a city guide to locate and identify landmarks in a new city. The main interest is in applications for traffic scenarios, mobile phone systems, sensor networks and future combat systems. Recent research has focused on topology related problems such as range optimization, routing mechanisms, or address systems, as well as security issues like traceability or encryption. In addition, there are very specific research interests such as the effects of directional antennas for InVANETs and minimal power consumption for sensor networks. Most of this research aims either at a general approach to wireless networks in a broad setting or focus on an extremely specific issue.

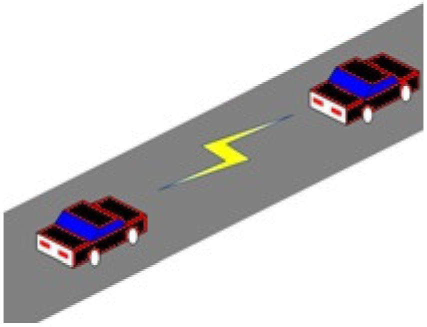


FIGURE 2: Illustration of Car–to–Car communication.

Above figure demonstrates the module of node to node communication[10]. In VANETs each and every node can be treated as vehicles.

2.2 Incorporating Wireless Communications in Traffic Network Simulators

In this section, we explain the work done towards providing a complete system that is proficient at simulating the vehicular communication network as a whole. Two approaches were followed towards this goal. The first one is Merging Traffic and Wireless Simulators which is concerned with integrating two currently available simulators. Second one is Creating New Platform. It involves the creation of a standalone platform which combines both capabilities from scratch. Prior to the idea of merging two existing simulators, several research papers have proposed their own platforms that combine the capabilities of traffic networks and wireless communication simulators, in an attempt to provide a vehicular communication network platform.

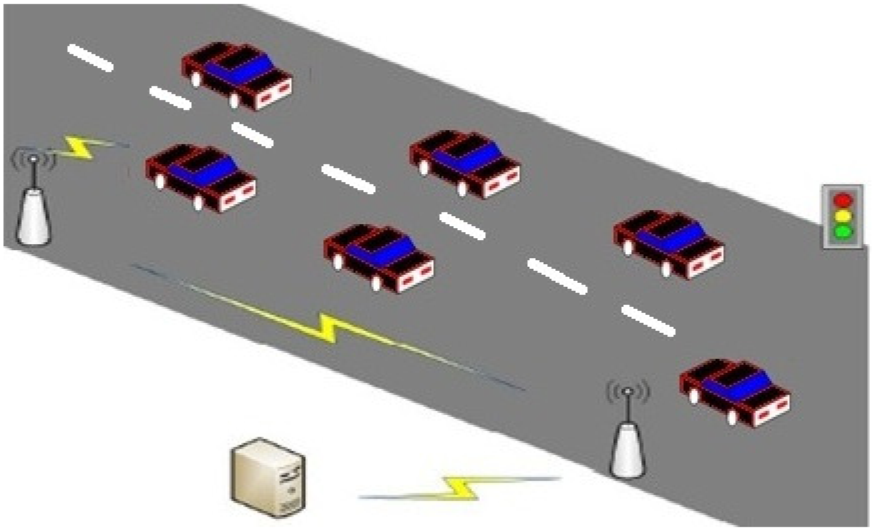


FIGURE 3: Scenario depicting communication between Monitoring server and Scanners that incorporates transmittors.

Above figure demonstrates the communication module that establishes interaction between Monitoring server and Scanners.

2.3 Freeway Management System

A freeway is a limited access highway with high speeds, and ramps to allow entry and exit which may or may not have tolls. Freeways [11] were originally intended to provide free-flowing, high-speed traffic flow over long distances.

Congestion occurs on a freeway when demand exceeds capacity. When this occurs on a freeway section, a bottleneck exists. A bottleneck occurs when:

- Demand increases to a level greater than capacity, or
- Capacity decreases to a level less than demand.

To understand what causes freeway congestion, to understand the theory of traffic flow. Important traffic flow parameters are

- Flow (V) = Number of vehicles passing a certain point during a given time period, in vehicles per hour (veh / hr)
- Speed (S) = The rate at which vehicles travel (mph)
- Density (D) = Number of vehicles occupying a certain space. Given as veh / mi.

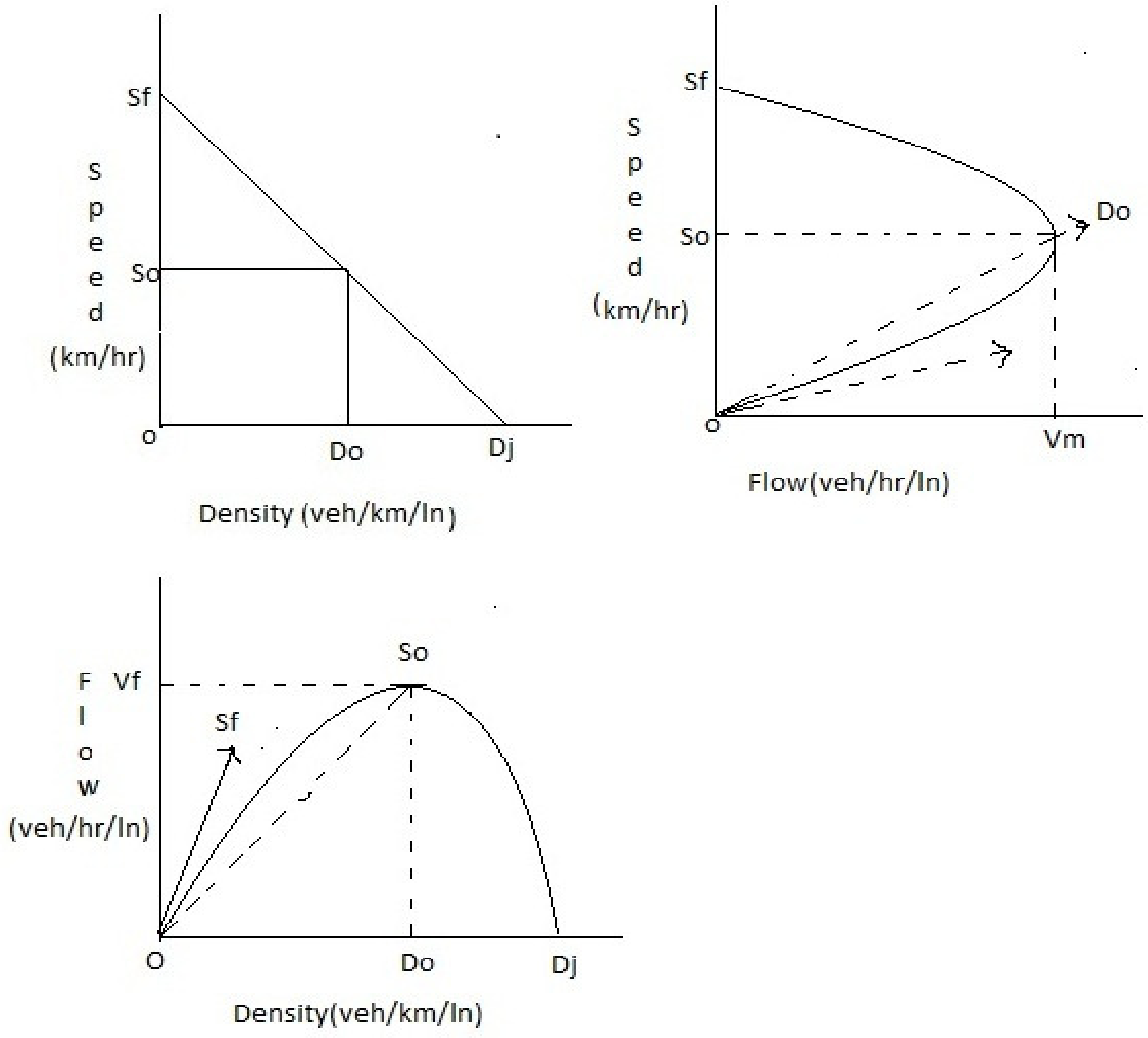


FIGURE 4: Depicts the analysis among various parameters that reflects the performance of Contended methodology

Above figure illustrates the Free flow speed (Sf) occurs during light traffic conditions. When density reaches the critical density (D0), the freeway reaches its maximum flow (Vm). Speed at that point is decreased to S0. When the density increases beyond the critical density, the flow actually decreases, until the density reaches the jam density (Dj), where the flow becomes zero and all traffic is stopped. When the density is below the critical density, the flow is said to be stable, or uncongested. When the density exceeds the critical density, the flow is said to be congested, or unstable, and the freeway capacity decreases. Because more vehicles are processed when the flow is stable, it is best for the density to be as close as possible to, but below the critical value so the freeway can operate at its full capacity.

3. METHODOLOGY

3.1 Modules

The proposed work has been segmented into three phases. The first phase deals with building network environment. The second phase establishes communication among the transmitters, scanners, vehicles, mobile devices. The third phase will explain about the mechanism to forward message which contains the information of vehicle deviation , which avoids the influence of abnormal activities, to control the traffic i.e., by scanning the vehicles through scanner and enabling the transmit to forward the message efficiently.

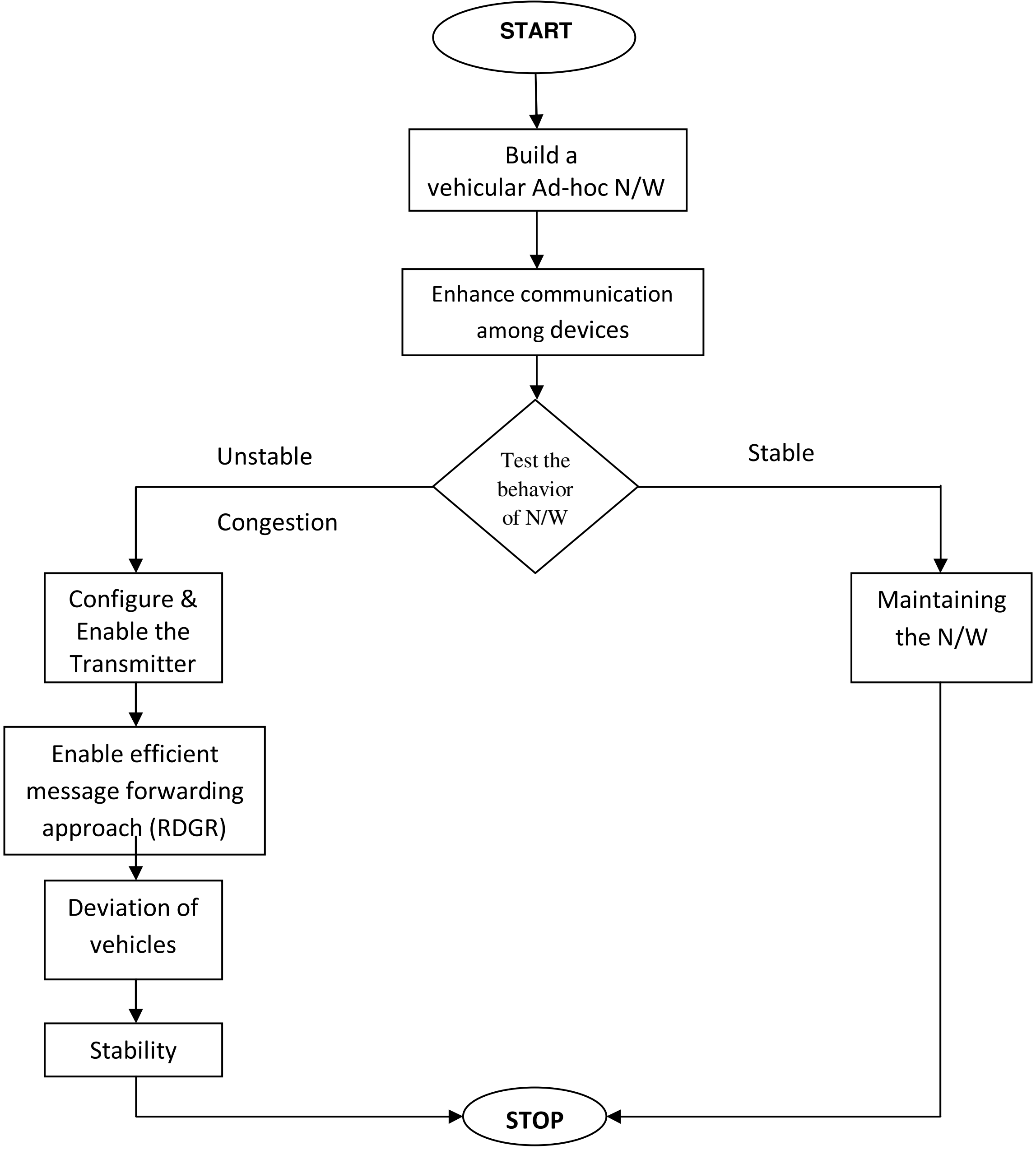

START
Build a vehicular Ad-hoc N/W
Enhance communication among devices
Test the behavior of N/W
Unstable
Congestion
Stable
Configure & Enable the Transmitter
Enable efficient message forwarding approach (RDGR)
Deviation of vehicles
Stability
Maintaining the N/W
STOP

FIGURE 5: Framework depicting the contended methodology.

Above figure illustrates the framework of the contended methodology and the modules implementing it.

3.1.1 Build Network

In the first stage, create VANET with a wide range. VANET is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other. The property of Mobile Ad-hoc network can be achieved by making the cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. In the network, vehicles information can be viewed on electronic maps using the internet. In this work SUMO simulator is used for mobility.

3.1.2 Establish Communication

In the second stage, here communication is established in between transmitter and vehicles. Communication capabilities in vehicles are the basis of an envisioned in VANET. Vehicles are enabled to communicate via access points (vehicle-to-roadside, V2R). Vehicular communication is expected to contribute to safer conditions and more efficient roads by providing timely information to drivers, and also to make travel more convenient. V2R provides better service for sparse networks and long distance communication. Providing vehicle-to-roadside communication can considerably improve traffic safety and comfort of driving and traveling.

3.1.3 Core Module of the Application

After designing the communication module, the next module to be taken into consideration is designing the core part of the contended methodology. The proposed strategy can be explored using efficient and effective procedure.

The network of the proposed framework comprises of transmitters, scanners, vehicles, mobile devices. The core part of the system is, first test the behavior of the network, which has to be scanned thoroughly. If the network is stable, simply maintain the network by controlling the traffic and by examining the routing traces comprised. If there are uneven disturbances in the network or the network is unstable, the following steps have to be taken into consideration.

First, the framework has to be designed in such a way that it has to be efficiently enabled and configure the transmitter devices. Second, enabling an efficient message forwarding approach to create awareness among the communicating parties of the network regarding event notifications and finally, make the mobile devices or vehicles deviate from their respective path and relocate them towards the safer paths.

3.2 Factors that Influence Abnormal State of the Network

While vehicles are passing in the network, nearby scanners are activated. According to the number of vehicles joined in the network, Roadway Congestion Index (RCI) is calculated. It is defined as a mathematical rating of highway capacity derived from the ratio of existing design hour traffic volumes to the practical hourly capacity of a rural highway system. If any variation occurred in the ratio, then congestion occurs.

$$\text{RCI}= \frac{((\text{Freeway DVMT per Lane}-\text{mile}) \ast \text{Freeway DVMT}) + ((\text{principal Arterial DVMT per Lane}-\text{mile}) \ast \text{principal Arterial DVMT})}{(14{,}000 \ast \text{Freeway DVMT}) + (5{,}500 \ast \text{principal Arterial DVMT})}$$

$$\text{Daily Vehicle Miles Travelled (DVMT)} = \frac{(\text{Annual vechile Miles Travelled (AVMT)})}{365}$$

$$\text{Freeway DVMT} = \text{Urban Freeway DVMT} + \text{Rural Freeway DVMT}$$

$$\text{Principal Arterial DVMT} = \text{Urban principal Arterial DVMT} + \text{Rural principal Arterial DVMT}$$

$$\text{Principal Arterial DVMT per Lane-mile} = \frac{\text{Urban principal Arterial DVMT}}{\text{Urban principal Arterial Lane}-\text{miles}} + \frac{\text{Rural principal Arterial DVMT}}{\text{Rural principal Arterial Lane}-\text{miles}}$$

$$\text{Freeway DVMT per Lane-mile} = \frac{\text{Urban Freeway DVMT}}{\text{Urban Freeway Lane}-\text{miles}} + \frac{\text{Rural Freeway DVMT}}{\text{Rural Freeway Lane}-\text{miles}}$$

3.3 Enable the Transmitter

The network of the proposed framework is configured, in such a way that it locates the scanners at intermediate stages. These Scanners are incorporated with the configurable sensors that have the capability of sensing abnormal events in the network. When disturbances occurred in the network, these sensors will get activated and they activate their respective scanners, which will send signals to the nearby monitoring server. This Server then sends the signal to activate the transmitters that are near by the notified scanners.

3.4 Message Forwarding Strategy

Transmitters have the ability to generate the congestion notification message and forward it to all the communicating parties in the network by implementing the strategy of broadcasting in that particular region. For the efficient message forwarding, Reliable Directional Greedy Routing (RDGR) algorithm [12] is used. RDGR is a reliable position based greedy routing approach. In this approach it takes the position, speed and link stability to choose next appropriate forwarding node.

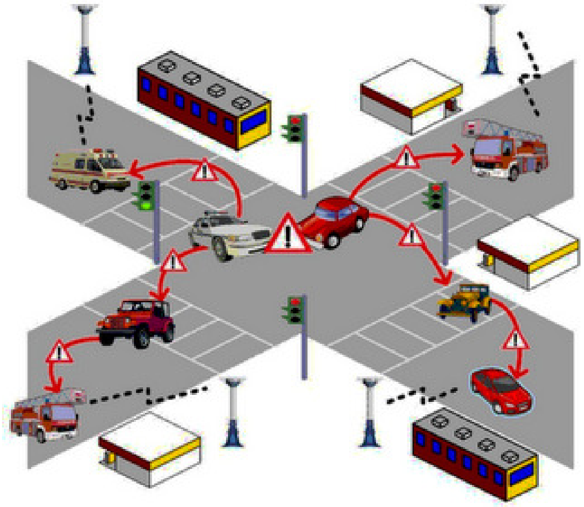


FIGURE 6: Message Forwarding System.

Figure 6 shows the interative module that implements the message forwarding approach.

To identify path stability we need to know individual link stability along the path. We define link stability in terms of link expiration time which means maximum time of connectivity between any two neighbour nodes. In order to calculate the link expiration time we assume motion parameters of any two neighbours are known. Let n_1 and n_2 be two nodes within the transmission range R and x_1' , y_1'' and x_2' , y_2' be the coordinate for node n_1 and n_2 with velocity v_1 and v_2 and the directions Θ_1 and Θ_2 respectively. Let after a time interval *t the* new coordinate will be x_1 , y_1 for n_1 and x_2 , y_2 for n_2 . For time *t* let d_1 and $d_2$be the distance travelled by node n_1 and n_2.

Formula for calculating d_1 and d_2 are

$$d_1 = v_1 t$$

$$d_2 = v_2 t$$

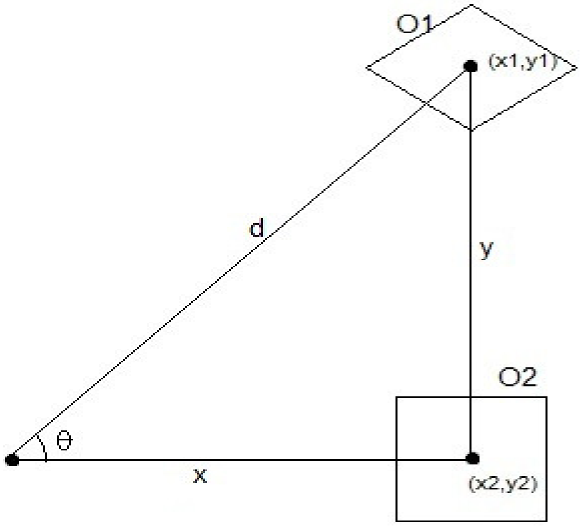


FIGURE 7: Representing the coordinates of two mobile devices.

From the above figure, the coordinates will be generated as

$$x = d\ cos\theta$$

$$y = d\ sin\theta$$

Formula for calculating new coordinates (with respect to old coordinates) is

$$x_1 = x_1' + x_1 = x_1' + d_1\cos\Theta_1 = x_1' + t(v_1\cos\Theta_1)$$
$$y_1 = y_1' + y_1 = y_1' + d_1\sin\Theta_1 = y_1' + t(v_1\sin\Theta_1)$$
$$x_2 = x_2' + x_2 = x_2' + d_2\cos\Theta_2 = x_2' + t(v_2\cos\Theta_2)$$
$$y_2 = y_2' + y_2 = y_2' + d_2\sin\Theta_2 = y_2' + t(v_2\sin\Theta_2)$$

Formulas for calculating distance between two nodes at time t are

$$D^2 = \{(x_1' - x_2') + t(v_1\cos\theta_1 - v_2\cos\theta_2)\}^2 + \{(y_1' - y_2') + t(v_1\sin\theta_1 - v_2 sin\theta_2)\}^2$$

Formula for calculating link stability between two nodes at time t is

$$LS = \frac{R}{D} = \frac{R}{\sqrt{\{(x_1' - x_2') + t(v_1\cos\theta_1 - v_2\cos\theta_2)\}^2 + \{(y_1' - y_2') + t(v_1\sin\theta_1 - v_2 sin\theta_2)\}^2}}$$

Where *LS:* link stability between any two nodes over time period t

R: Maximum transmission range

It compares all the ways to find the optimal path in forwarding the message. Finally it will choose optimal way, which has more speed, velocity and link stability and send messages to the vehicles and the mobile devices.

3.5 Deviation of Vehicles

The forwarded message contains the information regarding alternate path, which avoids the influence of abnormal activities, to control the traffic. Receivers equipped in the devices can sense the forwarded message and activates the GPS system configured in that mobile device. This GPS system drives the device to the desired optimal path where there will be lesser or zero impact of the uneven disturbances occurred in the network.

The network is going to be examined at regular levels to check out the stability of the network. If the network is stable, then it is sufficient to maintain the network by analyzing the traffic amount and respective traffic volume information of the network. If the network is not stable, then it is necessary to accelerate the sub modules necessitated to make the unstable network comes under stable state. The proposed strategy incorporates minimum and simple computations in transforming the network from unstable condition to the stable one.

4. RESULTS AND DISCUSSIONS

The realistic implementation of VANET is much costly and challenging. Thus, simulation is much practical and cost effective. In this work, a simulator called Veins (vehicles in network simulation) which consists of three components is used to simulate the real time scenario. These components include SUMO for mobility, OMNeT++ for network simulation and simulation control, and a TraCI to do the coupling.

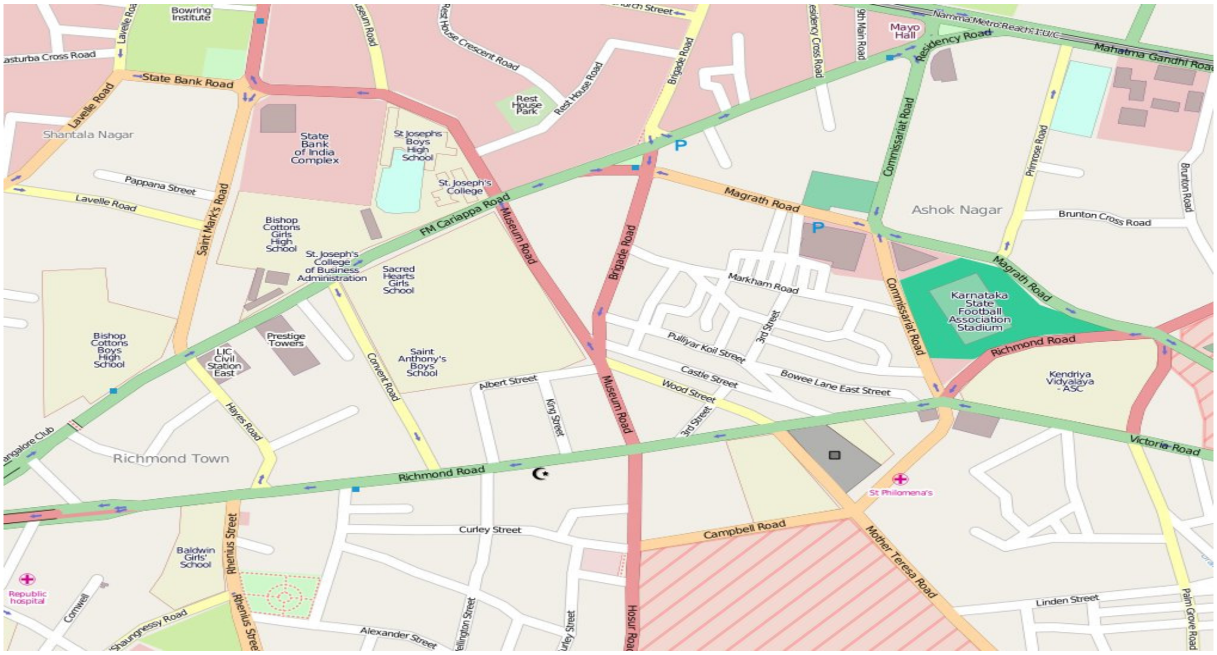


FIGURE 7: Image showing the real time scenario of a Bengaluru, Karnataka region.

Figure 7shows depicts the image real time scenario of a region, which provides input to the simulator that can effectively implements the proposed strategy.

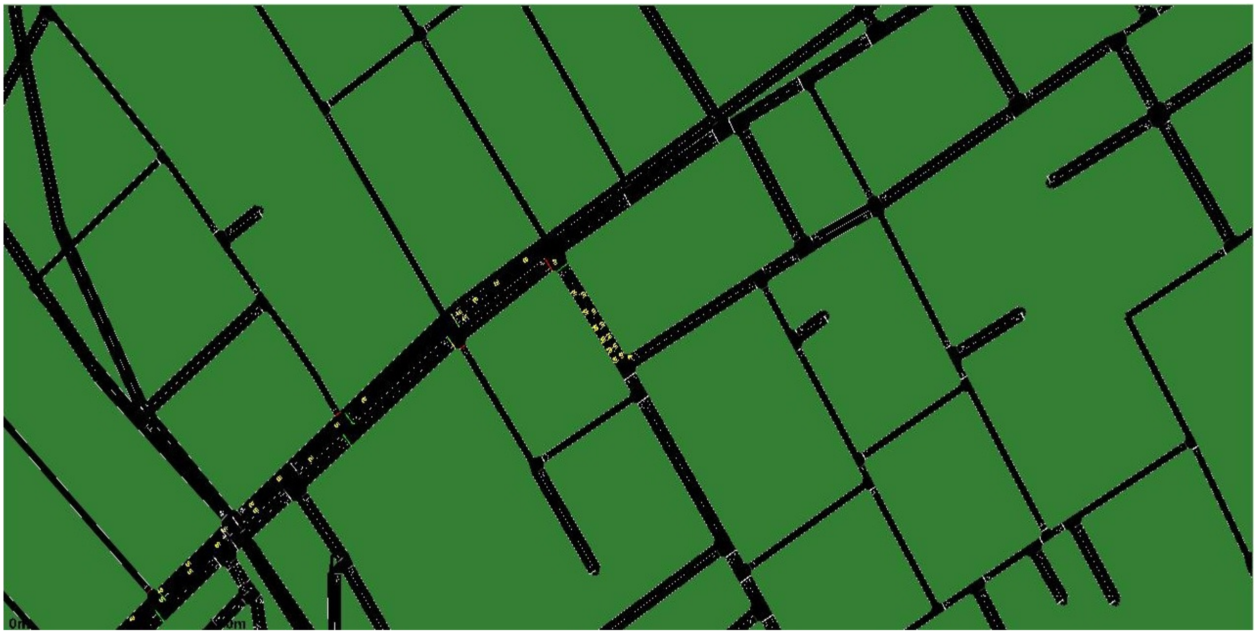


FIGURE 8: behaves as an input image to the simulator on which contended strategy applies.

Figure 8 shows the input image on which the yellow spots represents moving vehicles which forms Vehicular adhoc network.

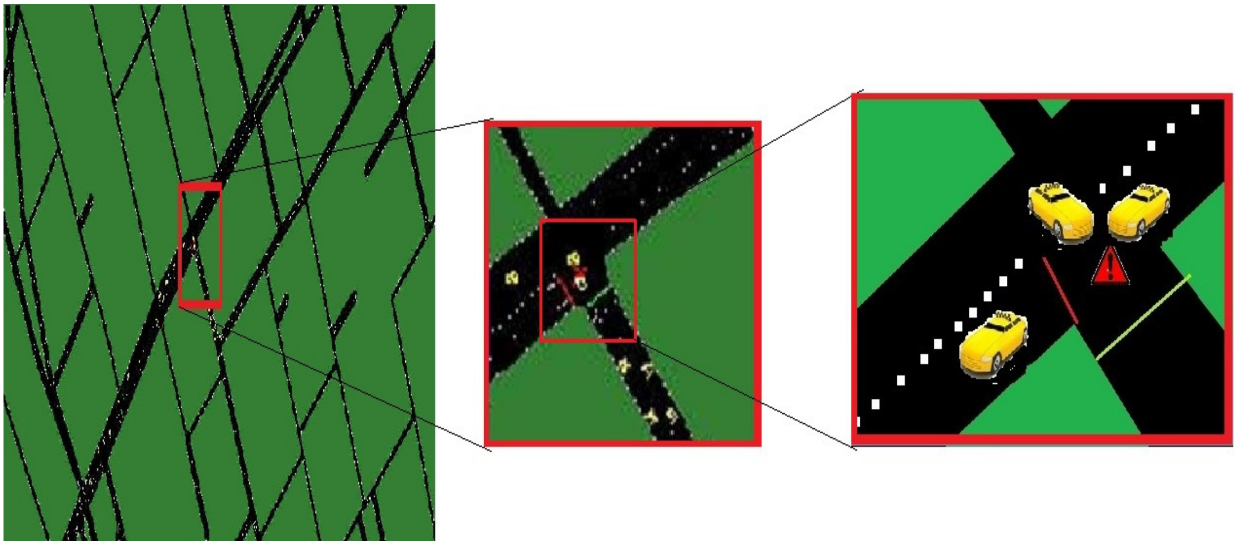


FIGURE 9: Scenario depicting uneven disturbances ocuured in the traffic.

Figure 9 shows the illustration of disturbances occurred among the vechiles in the network traffic .

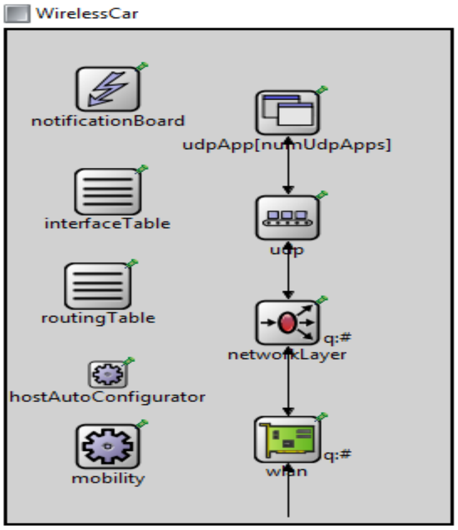


FIGURE 10 shows internal structure of the transmittor configured in the moving vehicles.

Above figure depicts the modules of the Transmittor internal structure that enhance the flexibility of message forwarding approach.

5. CONCLUSION

This works implements the framework capable of producing realistic vehicular mobility traces for network simulator. Simulation results were presented to understand the differences among various mobility levels in terms of vehicular density and speed distribution. The progressive introduction of stop signs, traffic lights, multiple lanes demonstrates how the modeling of each of these features brings the noticeable changes to the system performance.

The core part of the proposed system is, first to test the behavior of the network, which has to be scanned thoroughly. If the network is stable, simply maintain the network by controlling the traffic and by examining the routing traces comprised. If there are uneven disturbances in the network or the network is unstable, then the subsequent steps have to be taken into consideration. It is part of future work to investigate the actual impact of different traffic phenomena on a vehicular network, so to understand which factors must be considered and which can be neglected for a confident VANETs simulation study.

REFERENCES

[1] Gilbert held “inter and intra vehicle communication” by Taylor & Francis Group, LLC, 2008

[2] Vaishali D. Khairnar “Mobility Models for Vehicular Ad-hoc Network Simulation” *International Journal of Computer Applications (0975 – 8887) , Volume 11– No.4, December 2010*

[3] C. Bettstetter, “Smooth is Better than Sharp: A Random Mobility Model for Simulation of Wireless Networks.”, 4th ACM International Work-shop on Modelling, Analysis, and Simulation of Wireless and Mobile Systems (MSWiM 2001), Rome, Italy, July 2001.

[4] Nedal T. Ratout and Syed Masiur Rahman. “ A comparative analysis of currently used microscopic and macroscopic traffic simulation software.” The Arabian Journal for Science and Engineering, 34(1B) :121-133,2009

[5] Transportation Research Board of the National Academies. “Transportation Research Record: Journal of the Transportation Research Board”. Volume 1852/2003, January 2007.

[6] SHANG Lei, “RESEARCH OF URBAN MICROSCOPIC TRAFFIC SIMULATION SYSTEM” Vol. 5, pp. 1610 - 1614, 2005

[7] Baber Aslam and Cliff C. Zou, “Distributed Certificate Architecture for VANETs” School of Electrical Engineering and Computer Science University of Central Florida Orlando, FL, USA

[8] C. Gorgorin, V. Gradinescu, R. Diaconescu, V. Cristea, and L. Ifode. “An Integrated Vehicular and Network Simulator for Vehicular Ad-Hoc Networks.” In Proc. European Simulation and Modelling Conference (ESM), 2006.

[9] Francisco J. Martinez, Chai Keong Toh, Juan-Carlos Cano, Carlos T. Calafate and Pietro Manzoni “A survey and comparative study of simulators for vehicular *ad hoc* networks (VANETs)” WIRELESS COMMUNICATIONS AND MOBILE COMPUTING *Wirel. Commun. Mob. Comput.* (2009)

[10] Brandner, G, Schilcher, Bettstetter, “Proceedings of International Symposium on Communications, Control, and Signal Processing (ISCCSP)” march 2010

[11] John F. Kennedy “Freeway management systems and motor vehicle crashes”. Cambridge, MA 02138, June 2000

[12] K.Prasanth1 Dr.K.Duraiswamy2 K.Jayasudha3 and Dr.C.Chandrasekar4, “IMPROVED PACKET FORWARDING APPROACH IN VEHICULAR AD HOC NETWORKS USING RDGR ALGORITHM”

Performance of Various Mobile IP Protocols and Security Considerations

K.V.Ramana Ph.D. vamsivihar@gmail.com
Jawaharlal Nehru Technological University
Kakinada, 533003,India
.
Raghu.B.Korrapati Ph.D. raghu.korrapati@waldenu.edu
Walden University

K.S.S. Praveen Kumar praveen.kanakala@gmail.com
Jawaharlal Nehru Technological University
Kakinada, 533003,India.

Bh.V. Naveen naveen.bhimala@gmail.com
Jawaharlal Nehru Technological University
Kakinada, 533003,India

Abstract

Mobile IP is the underlying technology for support of various mobile data and wireless networking applications. Mobile IP can be thought of as the cooperation of three major subsystems. First , there is a discovery mechanism defined so that mobile computers can determine their new attachment points (new IP addresses) as they move from place to place within the internet. Second , once the mobile computer knows the IP address at its new attachment point , it registers with an agent representing it at its home network. Lastly , Mobile IP defines simple mechanisms to deliver datagram's to the mobile node when its is away from its home network. This work focuses on parameters based comparison for different mobile IP protocols. Parameters include Bandwidth , Time Delay and file size. An analytic model is adopted to propose for evaluating the mean signaling delay and the mean bandwidth per call according to the type of MT mobility. In this analysis, the MHMIP outperforms the DHMIP and MIP strategies in almost all the studied cases. The main contribution of this paper is the analytic model that allows the mobility management performance evaluation and basic security implementations on Agents. In future, Maintaining most computers on a private network, visible to the public Internet necessitated with highly secured environment.

Keywords: Mobile IP, Agents , Band width , Time delay, Mobility Management.

1. INTRODUCTION

Mobile Computing is becoming increasingly important due to the rise in the number of portable computers and the desire to have continuous network connectivity to the Internet irrespective of the physical location of the node. The Internet infrastructure is built on top of a collection of protocols, called the TCP/IP protocol suite. **Transmission Control Protocol (TCP)** and **Internet Protocol (IP) [1],[2]** are the core protocols in this suite. IP requires the location of any host connected to the Internet to be uniquely identified by an assigned IP address. This raises one of the most important issues in mobility, because when a host moves to another physical location, it has to change its IP address. However, the higher level protocols require IP address of a host to be fixed for identifying connections. **The Mobile Internet Protocol (Mobile IP) [3]** is an extension to the Internet Protocol proposed by the **Internet Engineering Task Force (IETF)** that addresses this issue. It enables mobile computers to stay connected to the Internet regardless of their location and without changing their IP address. More precisely, Mobile IP is a standard protocol that builds on the Internet Protocol by making mobility transparent to applications and higher level protocols like TCP.

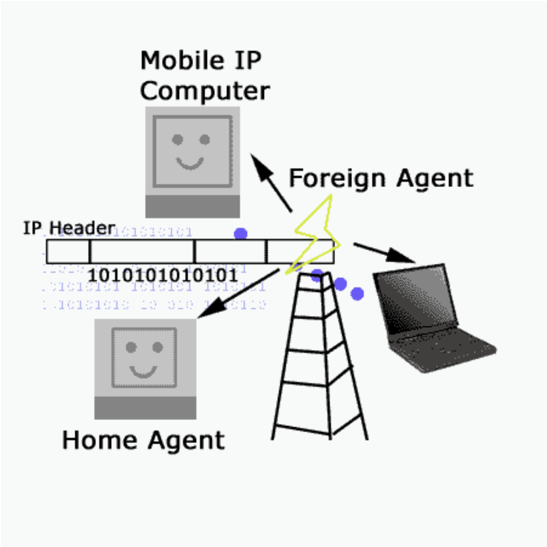
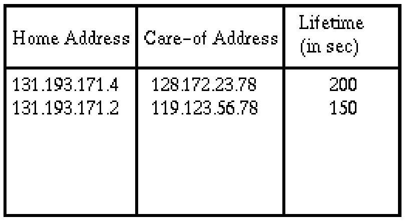


Figure 1: Mobile IP

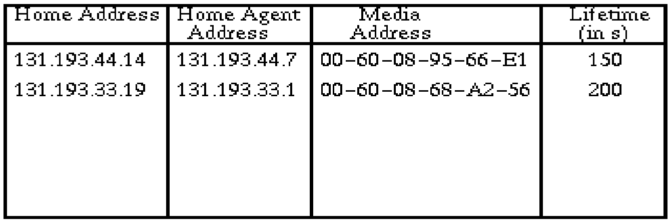
Mobile IP supports mobility by transparently binding the home address of the mobile node with its care-of address. This mobility binding is maintained by some specialized routers known as mobility agents. **Mobility agents** are of two types - **home agents and foreign agents**. The home agent, a designated router in the home network of the mobile node, maintains the mobility binding in a mobility binding table where each entry is identified by the tuple <permanent home address, temporary care-of address, association lifetime>. Table 1 shows a mobility binding table. The purpose of this table is to map a mobile node's home address with its care-of address and forward packets accordingly.



Home Address	Care-of Address	Lifetime (in sec)
131.193.171.4	128.172.23.78	200
131.193.171.2	119.123.56.78	150

TABLE 1: Mobility Binding Table

Foreign agents are specialized routers on the foreign network where the mobile node is currently visiting. The foreign agent maintains a visitor list which contains information about the mobile nodes currently visiting that network. Each entry in the visitor list is identified by the tuple: < permanent home address, home agent address, media address of the mobile node, association lifetime>. Table 2 shows an instance of a visitor list.



Home Address	Home Agent Address	Media Address	Lifetime (in s)
131.193.44.14	131.193.44.7	00-60-08-95-66-E1	150
131.193.33.19	131.193.33.1	00-60-08-68-A2-56	200

TABLE 2: Visitor List

In a typical scenario, the care-of address of a mobile node is the foreign agent's IP address. There can be another kind of care-of address, known as collocated care-of address, which is usually obtained by some external address assignment mechanism.

The basic Mobile IP protocol has four distinct stages. These are:

- **Agent Discovery:** Agent Discovery consists of the following steps:
    - Mobility agents advertise their presence by periodically broadcasting Agent Advertisement messages. An Agent Advertisement message lists one or more care-of addresses and a flag indicating whether it is a home agent or a foreign agent.
    - The mobile node receiving the Agent Advertisement message observes whether the message is from its own home agent and determines whether it is on the home network or a foreign network.
    - If a mobile node does not wish to wait for the periodic advertisement, it can send out Agent Solicitation messages that will be responded by a mobility agent.
- **Registration:** Registration consists of the following steps:
    - If a mobile node discovers that it is on the home network, it operates without any mobility services.
    - If the mobile node is on a new network, it registers with the foreign agent by sending a Registration Request message which includes the permanent IP address of the mobile host and the IP address of its home agent.
    - The foreign agent in turn performs the registration process on behalf of the mobile host by sending a Registration Request containing the permanent IP address of the mobile node and the IP address of the foreign agent to the home agent.
    - When the home agent receives the Registration Request, it updates the mobility binding by associating the care-of address of the mobile node with its home address.
    - The home agent then sends an acknowledgement to the foreign agent.
    - The foreign agent in turn updates its visitor list by inserting the entry for the mobile node and relays the reply to the mobile node.

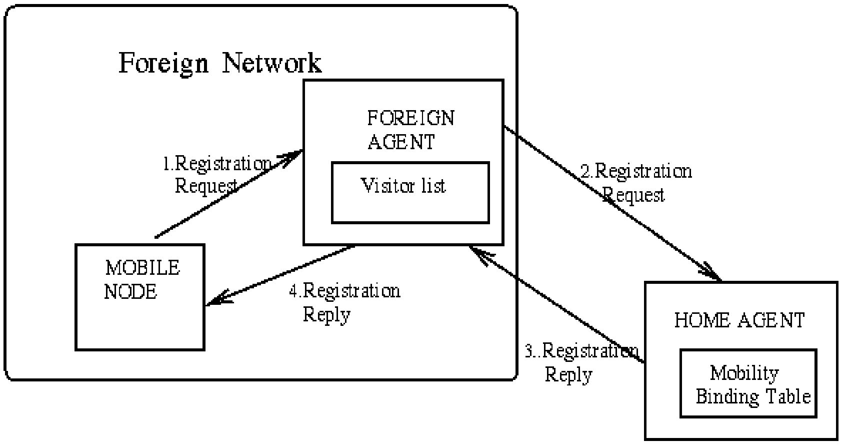


FIGURE 2: Registration process in Mobile IP

- **In Service:** This stage can be subdivided into the following steps:
  - When a correspondent node wants to communicate with the mobile node, it sends an IP packet addressed to the permanent IP address of the mobile node.
  - The home agent intercepts this packet and consults the mobility binding table to find out if the mobile node is currently visiting any other network.
  - The home agent finds out the mobile node's care-of address and constructs a new IP header that contains the mobile node's care-of address as the destination IP address. The original IP packet is put into the payload of this IP packet. It then sends the packet. This process of encapsulating one IP packet into the payload of another is known as IP-within-IP encapsulation, or tunneling.
  - When the encapsulated packet reaches the mobile node's current network, the foreign agent decapsulates the packet and finds out the node's home address. It then consults the visitor list to see if it has an entry for that mobile node.
  - If there is an entry for the mobile node on the visitor list, the foreign agent retrieves the corresponding media address and relays it to the mobile node.
  - When the mobile node wants to send a message to a correspondent node, it forwards the packet to the foreign agent, which in turn relays the packet to the correspondent node using normal IP routing.
  - The foreign agent continues serving the mobile node until the granted lifetime expires. If the mobile node wants to continue the service, it has to reissue the Registration Request.

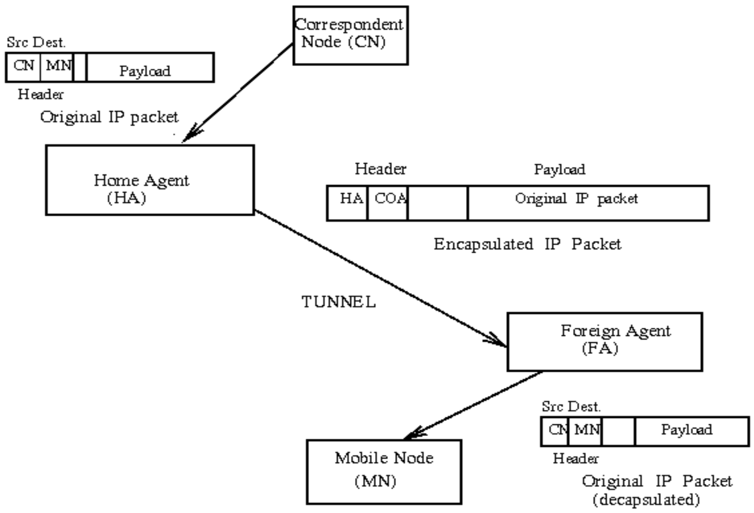


FIGURE 3: Tunneling operation in Mobile IP

- **Deregistration:** If a mobile node wants to drop its care-of address, it has to deregister with its home agent. It achieves this by sending a Registration Request with the lifetime set to zero. There is no need for deregistering with the foreign agent as registration automatically expires when lifetime becomes zero. However if the mobile node visits a new network, the old foreign network does not know the new care-of address of the mobile node. Thus datagram already forwarded by the home agent to the old foreign agent of the mobile node are lost.

The hierarchical mobile IP (HMIP) **[4]** protocol was proposed to employ the hierarchy of foreign agents (FAs) and the gateway FAs (GFAs) to reduce the number of registration operations and to reduce the signaling latency. However, since user mobility characteristics and network traffic load are always in changing, the centralized and pre-planned network topology of HMIP would become invalid or even lead more signaling cost if no adjustment to be adopted. This paper introduces a novel distributed and dynamic mobility management strategy for mobile IP where the signaling burden is evenly distributed and the regional network boundary is dynamically adjusted according to the real-time measurement of handover strength or traffic load in the networks.

The rest of the paper is organized as follows. In Section 2, demonstrates the related work which gives brief idea about existing system and proposed system. In Section 3, the core module of this work and the respective methodology is presented. In Section 4, Security issues are highlighted. In Section 5, the results and graphs of the proposed methodology are presented. Finally, Section 6 concludes the paper.

2. RELATED WORK

The mobile IP can provide continuous Internet access services for the mobile user and does provide a simple and scalable solution to user mobility. Yet, mobile IP is not a good solution for users with high mobility because it may cause excessive signaling traffic and long latency. The hierarchical mobile IP (HMIP) protocol was proposed to employ the hierarchy of foreign agents (FAs) and the gateway FAs (GFAs) to reduce the number of registration operations and to reduce the signaling latency.

However, since user mobility characteristics and network traffic load are always in changing, the centralized and pre-planned network topology of HMIP would become invalid or even lead more signaling cost if no adjustment to be adopted.

This paper introduces a novel distributed and dynamic mobility management strategy for mobile IP where the signaling burden is evenly distributed and the regional network boundary is dynamically adjusted according to the real-time measurement of handover strength or traffic load in the networks.

Thence, an analytic model is adopted to propose for evaluating the mean signaling delay **[5]** and the mean bandwidth per call according to the type of MT mobility. In this analysis, the MHMIP outperforms the DHMIP and MIP strategies**[6], [7]** in almost all the studied cases. The main contribution of this paper is the analytic model that allows the mobility management performance evaluation and basic security implementations on Agents.

2. METHODOLOGY

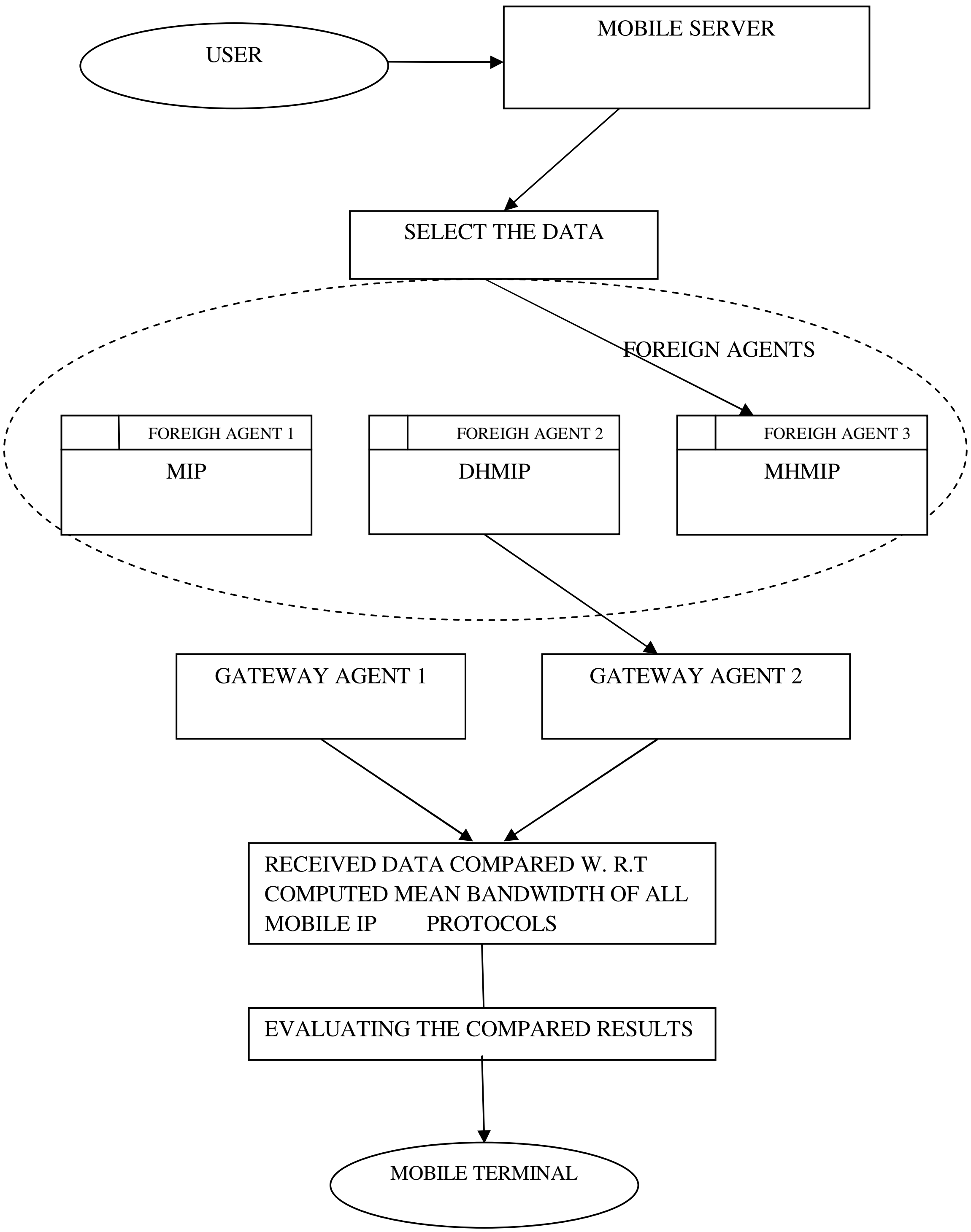
Working of Mobile IP

A mobile node can have two addresses - a permanent home address and a care of address (CoA), which is associated with the network, the mobile node is visiting. There are two kinds of entities in Mobile IP:

- A home agent stores information about mobile nodes whose permanent home address is in the home agent's network.
- A foreign agent stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses, which are used by Mobile IP.

A node wanting to communicate with the mobile node uses the permanent home address of the mobile node as the destination address to send packets to. Because the home address logically belongs to the network associated with the home agent, normal IP routing mechanisms forward these packets to the home agent. Instead of forwarding these packets to a destination that is physically in the same network as the home agent, the home agent redirects these packets towards the foreign agent through an IP tunnel by encapsulating the datagram with a new IP header using the care of address of the mobile node.

Control Flow Sructure of Proposed Methodology


USER
MOBILE SERVER
SELECT THE DATA
FOREIGN AGENTS
FOREIGH AGENT 1
MIP
FOREIGH AGENT 2
DHMIP
FOREIGH AGENT 3
MHMIP
GATEWAY AGENT 1
GATEWAY AGENT 2
RECEIVED DATA COMPARED W. R.T
COMPUTED MEAN BANDWIDTH OF ALL
MOBILE IP PROTOCOLS
EVALUATING THE COMPARED RESULTS
MOBILE TERMINAL

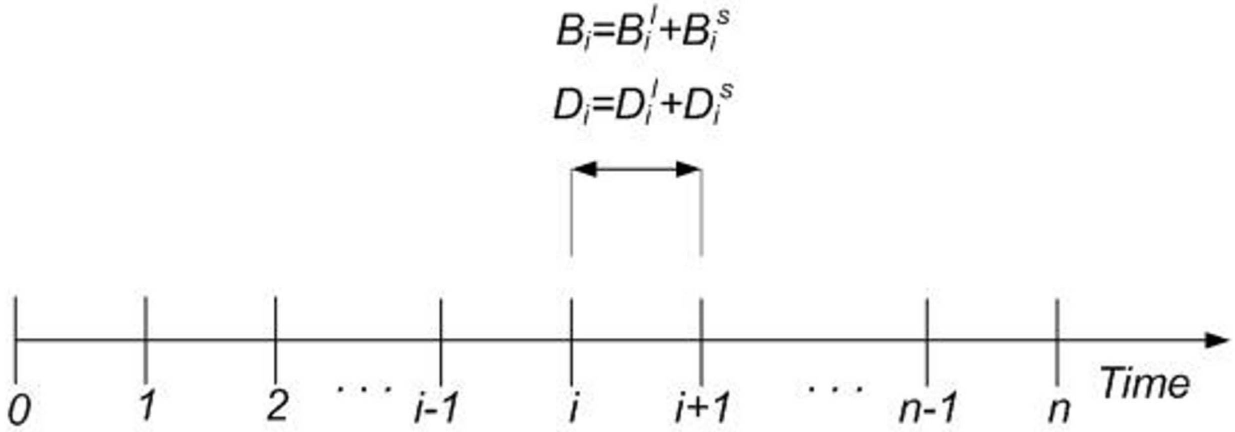
The above figure depicts the illustration of the contended methodology, the data entered by the mobile user is sent to the mobile terminal. The Mobile Terminals (MTs) registers with the Home Agents (HAs) When ever their Care-of-Addresses (CoAs) change. They use different Foreign Agents (FAs) and Gateway FAs (GFAs) hierarchy's to concentrate the registration processes. For high-mobility MTs, the Hierarchical MIP (HMIP) and Dynamic HMIP (DHMIP) strategies localize the registration in FAs and GFAs, yielding to high-mobility signaling. The Multicast HMIP strategy limits the registration Processes in the GFA's. We evaluate the mean signaling delay and the mean bandwidth per call according to the type of MT mobility at the mobile server.

When acting as transmitter, a mobile node sends packets directly to the other communicating node through the foreign agent, without sending the packets through the home agent, using its permanent home address as the source address for the IP packets. This is known as triangular routing. If needed, the foreign agent could employ reverse tunneling by tunneling the mobile node's packets to the home agent, which in turn forwards them to the communicating node. This is needed in networks whose gateway routers have ingress filtering enabled and hence the source IP address of the mobile host would need to belong to the subnet of the foreign network or else the packets will be discarded by the router.

The Mobile IP protocol defines the following:

- An authenticated registration procedure by which a mobile node informs its home agent(s) of its care-of-address.
- an extension to ICMP Router Discovery, which allows mobile nodes to discover prospective home agents and foreign agents; and
- The rules for routing packets to and from mobile nodes, including the specification of one mandatory tunneling mechanism and several optional tunneling mechanisms.

In order to understand the contended mechanism, an illustration is considered by taking as an example the mean bandwidth computation. In this figure, the holding time of ongoing call is divided into time intervals small enough that we may assume that in each time interval]i, i + 1], at most one handoff may occur.



In each interval, let

- n be the number of intervals for a call,
- B^l_i be the bandwidth used by a call during the time interval]i, i + 1],
- B^s_i be the signaling bandwidth used by a call during handoff that occurred in the time interval]i , i+1], and

- B^i be the total bandwidth used by a call during the time interval]i , i+1]

B^l_i and B^s_i are random variables with values that depend on the occurrence or not of a handoff during the interval]i, i+1] and on the possible path reestablishment once the handoff occurs.

The variable B^l_i can take two values. When a handoff occurs for a call in the interval]i; i + 1], B^l_i represents the sum of the allocated bandwidth over the original path and the one allocated over the links of the new established path.

Otherwise, it represents the bandwidth used on the link of the on-going connection. Bi represents the sum of the bandwidth used by the on-going call (B^l_i) and the bandwidth used for signalling (B^s_i). Otherwise, it represents the allocated bandwidth to the on-going call (B^l_i).

$$B_i = B^l_i + B^s_i \qquad (1)$$

$$B_i = B^l_i \qquad (2)$$

Equation (1), is applicable only if a handoff occurs in [i, i+1] and other Equation (2) is applicable.

The mean of B_i over the handoff events is given by the following equation,

$$E[B_i] = E[B^l_i] + E[B^s_i]$$

The computed mean bandwidth value is used as a parameter to evaluate the comparison among different Mobile IP protocols.

Motivation for The Mobile IP Design

The IP address of a host consists of two parts: 1) The higher order bits of the address determine the network on which the host resides; 2) The remaining low-order bits determine the host number.

IP decides the next-hop by determining the network information from the destination IP address of the packet. On the other hand, higher level layers like TCP maintain information about connections that are indexed by a quadruplet containing the IP addresses of both the endpoints and the port numbers. Thus, while trying to support mobility on the Internet under the existing protocol suite, we are faced with two mutually conflicting requirements: (1) a mobile node has to change its IP address whenever it changes its point of attachment, so that packets destined to the node are routed correctly, (2) to maintain existing TCP connections, the mobile node has to keep its IP address the same. Changing the IP address will cause the connection to be disrupted and lost.

Mobile IP, the standard proposed by IETF, is designed to solve the problem by allowing each mobile node to have two IP addresses and by transparently maintaining the binding between the two addresses. One of the IP addresses is the permanent home address that is assigned at the home network and is used to identify communication endpoints. The other is a temporary care-of address that represents the current location of the host. The main goals of Mobile IP are to make mobility transparent to the higher level protocols and to make minimum changes to the existing Internet infrastructure.

4. SECURITY ISSUES

To provide security for the network, it is essential to incorporate security mechanism in the communicating parties of the network. In this regard, Security modules configured for the router is much more vital. This section projects the demonstration of implementing security on Routers.

Implementing Security on Routers

The diagram below shows a simple network configuration.

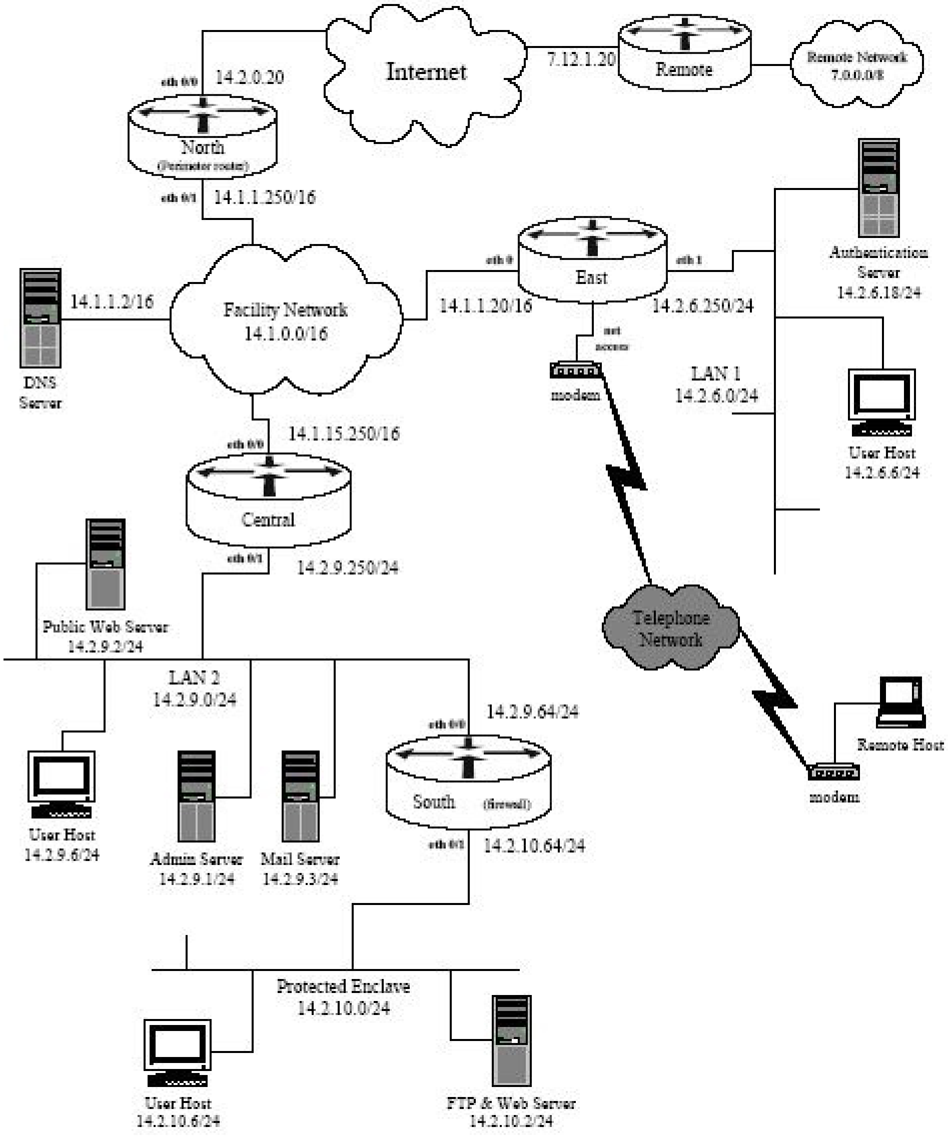


FIGURE 4: Example Network Architecture.

Above figure is simply a vehicle for presenting security guidance about routers, it is not a design for a secure network. However, this architecture reasonably reflects the kinds of networks found in many organizations.

Router Access Security

This includes various mechanisms used to protect the router itself. These include physical access, router network traffic and loopback interface, remote administration concerns, and configuration issues.

- **Physical Security**

  Network equipment, especially routers and switches, should be located in a limited access area. If possible, this area should only be accessible by personnel with administrative responsibilities for the router. In practice, physical security mechanisms and policies must not make access too difficult for authorized personnel, or they may find ways to circumvent the physical security precautions.

  To illustrate one reason why physical security is critical to overall router security, consider the password recovery procedure for routers. Using this procedure, an individual with physical access can gain full privileged (enable) access to a Router without using a password. The details of the procedure vary between router models, but always include the following basic steps. An administrator (or an attacker) can simply connect a terminal or computer to the console port and follow the procedure below

  Step 1 Configure the router to boot up without reading the configuration memory (NVRAM). This is sometimes called the test system mode.

  Step 2 Reboot the system.
  Step 3 Access enable mode (which can be done without a password if you are in test system mode).
  Step 4 View or change the password, or erase the configuration.
  Step 5 Reconfigure the router to boot up and read the NVRAM as it normally does.
  Step 6 Reboot the system."

- **Router Network Traffic and the Loopback Interface**

  The primary job of a router is forwarding traffic between networks, but routers also generate some network traffic. Routers and other network devices communicate using various management protocols, such as routing protocols, SNMP, NTP, and TFTP. When the router initiates a network connection, that connection must have some source address; typically a router will select a source address from one of the addresses bound to one of its network interfaces. This can be problematic in several ways, mainly because the source address for some services can vary.

  To create a loopback interface, simply assign it an IP address. For a border router, the loopback's address usually should be in the range of the internal or DMZ network, not the external network. Note that the loopback address cannot be the same as the address of any other interface, nor can it be part of the same network as any other interface.

  In general, router network services that can be bound to the loopback interface should be. Commands to set source interface bindings are given with the discussion of each service in the rest of the guide.

- **Remote Access**

  This document will discuss five connection schemes which can be used for router administration.

  1. No Remote – administration is performed on the console only.
  2. Remote Internal only with AAA – administration can be performed on the router from a trusted internal network only, and AAA is used for access control.
  3. Remote Internal only – administration can be performed on the router from the internal network only.
  4. Remote External with AAA – administration can be performed with both internal and external connections and uses AAA for access control.

5. Remote External – administration can be performed with both internal and external connections.

The five regimes listed above are listed in the order that best protects the router and allows for accounting of router activities.

- **Authentication, Authorization, and Accounting (AAA)**

  This is the router's access control facility for controlling access, privileges, and logging of user activities on a router. Authentication is the mechanism for identifying users before allowing access to a network component. Authorization is the method used to describe what a user has the right to do once he has authenticated to the router. Accounting is the component that allows for logging and tracking of user and traffic activities on the router which can be used later for resource tracking or trouble shooting. Section 4.6 contains details on configuring AAA in an example network.

Router Network Service Security

Routers support a large number of network services at layers 2, 3, 4, and 7. Some of these services can be restricted or disabled, improving security without degrading the operational use of the router. Some of these services are application layer protocols that allow users and host processes to connect to the router. Others are automatic processes and settings intended to support legacy or specialized configurations but which are detrimental to security. As stated in Section 3, general security practice for routers should be to support only traffic and protocols the network needs; most of the services listed below are not needed.

Turning off a network service on the router itself does not prevent it from supporting a network where that protocol is employed. For example, a router may support a network where the bootp protocol is employed, but some other host is acting as the bootp server. In this case, the router's bootp server should be disabled.

Access Control Lists, Filtering, and Rate Limiting

IOS uses access lists to separate data traffic into that which it will process (permitted packets) and that which it will not process (denied packets). Secure configuration of Routers makes very heavy use of access lists, for restricting access to services on the router itself, and for filtering traffic passing through the router, and for other packet identification tasks.

Access lists on routers provide packet selection and filtering capabilities. An access list consists of one or more rules. For IP traffic, there are two types of access lists available: standard and extended. Standard access lists only allow source IP address filtering.

Extended access lists can permit or deny packets based on their protocols, source or destination IP addresses, source or destination TCP/UDP ports, or ICMP or IGMP message types. Extended access lists also support selective logging. Both standard and extended IP access lists can be applied to router interfaces, vty lines (for remote access), IPSec, routing protocols, and many router features. Only standard IP access lists can be applied to SNMP.

- **Filtering Traffic Through the Router**

  The following examples illustrate methods to protect the router or the internal network from attacks.

  - **IP Address Spoof Protection**

    The filtering recommendations in this sub-section are applicable to border routers, and most interior routers. With backbone routers, it is not always feasible to define 'inbound' or 'outbound'.

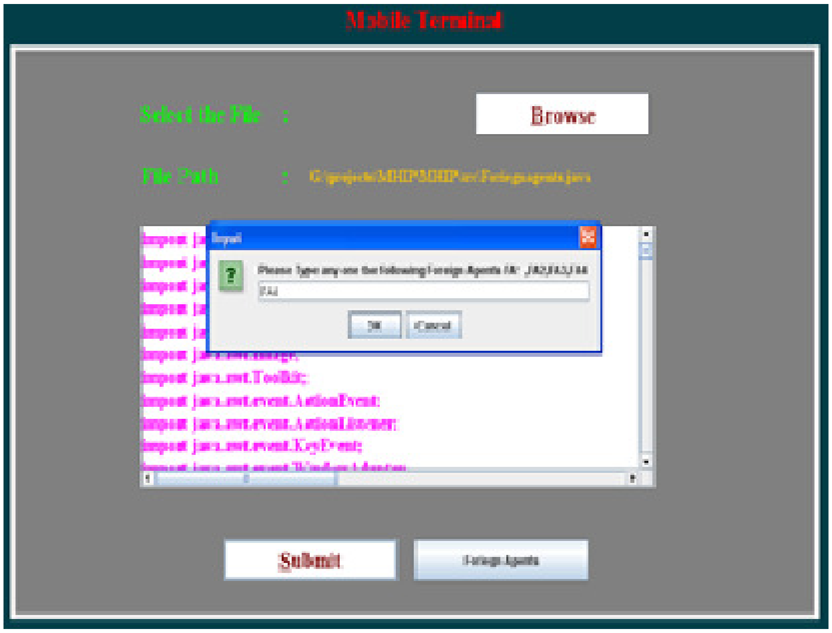
  - **Inbound Traffic**

Do not allow any inbound IP packet that contains an IP address from the internal network (e.g., 14.2.6.0), any local host address (127.0.0.0/8), the link-local DHCP default network (169.254.0.0/16), the documentation/test network (192.0.2.0/24), or any reserved private addresses (refer to RFC 1918) in the source field. Also, if your network does not need multicast traffic, then block the IP multicast address range (224.0.0.0/4).

- **Outbound Traffic**
  Do not allow any outbound IP packet that contains an IP address other than a valid internal one in the source field. Apply this access list to the internal interface of the router.

5. RESULTS AND DISCUSSIONS

An efficient analysis has been done on comparing various Mobile IP protocols and from the results of those analysis, it has been observed that MHMIP has taken minimum bandwidth, minimum time delay when compared with MIP and DHMIP.



Mobile Terminal

Select the File :

File Path : G:\projects\MHIP\MHIP\src\Foriegnagents.java

```
import ja
import ja
import ja
import ja
import ja
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
import java.awt.event.WindowAdapter;
```

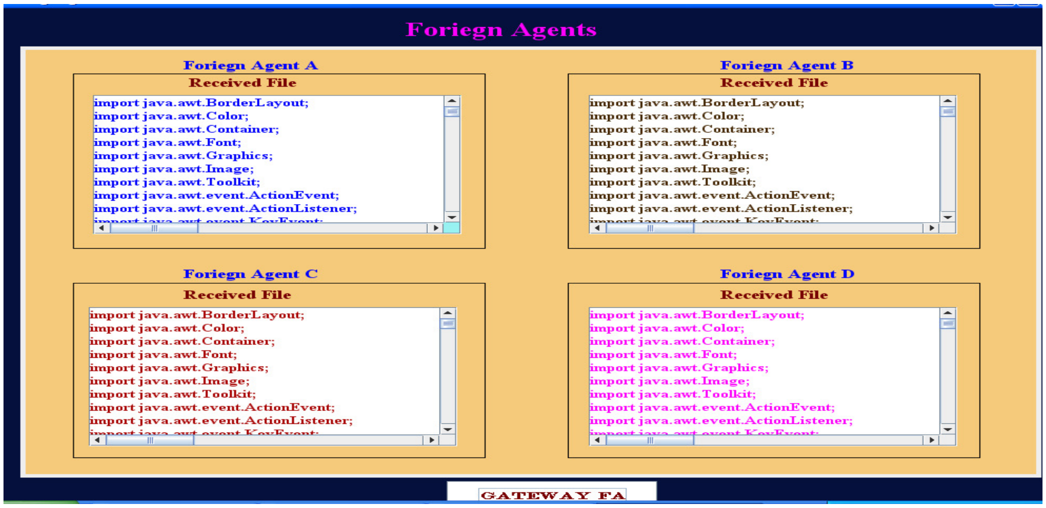
Input

Please Type any one the following Foreign Agents FA1 ,FA2,FA3,FA4

FA1

FIGURE 5: Scenario of selecting a file for flooding to foreign agent from Home Agent.

Figure 5 illustrates the demonstration of browsing the file for transmitting to foreign agent.



Foriegn Agents

Foriegn Agent A

Received File

```
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
```

Foriegn Agent B

Received File

```
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
```

Foriegn Agent C

Received File

```
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
```

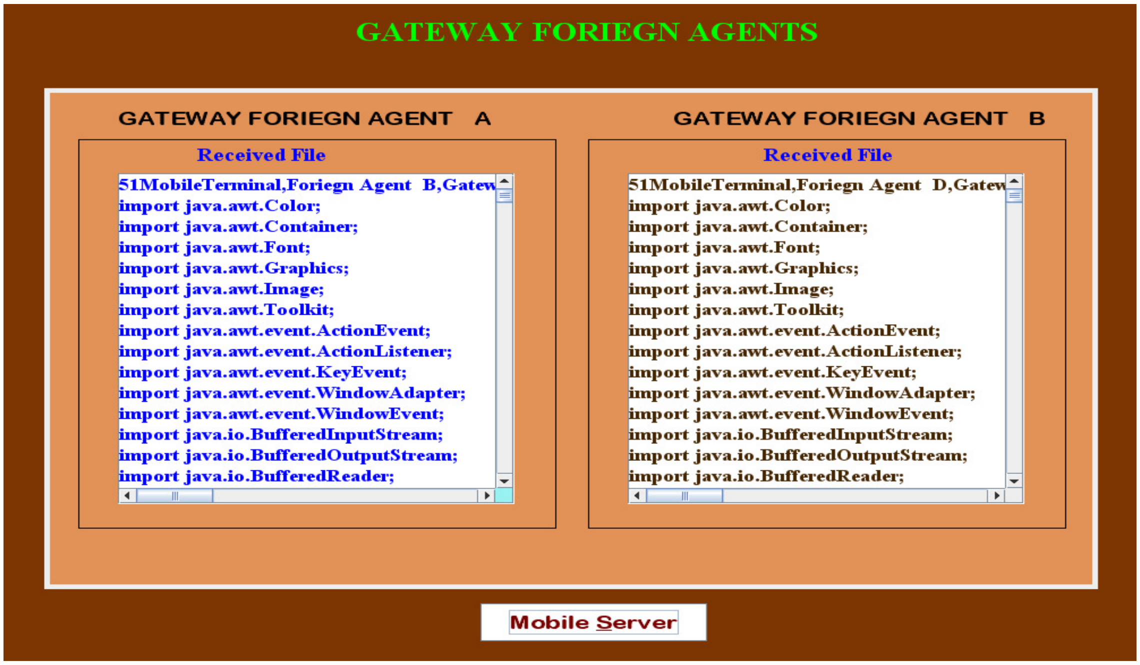
Foriegn Agent D

Received File

```
import java.awt.BorderLayout;
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
```

FIGURE 6: Data received by different foreign agents.

Figure 6 illustrates the phenomena of Information Dissemination to various Foreign Agents.

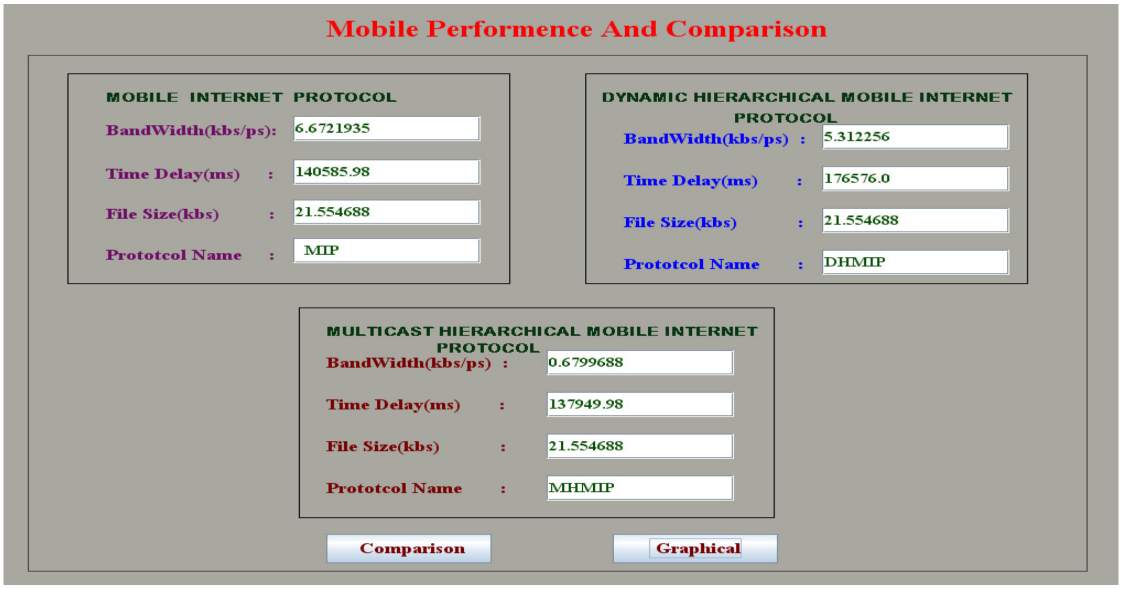


```
51MobileTerminal,Foriegn Agent  B,Gatew
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
import java.awt.event.WindowAdapter;
import java.awt.event.WindowEvent;
import java.io.BufferedInputStream;
import java.io.BufferedOutputStream;
import java.io.BufferedReader;
```

```
51MobileTerminal,Foriegn Agent  D,Gatew
import java.awt.Color;
import java.awt.Container;
import java.awt.Font;
import java.awt.Graphics;
import java.awt.Image;
import java.awt.Toolkit;
import java.awt.event.ActionEvent;
import java.awt.event.ActionListener;
import java.awt.event.KeyEvent;
import java.awt.event.WindowAdapter;
import java.awt.event.WindowEvent;
import java.io.BufferedInputStream;
import java.io.BufferedOutputStream;
import java.io.BufferedReader;
```

FIGURE 7: Scenario describing the data reception by two distinct Gateway Foreign Agents.

Figure 7 demonstrates the efffective reception of different Gateway Foreign Agents.



MOBILE INTERNET PROTOCOL

BandWidth(kbs/ps): 6.6721935

Time Delay(ms) : 140585.98

File Size(kbs) : 21.554688

Prototcol Name : MIP

DYNAMIC HIERARCHICAL MOBILE INTERNET PROTOCOL

BandWidth(kbs/ps) : 5.312256

Time Delay(ms) : 176576.0

File Size(kbs) : 21.554688

Prototcol Name : DHMIP

MULTICAST HIERARCHICAL MOBILE INTERNET PROTOCOL

BandWidth(kbs/ps) : 0.6799688

Time Delay(ms) : 137949.98

File Size(kbs) : 21.554688

Prototcol Name : MHMIP

FIGURE 8: Comaprison of various Mobile IP protocols.

Figure 8 shows comparison of various mobile IP protocols by considering multiple parameters like Bandwidth, Time Delay.

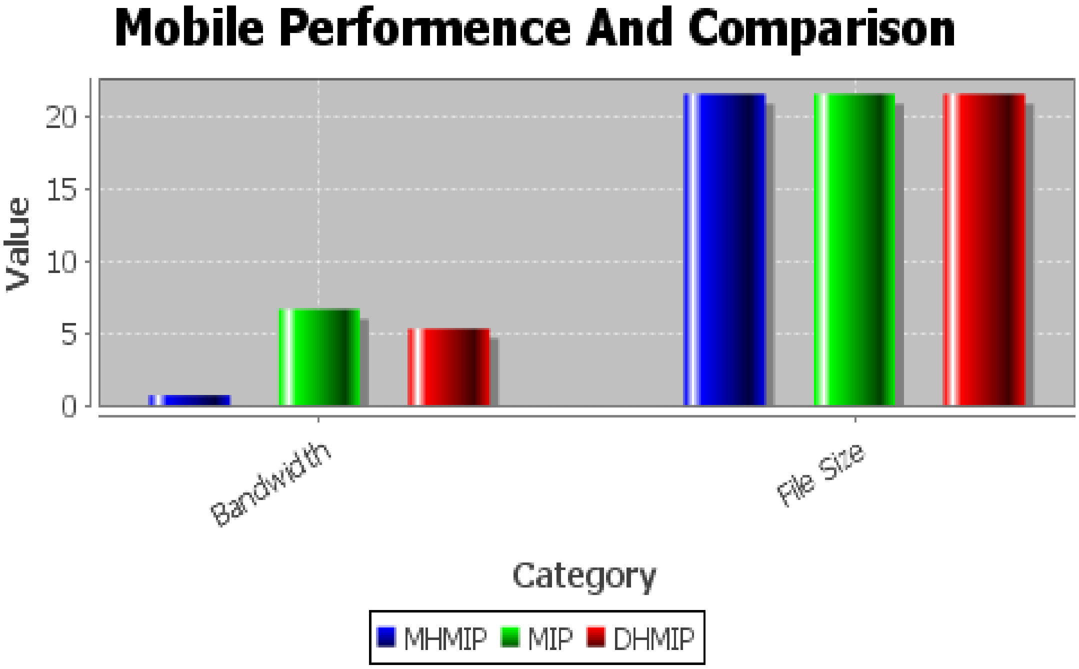


FIGURE 10: Histogram for Mobile IP comparisons.

Figure 10 compares the Mobile IP protocols In two categories. One w.r.t Bandwidth and other w.r.t.File Size.

6. CONCLUSION

In this work, an analytical model is proposed, which evaluates the mean handoff delay per call and the mean bandwidth per call of three mobility management approaches: MIP, DHMIP, and MHMIP. Numerical results show that the MHMIP mobility approach[8],[9],[10] ,[11] compares very favorably with the previously considered mobility approaches.

More specifically, our analysis gives in almost all cases a lower mean handoff delay per call and a mean bandwidth per call than those offered by the DHMIP and MIP approaches. It also shows the robustness of the MHMIP approach in the sense that for critical scenario corresponding to the extreme situation where all handoff events are localized at the multicast group borders, this approach essentially yields to-

1) A lower mean bandwidth per call than the DHMIP and MIP approaches;
2) A lower mean handoff delay per call than that offered by the MIP approach;
3) A lower mean handoff delay than that offered by the DHMIP except in case of frequent inter-GFAs handoffs with a network configuration having a high number of links involved in MHMIP path reestablishment.

Since we expect a diversity of multimedia applications for future IP mobile networks, we recommend using the MHMIP approach in networks parts carrying delay sensitive and/or low mean bandwidth consumption type of applications and this according to the mobility type

Future Enhancement

- It entails more configuration and administration to maintain usability.
- Not being fully visible on the Internet can cause some difficulty in connecting to certain services, such as streaming audio/video, chat/instant messaging programs, or some secure Web sites.

- Maintaining most computers on a private network, visible to the public Internet helps maintain a highly secure environment. While at the same time keeping them connected to the public Internet is the challenge.

7. REFERENCES

[1] C.E. Perkins, "IP Mobility Support for IPv4," *IETF RFC 3344, Aug.2002.*

[2] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," *IETF RFC 3775, June 2004.*

[3] R. Cancers and V.N. Padmanabhan, "Fast and Scalable Handoffs for Wireless Internetworks*," Proc. ACM MobiCom, pp. 56-66, 1996.*

[4] C. Castelluccia, "Extending Mobile IP with Adaptative Individual Paging: A Performance Analysis," *Proc. Fifth IEEE Symp. Computers and Comm., pp. 113-118, July 2000.*

[5] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management HMIPv6," *IETF RFC 4140, Aug. 2005.*

[6] E. Fogelstroem, A. Jonsson, and C. Perkins, "Mobile IPv4 Regional Registration," *IETF RFC 4857, June 2007.*

[7] H. Omar, T. Saadawi, and M. Lee, "Supporting Reduced Location Management Overhead and Fault Tolerance in Mobile IP Systems," *Proc. IEEE Symp. Computers and Comm., pp. 347-353, 1999.*

[8] S. Pack, T. You, and Y. Choi, "Performance Analysis of Robust Hierarchical Mobile IPv6 for Fault-Tolerance Mobile Services," *IEICE Trans. Comm., vol. E87-B, no. 5, pp. 1158-1165, May 2004.*

[9] J. Xie and I.F. Akyildiz, "A Novel Distributed Dynamic Location Management Scheme for Minimizing Signaling Costs in Mobile IP," *IEEE Trans. Mobile Computing, vol. 1, no. 3, pp. 163-175, July 2002*.

[10] Song, J. Huang, R. Feng, and J. Song, "A Distributed Dynamic Mobility Management Strategy for Mobile IP Networks*," Proc Sixth Int'l Conf. ITS Telecomm. 2006.*

[11] Nadjia kara , "Mobility Management Approaches for Mobile IP Networks : Performance Comparison and Use Recommendations," *IEEE Transactions On Mobile Computing , VOL 8 , NO ,10,OCTOBER 2009.*

A New Paradigm for Load Balancing in WMNs

Mohammad Shahverdy *shahverdy@iautb.ac.ir*
Department of Computer
Tafresh Branch, Islamic Azad University
Tafresh, 3951736874, IRAN

Misagh Behnami *misagh_behnami@yahoo.com*
Department of Computer
Arak Branch, Islamic Azad University
Arak, IRAN

Mahmood Fathy *mahfathy@iust.ac.ir*
Computer Engineering Faculty
Iran University of Science and Technology
Tehran, IRAN

Abstract

In this paper, we address the problem of load balancing in Wireless Mesh Networks. We consider a Cluster Based Wireless Mesh Architecture in which the WMN is divided into clusters that could minimize the updating overhead during topology change due to mobility of mesh nodes or congestion of load on a cluster. Each cluster contains a gateway that has complete knowledge about group memberships and link state information in the cluster. The gateway is often elected in the cluster formation process. We consider load of gateways and try to reduce it. As a matter of fact when a gateway undertakes to be an interface for connecting nodes of a wireless mesh network to other networks or internet, there would be some problems such as congestion and bottleneck, so we introduce a new paradigm for these problems. For solving bottleneck we use clustering to reduce load of gateways and after that by use of dividing cluster we prevent from bottleneck on gateways. We study how to detect congestion on a gateway and how can reduce loads of it that preventing from bottleneck on gateway and therefore increasing throughput of network to encountering many loads. So we propose an algorithm to detect bottleneck and remedies for load balancing in Wireless Mesh Networks. We also use Ns2-Emultion for implementing and testing the framework. Some qualitative results are provided to prove the correctness and the advantages of our framework.

Keywords: Wireless Mesh Networks, Load Balancing, Clustering, Bottleneck

1. INTRODUCTION

Wireless mesh networking is a new paradigm for next generation wireless networks. Wireless mesh networks (WMNs) consist of mesh clients and mesh routers, where the mesh routers form a wireless infrastructure/backbone and interwork with the wired networks to provide multi hop wireless Internet connectivity to the mesh clients. Wireless mesh networking has generated as a self-organizing and auto-configurable wireless networking to supply adaptive and flexible wireless Internet connectivity to mobile users. This idea can be used for different wireless access technologies such as IEEE 802.11, 802.15, 802.16-based wireless local area network (WLAN), wireless personal area network (WPAN), and wireless metropolitan area network (WMAN) technologies. WMNs Potential application can be used in home networks, enterprise networks, community networks, and intelligent transport system networks such as vehicular ad-hoc networks.

Wireless local area networks (WLANs) are used to serve mobile clients access to the fixed network within broadband network connectivity with the network coverage [1]. The clients in WLAN use of wireless access points that are interconnected by a wired backbone network to connect to the external networks. Thus, the wireless network has only a single hop of the path and the Clients need to be within a single hop to make connectivity with wireless access point. Therefore to set up such networks need access points and suitable backbone. As result a Deployment of large-scale WLANs are too much cost and time consuming. However, The WMNs can provide wireless network coverage of large areas without depending on a wired backbone or dedicated access points [1, 2]. WMNs are the next generation of the wireless networks that to provide best services without any infrastructure. WMNs can diminish the limitations and to improve the performance of modern wireless networks such as ad hoc networks, wireless metropolitan area networks (WMANs), and vehicular ad hoc networks [2,3,4 and 5]. WMNs are multi-hop wireless network which provide internet everywhere to a large number of users. The WMNs are dynamically self-configured and all the nodes in the network are automatically established and maintain mesh connectivity among themselves in an ad hoc style. These networks are typically implemented at the network layer through the use of ad hoc routing protocols when routing path is changed. This character brings many advantages to WMNs such as low cost, easy network maintenance, more reliable service coverage.

Wireless mesh network has different members such as access points, desktops with wireless network interface cards (NICs), laptops, Pocket PCs, cell phones, etc. These members can be connected to each other via multiple hops. In the full mesh topology this feature brings many advantages to WMNs such as low cost, easy network maintenance and more reliable service coverage. In the mesh topology, one or multiple mesh routers can be connected to the Internet. These routers can serve as GWs and provide Internet connectivity for the entire mesh network. One of the most important challenges in these networks happens on GW, when number of nodes which connected to the internet via GW, suddenly increased. It means that GWs will be a bottleneck of network and performance of the network strongly decreases [4, 5, and 6].

In section 2 we first introduce related works. In section 3 system model and assumptions are discussed. In section 4 we present a new method for load balancing via GW. Section 5 evaluates the performance of the proposed scheme by means of simulation. Finally we conclude the paper in Section 6.

2. RELATED WORK

The problem of bottleneck in wireless mesh networks is an ongoing research problem although much of the literature [7, 8, 9, 10] available, addresses the problem without an introducing method for removing bottleneck and/or a well-defined way to prevent congestion. In [11], the authors proposed the MeshCache system for exploiting the locality in client request patterns in a wireless mesh network .The MeshCache system alleviates the congestion bottleneck that commonly exists at the GW node in WMNs while providing better client throughput by enabling content downloads from closer high-throughput mesh routers. There is some papers related to optimization problems on dynamic and static load balancing across meshes [11].Optimal load balancing across meshes is known to be a hard problem. Akyildiz et al. [12] exhaustively survey the research issues associated with wireless mesh networks and discusses the requirement to explore multipath routing for load balancing in these networks. However, maximum throughput scheduling and load balancing in wireless mesh networks is an unexplored problem. In this paper we present for the first time, a load balancing scheme in wireless mesh networks by using clustering and finding the best cluster head for new cluster by a new formula and evaluate its performance.

3. MODELS AND ASSUMPTION

We consider an area with wireless nodes (figure 1). These nodes can connect together and they can connect to internet or external networks via GW. GWs are wireless nodes that can route internal traffic to external networks when number of requests to GW increase then GW can't service all requests punctually. Thus a load balancing method is needed to decrease workload of GW. We use the following metrics for evaluation our scheme.

Service ratio: service ratio is defined as the ratio of the number of nodes which receive service to the total number of nodes that send request to GW. A good load balancing method should service as many requests as possible in time confine.

Delay: delay is defined time distance between node request`s until node receive responses by GW. Delay is a good parameter to present a suitable scheme to have a good performance.

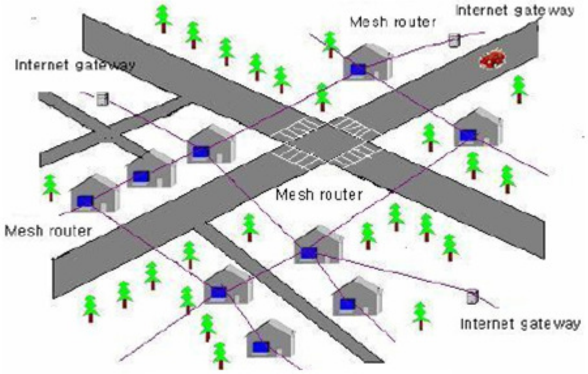


FIGURE 1: A wireless mesh network area

4. LOAD BALANCING VIA GATEWAY

The previous load balancing algorithms [7] do not spot fast traffic undulation. For instance, when the numbers of nodes (that are transferring data with a gateway) are increased suddenly then workload on transmission nodes and routers will be increased. This problem decreases performance of network because packets are aggregated in transmission nodes and cannot reach to destination on time. In first scheme for better control of workload on nodes we cluster nodes in specific groups. it is done thereby we put active nodes that are close together and can transmit data together directly in one cluster. Each cluster has a master that is called Gateway (GW). Each node in one cluster is aware of other nodes in this cluster. when a node wants to send data to a destination there will be two states: 1) if destination node is in the same cluster, transmission is occurred with one hop 2) if destination is not in the same cluster, at first data must be send to GW of its cluster and then this GW sends data to the destination cluster which the destination node exists in. The GW inside destination cluster sends data to destination node with one hop.

In a first look essence of a GW that all data transmit via them is bottleneck. In other word, when number of nodes that is sent data to outside of the cluster increased then workload of the GW is increased too. We implement node clustering for control of active node that worked with a GW. With this work we can control how many nodes are sending data via GW in specific time and when the number of these nodes is increased, we must decrease workload with suitable solution.

4.1 Breaking a Cluster

For controlling workload of a GW, we must control number of the nodes that transmit data to the GW until the amount of nodes do not overreach more than specified limitation. To attain to load balancing, GW should know its power and throughput. Namely GW must know how many nodes can transmit data by itself simultaneously. After that if the number of nodes that connected to the GW increases more than GW capacity, we have to decrease the load of GW with a suitable method. Assume that a GW is working with maximum capacity, the problem occurs when another node wants to get some services from GW. Now the GW can't respond to this request and the GW is converted to a bottleneck point. To solve congestion in GW we offer breaking cluster to two equal sections and then looking for a new GW for a new cluster (figure 2). After selecting new GW, it must connect to other GWs and connect to new cluster nodes. Therefore new cluster can operate such as the other clusters. Note that the nodes of a cluster must to be closed together geographically because of power saving and simple routing. A disadvantage of this breaking is time wasting for selecting a new suitable GW and making routes between it and other nodes. On the other hand, ordinary nodes that are registering in new cluster must reconstruct the routing table which will waste time again. For these reasons performance will decrement. In the following we present a new formula for selecting a new suitable GW for new cluster and then we propose a solution for above problems.

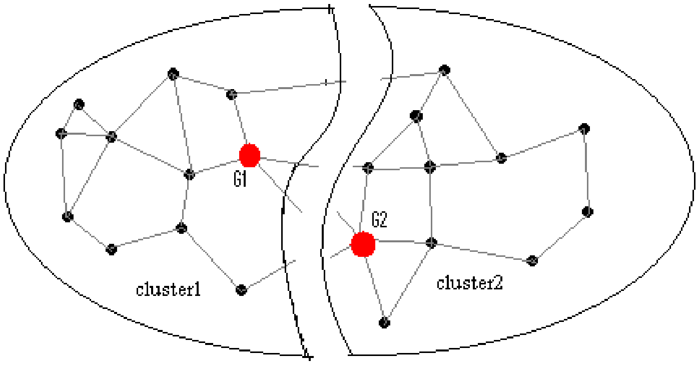


FIGURE 2: Breaking a cluster

4.2 Selecting a Suitable GW

When a cluster splits into two clusters, one of them has a GW but another one (new one) has no GW. So we need to find a suitable GW for the new cluster. Selecting Wrong GW can have effect on network performance. For example assume that if an inappropriate node is selected to be a GW then this GW may fail in its run time. So the cluster must select a new GW and establish a route table which is time wasting and this new GW may fail too. Therefore, random selecting GW causes low network performance because a failing GW causes accumulation data in a cluster and then increasing workload ascendant.

We survey parameters that effect on GW failures and then select a GW that has the best conditions via these parameters. The most effective parameters in stability of GW are: a) power supply, b) velocity of node, c) node constancy, d) distance to center of cluster and e) processing power of node.

The effect of power supply is that if each node that has high energy or has perennial power supply then it is more stable. Therefore the node that has this parameter is more suitable for being a GW because in the future it may be alive. The node with low velocity has less probability to go out from cluster. Therefore a node with low movement and low velocity is more suitable for being GW. In other words, if the node that has high velocity is accepted to be a GW then the GW may go out from the cluster and the cluster has to find and select a new GW again. Node constancy includes the time that a node exists in the cluster. For estimating this parameter each node can monitor a history of its lifetime in specific cluster and then each node that has longer lifetime is more constancy and more suitable for being GW. Central nodes have heavy workload rather than boundary nodes [1], as all nodes select shortest paths for optimal routing and these paths commonly pass from center of cluster. Hence traffic in central of cluster is very heavy. If a GW is selected in the center of a cluster then internal workload will add to external workload thus it is better that a GW is selected from the boundary of cluster. This parameter can be taken from GPS data. At last final parameter that we express is power of processing. A node with high processing power is more suitable for being a GW because it can do computation quickly. We integrated these parameters to a formula that is shown below:

$$G\_Value = \frac{Fower_{Supply} * Power_{CPU} * Constancy * Distance_{from\_center}}{Velocity}$$

In the above formula, we can calculate G_Value for each node in a cluster and then each node that has larger G_Value is more suitable for being a GW.

4.3 Breaking Cluster With Use of Threshold

In previous section we expressed that each GW knows the number of requests in service. If requests amount surpasses the ability of GW then the cluster will be broken. Selecting a new GW plus creating route table for GW and other nodes are time consuming, therefore performance decreases. We present a solution for this problem. We suggest selecting a new GW and creating a routing table before breaking the cluster. To denouement it attends to an example. Assume that a GW can service requests up to 10. It means that if 11th request is sent to the GW, it can`t respond to a new request, thus cluster is broken and then a new GW must be selected and routing table must be established.

In this new method each cluster has two thresholds. One threshold is for selecting a new GW that is called TS_GW and another threshold for established routing table that is called TS_routetable. For example assume that TS_GW is 5 and TS_routetable is 8. It means that if number of nodes which send requests are larger than 5 then cluster must select a new GW. The current GW can do it hereby current GW gets G_Value of all other nodes and each node that has high G_Value is selected for being new GW. With this method the new cluster does not waste any time for selecting a new GW because it is done before breaking cluster.

Also if number of nodes that send requests larger than 8, then pre routing is occurred and route table for GW and nodes of new cluster is made. When number of requests reaches up to 10 then current cluster will be broken. Therefore with this method cluster does not waste any time for selecting a GW and building route table. Simulation results show that breaking the cluster with threshold conquest other algorithms.

4.4 Incorporating Two Clusters

We express that when workload of a GW is increased inordinately, the cluster will be broken into two clusters. What will happen if we assume that workload of a cluster is decreased to zero. In this situation we envisage to several clusters that have low workload. Thus, it is necessary that clusters with low workload joint together. When two clusters are merged together we have to select a suitable GW between two GWs of two old clusters. So we choose the one which has more heavier workload and is more suitable to be the final cluster because the number of nodes that are routed from this GW is larger than the other GW, thereupon we can change previous formula to gain new formula to selecting a new GW in this section. There is a formula as following as below:

$$\text{G value join} = \frac{\text{n\_routetable}^2 * \text{Power}_{\text{Supply}} * \text{Power}_{\text{CPU}} * \text{Constancy} * \text{Distance}_{\text{From \_ center}}}{\text{Velocity}}$$

Where the power supply, power CPU, node constancy, node distance and node velocity parameters are like section 4.2 and n_routetable is number of nodes which are routed via GW, power 2 is to emphasis of this parameter, lastly each node that has high G_value_join is selected for GW of final cluster.

5. PERFORMANCE EVALUATION

We have performed several preliminary quantitative experiments. To this end, the performance of our proposed schemes was evaluated by using NS2 [13], [14].

5.1 Experimental Setup

In order to keep the results closest to real experiment, we used NS2. The simulation area is a 400*400 square as 200 nodes randomly positioned on it. Some of nodes move a little on the simulation area, other simulation parameters listed in table 1.

TABLE 1: Parameters of NS2 Simulation

Parameter	Value
Simulation time	100 sec
Transmission rate	64 Kbps
Node velocity	0-10 Kmph
Wireless coverage	50 meter
Packet size	1000 byte
Routing protocol	DSR
Ratio propagation model	Two ray. Ground
Antenna model	Omni antenna
Mac type	IEEE 802.11

5.2 Service Ratio Evaluation

A Major goal of load balancing is decreasing workload of GW and preventing from bottlenecks. Figure 3 shows the service ratio for different load balancing schemes. The x axis is the simulation time. In figure 3 three schemes are compared as follow: 1) load balancing without clustering, 2) load balancing with simple threshold clustering and 3) load balancing with hysteresis threshold clustering.

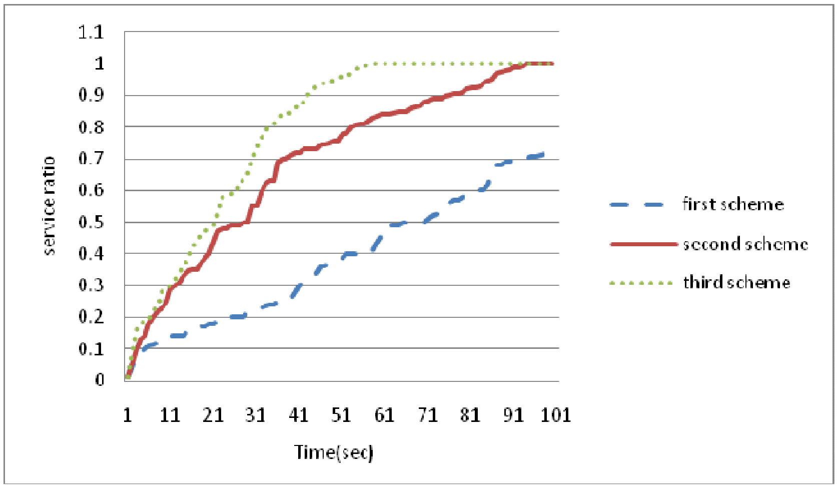


FIGURE 3: comparing service ratio for 3 schemes

As it follows from the figure 3 the third scheme leads to serving more requests in comparison to the other two schemes. The first scheme can't serve all requests because some request aggregate in queue of GW. The second scheme has low service ratio in each time in comparison to third scheme because delay of selecting GW and delay of making route table affect on service ratio.

5.3 The Effect of Workload

Figure 4 shows the effect of number of requests on load balancing performance for three schemes discussed in this paper. As shown in the figure 4 when the number of requests increases the service ratio of third scheme descends with a lower slope in comparison to the other two schemes. It follows figure 4 that in which the first scheme shows very poor performance.

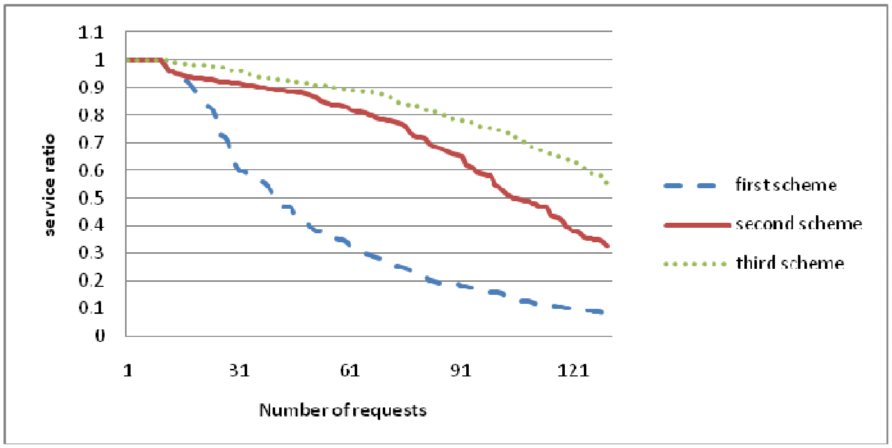


FIGURE 4: comparing service ratio with entered number of requests

5.4 Delay Evaluation

As shown in figure 5 when number of requests is increased then sum of delays in first scheme is increased with a high slope. This delay is the waiting time of requests in the GW queue. We dissemble other delays in network because they are similar in all schemes. Third scheme has least delay.

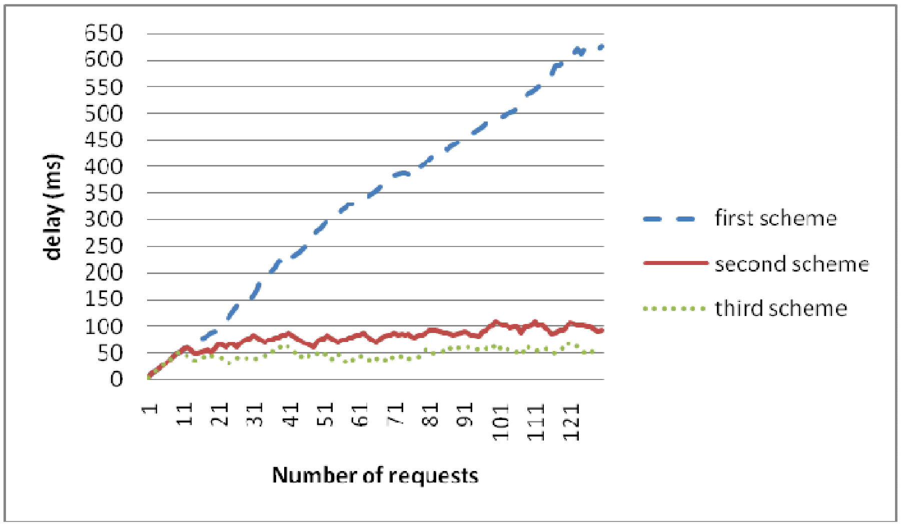


FIGURE 5: Effect of workload on delay

6. CONCLUSION AND FUTURE WORKS

In this paper we proposed load balancing schemes for WMNs. In first step we clustered all nodes to control the workload of them. If workload on a GW is increased up to maximum ability of the GW then the cluster is broken. Because selecting a new GW and establish a route table is time consuming, thus we propose a third scheme in which GW selection and creating rout table is done before breaking the cluster. Simulation results show that the proposed approach offers desirable performance and scalability. Although the paper considers most of the design aspects of the proposed infrastructure, it leaves some open issues and questions. For instance, surveying load balancing of multi channel GWs in clustering wireless mesh networks, finding maximum throughput of nodes in cluster based wireless mesh networks and how to find G_value for selecting a new GW with minimum overhead. Another open issue is using fuzzy logic for breaking the clusters.

7. REFERENCES

[1] J. Bicket, D. Aguayo, S. Biswas, R. Morris, Architecture and evaluation of an unplanned 802.11b mesh network, in: Proceedings of the 11th ACM Annual International Conference on Mobile Computing and Networking (MobiCom), ACM Press, Cologne, Germany, 2005, pp. 31–42.

[2] B. Aoun, R. Boutaba, Y. Iraqi, and G. Kenward, “Gateway Placement Optimization in Wireless Mesh Networks with QoS Constraints,” IEEE Journal on Selected Areas in Communications, vol. 24, Nov 2006.

[3] A.K.Hasan, A. A. Zaidan, A. Majeed, B. B. Zaidan, R. Salleh, O. Zakaria, and A. Zuheir, “Enhancement Throughput of Unplanned Wireless Mesh Networks Deployment Using Partitioning Hierarchical Cluster (PHC)”, World Academy of Science, Engineering and Technology 54 2009

[4] I.F.Akyildiz, X.Wang, W.Wang,” Wireless mesh networks: a survey”, Elsevier ,Computer Networks 47 (2005) 445–487

[5] K. Jain, J. Padhye, V. N. Padmanabhan, and L. Qiu, “Impact of interference on multi-hop wireless network performance,” in Proceeding of ACM MobiCom, 2003.

[6] I. Akyildiz and X. Wang, "A survey on wireless mesh networks," IEEE Communication Magazine, vol. 43, no.9, pp.s23-s30,Sep. 2005.

[7] B.S. MANOJ AND RAMESH R. RAO ,” WIRELESS MESH NETWORKING”, Chapter 8 : Load Balancing in Wireless Mesh Networks, page 263

[8] Saumitra M. Das, Himabindu Pucha and Y. Charlie Hu School of Electrical and Computer Engineering Purdue University, West Lafayette, “Mitigating the Gateway Bottleneck via Transparent Cooperative Caching in Wireless Mesh Networks” NSF grants CNS-0338856 and CNS-0626703.

[9] Jangeun Jun and Mihail L. Sichitiu Department of Electrical and Computer Engineering
North Carolina State University Raleigh,”The Nominal Capacity of Wireless Mesh Networks” NC 27695-7911

[10] Abu (Sayeem) Reaz1, Vishwanath Ramamurthi1, Dipak Ghosal1, John Benko2, Wei Li2, Sudhir Dixit3, and Biswanath Mukherjee1 ,”Enhancing Multi-hop Wireless Mesh Networks with a Ring Overlay”

[11] G. Horton, "A multi-level diffusion method for dynamic load balancing", Parallel Computing. 19 (1993), pp. 209-229

[12] I. Akyildiz, X. Wang, W. Wang, "Wireless Mesh Networks: A Survey", Computer Networks Journal 47, (Elsevier), March 2005. pp. 445-487.

[13] “The network simulator - ns2”,http://www.isi.edu/nsnam/ns/.

[14] Daniel Mahrenholz and Svilen Ivanov, "Real-Time Network Emulation with ns-2," Proceedings of The 8-th IEEE International Symposium on Distributed Simulation and Real Time Applications, Budapest Hungary, October 21-23, 2004.

[15] M. Shahverdy, M. Fathy, S. Yousefi, “Scheduling Algorithm for Vehicle to Road-Side Data Distribution”, ICHCC-ICTMF 2009, Berlin Heidelberg, CCIS 66, pp. 22–30, 2010.

INSTRUCTIONS TO CONTRIBUTORS

The International Journal of Computer Networks (IJCN) is an archival, bimonthly journal committed to the timely publications of peer-reviewed and original papers that advance the state-of-the-art and practical applications of computer networks. It provides a publication vehicle for complete coverage of all topics of interest to network professionals and brings to its readers the latest and most important findings in computer networks.

To build its International reputation, we are disseminating the publication information through Google Books, Google Scholar, Directory of Open Access Journals (DOAJ), Open J Gate, ScientificCommons, Docstoc and many more. Our International Editors are working on establishing ISI listing and a good impact factor for IJCN.

The initial efforts helped to shape the editorial policy and to sharpen the focus of the journal. Starting with volume 3, 2011, IJCN appears in more focused issues. Besides normal publications, IJCN intend to organized special issues on more focused topics. Each special issue will have a designated editor (editors) – either member of the editorial board or another recognized specialist in the respective field.

We are open to contributions, proposals for any topic as well as for editors and reviewers. We understand that it is through the effort of volunteers that CSC Journals continues to grow and flourish.

IJCN LIST OF TOPICS

The realm of International Journal of Computer Networks (IJCN) extends, but not limited, to the following:

- Algorithms, Systems and Applications
- ATM Networks
- Cellular Networks
- Congestion and Flow Control
- Delay Tolerant Networks
- Information Theory
- Metropolitan Area Networks
- Mobile Computing
- Multicast and Broadcast Networks
- Network Architectures and Protocols
- Network Modeling and Performance Analysis Network
- Network Security and Privacy
- Optical Networks
- Personal Area Networks
- Telecommunication Networks
- Ubiquitous Computing
- Wide Area Networks
- Wireless Mesh Networks
- Ad-hoc Wireless Networks
- Body Sensor Networks
- Cognitive Radio Networks
- Cooperative Networks
- Fault Tolerant Networks
- Local Area Networks
- MIMO Networks
- Mobile Satellite Networks
- Multimedia Networks
- Network Coding
- Network Operation and Management
- Network Services and Applications
- Peer-to-Peer Networks
- Switching and Routing
- Trust Worth Computing
- Web-based Services
- Wireless Local Area Networks
- Wireless Sensor Networks

CALL FOR PAPERS

Volume: 4 - **Issue:** 1 – February 2012

i. Paper Submission: November 31, 2011 **ii. Author Notification:** January 01, 2012

iii. Issue Publication: January / February 2012

CONTACT INFORMATION

Computer Science Journals Sdn BhD
B-5-8 Plaza Mont Kiara, Mont Kiara
50480, Kuala Lumpur, MALAYSIA
Phone: 006 03 6207 1607
006 03 2782 6991

Fax: 006 03 6207 1697

Email: cscpress@cscjournals.org

CSC PUBLISHERS © 2011
COMPUTER SCIENCE JOURNALS SDN BHD
M-3-19, PLAZA DAMAS
SRI HARTAMAS
50480, KUALA LUMPUR
MALAYSIA

PHONE: 006 03 6207 1607
006 03 2782 6991

FAX: 006 03 6207 1697
EMAIL: cscpress@cscjournals.org