Journal of Mobile Communication 1 (1): 6-12, 2007

Parametric Analysis of Mobile IPv6 Using Ns2

Shanthi Kuppusami Thoppe and L. Ganesan
Department of Electronics and Communication Engineering,
A.C. College of Engineering and Technology, Karaikudi, 630004, India

Abstract: Mobile IPv6 (MIPv6) is a protocol to deal with mobility for the next generation Internet (IPv6). However, the performance of MIPv6 has not yet been extensively investigated. Simulation using the famous network simulator Ns-2 will be used to highlight a hybrid wireless environment, over Mobile IPv6 protocol. Mobile IPv6 enables any IPv6 node to learn and cache the care-of address associated with a mobile node's home address and then to send packets destined for the mobile node directly to it at this care-of address using an IPv6 Routing header. In this study the overall throughput of the MIPv6 with different packet size and the packet loss is examined using TCP agent and the result is analyzed using Ns-2.

Key words: Mobile IPr6, Ns2, packet, mobile node

INTRODUCTION

Mobile IP allows transparent routing of IP packets to mobile nodes in the Internet. Each Mobile Node (MN) is identified by its home address, regardless of its current point of attachment to the Internet. A host that communicates with the mobile node is called a Correspondent Node (CN)[1]. The corresponding node does not have to be aware of the mobility of the mobile node. It can function as if the mobile node would be a normal stationary host in the Internet. The Mobile IP protocol identifies also two types of Mobility Agents (MAs), the Home Agent (HA) and the Foreign Agent (FA). The home agent resides at the home network of the mobile node, the same network, in which the home address of the mobile node is allocated. Packets from the CN to the MN are routed using the home address. The HA intercepts the packets and tunnels them to the current location of the MN. To be able to tunnel packets to the MN, the HA must be aware of the current location of the MN. For this purpose, the MN acquires a Care-of Address (CoA) from the network it is visiting. Every time the MN moves, the current CoA is registered to the HA. A foreign agent resides in the visited network. It offers routing services for the registered mobile nodes. The FA provides the MN with a CoA and detunnels and delivers data grams to the MN that were tunneled by the HA.

The FA can also serve as a default router for the registered Mns. Data grams sent by the CN to the home address of the MN are tunneled by the HA to the CoA of the MN. IP-IP encapsulation is the default tunneling method in Mobile IP. The IP-IP encapsulation attaches an extra IP header to the IP datagram. The routing is done according to the outer IP header, whose destination address is the CoA and the source address is the IP address of the HA. Thus, the resulting datagram is topologically sound. Inside the tunnel, the original packet remains unchanged. At the CoA, the inner IP packet is extracted and delivered to the MN. It appears to originate from the CN. The protocol stack of the MN receives the inner packet, whose destination IP address is the home address of the MN and source IP address is the address of the CN. The upper protocol stack of the MN does not have to be aware of the mobility. From the application point of view, the home address can be used as a static IP address of the host. As the MN sends packets to the CN, it uses the home address as a source address. Packets can be routed directly to the CN or tunneled via the HA. The later method is called reverse tunneling. In this case, the HA is the tunnel end-point for encapsulated data grams from the MN to the CN. The HA removes the outer header and redirects the packets to the CN. Reverse tunneling must be used in case of ingress filtering employed by many routers.

Corrersponding Author: Shanthi Kuppusami Thoppe, Selection Grade Lecturer,
Department of Electronics and Communication Engineering,
A.C. College of Engineering and Technology, Karaikudi-630004, India

Mobile IPv4: Mobile IP for IPv4 is comprised of following four components, Mobile Node (MN), Home Agent (HA), Foreign Agent (FA) and Correspondent Node (CN) as shown in Fig. 1. Any portable device like laptop, a data-ready cellular phone that can be carried by a mobile user is called a MN[2]. A MN is assigned to a particular network, known as its home network. MN can change its point of attachment from one network or subnet to another. This node can maintain ongoing communications while using its home address. A HA is a router on the home network of MN that maintains a list associations between home address of MN and its Care-of Address (CoA). A CoA represents current location of the MN on a foreign or visited network.

A FA is a router on foreign network that assists the MN in informing its current CoA to HA. The FA also acts as the default router for packets generated by MN while it is connected to foreign network. FA MNs visited this network IP address of MN on its home network is known as home address and it is static. The address of home agent is represented as HA address.

Mobile IPv6: In Mobile IPv6 each mobile node is always identified by its home address, regardless of its current point of attachment to the Internet. While away from its home 1P subnet, a mobile node is also associated with a care-of address, which indicates the mobile node's current location[3]. The Transmission Control Protocol (TCP) is a predominant protocol in the Internet service. The TCP/IP protocol was originally designed for fixed Internet without mobility in mind. With the increase of mobility Demands, it is important to understand how TCP performance is affected over various existing mobility protocols, which can in turn help design new protocols or pursue improvements. The Mobile IPv6 (MIPv6) protocol is designed to deal with mobility and to overcome some problems suffered by MIPv4. Although MIPv6 shares many features with MIPv4, there exist some differences. For instance, IPv6 uses a longer header; there is no need to deploy special routers as. foreign agents. In MIPv6; most packets sent to a mobile node while away from home are sent using an IPv6 Routing header rather than IP encapsulation, where MIPv4 must use encapsulation for all packets. Though it is interesting to know how MIPv6 affects the TCP performance, very little publication has been reported thus far. One of the reasons is that it is very difficult to analyze the protocols theoretically. This study is designed for dealing the TCP performance over the Mobile IPv6 Networks, discussing about the throughput of sending packets and dropping packets and analyzing the packet loss over the network.

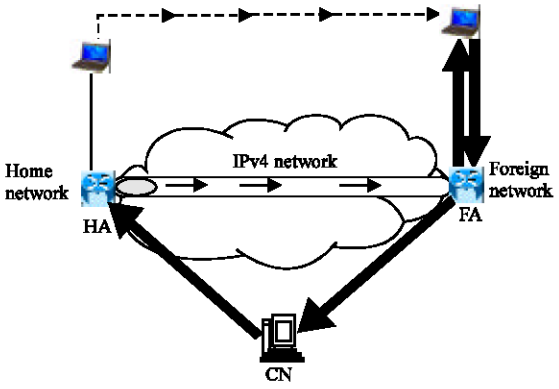

Fig. 1: General scenario of data transfer in mobile IPv4

Overview of mobile IPv6: IPv6 is derived from IPv4 and is in many ways similar to it. As such, the IETF Mobile IP Working Group's current protocol design for mobility of IPv4 nodes could be adapted for use in IPv6[4], with only the straightforward changes needed to accommodate differences between IPv4 and IPv6 such as the size of addresses. However, the development of IPv6 presents a rare opportunity, in that there is no existing installed base of IPv6 hosts or routers with which we must be compatible and in that the design of IPv6 may still be adjusted to account for the few special needs of mobile nodes. This research, therefore, considers how IPv6 can most naturally fulfill the support requirements for mobile nodes. Each mobile node is assigned a (permanent) IP address in the same way as any other node and this IP address is known as the mobile node's home address. A mobile node's home address remains unchanged regardless of where the node is attached to the Internet. The IP subnet indicated by this home address is the mobile node's home subnet and standard IP routing mechanisms will deliver packets destined to a mobile node's home address only to the mobile node's home subnet.

A mobile node is simply any node that may change its point of attachment from one 1P subnet to another, while continuing to be addressed by its home address. Any node with which a mobile node is communicating we refer to here as a correspondent node, which itself may be either mobile or stationary. A mobile node's current location while away from home is known as its care-of address, which is a globally-routable address acquired by the mobile node through IPv6 address auto configuration in the foreign subnet being visited by it. The association of a mobile node's home address with a care-of address, along with the Remaining lifetime of that association is known as a binding. While away from its home subnet, a

router on the mobile node's home subnet known as its home agent maintains a record of the current binding of the mobile node. The home agent then intercepts any packets on the home subnet addressed to the mobile node's home address and tunnels them to the mobile node at its current care-of address. The tunneling uses IPv6 encapsulation and the path followed by a packet while it is encapsulated is known as Tunnel as shown in Fig.2. The most important function needed to support mobility is the reliable and timely notification of a mobile node's current care-of address to those other nodes that need it, in order to avoid the routing anomaly known as triangle routing. But in IPv6, once a correspondent node has learned the mobile Node's care-of address, it may cache it and route its own packets for the mobile node directly there using an IPv6 Routing header, bypassing the home agent completely. Thus triangular routing is avoided in Mobile IPv6 which consumes more time.

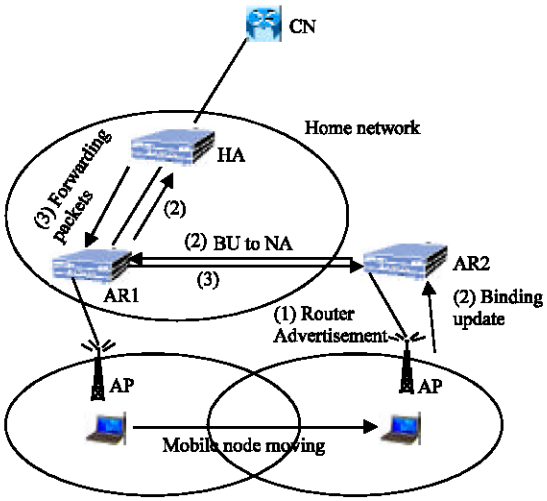

Fig. 2: Mechanism of MobileIPv6

Mobility management: Mobile IP in general and more specifically Mobile IPv6 solves the problem of mobility of a Mobile Node (MN) by managing the correspondence between the changing IP address of the MN, called the Care-of- Address (CoA) and an IP address permanently or semi permanently assigned to the MN. This permanent or semi permanent IP address is called the Home Address of the MN[4]. The Home Address of the MN has a network prefix of a link (or subnet) of the MN's so called home link. Thus, all the packets sent to the MN's Home Address by the communicating nodes (called Correspondent Node, CN) are routed to the home link, where the network entity called the Home Agent (HA) is present. The HA maintains a mapping between the CoA and the Home Address, called the binding, of the MN in a binding cache. When the MN is visiting a foreign network, the binding cache entry for the MN is activated and packets arriving for the MN are intercepted by the HA and tunneled (IPv6 in IPv6) to the CoA of the MN.

Ns2 network simulator and modifications: The version of NS-2 being used is 2.1b6. This version is the latest compatible[5] with all the required modules; Mobiwan module for Mobile IPv6, wireless and Mobile IPv4 modules. Mobile IPv4 module was contributed by Charles Perkins for use in wired simulations with an option for a simple wireless interface2. The author of this module is widely known for his work in Mobile IP. Mobiwan Mobile IPv6[6] is authored primarily by Thierry Ernst[7] from Inrialps Motorola Research Centre3. Wired nodes were enabled for basic IPv6 functionality required for Mobile IPv6, such as Binding Caches and Destination Option header for routing optimization. A new Network Routing protocol was devised as a replacement for the wireless adhoc routing protocols, with Mobile IPv6 functionality. As a consequence, Mobile Ipv6 is a wireless-client only simulation tool. The wired implementation of Mobile IPv4 was extended by the Rice Monarch Project for wireless capability. For completeness of their wireless module, MNs could interact with fixed base stations that were connected to wired nodes, to bring together wired and wireless topologies. The routing protocol used for this purpose is (DSDV) Destination-Sequenced Distance-Vector.

Other changes: A mistake was found in the wireless extension of Mobile IPv4, in the NS-2 simulator implementation. Incorrect behavior can arise if a care-of address is lost due to moving out of range while a second care-of address of the new base station is already known (which only occurs on the rare occasion of re-registering with the old base station within coverage overlap). This causes the MN to attempt to communicate with the new base station through the old base station. The mistake was to not set the node's base station when the care-of address is set, after the loss of the primary care-of address. Some default values in the NS-2 simulator needed attention to make comparison fair.

In the original NS-2 simulator implementation, for run-time optimization MIPv6 is defaulted to turn off sending router advertisements, so that simulation time is reduced for large scale topologies where a base station may not have any MNs to communicate with. Rather, these are turned on when the MN enters the site. However, this can cause a problem. Without the advertisements turned on by default, the mobile node must rely on solicitations

when entering a new coverage, removing any possibility for a smooth handover since a new base station cannot be detected While in coverage of the current one, but is only found after the current node is lost and the solicitation timer ends[6]. To solve this problem in our experiment, router advertisements were explicitly turned on for all base stations in the simulations.

Mobile IPv6 throughput: MIPv6 suffers a 1.35% increase in packet size due to its larger IP header; 1500 Bytes as compared to 1480 Bytes[8]. The packet TCP/IP packet size is different for Mobile IP versions so that final comparison can be made with identical payload (1440 Bytes) while including the different size of their respective headers.

Transmission control protocol: The Transmission Control Protocol is the reliable transport-layer protocol of the TCP/IP protocol suite that is responsible for error recovery and flow control. TCP is an ARQ protocol with a variable window size that is manipulated by the congestion avoidance algorithms. These algorithms are responsible for determining the congestion status of the sender-receiver pipe and enable the sender to adjust the amount of transmitted data. The TCP retransmission strategy is based on the retransmission timer. TCP is based on the assumption that network congestion is the reason for all packet loss. For this, the event of retransmission timeout is perceived by TCP as the main indication of network congestion. In the event of a timeout TCP resorts to exponential back-off. According to this algorithm TCP doubles the size of its timeout value. However, during MIP hand-offs a TCP communication will be forced to suffer several successive retransmissions which will extend the timeout value beyond the duration of the hand-off. As such even after its completion, a communication may not be resumed until the expiration of the extended timeout. The idle time that a TCP communication is required to sustain beyond the completion of the hand-off is termed as TCP back-off recovery time[9]. The congestion avoidance algorithms with greatest importance to this study are the Slow-Start and Fast-Retransmit. Slow-Start is always applied in the early stages of a communication when the capacity of the communication pipe is unknown. Slow-Start initially minimizes the congestion window and manages an exponential increase.

In the event of a TCP retransmission timeout the sender responds as if confronted by network congestion and repeats Slow-Start. However, a MIP hand-off is associated with extended service disruption and packet loss. Under such conditions TCP reacts falsely and resorts to Slow-Start which causes a minimization of the congestion window. Given the unknown congestion status of the incoming link, the reduction of the congestion window is not an unwanted effect. However, a complete minimization of the congestion window should be avoided. In the event of packet loss, all received packets that follow the lost packet are considered as out-of-sequence. Even though these packets are cached they can not be normally acknowledged. Instead TCP acknowledges the last in-order received packet for every out-of-sequence packet received. A series of out-of-sequence packets will cause the transmission of several duplicate acknowledgements (dupacks). If the number of dupacks supersedes a predefined threshold (usually 3) then the TCP sender determines that a packet has been lost. In this case TCP responds with the retransmission of the packet indicated by the dupacks plus an additional packet per dupack. This algorithm is known as Fast-Retransmit.

Simulation environment: The simulation scenario with all the participating entities and links is described in Fig. 3. The scenario consists of four 2Mbps Wireless LAN 802.11 DCF (Distributed Coordination Function) accordant Base Stations (BSs). All BSs are connected to different ARs and thus represent different IP subnet. During L2 handovers also L3 handovers are necessary to MNs. The BSs are connected via two routers (R1 and R2) and duplex links to the Border Router (BR), which acts as ingress and egress point to outer network. The border

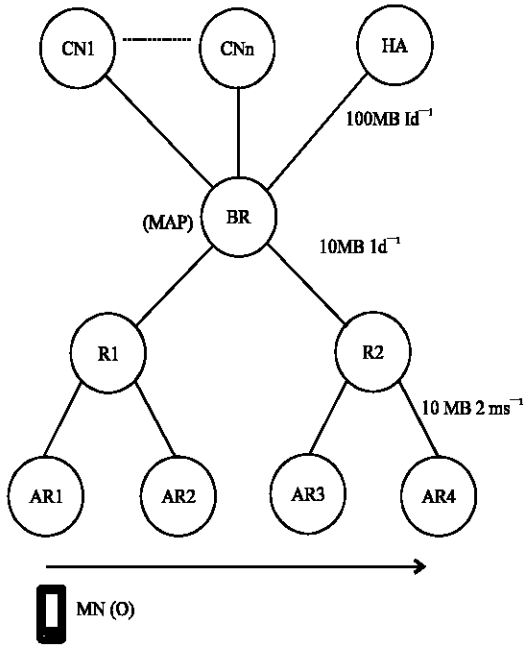

Fig. 3: Simulation scenario

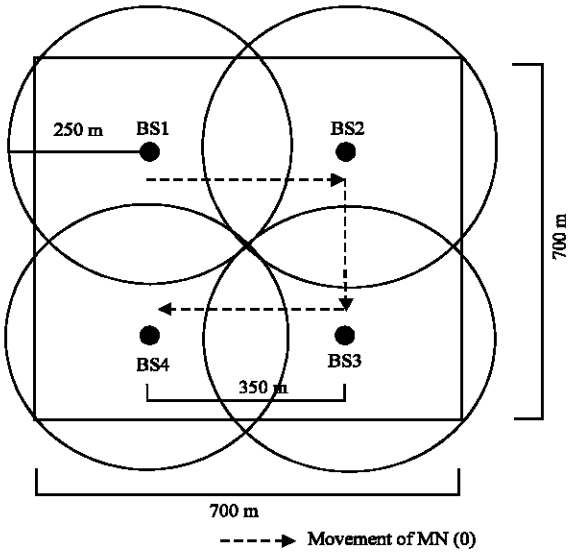

Fig. 4: The base station locations

router also functions as the mobility anchor point (MAP) for the Hierarchical MIPv6 handover method[10]. The HA and the CNs are located in the outer network.

Figure 4 presents the horizontal positions of the base stations. Movement area is 700×700 meters and the BSs cover the whole area. The transmission range of the BSs with omni directional antennas is about 250 meters and the minimum distance between the BSs is 350 m.

Simulation parameters and results: We can configure the parameters of the topology that already supported by NS-2. In order to simulate the real traffic, we set up-the Correspondent Node (CN) as a traffic source of a Constant Bit Rate (CBR) source over a Transmission Control Protocol (TCP), producing fixed length packets 200 bytes.

CN acts as a CBR traffic source can represent as a host that is streaming audio or Voice over Internet Protocol (VoIP). Then the Mobile Node (MN) acts as a sink receiving packets from CN. The setup link topology consists of wired link and wireless link. The wired link are fixed and used at the connection of CN to the Mobility Anchor Point (MAP) and MAP to the Access Router (AR). The bandwidth is set to the 100 Mbps and the Wired Link Propagation Delay is set to 2 ms. The Wireless link is used to the connection between AR to the mobile node. For the wireless link, bandwidth is considered 2 Mbps. The wireless delay can be as propagation delay and varies according to distance and the environment. For this simulation we may assume the propagation delay as the wireless link delay the delay varies from 10 to 50 ms. Throughput, Packet losses, packet roundtrip time and jitter occurrences are shown in figures below.

Simulation conditions: The network model for the simulation experiments consists of a fixed network and wireless network.

Topological conditions

- The number of MNs is 10. There are one HA, one BR (MAP), two routers R1, R2 and four BSs. Each BS has a circular cell whose radius is fixed to 250 m.
- For wireless communication, the transfer error is ignored and propagation delay is (distance between the R1 or R2 and the MN) / (speed of the light).
- Each MN has a uni-cast connection from the sender though the HA.
- The sender sends packets to the MN with a constant interval over TCP. The fixed packet length is 200 bytes.

General conditions

- An agent advertisement from each Router is periodically broadcasted every 0.2s within a whole cell area of the router. The MN's registration life time is 0.1-0.2 s.
- For wired connection Bandwidth is set to 100Mbps and propagation delay is 2 ms.
- For wireless link Bandwidth is 2Mbps and propagation delay varies between 10 to 50 ms according to the distance and the environment.

Mobility conditions

- The mobility is considered for the simple vehicular mobility in an urban area.
- The MN moves within a square of 700×700 m^2 including the overlapping regions.
- The MN straightly moves with in the square. The direction is randomly selected and the angle is restricted within ±90 degree from the current direction of the MN. However, the MN can select from all angles, when it stays less than 1m apart from any side of the square.

RESULTS AND DISCUSSION

From the Fig. 5 to 15 shown below throughput of the generating packets and sending packets is high enough. The number of lost packets will be very low. Round trip time relation ship also shown in graphs. Jitter occurrences are in Dropped packets also shown in Figures. We can

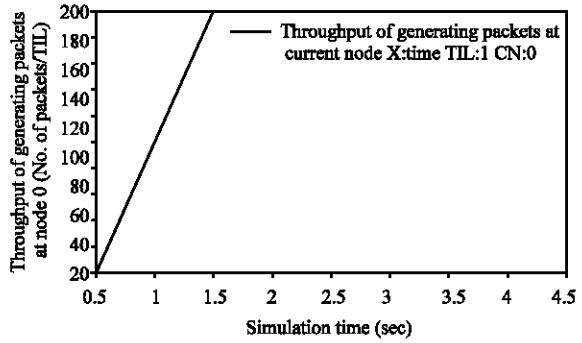

Fig. 5: Throughput of generating packets at current node Vs simulation time

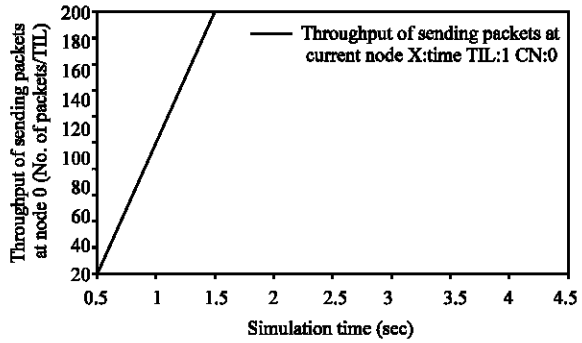

Fig. 6: Throughput of sending packets at current node Vs simulation time

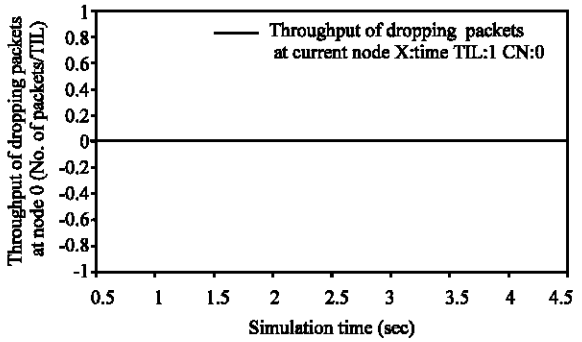

Fig. 7: Throughput of dropping packets at current node Vs drop event time

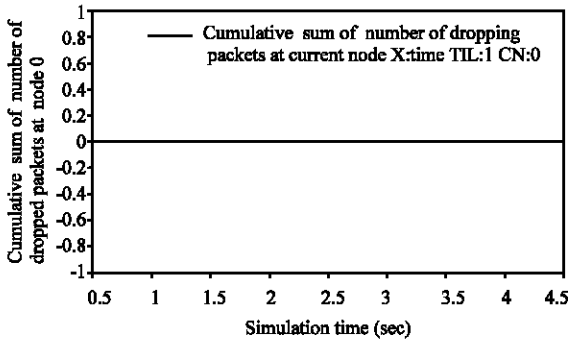

Fig. 8: Cumulative sum of dropped packets at current node Vs drop event time

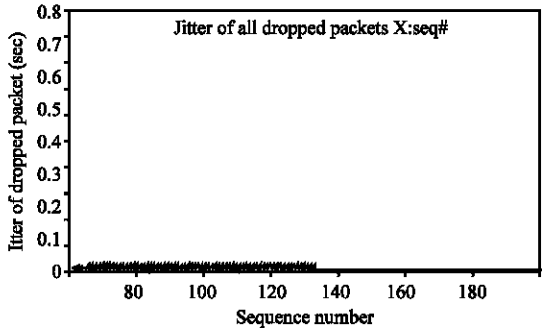

Fig. 9: Jitter of dropped packets Vs sequence number

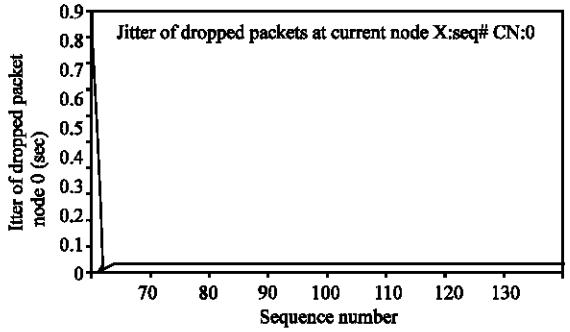

Fig. 10: Jitter of dropped packets at node 0 Vs sequence number

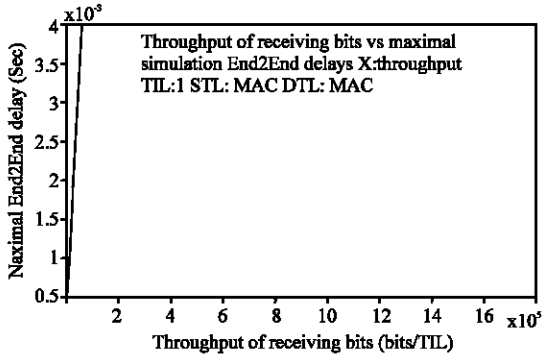

Fig. 11: Minimal end2end delay Vs throughput of receiving bits

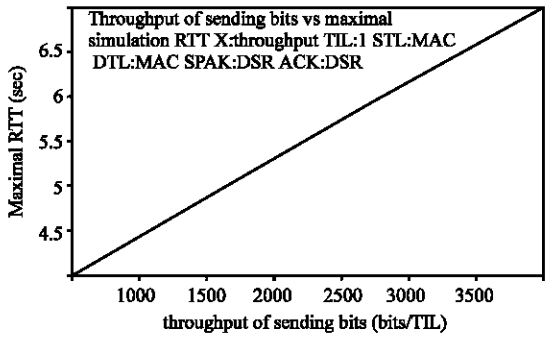

Fig. 12: Minimal RTT Vs throughput of sending bits

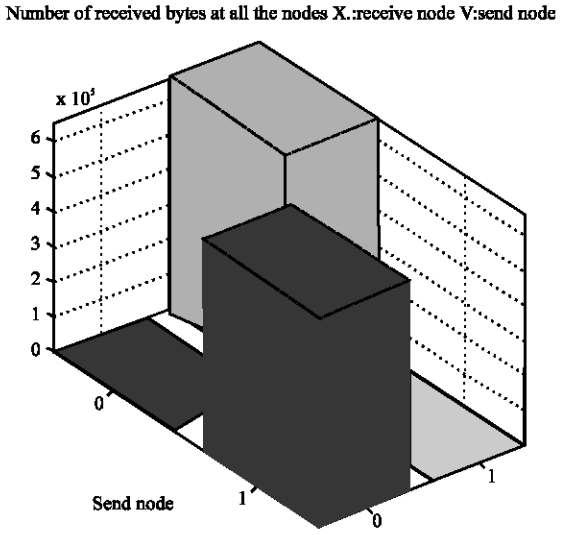

Fig. 13: Number of receiving bytes at all nodes

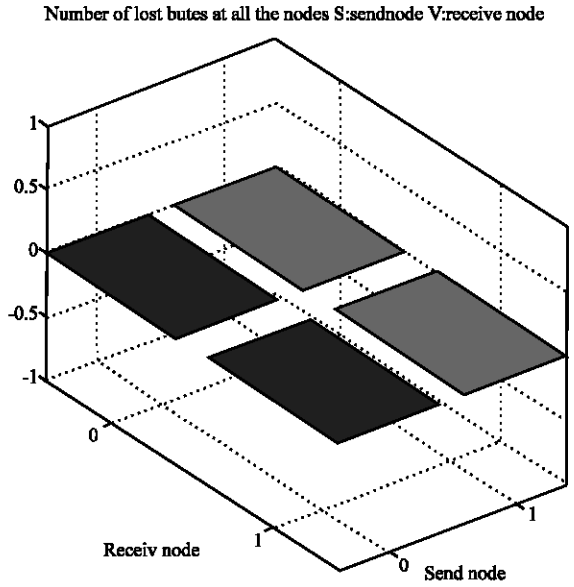

Fig. 14: Number of lost bytes at all nodes

conclude that performance of mobile IPv6 will be comparatively good and has been analyzed using graphs. In future, these results can be extended to the Hierarchical Mobile Ipv6 networks also.

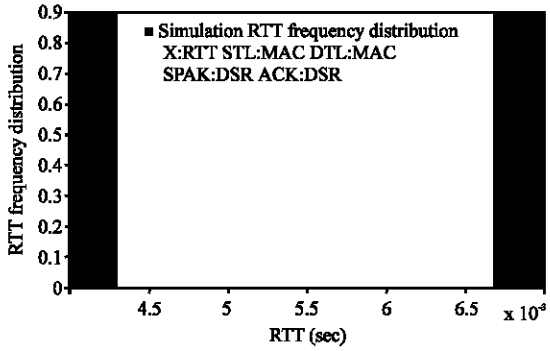

Fig. 15: RTT frequency distribution Vs RTT (sec)

REFERENCES

1. Information Sciences Institute, University of Southern California, 1981. Internet Protocol, Request for Comments 791, Internet Engineering Task Force.
2. Johnson, D., C. Perkins and J. Arkko, 2002. Mobility Support in IPv4. IETF RFC, pp: 3344.
3. Raicu, I., 2002. An Empirical Analysis of Internet Protocol version 6 (IPv6). Master Thesis, Wayne State University.
4. Johnson, D., C. Perkins and J. Arkko, 2004. Mobility Support in IPv6. IETF RFC, pp: 3775.
5. The Network Simulator (Ns-2), www.isi.edu/nsnam/ns
6. ns Mobiwan2.1b6 and ns-allinone-2.1b6 www.ns/inriaples/planet.fr
7. Ernst, T., 2001. Mobiwan: An Ns-2.1b6 simulation platform for mobileipv6 in wide area networks.
8. Damien Phillips and Jiankun Hu, 2002. Simulation study of TCP performance over mobile IPv4 and mobile IPv6.
9. Jaiswal, S. and S. Nandi, 2004. Simulation-based performance comparison of tcp-variants over mobile IPv6 based mobility management schemes 29th IEEE Local Computer Networks, November 2004, Tampa, Florida, USA.
10. Puttonen, J., A. Viinikainen, M. Sulander and T. Hamalainen, 2005. Performance Evaluation of Flow-based Fast Handover method for Mobile IPv6 Networks.