Tunneling-based Routing and Handover Decision Model for Proxy Mobile IPv6 Networks

Yunes Abdussalam Amgahd[1], Raghav Yadav[2]

[1]Computer Science and Information Technology, SHIATS-DU, Allahabad, India

[2]Computer Science and Information Technology, SHIATS-DU, Allahabad, India

Abstract: ***During mobile IPv6 route optimization, out-of sequence packets, communication disruption duration, and packet overhead may occur. In the network handover is important to achieve data communication during service degradation. To overcome these problems we introduced a novel tunneling based routing and handover decision model for Proxy Mobile IPv6 Networks. A tunneling based route optimization is useful in the architecture of PMIPv6 followed by a handover decision model for network selection based on various priority of traffic classes. We can observe the simulation results, how the proposed technique prevents the out-of sequence packets, minimize the communication disruption duration and packet overhead.***

Keywords: Mobile IPv6, Route Optimization, Handover, Tunneling-based routing

1. Introduction

1.1. Mobile IP Network

Mobile IP networks provide mobility support to the prevailing IP infrastructure with no need of adapting applications, fixed-end hosts, and routers. To optimize the route, fixed-end hosts provide additional support. IPv6 is an enhanced version of IPv4. IPv6 works better then IPv4 while providing important internetworking capabilities. IPv6 can also resolve the unanticipated IPv4 design problems. IPv6 increased ability, achieve scalability and quality of service to the next generation. The commercial-grade robustness for mobile connectivity, data communication, voice over IP and end-to-end interworking are the advantages of IPv6 [1].

1.2. Issues in Mobile IPv6 Network

Mobile IPv6 (MIPv6) suffers from various security problems even though it has a lot of features when compare with MIPv4. Some of the issues are as follows:

- Route optimization becomes insecure because there is no authentication mechanism between MN and CN.
- In case of connection hijacking, attacker redirects the packets to the random nonexistent address. This can be performed by hijacking the existing BU between two nodes for disturbing the communication.
- During denial of service attacks, the resources are not available to the intended users by the attackers. BU is spoofed to redirect data packets to random address, this cause to the network congestion.
- The eavesdropping attack occurs, when two nodes are communicate with each other at this time attacker listens to the traffic and obtains the essential information [3].
- When the attacker uses some modifying tools to set any desired IP address in the packet, impersonation attacks occur.
- The tunnels between the mobile device and the HA are sometimes attacked to make it appear that the mobile nodes are sending traffic when they are not sending.

1.3 Routing in Mobile IP Network

In mobile IP, the following are the fundamental assumptions made:

1) In routing the current location of node is identified and when node moves from one place to another place its IP address will be changed.
2) Routing infrastructure send packets to their intended destinations identified by their IP address.

The mobile device acquires a new care-of-address and informs the home agent (HA) about the address when it leaves its network and connects to another network. The new care-of address is recorded by HA in its binding table. MIPv6 routes the packet between mobile device and the correspondent nodes located on the IPv6 network. By using route optimization, the correspondent node caches the care-of address and then transfers the packets to the mobile device directly [2].

1.4 Media Independent Handover

Several Internet applications and services are developed and begins in market. Precise QOS should be ensured to the user to be a successful technology. Most of the current access systems can satisfy the QOS needs. However, satisfying the QOS demands becomes very challenging in heterogeneous environment.

The main aim of this standard is to improve handover performance between IEEE 802 networks comprising of both wired as well as wireless and also between IEEE 802 networks and non IEEE 802 networks irrespective of the media type in order to improve the user experience [11].

2. Related Works

An improved tunneling-based route optimization mechanism is proposed [4] to decrease the packet overhead. The tunnel manager is changed and binding update messages are changed for maintaining the compatibility with standard mechanisms. This mechanism shows that the reduced packet overhead when compared to bidirectional tunneling, route optimization, and tunneling-based route optimization. In mobile IP communication, more data can be transmitted via network because of less overhead for each packet. Overhead and delay are the performance metrics used. However, the total delay is same as that of the bidirectional tunneling, route optimization, and tunneling-based route optimization mechanisms; hence, it must be reduced [4].

Correspondent Information route optimization scheme is proposed [5], which removes the inefficient routing paths by forming the shortest routing path. This can be performed to address the triangle routing problem. Mobility and overhead are the performance metrics used. However, there is no ACK packet while transporting correspondent information from LMA to MAG. LMA did not know whether the binding process was complete. But, LMA re-transport correspondent message on next data transmission, accordingly not too extreme on correspondent information's loss for route optimization if the binding process was uncompleted

Time-based one-time password route optimization (TOTP-RO) [6] solves the longer service disruption and high overhead problems for mobile IPv6. The correspondent node compatibility test was executed along with the computation of the shared secret token and authentication via TOTP technique. This reduces the handover signaling and delay when the correspondent node does not have an active implementation of mobile IPv6. MN's authentication was through a shared secret token and TOTP that resulted in MN's direct authentication and reduced overall service disruption for real-time applications. However, there is more service disruption delay and overhead in the network.

The global IPv6 based MANET is proposed it can maintains the routing and addressing itself and having self-infrastructure and solve the connecting problems in MANET. This can be performed by supporting IPv6 mobility. The nodes are automatically organized into tree architecture. Their global IPv6 addresses are allocated based on the soft-state routing cache and longest prefix matching, unicast and multicast routing protocols are designed for IPv6-based MANET. They support mobile IPv6 and design a peer-to-peer information sharing system. A prototyping system can be implemented for demonstrating the possibility and efficiency of P2P information sharing system and IPv6-based MANET. The performance metrics of this system is number of packets delivered, average file search and delay. Even though it achieve routing protocol and P2P file sharing efficiently, but it have more power consumption.

A right-time path switching technique has been proposed [8] for providing PMIPv6 route optimization. By using signaling messages, this technique initiates the path switch when the optimized path is ready. Out-of-sequence packets are stop by this feature. The disruption duration is reduced in the route optimization procedure. By using actual PCs, this process is evaluated in an experimental test-bed. Results show that this method avoids out-of-sequence packets, whereas the baseline route optimization process causes them. During the route optimization procedure, this method has performance improvement in TCP throughput or seamless continuity of real-time applications. Communication disruption duration, delay gap, and number of out-of-sequence packets are the performance metrics used. However, it may be affected by malicious nodes in the network [8].

DMAPwSR [9] is a cross-layer integrated mobility and service management scheme in mobile IPv6 environments. This scheme reduces the overall mobility and service management cost in order to serve the mobile users with service characteristics and diverse mobility. Each mobile node (MN) can utilize its cross-layer knowledge to choose the smart routers as its dynamic mobility anchor points (DMAPs), thereby balancing the cost associated with packet delivery services versus mobility services. These smart routers perform the role of access routers in case of MIPv6 systems and process the binding messages sent from the MN. Then, the MN's present location can be stored in the routing table to forward the service packets that are destined to the MN. MN's DMAP varies dynamically since the MN roams across the MIPv6 network. In addition, DMAP service area dynamically varies by reflecting the dynamic MN's mobility and service behaviors. Unlike HMIPv6, DMAPwSR takes the integrated service management and mobility into account. An analytical model is built on the basis of stochastic Petri nets in order to analyze DMAPwSR and compare its performance against MIPv6 and HMIPv6. The performance metrics used are network cost. However, there are some load-balancing issues during DMAP selection, and several performance metrics are not considered [9].

The long-handoff latency, route optimization and bottleneck problems are solved by Cluster-based sensor proxy mobile IPv6 (CSPMIPV6) [10]. The clusters are created by grouping mobility access gateways (MAGs). A cluster head MAG is selected for each cluster to reduce the load on LMA. This can be performed by using intra-cluster handoff signaling and an optimized path for data communications. The local handoff delay, LMA load and transmission cost are the metrics to calculate. Results show that CSPMIPv6 performs well when compared to SPMIPv6 and PMIPv6 protocols. However, the other metrics such as overhead, energy consumption and so forth are not considered.

3. Proposed Solution

3.1 Overview

In this paper, we design a tunneling-based routing and handoff technique for Proxy Mobile IPv6 networks. In this technique, a tunneling based route optimization is applied in the architecture of PMIPv6. After the optimized path is established, a media independent handover method is initiated for network selection based on various priority of traffic classes.

3.2 Improved Tunneling Based Route Optimization

Let Nmo and Nco be the mobile and corresponding node respectively.

Let HA and CA be the home and care of address respectively

Let TM be the tunneling manager

An improved tunneling based rote optimization is applied in the architecture of PMIPv6 (Shown in Fig 1) to reduce the packet overhead. Initially a tunnel is launched between Nmo and Nco. In addition, a BU message is transmitted for constructing binding cache in CA and HA of the other node pair. The steps involved in this route optimization technique are as follows:

1) When Nmo wants to transmit a data packet to Nco, it sets source of the packet to HA of Nmo and destination of the packet to the HA of Nco.
2) When TM receives the packet, it updates the packet by modifying the source and destination address of the packet.

i.e.

- It modifies the source field from HA to CA.
- It detects the CA of the Nco and update it in a destination address field.
- TM then transmits the modified data packet to the Nco through the tunnel.
- When Nco collects the data packet, it performs the following:
- Modifies the destination of the packet from CA of Nco to the HA of Nco.
- Searches the CA of Nmo in the binding cache to detect HA
- Modifies the source of the packet from CA of Nmo to HA of Nmo.
- The updated packet is transmitted to the upper layers
- When Nco wants to transmit the data packet to Nmo, the following steps are performed.
- The address of the data packet is changed from HA of Nco to HA of Nmo.
- When the TM of Nco receives the packet, owing to the binding cache, the destination of the packet is modified from HA of Nmo to CA of Nmo and source of the packet from HA to CA.
- The updated packet is then tunneled to Nmn

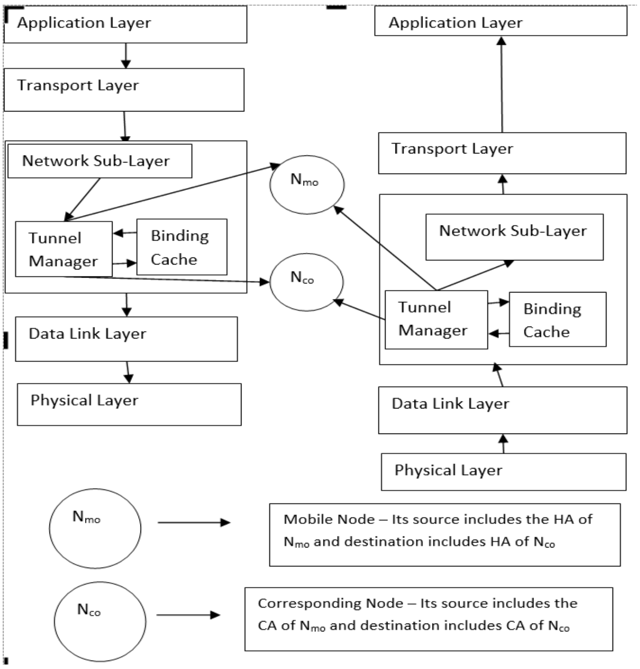

Figure 1: Route Optimization Protocol Model and Packet Transmission

In wireless networks the traffic can be transmit in different types, those are Constant Bit Rate (CBR), Variable Bit Rate (VBR) and Best effort traffic. The transmission of these type of traffic depends on some factors. But each traffic type is different from each other and depends on different factors. The CBR and VBR traffic depends on factors like received signal strength, bandwidth, data rate and battery power.

Due to different factors like received signal strength lower than computable threshold, lower power due to exhausted battery, unavailability of bandwidth due to congestion in the network or lower data rate these cause to network degradation. In this case, handover becomes necessary to sustain efficient data transmission. Using media this process is described in algorithm.

Algorithm:

1) When a MN experiences service degradation, it determines the traffic type that are being prone to degradation.
2) The traffic types that are subjected to degradation are prioritized in the following descending order: CBR (C1), VBR (C2) and best effort (C3).
3) In traffic prioritization the highest priority traffic is considered first, and the remaining traffic types are considered in the defined order.
4) The MN requests by sending Resource Allocation Check Request (RAC. Req. to the current serving network for resource availability check of the particular service through MIHF.

$$MN \xrightarrow{\text{RAC req.}} MAG \xrightarrow{\text{RAC req.}} MIHF$$

Where MAG is the mobile access gateway.

5) On receiving the request, the MAG and MIHF determine the RSSI value based on the RSSI [9] given according to (1).

$$RSSI = 10.n.\log_{10}(d) + A$$

6) Then the data rate (DR) is estimated based on the rate at which the date is streamed at the MAG.

7) Next the battery power (BP) is calculated according to (2)

$$BP = [BP_i - (BP_{tx} + BP_{rx})]$$

8) Finally, the bandwidth (BW) is determined by the channel capacity.
9) After estimating the values of all the parameters, the MIHF analyzes the values.
10) The MIHF responds with negative acknowledgement (Neg. ACK) indicating minimum availability of the requested resource.

$$MN \xleftarrow{\text{Neg. Ack.}} MAG \xleftarrow{\text{Neg. Ack.}} MIHF$$

11) After confirming the unavailability of the required resource, the MN initiates the handover process.
12) The MN sends a Resource Accessibility Request, (RA req.) to the serving MAG.

$$MN \xrightarrow{\text{RA. Req.}} MAG$$

13) Then the serving network MAG responds by Positive Acknowledgement permitting the handover process to initiate.

$$MN \xleftarrow{\text{Pos. ACK}} MAG$$

14) This depicts the initiation of the handover process and the total delay involved in the initiation phase is estimated by (3).

$$T_{initiation} = t_{MN_{req}} + t_{BS_{resp}}$$

Where $t_{MN_{req}}$ is the Time to request resource check in serving network by MN and $t_{BS_{resp}}$ is the Time taken by BS to respond back to MN.

15) Next the MIHF queries the MIIS server for the information related to the neighboring nodes that possess the resource in demand; which are considered as candidate nodes.

$$MIHF \xrightarrow{\text{Cand\_Info\_Req}} MIIS$$

16. The MIIS server responds by providing the information related to all the candidate nodes that can be accessed.

$$MIHF \xleftarrow{\text{Cand\_Info\_Req}} MIIS$$

16) The MIHF informs the MAG, and thus the MN, about all the available candidate nodes.

Thus, the MN experiencing service degradation collects the information about all the candidate nodes.

4. Simulation Results

4.1 Simulation Parameters

We use NS2 [11] to simulate our proposed Tunneling-based Routing and Handover decision model (TRHDM). We use the IEEE 802.11 for wireless LANs as the MAC layer protocol. It has the functionality to notify the network layer about link breakage. In our simulation, the packet sending rate is varied as 50, 100, 150, 200 and 250Kb. The area size is 600 meter x 600 meter square region for 50 seconds simulation time. The simulated traffic is Constant Bit Rate (CBR). The simulation topology and settings are given in figure 2 and table 1, respectively.

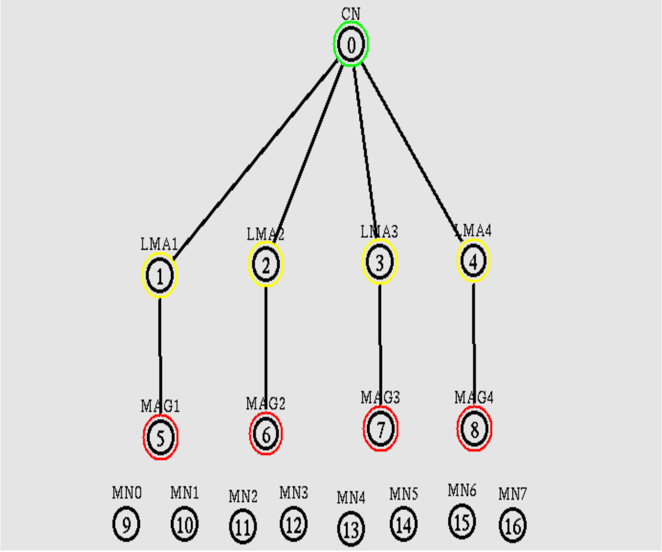

Figure 2: Simulation Topology

Table 1: Simulation parameters

Parameters	*Value*
No. of Mobile Nodes	8
Area	600 X 600
MAC	802.11
Simulation Time	50 sec
Traffic Source	CBR and Video (VBR)
Rate	50, 100, 150, 200 and 250Kb
Antenna	Omni-antenna
No. Of Wired Nodes	5
No. Of Base Stations	4

4.2 Performance Metrics

We calculate performance of the new protocol mainly according to the following metrics. The proposed TRHDM model is evaluated with the RPST [8] protocol.

Average Packet Delivery Ratio: The ratio between the numbers of packets delivered at destination and the number of packets sending by the source.

Average end-to-end delay: The end-to-end-delay is average taken by data packets to reach from the sources to the destinations.

Throughput: The throughput is the amount of data that can be sent from the sources to the destination.

Packet Drop: It is the number of packets dropped during the data transmission

4.3 Results & Analysis

In the experiment, we vary the transmission rate as 50, 100, 150.200 and 250 Kb for both CBR and VBR traffic.

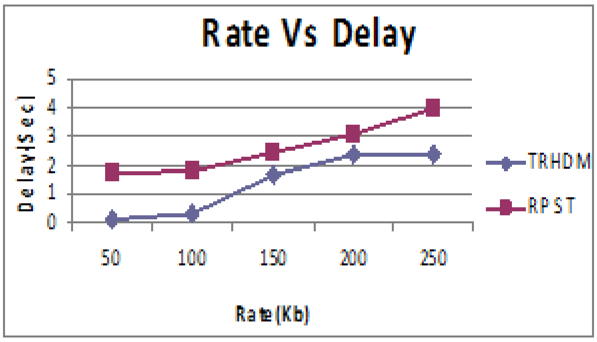

Figure 3: Rate Vs Delay

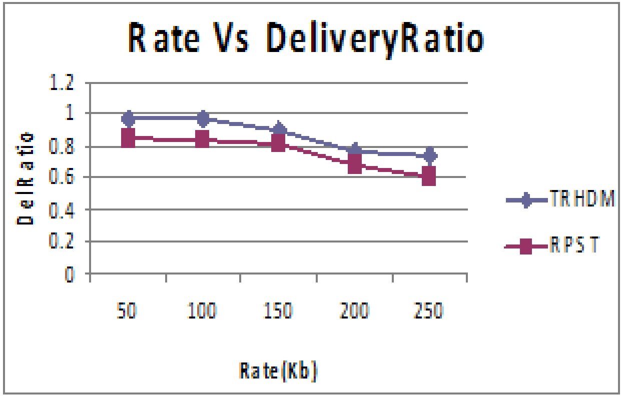

Figure 4: Rate Vs Delivery Ratio

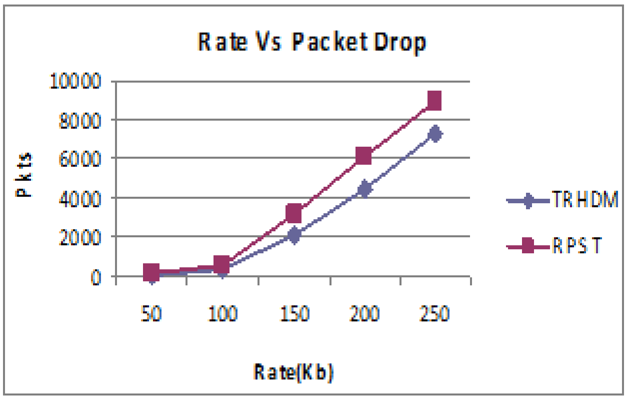

Figure 5: Rate Vs Drop

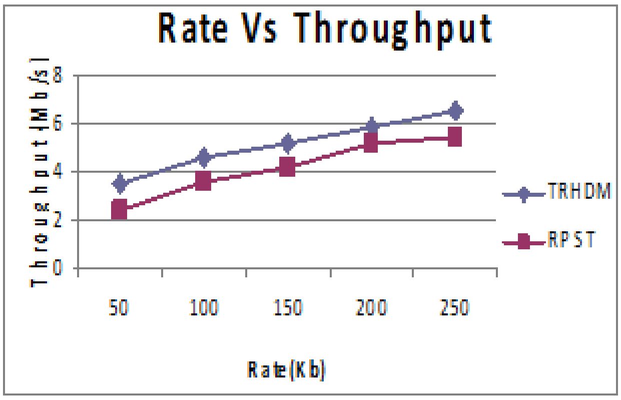

Figure 6: Rate Vs Throughput

Figures 3 to 6 show the results of delay, delivery ratio, packet drop, throughput by varying the rate from 50Kb to 250Kb for the CBR traffic in TRPST and RPST protocols. When comparing the performance of these two protocols, we infer that TRPST outperforms RPST by 53% in terms of delay, 12% in terms of delivery ratio, 31% in terms of packet drop and 20% in terms of throughput.

5. Conclusion

In this paper, we have designed a tunneling-based routing and handover decision model for Proxy Mobile IPv6 networks. Initially, a tunneling based route optimization is applied in the architecture of PMIPv6. After the optimized path is established, media independent handover decision model is initiated for network selection based on various priority of traffic classes. By simulation results, we have shown that the proposed technique prevents the out-of sequence packets, minimizes the communication disruption duration and packet overhead.

References

[1] Harith A. Dawood, "IPv6 Security Vulnerabilities", International Journal of Information Security Science, Vol. 1, No. 4.

[2] Abdel Rahman Alkhawaja & Hatem Sheibani, "Security issues with Mobile IP", Master's Thesis in Computer Network Engineering, 2011.

[3] Chitra Dhawale, Aumdevi K.Barbudhe, Vishwajit K.Barbudhe, "A Robust Secured Mechanism for Mobile IPv6 Threats", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 6, November- December 2012, pp.918-921.

[4] Hooshiar Zolfagharnasab, "Reducing Packet Overhead In Mobile IPv6", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.3, May 2012.

[5] Young-Hyun Choi, Tai-Myoung Chung, "Using Correspondent Information for Route Optimization Scheme on Proxy Mobile IPv6", Journal of Networks, Vol. 5, No. 8, August 2010.

[6] Peer Azmat Shah, Halabi B. Hasbullah, Ibrahim A. Lawal, Abubakar AminuMu'azu and Low Tang Jung, "A TOTP-Based Enhanced Route Optimization Procedure for Mobile IPv6 to Reduce Handover Delay and Signalling Overhead", Hindawi Publishing Corporation e Scientific World Journal, 16 pages.

[7] Chiung-Ying Wang, Cheng-Ying Li, Ren-Hung Hwang, Yuh-Shyan Chen, "Global Connectivity for Mobile IPv6-based Ad Hoc Networks".

[8] Yujin Noishiki, Yoshinori Kitatsuji, Hidetoshi Yokota, "Right-time Path Switching Method for Proxy Mobile IPv6 Route Optimization", ICNS 2011: The Seventh International Conference on Networking and Services, 2011.

[9] Ding-Chau Wang, Weiping He, Ing-Ray Chen, "Smart Routers for Cross-Layer Integrated Mobility and Service Management in Mobile IPv6 Systems", Wireless Pers Commun, Springer Science+Business Media, LLC. 2012.

[10] Adnan J Jabir, Shamala K Subramaniam, Zuriati Z Ahmad and Nor Asilah Wati A Hamid, "A cluster-based proxy mobile IPv6 for IP-WSNs", Journal on Wireless Communications and Networking 2012, 2012:173.

[11] P.Vetrivelan,P.Bhoopathi and P.Narayanasamy, "Application-Oriented Media Independent Vertical Handover Decision (AMIVHD) in 4G Heterogeneous Wireless Networks",The International Conference on Communication, Computing and Information Technology (ICCCMIT) 2012.

[12] Network Simulator: http:///www.isi.edu/nsnam/ns

Author Profile

Yunes Abdussalam Amgahd is a student of Ph.d in the department of Computer science and engineering from SHIATS, Allahabad. He received his M.tech degree from SHIATS, Allahabad.

Raghav Yadav is an assistant professor in Sam Higginbottom Institute of Agriculture, Technology and Sciences (SHIATS), Allahabad, India. He obtained Ph.D. and M.Tech degree in computer science and engineering from (MNNIT), Allahabad and B.E. degree in electronics engineering from Nagpur University. He guided various project and research at undergraduate and postgraduate level. He has published more than 20 research papers in national/international conferences and refereed journals. His research interests are in the field of optical network survivability, ad-hoc networks, and fault tolerance systems.