World Applied Sciences Journal 28 (8): 1134-1145, 2013
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2013.28.08.1481

Performance Analysis of QoS Scheme Supported in MIPV6 Network

Loay F. Hussien, A.H. Aisha-Hassan and Mohamed Hadi Habaebi

Department of Electrical and Computer Engineering, Faculty of Engineering,
International Islamic University Malaysia, 50728 Kuala Lumpur, Malaysia

Abstract: The contemporary Internet that we have been using today is based on Best-Effort (BE) service only, where packets are assigned and forwarded with the same priority. The BE service is acceptable only for traditional Internet applications like e-mail, web browsing and file transfer. However, it is not adequate for the applications like video conferencing, voice over IP (VoIP) and video on demand (VoD), which require high bandwidth, low delay and delay variation. Obviously, with the emergence of new real-time applications and Quality of Service (QoS) requirements, the Best Effort service becomes insufficient. Therefore, the Internet community has developed a number of new technologies to provide QoS in the Internet such as IntServ, DiffServ and MPLS. The differentiated service (DiffServ) is the most important distinct technology due to its simplicity and scalability benefits. It has been endorsed by Internet Engineering Task Force (IETF) to satisfy the requirements of new real-time applications. Internet Protocol was not designed taking into account mobility of users and terminals. In few years later, the IETF has developed protocols such as Mobile IPv4 (MIP) and Mobile IPv6 (MIPv6) for supporting seamless connectivity to mobile hosts. Mobile IPv6 is considered one of the important host mobility protocols, which was defined more in (RFC 3775 and RFC 6275). This paper acquaints with analytical analysis for the previously proposed scheme (DiffServ-MIPv6) that applies the DiffServ methodology techniques to Mobile IPv6 network in order to suit the needs of both QoS guaranteed and mobility in communication. The analytical study is investigated to evaluate the performance of the proposed scheme (DiffServ-MIPv6) compared to the native standard MIPv6 protocol in terms of signaling cost. The numerical results are measured against two factors, binding lifetime period and wireless link delay as well.

Key words: Quality of Service · DiffServ · Mobile IPv6

INTRODUCTION

Sustaining Quality of Service (QoS) in the Internet is deemed one of the main challenges facing many researchers nowadays. Concerning the network viewpoint, QoS is the ability of network elements (e.g. application, host and router) to provide some level of assurance that its traffic and service requirements can be satisfied. QoS manages bandwidth according to application demands and network management setting.

Native IP is connectionless and offers Best-Effort services. The service received by a user depends on the network load. Managing queues within routers is essentially through First in First out (FIFO) order. So the delivery time of packets is not guaranteed and packets may even be dropped because of congestion inside the network. This unpredictability doesn't mesh well with real-time applications, which cannot tolerate delay jitter or loss of data in transmission. To overcome these issues, Internet Engineering Task Force (IETF) has developed new technologies and standards to provide resource assurance and service differentiation in the internet, under the umbrella term QoS. These standards are Integrated Services (IntServ) [1], Differentiated Service (DiffServ) [2] and Multiprotocol Label Switching (MPLS) [3]. The positions of Integrated Services, Differentiated Service and MPLS in the network layers are depicted below in Figure 1.

Corresponding Author: Loay F. Hussien, Department of Electrical and Computer Engineering, Faculty of Engineering, International Islamic University Malaysia, 50728 Kuala Lumpur, Malaysia.

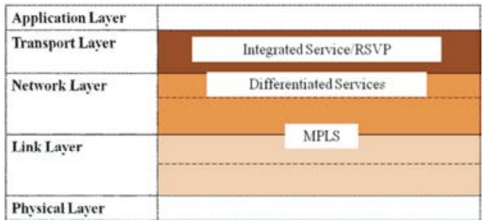

Fig. 1: The location of QoS standards

Integrated services use reservation to provide guarantee resources to individual flows. The differentiated services architecture takes a different approach. It combines edge policing, provisioning and traffic prioritization to provide different levels of services to customers. MPLS addresses the issues of the bandwidth provisioning and performance optimization in Internet backbones. The explicit route mechanism in MPLS adds an important capability to the IP-based network. These QoS solutions are designed in the context of a static environment (i.e. fixed hosts and networks). However, they are not effusively adapted to mobile environments. They demands to be extended and adjusted to meet up various challenges involved in mobile environments.

Mobile IPv6 is a network layer protocol for enabling mobility in IPv6 networks. It grants uninterrupted network connectivity while the mobile node (MN) roams among various access points and keeps changing its point of attachment into the network over time. Nevertheless, the MIPv6 protocol doesn't provide QoS guarantees to its users same as native Internet IP. Basically, all the users will have same level of services without considering about their application's requirement. This poses a problem to real-time applications that required QoS guarantees. To gain more effective control of the network, incorporated QoS is needed.

The remaining of this paper is prearranged as follows. Section 2 presents background and related works. Section 3 briefly spells out the proposed scheme that integrate DiffServ within mobile environment. Section 4 explores the performance evaluation. Finally, the conclusion is written in Section 5.

Background and Related Works: Mobility is an indistinct term that can be identified in several levels [4]. Usually, there are user mobility, personal mobility and host mobility. Mobile hosts can be connected to the Internet by using wireless network interfaces. Due to handover procedures the mobile node may change its point of attachment each time it moves to a new link. The Internet mobile users require special support to maintain connectivity. This support should provide transparency to mobile users. Namely, the higher level protocols should not be affected by adding this mobility support. Thus, it is became quiet urgent to propose an efficient protocols that must be able to inform the network about this movement. By doing so, the Internet data packets will be delivered in a seamless way to the new point of attachment. In short, mobility management is a process to enable a network to locate roaming users in order to deliver data packets (i.e. location management) and maintain connections with them when moving into a new subnet (i.e. handover management). The Mobile IPv4 and Mobile IPv6 are examples of mobility management protocols that will briefly discuss in the next following sub-sections.

Mobile IP (MIPv4): The Mobile Internet Protocol (Mobile IP) is an extension to the Internet Protocol. It was proposed by the Internet Engineering Task Force (IETF). Briefly, the Mobile IPv4 protocol (RFC 3344, 2006) allows a mobile node to maintain the same IP address (its home address) wherever it attaches to different networks. It purposes to provide the mobile user with the same services as in fixed user without changing the existing applications. Also, the mobile node has Care-of Address (CoA), which connects to the subnet where mn is currently located. The Care-of Address is managed by a Home Agent (HA), which is a device on the home subnet of the mobile device. It keeps tracking of the current location of the mobile node. Any packet addressed to the IP address of the mobile device is intercepted by the home agent and then forwarded on to the care-of address through a tunnel. Once it arrives at the end of the tunnel, the datagram is delivered to the mobile device through the foreign agent [5].

Mobile IP Operations: Mobile IP is a way of performing three related functions:

- Agent Discovery: Mobility agents advertise their availability on each link for which they provide service.
- Registration: When the mobile node is away from home, it registers its care-of address with the home agent.
- Tunneling: In order for datagrams to be delivered to the mobile node when it is away from home, the home agent has to tunnel the datagrams to the care-of address.

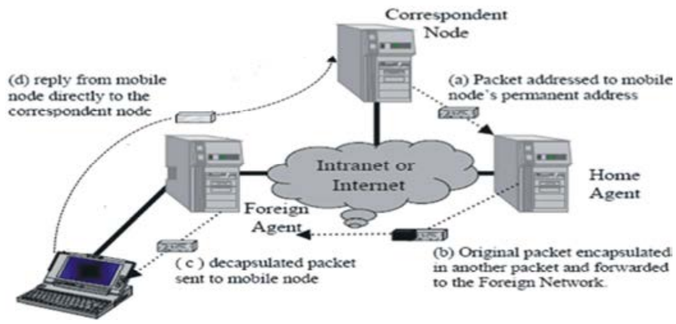

Fig. 2: Communication between a correspondent node and a mobile node on a foreign network [5]

Making the use of above-mentioned operations, the following theory will give a rough outline of the operation of Mobile IP protocol. Mobility agents (home agents and foreign agents) advertise their presence in the network by means of agent advertisement messages. The MN may optionally send an Agent Solicitation message on the link of the new foreign network to find the active mobile agents quickly. When the mobile node is connected with a network, it listens to advertisements broadcast by mobility agents. If the network prefix changes, the mobile node will detect a movement. The mobile may hear more than one prefix, thus it needs to make a decision about which network to log onto or perform a handover to. It is now located in a visited network and tries to acquire a new temporary address. The new address can either be obtained by an auto-configuration mechanism like Dynamic Host Configuration Protocol (DHCP)[6] or by the actual address of the Foreign Agent. The former is called Co-located Care-of-Address (CCOA) and the latter is called Foreign Agent Care-of-Address (FA-COA). The use of CCOA has the advantage that the mobile node does not need a foreign agent to be present at every network that it visits, but it does require that the DHCP server make a pool of IP addresses available for visiting mobile nodes. If CCOA is acquired, the mobile node registers this new temporary address with the Home Agent (HA) by exchanging registration requests and responses using CCOA as source address. If FA-COA is acquired, the mobile node cannot register itself to its home agent directly, but instead the foreign agent will dispatch the registration to the home agent.

Once the home agent has registered the care-of address for the mobile node in its new position, any packets intended for the home address of the mobile node are intercepted and encapsulated by the home agent and tunneled to the care-of address as shown in Figure 2.

The tunnel endpoint may be at a foreign agent (if the mobile node has a foreign agent care-of address), or at the mobile node itself (if it has a CCOA). In first case, packet arrives at the end of the tunnel is decapsulated and then is delivered to the MN’s CoA by the FA. In the second case, the packets are tunneled from the HA to the MN and then decapsulated by MN itself. A MN sends its packets directly to the CNs using normal IP routing, which does not need encapsulation. The MN uses its Home Address as the source address of all IP datagrams that it sends.

The main issues of MIPv4 are security and routing. Informing any agent in the routing infrastructure about the new location of the mobile node requires good authentication facilities, which are not commonly deployed in IPv4 nodes. The existing of the firewalls cause difficulty for Mobile IP because they block all classes of incoming packets that do not meet specified criteria. Even though this permits management of internal nodes without great attention to security, it presents difficulties for mobile nodes wishing to communicate with other nodes in their home enterprise networks. The triangle routing is also an issue that creates sub-optimal performance [7].

Mobile IPv6: Mobile IP support in IPv6 (RFC 3775, 2004) was designed to allow nodes to be reachable and maintain ongoing connections while changing their location within the topology. It can provide mobility support that combines the experiences gained from the development of Mobile IP support in IPv4 and the new features of the IPv6 such as Route Optimization (RO), additional automatic IP configuration and the increased number of available IP addresses (it is allowing about 2^128 or 340,282,366,920,938,463,463,374,607,431,768,211,456 addresses). The protocol also enables IPv6 nodes to cache the binding of a mobile node's home address with its care-of address and then to send any packets destined for the mobile node directly to it at this care-of address

[8]. In addition, there is no longer need to deploy special routers as Foreign Agents (FAs) that are used in Mobile IPv4. In Mobile IPv6, mobile nodes make use of the enhanced features of IPv6, such as Neighbor Discovery [9] and Address Auto-configuration [10], to operate in any location away from home without any special support required from the local router. Moreover, in MIPv6, the Home Agent (HA) no longer exclusively deal with the address mapping, but each CN can have its own 'binding cache' where home address plus care-of address pairs are stored. This enables 'route optimization' without the need to triangle routing via the HA that occurs in MIPv4 (a CN is able to send packets directly to a MN when the CN has a recent entry for the MN in its corresponding binding cache). The route optimization is now built in as a fundamental part of Mobile IPv6, rather than being added on as an optional set of extensions. To provide those optimizations Mobile IPv6 requires the exchange of additional messages, defined as IPv6 Destination Options.

Mobile IPv6 Operations: In Mobile IPv6, each MN is always given a Home Address (HoA) by the home network. While away from its home network, an MN is also associated with a care-of address (CoA), which provides information about the MN's current location. A special node home agent (HA) is designed to act as proxy for the MN when it moves away from the home network. Discovery of New Access Router (NAR) is performed through Router Solicitation/Advertisement (RS/RA) messages exchange. This procedure is referred to as movement detection. Furthermore, to ensure that a configured CoA (through stateless or stateful mode) is likely to be unique on the new link, the Duplicate Address Detection (DAD) procedure is performed by exchanging Neighbor Solicitation/ Advertisement (NS/NA) messages. If the sequent duplicate address detection (DAD) process is performed successfully (i.e. after acquiring a CoA) an MN performs binding update to the home agent (HA) through binding update (BU) and binding acknowledgment (BAck) messages exchange. To enable route optimization (RFC 4866, 2007), BU procedure is also performed to all active CNs. However, return routability (RR) procedure must be performed before executing a binding update process at CN in order to insure that BU message is authenticated and does not originate from a malicious MN. It is designed to verify that the mobile node is reachable at both its home address and its care-of address.

The home address must be verified to prevent spoofing of binding updates. While the care-of address must be verified to protect against denial-of-service attacks in which the correspondent node is tricked to flood a false care-of address with packets. Although RR procedure helps to avoid session hijacking, it increases delay of the BU procedure as illustrated in Figure 3. If the CN sends packet directly to a MN, it won't encapsulate the packet as the HA did when received packet from the CN, instead it makes the use of IPv6 Routing Header Option. When the CN does not have a binding cache entry for the MN, it will send the packet indirectly to the MN's home address. The Home Agent (HA) will then forward the packet to MN. Once the MN receiving encapsulated packets, it will inform the corresponding CN about the current CoA. The most significant difference between MIPv4 and MIPv6 is that MIPv6 is integrated into the base IPv6 protocol and is not an added-on as a new feature (as is the case with IPv4 and MIPv4). This integrated aspect of IPv6 with MIPv6 makes the standard MIPv6 more efficient and much easier to implement.

The authors in these papers [11, 12] identified the use of differentiated service (DiffServ) model to provide various demand of new application in mobile IPv6 networks. The major contribution of this work is to proposed operational procedures and cost evaluation schemes for seamless connection. Thus during the mobile node (MN) changes its point of attachment in network, the QoS requirement would be satisfied. Moreover, priority queue is used to manage three types of services and their performances are evaluated. Even though, the work presented procedures for acquiring the MN's service profile and additive information in the messages according to MN's moving area, fast handoff and security problems need to construct more efficiently.

Quality of Service and mobility for the wireless Internet approach [13] is the named paper that extends DiffServ to control resource utilization on each wireless cell and limits number of active hosts to keep the load sufficiently low. It also adopts the idea of IntServ by adding a QoS signaling for QoS negotiations between mobile nodes and access router. All mobile nodes and access routers provide Diffserv functions, i.e. the edge and core router functions, so that traffic sources are controlled in each wireless cell.

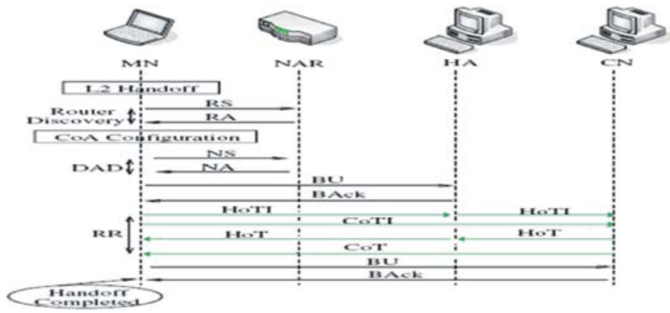

Fig. 3: Components of IPv6 handover

Another work in [14] investigated a study of profiled handoff for DiffServ-based mobile nodes, which shows transferring contexts to the new edge routers of wireless subnets helps various marking schemes reach stability earlier. This work is important in designing connection admission control algorithms at the radio edge router (RER). However, more investigation is required to analyze the relative performance impact on the traffic at the new AR caused by the flows that are handed over to the new AR.

The Proposed Scheme: This previous research work [15] has proposed a new scheme to support QoS in the next generation Internet. It integrates an existing QoS model over IP architecture with the standard MIPv6 protocol. The aim is to suit the needs of both QoS guaranteed and mobility in communication.

The proposed scheme (DiffServ-MIPv6) is built on the use of the basic mechanisms in DiffServ model such as traffic classifier and marker to enforce high priority to a particularly signal message in the standard MIPv6 protocol and then constrains the traffic accordingly. Therefore, these mechanisms expect to minimize the packet losses as well as reduce handover latency in the proposed scheme.

The topology depicted in Figure 4 is based on IPv6 network with mobility support and DiffServ model supported in the core network to offer privilege QoS guaranteed service. Where, ER is the edge router at ingress/egress of the network, CR is core router in the backbone network, CN is the correspondent node (it is considered to be a stationary node) and MN is the Mobile IPv6 node. Additionally, the Access Router (AR) is connected to one or more Base Stations (BS) to provide connectivity to mobile IPv6 nodes. It is also responsible for resource co-ordination for base stations to which is attached. BB is the bandwidth broker. It used to optimize the existing recourse by allocating and controlling the bandwidth. The models based on BBs decouple the QoS control plane from the data plane. Since many control plane functions are performed per flow, scalability can be greatly enhanced by off-loading these responsibilities from the core nodes [16]. For the sake of simplicity, it is assumed that the (ARi) supports functionality of the ingress edge routers. The mobile node intuitively moves from Old ARi (OARi) to a New ARi (NARi) when it performs handover procedure.

Performance Evaluation: In order to evaluate Quality of Service within Mobility environment, analytical framework is used to develop the performance of the proposed scheme (DiffServ-MIPv6) and compare it with the standard MIPv6 protocol in terms of signaling cost. The signaling cost is evaluated for various metrics such as binding lifetime period and wireless link delay. The intention of the analytic model is to demonstrate that the proposed scheme doesn't add much signaling overhead while improving QoS compared to MIPv6. Figure 5 shows the network topology that is used for analyzing the signaling cost. Also, the following notations will be used throughout this section as shown in Table 1.

It is assumed that the coverage area for the Access Network (AN) is circular with M subnets each with size S_{AR}. Also, it is assumed that the CN generates data packets destined to MN with mean rate (λ_p) and the MN moves from one access router (or subnet) to other with mean rate (μ). Packet to Mobility Ratio (PMR) is defined as the number of packets received by the MN from the CN per movement. It has the symbol (P) [17].

The PMR is given by:

$$P = \lambda_p / \mu \qquad (1)$$

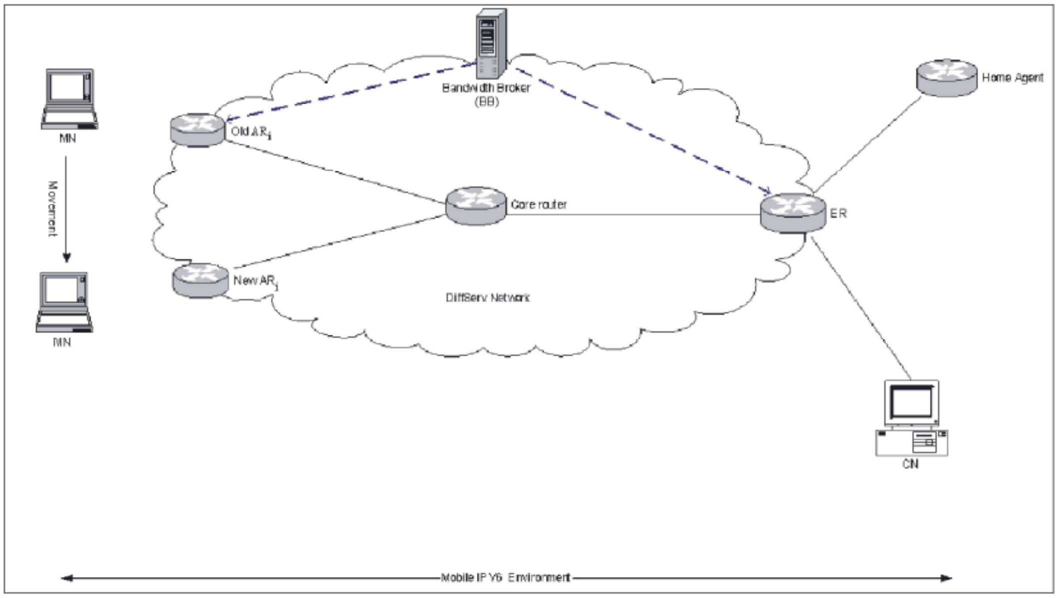

Fig. 4: DiffServ support within mobile IPv6 network

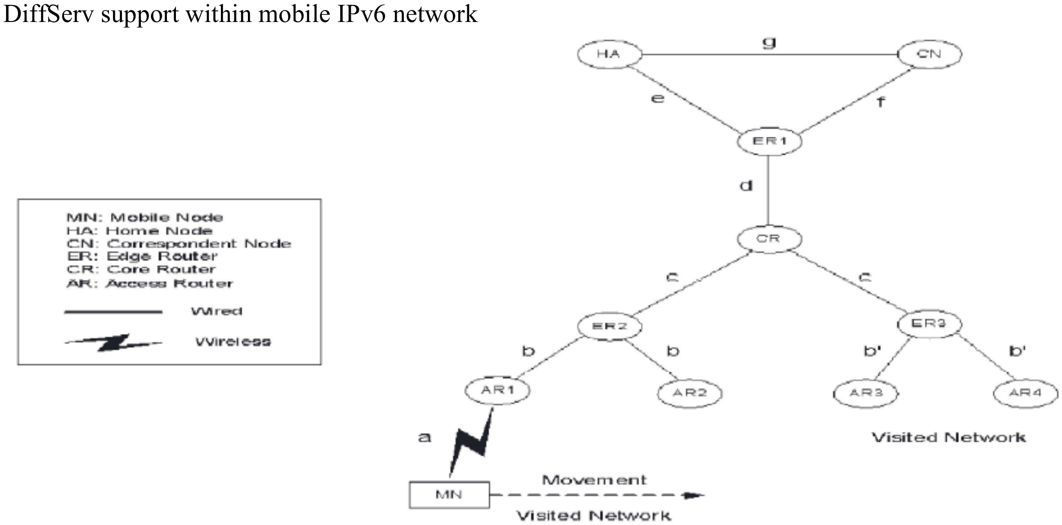

Fig. 5: The network topology used for the analysis

Table 1: Notations used in the analysis

Symbols	Descriptions
C_{rr}	Signaling cost for return routability procedure
C_{hc}	Binding update cost at HA and CNs
C^{l}	Local binding update cost to HA/CNs
C^{g}	Global binding update cost to HA/CNs
$C_{X,Y}$	Transmission cost of control/data packets between nodes *x* and *y*
$d_{X,Y}$	The number of hops between hosts *x* and *y* (distance)
M	Number of subnets in domain
N_{CN}	Number of CNs having binding cache entry with the MN
N_{E}	Number of edge routers between CN and MN
N_{g}	Number of domain crossing during inter-AN movements
N_{l}	Number of subnets crossing during intra-AN movements
PC_{X}	Processing cost for the control/data packet at node *x*
C^{M}_{TOT}	The total signaling cost for the standard MIPv6
C^{MD}_{TOT}	The total signaling cost for the proposed scheme(DiffServ-MIPv6)

The cost for transmitting data packet is η times greater than the control packet.

Here η is the ratio of:

$$\eta = l_d / l_c \quad (2)$$

where, the parameter (l_d) is the average length of data packet and (l_c) is the average length of control packet (e.g. ICMPv6). The average processing cost for control packets at HA/CN are assumed to be PC_{HA} and PC_{CN} respectively, while PC_E is the Edge Router (ER)'s processing cost. PC_E is assumed to be 2 times greater than the PC_{CN} because the edge router has not only forwarded the packets but also managed the MN's service profile and marked the packets [18].

The total signaling cost is C_{total}, which equal to location update cost and packet delivery cost.

$$C_{total} = C_{LU} + C_{PD} \quad (3)$$

C_{PD} is the packet delivery cost and C_{LU} is the location update cost. There are two types of location update that could be happen in the analysis. One happens when the MN is crossing subnet and another one occurs when the binding is about to expire. The first one known as Binding Update (BU) message and the second one refers to as the Binding Refresh (BR) message, receptivity [19]. Thus, the total signaling cost C_{total} could be rewritten and calculated as the sum of the binding update cost C_{BU}, binding refresh cost C_{BR} and packet delivery cost C_{PD}. So, equation (3) can be written as:

$$C_{total} = C_{BU} + C_{BR} + C_{PD} \quad (4)$$

The authentication and L2 handover latency were ignored in this analysis because their signaling cost is same as the standard MIPv6 and it won't be any change happened in the proposed scheme.

The MIPv6 handles local mobility of a mobile node in the same way as it handles global mobility. As a result, the MN has to send BU message to the HA and CN each time it changes its point-of-attachment regardless of locality. Therefore, the binding update cost for MIPv6 during intra/inter session time interval depends heavily on the computation of the number of location binding updates and it is given by:

$$C_{BU} = E(N_l)\, C^l \text{ or, } C_{BU} = E(N_g)\, C^g \quad (5)$$

where, $E(N_l)$, $E(N_g)$ are the average number of location binding updates when a MN is crossing subnets and Access Network (AN) domain, respectively. They are given by:

$$E(N_l) = \mu_l/\lambda_s \qquad \text{And } E(N_g) = \mu_g/\lambda_s \quad (6)$$

where, μ_l and μ_g are the border crossing rate of MN out of subnet/ access router and out of Access Network (AN) domain, respectively. λ_s is the session arrival rate [20]. The border crossing rates are given by:

$$\mu_g = \mu / \sqrt{M} \quad (7)$$

$\mu_l = 2\frac{v}{\sqrt{\pi S_{AR}}}$, $S_{AR} = \pi R^2$, where (í) is the average velocity of the MN and R is the access router radius. To realize the signaling overhead analysis, a performance factor known as session-to-mobility ratio (SMR) is used. It represents the relative ratio of session arrival rate to the user mobility rate. The binding update cost can be obtained by:

$$C_{BU} = \frac{1}{\lambda_8}\left(\mu_g C^g\right) = \frac{1}{SMR\sqrt{M}}(C^g) \quad \text{or,}$$
$$= \frac{1}{\lambda_8}\left(\mu_1 C^1\right) = \frac{\sqrt{M}}{SMR}(C^1) \quad (8)$$

The transmission cost in IP-based networks is proportional of the distance between the source and destination nodes. Besides, according to [21] the transmission cost in wireless link is usually larger than the transmission cost in wired link.

Consequently, the transmission cost of control packet between nodes X and Y belonging to the wired part of a network can be expressed as $C_{X,Y} = \tau\, d_{X,Y}$ while $C_{MN,AR} = \tau\kappa$, where (τ) is the transmission unit cost over wired link and (κ) the weighting factor for the wireless link. The global/local binding update signaling cost for MIPv6 is expressed by:

$$C^g_{MIPv6} = C^l_{MIPv6} = 4C_{MN,AR} + 2PC_{AR} + C^{MIPv6}_{hc} \quad (9)$$

where,

$$C^{MIPv6}_{hc} = 2(C_{MN,HA} + N_{CN}C_{MN,CN}) + PC_{HA} + N_{CN}PC_{CN} + C_{rr} \quad (10)$$

Here C_{hc} is the binding update cost at the HA and at all active CNs, while C_{rr} is the signaling cost due to return routability procedure.

The mobile node sends HoTI message to HA with cost $C_{MN,HA}$. The HA processes this message with cost PC_{HA} and afterwards the message is been forwarded to the CN with cost $N_{CN}C_{HA,CN}$. In the same way, the CN processes the received HoTI message with the cost $N_{CN}PC_{CN}$ before it responds with HoT message. So, the cost for home address test would be: $2[C_{MN,HA} + PC_{HA} + N_{CN}C_{HA,CN}] + N_{CN}PC_{CN}$. While in the care-of address test the CoTI and CoT messages are exchanged directly between the MN and CN. Subsequently, the care of address test cost is: $2N_{CN}C_{MN,CN} + N_{CN}PC_{CN}$.

The expression of C_{rr} can be deduced as follows:

$$C_{rr} = 2(C_{MN,HA} + N_{CN}C_{HA,CN} + N_{CN}C_{MN,CN} + PC_{HA} + N_{CN}PC_{CN}) \tag{11}$$

In the proposed scheme (DiffServ-MIPv6), when the MN performs handover the transmitted control packets that is required to determine the location update cost, have to go through Edge Router (ER). In order to reduce the loss of BU that could happen accidentally, the ER is configured to be giving high priority to BU in the flow of expedited forwarding. However, the processing cost for the edge router is assumed 2 times greater than the processing cost at any nodes because the ER is used to be in charge of admission control, packet classifying and marking.

Similar to the above equations, the binding update cost at the HA and all active CNs for the proposed scheme can be obtained as follows:

$$C_{hc}^{Diff-MIPv6} = 2\ (C_{MN,HA} + N_{CN}C_{MN,CN}) + PC_{HA} + N_{CN}PC_{CN} + N_E\ PC_E + C_{rr} \tag{12}$$

Also, this formula can be re-written as:

$$C_{hc}^{Diff-MIPv6} = 2\ [2C_{MN,AR} + 2\ \tau\ (d_{AR,ER} + d_{ER,CR} + d_{CR,ER}) + \tau(d_{ER,HA} + d_{ER,CR})] + PC_{HA} + N_{CN}PC_{CN} + N_E\ PC_E + C_{rr} \tag{13}$$

By using equations (11) and (13), the global and local binding update signaling costs for the proposed scheme (DiffServ-MIPv6) is derived by:

$$C_{Diff-MIPv6}^{g} = C_{Diff-MIPv6}^{l} - 4C_{MN,AR} + 2PC_{AR} + C_{hc}^{Diff-MIPv6} \tag{14}$$

Bindings are valid for lifetime included in the binding update message. The mobile nodes should refresh the bindings by sending another binding update before they expire or when the mobile node's care-of-address changes. Mobile IPv6 allows the receiver of the binding update to request that mobile node update its binding entry. This is done by using binding refresh request. The Binding Refresh (BR) message is usually used when the binding cache is in active use but the binding's lifetime is close to run out [8]. The performance evaluation in the most previous works did not take into consideration the cost of binding refresh and the impact of binding lifetime period. Nevertheless, these metrics may have significant effect on the total signaling cost. Let (T_H) and (T_C), be the binding lifetime period for the MN at HA and CNs respectively. The average rate of sending BR message from CN and from HA would be obtained $\left|1/(\mu_g T_H)\right|$ and $\left|1/(\mu_g T_C)\right|$ where, $|X|$ is the integer part of a real number X. Thus, the average binding refresh costs for MIPv6 can be obtained as follows:

$$C_{BR}^{MIPv6} = \left(\left|1/(\mu_g T_H)\right| C_{MN,HA} + \left|1/(\mu_g T_c)\right| N_{CN}C_{MN,CN}\right) \tag{15}$$

In the same way the average binding refresh cost for the proposed scheme can be deduced as follows:

$$C_{BR}^{Diff-MIPv6} = \left(\left|1/(\mu_g T_H)\right| (\tau\kappa + \tau\,(d_{AR,ER} + d_{ER,CR} + d_{CR,ER} + d_{ER,HA}) + \left|1/(\mu_g T_c)\right| \left(\tau\kappa + \tau\,(d_{AR,ER} + d_{ER,CR} + d_{CR,ER} + d_{ER,CN}\right)\right) + NE\ PCER \tag{16}$$

The packet delivery cost comprises the transmission of the data packet in addition to the processing cost. Also, it could be defined as the combination of packet tunneling cost (C_{tun}) and packet loss cost (C_{loss}). Let α and β be weighting factors which emphasize tunneling effect and dropping effect (where $\alpha + \beta = 1$). So, the packet delivery cost is computed as follows:

$$C_{PD} = \alpha C_{tun} + \beta C_{loss} \tag{17}$$

The mobile node cannot receive any IP packets on its new point of attachment until the handover process is completed. This period of time is known as handover latency or packet reception latency (t_P). Usually, the handover procedure in MIPv6 is been affected by the latency that occurs in two layers: Network layer L3 handover and Link layer L2 handover. However, in this study the handover latency distributes into three components: link switching or L2 handover latency (t_{L2}), IP connectivity latency (t_{IP}) and location update latency (t_U). L2 latency takes place when a MN detects the decrease of Received Signal Strength Indication (RSSI) of its attached access point [22]. So, it scans the currently available access points and chooses the best one to connect to. IP connectivity latency reflects how quickly an MN can send IP packets after L2 handover while location update latency is the latency of forwarding IP packets to MN's new IP address.

L3 handover latency can be defined by these delay parameters: movement detection delay (t_{MD}), addresses configuration and DAD procedure delay (t_{AC}), binding update latency (t_{BU}) and delay from completion of binding update and reception of first packet at the new IP address (t_{NR}).

Note that, initially there is no packet forwarding in MIPv6 until the handover is been completed; that is C_{tun}^{MIpv6} in equation (17) is equal to zero. Then, only packet loss cost takes a place and it can be computed as follows:

$$C_{loss}^{MIPv6} = \lambda_p c_{cm}^{f}(t_{L2} + t_{IP} + t_u) \quad (18)$$

where, λ_p defines as the packet arrival rate in unit of packet per time. And, $c_{cm}^{f} = \eta(c_{CN,PAR} + c_{PAR,MN})$, is the cost of transferring data packets from CN to MN via PAR when the handover fails. To calculate the location update latency (t_U) in equation (18), we should consider the transmission delay causes by forwarding the binding messages from MN to HA and CN (i.e. t_{HA} and t_{CN}), in addition to the delay from return routability procedure (t_{RR}). Simply, $t_U = t_{BU} + t_{NR}$ and $t_{BU} = t_{HA} + t_{RR} + t_{CN}$. In more details $t_{X,Y}$ is one way transmission delay for a message with size (l_c) between nodes X and Y. If one of the endpoints is MN, then $t_{X,Y}$ will be determined by:

$$t_{X,Y}\,(lc) = \frac{1-q}{1+q}\,(B_{\omega l} + L_{\omega l}) + (d_{X,Y} - 1)(\frac{lc}{B_\omega} + L_\omega + \varpi_q) \quad (19)$$

where q is the probability of wireless link failure, ω_q the average queuing delay at each router in the Internet which is presumed to be trivial in this equation [23], $B_{\omega l}$, B_ω are the bandwidth of wireless/wire link and $L_{\omega l}$, L_ω are the wireless/wired link delay. The handover latency associated in the MIPv6 is given by:

$$D_{HO}^{MIPv6} = t_{L2} + t_{RD} + t_{DAD} + t_{RR} + 2(t_{MN,HA} + t_{MN,CN}) \quad (20)$$

where, t_{RD} is Router discovery delay. The first half in equation (17) is represented the process of how to calculate the packet tunneling cost from the CN to MN optimally without going through HA. It obtains by [24]:

$$C_{tun}^{MIPV6} = \rho \times (\eta(C_{CN,NAR}^{MIPv6} + C_{NAR,MN}^{MIPv6}) + PC_{AR} \quad (21)$$

By summing up all of equations (17), (18) in (21), the packet delivery cost for MIPv6 is as follows:

$$C_{PD}^{MIPv6} = \alpha C_{tun}^{MIPv6} + \beta C_{loss}^{MIPv6} \quad (22)$$

Even though the data packets in MIPv6 forward directly from the CN to the MN avoiding the huge overhead of HA's processing cost (i.e. overcome the problem of triangle routing), they need to bypass through the ER to ensure QoS in the proposed scheme (DiffServ-MIPv6). This may cost extra time at ER for the processing, however this is considered negligible to total signaling cost if we perceive the significant profit of the QoS guaranteed to mobile node. Hence packet tunneling cost from the CN to MN via ER in the proposed scheme is given by:

$$\begin{aligned} C_{tun}^{Diff-MIPV6} &= \rho \times (\eta(C_{CN,NAR}^{Diff-MIPv6} + C_{NAR,MN}^{Diff-MIPv6}) + PC_{AR} + N_E PC_{ER} = \\ &\rho \times (\eta\tau(d_{CN,ER}^{Diff-MIPv6} + d_{ER,CR}^{Diff-MIPv6} + d_{CR,ER}^{Diff-MIPv6} + d_{ER,NAR}^{Diff-MIPv6} + \kappa) + \\ &PC_{AR} + N_E PC_{ER} \end{aligned} \quad (23)$$

As the result, the packet delivery cost for the proposed scheme (DiffServ-MIPv6) is as follows:

$$C_{PD}^{Diff-MIPv6} = \alpha C_{tun}^{Diff-MIPv6} + \beta C_{loss}^{Diff-MIPv6} \quad (24)$$

According to investigation that have done to study all of the binding update cost, binding refresh cost and packet delivery cost, the performance analysis of (DiffServ-MIPv6) and standard MIPv6 protocols would be determined easily. Using equations in (9), (15) and (22), we can come up with the total signaling cost of MIPv6 is as follows:

$$C^{M}_{TOT} = C^{M}_{BU} + C^{M}_{BR} + C^{M}_{PD} \quad (25)$$

Similarly, referring to equations in (14), (16) and (24), the total signaling cost of (DiffServ-MIPv6) is representing as follows:

$$C^{DM}_{TOT} = C^{DM}_{BU} + C^{DM}_{BR} + C^{DM}_{PD} \quad (26)$$

Referring to Fig. 3 the distance is defined as the number of hops between different hosts. It is assumed to be equals (i.e. $c = d = e = f =$g= 10). The distance between ingress ER and AR *(b, b')* are assumed to be = 2 and *a* is the distance between MN and AR which is set to 1. Further parameters used for signaling cost computation are defined as follows: $\tau = 1$, $\kappa = 10$, $\alpha = 0.2$, $\beta = 0.8$, $PC_{AR} = 8$, $PC_{HA} = 24$, $PC_{CN} = 4$ and $PC_{E} = 8$.

The location update cost, packet delivery cost and total signaling cost equations were derived and generated for a mobile node in case of the standard MIPv6 and the proposed scheme (DiffServ-MIPv6). Accordingly, the impact of various system parameters has been observed to evaluate the signaling cost ratio for the MIPv6 and (DiffServ-MIPv6). The aim of this study is to provide insight for a new scheme that should be deployed to co-exist with the standard MIPv6 protocol to provide QoS for mobile hosts. To generate numerical results from equations derived above, the system parameters shown in Table 2 are used. [25], [23], [21] and [19].

The Effect of Binding Lifetime Period on Binding Refresh Cost: This scenario is conducted using these parameters, the average speed of the MN (N=5.7 Km/h), the number of correspondent node (N_{CN}) is equal to 1, the subnet radius (R) is equal to 500m and the binding lifetime periods for the HA and CN (i.e. T_H and T_C respectively) are equals and adjusted per hours. The impact of binding lifetime period on the binding refresh cost ratio for the proposed scheme and MIPv6 (C^{DM}_{BR}/C^{M}_{BR}) are depicted in Figure 6. It can be deduced from the figure that the binding lifetime period got significant effect on the binding refresh cost ratio. Namely, when binding lifetime period is small the cost of BR ratio will increased because the mobility agents they will send a lot BRs to request MN to send BU before the timeout is about expire and vice versa. Which means when binding lifetime period is getting to be large the cost of binding refresh will decrease because the mobility agents have to wait long time to take action by sending BR before the timeout is expire. Namely, few BR message will be send that why the cost of BR will decrease accordingly. The binding refresh ratio cost appears unchangeable between binding lifetime periods (0.2 and 0.37) because the mobile node moves to the neighboring subnet before the new binding refresh message does occur. Similarly, if the binding lifetime period above 0.4, the binding refresh ratio cost will be close to zero because the residence time for the MN is less than the binding lifetime period. When binding lifetime period is small the MIPv6 performs better than the proposed schemed because of the transmission cost for BR that will send to MN. The BR message has to pass though ER (which means additional processing cost at ER). However, when binding lifetime period is larger the proposed scheme improves the signaling cost better than MIPv6 by decreasing the cost of BR ratio. Precisely, it assumed the use of binding update list that already maintained by MN to update the binding caches in the mobility agents. So by which the cost of sending BR will be reduced. Lastly, in the both schemes when the binding lifetime period is larger, the binding cache entry will increase at mobility agents (i.e. HA and CN) resulting on higher memory consumption and longer time is been taken in binding cache lookup table.

Table 2: System parameters

Parameters	Symbols	Values
Control packet size	l_c	96 bytes
Data packet size	l_d	200 bytes
The probability of wireless link failure	q	0.50
Wired link bandwidth	B_{ω}	100 Mbps
Wireless link bandwidth	$B_{\omega l}$	11 Mbps
Subnet radius	R	500 m
MN average speed	V	5.7 Km/h
Number of ARs in AN	M	2
Packet arrival rate	λ_p	10 packets/s
Wired link delay	L_{ω}	2 ms
Wireless link delay	$L_{\omega l}$	10 ms
DAD delay	t_{DAD}	500 ms
Router discovery delay	t_{RD}	100 ms
L2 handover delay	t_{L2}	50 ms

The Effect of Wireless Link Delay on Handover Latency: The last scenario presents the effect of wireless Link Delay on handover latency. The wireless link delay is

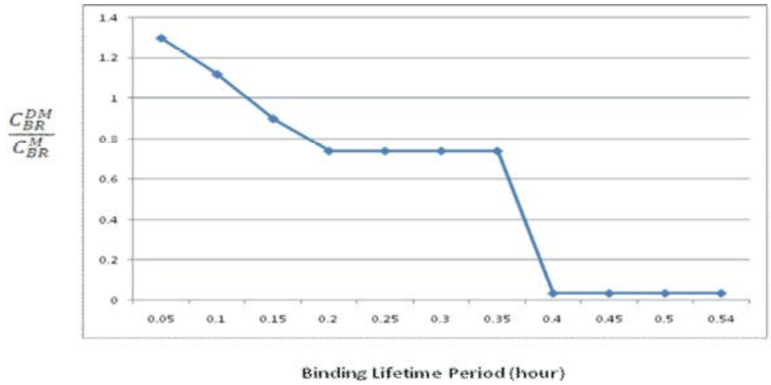

Fig. 6: Binding lifetime versus binding refresh cost

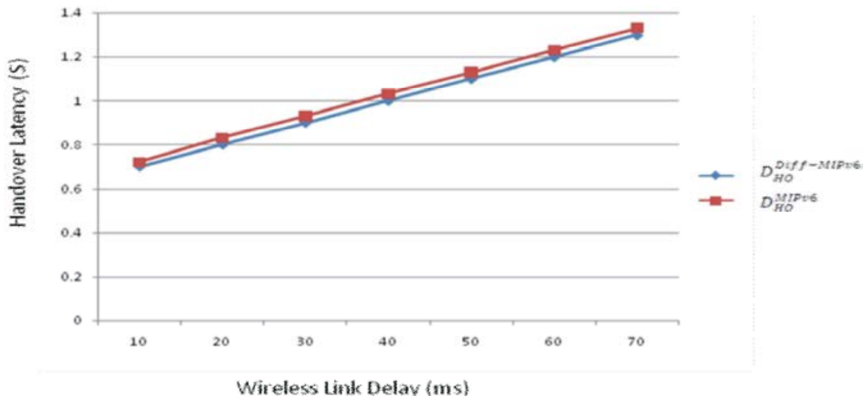

Fig. 7: Wireless link delay versus handover latency

adjusted from (10 to 70ms) in order to observe the impacts of the handover latency in the proposed scheme and the standard MIPv6. Figure 7 shows that the handover latency increases proportionally with the wireless link delay in the both schemes. The proposed scheme marginally improves the location update latency by minimizing the probability of BU loss. Therefore, it achieves better handover latency compare to the standard MIPv6. However, the overall handover latency of both schemes is adversely been affected by Duplicate Address Detection. In this analysis, it was set to 500 ms which is a huge delay to configure a new CoA.

CONCLUSION

Merging QoS within mobility environment is still ongoing exploration by computer network researchers. This paper deals with improving QoS in mobile IPv6. In general, DiffServ model is deployed in mobile IPv6-based network to achieve seamless handover and acceptable delivery of real-time traffic in mobile environment. Analytical analysis is developed to investigate the signaling cost. The derivation of the signaling cost for the proposed scheme is compared with the standard MIPv6 scheme for benchmarking. Two parameters are analyzed in this paper, binding lifetime period and wireless link delay. It has been found that the binding lifetime period has significant impact on the binding refresh cost. Additionally, it has been observed that handover latency increases with the wireless link delay in the both schemes. The achieved results demonstrate that the proposed scheme slightly outperforms the standard MIPv6 and doesn't add much signaling overhead while improving QoS for the mobile IPv6 users.

REFERENCES

1. Braden, R., D. Clark and S. Shenker, 1994.Integrated services in the internet architecture: an overview, RFC 1633.
2. Blake, S., D. Black, M. Carlson, E. Davies, Z. Wang and W. Weiss, 1998. An Architecture for Differentiated Services, RFC 2475.
3. Rosen, E., A. Viswanathan and R. Callon, 2001. Multiprotocol Label Switching Architecture, RFC 3031.

4. Manner, J. and M. Kojo, 2003. Mobility related terminology, Internet draft (work in progress), Internet Engineering Task Force, draft-ietf-seamoby-mobility terminology-04.txt, in AD Review.
5. Redi, J. and P. Bahl, 1998. Mobile IP: A Solution for Transparent, Seamless Mobile Computer Communications, Mobile Computing and Communications.
6. Droms, R., 1993. Dynamic Host Configuration Protocol, RFC 1541.
7. Perkins, C., 1996. IPv4 Mobility Support, RFC 2002.
8. Johnson, D. and C. Perkins, 2004. Mobility Support in IPv6, RFC 3775.
9. Narten, T., E. Nordmark and W. Simpson, 1998. Neighbor discovery for IP version 6 (IPv6), Internet Engineering Task Force, RFC 2461.
10. Thomson, S. and T. Narten, 1998. IPv6 stateless address auto-configuration, Internet Engineering Task Force, Request for Comments (Standards Track) 2462.
11. Kim, M. and Y. Mun, 2008. Distributed Control Scheme for DiffServ in Heterogeneous Mobile IP Networks, International Conference on Computational Sciences and Its Applications ICCSA.
12. Kim, M. and Y. Mun, 2007. Simple performace model for Differentiated services in Mobile IPv6 Networks, O. Gervasi and M.Gavrilova(Eds.), ICCSA 2007. LNCS 4706, Springer, Heidelberg, pp: 334-345.
13. Garcia-Macias, J. and R. F.S, 2003.Quality of service and mobility for the wireless internet. Wireless Networks, 9(4).
14. Jaseemuddin, M., J.A. Zubairi and O. Mahmoud, 2002. A study of profiled handoff for diffserv-based mobile nodes. Wireless Communications and Mobile Computing, 2(4): 339-356.
15. Hussien, L., A. Hassan Abdalla, F. Anwar, O.O. Khalifa, S. Ahmed Hameed and W. Alkateeb, 2011. Simulation evaluation of DiffServ Approach integrated in MIPv6 Networks, Australian Journal of Basic and Applied Sciences, ISSN 1991-8178, pp: 386-396.
16. Bouras, C.H. and S.K. 2007. An efficient architecture for Bandwidth Brokers in DiffServ networks, International Journal of Network Management, pp: 27-46, Patras-Greece.
17. 1Jain, R., T. Raleigh, C. Graff and M. Bereschinsky, 1998. Mobile Internet Access and QoS Guarantees using Mobile IP and RSVP with Location Registers, in Proc. ICC'98 Conf., pp: 1690-1695.
18. Kim, J. and Y. Mun, 2003. A study on Handoff Performance Improvement Scheme for Mobile IPv6 over IEEE 802.11 Wireless LAN.
19. Makaya, C. and S. Pierre, 2008. An Analytical Framework for Performance Evaluation of IPv6-Based Mobility Management Protocols. IEEE Transaction on Wireless Communications.
20. Fang, Y., 2003. Movement-based mobility management and trade off analysis for wireless mobile networks, IEEE Trans. Computers, 52(6): 791-803.
21. Xie, J. and I.F. Akyildiz, 2002. A novel distributed dynamic location management scheme for minimizing signaling costs in mobile IP, IEEE Trans. Mobile Computing, 1(3): 163-175.
22. Guozhi, B.J., Wei, A.Wei, Ke Xu and G. Dupeyrat, 2007. Optimization of Mobile IPv6 Handover Performance Using E-HCF Method, ICCS 2007, Part IV, LNCS 4490, Springer, Heidelberg, pp: 506-513.
23. McNair, J., I.F. Akyildiz and M.D. Bender, 2001. Handoffs for real-time traffic in mobile IP version 6 networks, in Proc. IEEE GLOBECOM, 6: 3463-3467.
24. Kim, M. and Y. Mun, 2006. Cost Evaluation of Differentiated QoS Model in Mobile IPv6 Networks. In: M. Gavrilova, O. Gervasi, V. Kumar, C.J.K. Tan, D. Taniar, A. Laganà, Y. Mun and H. Choo, (eds.) ICCSA 2006. LNCS, vol. 3984, Springer, Heidelberg, pp: 502-507.
25. Lai, W.K. and J.C. Chiu, 2005. Improving handoff performance in wireless overlay networks by switching between two-layer IPv6 and one-layerIPv6 addressing, IEEE J. Select. Areas Commun., 23(11): 2129-2137.