On Security-Effective Mobility-QoS Management Scheme in Heterogeneous Mobile Networks

Hyeungwoo Lee
Network Development Group
SAMSUNG SDS Co. Ltd.
Suwon, Gyeonggi-do, 443-822, Republic of Korea
e-mail: hw77.lee@samsung.com (zen016@naver.com)

Jae-Young Choi and Jongpil Jeong
College of Information & Communication Engineering
Sungkyunkwan University
Suwon, Gyeonggi-do, 440-746, Republic of Korea
e-mail: {jaeychoi, jpjeong}@skku.edu

***Abstract*—To support efficient mobility, host-based mobility management protocols have been developed. The Authentication, Authorization, Accounting, and Charging (AAAC) system is used in this paper to analyze the effectiveness of the existing Proxy Mobile IPv6 (PMIPv6) and Fast Handover for PMIPv6 (FPMIPv6) network security. Furthermore, the IPv6 Mobility Management Protocol (MMP) features, performance, and seamless transfer performance in terms of packet loss probability are also analyzed. Our scheme can be efficiently used to integrate Quality of Service (QoS) and mobility to manage and control resources using a QoS Broker (QoSB). The evaluation results show a better overall performance for the fast handover structure of mobility management techniques. PMIPv6 and FPMIPv6 are, in many respects, the most efficient structures possible. Specifically, the fast handover structure of the network-based mobility management schemes shows the best results.**

Keywords—Mobility-QoS; Security-Effective; Mobility Management Protocol; PMIPv6.

I. INTRODUCTION

The wireless mobile environment is rapidly growing in the digital environment that leads by human hands. The Mobility Management Protocol (MMP) is a core protocol of the wireless mobile environment. Mobile social networking, computing, shopping, and so on will be achieved using the mobility operating system. Various MMPs have been developed for various mobility services. Particularly at the network layer, mobility support techniques have been developed by the Internet Engineering Task Force (IETF). The Mobile IPv6 (MIPv6) specification was proposed, then the Fast Handovers for MIPv6 (FMIPv6) and Hierarchical MIPv6 (HMIPv6) specifications were developed as extensions. As MIPv6 was developed, analysis of IPv6 MMP was used to improve performance [1].

When host-based MMPs operated within the wireless mobile telecom infrastructure, the telecoms companies and technical developers became aware that it was not a suitable solution for mobile services, especially for service providers, as it was necessary to equip a Mobile Node (MN) with mobility support inside the network protocol stack. Therefore, MNs had to be upgraded or developed. This increased the construction costs and complexity of the MN. Host-based MMP has led to a lack of complex control operators. A new approach to mobility services was required.

The extended protocol of Proxy MIPv6 (PMIPv6), Fast Handover for PMIPv6 (FPMIPv6), has improved the transmission rate by reducing transmission latency and packet loss. In contrast to host-based MMP, network-based MMPs (such as PMIPv6 or FPMIPv6) are in the early stages of development. Improving the security of personal authentication using the FPMIPv6 by applying the Authentication, Authorization and Accounting (AAA) mechanism has been studied. When moving between domains in management, AAA techniques for authenticating the MN are required [2]. The AAA scheme for the various wired and wireless services performs authentication, authorization, and billing. Today, many techniques in conjunction with the AAA protocol are being investigated to perform the functions of MN AAA, which is the authentication process between the MNs. For instance, Zhou, H et al. [3] proposed an FPMIPv6-based authentication technique. When the MN enters a new network, this technique protects the authenticating MN from security threats, such as Replay Attack or Key Exposure.

In this paper, we propose a security-effective mobility management scheme for IPv6-based networks using a Quality of Service Broker (QoSB). This protocol can be efficiently used to integrate Quality of Service (QoS) and mobility to manage and control resources using a QoS Broker (QoSB). The time latency is not significantly affected because of the addition of the QoSB. In PMIPv6 and FPMIPv6, the new proposal performs better with respect to the handover latency, packet loss, and handover blocking rates than the traditional MIPv6 scheme. These results are shown for PMIPv6 and FPMIPv6 on a network security system that uses Authentication, Authorization, Accounting, and Charging (AAAC). Furthermore, in this paper, we propose a unified criterion to analyze both host-based and network-based MMPs.

This paper is organized as follows. Section 2 discusses related work, and Section 3 describes the operating procedures of the proposed scheme. In Section 4, a performance evaluation of the proposed method is presented. Finally, Section 5 presents some conclusions regarding these results.

II. RELATED WORK

The PMIPv6 domain structure is composed of a Local Mobility Anchor (LMA), Mobile Access Gateway (MAG), and MN. An LMA is one kind of Home Agent (HA) that serves as an MN in PMIPv6. In detail, a Home Network Prefix (HNP) is allocated to the MN that maintains the address and location information of all the MNs within the domain and also ensures connection. The MAG is responsible for network connectivity and routing functions on behalf of the MN. It also performs MN mobility signaling by tunneling through the LMA [4]. FPMIPv6 is a mobility protocol that reduces the handover latency and packet loss found in PMIPv6. It may reduce the loss of buffered packets by creating a bi-directional tunnel between the previous MAG (pMAG) and new MAG (nMAG) before making the link-layer handover. And it consists of two modes: predictive and reactive [5] [6] [7].

The QoS architecture is easily able to support end-to-end QoS in terms of the operator. When the MN is moving, it is guaranteed end-to-end connectivity and user maintenance. The architecture is designed to control the scalable deployment of resources in the access network. The core aim of the architecture is the simultaneous support of mobility and QoS. The QoS frameworks of various IETFs have considered both purposes before the final design of the QoS architecture. The advantages and disadvantages of Integration Services (Intserv) [8] and Differentiated Services (Diffserv) [9] have been discussed widely and are well known. However, they do not specifically support mobility and no hybrid solution integrates mobility and QoS. Therefore, the aim of user mobility suggests an innovative use of QoSB-related Fast HandOver (FHO) that includes a Diffserv system to efficiently control and manage the resources available [10]. This architecture is based on the concept that the user is authorized by the service provider of a contract. The QoSB, according to the user's agreement, is responsible for resource allocation in an individual subscription service. As proposed in [11], these services are generally fixed transmission services (for example, a “Guaranteed Rate of 64 KB/s,” or “Target Rate of 32 KB/s”) but are equipped with a potential mechanism for flexible service negotiation. The QoSB can manage the flow of resources in the core network. To reduce the signal overhead, the system is designed for a user/terminal so that it is not necessary to explicitly reserve or release resources. The services are requested by a simple Diffserv Code Point (DSCP) marking to the outgoing packet. If the MAG receives a packet from a particular user’s DSCP value, it sends the required QoSB configuration. The QoSB configures the MAG to fit the appropriate QoS policy based on the information about the user. Services are implicitly suspended by an inactivity timeout. This concept is explained in more detail in [11].

III. PROPOSED SCHEME

The AAAC architecture is shown in Figure 1. It is based on the AAA architecture, which is optimized for IPv6 enhanced auditing, metering, and charging. Considering that AAAC is used for QoS in a PMIPv6 environment, the architecture is designed to offer new functionality and optimize the performance of the overall system.

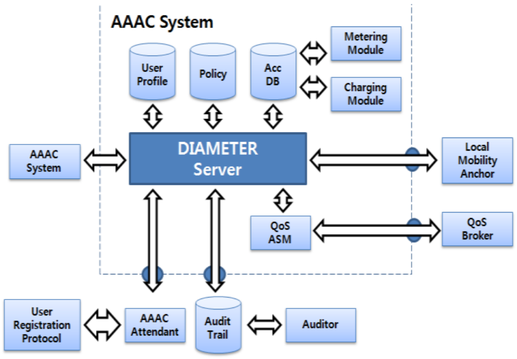

Figure 1. Enhanced Generic AAA Architecture That Supports QoS-enabled Mobility Management.

This architecture enables the subsequent auditing of AAAC using the AAAC audit trail and other factors. Hence, the policy repository is considered as a part of the policy-based AAAC system. The AAAC system supports multiple interfaces. AAAC performers can be treated with MN and interfaces. Communication is performed by the User Registration Protocol (URP). The Application Specific Module (ASM) communicates with the QoSB. The advantage of ASMs is additional flexibility, as various service equipment can be easily processed using the same method from the point of view of the AAAC system. ASM uses the AAAC protocol to communicate with the AAAC system and equipment-specified protocol to communicate with service equipment. There are clear differences in the services provided to the user in this architecture (e.g., QoS is possible and the charging system follows the AAAC requirements). For users previously provided and connected via the ASM and extended AAAC protocol, on the other hand, it is possible, if necessary, to communicate directly with the AAAC system using dedicated communication. AAAC system communication may be enhanced through an appropriate expansion by the DIAMETER default protocol. A key element of QoS service and charging is the means to measure the service used. In an IP-based measurement framework of the IETF Working Group, a variable was defined for the IP flow that depends on the needs of the network administrator. In the IPv6 network, the usage is measured according to the type of service subscribed to by the user and is sent to the QoS [2].

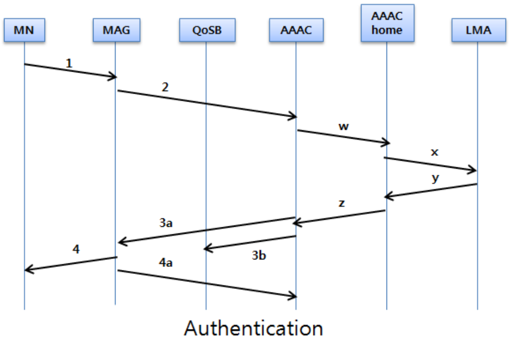

Figure 2. Registration Process.

For network operation and control, three steps may be specifically identified. 1) Registration: in this architecture, an MN/user can start using network resources after authentication and authorization, just as in today's networks. 2) Acceptance: users should be allowed to use a specific service prior to release by the network. 3) Handover: user mobility should preserve existing resources when transferring from one MAG to another.

The registration process to support end-to-end QoS is shown in Figure 2. The registration process begins after the CoA obtains the MN through automatic configuration with the two-layer identifier. When a Duplicate Address Detection (DAD) is performed, the uniqueness of the registered address is checked. When obtaining a non-authorized CoA, the user is authorized to consume only enough resources for the registration message. However, emergency calls can be made. However, as shown in Figure 2, the MN must start the authentication procedure by sending user authentication information (message 1) to the MAG for network connection. The request for this MAG is transmitted to the controlled AAAC system (message 2). For more complicated roaming, domain A (the AAAC domain) sends a registration request to the home AAAC (message w) of the MN. Domain A plays the role of a foreign domain that must contact the home AAAC of the MN. The AAAC checks first if there is a formal contractual relationship between the management domain and its own management domain (corresponding to the roaming agreement) as per the request. If the result is affirmative, the home AAAC performs authentication by verifying the provided credentials. The home AAAC sends a request to the user's LMA (message y). Finally, the home AAAC responds to the AAAC of domain A. A positive response consists of a user profile that contains the information necessary to provide the requested service in the foreign domain. The user profile contains the central management profile, including all relevant user-specific information related to the service provider. From a NVUP (network view of the user's profile), a part of the profile is sent from the AAAC server and it is necessary to provide the requested service in the foreign domain. The user profile contains the central management profile, including all relevant user-specific information related to the service provider. From a NVUP (network view of the user's profile), a part of the profile is sent from the AAAC server to the QoSB (message 3b) that also performs a DAD at this point. The other set of profiles is sent to the AAA Attendant in the MAG (message 3a). Along with the measurement and security information that is delivered to the AAA attendant, the NVUP includes all the required information related to network services. Further, the AAAC informs the MN that the registration is successful via the MAG (messages 3a and 4). After that, the MAG starts a task for the user and informs the AAAC (message 4a). Accordingly, the authentication phase is finished, and a user can access the network.

Figure 3 presents the process for granting authorization to each network service (messages 5–11). The MN sends a packet (message 5) with a DSCP code to request a specific subscription service (e.g., 256 KB/s for priority network access). One of the trailer packets, depending on the configuration of the MN, may be a dummy packet or a packet with real information. If the requested service does not comply with the policy that has already been set in the MAG, the MAG sends a request to QoSB via the QoS manager. According to the analysis, the user's NVUP, and the availability of resources for the request, the QoSB determines whether a message (message 7) is sent to the MAG. The QoS manager of the MAG sets (message 7a) the appropriate policy for the MAG, user and MN services, or notifies the user of the service denial (message 7b). After message 7a, the packet is sent to the MN that matches the configured policy rules (message 8). Packets that have different DSCP codes are subjected again to authentication. When the packet reaches the final domain with other users, it starts another QoS authorization process (message 8a). The QoS manager of the MAG sends a policy question to the QoSB (messages 9 and 10). If the QoSB has the resources, the QoSB manager receives a positive response and is configured for the MAG and its policies (message 10a). If it does not have the resources, the MAG sends a reject message regarding the service (message 10b). After message 10a, the next packet to meet the policy is able to arrive at the other terminal (message 11). In this way, two kinds of access networks can provide the QoS level of an agreement. The core network is monitored for performance (the end-to-end QoS) as expected.

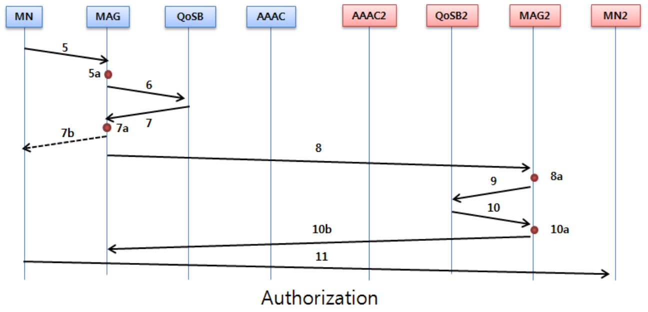

Figure 3. Authorization process.

One of the most difficult problems of IP mobility is ensuring a constant level of QoS. As shown in Figure 4, for user mobility in the network, the handover and network messages are exchanged between QoSBs using the FHO technique. When the MN begins to receive a weakened signal from the current MAG (message 1), it sends and receives the AS (Attendant Solicit), AA (Attendant Advertisement), AReq (Authentication Request) messages, and the handover procedure from the old MAG to a neighboring "new MAG" is started. The MN builds its own CoA and starts the handover process by sending an IP-handover request for the new MAG through the old MAG (message 4). The FHO module of the old MAG requests the FHO Module of the new MAG and submits it to the QoS manager module. The QoS manager immediately sends a request to the existing QoSB (message 5). The previous QoSB sends the handover request comprising the user's NVUP and a list of current user services to the new QoSB (message 6). By default, this task is transferred to a new

QoSB in the context of the existing QoSB. The new QoSB uses this information to check the availability of resources. The MN sends the message to determine whether to perform a handover to the QoS manager of the new MAG (message 7). This mechanism enables the QoSB to stop the handover because of QoS constraints (e.g., the loss of bandwidth resources). If the handover is possible, the QoS function manager sends this information to the FHO module (message 7a) and configures the new MAG to accommodate the moving MN. The new MAG starts the accounting process in the user's AAAC system account (messages 8 and 11). To complete the handover, the MN sends the LMA binding update (messages 9 and 10) to the LMA. In addition, the FHO module sends a handover response to the FHO module of the old MAG (message 12). The new MAG begins bi-casting. The MN handover to the new MAG is complete. If a handover is completed within a QoSB domain, the QoSB for controlling both MAGs is the same, and message 6 is not sent. The remaining messages are the same. Information-related security is exchanged between QoSBs in a similar way.

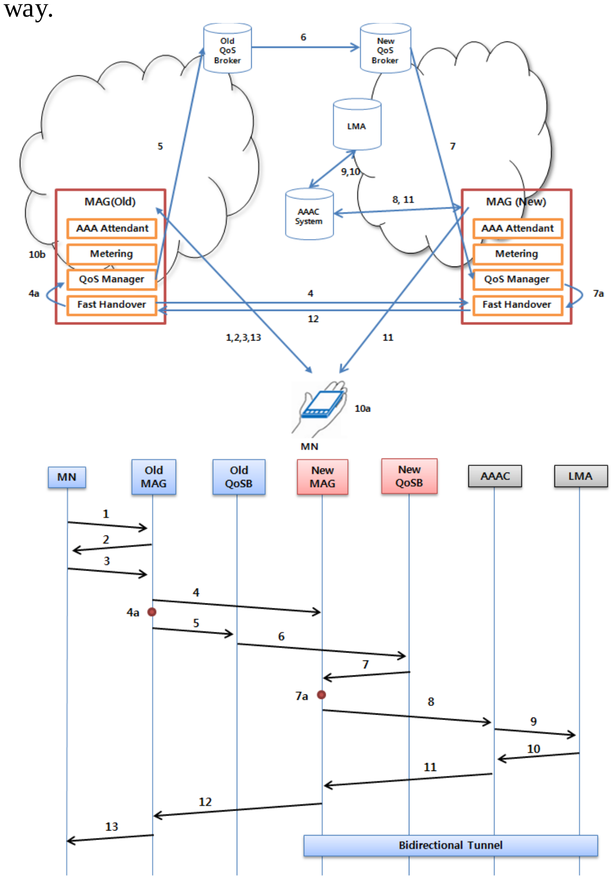

Figure 4. Handover with QoS for End-to-End QoS Support.

IV. PERFORMANCE ANALYSIS

This section evaluates the performance of the proposed method and the existing mobility management protocols.

A. Network Modeling

Figure 5 is shown a generic network topology model.

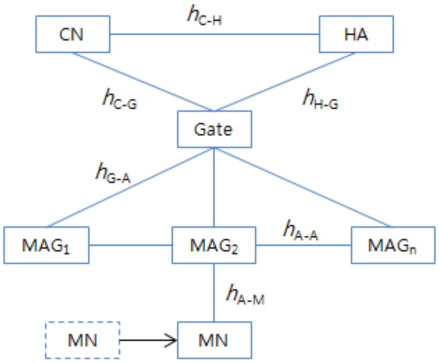

Figure 5. Network Model.

In Figure 5, the following hop count parameters are defined for describing particular paths between communication entities.

- h_{C-H}: It is the average number of hops between the correspondent node (CN) and the HA.
- h_{C-G}: It is the average number of hops between the CN and the gate.
- h_{H-G}: It is the average number of hops between the HA and the gate.
- h_{G-A}: It is the average number of hops between the gate and the MAG.
- h_{A-A}: It is the average number of hops between the neighbor MAGs.
- h_{A-M}: It is the average number of hops between the MAG and the MN.

The latency of registration lasts from when the user turns on a device until it becomes available for use. There are two types of latency. “Low-layer” latency refers to the delay when connecting to a technology after the device is ready for use. “High-layer” latency refers to the delay between sending message 1 and the arrival of message 4 (Figure 2).

$$\mathrm{Re}\,gistration\_Delay = LowLayerDelay + HigherLayerDelay \quad (1)$$

First, this technique does not depend on a particular network protocol or architecture. Second, it is dependent on the link speed. If the user is roaming, it is the “electronic distance” between the outside and home AAACs. The link latency that occurs between the MAG and AAAC system is small enough to be negligible, as it is normally the case that the management infrastructure overprovisions the link to the resource. The processing latency in the system occurs when there is an overload in the number of requests or a database is processing more requests that its capacity. However, in the actual production of the network, this is sufficiently possible to prevent using an appropriate computing or routing tool. Thus, if a user is roaming, the limiting factor is the distance between the external and home AAACs. In this case, the latency is determined by the registration time.

Session setup latency is the time required for the user to access the network. In Figure 3, the session setup latency is the delay between messages 5 to 11. This latency is composed of the processing time of the MAGs and QoSB, indicating the distance between the MAGs, and the link latency.

Handover latency can be an important parameter, depending on a user's sensitivity. The handover method should be quick as possible to provide seamless service to users. The handover latency is composed of transmission latency, computational latency, and two-layer handover latency.

$$\begin{aligned} Handover\_Delay = & \sum Transmission\_Delays + \\ & \sum Computation\_Delays + \\ & \sum Layler2\_Handover \end{aligned} \quad (2)$$

The transmission latency is the sum of the latency that occurs during MN-MAG, MAG-QoSB, QoSB-QoSB, and MAG-MAG communication. The global handover latency is the delay between messages 1 and 13, as shown in Figure 4. However, the time during no connectivity or when user terminal is not assigned resources is spent in the L2 handover. The handover operation is simulated to determine mobility seamlessness. After execution, measured values proving the architectural concept is obtained that showed reduced global handover latency, as well as low packet loss. The global handover latency affects the relationship between cell coverage of radio (range) and the speed at which the user can move, therefore affecting the cellular network plan.

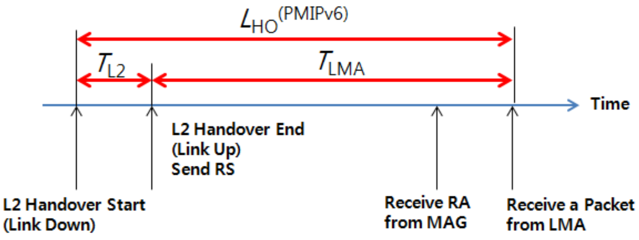

Figure 6. Timing Diagram for PMIPv6 Handover.

Figure 6 shows a timing diagram of a PMIPv6 handover. Here, $L_{HO}^{(PMIPv6)}$ is defined to be the handover latency of PMIPv6 and is expressed as follows.

$$L_{HO}^{(PMIPv6)} = T_{L2} + T_{LMA} \quad (3)$$

Furthermore, T_{LMA} refers to the time spent exchanging the PBU/PBAck messages between the MAG and LMA. During the time required to send the RS Message, the LMA receives the packet that is first sent.

$$T_{LMA} = d_{wl}(L_{RS}) + d_{wd}(L_{PBU}, h_{G-A}) + d_{lma-packet} \quad (4)$$

Variable $d_{lma-packet}$ denotes the time required for the first data packet to be sent from the LMA to the MN. Because it can be implemented by a static tunnel, a bi-directional tunnel between the LMA and MAG is not necessary. When the LMA receives a valid PBU message from the MAG, it sends a data packet and PBAck message to the MN.

$$d_{lma-packet} = d_{wl}(L_D) + d_{wd}(L_D + L_T, h_{G-A}) \quad (5)$$

Latency L_T is contained in the d_{wd} account because the data packet sent to the MN is tunneled between the LMA and MAG. This account is included in the total. The data packet is sent to the MN because of the tunnel between the LMA and MAG. This is different than in HMIPv6. Even if PMIPv6 and HMIPv6 send a similar message to the MN, the PMIPv6 reduces the packet transmission overhead of the wireless link. The FPMIPv6 has a concept similar to FMIPv6 and is composed of predictive and reactive modes.

Let $L_{HO}^{(\cdot)}$ be the handover latency in the mobility management protocol that was developed in the previous section. The $(\cdot)$ protocol is used as the indicator, $E[L_{HO}^{(\cdot)}]$ is the average value of $L_{HO}^{(\cdot)}$, *TR* is the residence time on the network, and its probability density function is denoted by $f_R(t)$. Here, $L_{HO}^{(\cdot)}$ is assumed to be exponentially distributed by the accumulation function $F_T^{(\cdot)}(t)$. Hence, $L_{HO}^{(\cdot)}$ is the element blocking the handover, and the handover block potential ρ_b is expressed as follows.

$$\begin{aligned} \rho_b &= \Pr(L_{HO}^{(\cdot)} > T_R) \\ &= \int_0^\infty (1 - F_T^{(\cdot)}(u)) f_R(u) d_u = \frac{\mu_c E[L_{HO}^{(\cdot)}]}{1 + \mu_c E[L_{HO}^{(\cdot)}]} \end{aligned} \quad (6)$$

where μ_c is the percentage of networks passing through a boundary of the MN. If the MAG coverage area is circular, μ_c is calculated as follows [12].

$$\mu_c = \frac{2v}{\pi R} \quad (7)$$

where v is the average speed of the MN and R is the radius of the MAG coverage area.

B. Numerical Results

Performance analysis is used with the following system parameter values:

h_{C-H}=4, h_{C-H}=6, h_{H-G}=4, h_{C-A}=4, h_{A-M}=1, *E(S)*=10, τ=20ms, *n*=3, L_f=19bytes, D_{wl}=[10,40]ms, D_{wired}=0.5ms, BW_{wired}=100Mbps, T_{L2}=45.33ms, T_{DAD}=1000ms.

In this analysis, ρ_f ranges from 0 to 0.7 in increments of 0.05. Figures 7 shows the comparison of the handover latency. The maximum value of ρ_f increases the probability of an error in a wireless link when a packet is transmitted. The number of retransmissions of the mobility signal increases and results in an increase of the handover latency.

As shown in Figures 7, the handover latency of each mobility management protocol is proportional to ρ_f.

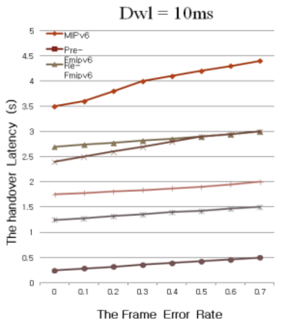

Figure 7. Handover Latency (ρ_f, D_{wl} =10ms).

Figure 8 (left) shows the transmission failure probability for v. As v increases, the MN must change rapidly. This means that the MN is required to complete the transfer of a high value in a shorter time. Therefore, as v increases, the transfer failure rate of the mobility management protocol also increases. In this analysis environment, if v is as high as 30 m, giving a handover probability of less than 0.05, only two predictive high-speed transport protocols, FMIPv6 and FPMIPv6, were able to function. Similar to the previous results, MIPv6 handover probability block performance was poor. This effect is notable as v increases. As seen in Figure 8 (right), most of the mobility management protocols are influenced by *R*. However, the performance of predictive FMIPv6 and FPMIPv6 is not affected. As with the results shown in Figures 8, the handover latency for predictive FMIPv6 and FPMIPv6 is short enough to avoid problems caused by v or *R*.

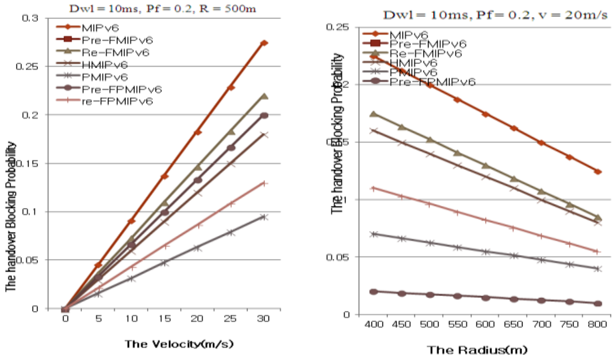

Figure 8. Handover Blocking Probability versus v (left) and *R* (right).

V. CONCLUSION

In this paper, we integrate QoS and mobility to control and manage the available resources effectively. This scheme has the advantage that the time latency is very small because of the added QoSB node. As shown in the results, the existing mobility protocols and the proposed scheme are analyzed with respect to handover latency, packet loss, and handover blocking probability in networks based on PMIPv6 and FPMIPv6. The evaluation results show a better overall performance for the FHO structure of mobility management schemes that is equally applicable in a network-based mobility management scheme. We can conclude that PMIPv6 and FPMIPv6 are the most efficient structures in many ways. In future, this approach will be applied to a variety of service platforms, such as Internet of Things (IoT) and verified in practical environments. We also plan to continue expanding its research scope.

ACKNOWLEDGMENT

This research was supported by Next-Generation Information Computing Development Program through the NRF funded by the Ministry of Science, ICT & Future Planning (NRF-2014M3C4A7030503) and Basic Science Research Program through the NRF funded by the Ministry of Education (NRF-2010-0024695).

REFERENCES

[1] J. H. Lee, J. M. Bonnin, and T. M. Chung, "Comparative Handover Performance Analysis of IPv6 Mobility Management Protocols." IEEE Tranaction on Industrial Electronics, Vol. 60, No. 3, 2013, pp. 1077-1088.

[2] V. Marques, X. P. Costa, and R. L. Aguiar, "Evaluation of a Mobile IPv6-Based Architecture Supporting User Mobility QoS and AAAC in Heterogeneous Networks," IEEE Journal on Selected Area in Communication, Vol. 23, No. 11, 2005, pp. 2138-2151.

[3] Zhou, H., Zhang, H. and Qin, Y, "An authentication method for proxy mobile IPv6 and performance analysis," Security Comm. Networks, 2009, pp. 445–454. doi: 10.1002/sec.83.

[4] H. W. Ko and J. P. Jeong, "dMMS: A Novel Distributed Dynamic Mobility Management Scheme for Minimizing Signaling Costs in Proxy Mobile IPv6 Networks," The Journal of The Institute of Webcasting, Internet and Telecommunication, Vol. 12, No. 4, 2012, pp. 65-80.

[5] S. H. Han and J. P. Jeong, "Intelligent Hierarchical Mobility Support Scheme in F-PMIPv6 Networks," The Journal of the KICS, Vol. 38, No. 4C, 2013, pp. 337-349.

[6] K. S. Go, U. S. Jung, and Y. S. Mun, "An Enhanced Fast Handover for Proxy MIPv6 Scheme for Efficient Mobile Environment of The Future Network," Journal of the institute of electronics engineerings of Korea, Vol. 48, No, 1, 2011, pp. 84-91.

[7] H. Yokota, K. Chowdhury, and R. Koodli, "Fast Handovers for Proxy Mobile IPv6," IETF RFC 5949, September 2010.

[8] R. Braden, D. Clark, and S. Shenker, "Integrated services in the Internet architecture: An overview," IETF, RFC 1633, June 1994.

[9] D. Black, M. Carlson, E. Davies, Z. Wang, and W. Weiss, "An architecture for differentiated services," IETF RFC 2475, December 1998

[10] C. Beaujean, N. Chaher, V. Marques, R. L. Aguiar, C. García, J. I. Moreno, M. Wetterwald, and T. Ziegler, "Implementation and evaluation of an end-to-end IP QoS architecture for networks beyond 3rd generation," in IST Mobile Summit, 2003, pp. 221–226.

[11] V. Marques, A. C. Casado, J. I. Moreno, and L. Rui, "A simple QoS service provision framework for beyond 3rd generation scenarios," in Proceeding of 10th International Conference on Telecommunications, 2003, pp. 1475–1481.

[12] R. Hsieh, Z.-G. Zhou, and A. Seneviratne, "S-MIP: A seamless handoff architecture for mobile IP," in Proceeding of INFOCOM, 2003, pp. 1774-1784.