3S: Scalable, Secure and Seamless Inter-Domain Mobility Management Scheme in Proxy Mobile IPv6 Networks

Jongpil Jeong[1], Min Kang[2], Younghwa Cho[1] and Jaeyoung Choi[1]

College of Information and Communication Engineering, Sungkyunkwan University
2066 Seobu-ro Jangan-gu Suwon Kyunggi-do, 440-746, Korea

[1]{jpjeong, choyh2285, jychoi1001}@skku.edu, [2]kang.min@hanmail.net

Abstract

PMIPv6 has received considerable attention between telecommunications and the Internet communities and does not require active participation of the Mobile Node (MN) by way of network-based mobility management. In this paper, we are proposing a novel 3S scheme for building Scalable, Secure, and Seamless PMIPv6 domains. In the proposed scheme, all of the Mobility Access Gateways (MAGs) are acting as the Local Mobility Anchor (LMA) combining a virtual ring with another MAG. General hashing is used in the efficient distribution-mapping between each MN and the MN's LMA for all MAGs. Also, the MAG and the MN are authenticated using the symmetric key. Through mathematical analysis, we verify the safety, scalability, and seamless service for 3S. Furthermore, we propose a handover procedure of 3S, which demonstrates its superiority over the existing schemes in terms of handover latency.

Keywords: *PMIPv6, Handover, SARP, Mobility Management, Chord*

1. Introduction

In the wake of the mobile era where the demand on wireless networks is surging high, as more mobile devices users are in need of better accessibility through the varied network technologies, featuring lower handover latency. With scores of IP-based devices roaming within such wireless network, it is instrumental to feature highly capable Mobile Nodes (MN) to be incorporated in such networks for better accessibility by the varied devices, while offering quality IP-based services [1].

One of the standardized protocols, for Network-based Localized Mobility Management (NETLMM) of Internet Engineering Task Force (IETF) [2] would be Proxy Mobile IPv6 (PMIPv6), deemed highly capable covering a wider scope of the MN with a decent latency. IP Nodes, if not modified by such PMIPv6, are set to be affiliated to the varied Access Routers (AR) within a pre-set interface without the necessity to modify their IP. The highly-touted PMIPv6 is now under study for its improved performance [4].

This paper hereby proposes '3S Approach' for a more scalable, secure, and seamless PMIPv6 domain, represented by the following merits: 1) Scalable Mobile Access Gateway (MAG) to perform as well as the MAG/LMA, 2) Enhanced Security mechanism for PMIPv6 domain, 3) Decent handover latency with faster handover and, 4) Easy and Practicable load balancing. As such, '3S Approach' becomes feasible the wider the scope of the MNs are to be covered, to the extent of 10^8 Nodes, a number more than sufficient in regards to most metropolitan areas.

The rest of this paper is organized as follows; Chapter 2 presents related work. Chapter 3 describes the proposed 3S schemes in detail. Chapter 4 presents analytical and numerical results. Finally, the paper concludes in Chapter 5.

2. Related Work

2.1. Proxy Mobile IPv6 Overview

PMIPv6 [2] allows the MN's mobility within different IPs, without the necessity of signaling thereof, provided that the MAG and the LMA, as the concerned network entities, are incorporated for IP mobility on behalf of the said MN. Such MN's mobility, being provided by the LMA of the concerned domain, is to be watched by the MAG, which upon the MN's mobility commences signaling toward the LMA of the MN, addressed to update the Home of Address (HoA) of the MN. Note that, such communication is done via the bi-directional tunnel linking between the MN and the LMA, without the necessity to alter the home link of the MN. The LMA, much like the Home Agent (HA) [3] handles Proxy Binding Update (PBU) and Proxy Binding Acknowledgement (PBA). The LMA, intercepting packets out of the MN and the bi-directional tunnel towards the MAG, offers additional functions that the PMIPv6 requests.

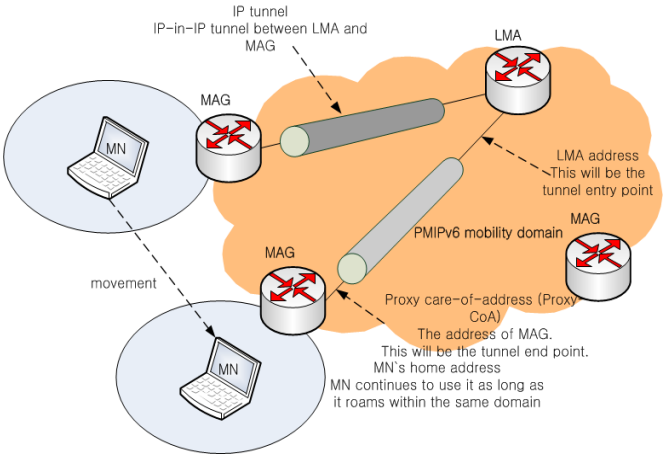


Figure 1. Overview of PMIPv6

Refer to Figure 1 for intra-domain mobility within PMIPv6. Note that the PMIPv6 domain remembers the allocation of the home network upon the mobility of the HoA and the MN. The MAG, when recognizing the MN's access, provides the home network of the MN in front of the access link, without the necessity of Care-of-Address (CoA) upon the MN's intra-domain mobility. Refer to the following Figure 2 on how the MN is handed-over, intra-domain, to the newer MAG (nMAG) from the previous MAG (pMAG) using following steps: 1) The MN is authenticated by its identity (*e.g.*, the MN-identifier), known to the nMAG upon the establishment of a connection. 2) The nMAG requests the policy storage (*e.g.*, authentication server / AAA server) to refer to the MN profile. 3) Such policy storage sends out, as requested, the MN profile together with the MN-identifier, the LMA address, and the nMAG address. 4) The nMAG sends out the PBU, together with the MN-identifier, to the LMA of the MN on behalf of the said MN. 5) The LMA, upon reception of the PBU, refers to the said policy storage for the authenticated state of the sender regarding the said PBU. 6) Such policy storage responds back to the LMA in reference to the authenticated state of the sender. 7) The LMA, upon such reference, sends out the PBA together with the home network prefix of the MN, and sets up the bi-directional tunnel towards the nMAG as what the said prefix defines. The bi-directional tunnel links the LMA and the nMAG. The LMA updates the binding cache.

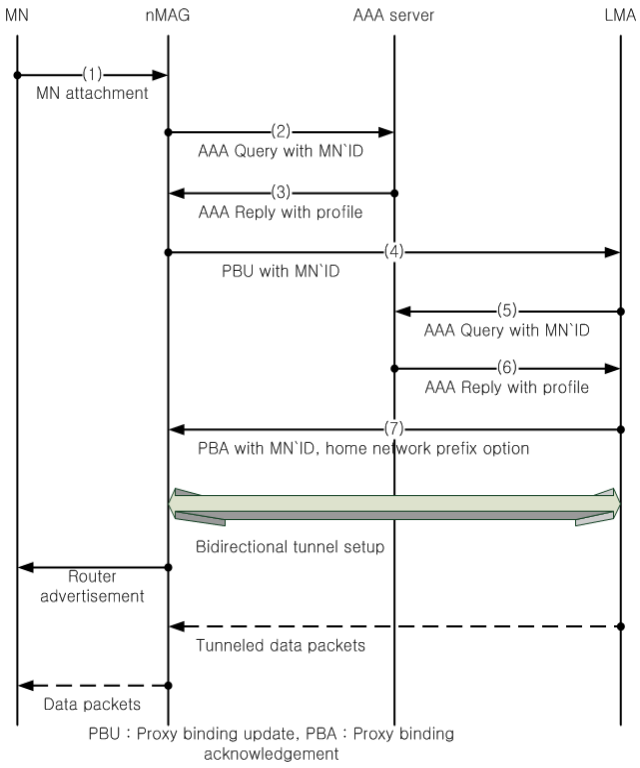


Figure 2. Handover Procedures of PMIPv6

Upon reception of the PBA, the nMAG concludes the reception of the necessary data without the MN altering its home network. The MN sends out the Router Advertisement (RA), together with the said home network prefix in order to set up a bi-directional tunnel towards the LMA through which packets are to be traded among the Nodes of the nMAG and MN. Note here that the said '3S Approach' does not modify the standards of IETF NETLMM, complementarily operating each other.

2.2. Chord System

Chord [5], the scalable distributed protocol method, is meant to detect Nodes out, on the basis of the keys. Note that, on the N-Node Chord System, each node retains O(logN) to remain alert of other nodes. Note further that such reference is to be done over the period of (1/2) logN, on average. The Chord, with the use of SHA-1 [6], allocates an 'm-bit identifier' for each node and key, uniformly hashing such nodes to allocate keys thereto [7]. Identifiers of nodes are to be out of the hashing process of IP addresses and keys thereof. Note that the length of the identifier, represented by 'm', is to be of a good length for the multiple numbers of interrelated nodes and keys, subject to a single hashing process.

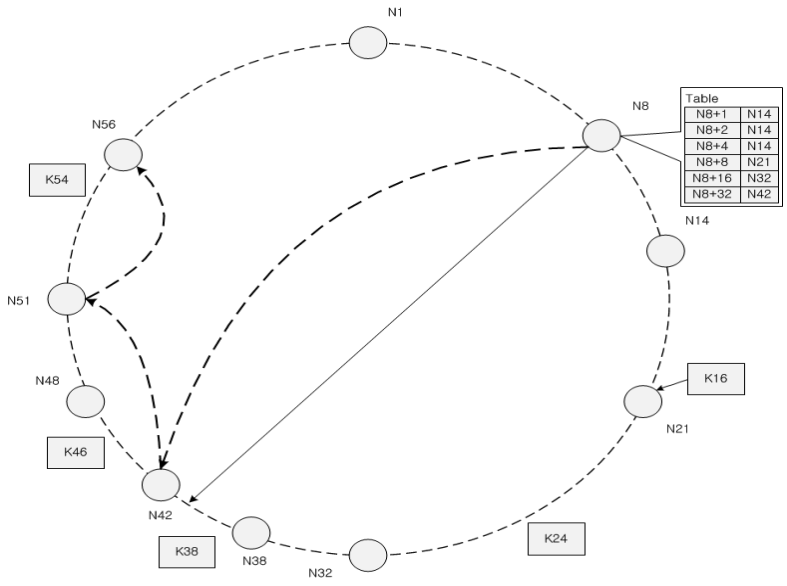


Figure 3. Illustration of Chord System

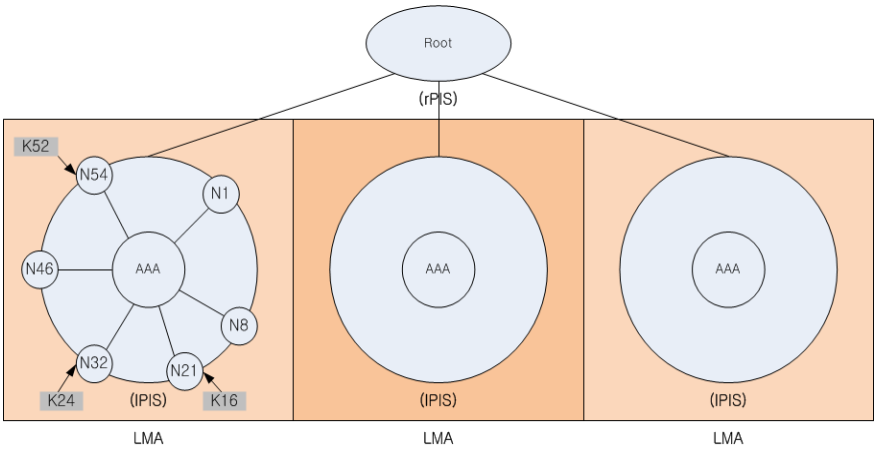
Refer to the said Figure 3 arranging identifiers, in a circular module of the Chord. Note that 'K' refers to the successor of the key K. Note further that the representation of the identifier, in the numerical form, refers to the clockwise order of the mode, from the said K. Further, the key of 'K' is to be allocated to the corresponding successor (K).

Nodes, within the circular module, are subject to minimal level interference upon its mobility. The key of the node (n), allocated to the previous successor, is to be re-allocated to N, upon combination of networks. The keys of such node (n), getting out of the concerned network, are to be re-allocated being the successor of the node (n). Note that, aside from the aforementioned, no further re-allocation is demanded.

3. 3S Mobility Control

3.1. System Architecture

In its goal to provide scalable, stable, and seamless PMIPv6, this paper presumes that every MAG of the concerned PMIPv6 domain is bearing the sufficient number of identifiers analogous to the MN-identifier as designated in [8], as well as comprised within a chord ring, by means of the uniformly conducted hashing procedure. Note that the LMA comprises the MAG of the MN, as well as the MNs access-linked to the MAG. This paper further supposes that the LMA of the PMIPv6 domain, composed by the network administrator or algorithm of the concerned domain, remains still upon its intra-domain mobility. For instance, the MN often stays still upon the device mobility, from workplace to home, meaning that it stays within the coverage of the MAG for a workplace or home. Note that packets can be sent to the MN, without the necessity of the tunnel much like the LMA/MAG, provided that the LMA is identical to the MAG as tunneling becomes necessary when case packets are attached to the LMA of the MN. On the contrary, the packets from the MAG sent to the MN are often intercepted by the LMA, without respect to the travel distance thereof. In these regards, the suggested methods improve cost-efficiency by locating the LMA near the often-referred MAG to reduce the cost of tunneling.



rPIS : root Proxy Inter gateway Server; IPIS : local Proxy Inter gateway Server

Figure 4. Root Proxy Inter-Gateway Server (rPIS) – Local PIS (lPIS)

Refer to Figure 4 for the LMA of the MN often composed out of the lesser-known network administrator, making the MAG unable to single out the LMA of the MN upon detection of the MN's access. Note that this can be resolved by the simple addition of a hashing mechanism to save the hash code (key, value) of the MAG, where the key and value refer to the hash value of the MN-identifier and the IPv6-form address of the concerned LMA, respectively. The MN-identifier is to be saved in the ensuing MAG, in the IPv6-form address regarding the concerned LMA.

Refer to the following Figure 4 for the hash code (key, value) of the MAG, saved within the MAG of N32. Such a saving procedure is to be done by another MAG, detecting MN access, requesting the QServer for the hash code (key, value) of the MAG, formulated as QServer (24) = 32.

Note that, since all MN accesses are not to be detected by the LMA of the MN, the Chord Systems are re-quested, in the form of the MN-identifier, the nMAG identifier, and the IPv6-form address, in reference to the LMA of the MN right in front of the Nodes for such a Chord, out of the QServer(MN). Also, the concerned MAGs are to be referred in the form of the IPv6-form address of the MN-identifier and hash value of (key, value). As the said QServer is requested, the LMA sends out the IPv6 address for the concerned LMA to the nMAG, which then saves it to the local LMA.

Note that the query, which should desirably be within a single hop (Distributed One Hop Hash Table) [9], may pass through multi-hop of the said chord circle. For the scalable domain, though, a single domain may be divided into the multiple routing domains. Note further that, the MAGs on such multiple routing domains and the DHT as well as the MAG address of a hop may not be known.

3.2. 3S Approach: Security

Note that the multiple chords sharing the same D1HT protocol do not trust each other. As the chord system herein presumes a single PMIPv6 domain, the MAGs basically need not to be protected from intrusion but are recommended as being so, in order to not to be spoofed by the mobile host.

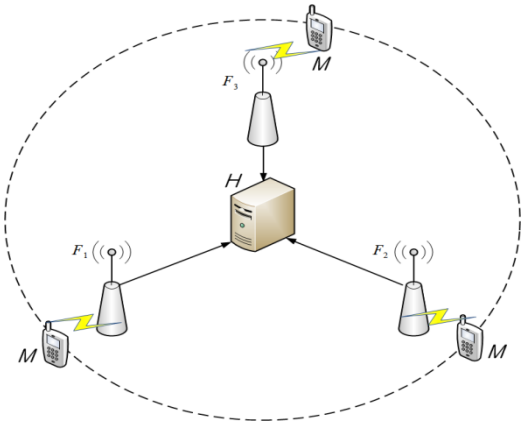


Figure 5. Roaming Path for Anonymous Roaming Service

Note that the roaming service is not to be run based on Open-key PKI server, but the Alternative-key, as suggested in [10], for highly efficient wireless authentication protocol.

Refer to the protocol in [10], compensating the defect from Chang's protocol [11], where SID are often binding each other and the unintended identification of the randomly chosen entity, within the home agent, takes place. The suggested protocol in [10] could be a resolution, incorporating the mutual authentication protocol, ensuring the anonymity and key-security during the course of confirming the user password and smart card. Refer to the following Figure 6 on how it works:

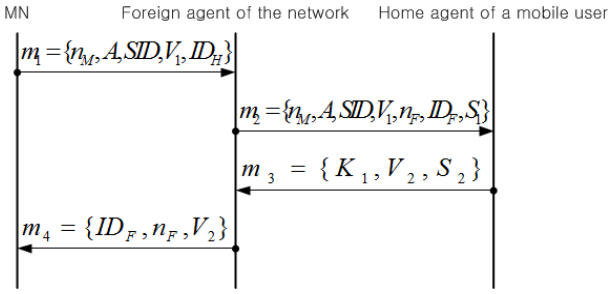


Figure 6. Operation Process of Authentication Mechanism

3.2.1. Registration: H is to choose the prime number p, q and q, out of the group of q-order multiples, as well as the secret key $b \in Z_a^*$ a properly defined one-way hash function of $h(0) = \{0,1\}^* \to Z_a^*$ in order of the following:

(1) M renders the identifier ID_M and password PW_M to H.

(2) Such H computes $B = g^b \bmod p$ and $u = h(ID_M \| b) \oplus PW_M$ to respond to the smart card information of $\{p, q, B, h(\sigma), u\}$ back to M.

3.2.2. Mutual authentication between M (Mobile Node) and F (Foreign Network): Refer Figure 6 for the mutual authentication and agreement upon the session key between M and F:

(1) M, upon entrance to the F-concerned external network, inputs the identifier ID_M and password PW_M for F to properly choose 'a' and 'n_M'. F is then computes.

(2) F, upon recognition of m_1, randomly chooses n_F, computes $S_1 = h(K_{FH} \| n_M \| A \| SID \| V_1 \| n_F \| ID_F)$ and sends out $m_1 = \{n_M, A, SID, V_1, n_F, ID_F, S_1\}$ to H. Note that K_{FH} is a symmetric key that F and H share.

(3) H, upon recognition of m_2, computes $S_1^* = h(K_{FH} \| n_M \| A \| SID \| V_1 \| n_F \| ID_F)$ to make sure of $S_1^* = S_1$ the appropriateness of ID_M^*, and $V_1^* = V_1$. H then goes on to compute $SK = h(D^* \| ID_M^* \| n_M \| ID_F \| n_F)$, $K_1 = SK \oplus h(K_{FH} \| n_F)$, and $V_2 = h(D^* \| n_M \| ID_F)$, $S_2 = h(K_{FH} \| n_F \| K_1 \| V_2)$ to send out $m_3 = \{K_1, V_2, S_2\}$ to F.

(4) M, upon recognition of m_3, computes $S_2^* = h(K_{FH} \| n_F \| K_1 \| V_1)$ and $SK = K_1 \oplus h(K_{FH} \| n_F)$ to make sure $S_2^* = S_2$ for the state authentication of M, entitled to recognize $m_4 = \{ID_F, n_F, V_2\}$.

(5) M, upon recognition of m_4, computes $V_2^* = h(D \| n_M \| ID_F)$ to make sure $V_2^* = V_2$ for the state authentication of F and to further compute $SK = h(D \| ID_M \| n_M \| ID_F \| n_F)$.

Note that the said method is based on mutual authentication, making sure of M, unable to pretend counterpart A, to be duly authenticated under any circumstances. M, from H by way of V_1, thereby authenticates $V_1 = h(C \| D)$, $C = u \oplus PW_M$, and $D = B^a \bmod p$, allowing, however, the intrusion by A which obtained one of M's identifiers or password. A, thereby does not know the M-authenticated 'u' or M's password PW_M and may not pretend to be H, deceiving F or M. Note further that S_2 protects F, protected and authenticated by K_{FH} and n_F while V_2 does the same for M by D and n_M, respectively.

3.3. 3S Approach: Mobility

The MN, upon its mobility to the nMAG, accesses CN and commences the handover process. Refer to the following Figure 7 on how it works:

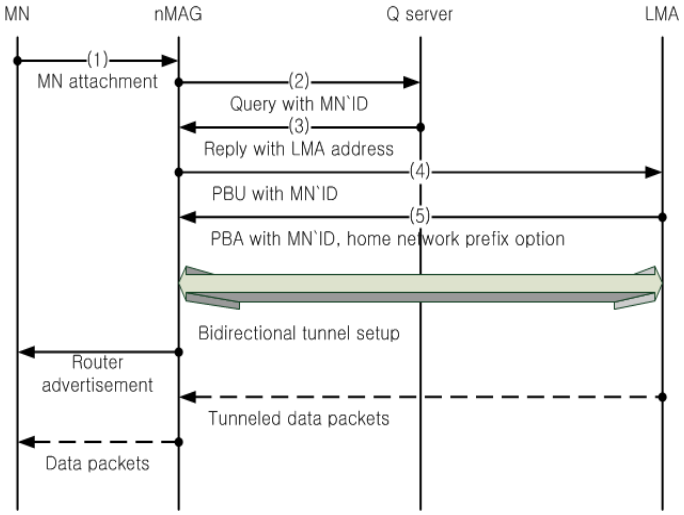


Figure 7. Basic Handover Procedures in 3S

(1) The MN, upon access to the nMAG, is to be authenticated by its identifier in order to obtain the nMAG information.

(2) The nMAG, to obtain IPv6-form address of the concerned LMA, is to request the chord system. Such a re-quest is to be routed in the form of the Chord Node. Note that such a request is to be authorized by the nMAG, in the form of the private Key.

(3) The QServer of the MN, authorizing the query upon recognition, sends out the said IPv6-form address to the nMAG.

(4) The nMAG on behalf of the MN sends out the PBU to the LMA of the MN, together with the said MN-identifier.

(5) The LMA, upon reception of the PBU, authenticates the genuineness of the PBU, by means of the public key. If authenticated, the LMA is to be authenticated, the PBA (together with the MN-identifier) is to be sent out, the MN address is to be set, and Home Network Prefix (HNP) of the MN is to be set for the nMAG. The nMAG is to be accessed, by way of the bi-directional tunnel, by the HNP of the MN.

The nMAG, upon recognition of the PBA, is to perform what PMIPv6 is set to do. Note that such the nMAG is to request the chord system for the said IPv6-form address of the concerned the LMA. As every message has been, before being sent out, authenticated by the private key is trustworthy. Note that the nMAG and the LMA of the MN need not to query to AAA server.

The said procedure, however, must incorporate the extensive handover as the nMAG queries to multi-hop chord system. Refer to the following Figure 8 for fast handover resolving latency. Note that the nMAG is not known the affiliation of the LMA of the MN, not being the condition where F-PMIPv6 can be incorporated.

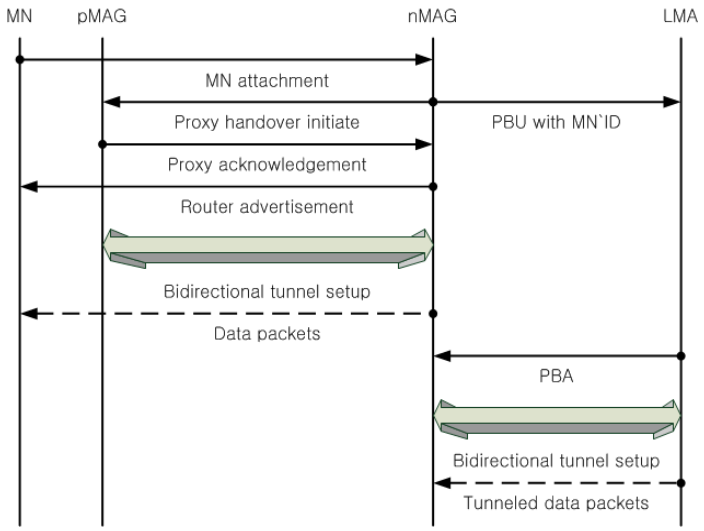


Figure 8. Handover Message Flows in Fast-PMIPv6

(1) The MN, upon access to the nMAG, is to be authenticated by its identifier to obtain information from the nMAG. (identical to Phase 1 for basic handover)

(2) The nMAG sends out Proxy Handover Initiate (PHI), together with the MN-ID, to the pMAG.

(3) The pMAG, upon recognition of PHI, responds back to PA, together with the IPv6-form address of the concerned LMA and the MN-ID (the MN profiles), to the nMAG, as well as setting up the MN address and the HNP.

(4) Such the nMAG, upon recognition of the MN profiles, emulates the home network of the MN and thereby sends out the RA to the MN, while sending out the PBU to the LMA of the MN.

(5) The pMAG sends out data packets, by way of the bi-directional tunnel, to the nMAG, where the nMAG, upon reception of the packets, hands them over to the MN.

(6) The LMA of the MN, upon recognition of the PBU from the nMAG, updates the locational information of the MN in the binding cache entry and sends out the PBA to the nMAG by way of a bi-directional tunnel. Any packets sent out to the nMAG are to be done by the LMA of the MN.

(7) The nMAG, upon recognition of the PBA from the LMA of the MN, is to set the route, by way of the said tunnel towards the LMA of the MN, for the HNP of the MN and establish a bi-directional tunnel towards the pMAG.

Note that every message sent is to be authenticated by the sender. Also, the newer access router sends out the PHI, in [12], by the previous access router for Router Sends a Router Solicitation for Proxy (RtSolPr). The aforementioned procedure proves that the overall latency of the handover has been dramatically reduced.

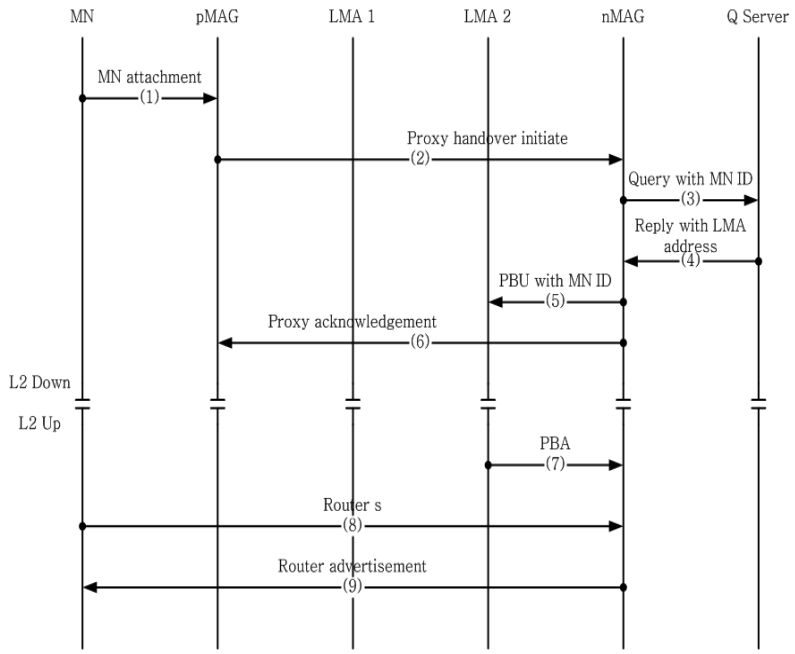


Figure 9. Handover Message Flows for Fast Handover in 3S

Refer to Figure 9 for the faster handover flows, featuring the duality of the nMAG in sending messages. Note that the nMAG sends out the PHI to the pMAG and the PBU to the LMA at the same time, provided that the MAG recognizes the PA. Moreover, the nMAG does not know the affiliation of the LMA for the MN and the PBU origin, as opposed to PMIPv6, which is able to send out the PBU to the LMA of the MN on its own. Such a difference

creates excessive and unnecessary packets, namely the PBU, sent out to the nMAG. Figure 8 and Figure 9 demonstrate that the time elapsed regarding the round-trip of packets, in 'second' or 'millisecond' units, are identical to the latency. Refer to the following chapter to compare the time that the MN is stationed within the MAG's coverage and the latency, the latter of which is much shorter.

4. Performance Evaluation

4.1. System Modeling

Suppose M and N are the number for the MAG and the MN of the PMIPv6 domain, respectively, C is the capacity of the MAG, and p is the per-second handover of the MAG.

4.1.1. Storage Requirement: the MAG is to ensure the following four tables:

-A table for binding update history and policies, in regards to the MN

-A table for binding cache of each MN is within the LMA of the MAG

-A table for the MN outlines for the LMA of the MAG

-A table for chord system reference

Note that the binding update history and policy of the MAG and the MN-concerned interfaces are to be saved. Such binding update history and policy are comprehensively inclusive of the MN-identifier (128 bits, at maximum), the link layer identifier of the MN-concerned interfaces (16 bits), the IPv6 home network list heading the MN-concerned interface (128 bits, each), the MAG link local address of the MN and the shared access link (128 bits), the IPv6-form address for the LMA of the MN (128 bits), the point-to-point link interface between the MAG and the MN (128 bits, for most of the cases), the bi-directional tunnel interface identifier between the LMA of the MN and the MAG (128bits, at maximum), the policy profile with the MN-ID (128 bits, for most of the cases), the IPv6-form address of the LMA of the MN (128bits), and other option fields (200 bits, for most of the cases), totaling (1,600 + 128 * S), where S denotes the MN-concerned interfaces, projected to be around 3,000 bits.

Another 3,000 bits are to be reserved for the MAG, for its own binding update fields, binding cash, and policy profile. Note that each field comprise the key (128 bits, presumably) and the IPv6-form address of the ensuing hop (128 bits), totaling up to 256 bits. Note, however, that upon the said condition the table is short of accommodating all the fields listed, almost demanding 6,000 bits. The modern-day DRAM allows 2 Gbytes per unit, allowing a single MAG to save more than 300,000 MNs.

4.1.2. Throughput: How the MAG is capable of processing is another instrumental aspect that matters for SARP performance. The nMAG, upon recognizing the MN access, requests the chord system for the IPv6-form address of the concerned LMA. Note that, for the N-node chord system, the router message is queried $\log N/2$ times on average, the QServer of the MN, as requested, is to refer to its costs for the said IPv6-form address. The LMA of the MN, upon recognition of the nMAG, sends out the PBA and the PBU to the MAG of the MN and the LMA of the MN, respectively. Note that the cost of the handover for the MN is $(\log N/2+4)$. Supposing 'p' denotes the period of handover and M_v denotes per-second handover, the chord system is to process $(\log N/2+4)M_v$ amount of the handover. Supposing further that most of

the said amount is processed without failure, a single MAG processes $(\log N/2+4)M_v/N$ amount, bound by 'C' ($(\log N/2+4)M_v/N \le C$), where $N=2^s$ settles the imbalance.

$$M \le \frac{C \times 2^{s+1}}{p \times (s+8)}$$

In these regards, the total number for the MN subject to the SARP domain is to be:

$$M \le \min\left(\frac{C \times 2^{s+1}}{p \times (s+8)}, 300000 \times 2^s\right)$$

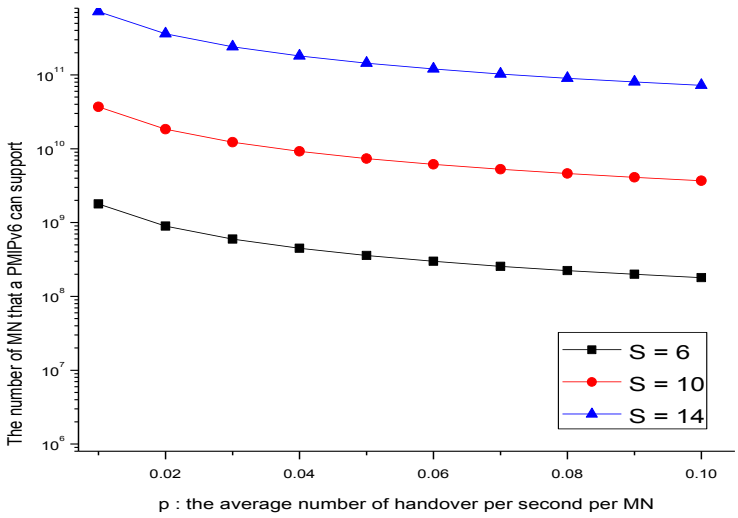


Figure 10. The Number of MNs that a SARP Domain can Support when p and s Vary

The procedure for the authorization of messages, by the MAG as necessary, by means of the private keys, is to be done by a 3 GHz processor and a fast encryption system (ESIGN, *etc.*,) at the rate of 2,048 bits per 100~150 microseconds. This states that such a 3 GHz processor is capable of confirming 6,600 keys and 10,000 authorizations per second. With the advent of a multi-core processor, the MAG will be capable of 10,000 messages per second (C = 10,000) in the near future.

Refer to Figure 10 for the number of MNs subject to the SARP domain for the different 'p' and 's'. Note that a 'p' has been set the greatest value possible, stated hereunder. As 'p' varies, with 's' remaining still, at P = 0.01 and S = 6 (64 MAGs) and supposing the SARP domain supports 10^7 the MNs, the number of MNs the SARP domain supports will decrease. Note that as 'p' is ticked up by 0.1 the number of MNs decreases to 10^6. Supposing p=0.1, the number of MNs returns back to 10^7 for s=10 (1,024 MAGs) stating that a SARP domain, comprising 1,024 the MAGs, is able to support 10^7 MNs at p=0.1.

Refer to the following Figure 11 where a single SARP domain supports MNs at N=16,384(*i.e.*, s=14) and p=0.1. Note that the SARP domain supports more of MNs with the greater number of MAGs.

4.1.3. Estimation of 'p': Suppose that 'p' is within the scope of 0.01 ~ 0.1, sitting between the average handover and per-second processing of the MN by the MAG, often lower than the failed handovers upon the MAG's access to the varied APs. The average period of the MN situated within the MAG's coverage is to be assessed herein, in light of the random coordinate mobility model [14], the model often referred to mobile networks. The randomly chosen MN, uniformly distributed, chooses the coordinate, within the concerned area, and makes a linear move at a constant velocity ($V_{\min}$, $V_{\max}$). The MN, upon mobility, halts its movement to start again, at a velocity newly set. Suppose that T and L are the time elapsed and distance moved, respectively, while the MN is deemed stationary over such time before halt.

The average transition time (E[T]) and the average number of transverse within the MAG's coverage relate as follows:

$$p = E[C]/E[T]$$

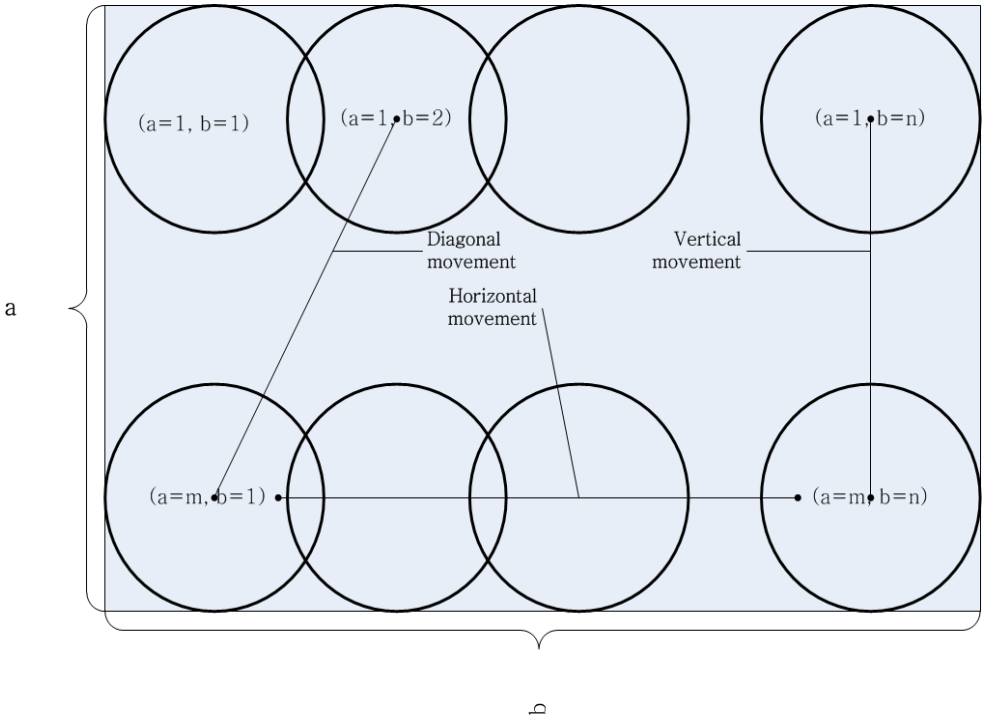


Figure 11. Rectangular Network Topology

Refer to Figure 11 for reference of length 'b' and width 'a', each being a side of the rectangular shape, to derive E[C] and E[T]. Supposing that such rectangular shape covers the MAG's coverage, within row 'm' and column 'n', at E[L] as given by [14]:

$$E[L] = \frac{1}{15}\left[\frac{a^3}{b^2} + \frac{b^3}{a^2} + \sqrt{a^2+b^2}\left(3 - \frac{b^2}{a^2} - \frac{a^2}{b^2}\right)\right] + \frac{1}{6}\left[\frac{b^2}{a}\Phi\left(\frac{\sqrt{a^2+b^2}}{b}\right) + \frac{a^2}{b}\Phi\left(\frac{\sqrt{a^2+b^2}}{a}\right)\right]$$

$$\Phi(x) = \ln\left(x + \sqrt{x^2-1}\right)$$

As the transitional length L and velocity V are both independent from the randomly chosen coordinate model, the average transition time E[T] is to be:

$$E[T] = E[L/v] = E(L)E(1/v)$$

As the velocity V is uniformly distributed within (V_{min}, V_{max}):

$$E(1/v) = \int_{V_{min}}^{V_{max}} \frac{1}{v} \times \frac{1}{V_{max} - V_{min}} dv = \frac{\ln(V_{max}/V_{min})}{V_{max} - V_{min}}$$

The average transition time E[T], E[L], and E[1/v] are comprehensively abstracted out of equations mentioned before. Note that the computation of E[C] should be done in light of the three different (vertical, horizontal, and diagonal) movements, as depicted in Figure 11. Refer to the following formula for mobility between the MAG (from the MAG(α_i, β_i) to the MAG(α_j, β_j)), in light of the transverse c(α_i, β_i, α_j, β_j) [15]:

$$c(\alpha_i, \beta_i, \alpha_j, \beta_j) = |\alpha_i - \alpha_j| + |\beta_i - \beta_j|$$

Note that the average transverse E[C] is to be computed from the average of feasible c(α_i, β_i, α_j, β_j):

$$E[c] = \frac{1}{m^2 n^2} \sum_{\alpha_i=1}^{m} \sum_{\beta_i}^{n} \sum_{\alpha_j=1}^{m} \sum_{\beta_j=1}^{n} c(\alpha_i, \beta_i, \alpha_j, \beta_j)$$

Refer to the following formula, in replacement of c(α_i, β_i, α_j, β_j), by the above formula:

$$E[C] = \frac{1}{m^2 n^2} \sum_{\alpha_i=1}^{m} \sum_{\beta_i}^{n} \sum_{\alpha_j=1}^{m} \sum_{\beta_j=1}^{n} \left(|\alpha_i - \alpha_j| + |\beta_i - \beta_j| \right)$$

Given a, b, and R:

$$m = (a - L_0)/(2R - L_0),\ n = (b - L_0)/(2R - L_0)$$

where denotes the overlapping extent of the two different the MAGs. Note that P is derived from the above equations.

Refer to Figure 12 for ‘p’, the average of R_S varies (upon V_{min} =1 and V_{max}, at L_0 =20 meters, a=80,000 meters, and b=60,000 meters). As seen in Fig. 11, V_{max} has been clocked at 50 m/s at p=0.094 and R=100 meters. Note that such ‘p’ reduces as the MAG covers more. For instance, ‘p’ is to be reduced to 0.045 at R = 200m and V_{max} =50m/s and remains below 0.03 with R greater than 200m and V_{max} sitting below 30m/s.

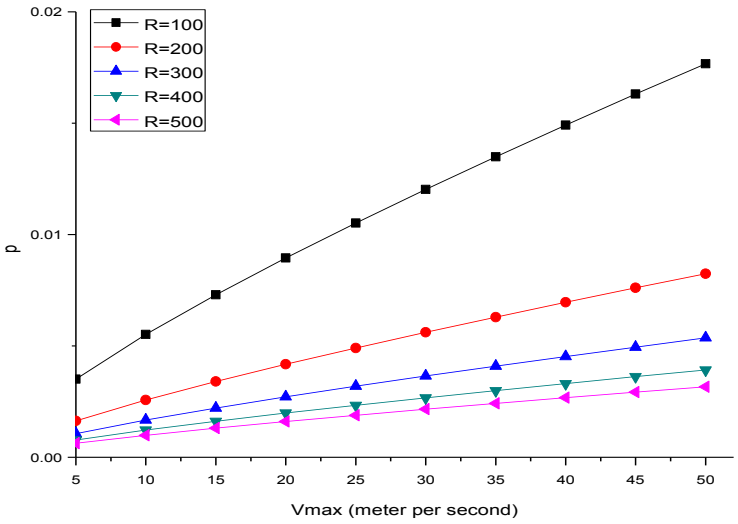


Figure 12. The Average Value of p with varied R (V_{min}=1, L_0=20 meters, a=80,000 meters, and b=60,000 meters)

Refer to the following Figure 13 for the average value of 'p', upon variation of V_{max} at V_{min} =1, L_0 =20m, a=30,000m, and b=10,000m, depicted analogous to that of Figure 12, deemed highly feasible, as far as the SARP domain is concerned, over a 'p' scope of 0.01 ~ 0.1. Note that the MNs are around the MAG's coverage for at least 10 seconds.

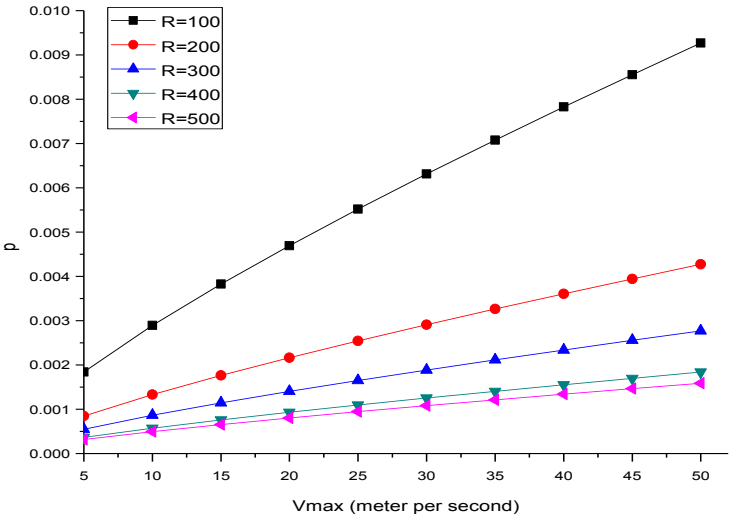


Figure 13. The Average Value of p with Varied R (V_{min}=1, L_0=20 meters, a=30,000 meters, and b=10,000 meters)

4.2. Handover Latency

The handover for 3S Approach, the SARP domain, and fast handover of the SARP domain are to be compared herein to analyze latency thereof. As handover latency, in its analysis, can rarely be standardized, the model in [13] and the analytical result of [14] have been incorporated to depict the following Figure 14:

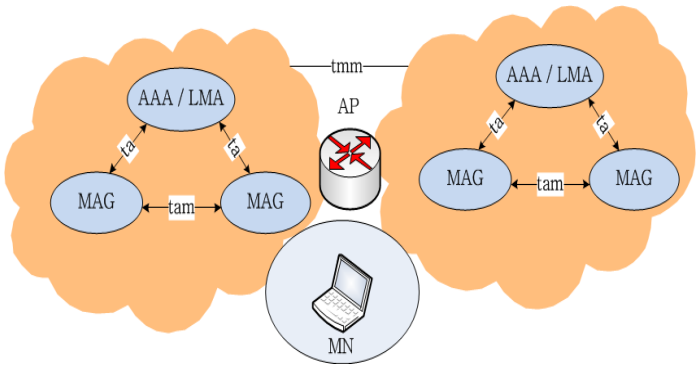


Figure 14. An Analytic Model for Handover Latency Analysis

Refer to t_{mm}, the average latency between the MAG and the MN and inter-MAG for packet transmission. Supposing t_{am}, the average latency between the MAG and the LMA, is not lost, upon the intra-MAG of the PMIPv6 domain, the average handover latency, in light of the model in [14] is to be:

$$D_{3S}^{Intra} = t_{mm}$$

$$D_{3S}^{Inter} = D_{3S}^{Intra}$$

The average handover latency comprises t_{mm}, T_{query}, t_{am}, and $2t_{am}$ denoting the average latency of the MAG to the MN, the average latency of the MAG requesting the QServer, the average latency of the QServer and the MAG, and the round-trip latency between the MAG and the LMA, respectively. Note that $t_{am} = t_a$, in any cases where the QServer does not connect to the MAG. Note further that T_{query} is dependent on 'h' (Hops count), passing queries within the chord system, and the average latency thereof t_{aa}. Suppose $t_{aa} = t_a$, as done for t_{am}, to estimate t_a of the average latency out of the MAG's inability to access the AAA Server. Note that, in [5], the average of [0, logN](h $\in$ [0, s]) is to be $\frac{s}{2}$, thereby incorporating the average handover latency of:

$$D_{SARP-basic}^{Intra} = T_{query} + t_{am} + 2t_{am} = h \times t_a + t_a + 2t_{am} + t_{mm} = (h+1)t_a + 2t_{am} + t_{mm}$$

$$D_{SARP-basic}^{Inter} = D_{SARP-basic}^{Intra}$$

Refer to the following formula for the average MAG-MN and the nMAG-pMAG handover latencies of t_{mm} and $2t_{am}$, respectively:

$$D_{SARP-fast}^{Intra} = 2t_{am} + t_{mm}$$

$$D_{SARP-fast}^{Inter} = D_{SARP-fast}^{Intra} + 2t_{am}$$

Note that, upon fast handover, the nMAG of the MN and the LMA of the MN are not subject to latency as the LMA of the MN is able to directly send packets to the pMAG of the MN, thereby allowing the MN to receive packets from the nMAG via the bi-directional tunnel.

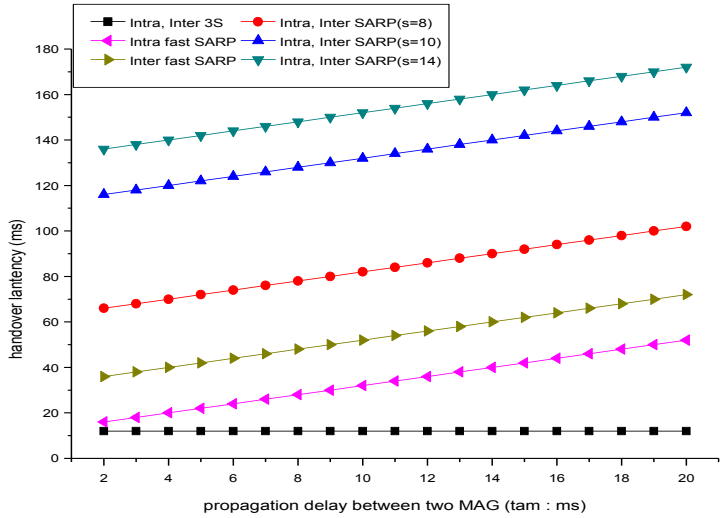


Figure 15. Comparison of Handover Latency for the Four Handover Approaches when t_{mm}=12ms and t_a=10ms

Refer to Figure 15, where t_{mm} = 12ms and t_a = 10ms, to compare handover latencies upon the different approaches. Suppose that the average handover latency is to be h=s/2.

Note that the 3S Approach features the lowest handover latency as adjoining the concerned MAGs. Note further that the fast handover features a much lower latency compared to the basic one.

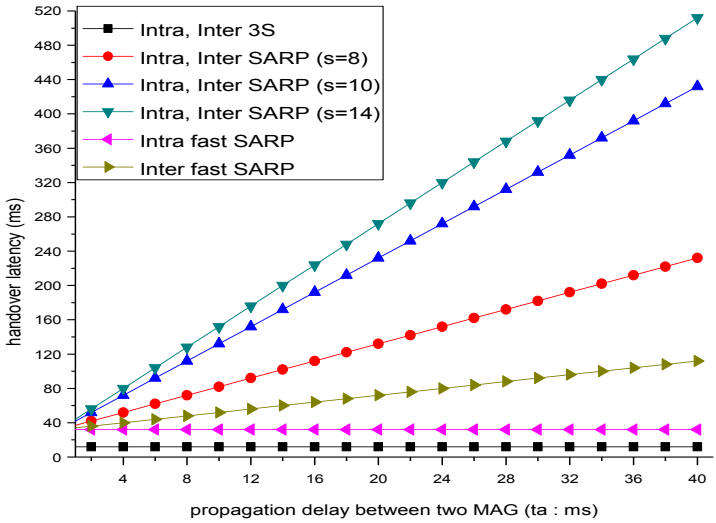


Figure 16. Comparison of Handover Latency for the Four Handover Approaches when t_{mm}=12ms and t_{am}=10ms

Refer to the said Figure 16, where t_{mm} = 12ms and t_a = 10ms, to further compare handover latencies upon the different approaches. As greater t_a (*e.g.*, 40ms) elongates latency, most real-time applications demand a handover latency below 150ms. Note that, upon t_a variation from 2ms to 40ms, the basic handover for the 3S Approach and the fast handover of the SARP often incorporate below-average latencies, not being dependant on the said variation, thereby proving the effectiveness thereof.

4.3. Comparison with SARP

A single PMIPv6 domain and SARP together cover the same extent of the MN greater than 10^8 (covering the Metropolitan area) without inter-domain handover. Refer to Figure 17 for the necessity of inter-domain PMIPv6 handover, much lingering compared to that of the average SARP domain:

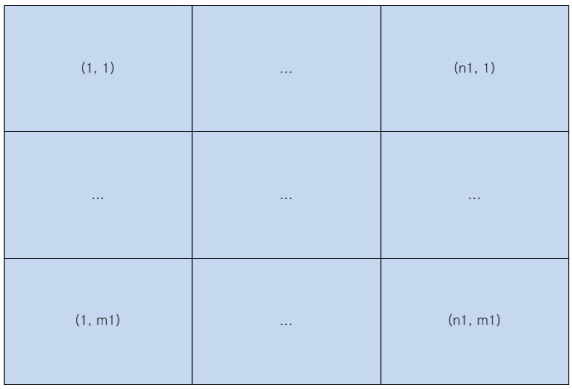


Figure 17. Layout of PMIPv6 Domains

Refer to the following feasibility analysis, incorporating the randomly chosen coordinate model and the perpendicular-form service area. Supposing that, for the standard PMIPv6, the LMA can refer to the traffic of the Q MN and the S MN per km^2, the total counts of the MN within such a perpendicular area (with length of 'A'm and width of 'B'm) is to be:

$$M = \frac{a}{1000} \times \frac{b}{1000} \times S = 10^{-6} \times a \times b \times S$$

Supposing further that every PMIPv6 domain maintains a single LMA then the total PMIPv6 domains necessary to cover the concerned area is to be:

$$N_D = \frac{M}{Q} = \frac{a \times b \times S}{10^6 \times Q}$$

Supposing further that the scope of the PMIPv6 domain stretches through, vertically and horizontally, M and N without loss thereof, the average inter-domain handover, over a single transverse, is to be:

$$E[C] = \frac{1}{3}\left(m_1 + n_1 - \frac{1}{m_1} - \frac{1}{n_1} \right)$$

As $m_1 \times n_1 = N_D$, the derived E[C] is at its minimum, upon $m_1 = n_1 = \sqrt{N_D}$.

$$E[C]_{\min} = \frac{1}{3}\left(\sqrt{N_D} + \sqrt{N_D} - \frac{1}{\sqrt{N_D}} - \frac{1}{\sqrt{N_D}}\right) = \frac{2}{3}\left(\sqrt{N_D} - \frac{1}{\sqrt{N_D}}\right) = \frac{2}{3}\left(\sqrt{\frac{a \times b \times S}{10^6 \times Q}} - \sqrt{\frac{10^6 \times Q}{a \times b \times S}}\right)$$

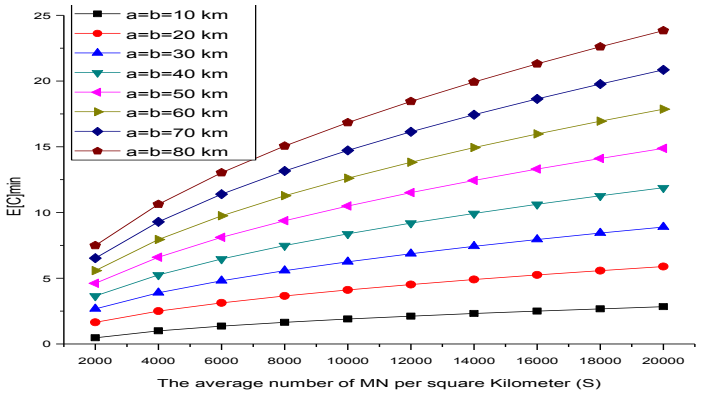


Figure 18. The Average Number of Handovers per Transition (Standard PMIPv6 LMA Deals with 100,000 MN's)

Refer to the said Figure 18 for E[C]min as 'a', 'b', and 'S' vary at Q=100,000. Note that, aside from any cases when a=b=10km and S=1,000, the handover counts are, at any time, greater than 0. As 'S' (Density of the MN), namely the network service area, increases, so does the average handover count.

Note that, for the stationary 'S', the handover average increases by 3 from its initial value 0 as the service area expands, stating that the total MN count is to be 1.28×10^8, beyond S = 20,000, without respect to the coverage of a single SARP domain (6,400km). This still is regarded as what a single SARP domain is unable to overcome.

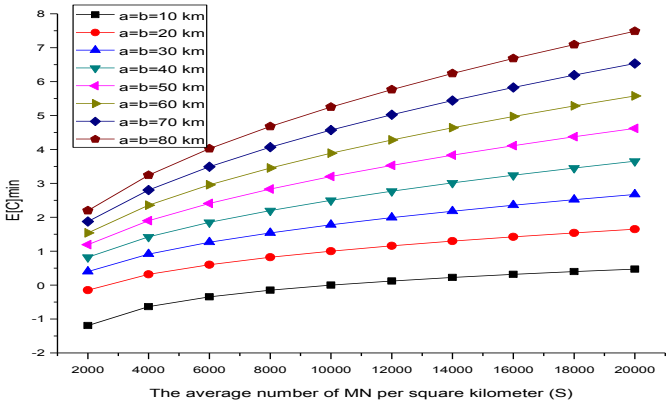


Figure 19. The Average Number of Handovers per Transition (standard PMIPv6 LMA deals with 1,000,000 MN's)

Aside from the case where a single LMA supports the plural MN's of 100,000 or more, Figure 19 depicts where S = 1,000,000, E[C] min. The average inter-domain handover is more or less greater than 0, in the decreasing trend thereof.

5. Conclusion

So far the paper has proposed '3S Approach' for more scalable and reliable PMIPv6 domain. MAGs, being the core component of the Chord-based domain, operate based on LMA, being the core composition. Binding between LMA and MN is established through the constant hashing and distributed via the chord system, the noted distributed hashing table protocol. The domain maintains PKI server to be known public/private key composition, while the 3S designed domain authorizes every handover message for security. The paper has also proposed the handover procedure that best fits 3S considered domain and analyzed its feasibility, demonstrating its capability to support wider scope of MNs. As the 3S Approach is projected to develop more, the wider scope of MNs is expected to be supported with lower inter-/intra-domain latency.

Acknowledgements

This research was supported by Next-Generation Information Computing Development Program (2012- 0006426) and Basic Science Research Program (2011-0027030) through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology.

References

[1] I. Al-Surmi, M. Othman and B. Mohd Ali, "Mobility management for IP-based next generation mobile networks: Review, challenge and perspective", Journal of Network and Computer Applications, vol. 35, **(2012)** January, pp. 295-315.
[2] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury and B. Patil, "Proxy mobile IPv6", IETF RFC 5213, **(2008)** August.
[3] D. Johnson, C. Perkins and J. Arkko, "Mobility support in IPv6", IETF RFC 3773, **(2004)** June.
[4] H. Luo, H. Zhang, Y. Qin and V. Leung, "An Approach for Building Scalable Proxy Mobile IPv6 Domains", IEEE Trans. Netw., vol. 8, no. 3, **(2011)** September.
[5] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek, F. Dabek and H. Balakrishnan, "Chord: a scalable peer-to-peer lookup protocol for Internet applications", IEEE/ACM Trans. Netw., vol. 11, no. 1, pp. 17-32, **(2003)** February.
[6] D. Eastlake and P. Jones, "US secure hash algorithm 1 (SHA1)", IETF RFC 3174, **(2001)** September.
[7] D. R. Karger, E. Lehman, F. Leighton, M. Levine, D. Lewin and R. Panigrahy, "Consistent hashing and random trees: distributed caching protocols for relieving hot spots on theWorldWideWeb", Proc. 29th Annu. ACM Symp. Theory Comput., **(1997)** May, pp. 654-663.
[8] A. Patel, K. Leung, M. Khalil, H. Akhtar and K. Chowdhury, "Mobile node identifier option for mobile IPv6 (MIPv6)", IETF RFC 4283, **(2005)** November.
[9] L. R. Monnerat and C. L. Amorim, "D1HT: a distributed one hop hash table", Proc. 20th IEEE International Parallel & Distributed Processing Symposium, **(2006)** April.
[10] Q. Pu, "An Enhanced Authentication Scheme with Anonymity for Roaming Service in Global Mobility Networks", MMIT 2010, vol. 2, **(2010)** April, pp. 219-222.
[11] C. C. Chang, C. Y. Lee and Y. C. Chiu, "Enhanced authentication scheme with anonymity for roaming service in global mobility networks", Com. Commu., **(2009)**, pp. 611-618.
[12] R. Koodli, "Fast handovers for mobile IPv6", IETF RFC 4068, **(2005)** July.
[13] K.-S. Kong, W. Lee, Y.-H. Han, M.-K. Shin and H. You, "Mobility management for all-IP mobile networks: mobile IPv6 vs. proxy mobile IPv6", IEEE Wireless Commun., vol. 15, no. 2, **(2008)** April.
[14] Q. B. Mussabbir, W. Yao, Z. Niu and X. Fu, "Optimized FMIPv6 using IEEE 802.21 MIH services in vehicular networks", IEEE Trans. Veh. Technol., vol. 56, no. 6, **(2007)** November, pp. 3397-3407.
[15] C. Bettstetter, H. Hartenstein and X. Perz-Costa, "Stochastic properties of the random waypoint mobility model", Wireless Netw., vol. 10, no. 5, **(2004)** September, pp. 555-567.

Authors

Jongpil Jeong he received his B.S. degree in engineering from Sungkyunkwan University and the M.S. and Ph.D. degrees in computer engineering from Sungkyunkwan University, Suwon, Korea, in 2003 and 2008, respectively.

He was a Research Professor with Sungkyunkwan University in 2008-2009 and 2011, and a visiting professor with the Department of Interaction Science in Sungkyunkwan University in 2009-2010. He started his academic profession at Sungkyunkwan Univeristy, Korea in 2012 as an assistant professor. His research interests include mobile computing, mobility management for vehicular networks, sensor networking, protocol operation based performance analysis, Internet security, MIPv6 and ubiquitous computing.

Min Kang he received his M.S. degree in computer engineering from Sungkyunkwan University, Suwon, Korea, in 2012.

His current research interests include quality-of-service provisioning, resource allocation in multimedia wireless communications, network mobility, and network security.

Younghwa Cho he received his B.S. degree in statistics and the M.S. degree in computer science from Sungkyunkwan University in 1977 and 1990, respectively. In 1999, he completed his Ph.D. degree in computer science from Chungbuk University, Korea.

He was with KISTI(Korea Institute of Science and Technology Information) as a President from 2001 to 2006. He has also served as a President at KISTEP(Korea Institute of S&T Evaluation and Planning) from 2007 to 2008. He joined Kyungwon University as a visiting professor from 2008 to 2010. He is currently a distinguished visiting professor in the college of information and communication engineering at the Sungkyunkwan University, Korea. His current research interests cover software engineering, data base, information communication technology, R&D strategies and so on.

Jaeyoung Choi he received his B.S. degree in mathematics in 1995, and the M.S. and Ph.D. degrees in computer science from the Kyungwon University, Korea, in 1999 and 2004, respectively.

From 2004 to the middle of 2006, he joined the Vision Laboratory at the UCLA, USA, as a postdoctoral research assistant. He has also served as a BK21 research professor at Kyungwon University from 2006 to 2010. Since 2010, he has been a professor with the department of computer engineering, college of information and communication engineering at the Sungkyunkwan University, Korea.