Full Title:

An Operational Mobility Model over IPv6 (OMIPv6): Design, Modelling and Evaluation

Short Title:

An Operational Mobility Model over IPv6

Yulei Wu, Jingguo Ge, Junling You, and Yuepeng E

Computer Network Information Center, Chinese Academy of Sciences, Beijing, 100190, P.R. China

Email: {wuyulei, gejingguo, youjunling, eyp}@cstnet.cn

The corresponding author:

Yulei Wu

Address: CSTNet, Computer Network Information Center, Chinese Academy of Sciences, Beijing, 100190, P.R. China

Email: wuyulei@cstnet.cn

Telephone: +86 10 58813820

Fax: +86 10 58812888

An Operational Mobility Model over IPv6 (OMIPv6): Design, Modelling and Evaluation

Yulei Wu, Jingguo Ge, Junling You, and Yuepeng E

Computer Network Information Center, Chinese Academy of Sciences, Beijing, 100190, P.R. China

Email: {wuyulei, gejingguo, youjunling, eyp}@cstnet.cn

Abstract

The fast Internet evolution and rapid development of wireless technologies have made it possible for users to communicate while on the move. Mobile IPv6 (MIPv6) is a candidate solution for next generation mobile Internet. Despite its popularity, MIPv6 still suffers various limitations, e.g., lack of business model and management of enormous and discrete home agents, preventing it from being deployed in large-scale commercial environments. Recently, the ID/Locator split architecture has demonstrated its significant predominance in next generation mobile networks. With the aim of pushing the global deployment of mobility support over IPv6, this study makes an effort to design and evaluate an operational mobility model over IPv6 (OMIPv6) based on ID/Locator split architecture to tackle the problems raised by the current form of MIPv6. In particular, a distributed cloud mobility management system (D-CMMS) is employed to be responsible for maintaining the identification and locations of mobile hosts, as well as providing the name resolution services to the mobile hosts. Furthermore, this paper develops an analytical model considering all possible costs required for the operation of OMIPv6, and adopts it as a cost-effective tool to evaluate various costs and operation overheads on the performance of OMIPv6 protocol.

Keywords: Mobile Internet, Operational Networks, Mobile IP, Cost Analytical Model

1. Introduction

The fast Internet evolution and rapid development of wireless technologies (e.g., Wi-Fi, WiMAX, cellular networks, etc.) have made it possible for users to communicate while on the move [1, 14, 17]. Mobile IP, developed by Internet Engineering Task Force (IETF), is a solution to provide continual Internet connectivity to mobile users. The proposed mobile IPv4 (MIPv4) [18], mobile IPv6 (MIPv6) [6] and their variants are the main protocols for mobility support over IP in the Internet. In comparison with MIPv4, MIPv6 offers a number of improvements mainly due to the capabilities inherited from the IPv6 [13, 21], such as enormous address space for every conceivable application/device, stateless address auto-configuration for acquiring temporary care-of-address, etc., making it a candidate solution for next generation mobile Internet.

The modelling and analysis of MIPv6 and its variants have been widely reported in the literature [5, 10, 12, 15]. Despite its popularity, MIPv6 still suffers various limitations preventing it from being deployed in large-scale commercial environments. Among these is the lack of management of discrete home agents, which are mainly responsible for maintaining the home-of-address (i.e., permanent address) and care-of-address (i.e., temporary address) mappings of mobile hosts.

The identification/locator (ID/Locator) split architecture [7], which uses distinct sets of values for ID and Locators of mobile hosts, has demonstrated its significant predominance in next generation mobile networks. In particular, several arguments [16] have shown that MIPv6 can be considered as a typical example of ID/Locator split architecture where home-of-address represents the ID of the mobile host and the care-of-address denotes the Locator of the mobile host. With the aim of pushing large-scale commercial deployment of mobility support over IP, this study makes an effort to design and evaluate a new operational mobility model over IPv6 to

achieve the purpose of 1) realising ID/Locator split architecture to support global mobility, and 2) maintaining a distributed global mobility management mechanism to replace enormous and discrete home agents over the world. In particular, this study makes the following contributions:

- A naming mechanism is provided to name the mobile hosts, and a promising address model is proposed to accommodate the ID of mobile host and its location in the 128-bit IPv6 address space to realise ID/Locator split architecture.
- Based on the idea of Cloud computing and MIPv6, this study proposes a new operational mobility model over IPv6 (OMIPv6) with a distributed cloud mobility management system (D-CMMS) being responsible for maintaining the IDs and Locators of mobile hosts, as well as providing the name resolution services to the mobile hosts. The D-CMMS is designed in a hierarchical scheme to relief the burden of its components.
- A business model with billing strategies for OMIPv6 is presented to increase the profit of access routers and incent the selfish access routers to forward packets.
- An analytical model is then developed to calculate all possible costs required for the operation of OMIPv6 protocol, including the query cost, registration and update cost, lookup cost, and the packet delivery cost.
- To illustrate its applications, the proposed analytical model is then adopted as a cost-effective tool to evaluate and analyse the performance of OMIPv6 protocol.

The remaining of this paper is organised as follows. Section 2 reviews the standard MIPv6 protocol which facilitates the understanding of subsequent sections. The design of OMIPv6 is presented in Section 3. Section 4 compares the devised OMIPv6 protocol and the standard MIPv6. An analytical cost model for the operation of OMIPv6 is then developed in Section 5. Section 6 carries out performance analysis of OMIPv6 protocol by virtue of the proposed cost model. Finally, Section 7 concludes this study.

2. Related Work

The MIPv6 has been proposed for mobility support in IPv6 wireless/mobile networks. To reduce high signaling overhead incurred in MIPv6 networks in the presence of frequent handovers, hierarchical mobile IPv6 (HMIPv6) [20] introduced a new concept of mobility anchor point (MAP) to handle binding update requests pertaining to intra-domain handovers in a localised manner. In addition, fast handovers for mobile IPv6 (FHMIPv6) [9] was proposed to reduce the service degradation of mobile hosts due to the changes in its point of attachment. To achieve a network-based mobility management approach, proxy mobile IPv6 (PMIPv6) [4] was standardised by the IETF NETLMM Working Group in 2008. However, all these protocols adopt discrete home agents to maintain the home-of-address (i.e., permanent address) and care-of-address (i.e., temporary address) mappings of mobile hosts, which lacks of management scheme, and, thus prevents them from being deployed in large-scale commercial environments. Our designed OMIPv6 borrows the idea of Cloud computing and introduces a new concept of D-CMMS being responsible for maintaining the permanent addresses (i.e., identifications) and temporary addresses (i.e., locations) of mobile hosts. The specification of D-CMMS is presented in Section 4.2.2.

The modelling and analysis of MIPv6 and its variants (i.e., HMIPv6, FHMIPv6 and PMIPv6) have been widely reported [5, 10, 12, 15]. For instance, Lee, Ernst and Chung [10] proposed cost models to evaluate and compare the performance of existing and widely reported IP mobility management protocols including MIPv6 and its variants in terms of signalling cost, packet delivery cost, and tunnelling cost. In addition, an analytical model [5] was developed to estimate and analyse the cost of key mobility management entities in the variant of MIPv6 networks and show the impact of network size, mobility rate, traffic rate and data volume on the cost of

mobility entities. The authors in [15] conducted the performance evaluation of MIPv6 and its variants by virtue of simulation experiments. Liang et al. [12] proposed an analytical model to study the queueing effects on the handoff performance of MIPv6 protocol. Due to the popularity of cost analysis on mobility protocols, in this paper, we develop an analytical cost model for the operation of OMIPv6.

The ID/Locator split architecture [7] has demonstrated its significant predominance in next generation mobile networks. Many researchers [8, 16, 19] have adopted such an architecture to support mobility, multi-homing and scalability in the future Internet research. Consequently, in this study, we adopt the ID/Locator split architecture to support mobility in the proposed OMIPv6.

3. Mobile IPv6 (MIPv6)

For the sake of readily understanding of our proposed mobility model, this section briefly reviews the standard MIPv6 protocol, and its specifications can be found in [6]. The key components of MIPv6 consist of mobile hosts (MHs), home agents (HAs), and correspondent hosts (CHs). An MH maintains two 128-bit IPv6 addresses: a permanent home-of-address (HoA) which is obtained from its HA in the home network and a temporary care-of-address (CoA) which is automatically allocated in the foreign network due to the stateless address auto-configuration feature of IPv6. An MH is identified by its HoA, regardless of its current point-of-attachment to the Internet. The HAs located in the home network of an MH are dedicated nodes in the MIPv6 protocol and keep the mappings between HoA of an MH and its current CoA. In addition, each CH has its own binding cache to store the pairs of HoA-CoA mapping of an MH to achieve the purpose of route optimisation. The communication between the MH and the CH is carried out in the following two cases:

1) *MH locates at the home network*: an MH would communicate with its CH based on the standard IPv6 protocol;
2) *MN moves to a foreign network*: the MH would acquire a new temporary CoA and notify its HA and CHs of the location update before starting to communicate with the CHs. In order to insure that the location update message is authentic and avoid malicious attack to the CH, a return routability procedure must be performed before executing an update process at the CHs.

3.1 The drawbacks and limitations of MIPv6

MIPv6 is announced in 2004 but has not yet been deployed in large-scale commercial environments due to the following limitations:

- Since the potential billions of mobile handheld and devices are expected to connect through the Internet [16], in MIPv6, enormous HAs will be located discretely over the world, which makes them unmanageable, lacks of business model and is hard for billing statistics.
- Since the access routers may be owned by different profit-oriented independent agents, such as restaurants, small business offices, airports, etc., they are indeed selfish. MIPv6 is unable to provide a mechanism (e.g., payment) to incent the access routers to forward packets. Therefore, an MH which moves to a new sub-network is difficult to have its packets forwarded in the realistic working environment.
- In the standard MIPv6, the data packets received by the HA need to be encapsulated and tunneled to the MH, which requires additional encapsulation cost. In addition, the extension header is used during the communication between the MH and CH. This also requires extra transmission cost and extension header handling cost.

In the next section, we aim to address these problems and develop new mobility architectures over IPv6. In particular, based on the idea of Cloud computing, we propose to realise the functionality of the HAs by the D-CMMS to achieve an operational mobile network over IP.

4. Operational Mobility Model over IPv6 (OMIPv6)

OMIPv6 is proposed to provide an operational and manageable mobility support over IPv6. The key components of OMIPv6 consist of the MH, CH, autonomous system (AS), a naming mechanism, and the D-CMMS, as shown in Fig. 1, where the D-CMMS contains the name resolution mechanism and billing statistic systems for mobile hosts. In what follows, the principles and implementation of OMIPv6 protocol will be shown separately.

4.1 The principles of OMIPv6

The principles of OMIPv6 protocol are presented as follows:

1) The naming mechanism gives the name to each MH.
2) Each MH entering the network which is connected to the Internet should register its information including unique identification and network prefix (representing current point-of-attachment) to the D-CMMS.
3) Once moving to a new network, the MH could acquire a new network prefix and should update it to the D-CMMS.
4) To communicate with the MH, the CH need obtain the identification and network prefix of the MH by searching the mapping tables with the index (i.e., the name of MH) in the D-CMMS before starting the data communication.

4.2 The implementation of OMIPv6

The implementation of OMIPv6 includes the address architecture and configuration, the detailed functionality of D-CMMS, and the communication process of the protocol. A case study with three typical scenarios will be shown at the end of this section.

4.2.1 Address architecture and configuration

OMIPv6 is based on the ID/Locator split concept and follows the conventional 128-bit IPv6 address architecture. The upper 64-bit represents the network prefix (NPF) and the lower 64-bit denotes the host ID (HID). The NPF identifies the location of a sub-network, while the HID indicates the ID of an MH and is globally unique.

Each MH is always identified by its HID and is associated with an NPF providing the information of the MH's current point-of-attachment. When an MH moves from one sub-network to another, the new access router (AR) is discovered through the router advertisement (RA) message. After acquiring a new NPF, the MH performs the update to the D-CMMS (its specification is presented in Section 4.2.2) through binding update (BU) and binding acknowledgement (BAck) message exchange.

To maintain the communication session while the MH is moving, OMIPv6 requires a mechanism at the MH to keep a constant IPv6 address for transport layer and upper layer. This can be done by filling with a constant value (CV) in the upper 64-bit of the address (see Fig. 2). On the other hand, the network layer adopts an actual network prefix, i.e., NPF, in the upper 64-bit of the address.

Recall that each MH should be given a unique name by the naming mechanism. Specifically, the *naming mechanism* gives the host full name (HFN) to the MH. The HFN is human readable and memorable characters and is configured by concatenating the host name and the domain

name using @ symbol, e.g., host@domain. The HFN is globally unique, rather than the host name which is only unique with respect to the domain name.

4.2.2 Distributed Cloud mobility management system (D-CMMS)

D-CMMS is mainly responsible for maintaining name-ID-Locator mappings of MHs and contains name resolution mechanisms to perform name resolving services to the MHs.

The *name resolution mechanism* consists of three key components: 1) domain name resolver (DNR) used for maintaining the domain names, 2) host name resolver (HNR) used for maintaining the host names, 3) autonomous system manager (ASM) used for managing the sub-networks. The resolution mechanism is designed in a hierarchical scheme to relief the burden of DNR, HNR and ASM in the D-CMMS. In particular, the DNR can be viewed as a global managing system providing the domain resolution service to the MHs, ASM can be viewed as an intermediate-level managing system providing the autonomous system resolution service, while the HNR can be seen as a local managing system providing the HFN resolution service to the MHs. From the perspective of engineering, the name resolution systems including the DNR, ASM and HNR can be achieved by the technology of Cloud computing [3], because it is a promising technique for enabling ubiquitous, convenient, on-demand network access, particularly it is suitable for the case of increasingly large volume users and high computing capabilities.

Fig. 3 shows the resolution system of the DNR, ASM and HNR, respectively, where the DNR maintains the domain names, the ASM maintains host-AS mappings and the HNR mainly maintains the HFN-NPF-HID mappings of the MHs. Due to the selfish nature, ARs will forward packets only when the profit they make exceeds the cost they spend in forwarding. We assume the MHs and ARs have contract with network operators or service providers, which are responsible for managing the charge information of MHs. Such information is stored in the Bill

section of the mapping table in the HNR, as shown in Fig. 3(c). The profit of ARs will be settled by the network operators or service providers depending on the business model presented in Section 4.2.3.

4.2.3 An incentive mechanism for cooperation among selfish ARs

A business model will be proposed to 1) increase the profit of ARs and 2) incent the selfish ARs to forward packets. In particular, we consider two kinds of virtual currency: credits and tokens [11]. Each AR generates credits by forwarding packets for newly-entered MHs and consumes credits in sending packets for its local MHs. It is worth noting that the ARs are unable to send packets for their local MHs if they do not have enough credits. In this way, the selfish ARs can be encouraged to increase their credits by participating packet forwarding for newly-entered MHs. On the other hand, the local MHs need pay tokens to their attached ARs for sending their packets. The required amount of credits and tokens for packet forwarding of newly-entered MHs and local MHs can be determined by network operators or service providers.

The credits have no monetary value, while the tokens have real monetary value and can be either used to buy credits or cashed from the central bank, which may be owned by network operators or service providers and can get profit through the differences in the selling and buying prices of tokens. The generation and management of credits and tokens can be audited either by a special hardware or software equipped with the ARs as in [2], or by a fair third party such as the central bank through a secure connection as in [23].

Let C_f^+ and C_f^- denote the number of credits obtained by forwarding one unit data packet for newly-entered MHs and local MHs, respectively. Let T_f represent the number of tokens paid by local MHs for sending one unit data packet. We assume the tokens, credits and cash maintain the following relationship:

$$1 \times Token = R \times Credits \tag{1}$$

Let x and y denote the total data packets forwarded for newly-entered MHs and local MHs, respectively, per year per AR. Therefore, the annual profit, A_{ar}, of an AR can be expressed as

$$A_{ar} = \begin{cases} T_f y + \dfrac{\left| C_f^+ x - C_f^- y \right|}{R} & C_f^+ x - C_f^- y \geq 0 \\ T_f y - \dfrac{\left| C_f^+ x - C_f^- y \right|}{R} & C_f^+ x - C_f^- y < 0 \end{cases} \tag{2}$$

4.2.4 Operation process of OMIPv6

Fig. 4 represents the sequence of message flow control in OMIPv6 based on the stateless address auto-configuration of IPv6. When entering the sub-network, the MH acquires an NPF and register its <HFN-NPF-HID-Bill> with the HNR, and register its <host-AS> with the ASM (the locator of the ASM could be obtained by performing the lookup action at the mapping table of the DNR).

The movement of MH between sub-networks is detected by the RA message. Upon moves to a new AR under the same AS, the MH acquires an NPF and updates its new NPF and the bill information which could be made by the new AR to the HNR by BU/BAck message exchange. As long as the MH moves across ASs, besides the update to the HNR, an update must be made to the ASM from the HNR with its received information (the locator of ASM could be obtained by performing the lookup action at the DNR). Meanwhile, a negotiation process between the new registered HNR and previous HNR need to be carried out to perform mapping table update at previous HNR. To communicate with the MH, a CH (assume it knows the HFN of an MH) first sends a query message to the DNR to acquire the locator of corresponding domain by performing the lookup action with the index (i.e., domain name of the MH). Then, the MH could obtain the

locator of corresponding AS by performing the lookup action with the index (i.e., host name of the MH). With the known information of the AS, the CH sends a query message to the corresponding HNR to obtain the NPF and HID of the MH by performing the lookup action with the index (i.e., HFN of the MH). Once getting the required information, the HNR responds to the CH with the NPF and HID of the MH. Meanwhile, the HNR sends the NPF and HID of the CH to the MH; this can be achieved because the lookup message sent by the CH contains the required information. Till now, both the MH and the CH can carry out verification and security check to avoid malicious attack or directly start data communications.

4.2.5 A case study

Let us consider three typical scenarios (depicted in Fig. 5) as follows:

1) CH.1 communicates with MH.1 in the coverage of AR.1;
2) CH.1 communicates with MH.1 which is moving from the coverage of AR.1 to AR.2 (both ARs are under the AS.1);
3) CH.1 communicates with MH.1 which is moving from the coverage of AR.2 to AR.3 (AR.2 and AR.3 are under the AS.1 and AS.2, respectively).

Once the MH and CH complete the registration process, the network entities, i.e., HNR, ASM and DNR, maintain the mapping tables shown in Fig. 6.

For scenario 1, as the CH.1 knows the HFN of MH.1 (i.e., host.1@domain.2), it is able to obtain the locator of ASM (i.e., ASM:domain.2) and the locator of AS (HNR:AS.1) by performing the lookup action at the mapping tables in the DNR and the ASM, respectively. Once acquiring the AS.1 for MH.1 in the ASM, the CH.1 searches the mapping table in HNR:AS.1 and obtains the required address (i.e., NPF.1 and HID.1) for MH.1 before starting data communication.

For scenario 2 where MH.1 moves from the coverage of AR.1 to the coverage of AR.2 (both ARs are under the AS.1), the MH.1 acquires a new NPF (e.g., NPF.2) when entering the coverage of AR.2 and updates it with the HNR:AS.1; the resulting mapping tables in HNR:AS.1 are shown in Fig. 7. The remaining communication processes are similar to scenario 1.

For scenario 3 where MH.1 moves from the coverage of AR.2 to the coverage of AR.3 (AR.2 and AR.3 are under the AS.1 and AS.2, respectively), similar to scenario 2, the MH.1 acquires a new NPF.3 and registers it with the HNR:AS.2; meanwhile, the HNR:AS.2 notifies the HNR:AS.1 to delete its record (see Fig. 8b). As the MH.1 moves across the ASs, it should update its current point-of-attachment to the ASM. The locator of ASM (i.e., ASM:domain.2) could be found by performing the lookup action at the DNR. The resulting mapping tables in the ASM:domain.2 are shown in Fig. 8a. The remaining communication processes are similar to scenario 1.

5. OMIPv6 vs. MIPv6

In contrast to the MIPv6 which requires one or more HAs in the home network, OMIPv6 does not employ any HA; instead, it adopts a distributed management system to store the locations of MHs. A hierarchical scheme is adapted to relief the burden of each entity in this mechanism. The use of such a system is able to facilitate the location management of MHs and their billing statistics in order to achieve the purpose of commercial deployment of mobility support over IP.

The data packets received by the HA need to be encapsulated and tunneled to the MH in the standard MIPv6 protocol, which requires additional encapsulation cost. In contrast, in OMIPv6, upon receiving the NPF and HID of MH and CH, they can start data communications directly without any tunneling cost.

In standard MIPv6 protocol, the MH uses its HoA in the extension headers when originates the communication with the CH, which also requires extra transmission cost and routing header handling cost. In contrast, the OMIPv6 protocol does not use any extension headers to cope with the communication between MHs and CHs.

The standard MIPv6 uses 128-bit home-of-address and 128-bit care-of-address to realise the ID/Locator split architecture to support mobility, in contrast, the address architecture adopted in OMIPv6 consists of 64-bit network prefix and 64-bit host ID in order to achieve the aim of ID/Locator split architecture.

6. The Analytical Model

Having designed our mobility support solution, in this section, an analytical cost model will be developed to evaluate the performance of OMIPv6. The model is based on the following assumptions, which has been widely adopted in the related studies [5, 10].

a) The session arrival for the MHs follows Poisson process with the mean rate of λ_m, and the session length in packets is $E(s)$;
b) ARs are uniformly distributed in a grid manner over the network and an MH can move from the coverage of one AR to another in one movement;
c) The binary search is performed at the mapping tables of D-CMMS.

Recall that N_{AR} ARs are located in the network and each AS covers N_{AS-AR} ARs, the probability that a movement of the MH will be within the coverage of the same AS can be given by

$$P_{in} = \frac{N_{AS-AR}}{N_{AR}} \tag{3}$$

Therefore, the probability that the MH moves out of the coverage of an AS in the *i*-th movement can be given by $P_{in}^{i-1}(1-P_{in})$, and the expected number of movements for an MH to move out the coverage of an AS can be expressed as

$$E(M)=\sum_{i=1}^{\infty} iP_{in}^{i-1}(1-P_{in})=(1-P_{in})\sum_{i=1}^{\infty} iP_{in}^{i-1}=\frac{N_{AR}}{N_{AR}-N_{AS-AR}} \tag{4}$$

The total cost of OMIPv6 includes the cost, $E(C_Q)$, for queries at the DNR, ASM and the HNR, the cost, $E(C_L)$, for lookup the mapping tables at the DNR, ASM and the HNR, the cost, $E(C_R)$, for registration and update information at the DNR, ASM and the HNR, and the cost, $E(C_D)$, for delivering data packets between the MH and the CH. Therefore, the total cost can be expressed as

$$E(C)=E(C_Q)+E(C_L)+E(C_R)+E(C_D) \tag{5}$$

In OMIPv6 protocol, the CH need send a query message to the DNR, ASM and the HNR to acquire the required information of the MH. Let N_{MH} denote the number of MHs in the network and N_{CH} represent the number of CHs for an MH. Thus, the total number of CHs in the network can be expressed as $N_{MH}N_{CH}$. The transmission cost for the query messages and their reply messages towards and from the DNR, ASM and the HNR can be given by

$$\begin{aligned} E(C_Q)=&N_{MH}N_{CH}\lambda_m(2H_{CH-DNR}Z_q)+N_{MH}N_{CH}\lambda_m(2H_{CH-ASM}Z_q)\\ &+N_{MH}N_{CH}\lambda_m(2H_{CH-HNR}Z_q)+N_{MH}\lambda_m(H_{MH-HNR}Z_q) \end{aligned} \tag{6}$$

where H_{CH-DNR}, H_{CH-ASM}, H_{CH-HNR}, and H_{MN-HNR} denote the average distance in hops between the CH and DNR, between the CH and ASM, between the CH and HNR, and between

the MH and HNR, respectively. Z_q is the per hop transmission cost for query messages and their reply messages.

The cost for searching the mapping tables at the DNR, ASM and the HNR to lookup the required information of the MH can be estimated as

$$E(C_L) = N_{MH} N_{CH} \lambda_m \alpha \log k + k N_{MH} N_{CH} \lambda_m \beta \log \frac{N_{MH}}{k} + m N_{MH} N_{CH} \lambda_m \gamma \log \frac{N_{MH}}{m} \quad (7)$$

where k and m denote the number of domain names and the number of ASs in the network, and the cost for mapping table lookup with x entries is proportional to $\log x$ [5]. α, β and γ represent the linear coefficient for lookup cost at the DHR, ASM and the HNR, respectively.

The movement of MH may cause the registration and processing cost at the ASM and HNR. Specifically, the crossing of the sub-networks between ARs under the same AS will happen in every T_{sub} seconds and will cause the cost of

$$E(C_{R-HNR}) = N_{MH} \frac{2(H_{MH-HNR} - 1 + \delta) Z_{rh} + G_h}{T_{sub}} \quad (8)$$

where δ is the proportionality constant of wireless link over wired link, and Z_{rh} and G_h denote the per hop transmission cost and processing cost, respectively, for the registration messages at the HNR. The crossing of the sub-networks between ARs under different ASs will happen in every $E(M)T_{sub}$ seconds and will cause the cost of

$$\begin{aligned} E(C_{R-HNR-ASM}) = {} & N_{MH} \frac{2(H_{MH-HNR} - 1 + \delta) Z_{rh} + G_h}{E(M)T_{sub}} + N_{MH} \frac{2H_{HNR-HNR} Z_{rh} + G_h}{E(M)T_{sub}} \\ & + N_{MH} \frac{2H_{HNR-ASM} Z_{ra} + G_a}{E(M)T_{sub}} \end{aligned} \quad (9)$$

where $H_{HNR-ASM}$ and $H_{HNR-HNR}$ represents the average distance in hops between the HNR and ASM, and between the tables stored the information of the new attached AS and previous attached AS. Z_{ra} and G_a are the per hop transmission cost and processing cost, respectively, for the registration messages at the ASM. It is worth noting that the cost for lookup when performing the registration/update process is ignored because it is relatively small comparing with that required for data communication. The total registration cost can be given by the sum of the cost at HNR and the cost at ASM. Therefore, we have

$$E(C_R) = E(C_{R-HNR}) + E(C_{R-HNR-ASM}) \tag{10}$$

Upon receiving each other's HID and NPF, the MH and CH can start the communication process. As the error of data packets may happen due to the collisions in wireless channels, the retransmissions of the data packets will be considered to accommodate such corruptions. We assume that R retransmissions take place for each data packet transmission. Therefore, the packet transmission cost can be given by

$$E(C_D) = N_{MH} N_{CH} \lambda_m E(s)\{(R+1)[H_x Z_{dp} + Z_p] + H_x Z_{da} + 3Z_p + \nu \log N_{AR}\} \tag{11}$$

where Z_{dp} and Z_{da} represent per hop transmission cost for data packet and data acknowledgement packet. Z_p denotes the cost for address configuration between network layer and upper layer, as shown in Fig. 2. The term, $\nu \log N_{AR}$, is the cost for IP routing table lookup, where ν is the linear coefficient for IP routing table lookup. The number of hops between MH and CH, H_x, can be given by

$$H_x = \begin{cases} H_{MH-CH} - 1 + \delta & \text{CH is a fixed node} \\ H_{MH-CH} - 2 + 2\delta & \text{CH is a mobile node} \end{cases} \tag{12}$$

The overheads of OMIPv6 protocol include the cost for query message at the HNR, ASM and the DNR, the cost for the lookup of the mapping tables at the HNR, ASM and the DNR, the cost for registration and update information at the HNR and ASM. In this model, we investigate the percentage overhead in the cost required for the operation of OMIPv6. The percentage is calculated by dividing the overheads of OMIPv6 protocol in total costs and can be expressed as

$$O_{overhead}\% = \frac{E(C_Q) + E(C_L) + E(C_R)}{E(C)} \times 100 = \left[1 - \frac{E(C_D)}{E(C)}\right] \times 100 \tag{13}$$

7. Performance Analysis

In this section, we first evaluate the performance of the devised OMIPv6 protocol based on the developed cost model, and then analyse the presented incentive mechanism for cooperation among selfish ARs.

7.1 The cost analysis of OMIPv6

The total cost for the operation of OMIPv6 and the overheads of the protocol are used as two key performance metrics to achieve this purpose. For the sake of specific illustration, we consider a typical case where some of parameter values are set similar to those adopted in the related studies [5, 10, 22]: 45×60 ARs are distributed uniformly in the grid manner over the network and each AS covers an average of 50 ARs; The DNR contains 10 domain names; Average distances in hops between the CH and DNR, between the CH and HNR, between the CH and ASM, between the HNR and DNR, between the HNR and ASM, between the MH and HNR, between the new attached HNR and previous HNR, between the MH and CH are set to be 35, 35, 35, 5, 5, 35, 5, and 80, respectively; Per hop transmission cost for query messages, registration and reply messages at the HNR, ASM and the DNR, and data Ack packets are set to be 0.6, and that for

data packet delivery is set to be 5.72; The cost for address configuration between the network layer and upper layer is set to be 0.2; Linear coefficients for lookup cost at the HNR, ASM and the DNR are 0.4, and that for IP routing table lookup cost is set to be 0.2; Processing costs for the registration at the HNR and ASM are set to be 30; An average of 3 retransmissions for the data/Ack packet delivery is taken into account.

Fig. 9 depicts the total cost of OMIPv6 protocol predicted by the cost model against the session arrival rate with 50, 100, and 150 packets in a session, the number of MHs is set to be 100000, and the subnet residence time is 5 seconds. As shown in the figure, the total cost required for the operation of OMIPv6 protocol increases for a larger value of session arrival rate. In addition, the increase of session length, $E(s)$, degrades the network performance as the total cost of OMIPv6 goes up. This is because increasing the session arrival rate and/or session length will ultimately lead to an increase in the volume of data packets and overheads (e.g., query messages, registration messages, and lookup messages) to be processed in the network.

Fig. 10 shows different costs (i.e., query cost, lookup cost, registration/update cost and data packet delivery cost) required for the operation of the OMIPv6 protocol against the number of MHs. As can be seen, the data packet delivery cost dominate the cost performance of OMIPv6, because it is the core part during the data communications. Moreover, as the number of MHs increases, the data packet delivery cost goes up because more data are sent by the MHs. To have a deeper understanding of the other cost (i.e., query cost, lookup cost and registration/update cost), Fig. 11 depicts them against the number of MHs. From this figure, we can find that the impact of registration/update cost is more significant than that of query cost and lookup cost. This is because the registration/update process happens more frequently than query and lookup process, especially when the number of MHs increases.

Fig. 12 depicts the percentage overhead of OMIPv6 obtained by the analytical cost model against the number of MHs with varying subnet residence time (i.e., 5, 10, and 15 seconds), the session arrival rate is set to be 0.05 and the session length is 50 packets. From the figure, we can find that a shorter stay in the coverage of AR will cause a higher overhead of the protocol, because the MH moves faster between ARs and produce more signaling overheads. Moreover, the overheads increase when the number of MHs is smaller than 3.0e4, in contrast, a smooth horizontal line in the overheads is shown in the figure as the number of MHs varies from 3.0e4 to 1.0e5. This is because as the number of MHs rise, the cost for data packet transmission will dominate the total cost required for the operation of OMIPv6.

7.2 The analysis of incentive mechanism for cooperation among selfish ARs

To have a deep understanding of the proposed incentive mechanism in Section 4.2.3, a quantity analysis will be presented. For the sake of specific illustration, C_f^+ and C_f^- (characterising the number of credits obtained by forwarding one unit data packet for newly-entered MHs and local MHs) are set to be 1 credit and 2 credits, and T_f (characterising the number of tokens paid by local MHs for sending one unit data packet) is set to be 1 token. In addition, 1 token can exchange for 1.5 credits. Fig. 13 depicts the annual profit of an AR against the data packets forwarded for newly-entered MHs and local MHs, respectively, per year per AR predicted by the incentive mechanism based on Eq. (2). From this figure, we can readily analyse the annual profit and deficit of each AR according to the amount of data packets forwarded and sent.

8. Conclusions

Based on the ID/Locator split architecture, this paper has developed a new operational mobility model over IPv6, called OMIPv6, with a distributed cloud mobility management system (D-CMMS) being mainly responsible for maintaining the ID and Locator mappings of mobile hosts, as well as providing the name resolution services to the mobile hosts. The D-CMMS has been designed in a hierarchical manner to relief the burden of domain-name resolvers, host-name resolvers and autonomous system managers. Moreover, a business model with billing strategies for OMIPv6 is presented to increase the profit of access routers and incent the selfish access routers to forward packets. Based on the designed mobility support solution, an analytical model has been proposed to calculate all possible costs including query cost, registration and update cost, and lookup cost at network entities, and the cost for data packet delivery in the operation of OMIPv6. Furthermore, we have derived the expression for the overheads of OMIPv6 protocol. To illustrate its applications, the analytical model has been adopted as a cost-effective tool to evaluate and analyse the performance of OMIPv6. In the future work, we will devise a smooth handoff scheme based on the OMIPv6 protocol to take into account the heavy burden caused by frequent update at D-CMMS.

References

[1] Y. Amir, C. Danilov, R. Musuăloiu-Elefteri, and N. Rivera. The SMesh Wireless Mesh Network. *ACM Trans. on Computer Systems* 2010; 28, Article No. 6.

[2] L. Buttyan and J.-P. Hubaux. Enforcing Service Availability in Mobile Adhoc WANs. in *proc. of First Annual Workshop on Mobile and Ad Hoc Networking and Computing (MobiHOC'00)* 2000; 87-96.

[3] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic. Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility *Future Generation Computer Systems* 2009; 25: 599-616.

[4] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil.Proxy Mobile IPv6. Request for Comments (RFC) 5213, Internet Engineering Task Force (IETF), 2008.

[5] M. S. Hossain, M. Atiquzzaman, and W. Ivancic. Cost Analysis of Mobility Entities of Hierarchical Mobile IPv6. in *proc. of IEEE Military Communications Conference (MILCOM)* 2010; 2280-2285.

[6] D. Johnson, C. Perkins, and J. Arkko.Mobility Support in IPv6. Request for Comments (RFC) 3775, Internet Engineering Task Force (IETF), 2004.

[7] V. P. Kafle, H. Otsuki, and M. Inoue. An ID/Locator Split Architecture for Future Networks. *IEEE Communications Magazine* 2010; 48: 138-144.

[8] J.-S. Kang and K. Okamura. Mobility Support through Locator/ID Split Architecture. in *proc. of 2011 International Conference on Information Networking (ICOIN'11)* 2011; 404-409.

[9] R. Koodli.Fast Handovers for Mobile IPv6. Request for Comments (RFC) 4068, Internet Engineering Task Force (IETF), 2005.

[10] J.-H. Lee, T. Ernst, and T.-M. Chung. Cost Analysis of IP Mobility Management Protocols for Consumer Mobile Devices. *IEEE Trans. on Consumer Electronics* 2010; 56: 1010-1017.

[11] J. Lee, W. Liao, and M. C. Chen. An Incentive-Based Fairness Mechanism for Multi-Hop Wireless Backhaul Networks with Selfish Nodes. *IEEE Trans. on Wireless Communications* 2008; 7: 697-704.

[12] Z. Liang, J. Zheng, S. Ma, S. Yang, B. Wang, and J. Liu. Modeling and Analysis of Queuing Effect on Mobile IPv6 Handoff Performance. in *proc. of IEEE International*

Symposium on Personal Indoor and Mobile Radio Communications (PIMRC) 2010; 2282-2287.

[13] C. Makaya and S. Pierre. An Analytical Framework for Performance Evaluation of IPv6-Based Mobility Management Protocols. *IEEE Trans. on Wireless Communications* 2008; 7: 972-983.

[14] A. d. l. Oliva, C. J. Bernardos, M. Calderon, T. Melia, and J. C. Zuniga. IP Flow Mobility: Smart Traffic Offload for Future Wireless Networks. *IEEE Communications Magazine* 2011; 49: 124-132.

[15] X. Pérez-Costa, M. Torrent-Moreno, and H. Hartenstein. A Performance Comparison of Mobile IPv6, Hierarchical Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination. *ACM SIGMOBILE Mobile Computing and Communications Review* 2003; 7: 5-19.

[16] J. Pan, R. Jain, S. Paul, and C. So-in. MILSA: A New Evolutionary Architecture for Scalability, Mobility, and Multihoming in the Future Internet. *IEEE Journal on Selected Areas in Communications* 2010; 28: 1344-1362.

[17] E. Perera, V. Sivaraman, and A. Seneviratne. Survey on Network Mobility Support. *SIGMOBILE Mobile Computing and Communications Review* 2004; 8: 7-19.

[18] C. Perkins.IP Mobility Support for IPv4. Request for Comments (RFC) 3344, Internet Engineering Task Force (IETF), 2002.

[19] C. So-In, R. Jain, S. Paul, and J. Pan. A Policy Oriented Multi-Interface Selection Framework for Mobile IPv6 Using the ID/Locator Split Concepts in the Next Generation Wireless Networks. in *proc. of 2nd International Conference on Computer and Automation Engineering (ICCAE'10)* 2010; 580-584.

[20] H. Soliman, C. Castelluccia, K. E. Malki, and L. Bellier.Hierarchical Mobile IPv6 Mobility Management (HMIPv6). Request for Comments (RFC) 4140, Internet Engineering Task Force (IETF), 2005.

[21] G. Wood. IPv6: Making Room for the World on the Future Internet *IEEE Internet Computing* 2011; 15: 88-89.

[22] J. Xie and I. F. Akyildiz. A Novel Distributed Dynamic Location Management Scheme for Minimizing Signaling Costs in Mobile IP *IEEE Trans. on Mobile Computing* 2002; 1: 163-175.

[23] S. Zhong, J. Chen, and Y. R. Yang. Sprite: A Simple, Cheat-proof, Credit-based System for Mobile Ad Hoc Networks. in *proc. of 22nd Annual Joint Conference of the IEEE Computer and Communications (INFOCOM'03)* 2003; 1987-1997.

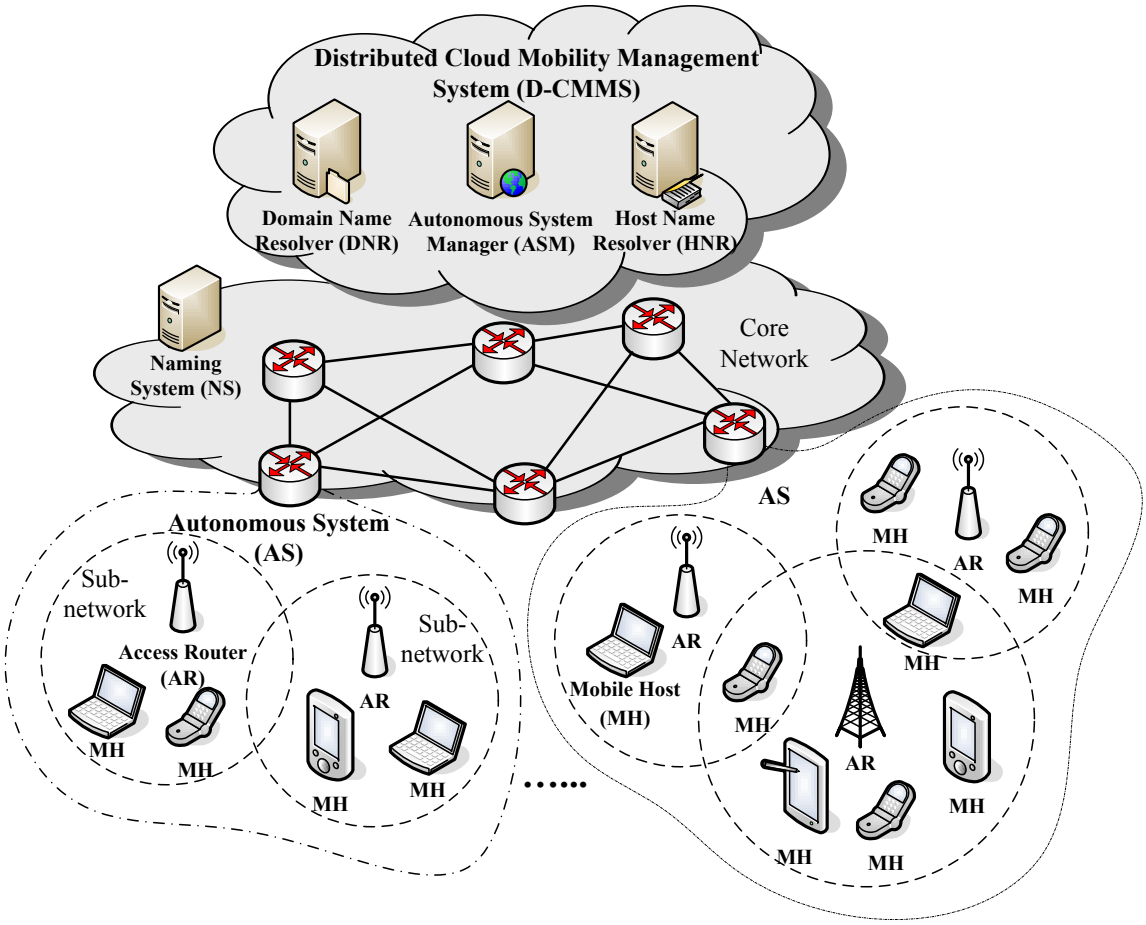

Figure 1: The architecture of OMIPv6

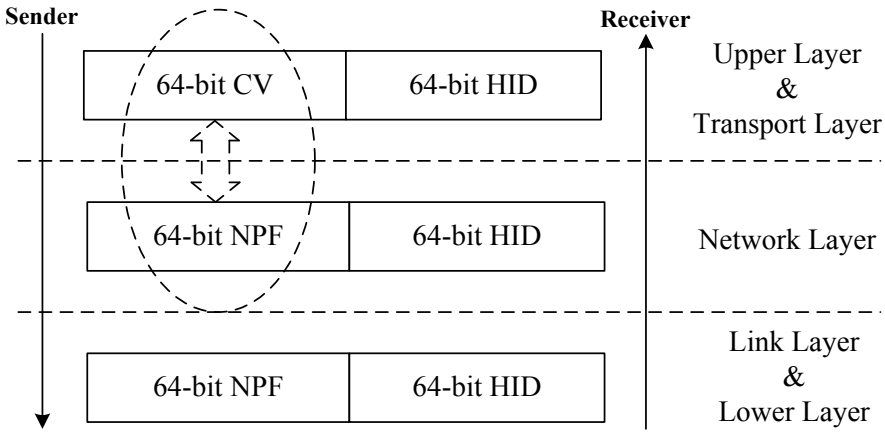

Figure 2: Address architecture and its configuration

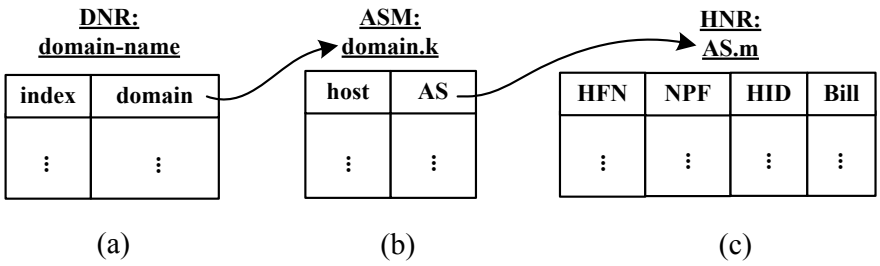

Figure 3: The mapping tables stored in (a) DNR, (b) ASM, and (c) HNR, where k and m denote the number of domain names and the number of ASs

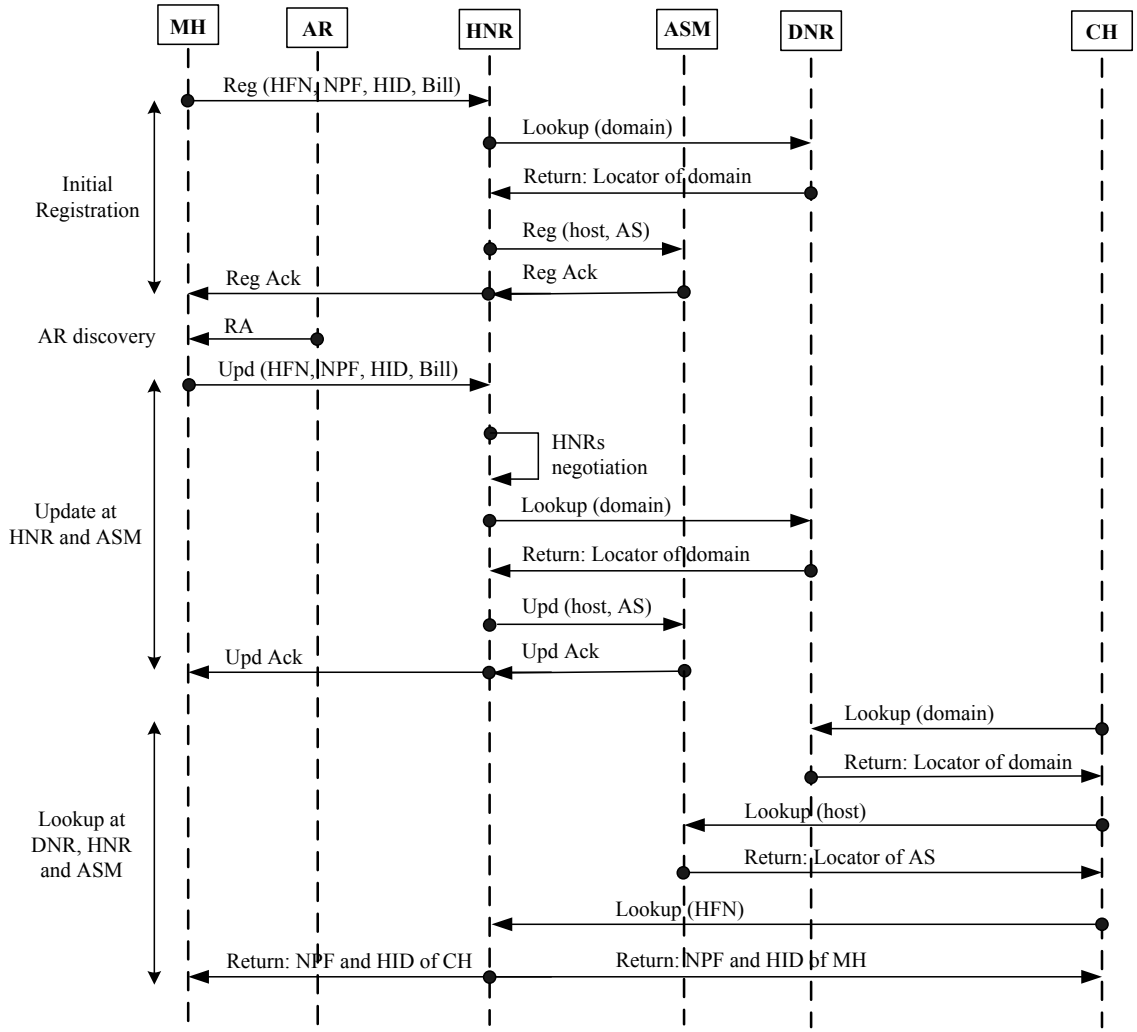

Figure 4: Sequence of message flow control in OMIPv6

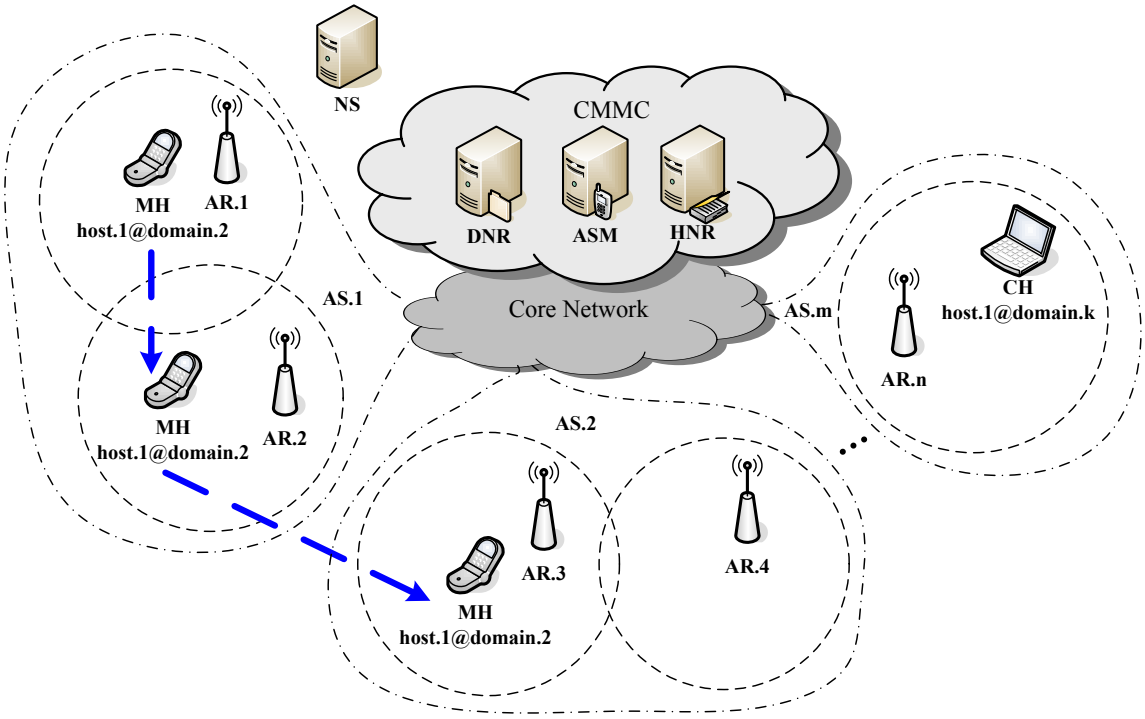

Figure 5: Typical scenarios of OMIPv6 operation for the case study

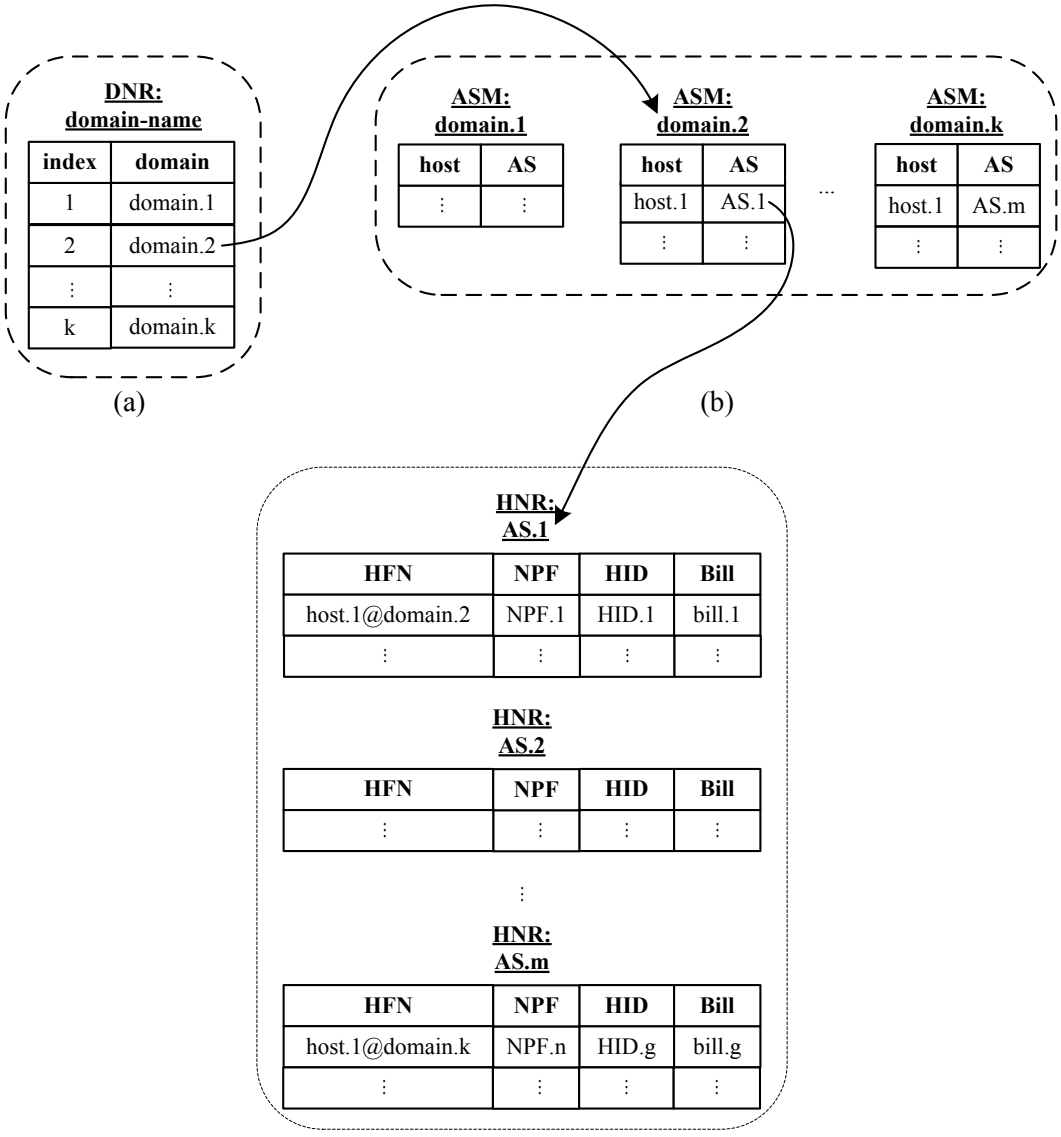

Figure 6: The mapping tables stored in (a) DHR:domain-name, (b) ASM:domain.2 and ASM:domain.k, and (c) HNR:AS.1 and HNR:AS.m, where n and g denote the number of ARs and the number of MHs

HNR:
AS.1

HFN	NPF	HID	Bill
host.1@domain.2	NPF.2	HID.1	bill.1

Figure 7: The mapping table stored in HNR:AS.1 under scenario 2).

ASM: domain.2

host	AS
host.1	AS.2

(a)

HNR: AS.1

HFN	NPF	HID	Bill
~~host.1@domain.2~~	~~NPF.2~~	~~HID.1~~	~~bill.1~~

HNR: AS.2

HFN	NPF	HID	Bill
host.1@domain.2	NPF.3	HID.1	bill.1

(b)

Figure 8: The mapping tables stored in (a) ASM:domain.2, and (b) HNR:AS.1 and HNR:AS.2 under scenario 3).

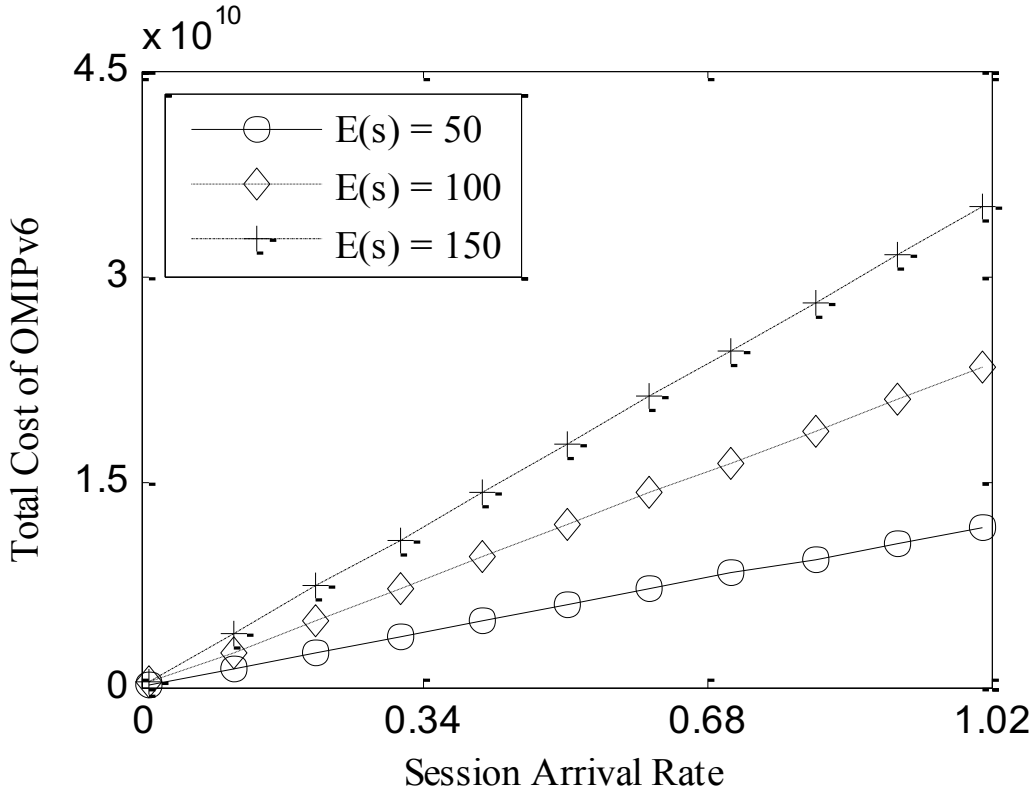

Figure 9: Total cost of OMIPv6 predicated by the analytical cost model with varying mean session length in packets

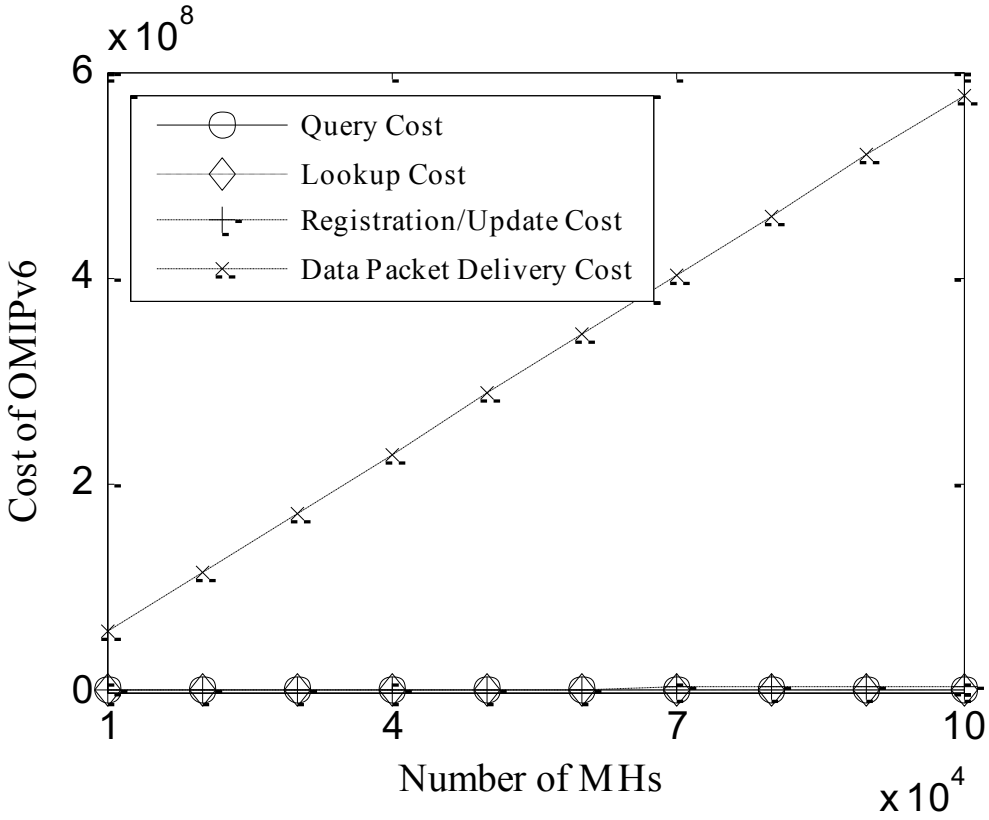

Figure 10: The comparison of query cost, lookup cost, registration/update cost, and data packet delivery cost for the operation of OMIPv6 predicated by the analytical cost model

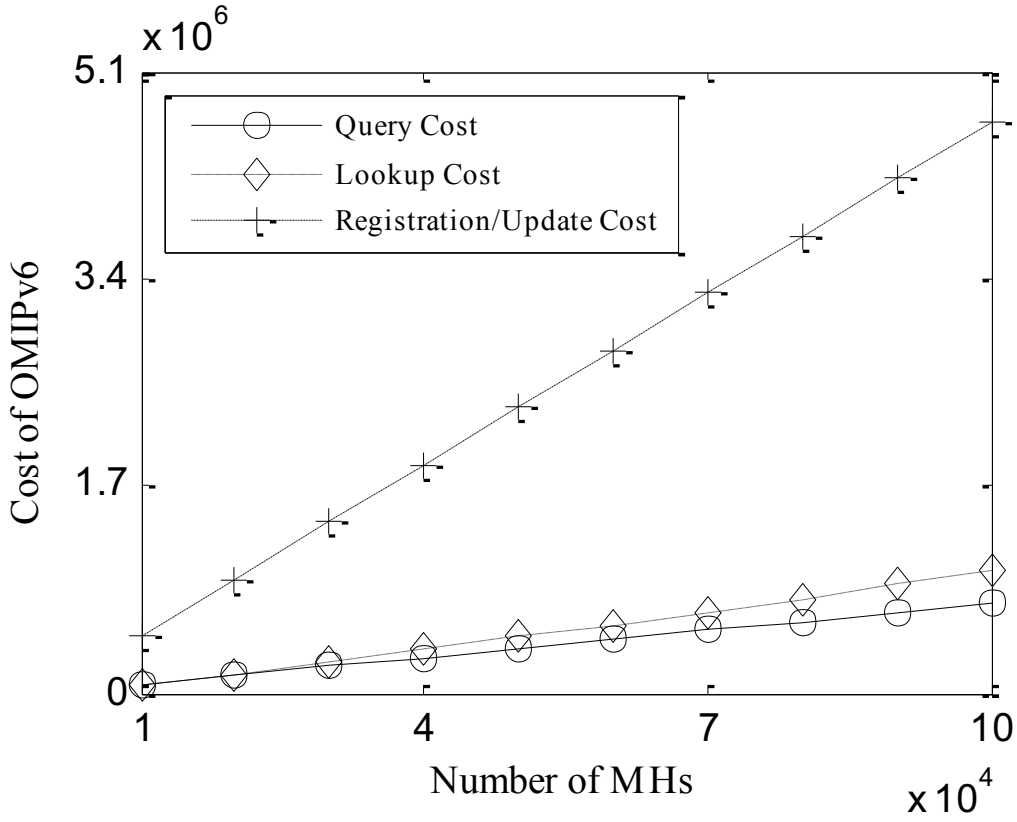

Figure 11: The comparison of query cost, lookup cost, and registration/update cost for the operation of OMIPv6 predicated by the analytical cost model

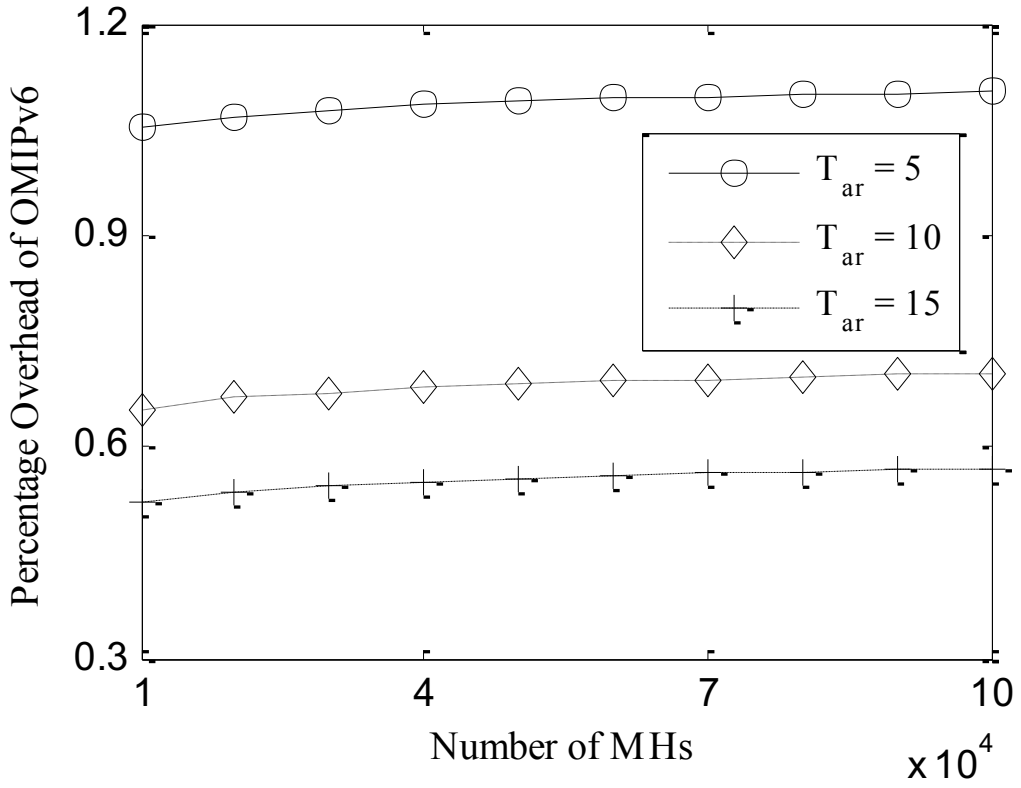

Figure 12: Percentage overhead of OMIPv6 predicated by the analytical cost model with varying subnet residence time

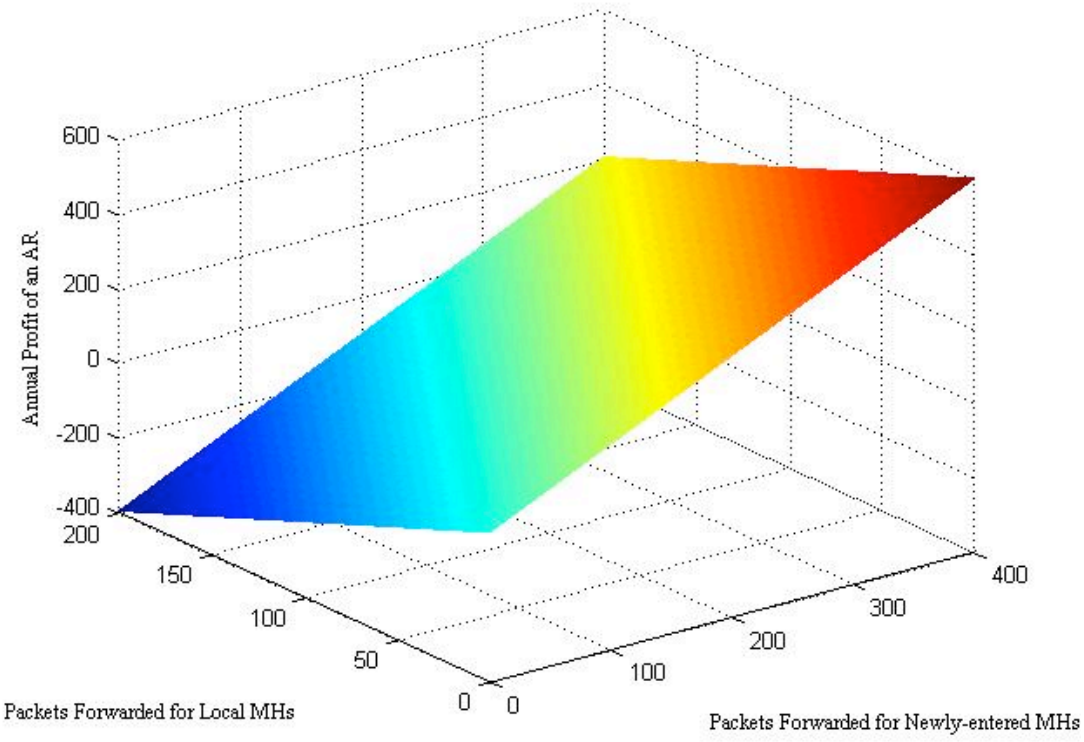

Figure 13: Annual profit/deficit of an access router against the data packets forwarded for newly-entered MHs and local MHs predicted by the incentive mechanism