Enhancement of Return Routability Mechanism for Optimized-NEMO Using Correspondent Firewall

Samer Sami Hasan and Rosilah Hassan

Network Mobility (NEMO) handles mobility of multiple nodes in an aggregate manner as a mobile network. The standard NEMO suffers from a number of limitations, such as inefficient routing and increased handoff latency. Most previous studies attempting to solve such problems have imposed an extra signaling load and/or modified the functionalities of the main entities. In this paper, we propose a more secure and lightweight route optimization (RO) mechanism based on exploiting the firewall in performing the RO services on behalf of the correspondent nodes (CNs). The proposed mechanism provides secure communications by making an authorized decision about the mobile router (MR) home of address, MR care of address, and the complete mobile network prefixes underneath the MR. In addition, it reduces the total signaling required for NEMO handoffs, especially when the number of mobile network nodes and/or CNs is increased. Moreover, our proposed mechanism can be easily deployed without modifying the mobility protocol stack of CNs. A thorough analytical model and network simulator (Ns-2) are used for evaluating the performance of the proposed mechanism compared with NEMO basic support protocol and state-of-the-art RO schemes. Numerical and simulation results demonstrate that our proposed mechanism outperforms other RO schemes in terms of handoff latency and total signaling load on wired and wireless links.

Keywords: Network Mobility, Return Routability Procedure, firewall, route optimization.

Manuscript received Dec. 23, 2011; revised July 11, 2012; accepted July 23, 2012.

Samer Sami Hasan (phone: +60 178461374, iirraaqqii@yahoo.com) and Rosilah Hassan (rosilah@ftsm.ukm.my) are with the Department of Computer Science, Universiti Kebangsaan Malaysia, Selangor, Malaysia.

http://dx.doi.org/10.4218/etrij.13.0111.0804

I. Introduction

Ubiquitous mobile devices and services are widely proliferated. The surge in cellular communication reflects user interest in mobile accessibility. However, these networks should provide not only voice services but also data services for the mobile entity across heterogeneous environments. Internet protocol (IP) is the basis for these networks' continuous Internet connectivity.

Users, via IP layers, can access the Internet from anywhere, at any time. The Internet Engineering Task Force (IETF) for mobile IPs supports the movement of the IP node from one point of attachment to another by supporting mobile IP (MIP) [1] for IPv4 and MIPv6, to support mobility in the IPv6 node [2]. The MIPv6 protocol was proposed to support host mobility. Each mobile node (MN) requires two types of IPv6 addresses. One is home of address (HoA), which is acquired from the home link; the other is care of address (CoA), which is acquired from the foreign access router to maintain global connectivity and accessibility. This mobility can be achieved by registering the CoA with the home agent (HA) at the home link. The MIPv6 protocol allows the packets to reach the destined MN transparently through the HA. This protocol suffers from pinball problems while routing the packets from the MN to the correspondent node (CN) because the packets are always tunneled through the HA in the home link. Route optimization (RO) is used to enhance network performance by making a direct connection between the MN and the CN, thus bypassing the HA [3]. This provides an optimal path between the MN and the CN. Currently, the MN uses a mechanism known as the Return Routability Procedure (RRP). This mechanism allows the CN to verify and assure that the collection of the MN's HoA and CoA is owned by the

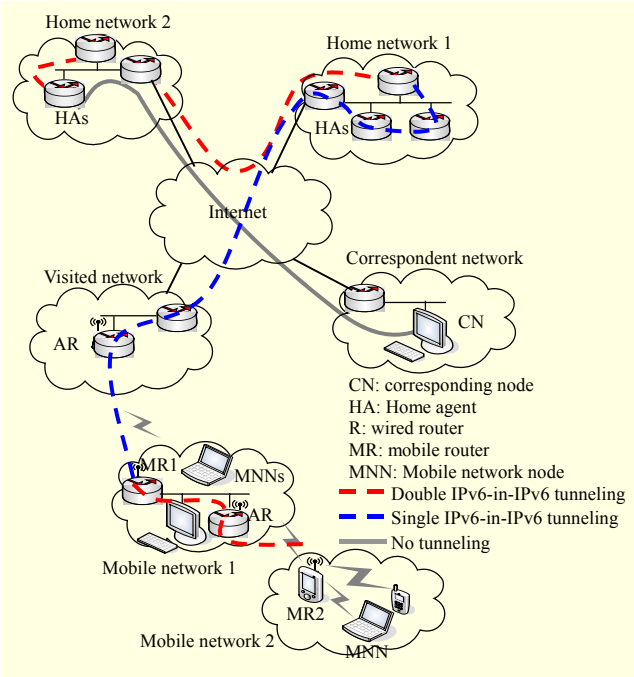

Fig. 1. Architecture of NEMO showing suboptimal path in nested NEMO.

MN. Next, the MN and CN implement the RO. With its optimization, the MIPv6 protocol is satisfactory for host mobility but not for a group of nodes moving as a single unit (similar to a PAN and vehicle network) attached to the Internet through its egress interface.

The IETF has developed a new protocol for network mobility known as Network Mobility basic support protocol (NEMO bsp) [4]. The NEMO bsp extension ensures session continuity for each MN (supported by MIPv6) or fixed node (not sophisticated enough to support MIPv6) inside the mobile network. NEMO handles network traffic as a central point of management and provides reachability and connectivity for each node within its network during its movement. In a NEMO network, units are attached and moved to different points in the Internet via a specific gateway known as the mobile router (MR). This MR has two virtual interfaces [5]: one is the egress interface that connects with the Internet in the home or via a foreign link, and the other is the ingress interface that connects with the whole node underneath the MR for both fixed nodes and MNs. Each MR has its own HA at its home link. Each packet that is designated by the MR at the home link can be reached by the HoA acquired from the HA when the MR is moved and attached to a new arbitrary access point. First, the MR acquires a new address from the foreign access router (AR), that is, the CoA. Second, it delegates a new prefix or set of prefixes (PFs) from the access router. Finally, the MR registers the CoA and, optionally, the delegated PFs with their corresponding HA by sending a binding update (BU) message containing all NEMO features [4]. When a packet is designated, one of the mobile network nodes (MNNs) inside the MR path of the routed packet is CN → HA-MNN→ HA-MR2 → HA-MR1 → MR1→ MR2→ MNN, as shown in Fig. 1.

NEMO allows the creation of "nested networks," wherein a mobile network attaches to another mobile network to gain arbitrary depth. However, for each level of nesting, traffic is encapsulated and tunneled to reach the destination. This leads to increased overhead (encapsulation) and to suboptimal paths (tunneling without consideration for actual network topology) [6].

This NEMO bsp suffers from a suboptimal pathway in using multiple tunnels through multiple HAs of the mobile networks, thus resulting in several encapsulations. NEMO-RO is similar to that adopted by MIPv6-RO. MIPv6 runs the RRP to initiate RO. MIPv6-RRP is inadequate because it does not support the link prefix or verify whether it is in fact handled by the mobile entity inside the NEMO.

II. Overview of RRP

The return routability (RR) is a mechanism that authorizes registrations between the CN and the MN via a cryptographic token (that is, a number supplied by the CN to enable the MN to complete the necessary binding management key for BU authorization) exchange [2]. This can be accomplished by verifying that the payloads addressed to the collection of the two claimed addresses are not routed to a false node. MIPv6 runs the RRP to initiate RO. Different approaches have been proposed to address the problem of RO in NEMO networks. For instance, NEst Route Optimization for NEMO (NERON) [7] offers a mechanism that aims to solve pinball routing, race condition, and loop formation issues in nested mobile networks. NERON enables direct intercommunication of packets between two MNNs residing inside the same NEMO domain but in different subnets, without the data packets leaving the NEMO only to be tunneled back. However, in the case of RO between the MNN in nested NEMO and CN, RO returns to the standard NEMO RRP with all the inefficiencies described in section I but remains independent of the nest depth. On the other hand, approaches such as the MIPv6-based RO (MIRON) [8], protocol for carrying authentication for network access (PANA), and dynamic host configuration protocol for IPv6 (DHCPv6) are used by the MNN to obtain a CoA from the foreign network as the MNN moves. MIRON allows the visited MNN to manage its own mobility; additionally, MIRON enables each visited MNN to perform RO with CNs by performing the PANA and DHCPv6 with MIPv6-RRP. This imposition makes the MIRON more complex in the MR and the visited MNN more complicated to be deployed. In NEMO

RO, no scheme exists that suits all mobility scenarios and characteristics [9]. Therefore, in the case of a large number of CNs, peer MNNs, and/or a large number of PFs inside NEMO, our proposed mechanism produces better performance than other schemes.

The following is a list of steps for the original RRP.

1) The MN sends a test message to the CN to verify if the CN is able to supply a proof. This is determined by passing the home of test initiate (HoTi) to the HA, where the source is the HoA.
2) Next, the HA passes the test message to the CN.
3) The CN then generates a cryptographic token for the HoTi message according to the HoTi flags and parameters (similar to cookies).
4) After the MN sends the HoTi, the MN will send a care of test initiate (CoTi) message to the CN where the source address is the CoA.
5) The CN also generates a cryptographic token for the CoTi.
6) Next, the CN sends back the home of test (HoT) for the HoTi through the HA and care of test (CoT) for the CoTi.
7) The RRP is completed once the MN has received both the HoT and the CoT and sends the BU to the CN with its kbm key (the kbm is the concatenation of the home key token with a care of key token), as shown in Fig. 2.
8) An optimized channel is opened between the CN and the MN after the binding acknowledgment (BA) message is received.

1. Weakness of Existing RRP

The original RRP, when adapted to network mobility, mainly suffers from not supporting the prefixes in the RRP shacking procedure, which leads to a lack in security. The mobile network prefixes (MNPs) option may be under attack by the change or insert options. This attack will lead to the CN sending data meant for the MR to false networks. Likewise, the RRP incurs additional signaling over bandwidth in limited wireless and wired channels. This scenario contradicts one of the initial objectives of NEMO as a scheme to reduce signaling over channels. Moreover, the amount for signaling is likely to increase with the increasing number of MNNs and/or CNs and may be amplified with the nesting of mobile networks. Such signaling may scale to unacceptable heights, especially to the resource-scarce MN, which typically has limited power, memory, and processing capacity.

III. New Firewall-RRP for NEMO

This proposed RR mechanism provides a level of security similar to that of the IPv4, by means of reusing the MIPv6

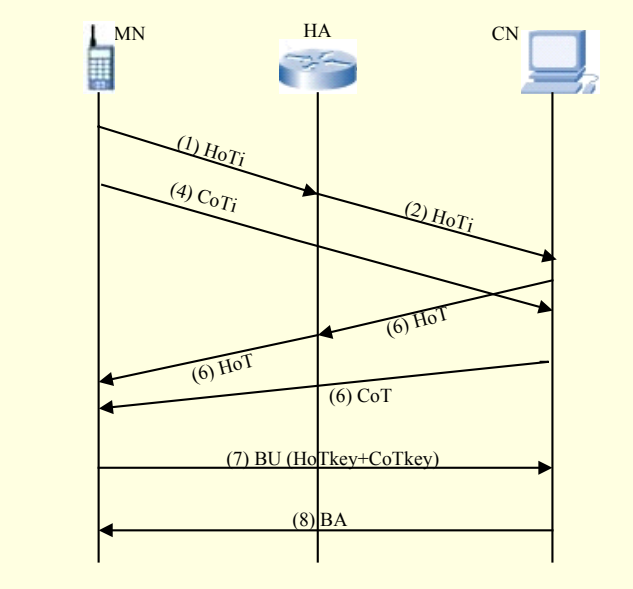

Fig. 2. Message sequence diagram for RRP.

security concepts and using a cryptographic key to generate a crypto address [10] in-line with firewall and NEMO environments. In this enhanced RRP, the MR can extend the HoTi message to include one or more selected numbers of the network prefixes underneath the MR. Following this new mechanism, the MR will first check whether its own listed prefixes are able to provide the RO. This verification will occur depending on the flag bit added to the mobile header by the MN, to inform the MR if the MNN is sophisticated enough for the RO. This flag is called the "z" flag. When the flag is set to "on," it means that the MNN is sophisticated enough for the RO; otherwise, the flag is set to "off." This flag is added to the MR prefixes list for verification purposes. The MR will send the extended mobility header with a list of prefixes that are able to function under the RO to the HA_MR using the HoTi message.

On the other side of the network, the modified firewall [11] protects either the CN or the corresponding router (CR) in the correspondent network. Various types of firewalls are in use [12], [13]. Independent of the adopted methods, firewalls generally consider five parameters of the arriving messages (source IP address, destination IP address, protocol type, source port number, and destination port number). Based on these five parameters, packets are dropped or passed through a firewall [14]. The MIPv6 firewall should consider newly developed stateful filtering rules that allow the packets destined to or from the HA or MNN to pass to or from the CN network, without filtering the data messages and the signaling, thus passing through in accordance with the problems noted in a previous study [15]. This firewall will be supported by the RR proposed mechanism for NEMO, to provide a NEMO-RO without any

modification on the CN's entities. In addition, RO using this scenario can be easily maintained, even though the CN is not sophisticated enough to support the RO without adding new entities to the infrastructure [16]. Most Internet infrastructures today are client/servers operating under tiered client/server systems. Therefore, most of the CNs may work as servers under heavy traffic conditions. This construct causes major difficulties in updating or modifying throughout various CNs. In the firewalled network, where the CN is easy to "plug and play," applying modifications to a firewall is more reliable and scalable than trying to modify the CN.

When the HA_MR receives the HoTi from the MR, as shown in Fig. 3, the HoTi will be processed and forwarded to the firewall with the following header options [17]:

```
IPv6 Header {
        Source = home address of mobile router
        Destination = correspondent node
        }
        Mobility Header {
            MH Type = Home Test Init
            Home Init Cookie = random value
            Flag R //new extended (allowing the firewall to work in
              both modes original and extended)
            Mobile Network Prefix Option {
                Prefix Length = length of prefix
                List of Selected Mobile Network Prefixes =
                prefixes of the mobile network // new extended
                header.
        }
}
```

As shown in Fig. 4, the MR will simultaneously send the CoTi message to the modified firewall with the header option below; this message is similar to the original CoTi message obtained by the original MIPv6 RRP:

```
IPv6 Header {
        Source = care-of address of mobile router
        Destination = correspondent node
        }
        Mobility Header {
        MH Type = Care-of Test Init
        Care-of Init Cookie = random value }
```

Then, the firewall will operate as a CN agent to generate cryptographic tokens for the HoA and the entire prefix sent by the HA_MR in the HoTi message. This operation is performed as illustrated below. A cryptographic token is also generated for the CoTi, and the CoT message is returned directly to the MR.

- HoA key token generation:
  First (64, HMAC_SHA1 ($K_{firewall}$, HoA|nonce|0)) //represent the first 64 bits in Hashing message authentication code based on SHA1 algorithm and use K to the key function to operate with options. "0" represents HoA.
- CoA key token generation:
  First (64, HMAC_SHA1 ($K_{firewall}$, CoA|nonce|1))
- $MNP_{(s)}$ key $token_{(s)}$ generation:
  First (64, HMAC_SHA1 ($K_{firewall}$, $MNP_{(s)}$ |$nonce_{(s)}$ |0))

When the firewall finishes verifying tokens for each PF, it will cache these tokens into a cached list. This list is a record of network prefixes with tokens generated for each one. The cost required for these processes is very small, as described in [18]. The firewall will collect this list and create the new extended HoT (xHoT) message with the headers illustrated below:

```
xHoT header option:
IPv6 Header {
        Source = Destination of HoTi
        Destination = Source of HoTi
        }
        Mobility Header {
        MH Type = 3
        Home Init Cookie = copy from HoTi cookie
        Key of Home = Hashed key for HoA
        Flag R
        Mobile Network Prefix Option (1) {
        Prefix option
        Prefix Length = MNP (1) length
        MNP (1) _key_message}
        Mobile Network Prefix Option (2) {
        Prefix option
        Prefix Length = MNP (2) length
        MNP (2) _key_message}
            .
            .
            .
        Mobile Network Prefix Option (n) {
        Prefix option
        Prefix Length = MNP (n) length
        MNP (n) _key_message} // (n) is represent the Max number of
        MNPs in received HoTi list
        }
```

Next, the firewall will send the xHoT message to the HA_MR to pass to the MR. This operation, which occurs in the firewall, will reduce the load on the wireless bandwidth by eliminating messages sent to the MR (that is, MNP_Key_messages for each prefix) within the limitation of the wireless channel between the AR and the MR. Finally, after the MR receives the xHoT and CoT, the MR is positioned to generate a binding management key (Kbm). This operation is performed as follows:

Kbm = SHA1 (HoA keygen token | CoA keygen token | MNP(s) token(s)).

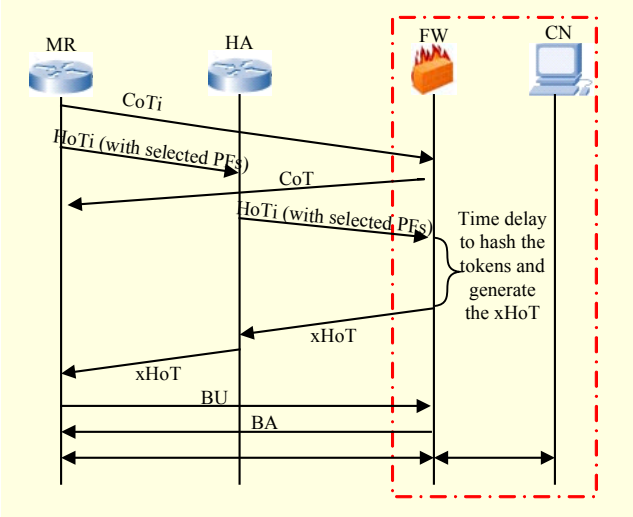

Fig. 3. Message exchange with firewall environments.

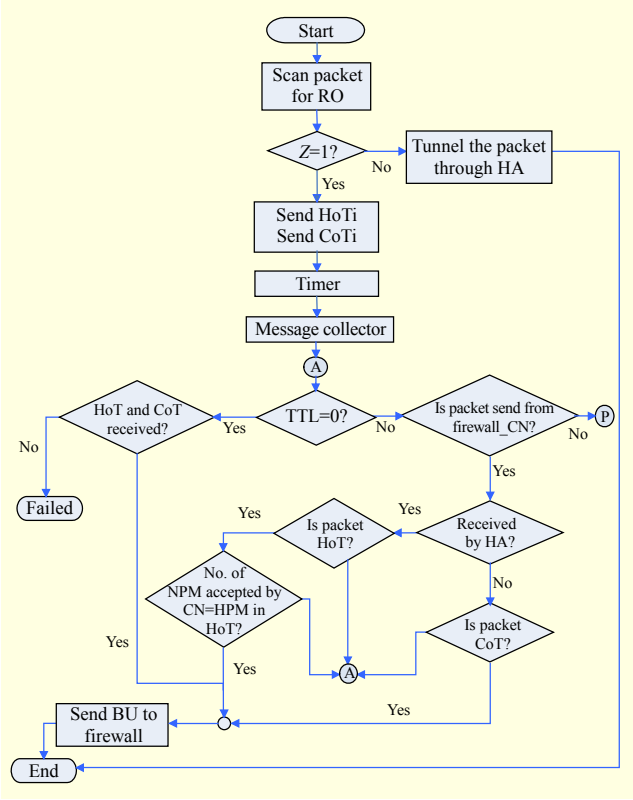

Fig. 4. Mobile router packet flow.

Next, the MR will send the BU message with Kbm and the mobility options header to the modified firewall as follows:

Auth_Data = First (96, MAC (Kbm, Mobility options)),

where the Mobility options are as follows:

Mobility options = CoA | Final Destination | Mobility header type | Flags.

Consequently, a direct channel is opened between the MR and the CN through the attached firewall.

NEMO signaling rules are always generated as a pair of messages (that is, HoTi/HoT, CoTi/CoT, or BU/BA), as illustrated above. The firewall should establish filter rules to allow these messages to pass through. The firewall should also establish the MIPv6 mobility header options described in [2]. These new rules are added to the firewall frame, as shown in Fig. 5, to allow both the data packets and signaling packets to pass through.

The transmission flow between the CN to/from the firewall is started when an incoming packet received from the IP address of the MR is designated to the IP address of the CN attached to the firewall. The firewall must trace the incoming IP header to check the packet type once received. The firewall checks the mobility header and the HoA option. If the incoming packet does not include either, then the firewall will forward the incoming packet without any update, depending on the normal routing policy. If the incoming packet includes the HoA option but not the mobility options, then the firewall recognizes the message as one that does not belong to the mobility signaling messages. The firewall should then check its firewall RO cache table (FWROCache) that depends on the HoA and source and destination address of the received packet. The existence of this entry in the FWROCache indicates that RO exists between the two nodes. The firewall then replaces the source address (MR CoA) from the received packet with the MR HoA, removes the HoA option from the packet, and sends the packet directly to the corresponding entity behind this firewall.

From the other side, the outgoing packet from the CN that is attached to the firewall is sent to the MR. The firewall receives the packet from the CN, then checks its FWROCache table using the source and destination addresses of the packet. If an entry does not exist, then the packet is forwarded through the home agent of the destination address without RO. If the cache entry exists, the firewall uses the type 2 header option to route the packet to the designated address with the cache entry information.

IV. Performance Evaluation

In this section, the superiority of the proposed RO is shown by analyzing and implementing its efficiency in solving NEMO problems with a large number of prefixes and CNs.

1. Analytical Model

In this section, we develop an analytical model for the NEMO bsp based on RO. The network topology considered for analysis is illustrated in Fig 6. For simplicity, we consider the same number of hops ($d_{x\text{-}y}$) between connected entities.

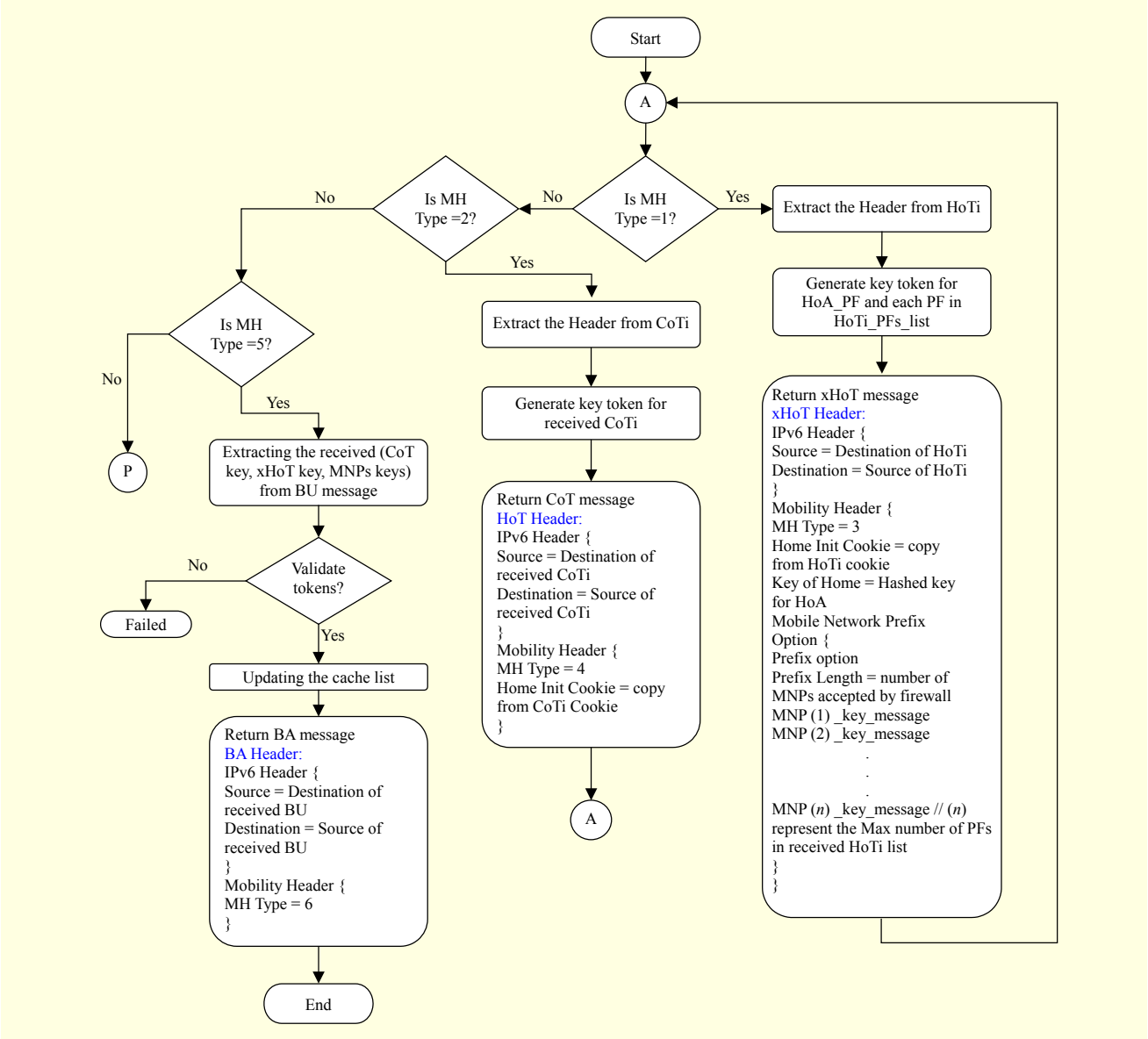

Fig. 5. Modified firewall with new filtering rules.

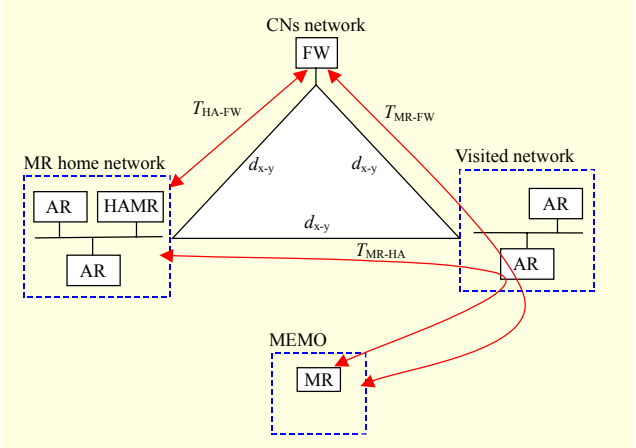

Fig. 6. Network model for numerical analysis.

Moreover, all costs are deemed symmetric, that is, $T_{\text{MR-HA}} = T_{\text{HA-MR}}$.

For NEMO bsp, the handoff latency is derived by

$$h_{\text{NEMO}} = t_{\text{L2}} + t_{\text{RD}} + t_{\text{DAD}} + t_{\text{r}} + t_{\text{RR}}, \quad (1)$$

where t_{L2} is the link layer switching delay, t_{RD} is the round-trip delay for router discovery, t_{DAD} is the delay for the duplicate address detection procedure, and t_{r} is the MR CoA registration time with its HA, which is calculated as

$$t_{\text{r}} = \left(T^{\text{BU}}_{\text{MR-HAMR}} + BU_{\text{proc}} + T^{\text{BA}}_{\text{HAMR-MR}} + BA_{\text{proc}}\right). \quad (2)$$

The one-way transmission delay (T^{Z}_{X-Y}) between nodes X and Y over wired and wireless links depends on packet size (p), link delay ($\lambda_{\text{wireless}}, \lambda_{\text{wired}}$), bandwidths ($R_{\text{wireless}}, R_{\text{wired}}$), the

probability of wireless link failure (β), the number of hops between X and Y (d_{X-Y}), and the queuing delay at each router hop (D_{queue}) [19]:

$$T_{X-Y}^{Z}(p)=\frac{1-\beta}{1+\beta}\left[\frac{p}{R_{\text{wireless}}}+\lambda_{\text{wireless}}\right] +(d_{X-Y}-1)\left[\frac{p}{R_{\text{wired}}}+\lambda_{\text{wired}}+D_{\text{queue}}\right]. \quad (3)$$

The delay for the NEMO return routability procedure is calculated as follows:

$$\begin{aligned} t_{\text{RR}}^{\text{NEMO}} = \text{Max}[&(T_{\text{MR-CN}}^{\text{CoTi}}+CoT_{\text{proc}}+T_{\text{CN-MR}}^{\text{CoT}}),\\ &(T_{\text{MR-HAMR}}^{\text{explicitHoTi}}+HoTi_{\text{proc}}^{\text{HAMR}}+T_{\text{HAMR-CN}}^{\text{explicitHoTi}}\\ &+2NPT_{\text{proc}}+T_{\text{CN-HAMR}}^{\text{NPT}}+T_{\text{HANR-MR}}^{\text{NPT}}(n+1))]\\ &+(T_{\text{MR-CN}}^{\text{BU}}+BU_{\text{proc}}+T_{\text{CN-MR}}^{\text{BA}}+BA_{\text{proc}}). \end{aligned} \quad (4)$$

In cases in which the mobility scenario contains a large number of CNs, then the RR delay for NEMO is calculated as

$$t_{\text{RR}}=t_{\text{RR}}^{\text{NEMO}}\cdot N_c. \quad (5)$$

In (2), the symbol n represents the number of prefixes received from the MR and is added by one of the HoA tokens, whereas $X_{\text{proc}}=\alpha \log(n+1)$ represents the processing cost as a function of network prefixes. NPT represents the network prefix test message sent from the CN to the HA_MR for each PF in the HoTi list. The RR delay in our proposed mechanism is calculated as follows:

$$\begin{aligned} t_{\text{RR}}^{\text{Enhanced}} = \text{Max}[&(T_{\text{MR-FW}}^{\text{CoTi}}+CoT_{\text{proc}}+T_{\text{FW-MR}}^{\text{CoT}}),\\ &(T_{\text{MR-HAMR}}^{\text{explicitHoTi}}+HoTi_{\text{proc}}^{\text{HAMR}}+T_{\text{HAMR-FW}}^{\text{explicitHoTi}}\\ &+xHoT_{\text{proc}}^{\text{FW}}+T_{\text{FW-HAMR}}^{x\text{HoT}}+T_{\text{HAMR-MR}}^{x\text{HoT}})]\\ &+\left(T_{\text{MR-FW}}^{\text{BU}}+BU_{\text{proc}}+T_{\text{FW-MR}}^{\text{BA}}+BA_{\text{proc}}\right). \end{aligned} \quad (6)$$

Based on (6), the global signaling during handoff is reduced, which results in shorter handoff delays. In addition, this formula reduces the bandwidth load between AR-MR and FW-HA_MR such that if the RRP uses the original HoT message instead of the extended message for each prefix in the MR, the result will be performance degradation, especially when the number of mobile entities is increased inside the MR. Furthermore, in this proposed scheme, increasing N_c does not cause a signaling storm problem during handoffs, due to the firewall's new functionality. The enhanced RO handoff delay is calculated as

$$h_{\text{EnnacedRO}}=t_{\text{L2}}+t_{\text{RD}}+t_{\text{DAD}}+t_{\text{r}}+t_{\text{RR}}^{\text{Enhanced}}+2nT_{\text{MNN-MR}}. \quad (7)$$

The handoff delay in MIRON might suffer from binding update storm problems during handoff. Thus, the MR should notify each MNN to obtain a CoA from the MR prefixes using PANA and DHCP to inform the MNNs-HA and CNs of its current address after each handoff. Therefore, MIRON has more signaling than NEMO. The formula for MIRON total handoff delay is written in [9]:

$$\begin{aligned} h_{\text{MIRON}} &= t_{\text{L2}}^{\text{MR}}+t_{\text{RD}}^{\text{MR}}+t_{\text{DAD}}^{\text{MR}}\\ &\quad +n(4T_{\text{MNN-MR}}^{\text{PANA}}+2T_{\text{MNN-MR}}^{\text{DHCPv6}}+t_{\text{r}}+t_{\text{RR}}^{\text{MIPv6}}\cdot N_c), \end{aligned} \quad (8)$$

where

$$\begin{aligned} t_{\text{RR}}^{\text{MIPv6}} = \text{Max}\ &[(T_{\text{MNN-CN}}^{\text{CoTi}}+CoT_{\text{proc}}+T_{\text{CN-MNN}}^{\text{CoT}}),\\ &(T_{\text{MNN-HAMNN}}^{\text{implicitHoTi}}+HoTi_{\text{proc}}^{\text{HAMNN}}+T_{\text{HAMNN-CN}}^{\text{implicitHoTi}}\\ &+(2HoT_{\text{proc}}+T_{\text{CN-HAMNN}}^{\text{HoT}}+T_{\text{HAMNN-MNN}}^{\text{HoT}}))]\\ &+(T_{\text{MR-CN}}^{\text{BU}}+BU_{\text{proc}}+T_{\text{CN-MR}}^{\text{BA}}+BA_{\text{proc}}). \end{aligned} \quad (9)$$

NERON supports optimization by using the legacy NEMO-prescribed RR process as the base for its RO process. NERON also supports optimization between nested entities inside NEMO without tunneling through HAs and merely depends on the discovery of PFs through a route notification message. The NERON RO mechanism incurs a similar effect on handoff signaling as the NEMO bsp. The bit difference is due to the new header option added to the router advertisement message, called "the mobile network gateway option," with 20 bytes and a nest gate option added to the BU message in a format similar to that of the alternative CoA. Accordingly, the NERON handoff delay (considering that the new size of the control messages consumes delay as ω) can be calculated as

$$h_{\text{NERON}}=h_{\text{NEMO}}+\omega. \quad (10)$$

The total handoff delay is depicted in Fig. 7 as a function of MR link prefixes (n). We observe that total handoff delay increases proportionally with n, for all schemes. However, the enhanced mechanism is significantly less affected by the increasing of n due to the reduction of burst signaling, while both NEMO bsp and NERON have the same effects. MIRON is depicted as being highly affected by increasing n due to additional signaling for each MNN. Similar analysis is performed for RR delay in comparing with n, but with increasing number of CNs (N_c), as shown in Fig. 8. The MR needs to send binding updates to all the CNs of the MNNs served by the MR. This burst of RR signaling messages leads to an increase in the total RR delay for all schemes, unlike in the new mechanism, which is significantly less affected.

The results in Figs. 9 and 10 illustrate the impact of the wired and wireless link delay on the RR delay. In Fig. 9, the RR delay is calculated by changing the wired link delay between the communicating entities. The respective RR delay for NEMO, NERON, and MIRON is significantly increased with the

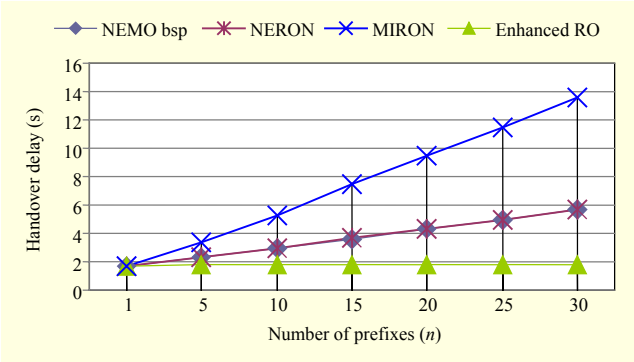

Fig. 7. Effect of MNPs on total handoff delay.

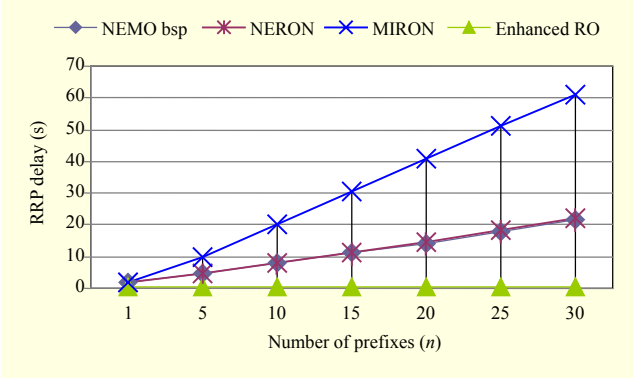

Fig. 8. Effect of MNPs on RR delay with N_C=5.

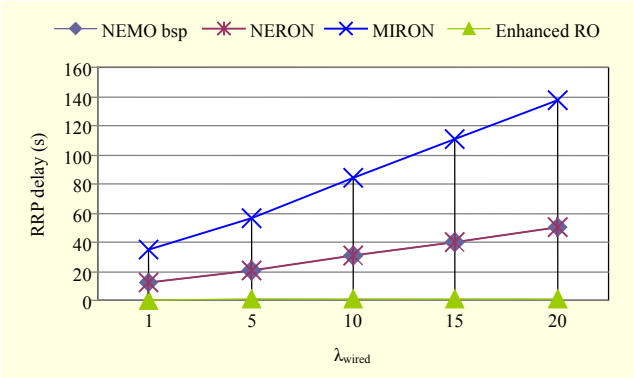

Fig. 9. Effect of λ_{wired} on RR delay.

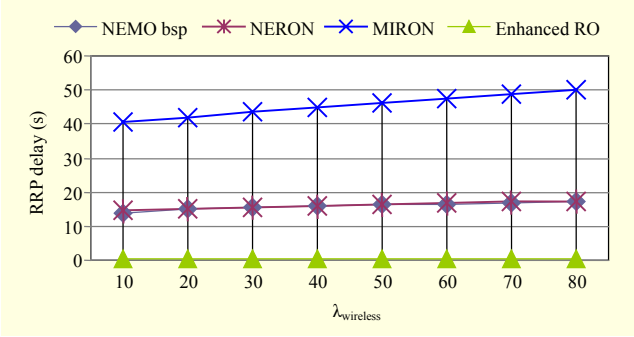

Fig. 10. Effect of $\lambda_{wireless}$ on RR delay.

increasing wired link delay, compared with the enhanced mechanism, which is less affected because of the reduction in signaling due to embedding the NPT messages into a single message (that is, xHoT). Figure 10 shows the effect of the wireless link delay on the total RR delay. The RR delay for all schemes is slightly increased with the wireless link delay increment. However, the enhanced scheme performs better than other schemes due to the reduction in on-the-air signaling cost.

2. Simulation

The NEMO bsp protocol extension is successfully installed on a Windows machine (hardware: Pentium-IV 2.00 GHz CPU; operating system: Windows XP, Cygwin; software: Ns-2.28, eclipse; and programming language: C++, Otcl, awk). This package is an extension of the MobiWan package built in Motorola Labs and calibrated by the INRIA Company [22]. The script is tested through the MobiWan extension under NS-2.28 using a Cygwin tool. Figure 11 shows the test network topology used in simulation. Network topology defined in this script has a total area of 1,600 × 800 and four base stations (bs_1, bs_2, bs_3, and bs_4 addressed as 1.1.0, 1.2.0, 1.3.0, and 1.4.0, respectively) located at (200, 200), (600, 200), (200, 600), and (600, 600). Each base station is connected to the router (R) by a duplex link, and the R address is (1.0.0). The firewall entity (a router without firewall filtering rules) defined in this topology is connected to the R from one side by the duplex link and to the CN from another side by the simplex link. The MR is also defined in this topology, with the address 1.1.256 and the location (190, 190). Two routers are underneath this MR, with the respective addresses 1.1.258 and 1.1.259, connected with the MR using the NS-2 command "create-mobile-network," wherein the total number of prefixes used in this scenario is 10 prefixes. In previous extensions of the MobiWan system, RO starts without MR prefix verification. In our extended MobiWan, the RO begins when the return routability procedure completes its verification (using both the packet sequence number and the nonce as a random value) to the MR_HoA, MR_CoA, and MR_PFs. Finally, once the BA returns (that is, CN_OPT_BACK=16), then RO is completed.

After running the old extension of NEMO without PF verification and the new extension with the new RR mechanism supporting PF verification, two trace files are generated. A comparison of these two files is presented in Table 2.

Table 2 shows that the duration of the new mechanism is 1.256 s, whereas the original extension of the NEMO without PF verification in the MobiWan system lasts 1.04 s, which is still acceptable in real-time environments. According to [2],

Table 1. System parameters and typical values used in literature [2], [19]-[26].

Parameter	Notation	Value
Link layer (L2) switching delay	t_{L2}	50 ms
Router discovery delay in MIPv6	t_{RD}	100 ms
Duplicate address detection delay	t_{DAD}	500 ms
Wireless link failure probability	β	0.5
Wireless link bandwidth	$R_{wireless}$	11 Mbps
Wired link bandwidth	R_{wired}	100 Mbps
Wired link delay	λ_{wired}	2 ms
Wireless link delay	$\lambda_{wireless}$	10 ms
Number of hops between X and Y	$d_{x\text{-}y}$	10 hops
Simple processing delay unit for each entry	α	3 ms
Number of CNs	N_c	5
Number of prefixes	n	1, 5, 10, 15, 20, 25, 30
Average queuing delay	D_{queue}	5 ms
HoTi control message size from MR to HA	$p^{HoTi}_{MR,HA}$	128 bytes
HoTi control message size from HA to FW	$p^{HoTi}_{HA,FW}$	56 bytes
HoT control message size from FW to HA	$p^{HoT}_{FW,HA}$	64 bytes
HoT control message size from HA to MR	$p^{HoT}_{HA,MR}$	136 bytes
CoTi control message size from MR to FW	$p^{CoTi}_{MR,FW}$	56 bytes
CoT control message size from FW to MR	$p^{CoT}_{FW,MR}$	64 bytes
BU control message size from MR to HA	$p^{BU}_{MR,HA}$	136 bytes
BU control message size from MR to FW	$p^{BU}_{MR,FW}$	72 bytes
BA control message size from HA to MR	$p^{BA}_{HA,MR}$	128 bytes
BA control message size from FW to MR	$p^{BA}_{FW,MR}$	72 bytes

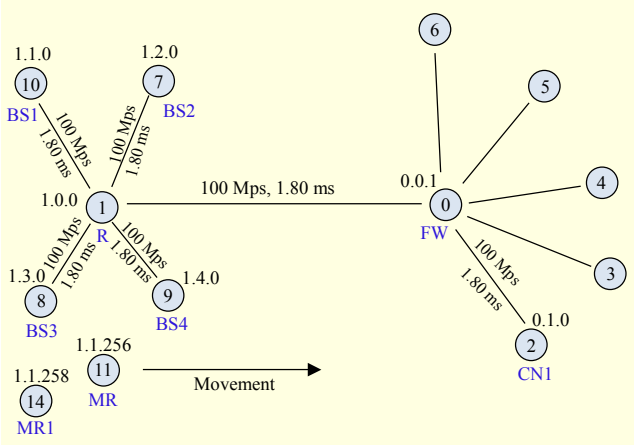

Fig. 11. Network topology in simulation.

any security enhancements will result in performance degradation in real-time environments, particularly affecting the handoff procedure. Comparing the simulation results with the mathematical model shows that both exhibit the same system behaviors with a slight difference in the system values.

Table 2. Time duration for return routability procedure.

Time (s)	Sent HoTi & CoTi	Received CoT	Received HoT, xHoT	Sent BU	Received BA
Original NEMO	20.0000	20.0643	20.0776	20.0776	20.1040
Extended NEMO	20.0000	20.0701	20.0896	20.0896	20.1256

V. Conclusion

In this paper, we proposed a new RR mechanism for network mobility in IPv6 environments. This proposed mechanism retains the basic advantages of using the firewall to ensure a highly secure level and to develop more advantages in updating scalability and firewall modification. Thus, the firewall acts as an agent for the CNs without modifying these nodes to maintain the new RRP in the NEMO instead of the CN(s). This proposed system is lightweight, especially when more than one MNN inside the NEMO communicates with the same CN or with several CNs that are protected by the same firewall. This mechanism also reduces the signaling load between the MR and the AR within limited wireless channels and the signaling load in wired links. Finally, the proposed work provides an acceptable RO solution for network mobility, notably without altering CN entities. Our future work will include implementing multiple CoA registrations using a binding identification number in the return routability procedure for both the NEMO and the MIPv6 within a firewall setting. Additionally, future investigations could focus on the mobility of the CNs.

References

[1] C. Perkins, "IP Mobility Support for IPv4," RFC 3220, Jan. 2002.

[2] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004.

[3] S.S. Hassan and R. Hassan, "IPv6 Network Mobility Route Optimization Survey," *Am. J. Appl. Sci.*, vol. 8, no. 6, 2011, pp. 579-583.

[4] V. Devarapalli et al., "Network Mobility (NEMO) Basic Support Protocol," RFC 3963, Jan. 2005.

[5] T. Ernst and H.Y. Lach, "RFC 4885: Network Mobility Support Terminology," IETF, 2007. http://tools.ietf.org/pdf/rfc4885.pdf

[6] M.C. Chuang and J.F. Lee, "DRO: Domain-Based Route Optimization Scheme for Nested Mobile Networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2011, no. 70, 2011, pp. 1-19.

[7] F.Z. Yousaf and C. Wietfeld, "Solving Pinball Routing, Race Condition and Loop Formation Issues in Nested Mobile Networks," *Computer Netw*., vol. 56, no. 4, Mar. 2012, pp. 1357-1375.

[8] M. Calderón et al., "Design and Experimental Evaluation of a Route Optimization Solution for NEMO," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 9, 2006, pp. 1702-1716.

[9] A. Shahriar, Md. S. Hossain, and M. Atiquzzaman, "A Cost Analysis Framework for NEMO Prefix Delegation-Based Schemes," *IEEE Trans. Mobile Computing*, vol. 11, no. 7, 2012, pp. 1192-1206.

[10] C.J. Bernardos et al., "VARON: Vehicular Ad hoc Route Optimization for NEMO," *Computer Commun*., vol. 30, no. 8, June 2007, pp. 1765-1784.

[11] S. Krishnan, Y. Sheffer, and N. Steinleitner, "Guidelines for Firewall Vendors Regarding MIPv6 Traffic," IETF, Internet-Draft, Mar. 14, 2011.

[12] S. Bellovin and W. Cheswick, "Network Firewalls," *IEEE Commun. Mag*., vol. 32, no. 9, Sept. 1994,. pp. 50-57.

[13] W. Stallings, *Network Security Essentials: Applications and Standards*, 4th ed., Pearson Education Asia, 2003. DOI: 10.1109/MNET.2000.826358.

[14] P.J. Li and C.S. Zhi, "A Mobile IPv6 Firewall Traversal Scheme Integrating with AAA," *IEEE, WiCOM*, Sept. 2006, pp. 1-6.

[15] F. Le, S. Faccin, and B. Patil, "Mobile IPv6 and Firewalls: Problem Statement," RFC 4487, May 2006.

[16] X. Cui, A. Makela, and P. McCann, Eds., "Proxy Correspondent Node Operation for Mobile IPv6 Route Optimization," IETF, Internet-Draft, July 4, 2011.

[17] C.Ng, J. Hirano, "Extending Return Routability Procedure for Network Prefix (RRNP)," IETF, Internet-Draft, Oct. 2004.

[18] C. Perkins, D. Johnson, and J. Arkko, "Mobility Support in IPv6," IETF, Internet-Draft, Mar. 11, 2011.

[19] J. McNair, I.F. Akyildiz, and M. Bender, "Handoffs for Real-Time Traffic in Mobile IP Version 6 Networks," *Proc. IEEE GLOBECOM*, vol. 6, Nov. 2001, pp. 3463-3467.

[20] K. Wang and J. Huey, "A Cost Effective Distributed Location Management Strategy for Wireless Networks," *Wireless Netw.*, vol. 5, no. 4, 1999, pp. 287 -297.

[21] C. Makaya and S. Pierre, "An Analytical Framework for Performance Evaluation of IPv6-Based Mobility Management Protocols," *IEEE Trans. Wireless Commun.*, vol. 7, no. 3, Mar. 2008, pp. 972-983.

[22] J. McNair, I.F. Akyildiz, and M. Bender, "An Inter-System Handoff Technique for IMT-2000 System," *Proc. INFOCOMM*, Mar. 2000, pp. 208-216.

[23] J. Xie and I.F. Akyildiz, "A Novel Distributed Dynamic Location Management Scheme for Minimizing Signaling Costs in Mobile IP," *IEEE Trans. Mobile Computing*, vol. 1, no. 3, July-Sept. 2002, pp. 163-175.

[24] W.K. Lai and J.C. Chiu, "Improving Handoff Performance in Wireless Overlay Networks by Switching Between Two-Layer IPv6 and One-Layer IPv6 Addressing," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 11, Nov. 2005, pp. 2129-2137.

[25] C. Makaya and S. Pierre, "An Architecture for Seamless Mobility Support in IP-Based Next-Generation Wireless Networks," *IEEE Trans, Veh. Technol.*, vol. 57, no. 2, Mar. 2008, pp. 1209-1225.

[26] MobiWan: Ns-2 Extensions to Study Mobility in Wide-Area IPv6 Networks, 2002. Available: http://www.inrialpes.fr/ planete/ mobiwan/

Samer Sami Hasan received his BSc and MSc in computer science from Saddam University, Baghdad, Iraq, in 2000 and 2003, respectively. In April 2010, he joined the Network and Communication Technology Group in the Facility of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia, as a PhD student. He served as the IT manager in the Ministry of Science and Technology in Iraq from April 2004 to April 2005. Mr. Hasan is also a senior lecturer (staff member) at the University of Baghdad, Baghdad, Iraq, in the Department of Computer Science. His research interests include network mobility and wireless network management. He is a member of IEEE and the CCNA local academy, Iraq. He has had several conference and journal papers published by IEEE and other journals.

Rosilah Hassan obtained her MEE from the Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia, in 1999. She received her PhD in 2008 from the Faculty of Electrical Engineering and Electronics, University of Strathclyde, Glasgow, Scotland, UK. She is currently a senior lecturer at the School of Computer Science at the Universiti Kebangsaan Malaysia, where she also leads a network and communication technology research group. She is the co-author of several book chapters and over 50 articles for refereed publications, available at http://www.ftsm.ukm.my/network/ and http://www.ftsm.ukm.my/rosilah. Her research interests include QoS, wireless and mobile networks, and ad hoc networks.