13

Performance Analysis of Seamless Handover in Mobile IPv6-based Cellular Networks

Liyan Zhang[1], Li Jun Zhang[2] and Samuel Pierre[3]
[1]*School of Electronics and Information Engineering, Dalian Jiaotong University*
[2]*Division R&D, Geninov Inc.*
[3]*Department of Computer Engineering, Ecole Polytechnique de Montreal*
[1]*China*
[2,3]*Canada*

1. Introduction

The commercial proliferation of cellular voice and data service has placed a new challenge for mobile communication systems. Next-generation wireless systems are envisioned to have an all-IP-based infrastructure with the support of heterogeneous access technologies (Akyildiz et al., 2004). Under the circumstance, the Internet Protocol (IP) is selected as the common interconnection protocol to integrate disparate wireless systems, so that mobile users can roam among multiple wireless networks, regardless of the underlying different radio access technologies (Akyildiz et al., 2005; Makaya & Pierre, 2008; Mohanty & Xie, 2007). However, with the advent of new value-added services (video-conference, multimedia streaming, etc.) and novel concepts introduced into Long Term Evolution (LTE) architecture of the 4th Generation (4G) networks, provisioning efficient mobility management with quality of service guarantees and seamless handoff feature become even more important for next-generation wireless network design.

Generally, *mobility management* allows mobile communication systems to locate roaming terminals for voice/data delivery as well as maintaining network connectivity when the terminal moves into a new service area (Akyildiz et al., 1999). Typically, such process contains two aspects: location management and handoff management (Quintero et al., 2004; Zhang et al., 2010).

Location management enables telecommunication systems to find out the network attachment points of roaming nodes for call/data delivery. It usually contains two components: *location update* and call delivery (or data delivery). The former requires mobile nodes to provide the system with their location information, while the latter indicates that the system is queried for the location information of specific mobile nodes, and then services are delivered to them while they are away from their home network (Zhang et al., 2010).

Handoff management aims to maintain network connectivity when mobile nodes change their network attachment points or access points. Obviously, handoff protocols need to preserve mobile users' network connectivity as they move from one network to another, while simultaneously reducing disruption to the ongoing call/data sessions. Therefore, reducing handoff delay and maximizing session continuity are always the primary goals of handoff management (Dimopoulou et al., 2005). Generally, *handoff seamlessness* means lower packet

losses, minimal handoff latencies, lower signaling overheads and limited handoff failures (Makaya & Pierre, 2008).

Handoff can be classified into: horizontal (or intra-system) and vertical (or inter-system) handover due to the coexistence of various radio access technologies in the next-generation wireless networks. *Horizontal handoff* takes place when mobile nodes move between access points supporting the same network technology while *vertical handoff* happens when mobile terminals move among access points supporting different network technologies (Nasser et al., 2006). This chapter proposes IP-layer-based mobility management solutions, which are suitable for both intra-system and inter-system handoff.

Handoff latency is defined as the time taken for a mobile node to obtain a new IP address from a visiting network and register itself with its home network (Haseeb & Ismail, 2007), during which the mobile node cannot send or receive any data packets. The handoff latency is the primary cause of packet losses in a network, and needs to be minimized as much as possible, particularly for supporting real-time applications.

According to handled object, mobility can be classified into: *network mobility* (NEMO) (Devarapalli et al., 2005) and *host mobility*. NEMO-based schemes aim to manage the mobility of an entire network (Ernst & Lach, 2007). Such protocols allow a mobile network to change its point of attachment to the Internet, and ensure its reachability in the topology, without interrupting packet delivery to/from that mobile network (Manner & Kojo, 2004).

The NEMO basic support protocol (Devarapalli et al., 2005) enables mobile networks to attach to different access points in the Internet. Such a protocol is an extension of mobile IPv6 (MIPv6) (Johnson et al., 2004) and allows session continuity for every node in the mobile network as the network moves. It also enables every roaming node in such a network to be reachable (Devarapalli et al., 2005). A number of solutions are proposed for network mobility. For example, a novel architecture is recently proposed to provide NEMO support in proxy MIPv6 domain, namely *N-PMIPv6* (Soto et al., 2009). Such a protocol handles mobile networks' connectivity in network-based localized mobility domain. To improve handover performance, issues that combine network mobility and host mobility are discussed in this proposal.

Host mobility management allows a mobile node to change its point of attachment to the network, without interrupting IP packet delivery to/from that node (Manner & Kojo, 2004). Numerous protocols are designed within the Internet Engineering Task Force (IETF) working groups for host mobility, such as MIPv6 (Johnson et al., 2004), hierarchical mobile IPv6 (HMIPv6) (Soliman et al., 2008), mobile IPv6 fast handovers (FMIPv6) (Koodli, 2008), fast handovers for HMIPv6 (F-HMIPv6) (Jung et al., 2005), and proxy mobile IPv6 (PMIPv6) (Gundavelli et al., 2008), etc. Moreover, some working groups are still striving to improve the performance of such specifications. And this chapter focuses on host mobility support issues.

The remainder of this chapter is organized as follows. We provide an overview of the related work pertaining to mobility management in IPv6-based wireless networks in Section II. Then, we elaborate the proposed seamless mobility management schemes, namely seamless mobile IPv6 (SMIPv6) in Sections III. To assess its efficiency, we design analytical models and present the analysis of numerical results in Section IV. Finally, we draw our conclusion marks in the last section.

2. Background and related work

In all-IP-based wireless networks, mobile nodes can freely change their network attachment points while communicating with correspondent nodes. Accordingly, *mobility management* becomes a critical issue to track mobile users' current location and to efficiently deliver services to them when they are away from their home network.

Generally, IP mobility includes *macromobility* and *micromobility*. Macromobility designates mobility over a large area; this refers to situations where mobile nodes move between different IP domains (Manner & Kojo, 2004). Typically, protocols such as mobile IPv4 (MIPv4) (Perkins, 2002), MIPv6 (Johnson et al., 2004) and PMIPv6 (Gundavelli et al., 2008) are best suited for macromobility management. This chapter only addresses mobility management in IPv6-based wireless networks.

Micromobility refers to mobility over a small area, i.e. within an IP domain. Usually, micromobility protocols maintain a location database that maps mobile host identifiers to location information, and they complement IP mobility by offering fast and seamless handoff control in limited geographical areas and IP paging in support of scalability and power conservation (Campbell et al., 2002). Typical micromobility management protocols are Cellular IP (Valko, 1999), handoff-aware wireless access internet infrastructure (HAWAII) (Ramjee et al., 2002), HMIPv6 (Soliman et al., 2008), FMIPv6 (Koodli, 2008) and F-HMIPv6 (Jung et al., 2005).

Cellular IP and HAWAII use two approaches to optimize handoff performance: bicasting, buffering & forwarding techniques (Campbell et al., 2002; Ramjee et al., 2002; Valko, 1999). HMIPv6, FMIPv6 and F-HMIPv6 confine mobility related signaling within a local domain. Therefore registrations with distant home agent and correspondent nodes are eliminated as long as mobile nodes remain inside their local domain. Accordingly, micromobility protocols yield better performance than macromobility solutions for roaming within a local domain, namely *intra-domain movement*.

MIPv6 (Johnson et al., 2004) is the baseline host-based mobility management protocol, which provides mobile users with unbroken network connectivity while they move around the Internet. Regardless of its current location, a mobile node is always identified by its home address. While away from the home network, the mobile node configures a new IP address (care-of-address), which indicates its current location within the Internet topology. The uniqueness of such a new address must be verified before utilization through neighbor discovery procedure defined in (Narten et al., 2007). Such verification is called *duplicate address detection* (Thomson et al., 2007). Each time when this mobile moves, it has to inform a router called home agent of its new IP address. However, this results in triangular routing problem. To fix this, route optimization is designed to allow mobile and correspondent nodes to communicate via a direct routing path (Arkko et al., 2007).

Usually, handover takes place when a mobile node changes its network attachment point. After acquiring a new IP address from the visiting network and successfully executing the duplicate address detection, the mobile node sends a *binding update* (BU) message to its home agent, which is a default router at the home network. The home agent then binds the mobile's home address to the new care-of-address, and replies the mobile with a *binding acknowledgement* (BA) message. Subsequently, the home agent intercepts the packets addressed to the mobile and tunnels them to the mobile's new location.

Following by successful home registration, return routability tests are carried out to ensure communication security between the mobile and each correspondent node. Upon completion, corresponding registration is done by exchanging BU and BA messages between the mobile

and correspondent nodes. As a result, correspondent nodes can directly communicate with mobile node without bypassing the home agent.

Generally, the overall handoff process includes *link layer switching* (or layer two handoff), *movement detection* to discover new access networks, new care-of *address configuration*, *duplicate address detection*, *home registration*, *return routability tests*, and *correspondent registration*. Eventually, handoff latency results in packet loss and degrades network performance, which is unacceptable and detrimental to real-time traffic causing user perceptible service deterioration (Kempf et al., 2003). Thus improving the performance of MIPv6 is one major challenge for wireless networks to provide mobile users with seamless mobility, session continuity and guaranteed quality of service.

As MIPv6 handles local mobility and global mobility in the same fashion (Haseeb & Ismail, 2007), mobility management induces lengthy registration delays and unavoidable packet losses. Thereby separating local and global mobility domain is necessary. Under such circumstances, protocols such as Cellular IP (Valko, 1999), HAWAII (Ramjee et al., 2002), HMIPv6 (Soliman et al., 2008), FMIPv6 (Koodli, 2008), F-HMIPv6 (Jung et al., 2005) are designed to improve handoff performance.

Cellular IP (Valko, 1999) is a lightweight and robust protocol to support local mobility, it uses distributed caching techniques for location management and routing. Distributed paging cache coarsely maintains the position of idle mobile nodes in a service area while distributed routing cache maintains the position of active mobile nodes in the service area and dynamically updates the routing state of mobile nodes when they move to other service areas (Valko, 1999). Handoff is initiated by a mobile node through sending out a message to the old access point, which then modifies its routing cache, configures a new routing path for the mobile along with a timer. Before time out, packets destined to the mobile are delivered at both the old and new access points. Such delivery technique is called *bicasting*, which helps to reduce packet losses caused by handoff. Cellular IP shows great benefit for environments where mobile nodes migrate frequently. However, it requires the capability of mobile node to listen simultaneously two logical channels because of bicasting, this limits its applicability for mobiles with only one radio device.

HAWAII (Ramjee et al., 2002) is a protocol designed for micromobility management. It segregates the network into a hierarchy of domains, and each domain is controlled by a domain root router. Such router maintains a forwarding table with host-based entries. When a mobile node enters into a foreign domain, traditional Mobile IP mechanisms (Perkins, 1996) are executed. The mobile node is assigned a new care-of-address by a DHCP server. Such procedure is called *stateful address configuration*. The mobile node then executes duplicate address detection. Upon success, it carries out home registration with the home agent. As a result, packets addressed to the mobile are intercepted by its home agent, which then tunnels them to the mobile's new location, identified by the new care-of-address. When moving within the same domain, the mobile retains its care-of-address unchanged, and IP connectivity is maintained using dynamically established paths configured by the protocol HAWAII (Ramjee et al., 2002). Therefore, disruption to ongoing sessions is minimized during handoff.

HMIPv6 (Soliman et al., 2008) is designed to reduce the signaling cost and location update delay outside a local mobility domain. Like HAWAII, this protocol also divides the network into a hierarchy of domains, and each domain is managed by a mobility anchor point (MAP). While entering a MAP domain, a mobile node configures two IP addresses: an on-link local care-of-address (LCoA) and a regional care-of-address (RCoA). The mobile node then

verifies the uniqueness of the LCoA through duplicate address detection. Upon success, it sends a *local binding update* (LBU) message to the MAP, which then verifies the uniqueness of the RCoA, binds the mobile's LCoA with the RCoA, and replies the mobile with an acknowledgment message. As a result, a bidirectional tunnel is established between the mobile node and MAP (Soliman et al., 2008). Afterward, the mobile informs its home agent and each correspondent node of the RCoA. Accordingly, they bind the mobile's RCoA with its home address. Packets destined to the mobile are intercepted by the MAP, encapsulated and forwarded to the mobile's LCoA. A movement within the MAP domain merely incurs LBUs to the MAP without further propagation to home agent and correspondent nodes, thus significantly reducing signaling load and handoff latency for local movements (Zhang, 2008).
FMIPv6 (Koodli, 2008) is known as low latency address configuration protocol, which enables mobile nodes to rapidly detect their movements and to obtain a prospective IP address with a new access router before disconnecting with the current access router. It also offers mobile nodes the opportunity to utilize available link layer event notification (triggers) to accelerate network layer handoff (Kempf et al., 2003). Hence, delays pertaining to access network discovery and new IP address generation are completely removed from handoff latency. Moreover, a bidirectional tunnel is setup between the previous access router (PAR) and new access router (NAR) to avoid packet losses. The PAR binds the mobile's previous care-of-address with the new care-of-address. Therefore, packets addressed to the mobile are intercepted by the PAR, tunneled to the NAR, which then decapsulates and forwards them to the mobile node. During handoff, no registration is necessary with either the home agent or any correspondent node. However, because of the utilization of pre-handover triggers, the performance of FMIPv6 largely depends on the trigger time. In case where the pre-handoff trigger is delivered too closely to the actual link switching, the communication using FMIPv6 becomes unreliable (Kempf et al., 2003).
Both FMIPv6 and HMIPv6 are designed in their own fashion to improve the MIPv6 performance, it is necessary to combine them together. However, simple superimposition of FMIPv6 over HMIPv6 induces unnecessary processing overhead for re-tunneling at the PAR and inefficient usage of network bandwidth (Jung et al., 2005). To resolve such problems, F-HMIPv6 (Jung et al., 2005) enables mobile nodes to exchange handoff signaling messages with a MAP and to establish a bidirectional tunnel between the MAP and NAR, instead of between the PAR and NAR. However, the performance of this protocol is largely dependent on various wireless system parameters such as user mobility model, user density, domain size, session-to-mobility ratio, etc (Zhang, 2008).
The aforementioned protocols present typical solutions in the literature for mobility management in wireless networks. However, these protocols all have pros and cons. Cellular IP requires mobile nodes to be equipped with multiple radio interfaces. HAWAII needs the capability of working together with Mobile IP mechanisms, and its forwarding technique requires more buffer space at access routers. MIPv6 is suitable for macromobility management with some drawbacks such as high signaling overheads, unacceptable packet losses and lengthy handoff latencies, thus cannot support real-time traffic. HMIPv6 cannot meet the requirements for delay-sensitive traffic, such as voice over IP (VoIP), due to high packet loss rate and long handoff delay (Makaya & Pierre, 2008). FMIPv6 is hindered by the problems of supporting quality of service and scalability. Additionally, neither signaling overheads nor packet losses are effectively reduced using FMIPv6, thus supporting seamless mobility becomes impossible. F-HMIPv6 allows mobile users to benefit from both FMIPv6 and HMIPv6, but the handoff latency for intra-domain roaming lasts about 90*ms* whereas the

handover delay for inter-domain roaming rises to about 240*ms* (Jung et al., 2005), making this protocol unsuitable for multimedia streaming traffic (Zhang & Pierre, 2008). As a result, none of these protocols provides a perfect solution for seamless mobility management.
Under the circumstance, we propose a new protocol called seamless mobile IPv6 (SMIPv6) (Zhang et al., 2005; Zhang & Marchand, 2009; Zhang & Pierre, 2008; 2009). Compared with current alternatives, the key advantage of our proposal is that (1) mobile nodes don't have to be equipped with multiple radio interfaces; (2) forwarding IP packets from the PAR to NAR is carried out much earlier than FMIPv6 and F-HMIPv6; (3) Ongoing real-time session is resumed on the new link much earlier than FMIPv6 and F-HMIPv6; (4) it is flexible to work with MIPv6 and HMIPv6; (5) SMIPv6 can support multimedia streaming traffic during handoff.

3. Proposed seamless mobile IPv6

The main idea of SMIPv6 (Zhang et al., 2005; Zhang & Marchand, 2009; Zhang & Pierre, 2008; 2009) is to pre-configure bidirectional secure tunnels among access routers before actual handover and to utilize such tunnels to accelerate mobility management procedure of FMIPv6 (Koodli, 2008). The quality of service related parameters (e.g. delay, jitter, packet loss), and security aspects (e.g. authentication methods, tunneling keys) are specified for each unidirectional tunnel through negotiation between radio access networks (Zhang & Marchand, 2006; Zhang & Pierre, 2009). Such access networks can be managed by either the same or different operators. The utilization of pre-established tunnels enables network operators to serve their own mobile users and those from their competitors. As a result of negotiation, a set of specific mobile users is given the opportunity to exploit pre-configured tunnels during handoff. Additionally, using pre-established bidirectional tunnels allows mobile nodes to retain their previous valid IP addresses unchanged in a new visiting network or domain (Zhang & Marchand, 2009; Zhang & Pierre, 2009). This minimizes interruption of ongoing multimedia sessions during handoff. And new routing policy is added to access routers, this enables the delivery of packets to mobile nodes that use a topologically invalid address within an access network.
The proposed mobility management procedure in SMIPv6 comprises two stages: configuring bidirectional secure tunnels between radio access networks prior to actual handoff and using such tunnels to accelerate mobility management procedure during handoff.

3.1 Tunnel establishment

The first stage of SMIPv6 consists of using *tunnel establishment* method (Zhang & Marchand, 2006; Zhang & Pierre, 2009) to set up bidirectional secure tunnels among access routers. This method allows dynamically establishing a tunnel with a set of minimal characteristics between two tunnel endpoints. Such tunnels enable radio access networks to establish business and security relationship with their neighborhood. Consequently, communication services are offered to a list of subscribers from either the same or various mobile operators.
Tunnel establishment method requires that each node (access router in our case) comprises a tunneling protocol module. The source node determines a first set of desired characteristics of the tunnel. Its tunneling protocol module sends a *tunnel request* message to a destination node. Such request comprises the specific conditions of the unidirectional tunnel and a shared secret key with an index value thereof. The destination node then determines a second set of desired characteristics, and replies with a *tunnel reply* message. Upon reception of this message, the source node verifies if the second set of characteristics is at least equal to the

set of minimal characteristics. If so, it replies a *tunnel acknowledgment* message. Otherwise, negotiation keeps on between the involved nodes until time out. The shared secret is used to encrypt data and the index value indicates which shared secret is used during subsequent communication. Usually, such negotiation is done before mobile users handoff from one access network to another. With the determined characteristics, both nodes configure their *Forwarding* and *Reverse Tunnels Lists*, respectively (Zhang & Marchand, 2006; Zhang & Pierre, 2009).

3.2 Seamless mobility management

The seamless mobility management procedure in SMIPv6 allows mobile nodes to utilize pre-configured bidirectional secure tunnels during handoff (Zhang & Marchand, 2009). To realize such functionality, we introduce a new network entity, called intelligent access router (iAR) with novel routing policy, which allows it to handle the traffic using topologically invalid addresses within the access network, and to handle tunneled packets, of which the ultimate destination node is not yet attached to the network.

The following example shows the way of an iAR handling tunneled packets, of which the final destination is not within its network. The iAR receives a tunneled packet from another access router, which format is shown in Table I. Upon receiving such packet, the iAR (NAR in our case) usually removes the outer header, verifies the IP address of the destination node, and finds out that the destination (MN in our case) is not in its subnet. Normal IP routing policy requires the destination router to forward such packet to the source router (PAR in our case) with which the destination node is supposed to be attached. This induces the routing loop problem, which still exists in FMIPv6. SMIPv6 fixes such problem by allowing the iAR to buffer such packet for a certain of time, waiting for the attachment of the mobile node. Upon timeout and the absence of the MN, the destination router (iAR) simply discards the received tunneled packet.

source-addr 1	dest-addr 1	source-addr 2	dest-addr 2	token	data
PAR-addr	NAR-addr	CN-addr	MN-PCoA	TK1	data

Table 1. Example of a tunneled packet

The subsequent example shows the way of an intelligent access router (iAR) handling a packet from a topologically invalid address within the access network. The iAR (NAR in our case) receives from a mobile node (MN) a packet, which format is shown in Table II. Generally, such kind of packets are dropped by access router due to ingress filtering. However, SMIPv6 allows the iAR to verify the IP address of the source node (MN in our case), finds out the IP address of the associated router, from which the source node obtained its valid IP address, namely previous care-of-address (PCoA). The iAR (or NAR) then checks out if there are pre-established tunnels between the two involved access networks. If so, it tunnels the packets to the previously associated router (PAR). The PAR then removes the outer header of the tunneled packets, carries out ingress filtering, and decrypts the data using a pre-shared key with the MN. Upon success, the PAR then sends the packets with the decrypted data to the correspondent node (CN).

source-addr	dest-addr	encrypted data
MN-PCoA	CN-addr	encrypted data using pre-shared key between MN-PAR

Table 2. Example of a packet from MN to NAR

Since SMIPv6 empowers mobile nodes to use their valid previous care-of-address (PCoA), the context information of mobile nodes can be kept intact at previous access router. Hence, delay pertaining to context transfer process (Loughney et al., 2005) is eliminated completely from handoff latency. Additionally, mobile nodes can resume and initiate communication on the new link using their valid PCoAs due to pre-configured tunnels. Compared with the bidirectional edge tunnel handover for IPv6 (BETH) (Kempf et al., 2001), SMIPv6 does not need to exchange *handover request* and *handover reply* messages to establish bidirectional tunnels during handoff; neither does it exploit link layer pre-triggers to facilitate IP layer handoff. Given that both FMIPv6 (Koodli, 2008) and BETH (Kempf et al., 2001) protocols utilize pre-handover triggers, their performance, in terms of packet loss and handoff latency, depends greatly on the pre-handoff trigger time, thus becoming unreliable when such trigger is delivered too closely to the actual link switching (Gwon & Yegin, 2004; Kempf et al., 2003).

3.2.1 Predictive SMIPv6

We assume that mobile nodes (MNs) roam in the IPv6-based wireless networks, and each MN acquires a valid care-of-address (CoA) from its previous access router (PAR). Additionally, the MN has established a security association with the PAR before actual handoff. As a result, both of them configure a pre-shared key (PSK). In an overlap zone covered by the PAR and its neighbors, a mobile node receives beacons from nearby access points (APs). Such beacons contain APs' identifiers (AP-ID). Horizontal handoff requires the mobile to select the most suitable AP by analyzing the received signal strength, while vertical handoff asks for the mobile to use techniques such as score function (McNair & Zhu, 2004). Upon selection the best AP, the mobile node sends a *seamless binding update* (SBU) message to the PAR before breaking their connection. Such message contains the new AP's identifier (NAP-ID) and a session token generated by the mobile. Such token will be used to avoid replay attack.

Like FMIPv6 (Koodli, 2008), we assume that the PAR has some knowledge about its neighbors, such as their IP address, the associated APs' identifiers, etc. Upon receiving the SBU message, the PAR maps the NAP's ID to the IP address of the corresponding router (NAR in our case) and starts intercepting packets destined to the mobile. The PAR caches one copy of the intercepted packets, and then tunnels them to the NAR. An example of such tunneled packets is shown in Table I. The session token is inserted into the tunneled packet. Afterwards, the PAR adds an entry to its *Forwarding Tunnels List*. Such list is used to track the state of the tunnel from the PAR to NAR. Note that packets buffered by the PAR will be forwarded to the mobile in case of *ping pong* and *erroneous* movements. The former implies that mobile nodes move between the same two access routers rapidly while the latter connotes that mobile nodes think entering into a new network, but they are actually either moving to a different access network or aborting their movements by returning to the old access network (Zhang & Pierre, 2009).

Upon receipt of the tunneled packets from the PAR, the NAR removes the outer header, verifies the presence of the destination node in its subnet. In case of absence, the NAR puts the inner packets into a buffer and starts a timer. Subsequently, the NAR extracts the session token from the inner packets and puts it into the *Token List*. Note that each intelligent AR (iAR) manages a token list, which is indexed by mobile's IP address to facilitate information retrieval. The NAR also creates a *host route entry* for the mobile's previous care-of-address (PCoA), and allocates a unique new care-of-address (NCoA) to the pending mobile node. Here we advocate that each iAR manages a private address pool and guarantees the uniqueness of

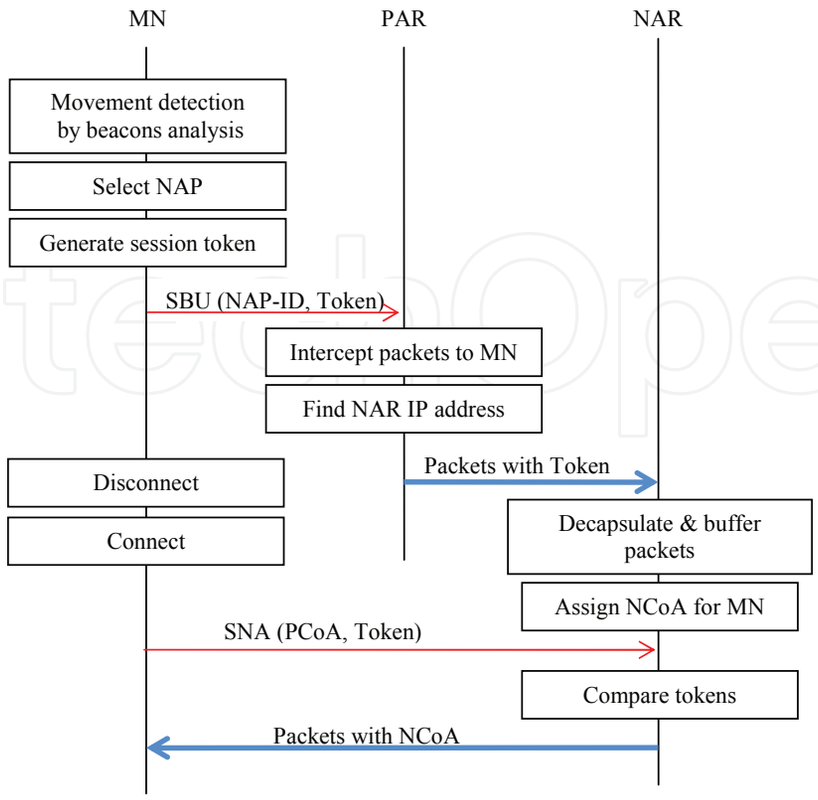


Fig. 1. Mobility management with predictive SMIPv6

each address in the pool. By this means, duplicate address detection can be removed from the overall handoff, thus improving handover performance (Zhang & Pierre, 2009).

Once attached to the new link, the MN sends a *seamless neighbor advertisement* (SNA) message to the NAR immediately. Such a message includes all the fields of *unsolicited neighbor advertisement* (UNA) (Narten et al., 2007), the IP address of the PAR, and a session token that is the same as the one sent to the PAR at the beginning of handoff. The latter two fields will be added as new options into the UNA. The IP source address of the SNA is the mobile's PCoA, and IP destination address is typically the all-nodes multicast address. The source link layer address (LLA) is the mobile's MAC address and the destination LLA is the new AP's link layer address.

Upon receipt of the SNA message, the NAR retrieves the token from its *Token List* with the assistance of the mobile's PCoA. The NAR also verifies whether the received token from the mobile node is the same as the one from the PAR. If they are identical, the NAR retrieves those buffered packets addressed to the mobile, and forwards them to the mobile node, along with the assigned NCoA. Figure 1 illustrates mobility management using predictive SMIPv6.

In case where those two tokens are different, the NAR obtains the IP address of the PAR from the SNA, and sends a *fast binding update* (FBU) message to the PAR on behalf of the mobile node. Such a message contains the mobile's MAC address and its PCoA. The PAR then verifies the mobile's identities and replies with a *fast binding acknowledgment* (FBack) message. Soon afterward, the PAR adds an host entry into its *Forwarding Tunnels List* and *Reverse Tunnels List*, respectively. Upon receiving the FBack message, the NAR forwards the buffered packets and the NCoA to the mobile. Consequently, the mobile becomes reachable on the new link under both CoAs: PCoA and NCoA (Zhang & Pierre, 2009).

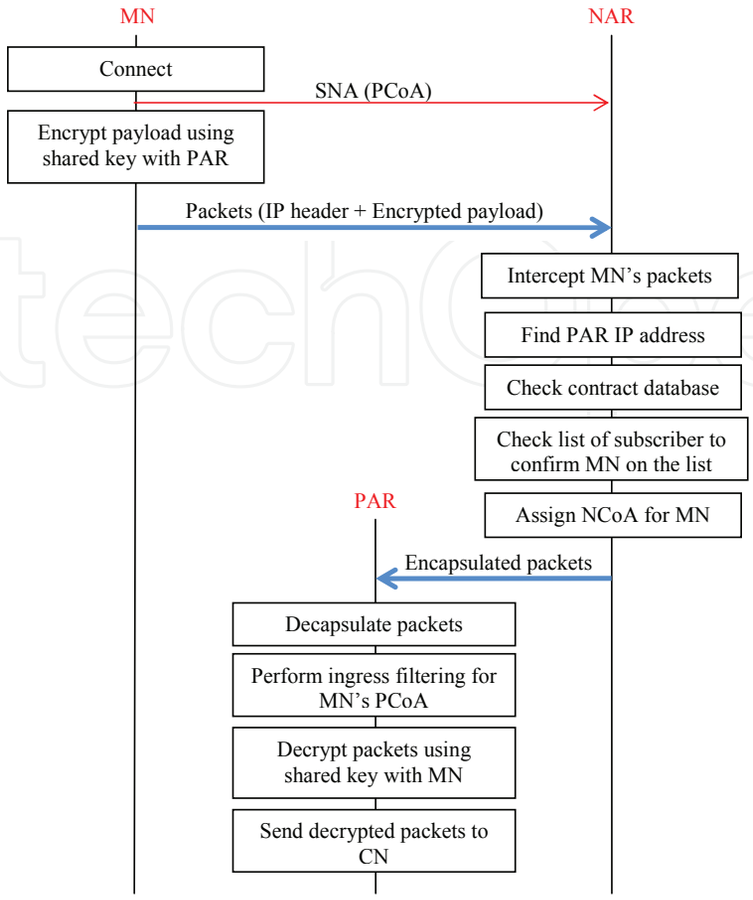


Fig. 2. Mobility management with reactive SMIPv6

3.2.2 Reactive SMIPv6

Typically, a *session* is identified by a group of information such as session ID, source address, destination address, source port number, destination port number, etc. When moving from one network to another, an mobile node loses its network connectivity and becomes unreachable because its previous IP address is invalid in the visiting network. Under the circumstances, the mobile node has to acquire a new IP address and registers the new address with its home agent and all active correspondent nodes. Prior to successful registration, the mobile cannot receive and send packets in the foreign network, thus the ongoing session is disrupted during handoff. In case where the mobile executes multimedia applications such as video-streaming, it cannot tolerate the degraded quality of the session. SMIPv6 resolves such problem by allowing mobile nodes to utilize their previous valid IP addresses on the new link via pre-configured bidirectional secure tunnels, thus guarantee seamless roaming with ongoing real-time sessions.

Reactive mobility management takes place when a mobile node (MN) initiates a new communication session with a correspondent node (CN) on a new link using a topologically invalid IP address. The mobile sends *seamless neighbor advertisement* (SNA) message to the NAR immediately after attachment (Zhang & Pierre, 2009). Figure 2 illustrates mobility management using reactive SMIPv6 (Zhang & Pierre, 2009).

For the sake of security, we advocate that mobile nodes encrypt the outgoing packets using the pre-shared key with the previous access router (PAR) before transmitting them over a

visiting network. Note that instead of using the pre-shared key, the encapsulating security payload (ESP) protocol (Kent, 2005) may also be applicable to provide confidentiality, data origin authentication, connectionless integrity, and anti-replay service.
The new access router (NAR) then intercepts these outgoing packets, of which the source node utilizes its previous care-of-address (PCoA). An example of such packets is shown in Table II. Normally, the NAR should drop these packets because of ingress filtering, this induces high packet losses during handoff. To resolve such problem, SMIPv6 allows the NAR to extract the subnet prefix information from the mobile's PCoA, and obtains the IP address of the previously associated router (PAR). The NAR then checks out if there are any pre-established tunnels to the PAR. Such information is stored in a *contract database* (CD). The NAR also verifies if the mobile node is given the priority to use those pre-configured tunnels. If so, the NAR tunnels the intercepted packets to the PAR, and adds an entry into the *Reverse Tunnels List* for further tunnel maintenance and billing issues. If there is no pre-established tunnels, the NAR uses the *tunnel establishment* method to set up tunnels to the PAR. Upon success, the NAR tunnels the outgoing packets of the mobile to the PAR. If the mobile is not on the list of pre-configured subscribers who can benefit from the value-added service, the NAR will simply drop the packets, the same way as FMIPv6.
Upon receipt of the tunneled packets from the NAR, the PAR removes the outer header, performs ingress filtering for the mobile node's PCoA. Upon success, the PAR decrypts the inner packets using a pre-shared key with the mobile. On completion, the PAR forwards the decrypted packets to the destination node, a correspondent node (CN). The PAR also adds a host entry into its *Reverse Tunnels List*. Once terminating its ongoing session using the PCoA on the NAR's link, the MN can follow the legacy MIPv6 (Johnson et al., 2004) or HMIPv6 (Soliman et al., 2008) registration procedures.

3.3 Tunnel maintenance

Tunnel maintenance usually takes place after handoff, during which a mobile node may send a *Tunnel Bye* message to the new access router (NAR), which then releases the reserved bandwidth for the specific mobile, and forwards the same message to the previous access router (PAR) (Zhang & Marchand, 2006; Zhang & Pierre, 2009). As a consequence, entries in *Forwarding Tunnels List* and *Reverse Tunnels List* are removed or refreshed. However, SMIPv6 requires bidirectional tunnel remains active until mobile nodes complete the binding update procedures with their correspondents, same as the way of FMIPv6.

3.4 Summary

Using FMIPv6 (Koodli, 2008), even though a mobile node is IP-capable on the new link, it cannot use the new care-of-address (NCoA) directly with a correspondent node (CN) before the CN binds the mobile's NCoA with its home address, neither can the mobile use its previous care-of-address (PCoA) on the new link because of ingress filtering. In other words, FMIPv6 delivers better performance for downlink traffic. However, our proposed SMIPv6 allows mobile nodes to utilize their valid PCoAs immediately after attaching to a new link. Hence, the new proposal provides not only expedited forwarding packets to mobile nodes but also accelerated sending packets to their correspondents via a direct routing path, thus optimizes handoff performance.
On the other hand, the protocol SMIPv6 (Zhang et al., 2005; Zhang & Marchand, 2009) is independent of any network architecture. As a result, bidirectional secure tunnels can be pre-configured between any network entities acting as tunnel end-points. When such

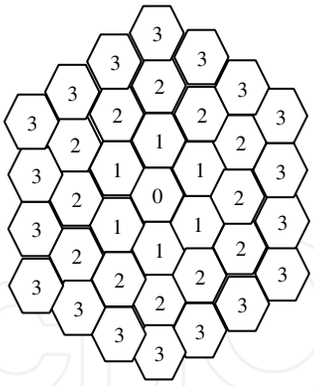


Fig. 3. An example of a MAP domain with 3 rings

tunnels are established between mobility anchor points, handoff delays and packet losses are reduced for both intra-domain and inter-domain movements, thus improves the handover performance of HMIPv6 (Soliman et al., 2008) and F-HMIPv6 (Jung et al., 2005) protocols. Furthermore, SMIPv6 can be freely implemented at any access network, this solves the problem of scalability in FMIPv6. When SMIPv6 mobility management mechanism is unavailable, mobile nodes can rely on the FMIPv6 (Koodli, 2008) protocol. In addition, intermediate routers are not involved in the tunnel setup and tunneling procedures, thus no extra overhead is added to them, this optimizes network resource usage.

4. Evaluation using analytical models

Performance evaluation of mobility management schemes is usually based on simulation and test-bed approaches (Gwon et al., 2004; Perez-Costa & Hartenstein, 2002; Perez-Costa et al., 2003). However, network scenarios for simulations vary greatly, the handoff performance comparison of the aforementioned mobility management protocols is rarely viable. Under the circumstance, analytical models are designed to evaluate system performance for users roaming in IPv6-based wireless cellular networks.

We assume that mobile service areas are partitioned into cells of equal size. Each cell is surrounded by rings of cells, except for cells in the outermost ring. Each domain is composed of n rings of the same size. We name the inmost cell "0", the central cell. Cells labeled "1" constitute the first ring around cell "0", and so on. Each ring is labeled in accordance with the distance to the cell "0". We assume that each cell is managed by one access router. Figure 3 shows an example of a MAP domain with three rings (Zhang & Pierre, 2008).

4.1 Mobility models

There are two mobility models proposed in the literature: the fluid-flow and random-walk models (Akyildiz & Wang, 2002). The former is more suitable for mobile users with high mobility, sporadic speed and direction changes. The latter is often used for pedestrian mobility, which is mostly limited to small geographical areas such as residential sites or premises.

4.1.1 The random-walk model

Under the random-walk model, the next position of a mobile node is determined by its previous position plus the value of a random variable with an arbitrary distribution. Assuming that a mobile node is located in a cell of ring r, the probability for the mobile to

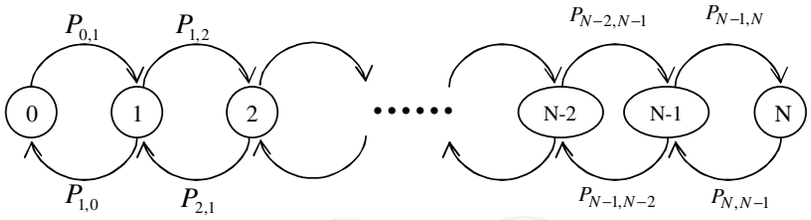


Fig. 4. State diagram for the random-walk model

move forward to a cell of ring $r+1$ ($p^+(r)$) and backward to a cell of ring $r-1$ ($p^-(r)$) are shown as follows (Zhang & Pierre, 2008):

$$p^+(r) = \frac{1}{3} + \frac{1}{6r} \tag{1}$$

$$p^-(r) = \frac{1}{3} - \frac{1}{6r} \tag{2}$$

We present the random-walk model with a one-dimensional Markov chain in which the state is defined as the distance between the current cell located the mobile node and central cell. Thus a mobile node is in state r if and only if it is now residing in a cell of ring r. Figure 4 shows the state transition diagram of this Markov chain (Zhang & Pierre, 2008).
Assuming that the probability for a mobile node to stay in the current cell is q, the probability for the mobile node to move to another cell is $1-q$. The transition probability $P_{r,r+1}$ and $P_{r,r-1}$ represent the probabilities that a mobile node moves from its current state r to the state $r+1$ and $r-1$, shown as follows (Zhang & Pierre, 2008):

$$P_{r,r+1} = \begin{cases} 1-q \ if \ r=0 \\ (1-q) \times (\frac{1}{3} + \frac{1}{6r}) \ if \ 1 \le r \le n \end{cases} \tag{3}$$

$$P_{r,r-1} = (1-q) \times (\frac{1}{3} - \frac{1}{6r}) \tag{4}$$

Let $\Phi_{r,n}$ be the steady-state probability of state r within a mobility anchor point (MAP) domain of n rings. Using the transition probabilities in Equations (3) and (4), $\Phi_{r,n}$ is shown as follows (Zhang & Pierre, 2008):

$$\Phi_{r,n} = \Phi_{0,n} \prod_{i=0}^{r-1} \frac{P_{i,i+1}}{P_{i+1,i}} \tag{5}$$

As $\sum_{r=0}^{n} \Phi_{r,n} = 1$, the expression of $\Phi_{0,n}$ is also given as follows (Zhang & Pierre, 2008):

$$\Phi_{0,n} = \frac{1}{1 + \sum_{r=1}^{n} \prod_{i=0}^{r-1} \frac{P_{i,i+1}}{P_{i+1,i}}} \tag{6}$$

Assuming that a mobility anchor point (MAP) domain is composed of n rings, and each cell is controlled by an access point integrating the functionality of an access router. The probability for a mobile node to perform an inter-domain mobility P is given as (Zhang & Pierre, 2008):

$$P = \Phi_{n,n} \times P_{n,n+1} \tag{7}$$

Where the $\Phi_{n,n}$ is the steady-state probability of the state n, $P_{n,n+1}$ is the probability that a mobile node moves from a cell in ring n to a cell in ring $(n+1)$.

4.1.2 The fluid-flow model

Using the fluid-flow model, the movement direction of a mobile node (MN) within a mobility anchor point (MAP) domain is distributed uniformly in the range of $(0, 2\pi)$. Let v be the average speed of an MN (m/s); R the cell radius (m); L_c and L_d the perimeters of a cell and a MAP domain with n rings (m); S_c and S_d the areas of a cell and a MAP domain with n rings (m^2); R_c and R_d be the cell and domain crossing rates, which denote the average number of crossings of the boundary of a cell and a domain per unit of time $(/s)$, shown as follows (Zhang & Pierre, 2008):

$$R_c = \frac{v \times L_c}{\pi \times S_c} = \frac{v \times 6R}{\pi \times 2.6R^2} = \frac{6v}{\pi \times 2.6R} \tag{8}$$

$$R_d = \frac{v \times L_d}{\pi \times S_d} = \frac{v \times (12n+6)}{\pi \times [3n \times (n+1)+1] \times 2.6R} \tag{9}$$

4.2 Cost functions

To analyze the performance of SMIPv6, we define the total cost as the sum of the mobility signaling cost and the packet delivery cost (Zhang & Pierre, 2008; Zhang et al., 2010).

4.2.1 Mobility signaling cost

Generally, mobile nodes perform two types of movements: intra-domain and inter-domain. The former are movements within an administrative domain while the latter implies movements between domains. Accordingly, two mobility management procedures are carried out for HMIPv6 and F-HMIPv6: the intra-domain and inter-domain cases. The latter includes the intra-domain and legacy MIPv6 mobility management procedures. However, FMIPv6 and SMIPv6 only address the problem of inter-cell handoff, because their domain is defined as a set of access routers.

We assume that mobility management protocols such as HMIPv6 (Soliman et al., 2008), F-HMIPv6 (Jung et al., 2005), FMIPv6 (Koodli, 2008) and SMIPv6 all support route optimization (RO) and only a pair of messages (*neighbor solicitation* and *neighbor advertisement*) exchanged for duplicate address detection. In addition, we assume that the distance between the previous access router (PAR) and MAP equals the one between the new access router (NAR) and MAP. And processing costs at the mobile node and correspondent node are ignored during analysis.

The mobility signaling overhead functions for MIPv6 (Johnson et al., 2004) with tunnel and RO modes, intra- and inter-domain HMIPv6, predictive and reactive FMIPv6, intra- and inter-domain F-HMIPv6 are given in (Zhang, 2008; Zhang & Pierre, 2008). The signaling overhead functions for predictive SMIPv6 (P-SMIPv6) and reactive SMIPv6 (R-SMIPv6) are expressed as follows (Zhang & Pierre, 2008; Zhang et al., 2010):

$$S_{P-SMIPv6} = 2\kappa \tag{10}$$

$$S_{R-SMIPv6} = \kappa \tag{11}$$

Where κ represents the unit transmission cost in a wireless link. Equation (10) implies that for predictive SMIPv6, 2 messages (SBU and SNA) are exchanged between a mobile node and

intelligent access routers (iARs) via radio link during handover, and the signaling cost for each message is represented by κ. The same principle applies to Equation (11).
Under the random-walk model, the mobility signaling cost functions for MIPv6 with tunnel and route optimization (RO) modes, HMIPv6, predictive FMIPv6 (P-FMIPv6), reactive FMIPv6 (R-FMIPv6), F-HMIPv6 are given in (Zhang & Pierre, 2008). The mobility signaling cost functions for predictive SMIPv6 (P-SMIPv6) and reactive SMIPv6 (R-SMIPv6) are expressed as follows (Zhang & Pierre, 2008; Zhang et al., 2010):

$$C^s_{P-SMIPv6} = \frac{S_{P-SMIPv6} \times (1-q)}{E(T)} \tag{12}$$

$$C^s_{R-SMIPv6} = \frac{S_{R-SMIPv6} \times (1-q)}{E(T)} \tag{13}$$

Where q is the probability that a mobile node remains in its current cell, $E(T)$ is the average cell residence time (s), $S_{P-SMIPv6}$ and $S_{R-SMIPv6}$ represent the mobility signaling overheads obtained from Equations (10) and (11).
Using the fluid-flow model, the mobility signaling cost functions for MIPv6 (Johnson et al., 2004) with tunnel and RO modes, HMIPv6 (Soliman et al., 2008), predictive and reactive FMIPv6 (Koodli, 2008), F-HMIPv6 (Jung et al., 2005) are given in (Zhang & Pierre, 2008). The mobility signaling cost functions for predictive SMIPv6 (P-SMIPv6) and reactive SMIPv6 (R-SMIPv6) are expressed as follows (Zhang & Pierre, 2008; Zhang et al., 2010):

$$C^s_{P-SMIPv6} = R_c \times S_{P-SMIPv6} \times (1-q) \tag{14}$$

$$C^s_{R-SMIPv6} = R_c \times S_{R-SMIPv6} \times (1-q) \tag{15}$$

Where R_c is the cell crossing rate, i.e. the average number of crossings of the boundary of a cell per unit of time ($/s$), q is the probability that a mobile node remains in its current cell, $S_{P-SMIPv6}$ and $S_{R-SMIPv6}$ represent the mobility signaling overheads obtained from Equations (10) and (11).

4.2.2 Packet delivery cost

Packet delivery cost per session are defined as the cost of delivering a session from a source node to a destination node, which includes all nodes' processing costs and link transmission costs from the source to the destination.
We assume that HMIPv6 (Soliman et al., 2008), FMIPv6 (Koodli, 2008), F-HMIPv6 (Jung et al., 2005) and SMIPv6 (Zhang et al., 2005; Zhang & Marchand, 2009; Zhang & Pierre, 2008) support route optimization (RO). Under this mode, only the first packet of a session is transmitted to a home agent (HA) to detect whether a mobile node is away from its home network or not. All successive packets of the session are routed directly to the mobile's new location. Under the circumstance, the processing cost at a home agent is expressed as (Zhang & Pierre, 2008):

$$P_{HA} = \lambda_p \times \theta_{HA} \tag{16}$$

Where λ_p denotes the arrival rate of the first packet of a session, which is assumed to be the average packet arrival rate (packets per second). θ_{HA} indicates the unit cost for processing packets at the home agent (HA), which is assumed to be identical for all nodes' home agents.

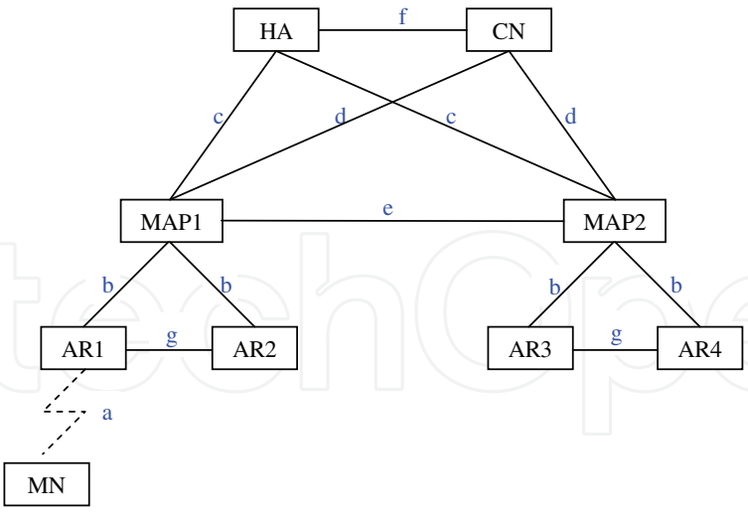


Fig. 5. Network topology for performance analysis

The packet delivery cost functions for MIPv6 with tunnel and RO modes, HMIPv6, FMIPv6 and F-HMIPv6 are given in (Zhang, 2008; Zhang & Pierre, 2008). The packet delivery cost for SMIPv6 is expressed as follows (Zhang & Pierre, 2008; Zhang et al., 2010):

$$C^{p}_{SMIPv6} = P_{AR} + C^{p}_{MIPv6-RO} + \tau \times \lambda_s \times d_{PAR-NAR} \tag{17}$$

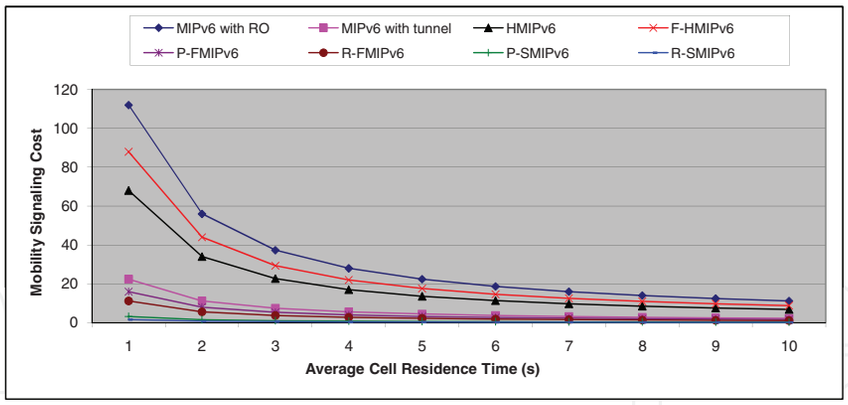
Where λ_s denotes the session arrival rate (packets per second), P_{AR} the processing cost at access router (AR), d_{x-y} the hop distance between network entities x and y, τ is the unit transmission cost in a wired link, and $C^{p}_{MIPv6-RO}$ represents the packet delivery cost for MIPv6 with route optimization (RO) mode.
Using SMIPv6 (Zhang et al., 2005; Zhang & Marchand, 2009; Zhang & Pierre, 2008), intelligent access routers manage Forwarding and Reverse Tunnels Lists, so the processing cost at an access router mainly comprises the lookup costs for searching such lists. We assume that such cost is proportional to the number of mobile nodes served by the access router, and identical for each access router. Accordingly, the processing costs at an access router can be expressed as follows (Zhang & Pierre, 2008):

$$P_{AR} = \lambda_s \times (\epsilon \times E_{MN}) \tag{18}$$

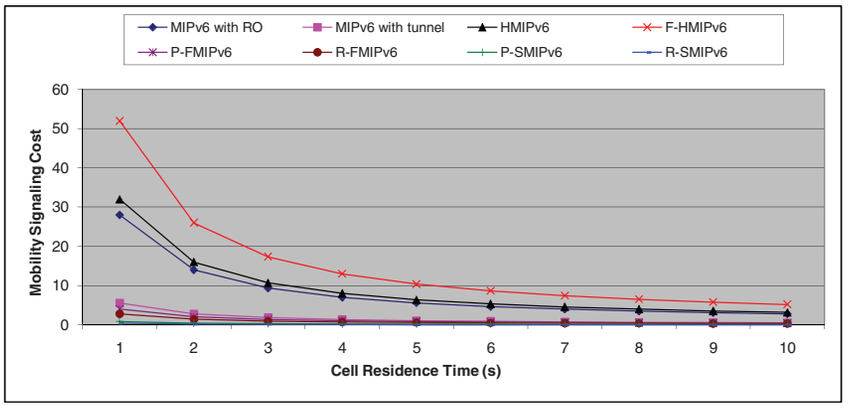
Where λ_s is the session arrival rate (packets per second), ϵ is a weighting factor showing the relationship between the lookup cost and size of the tunneling lists, and E_{MN} the average number of mobile nodes in a cell.

4.3 Numerical results

This section analyzes the impact of various wireless system parameters on the above-mentioned costs. The parameter values are taken from (Pack & Choi, 2003; Woo, 2003; Zhang et al., 2002), i.e. $\alpha = 0.1$ and $\beta = 0.2$, $\lambda_s = 1$, $\lambda_p = 0.1$, $\theta_{HA} = 20$, $\tau = 1$, $\kappa = 2$, $N_{CN} = 2$, $L_c = 120m$. The network topology is shown in Figure 5 (Zhang & Pierre, 2008). In addition, we fix the value of $\epsilon = 0.1$, $R = 20m$. The hop distance between different domains is assumed to be identical, i.e. $d_{HA-CN} = f = 6$, $d_{CN-MAP} = d = 4$, $d_{HA-MAP} = c = 6$, $d_{AR-MAP} = b = 2$, $d_{AR1-AR2} = d_{PAR-NAR} = 2$. And all links are assumed to be full-duplex in terms of capacity and delay.



(a) $q = 0.2$



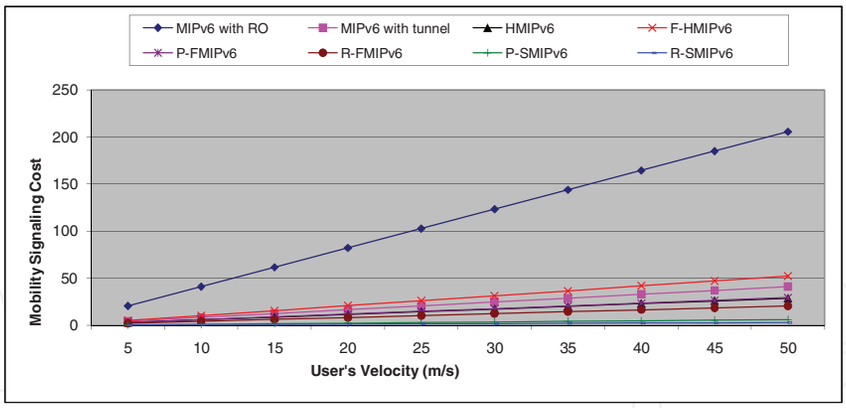
(b) $q = 0.8$

Fig. 6. Signaling cost vs. cell residence time

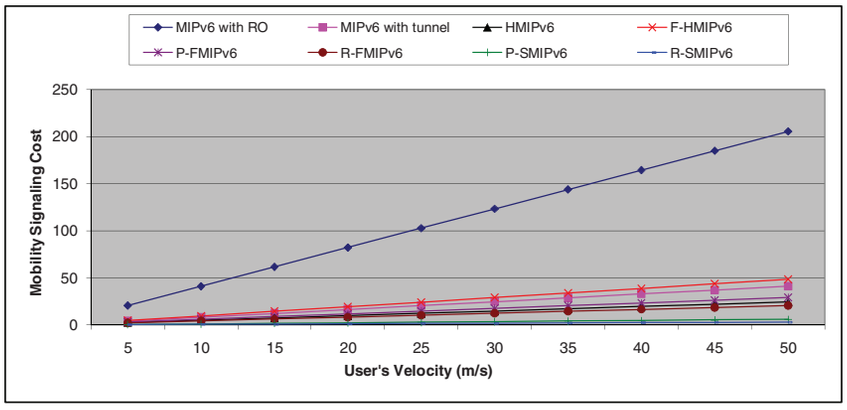
4.3.1 Signaling cost versus cell residence time

Figures 6.a and 6.b show the relationship between the mobility signaling cost and average cell residence time for $q = 0.2$ and $q = 0.8$, using the random-walk model. Mobile nodes are roaming in a mobility anchor point (MAP) domain with one ring. Note that q represents the probability that a mobile node remains in its current cell. Figure 6.a shows dynamic mobile users, who are eager to move to other cells, while Figure 6.b illustrates the mobility signaling costs for static mobile nodes. The longer a mobile node remains in a current cell, the lower the mobility signaling cost. We explain this as the mobile node is less likely to move between subnets, so fewer handoffs are required when the mobile stays longer in its current cell. In addition, both predictive and reactive SMIPv6 deliver better performance than MIPv6 and its extensions. On the other hand, MIPv6 (Johnson et al., 2004) with route optimization (RO) mode requires the most signaling cost when $q = 0.2$, and F-HMIPv6 (Jung et al., 2005) demonstrates the highest signaling cost when $q = 0.8$.

Compared with MIPv6 with RO mode, predictive SMIPv6 presents 97.13% less signaling cost for $q = 0.2$ and 97.20% less for $q = 0.8$; reactive SMIPv6 presents 98.57% less signaling cost for $q = 0.2$ and 98.54% less for $q = 0.8$. Compared with MIPv6 with tunnel mode, predictive SMIPv6 needs 85.67% less signaling cost for $q = 0.2$ and 85.98% less for $q = 0.8$; reactive SMIPv6 needs 92.84% less signaling cost for $q = 0.2$ and 92.68% less for $q = 0.8$.



(a) $n = 1$



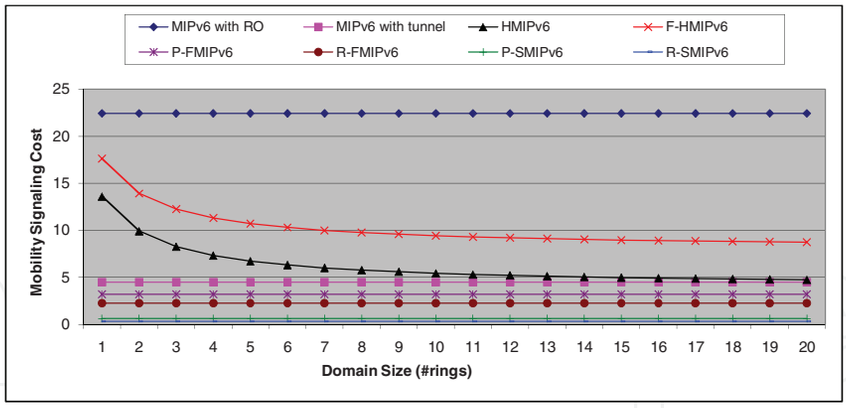
(b) $n = 4$

Fig. 7. Signaling cost vs. user's velocity

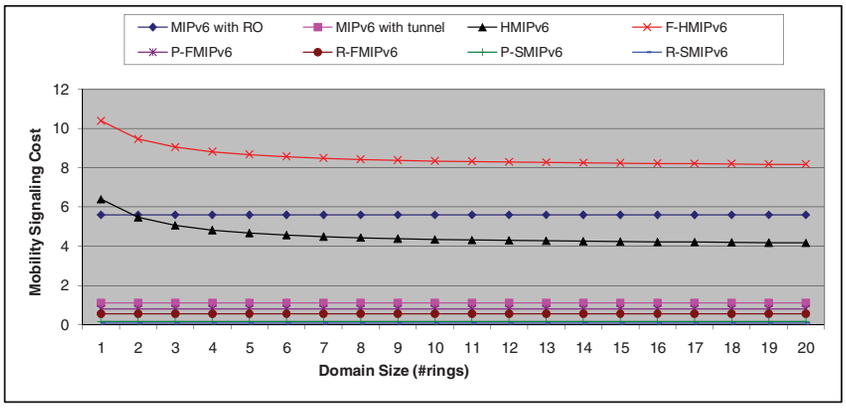
Compared with HMIPv6, predictive SMIPv6 requires 95.28% less signaling cost for $q = 0.2$ and 97.55% less for $q = 0.8$; reactive SMIPv6 requires 97.64% less signaling cost for $q = 0.2$ and 98.72% less for $q = 0.8$.
Compared with predictive FMIPv6, predictive SMIPv6 presents 79.96% less signaling cost for $q = 0.2$ and 80.34% less for $q = 0.8$; reactive SMIPv6 presents 89.98% less signaling cost for $q = 0.2$ and 89.74% less for $q = 0.8$. Compared with reactive FMIPv6, predictive SMIPv6 needs 71.34% less signaling cost for $q = 0.2$ and 71.95% less for $q = 0.8$; reactive SMIPv6 needs 85.67% less signaling cost for $q = 0.2$ and 85.37% less for $q = 0.8$.
Compared with F-HMIPv6, predictive SMIPv6 requires 96.35% less signaling cost for $q = 0.2$ and 98.49% less for $q = 0.8$; reactive SMIPv6 requires 98.18% less signaling cost for $q = 0.2$ and 99.21% less for $q = 0.8$.
Comparing the two figures, we find that increasing the probability that mobile nodes remain in their current cells leads to significant reduction of mobility signaling over the network. This is because mobile nodes are less likely to perform handoffs.

4.3.2 Signaling cost versus user velocity

Figures 7.a and 7.b demonstrate the relationship between the mobility signaling cost and user's average velocity for MAP domains of one ring and four rings, using the fluid-flow model (Zhang & Pierre, 2008). The probability that a mobile node remains at its current cell



(a) $q = 0.2$



(b) $q = 0.8$

Fig. 8. Signaling cost vs. domain size

is set to 0.2. A lower velocity leads to a lower cell and domain crossing rate and results in less signaling cost. In addition, we find that predictive and reactive SMIPv6 (Zhang & Pierre, 2008) deliver better performance than MIPv6 (Johnson et al., 2004) and its extensions.

For $n = 1$, shown in Figure 7.a, MIPv6 with route optimization (RO) mode engenders the most exorbitant cost, which rises to 113.12, on average. In comparison, F-HMIPv6 (Jung et al., 2005) climbs to 28.74; MIPv6 with tunnel mode needs 22.62; predictive FMIPv6 (P-FMIPv6) rises to 16.16, HMIPv6 (Soliman et al., 2008) requires 15.85, reactive FMIPv6 (R-FMIPv6) is about 11.31. However, the average signaling cost for predictive SMIPv6 (P-SMIPv6) is 3.23, and 1.62 for reactive SMIPv6 (R-SMIPv6).

Comparing the two figures, we find that increasing the MAP domain size leads to significant reduction of mobility signaling cost for localized domain-based mobility management schemes, such as HMIPv6 (Soliman et al., 2008) and F-HMIPv6 (Jung et al., 2005). We explain this as a mobile node roaming in a domain with larger size is less likely to perform inter-domain movements. As a result, Figure 7.b shows that F-HMIPv6 descends to 26.64, which presents 7.31% less signaling cost than that in Figure 7.a. At the same time, HMIPv6 descends to 13.38, on average. This presents 15.58% less signaling cost than that in Figure 7.a. However, signaling costs for other protocols remain unchanged while increasing the MAP domain size.

4.3.3 Signaling cost versus domain size

Figures 8.a and 8.b show the relationship between the mobility signaling cost and domain size for $q = 0.2$ and $q = 0.8$, using the random-walk model (Zhang & Pierre, 2008). The average cell residence time is set to $5s$. The larger the domain, the lower the mobility signaling cost for localized domain-based mobility protocols like HMIPv6 (Soliman et al., 2008) and F-HMIPv6 (Jung et al., 2005). However, the performance of MIPv6 (Johnson et al., 2004) with tunnel and RO modes, predictive and reactive FMIPv6, predictive and reactive and SMIPv6 remain unchanged while increasing the domain size; the same observation as that from Figures 7.a and 7.b. On the other hand, we find that SMIPv6 delivers better performance than other protocols.

For $q = 0.2$, the average signaling cost for MIPv6 with RO mode is 22.40; 10.22 for F-HMIPv6, 6.22 for HMIPv6, 4.48 for MIPv6 with tunnel mode, 3.20 for predictive FMIPv6 (P-FMIPv6) and 2.24 for reactive FMIPv6 (R-FMIPv6), 0.64 for predictive SMIPv6 (P-SMIPv6) and 0.32 for reactive SMIPv6 (R-SMIPv6). These values are shown in Figure 8.a.

For $q = 0.8$, the average signaling cost for F-HMIPv6 is 8.56, 5.60 for MIPv6 with RO mode; 4.56 for HMIPv6, 1.12 for MIPv6 with tunnel mode, 0.80 for predictive FMIPv6 (P-FMIPv6) and 0.56 for reactive FMIPv6 (R-FMIPv6), 0.16 for predictive SMIPv6 (P-SMIPv6) and 0.08 for reactive SMIPv6 (R-SMIPv6), as shown in Figure 8.b.

Comparing the two figures, we find that increasing the probability that mobile nodes remain in their current cells leads to significant reduction of signaling cost. This is because mobile nodes are less likely to perform handover from one cell to another.

4.3.4 Packet delivery cost versus session arrival rate

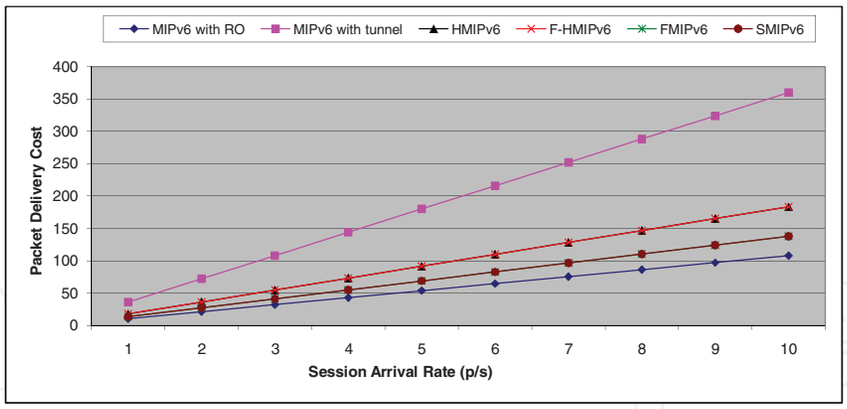
Figures 9.a and 9.b show the relationship between the packet delivery cost and session arrival rate for MAP domains with one ring and four rings (Zhang & Pierre, 2008). The average number of mobile nodes in a cell is set to 10. Generally, the higher the session arrival rate, the higher the packet delivery cost.

For MAP domains with 1 ring, MIPv6 with tunnel mode requires the highest costs amongst all schemes. We explain this as all of the session packets must cross a triangular path via a home agent, whose steep processing costs are detrimental. On the other hand, MIPv6 with route optimization (RO) mode delivers better performance than other approaches, since all the packets (except the first one) in a session are delivered to mobile nodes via a direct path, and there is no additional processing cost at the MAP neither at the access router. HMIPv6 (Soliman et al., 2008) and F-HMIPv6 (Jung et al., 2005) deliver identical performance, as do FMIPv6 (Koodli, 2008) and SMIPv6 (Zhang et al., 2005; Zhang & Marchand, 2009; Zhang & Pierre, 2008; 2009).

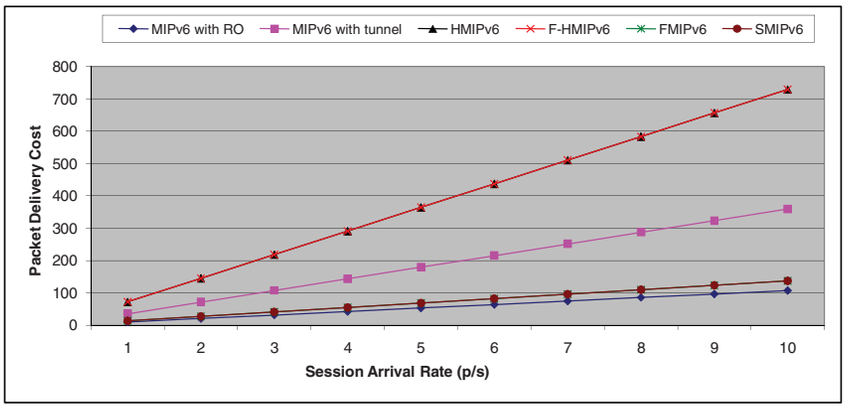
For MAP domains with 1 ring, shown in Figure 9.a, the mean packet delivery cost is 198.00 for MIPv6 with tunnel mode, 100.99 for F-HMIPv6 and HMIPv6, and 75.90 for FMIPv6 and SMIPv6, 59.40 for MIPv6 with RO mode.

For MAP domains with 4 ring, shown in Figure 9.b, the mean packet delivery cost is 401.42 for F-HMIPv6 and HMIPv6, which present 297.48% more cost for delivering packets. However, the performance of MIPv6, FMIPv6 and SMIPv6 remain unchanged while increasing the domain size; the same observation as that from Figures 7.a, 7.b, 8.a and 8.b.

The two figures also show that increasing the MAP domain size leads to a rapid augmentation of packet delivery cost for domain-based localized mobility management protocols, like F-HMIPv6 and HMIPv6; this is due to the processing cost at the MAP, especially the routing



(a) $n = 1$



(b) $n = 4$

Fig. 9. Packet delivery cost vs. session arrival rate

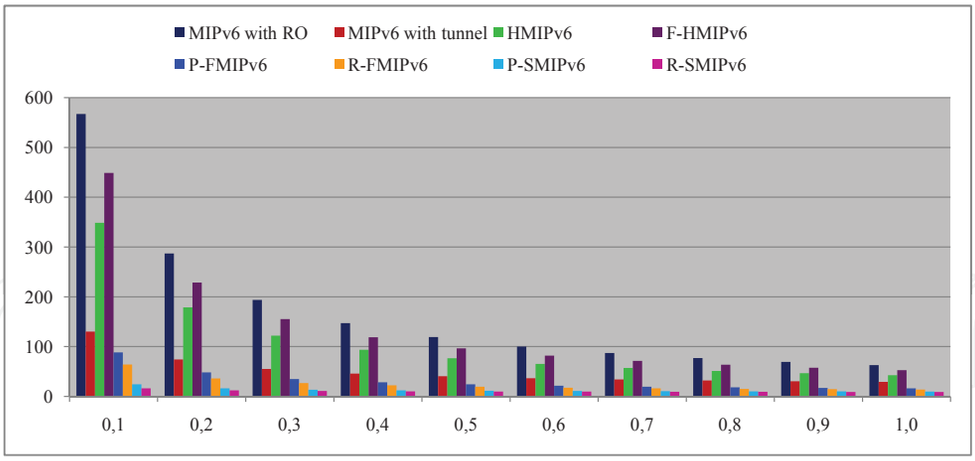
cost, which is proportional to the logarithm of the number of access routers in a MAP domain (Zhang & Pierre, 2008).

4.3.5 Total cost versus session-to-mobility ratio

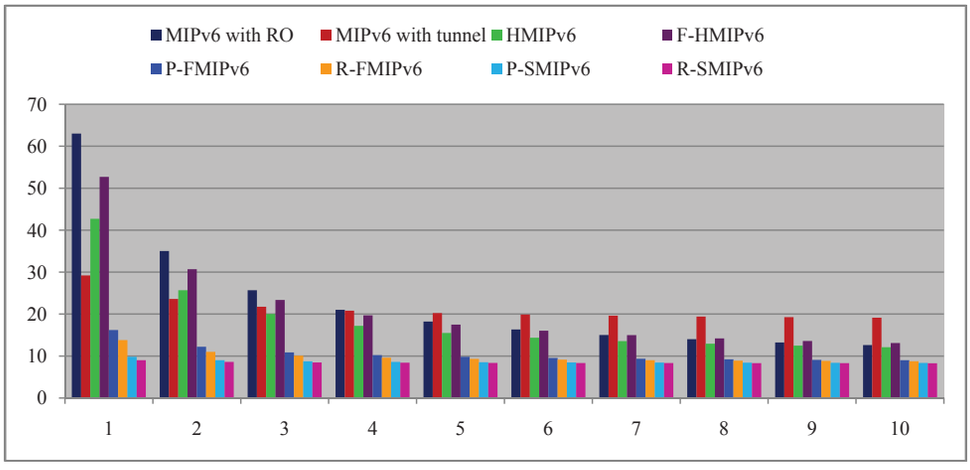
Figures 10.a and 10.b show the relationship between the total cost and average session-to-mobility ratio for MAP domains with one ring, using the random-walk model (Zhang & Pierre, 2008). The *session-to-mobility ratio* (SMR) is defined as the ratio of the session arrival rate to the user mobility ratio, it is analogous to the call-to-mobility ratio (CMR) used in cellular networks.

Under the random-walk model, $SMR = \frac{\lambda_s}{\frac{1}{E(T)}} = \lambda_s \times E(T)$, i.e. the session arrival rate divided by the cell crossing rate. E(T) denotes the average cell residence time. As the value of λ_s is fixed to 0.5, the augmentation of the SMR implies an increase of the cell residence time. as a result, reducing the total cost.

In case of $SMR \leq 1$, i.e. $\lambda_s \leq \frac{1}{E(T)}$, the mobility signaling cost is more dominant than packet delivery cost over the total cost, shown in Figure 10.a. Under this circumstance, MIPv6 with RO mode has the highest total cost amongst all schemes. The total cost in descent order is MIPv6 with RO mode (171.02, on average), F-HMIPv6 (137.56), HMIPv6 (108.27), MIPv6 with



(a) $SMR \leq 1$



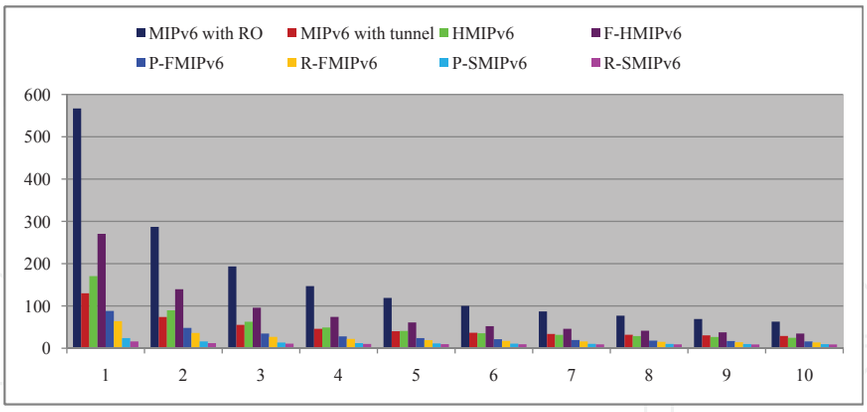
(b) $1 \leq SMR \leq 10$

Fig. 10. Total cost vs. SMR for $n = 1$

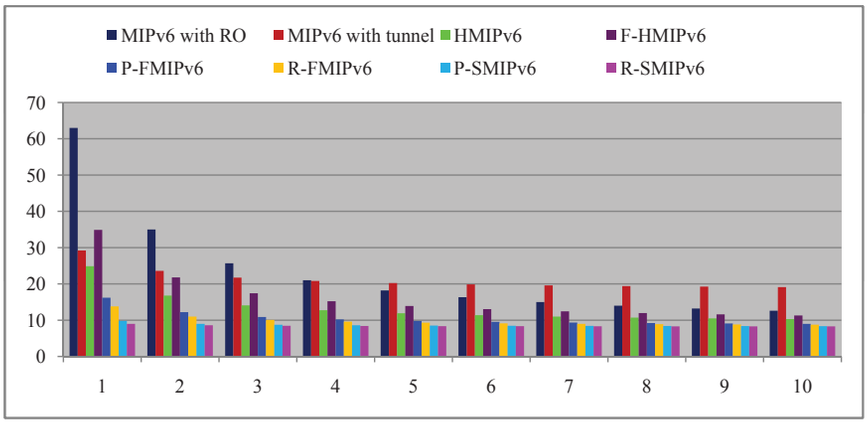
tunnel mode (50.80), predictive FMIPv6 (31.63), reactive FMIPv6 (24.60), predictive SMIPv6 (12.89), and reactive SMIPv6 (10.54).

In addition, as $SMR \geq 1$, the impact of mobility signaling cost on the total cost reduces while packet delivery cost becomes more important over the total cost. The higher the SMR, the more important is the packet delivery cost over the total cost. As a result, when $SMR \geq 5$, MIPv6 with tunnel mode requires the highest cost than other protocols. The total cost on average in descent order is MIPv6 with RO mode (23.40), F-HMIPv6 (21.57), MIPv6 with tunnel mode (21.28), HMIPv6 (18.64), predictive FMIPv6 (10.54), reactive FMIPv6 (9.84), predictive SMIPv6 (8.67), and reactive SMIPv6 (8.43). Such values are shown in Figure 10.b. Besides, SMIPv6 yields the best performance amongst all schemes, due to lower signaling cost and no additional processing cost at the MAP.

Figures 11.a and 11.b also illustrate the variation of total cost as the average session-to-mobility ratio changes for MAP domains with four rings, using the random-walk model. The total cost decreases as the SMR augments, the same observation applies to Figures 10.a and 10.b. Besides, increasing the MAP domain size leads to a reduction of total cost for HMIPv6 and F-HMIPv6, yet no impact on MIPv6, FMIPv6 and SMIPv6 protocols.



(a) $SMR \leq 1$



(b) $1 \leq SMR \leq 10$

Fig. 11. Total cost vs. SMR for $n = 4$

In case of $SMR \leq 1$, the total cost in descent order is MIPv6 with RO mode (171.02, on average), F-HMIPv6 (85.41), HMIPv6 (56.12), MIPv6 with tunnel mode (50.80), predictive FMIPv6 (31.63), reactive FMIPv6 (24.60), predictive SMIPv6 (12.89), and reactive SMIPv6 (10.54). We find that F-HMIPv6 presents 37.91% less total cost than that shown in Figure 10.a and HMIPv6 presents 48.17% less total cost than that shown in Figure 10.a.
However, with $SMR \geq 1$, the total cost in descent order is MIPv6 with RO mode (23.40), MIPv6 with tunnel mode (21.28), F-HMIPv6 (16.35), HMIPv6 (13.42), predictive FMIPv6 (10.54), reactive FMIPv6 (9.84), predictive SMIPv6 (8.67), and reactive SMIPv6 (8.43). Such values are shown in Figure 11.b. This is because the impact of packet delivery cost over total cost increases as SMR augments. When $SMR \geq 5$, MIPv6 with tunnel mode requires the highest cost than other protocols. We also observe that predictive FMIPv6 tends to deliver the same performance as reactive FMIPv6, and predictive SMIPv6 tends to provide the same performance than reactive SMIPv6, shown in Figure 11.b.

5. Conclusion

This chapter proposes a new seamless mobility management protocol, called SMIPv6. The novelty of this protocol consists of pre-configuring bidirectional secure tunnels before handoff and utilizing such tunnels to accelerate mobility management procedure during handoff. To

evaluate the efficiency of the proposal, we employ analytical models, numerical results show that SMIPv6 delivers better performance than MIPv6 and its extensions.
Even though SMIPv6 delivers better performance than MIPv6 (Johnson et al., 2004) and its enhancements such as HMIPv6 (Soliman et al., 2008), FMIPv6 (Koodli, 2008) and F-HMIPv6 (Jung et al., 2005), we notice that such schemes are always host-centric. They require mobile nodes to signal mobility to other network entities. In addition, this chapter only focuses on mobility management issue without considering security aspect. In fact, each time before mobile users obtains a service from the visiting network, they have to undergo authentication and authorization procedure. This results in additional delays. Accordingly, new fast authentication protocol is required for seamless mobility management.

6. References

Akyildiz, I.F., McNair, J., Ho, J.S.M., Uzunalioglu, H. & Wang, W. (1999). Mobility management in next-generation wireless systems, *Proceedings of the IEEE*, Vol. 87, No. 8, pp. 1347-1384, ISSN: 0018-9219.

Akyildiz, I.F., Mohanty, S. & Xie, J. (2005). Ubiquitous mobile communication architecture for next-generation heterogeneous wireless systems, *IEEE Communications Magazine*, Vol. 43, No. 6, pp. 529-536, ISSN: 0163-6804.

Akyildiz, I.F. & Wang, W. (2002). A dynamic location management scheme for next-generation multitier PCS systems, *IEEE Transactions on Wireless Communications*, Vol. 1, No. 1, pp. 178-189, ISSN: 1536-1276.

Akyildiz, I.F., Xie, J. & Mohanty, S. (2004). A survey of mobility management in nextgeneration all-IP-based wireless systems, *IEEE Wireless Communications*, Vol. 11, No. 4, pp. 16-28, ISSN: 1536-1284.

Arkko, J., Vogt, C. & Haddad, W. (2007). Enhanced route optimization for mobile IPv6, RFC 4866, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc4866.txt.

Campbell, A.T., Gomez, J., Kim, S., Wan, C.-Y., Turanyi, Z.R. & Valko, A.G. (2002). Comparison of IP micro-mobility protocols, *IEEE Wireless Communications*, Vol. 9, No. 1, pp. 72-82, ISSN: 1536-1284.

Devarapalli, V., Wakikawa, R., Petrescu, A. & Thubert, P. (2005). Network mobility (NEMO) basic support protocol, RFC 3963, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc3963.txt.

Dimopoulou, L., Leoleis, G. & Venieris, I. S. (2005). Fast handover support in a WLAN environment: challenges and perspectives, *IEEE Network*, Vol. 19, No. 3, pp. 14-20, ISSN: 0890-8044.

Ernst, T. & Lach, H.-Y. (2007). Network mobility support terminology, RFC 4885, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc4885.txt.

Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K. & Patil, B. (2008). Proxy mobile IPv6, RFC 5213, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc5213.txt.

Gwon, Y. & Yegin, A. (2004). Enhanced forwarding from the previous care-of address (EFWD)for fast handovers in mobile IPv6, *Proceedings of 2004 IEEE Wireless Communications and Networking* (IEEE WCNC 2004), pp. 861-866, ISBN: 0-7803-8344-3, Atlanta, Georgia, USA, 21-25 March 2004, IEEE.

Gwon, Y., Kempf, J. & Yegin, A. (2004). Scalability and robustness analysis of mobile IPv6, fast mobile IPv6, hierarchical mobile IPv6, and hybrid IPv6 mobility protocols using a large-scale simulation, *Proceedings of 2004 IEEE International Conference on*

Communications (ICC 2004), pp. 4087-4091, ISBN: 0-7803-8533-0, Paris, France, 20-24 June 2004, IEEE.

Haseeb, S. & Ismail, A.F. (2007). Handoff latency analysis of mobile IPv6 protocol variations, *Computer Communications*, Vol. 30, No. 4, pp. 849-855, ISSN: 0140-3664.

Johnson, D., Perkins, C. & Arkko, J. (2004). Mobility support in IPv6, RFC 3775, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc3775.txt.

Jung, H.Y., Kim, E.A., Yi, J.W. & Lee, H.H. (2005). A scheme for supporting fast handover in hierarchical mobile IPv6 networks, *ETRI Journal*, Vol. 27, No. 6, pp. 798-801.

Kempf, J., Calhoun, P., Dommety, G., Thalanany, S., Singh, A., McCann, P.J. & Hiller, T. (2001). Bidirectional edge tunnel handover for IPv6, draft, Internet Engineering Task Force. URL: http://tools.ietf.org/id/draft-kempf-beth-ipv6-02.txt.

Kempf, J., Wood, J. & Fu, G. (2003). Fast mobile IPv6 handover packet loss performance: measurements for emulated real time traffic, *Proceedings of 2003 IEEE Wireless Communications and Networking* (WCNC 2003), pp. 1230-1235, ISBN: 0-7803-7700-1, New Orleans, Louisiana, USA, 20-20 March 2003, IEEE.

Kent, S. (2005). IP encapsulating security payload (ESP), RFC 4303, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc4303.txt.

Koodli, R. (2008). Mobile IPv6 fast handovers, RFC 5268, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc5268.txt.

Loughney, J., Nakhjiri, M., Perkins, C. & Koodli, R. (2005). IP mobility support, RFC 4067, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc4067.txt.

Makaya, C. & Pierre, S. (2008). An architecture for seamless mobility support in IP-based nextgeneration wireless networks, *IEEE Transactions on Vehicular Technology*, Vol. 57, No. 2, pp. 1209-1225, ISSN: 0018-9545.

Manner, J. & Kojo, M. (2004). Mobility related terminology, RFC 3753, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc3753.txt.

McNair, J. & Zhu, F. (2004). Vertical handoffs in fourth-generation multinetwork environments, *IEEE Wireless Communications*, Vol. 11, No. 3, pp. 8-15, ISSN: 1536-1284.

Mohanty, S. & Xie, J. (2007). Performance analysis of a novel architecture to integrate heterogeneous wireless systems, *Computer Networks*, Vol. 51, No. 4, pp. 1095-1105, ISSN: 1389-1286.

Narten, T., Nordmark, E., Simpson, W. & Soliman, H. (2007). Neighbor discovery for IP version 6 (IPv6), RFC 4861, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc4861.txt.

Nasser, N., Hasswa, A. & Hassanein, H. (2006). Handoffs in fourth generation heterogeneous networks, *IEEE Communications Magazine*, Vol. 44, No. 10, pp. 96-103, ISSN: 0163-6804.

Pack, S. & Choi, Y. (2003). Performance analysis of hierarchical mobile IPv6 in IP-based cellular networks, *Proceedings of 2003 IEEE Conference on Personal, Indoor and Mobile Radio Communications* (PIMRC 2003), pp. 2818-2822, ISBN: 0-7803-7822-9, Beijing, China, 7-10 September 2003, IEEE.

Perez-Costa, X. & Hartenstein, H. (2002). A simulation study on the performance of mobile IPv6 in a WLAN-based cellular network, *Computer Networks*, Vol. 40, No. 1, pp. 191-204, ISSN: 1389-1286.

Perez-Costa, X., Torrent-Moreno, M. & Hartenstein, H. (2003). A performance comparison of mobile IPv6, hierarchical mobile IPv6, fast handovers for mobile IPv6 and their

combination, *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol. 7, No. 4, pp. 5-19, ISSN: 1559-1662.

Perkins, C. (1996). IP mobility support, RFC 2002, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc2002.txt.

Perkins, C. (2002). IP mobility support for IPv4, RFC 3344, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc3344.txt.

Quintero, A., Garcia, O. & Pierre, S. (2004). An alternative strategy for location update and paging in mobile networks, *Computer Communications*, Vol. 27, No. 15, pp. 1509-1523.

Ramjee, R., Varadhan, K., Salgarelli, L., Thuel, S.R., Wang, S.-Y. & La-Porta, T. (2002). HAWAII: a domain-based approach for supporting mobility in wide-area wireless networks, *IEEE/ACM Transactions on Networking*, Vol. 10, No. 3, pp. 396-410, ISSN: 1063-6692.

Soliman, H., Castelluccia, C., El-Malki, K. & Bellier, L. (2008). Hierarchical mobile IPv6 (HMIPv6) mobility management, RFC 5380, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc5380.txt.

Soto, I., Bernardos, C., Calderon, M., Banchs, A. & Azcorra, A. (2009). NEMO-enabled localized mobility support for Internet access in automotive scenarios, *IEEE Communications Magazine*, Vol. 47, No. 5, pp. 152-159, ISSN: 0163-6804.

Thomson, S., Narten, T. & Jinmei, T. (2007). IPv6 stateless address autoconfiguration, RFC 4862, Internet Engineering Task Force. URL: http://tools.ietf.org/rfc/rfc4862.txt.

Valko, A.G. (1999). Cellular IP : a new approach to Internet host mobility, *ACM SIGCOMM Computer Communication Review*, Vol. 29, No. 1, pp. 50-65, ISSN: 0146-4833.

Woo, M. (2003). Performance analysis of mobile IP regional registration, *IEICE Transactions on Communications*, Vol. E86-B, No. 2, pp. 472-478, ISSN: 0916-8516.

Zhang, L.J. (2008). Fast and seamless mobility management in IPv6-based next-generation wireless networks, *PhD thesis*, Ecole Polytechnique de Montreal, Montreal, Canada.

Zhang, L.J. & Marchand, L. (2006). Tunnel establishment, *US Patent Application*, US 11/410,205. Filed on April 25, 2006.

Zhang, L.J., Marchand, L. & Pierre, S. (2005). Optimized seamless handover in mobile IPv6 networks, *US Patent*, US 60/674,356 . Published on April 25, 2005.

Zhang, L.J. & Marchand, L. (2009). Handover enabler, *US Patent*, US 7,606,201 B2. Published on October 20, 2009.

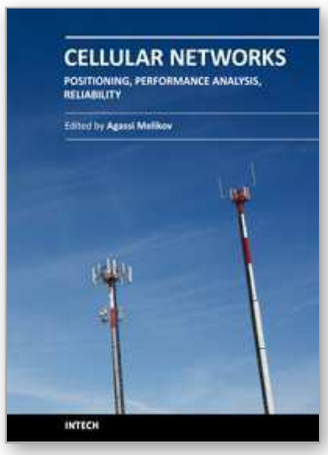
Zhang, L.J. & Pierre, S. (2008). Evaluating the performance of fast handover for hierarchical MIPv6 in cellular networks, *Journal of Networks*, Vol. 3, No. 6, pp. 36-43, ISSN: 1796-2056.

Zhang, L.J. & Pierre, S. (2009). *Next-Generation Wireless Networks: Protocols, Architectures, Standards, Mobility and Performance*, LAP LAMBERT Academic Publishing, ISBN: 3-8383-1906-0, Cologne, Germany.

Zhang, L.J., Zhang, L., Marchand, L. & Pierre, S. (2010a). A survey of IP-layer mobility management protocols in next-generation wireless networks, in *Next Generation Mobile Networks and Ubiquitous Computing*, Samuel Pierre (ed.), chapter 9, Information Science Publishing, ISBN: 1-6056-6250-X, Hershey, PA, USA.

Zhang, L.J., Zhang, L., Marchand, L. & Pierre, S. (2010b). Mobility management protocols design for IPv6-based wireless and mobile networks, in *Fixed Mobile Convergence Handbook*, Syed A. Ahson & Mohammad Ilyas, (Ed.), chapter 9, CRC Press, Taylor & Francis Group, ISBN: 1-4200-9170-0, New York, NY, USA.

Zhang, X., Castellanos, J.G. & Campbell, A.T. (2002). P-MIP: paging extensions for mobile IP, *Mobile Networks and Applications*, Vol. 7, No. 2, pp. 127-141, ISSN: 1383-469X.



Cellular Networks - Positioning, Performance Analysis, Reliability
Edited by Dr. Agassi Melikov

ISBN 978-953-307-246-3
Hard cover, 404 pages
Publisher InTech
Published online 26, April, 2011
Published in print edition April, 2011

Wireless cellular networks are an integral part of modern telecommunication systems. Today it is hard to imagine our life without the use of such networks. Nevertheless, the development, implementation and operation of these networks require engineers and scientists to address a number of interrelated problems. Among them are the problem of choosing the proper geometric shape and dimensions of cells based on geographical location, finding the optimal location of cell base station, selection the scheme dividing the total net bandwidth between its cells, organization of the handover of a call between cells, information security and network reliability, and many others. The book focuses on three types of problems from the above list - Positioning, Performance Analysis and Reliability. It contains three sections. The Section 1 is devoted to problems of Positioning and contains five chapters. The Section 2 contains eight Chapters which are devoted to quality of service (QoS) metrics analysis of wireless cellular networks. The Section 3 contains two Chapters and deal with reliability issues of wireless cellular networks. The book will be useful to researches in academia and industry and also to post-gradute students in telecommunication specialitiies.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821