This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2010 proceedings

Virtual ID: A Technique for Mobility, Multi-Homing, and Location Privacy in Next Generation Wireless Networks

Chakchai So-In, *Student Member*, *IEEE*, and Raj Jain, *Fellow, IEEE*
Subharthi Paul and Jianli Pan, *Student Members, IEEE*

***Abstract*—Cellular networking standards organizations such as the 3rd Generation Partnership Project (3GPP) are currently developing System Architecture Evolution (SAE) as their core network architecture. SAE is all-IP based. However, IP-based networks face several known issues, such as mobility, multi-homing, location privacy, path preference, etc. Mobile IP (MIP) and its variants, such as Mobile IPv6 (MIPv6), Hierarchical MIP, and Proxy MIP, have been developed primarily to alleviate the mobility problem. These variation and extensions, however, still do not provide many of the features required in Next Generation Wireless Networks (NGWN). The limitations are especially due to the overloading of IP addresses as both node identity and locator. In this paper, we propose an extension to MIPv6 called Virtual ID. This concept applies the ID/Locator split idea into a Mobile IPv6 environment. Virtual ID and its extensions provide many features that would be desired in the NGWN. Since our proposed scheme is based on the standard MIPv6 and Proxy MIPv6, the scheme is fully compatible with the legacy MIPv6.**

***Index Terms*—Mobile IP, Virtual Identity, Mobility, Multi-Homing, User Location Privacy, NGWN, ID/Locator Split.**

I. Introduction

System Architecture Evolution (SAE) is the core networking architecture being developed by the 3rd Generation Partnership Project (3GPP) [1] for the next generation of cellular wireless networks. SAE is all-IP based. In this paper, we discuss issues that the next generation wireless networks (NGWN) will face after SAE deployment. We call these post-SAE networks. These networks, which will result from converging wired and wireless networks, will include a variety of wireless technologies such as cellular networks (2G/3G/4G), wireless broadband networks (e.g., Mobile WiMAX and LTE), wireless sensor networks, and so on. The interoperability among traditional wired networks, such as Ethernet, and wireless technologies also needs to be maintained. The applications on these networks may include voice, video, TV broadcasting, online games, and data services with a guaranteed quality of service (QoS).

With the emergence of billions of mobile users and wireless devices, scalability and deployability issues arise and will need to be considered when designing the next generation networks. Compared to wired networks, the channel capacity in wireless networks is not constant over time and distance. In addition, mobile users may move from one location to another at a high speed. As a result, disruptions may occur more frequently. Therefore, mobility is clearly one of the key issues in the NGWN.

With the advance of networking technologies, multiple networking interfaces with different combination of wired and wireless technologies are becoming common. So the issue of multi-homing, especially device and user multi-homing, will play an important role in backup, load balancing, sharing, and traffic engineering in future networks. The networks are becoming more user-centric, that is, they will allow users to make their own decisions. Network service providers may only provide suggestions with inherent security. For example, with multiple networking interfaces in a single mobile device, the mobile users may choose their preferred paths for each task, probably based on the price paid and on the quality of the service offered by various service providers. The users may be required to pay air-time charges, similar to a traditional cellular phone system. In addition, users may want to keep their location information private from their correspondent users. This is the so-called user location privacy issue. Finally, the security of data is always of concern to users.

The issues we have described above: mobility, multi-homing, scalability, security, deployability, and user location privacy, are key required for the design of next generation networks. Since future networks are expected to be all-IP based, the question is how to make them support these features.

There have been many attempts to resolve some of these key issues, especially in traditional all-IP based wired-networks [2, 3, 4]. However, no clear consensus has been reached. The problem is more serious within the mobile wireless environment. In the current Internet, the main hurdle in resolving the mobility and multi-homing issues is the overloading of IP addresses as both identity and location [2, 3]. The techniques to resolve these problems are based on redirection and indirection techniques [2, 3]. The main differences among these techniques are their varying focuses *on the different protocol layers, on the introduction of new naming spaces, on the required changes of a protocol stack, and on the ways to separate a host's identity from its locator*. We will briefly discuss the detailed concepts. Mobile IP [5 to 9] is another well known approach primarily designed to

Manuscript received September 7, 2009, revised October 15, 2009.

Corresponding authors: C. So-In, R. Jain, S. Paul, and J. Pan are with the Computer Science and Engineering Department, Washington University in St. Louis, MO 63143 USA (e-mail: cs5, jain, paul, and jp10@cse.wustl.edu).

resolve the mobility issue. However, Mobile IP and its extensions fail to fully support important other features for NGWN.

In this paper, our focus is on a network layer approach to mobility. A key advantage of this approach is that the network-layer based solutions require no change in the higher layers of the protocol stack, and so the solutions work for all applications. We apply the ID/locator split idea explicitly into the Mobile IP, especially for a mobile wireless environment. We introduce Virtual ID as a node identity for the mobile user. This add-on feature makes Mobile IPv6 to fully support mobility, multi-homing, and user location privacy. This concept and its extensions are built on the standard Mobile IPv6 and Proxy MIPv6. Note that several other proposals focus on scalability (e.g., the use of DNS and provider-aggregatable addresses) and security, such as IPsec and secure Mobile IP signaling. We do not handle these issues in this paper.

This paper is organized as follows. In Section II, we briefly describe the general concept of ID/locator split approaches as well as the pros and cons of these approaches in terms of mobility, multi-homing as well as user path preference, and user location privacy. In Section III, we discuss Mobile IPv6 and its variants considering these criteria. Then, in Section IV we introduce Virtual ID and its extensions by applying the concept of the ID/locator split into Mobile IPv6, to fully support user mobility, multi-homing as well as user path preference, and user location privacy. We illustrate these Virtual ID ideas with several detailed examples in Section V. Finally, the conclusions are discussed in Section VI.

II. ID/LOCATOR SPLIT

The ID/locator split [5, 6] is a well-known approach used to resolve both mobility and multi-homing issues. Basically, the idea is to separate the functionality of the identity from that of the locator. Each mobile node (MN) has its own unique identity. When the node moves, its identity does not change, but its locator does. The identity can be a string of characters or digits. The locator represents the current point of attachment to the network. In other words, the locator helps decide where the packet should be routed.

Currently, there are two ways to implement an ID/locator split: placing a split in the end host (e.g., HIP, SHIM6, and MILSA, etc. [2]) or in the network (LISP [2]). The former approach requires the insertion of a new ID sub-layer usually between the transport and the network layers. Thus, the upper layers are bound to an ID instead of locator. HIP and MILSA introduce new secure naming spaces but SHIM6 uses one of its current locators as the identity.

Note that although these splitting techniques can support full mobility, multi-homing, and location privacy since the identity is used instead of the node location, such indirection mechanisms also require new naming and name resolution mechanisms. In addition, there is no detailed discussion of the path selection issue. The second set of splitting techniques implements an ID/locator split in the network. The basic idea is that there is no change to the end host. The routers take care of the split. At the edge of the network, the IDs are resolved into the locators needed for communication. This requires changes to network infrastructure devices (routers).

III. MOBILE IPV6 AND ITS VARIANTS

Mobile IP (MIP) [5, 6] and its variants are well-known techniques designed to resolve the mobility problem in traditional wired and wireless networks. 3GPP has adopted these concepts for System Architecture Evolution (SAE). Most of the concepts discussed in this paper apply to both IPv4 and IPv6. However, for simplicity, we limit our discussion to IPv6 since it has sufficient address space and is preferred for public wireless networks.

Consider mobility. If nodes change their networks and/or locations, then their IP addresses also change. Consequently, their TCP connections at the transport layer are broken. The Mobile IPv6 is potentially used to maintain the connection and/or session regardless of time and location with an IP-in-IP encapsulation technique. In other words, the Mobile IPv6 is used to preserve the connection.

Briefly, the Mobile IPv6 functions as follows: the node's home IP address is used as the node's identity. When the node moves from one network to another network, it informs its home network (home agent, HA) about its new IP address (care-of-address or CoA). In case a correspondent node (CN) wants to contact this node, the CN sends packets to the home network; the packet is intercepted by the home agent and forwarded to the mobile node's new address (CoA).

Several extensions of Mobile IP have been proposed to mitigate the route-to-home network delay and/or hand-off latency such as HAWAII, Cellular IP, and HMIP (Hierarchical MIP) [7]. These approaches deploy several home agents in a hierarchical manner, especially at the edge routers. With HMIP, the binding update is sent to the local HA, which decreases delay latency. However, these approaches require synchronization among HAs and additional nodes.

Proxy-MIP [8] was originally introduced to improve the deployability of MIP. The idea is to use the router or proxy agent to act on behalf of the mobile node and to perform the MIP functionality. In other words, with the Proxy-MIP, the mobile node does not need to support the MIP.

Now let us consider multi-homing and user path preference. Mobile IPv6 can't support multi-homing because each single mobile node is bound to only one IP address. Recently, some have suggested allowing multiple care-of-addresses registrations [9] to allow multi-homing. There is no detailed discussion on user path selection issue.

Consider user location privacy. When nodes move away from their home networks, Mobile IP implicitly supports location privacy because the current location is no longer bound to the home address. However, this scenario introduces a triangular routing problem as indicated earlier. This problem can be mitigated using HMIP to reduce the delay latency by placing the home agent close to both the MN and the CN. In Mobile IPv6, a route optimization feature was introduced to resolve this triangular routing problem, that is, to allow the MN and CN to communicate to each other directly. But again, this direct communication introduces the user location privacy issue for mobile users.

In summary, a traditional Mobile IPv6 and its variants - Proxy MIPv6 and Hierarchical MIPv6 - fail to provide a full support for mobility, multi-homing, and user location privacy. In next section, then we introduce the concept of Virtual ID and its extensions to overcome these drawbacks of the traditional Mobile IPv6 by applying the concept of ID/locator split explicitly to a Mobile IPv6 environment.

IV. VIRTUAL ID AND ITS EXTENSIONS

In this section, we first describe the idea of Virtual Identity (ID) applied to Mobile IPv6. We also discuss how to apply this concept to solve two different problems: user location privacy and multi-homing.

A. Virtual ID

In IPv6, a 128-bit address is used for both node identity and locator which introduces many disadvantages, as indicated earlier. In a mobile wireless environment, Mobile IPv6 also mixes these functionalities. When the mobile node is in the home network, a single IPv6 home address represents both node identity and locator. But when the mobile node is outside the home network, Mobile IPv6 can be treated as an ID/Locator split scheme because another IP address, CoA, is involved. This CoA can be treated as the node locator (the indicator of where the node is). The node's home address does not change with its location and, therefore, serves as the node's identity.

To clearly separate the function of identity from that of locator in Mobile IPv6, we introduce the concept of a "virtual home address". Similar to SHIM6, this 128-bit address format is used to represent the node's identity. However, we do not use one of the node current addresses as its identity. Instead, we use the virtual home address, called virtual ID.

The virtual ID is pre-defined and randomly assigned by the service provider. This ID is permanent and thus no longer bound to the home networks and/or locations. In other words, the virtual ID is used even when the mobile node resides in the home network. As in Mobile IPv6, the IP-in-IP encapsulation is applied in that the nodes update their CoAs when they are in different location/networks.

We use the 128-bit IPv6 address format to represent the node's identity. This allows backward compatibility since legacy nodes (virtual ID unaware nodes) treat these identities as addresses.

B. User Location Privacy

The concept of the virtual ID formed by separating the node identity from its location helps to resolve the issue of user location privacy in that the correspondent nodes do not know the location of the mobile node; only the node identity. Note that basically there are two levels of mapping: from node name (FQDN) to node identity, and then from node identity to node location. The result of the DNS resolution is the node's identity, not its location. The other mapping level can be done at rendezvous servers. In a Mobile IPv6 environment, the home agent does the second level mapping. With Virtual ID, an additional mapping from the virtual home address to the Mobile IPv6 home address is also required. Optional additional mapping servers or extensions of the home agent can do this mapping.

The correspondent nodes are required to send the packets through the mobile node's home network. Therefore, there is a triangulation issue, as discussed earlier. To solve this problem, we propose an add-on feature to Proxy Mobile IPv6 [9]. Traditionally, in Proxy MIPv6, a mobile access gateway or proxy node is used to provide Mobile IP functionality on behalf of Mobile-IP unaware nodes. In this add-on, the mobile nodes no longer require the location information; instead the proxy node does this work. The proxy can optionally rewrite the address with its selected anonymity proxy address to hide the exact location or CoA in case the Mobile IP functionality is performed at the end node.

C. Multi-Homing

In NGWN, mobile users will want to exercise user path selection because they will have to pay for their choices according to bandwidth constraints and other quality of service controls. For example, suppose Alice buys access services from two different service providers: one services a 3G network accessible to her cellular phone; the other is over WLAN. When she is at home or when WLAN is available, Alice would prefer accessing the Internet service through WLAN and also probably disable the 3G service, especially when air-time charges are high.

To meet these requirements of multi-homing and user path selection, again a 128 bits Virtual ID is used as the unique identity. We do not change the identity regardless of the networks and/or locations. Only the physical locations or care-of-addresses can be changed with a change of locations. Unlike SHIM6, we do not change the protocol stack, but instead we apply the concept of multiple CoAs registrations at the home agent to support multi-homing feature [9].

In NGWN, users should be able to choose both their own ingress and egress paths, based on the price paid and the quality of service constraints. For simplicity, we use a weight factor along with the CoA registration when the nodes update the address to the home agent. In a more general case, the users could specify a set of connection rules. The home agent will forward the packets to the node according to pre-selected user path rules.

V. VIRTUAL ID AND ITS EXTENSIONS: EXAMPLES

In this section, we provide detailed examples for the Virtual ID concept and its extension. For user location privacy, we show that the concept of Virtual ID can protect the user location information. We also show that home agent chaining can be used to support user and/or device multi-homing as well as how to support a user path selection feature.

A. Virtual ID Example

Fig. 1 shows an example of Virtual ID. In this figure, Alice's node's name is *Alice.xyz.com* registered at a domain name server or DNS. The service provider (SP) allocates a virtual address (Virtual ID), *::10.2.1.2*, as Alice's identity. Suppose the SP networks are *::10.x.x.x* with *::10.3.x.x* and

::10.4.x.x sub-networks assigned into different physical regions. The virtual addresses *::10.2.x.x* are specifically dedicated as the virtual ID. Only the SP knows the mapping between the virtual ID or node identity (*::10.2.1.2*) and the physical address (*::10.3.1.2*) or current IP address. This mapping can be stored at rendezvous servers.

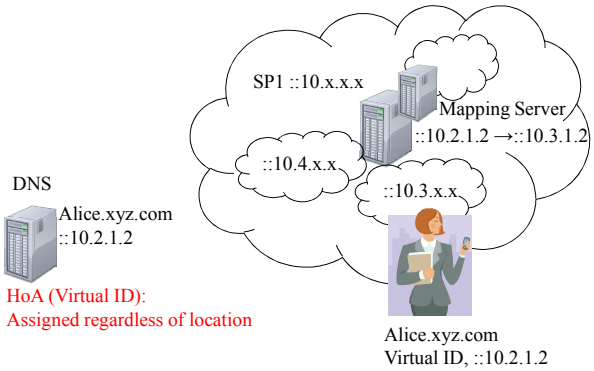

Fig. 1. Virtual ID Example

B. User Location Privacy Example

This section describes two main scenarios that use Virtual ID to achieve a user location privacy requirement in NGWN: when the correspondent code (CN) resides either out of the home network or inside the home network.

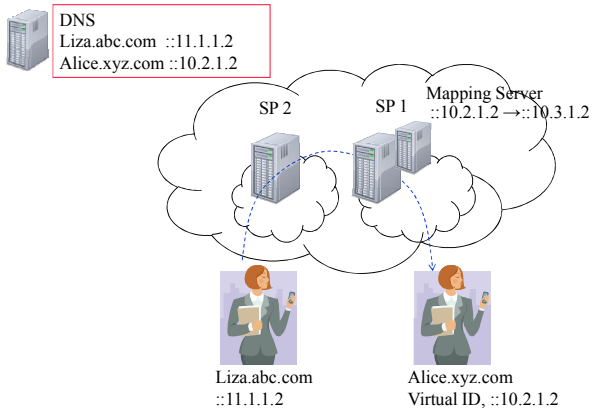

Fig. 2. Virtual ID with User Location Privacy Example

The first scenario is when the node is in a different network. Fig. 2 shows the correspondent node or *Liza.abc.com* in SP2 contacting *Alice.xyz.com,* which is in SP1. First, Liza retrieves Alice's identity, *::10.2.1.2*, from a DNS resolution process and uses that ID to route packets to Liza's home network. Since Alice's ID is used instead of her physical attached address, *::10.3.1.2*, Alice's location privacy can be maintained. Notice that if Alice is in foreign networks, her user location privacy is implicitly maintained. This scenario is similar to a traditional Mobile IPv6 because the permanent home address is different from the virtual ID.

The other scenario is when Liza is within the same network, say in an SP1 network, with *::10.x.x.x* networks. Suppose Liza's address is *::10.4.1.2* and again Alice is at *::10.3.1.2*, within her home network. With a traditional Mobile IPv6, Liza knows where the current location of Alice is. However, with Virtual ID, Alice's identity is used instead, *::10.2.1.2*; therefore, Liza no longer knows Alice's location information.

C. Proxy-assisted User Location Privacy Example

Fig. 3 shows an example of Proxy-assisted Mobile IPv6 and Virtual ID providing user location privacy. In this figure, Liza, a correspondent node, wants to contact Alice, who is not in her own home network. Note that the proxy will do both the binding update and the Mobile IP functionality on behalf of the mobile nodes. The binding update refers to a pairing of the virtual ID and the proxy locator: *::9.1.1.2* and *::11.5.1.1* for Liza and *::10.1.1.2* and *::12.5.1.1* for Alice. Liza does not know Alice's location and vice versa. Notice that each proxy has local node location information so that the proxy can forward the packets to the correct final destination.

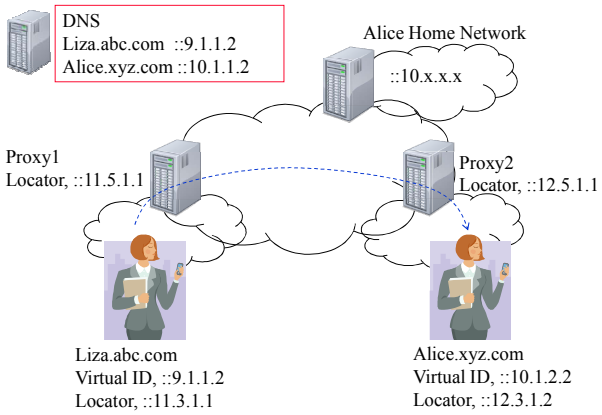

Fig. 3. Proxy-assisted User Location Privacy Example

D. Multi-Homing Example

In this section, we provide the details of how to incorporate the multi-homing feature into NGWN. Our proposal is based on home agent chaining among service providers.

We consider two main scenarios: when the multi-homing attachments are either to the same service provider or to different service providers.

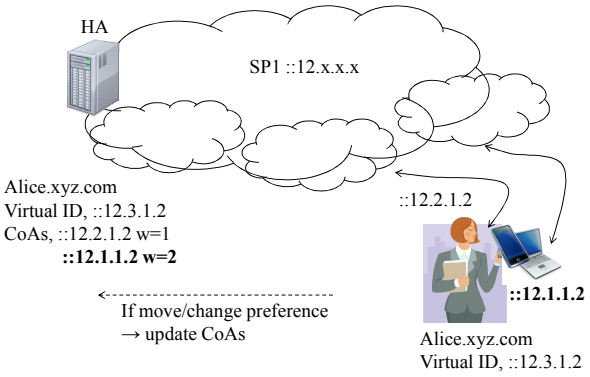

Fig. 4. Multiple CoAs Registration Example

The first scenario, Fig. 4 shows the process of multiple CoAs registrations with the preferred path selection when both networking attachment points are with the same service provider (SP1). In this figure, Alice has two access technologies with the same service provider (*::12.x.x.x*): toward cellular networks and toward WLAN on her single mobile device. Alice's virtual ID is*::12.3.1.2*, and the two physical locators or CoAs are *::12.2.1.2* (on a 3G network), and *::12.1.1.2* (on WLAN). When Alice is at home, she can send the update to her home agent to set a higher priority

toward the WLAN interface so that the inbound traffic can be forwarded toward this WLAN interface.

The other scenario is when mobile users have multiple access services from different network providers. Fig. 5a shows this configuration. As shown, Alice has two access services from two different service providers: SP1 cellular networks and SP2 WLAN. Since there are different SPs, Alice can acquire two different virtual IDs. Alice can send the update to the DNS server with her preferred path selections (with different weights). In this scenario, Alice is at home and she prefers the WLAN path (with a higher weight, or higher priority), which is toward SP2 or *::11.x.x.x* networks.

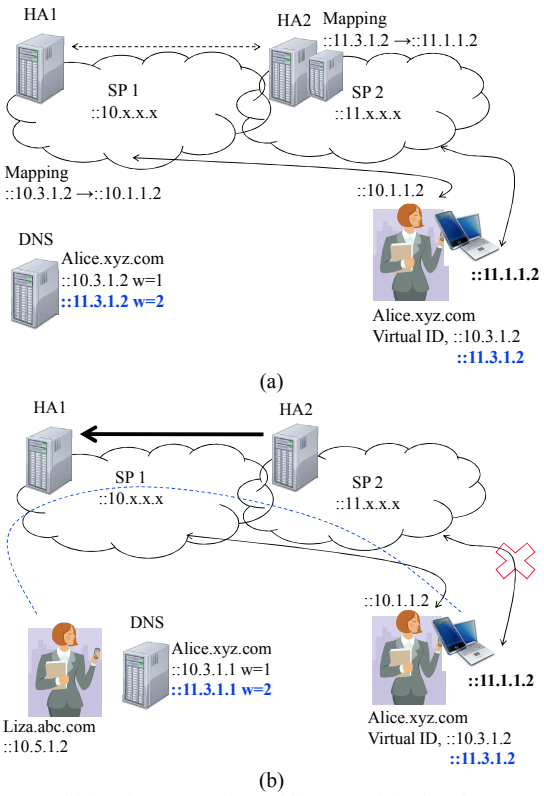

Fig. 5. Multi-homing Feature in Mobile IPv6 with Virtual ID Example

Note that the CoA address of Alice on the SP2 network is *::11.1.1.2*, not the Virtual ID *::11.3.1.2*. In this scenario, the packets are sent only towards WLAN as long as Alice does not update her preferred path on its DNS. There are no requirements for cooperation and interaction between two service providers.

When WLAN is not working, as shown in Fig. 5b, either SP2 or Alice can detect the disconnection. Without the interaction between the SPs, the packets can continue to flow to SP2 until Alice sends the update to the DNS server. Therefore, an additional operation is required. We recommend the concept of *home agent chaining*. Similar to the cellular phone system roaming mechanism, both service providers should have an agreement based on their user roaming policy to provide a packet forwarding mechanism. In this example, suppose SP1 and SP2 have a roaming agreement, and mobile users agree to pay for the additional cost of roaming.

During the disconnection, the steps in Fig. 5 are as follows: Liza, *::10.5.1.2*, originally sends her packets to Alice through SP2. Due to a link failure, the WLAN interface of Alice is unreachable. After the link failure detection, HA2 (from SP2) redirects all packets with Alice indicated as the destination to HA1 in order to reach Alice. Again, this redirection is based on a roaming policy. Whenever Alice sends the update to the DNS server to withdraw the disconnected path and/or to set a lower preference, this redirection will be terminated. Note that this example shows two service providers; however, the chaining concept can still apply with more service providers with multiple networking interfaces.

VI. Conclusions

Next Generation Wireless Networks, or NGWN, will be a cloud of all IP-based networks. The main features of these networks will be to fully support user mobility, multi-homing, user location privacy, and so on. Mobile IP and its variants have been introduced to resolve some of these issues. These proposals focus on a network layer technique. Some of these techniques have been selected by 3GPP for the System Evolution Architecture standard. However, these techniques have several limitations, especially due to the problem of identity and locator overloading.

In this paper, we discussed Mobile IP and its variants and also pointed out several drawbacks. In addition, we introduced a new technique called Virtual ID and its extensions, to make the Mobile IP fully support mobility, multi-homing, and user location privacy as well as user path selection. These add-ons are based on the standard Mobile IPv6 and its extensions and are therefore easy to be deployed along with Mobile IPv6.

References

[1] 3GGPP TS 23.402 V8.0.0 3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; Architecture enhancements for nono-3GPP accesses, Dec. 2007, 131 pp.

[2] R. Jain, "Internet 3.0: Ten Problems with Current Internet Architecture and Solutions for the Next Generation," in *Proc. IEEE Military Comm. Conf.*, 2006, pp. 1-9.

[3] C. So-In, R. Jain, J. Pan, and S. Paul, "Next Generation Wireless Networks: key issues and survey," Submitted to *EUSASIP Journal on Wireless Communicaiton and Networking*, Oct. 2009.

[4] S. Paul, J. Pan, and R. Jain, "A Survey of Naming Systems: Classification and Analysis of the Current Schemes Using a New Naming Reference Model," To appear in *Computer Communicatoin*, May 2010.

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

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

[7] A.T. Campbell, J. Gomez, K. Sanghyo, W. Chieh-Yih, Z.R. Turanyi, and A.G. Valko, "Comparison of IP micromobility protocols," *IEEE Wireless Comm. Mag.*, vol. 9, no. 1, pp. 72-82, Feb. 2002.

[8] S. Gundavelli, Ed. K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC 5213, Aug. 2008.

[9] R. Wakikawa, V. Devarapalli, G. Tsirtsis, T. Ernst, and K. Nagami, "Multiple Care-of Addresses Registration," Internet-Draft, draft-ietf-monami6-multiplecoa-14.txt, May 2009.