Motivations and Challenges of Global Mobility with Universal Identity: A Review

Walaa F. Elsadek, Mikhail N. Mikhail
Department of Computer Science and Engineering, the American University in Cairo,
P.O. Box 74, New Cairo 11835, Egypt
walaa.farouk@aucegypt.edu, mikhail@aucegypt.edu

***Abstract* — Researchers are directing enormous efforts to achieve the aim of global mobility by enhancing the standard mobile IP with various routing schemes focusing on best routes and least cost while ignoring the facts of the organizations usual use of private IP's and the presence of firewalls. Nevertheless, existing Mobile IP models are still missing three basic concepts that hinder their applicability in real environment. First, global mobility must be independent of the different infrastructure technologies (e.g., Wi-Fi, WiMAX, UMTS, etc.). Second, a secure authentication mechanism for guiding the access of mobile nodes to the corporate network's resources is certainly needed. Third, the capability of correlating the mobile node's activities to a real world identity is a requirement of security in a wider since i.e., network, web, and national security. This paper defines the role of global mobility in facilitating and improving mobile business performance. It, also, presents a review of literature for the existing standards and schemes of mobility and analyzes their limitations. Finally, a reference is made to a practical approach for secure global mobility without the current limitations.**

Keywords- Mobile Computing; Interworking; Mobility; Mobile IP; Security; Wireless.

I. INTRODUCTION

Mobility in the enterprise is derived by both technology availability and the increase in user demand. The merging of 4G and WLAN networks prompts the needs of operators to increase their coverage with a blended service offering that makes best use of their old investments in legacy infrastructure, low price technology and new technology at least price to address the higher volume of delivered rich data services [1]. Many people think of wireless and mobility as plumbing – focusing only on infrastructure and the fundamental technical security challenges, privacy, platform standardization, and legacy system integration [2]. However, the real target should be the ability to drive business improvement, and that requires vision in scoping mobility to fit the enterprise while preserving the privacy and security of mobile users accessing critical applications and identifying them with unique universal digital identities. For true global mobility, the following key features need to be emphasized:

- Seamless roaming between heterogeneous wireless, wired, and ad-hoc networks as illustrated in Figure 1.
- No restriction on the type of the hardware (mobile sets, PDA, laptop, etc.) or their operating systems.
- The connection between different mobile operators and internet service providers must be smooth without the need of complex reconfiguration.
- Enhanced security mechanism to facilitate the creation of e-commerce, banking services as well as any other services that need strong authentication.
- Transparency to end-user that does not need complex application or am increase in power consumption.
- Scalable routing mechanism that is flexible in adopting large-scale macro-mobility and local scale micro-mobility.
- Minimum handover interruptions to enhance availability and reliability of the services provided either to or by roaming clients.
- The capability of correlating the user activities to a unique universal digital identity.

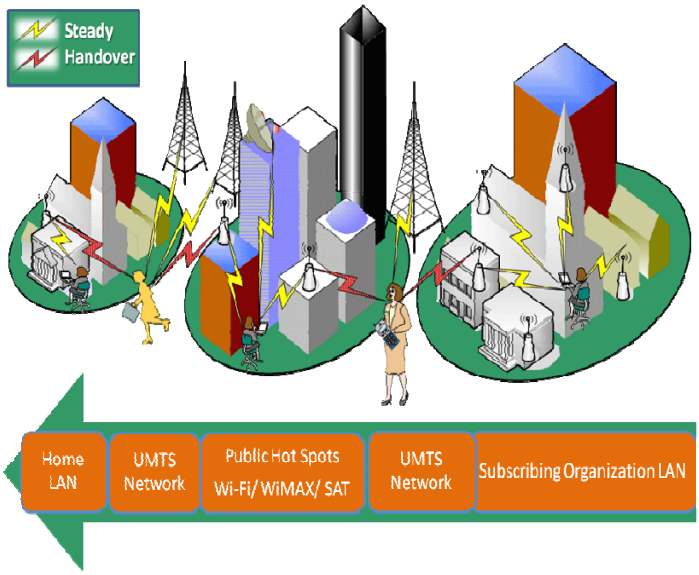

Figure 1. Overview of Global Mobility

II. MOTIVATIONS FOR GLOBAL MOBILITY WITH UNIVERSAL IDENTITY

A. Carriers' Motivations

Threats such as distributed-denial-of-service (DDoS) attacks, turbo worms, phishing, viruses and e-mail spam generates a huge amount of infected traffic that lead to subsequent outbreaks and disrupt the normal operation of a modern network. The primary challenges faced by today's service providers are maintaining service availability in the presence of such outbreak of malicious traffic. Security has become a critical characteristic of all services due to the direct effects reflected on the profit line of service providers. Universal digital identity can help in identifying the real identity of sources of threats then blocking their traffic or redirecting it to fake destinations.

Carriers are, also, challenged to meet the demand of their subscribers of enhanced mobility. They have to do so while avoiding new huge investment in remote areas by signing service level roaming agreements (SLRA) with other operators to make use of other infrastructure.

B. Subscribers' Motivations

New devices and business practices, such as PDAs and the next-generation of data-ready cellular phones and services, are the driving interest in the ability of a user to roam while maintaining two-way network connectivity:

- Roaming employees need to remain connected to their home corporate accessing local resources without any change to the corporate security policy and with least cost.
- Corporate employees need to keep accessing resources or services hosted by their roaming colleagues independent of their physical location using the same local private addresses.

In addition, the Mobile Nodes should remain transparently accessible to any corresponding node. Corresponding nodes are able to keep using the same addresses and with no need to any additional software.

C. Governments' Motivations

Criminals and terrorists are migrating to the digital world as it is tremendously lucrative and has less risk. They are willing to commit identity fraud and eager to sell it for profit. Negative impacts are induced on trusted transactions in online commerce, cyber investigations, authenticated individuals, or organizations, who want to gain access to services, systems, and facilities. Protection of assets and critical infrastructure such as telecommunications, public health, and the power grid, are necessary for the functioning of society [3]. In battle, war fighters must be able to identify people and determine if they are friend or foe, as well as if and how much of a risk they present. The challenge is to provide the war fighter with real time accurate information [4].The resultant escalation of cyber crimes and cyber attacks has resulted in the need for improved cyber investigations, security, and cyber defense. Grouping the network activities by universal digital identities enhances the cyber crime investigations with a tool that can simply reveal the real-world identities.

1) The Cyber Threats [4]

- Account take-over fraud in banking sectors, retailer, and healthcare provider.
- Access fraud on credit and financial information.
- Identity fraud in thin file situations and attack on an identity database.
- Cyber threat to enterprise attribute-based controls.
- Internal abuse of corporate assets and information.
- Wrest or hijack identity using Zombie networks.

2) The Cyber Challenge [4]

- Cyber security includes data protection, fraud detection, and preventions.
- Policy management that relies on security policies legislation to protect from identity theft.
- Breach detection by monitoring unauthorized system access or data acquisition using intrusions detection systems.
- Tracing and monitoring the usage of identities to detect unauthorized usage.
- Strong authentication methodology that correlates the identity user to the real identity owner.

III. REVIEW OF STANDARD MOBILE IP IN IPV4

Mobile IP (MIP) is an open standard, defined by the Internet Engineering Task Force (IETF) RFC 3344. Mobile IP enables users to keep the same IP address while traveling to a different network, ensuring that a roaming individual can continue communication [5]. Mobile IP does not drop the network prefix of the IP address of the node. Consequently, IP routing will succeed to route the packets to the node after movement to the new link [6]. RFC 3344 is considered the base for MIP. It defines the various entities involved in Mobile IP protocol and how they interact together to enable the registration of a roaming mobile node (MN) to the home network thus the home agent can forward the packet destined to MN to its care-of-address obtained from the foreign network.

RFC 4721: "Mobile IPv4 Challenge/Response Extensions" updates RFC 3344 by including a new authentication extension called the Mobile-Authentication, Authorization, and Accounting (AAA) Authentication extension. This new extension enables a mobile node to supply credentials for authorization, using commonly available AAA infrastructure elements. This authorization-enabling extension may co-exist in the same Registration Request with authentication extensions defined for Mobile IP Registration by RFC 3344 [6].

RFC 3344 assumes that tunneling is required for packet from the home agent to the mobile node's care-of address, but rarely in the reverse direction. It assumes that routing is independent of the source address and MNs can send their packet through the router in the foreign network. This assumption is not valid. This raises a need to establish a topologically correct reverse tunnel from the care-of address to the home agent [7]. RFC 2344: "Reverse Tunneling for

 ISBN:978-1-61208-113-7

Mobile IP" proposes backwards-compatible extensions to Mobile IP in order to support topologically correct reverse tunnels. When the mobile node joins a foreign network, it listens for agent advertisements and selects a foreign agent that supports reverse tunnels. It requests this service when it registers through the selected foreign agent. At this time, and depending on how the mobile node wishes to deliver packets to the foreign agent, it also requests either Direct or Encapsulating Delivery Style.

- **In the Direct Delivery Style:** the mobile node designates the foreign agent as its default router and proceeds to send packets directly to the foreign agent, that is, without encapsulation. The foreign agent intercepts them, and tunnels them to the home agent.
- **In the Encapsulating Delivery Style:** the mobile node encapsulates all its outgoing packets to the foreign agent. The foreign agent decapsulates and re-tunnels them to the home agent, using the foreign agent's care-of address as the entry-point of this new tunnel.

The MIP RFC3344 standard falls short of the promise in fulfilling the need of an important customer segment, corporate users (using VPN for remote access), who desire to add mobility support to have continuous access to Intranet resources while roaming outside the Intranet from one subnet to another, or between the VPN domain (i.e., trusted domain) and the Internet (i.e., un-trusted domain). Both firewall and VPN devices typically guard access to the Intranet. The Intranet can only be accessed by respecting the security policies in the firewall and the VPN device. In addition, any solutions to be proposed would need to minimize the impact on existing VPN and firewall deployments [8]. IP-in-IP tunneling does not generally contain enough information to permit unique translation from the common public address to the particular care-of address of a mobile node or foreign agent, which resides behind the NAT; in particular, there are no TCP/UDP port numbers available for a NAT to work with. For this reason, IP-in-IP tunnels cannot in general pass through a NAT, and Mobile IP will not work across a NAT [9].

RFC 3591: "Mobile IPv4 Network Address Translation (NAT) Traversal" enables mobile devices in collocated mode that use a private IP address (RFC 1918) [10] or foreign agents (FAs) that use a private IP address for the care-of address (CoA) are able to establish a tunnel and traverse a NAT-enabled router with mobile node (MN) data traffic from the home agent (HA) [9]. However, if the network does not allow communication between a UDP port chosen by a MN and the HA UDP port 434, the Mobile IP registration and the data tunneling will not work. Only the IP-to-UDP encapsulation method is supported.

The need is increasing for enabling mobile users to maintain their transport connections and constant reach ability while connecting back to their target "home" networks protected by Virtual Private Network (VPN) technology. This implies that Mobile IP and VPN technologies have to coexist and function together in order to provide mobility and security to the enterprise mobile users. RFC 4093: "Mobile IPv4 Traversal OF Virtual Private Network (VPN) Gateways" addressed the previous limitation by forcing any MN roaming outside the Intranet to establish an IPSec tunnel to its home VPN gateway first, in order to be able to register with its home agent. This is because the MN cannot reach its' HA (inside the private protected network) directly from the outside. This implies that the MIPv4 traffic from the MN to a node inside the Intranet is forced to run inside an IPSec tunnel. This in turn leads to distinct problems depending on whether the MN uses co-located or non-co-located modes to register with its HA

In co-located mode, successful registration is possible but the VPN tunnel has to be re-negotiated every time the MN changes its point of network attachment, as the MN's IP destination address changes on each IP subnet handoff, IPSec tunnel needs to be re-established. This could have visible performance implications on real-time applications and in resource-constrained wireless networks [11].

In foreign agent care-of address, MIPv4 registration becomes impossible. This is because the MIPv4 traffic between MN and VPN gateway is encrypted, and the FA (which is likely in a different administrative domain) cannot inspect the MIPv4 headers needed for relaying the MIPv4 packets. The use of a 'trusted FA' that is actually a combined VPN GW and FA can work fine in this case, as the tunnel end-points are at the FA and the VPN gateway as shown in Figure 2.

Limitation:

(i) However, due to security limitation, this scenario is not realistic in the general mobility case. It is not expected that the FA in access networks (e.g., wireless hot spots or CDMA 2000 networks) will have security associations with any given corporate network to apply 'trusted FA'.

(ii) This solution would leave the traffic between FA and MN unprotected. This is clearly undesirable as this link in particular may be a wireless link

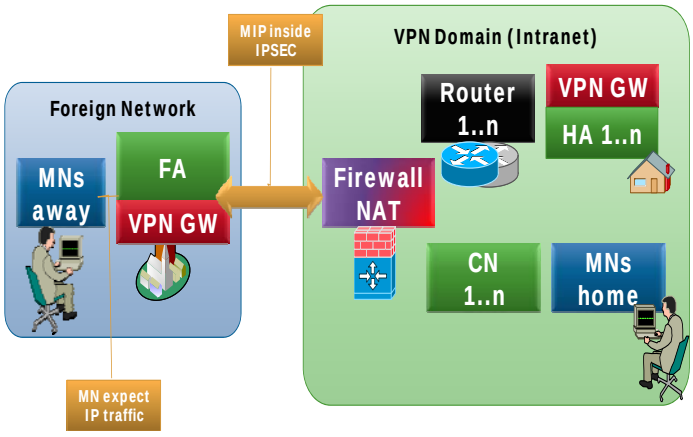

Figure 2. The use of a 'trusted FA' In foreign agent care-of address

IV. REVIEW OF STANDARD MOBILE IP IN IPv6

3775: “Mobility Support in IPv6” specifies a protocol, which allows nodes to remain reachable while moving around in the IPv6 Internet. This protocol allows a mobile node to move from one link to another without changing the mobile node's "home address". Packets may be routed to the mobile node using this address regardless of the mobile node's current point of attachment to the Internet. The movement of a mobile node away from its home link is thus transparent to transport and higher-layer protocols and applications [12]. A mechanism, known as "dynamic home agent address discovery" is added in Mobile IPv6 to provide support for multiple home agents and the home network reconfiguration. This mechanism allows a mobile node to dynamically discover the home agent IP addresses on its home link, even when being away from home. Mobile nodes can also learn new information about home subnet prefixes through the "mobile prefix discovery" mechanism.

A. Comparison between Mobile IPV4 and IPv6

1. There is no need to deploy special routers as "foreign agents", as in Mobile IPv4. Mobile IPv6 operates in any location without any special support required from the local router.
2. Support for route optimization is a fundamental part of the protocol, rather than a nonstandard set of extensions.
3. Mobile IPv6 route optimization can operate securely even without pre-arranged security associations
4. Support is also integrated into Mobile IPv6 for allowing route optimization to coexist efficiently with routers that perform “ingress filtering" [13].
5. The IPv6 Neighbor Unreachability Detection assures symmetric reachability between the mobile node and its default router in the current location.
6. Most packets sent to a mobile node while away from home in Mobile IPv6 are sent using an IPv6 routing header rather than IP encapsulation, reducing the amount of resulting overhead compared to Mobile IPv4.
7. Mobile IPv6 is decoupled from any particular link layer, as it uses IPv6 Neighbor Discovery instead of ARP. This also improves the robustness of the protocol.
8. The use of IPv6 encapsulation (and the routing header) removes the need in Mobile IPv6 to manage "tunnel soft state".
9. The dynamic home agent address discovery mechanism in Mobile IPv6 returns a single reply to the mobile node. The directed broadcast approach used in IPv4 returns separate replies from each home agent.

B. Summary of Mobile limitations

Unluckily, standard MIP faced many limitations that hindered its applicability in real environments as:

1. Ignoring that the Mobile Node (MN) can exist behind a Firewall or NAT device.
2. Considering only Forward Tunnel; that Corresponding Node (CN) packets has to be forwarded by Home Agent (HA) to MN while Ignoring Reverse Tunnel; that MN needs to access the corporate services.
3. With updated RFC 2344, that includes Reverse Tunnel; MIP becomes subjected to DoS and Session Hijacking due to the lack of a secure method for authenticating MN [7].
4. Ignoring the corporate security policy, during the tunnel establishment phase or the MN’s registration with the HA.
5. Ignoring that the DNS domain name is used for locating and addressing devices worldwide.
6. The VPN tunnel has to be re-negotiated every time the MN changes its point of attachment.
7. Ignoring the Scalability Factor; Home agent and Foreign agents are a single point of failure.

V. NEW MOBILITY ARCHITECTURE

In the paper: “Universal Mobility with Global Identity (UMGI) Architecture” [14], a new mobile IP concept has been introduced to address the limitations of previous proposed mobile IP. The UMGI correlates mobile users’ credentials as IP, hostname, and network equipment identifiers (ex. network cards or mobile sets) with their (U)SIM (Universal subscriber identity module) cards .Not only this corelation provides a strong method for authenticating subscribers but also it acts as the foundation of the newly proposed mobile IP protocol. The extracted “Country codes” and “Carrier Code” stored in the (U)SIM enable the dynamic discovery of the home agent thus facilitate routing the traffic to the home network. In addition, this paper has discussed the integration of the MN authentiation with the standard methods of authentionation in the UMTS network. This architecture extends the capabilities of standard mobile IP, solves its applicability problems, and links mobile users’ activities to unique universal identities

A. Advantages of the suggested UMGI:

1. Not like the standard MIP, which runs on the mobile node and keeps monitoring the network prefix, the UMGI Architecture makes the mobile node unaware of any procedure. All UMGI services and modules run on distributed servers administrated by the carriers or the corporate networks thus enhancing the performance of mobile subscriber while decreasing the battery consumption of the MN.
2. Standard MIP has not considered any handover procedure. It focuses on stationary hosts that moved to different location other than the home network. UMGI MIP inherits its mobility from the wireless technology adopted. It opens rooms for programmers to enhance the handover procedures thus movement can be unnoticeable.

 ISBN:978-1-61208-113-7

3. The security policy of the corporate network is preserved:
   a. By restricting the Home UMGI IPSec tunnel establishment to authorized the carrier gateways and the predefined UMGI Tunnel Subnet.
   b. The corporate firewall can be configured with an advanced security policy controlling the UMGI roaming subscribers' access and privileges.
4. DHCP Classification: preserves the UMGI roaming subscriber's CoA during the movement inside Hot Wi-Fi spots covering one or more buildings that have multiple APs but with a single border gateway and during the movement between multiple Node B or BTSs connected to the same access point on the GGSN. The UMTS or (E) GPRS access point can cover a country region.
5. Automatic private IP addressing procedure: Preserves the mapping of UMGI subscriber public address and private addresses as well as the DNS domain name while roaming in the foreign network. This enables MNs, in either foreign carrier, to handoff between multiple Wi-Fi hotspots and multiple UMTS or (E) GPRS access point even if the CoA obtained from the DHCP server is changed. The only challenge is the time required to update the mapping on the FG of the network to which the subscriber is attached. The FA should be capable to update the FG in few seconds. In TCP traffic, no packet will be lost as this will be regarded as congestion and retransmission will occur. For UDP, any packet lost in range of few seconds will not be noticed.
6. The combination of "UMGI Trust Relation" and the "Hierarchical Discovery Routing Procedure" increases the scalability and the security of the new mobile IP architecture while preserving the security of communication between foreign and home networks. The combination makes the architecture extremely customizable fitting small ISPs and large carriers. In addition, it increases the architecture flexibility to adopt several designs and different types of agreement starting from small ISPs inside the country and ending with regulators agreements cross-countries boundaries.
7. The carriers can freely add or modify the configuration of its gateway even the IP addresses without any need to update any other carrier under UMGI SLRA.
8. The architecture solves the current MIP applicability limitation. With UMGI, it is simple to create dynamic IPSec tunnel on demand with the home VPN gateway and to path through any firewall security policy.
9. Added a security layer that is boasted by a strong client authentication mechanism as EAP. This provides a strong protection against session hijacking and Denial of Service attack.
10. Using a single path between remote and local carrier, UMGI Remote Tunnel, to carry the MNs' traffic from multiple corporate networks connected to the same carrier gateway, decreases the UMGI subscriber's joining time by avoiding the process of "Tunnel setup Procedures" for MNs belonging to the same carrier.
11. The synchronization between both foreign and home carrier through AAA and HLR enforces the status consistency and increases the security by restricting access to only one UMGI subscriber per IMSI at time, even if having multiple registered equipments.
12. Mobile IP leaves transport and higher protocols unaffected. Other than mobile nodes/routers, the remaining routers and hosts will still use current IP address format without any modification. Unlike, Standard MIP, UMGI MIP does not need enabling jumbo frames or any change in the IP frame format. Thus, UMGI suits LAN/WAN topology.
13. UMGI is Multi-Vendor Interoperable. It can be considered as an organized setup of the standard protocols thus, no need to any software upgrade or any major change to the existing infrastructure.

VI. CONCLUSION

Enhancements to the standard Mobile IP techniques are being developed to improve mobile communications and to overcome the existing limitations by making the process more secure and more efficient. Researchers are continuously adding achievement to augment its applicability to the new business needs. In this paper, the importance of secure global mobility as motivated by the needs of corporate organizations, service providers, and governments is highlighted. State of the art schemes and standards dealing with facilitating and managing mobile computing both in the current IPv4 and the coming IPv6 are reviewed.

A reference is made to a suggested architecture that is aimed at overcoming the current practical limitations. As it should be, the suggested scheme is transparent, secure, scalable, independent of any communication protocol, and valid for hybrid infrastructure. This shows that designing an architecture for global mobility with universal identity that satisfies the requirements of service providers, governments, and corporate organizations is a challenge and needs an enterprise secure cooperations between the various entities. This architecture has proposed a new mobile IP that solves the standard mobile IP scalabilty limitations by proposing a solution that can be easily deployed with the presence of firewalls and VPNs. Also, the proposed solution has shown that a mobile user can handover hybrid infrastructure with very short delay without changing its real IP address or DNS domain name. Solving the challenges that hindered the applicability of standard Mobile IP becomes possible by adopting the new mobile IP protocol as it has correctly analyzed all the obstacles in standard mobile IP and proposes a complete solution fitting the different wireless technologies and the new business needs. Finally, the proposed correlation of the mobile users' credentials as IP, hostname, and network equipment identifiers with their (U)SIM cards provides a

 ISBN:978-1-61208-113-7

strong method for authenticating and authorizing mobile users while creating a unique universal identity that can reveal the real world identity. Without doubt this can facilitate the cyber crime investigation and enhance the cyber security.

REFERENCES

[1] A. Durresi1, L. E.s, V. Paruchuri, and L. Barolli: "Secure 3G User Authentication in Adhoc Serving Networks", Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), June 2006.

[2] J. LaFlamme and M. Litwin, Deloitte Development LLC "Wireless and Mobility", 2010.

[3] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang, "Self-securing Ad Hoc Wireless Networks", UCLA Computer Science Department.

[4] CAIMR (Center for applied Identity Management Research), "An Applied Research Agenda for confronting Global Identity Management Challenges, May 2009."

[5] C. Perkins, Ed. Nokia Research Center, "IP Mobility Support for IPv4," RFC 3344, August 2002.

[6] C. Perkins - Nokia Research Center, P. Calhoun - Cisco Systems, Inc., J. Bharatia - Nortel Networks, "Mobile IPv4 Challenge/Response Extensions (Revised)", IEFT RFC 3775, January 2007.

[7] G. Montenegro, Sun Microsystems, Inc., "Reverse Tunneling for Mobile IP", RFC 2344, May 1998

[8] F. Adrangi, Ed. Intel and H. Levkowetz, Ed. Ericsson, "Mobile IPv4 Traversal of Virtual Private Network (VPN) Gateways," RFC 4093, August 2005.

[9] Cisco Systems, Inc. , Design of the Mobile IP—Support for RFC 3519 NAT Traversal Feature, 2007

[10] Y. Rekhter - Cisco Systems, B. Moskowitz - Chrysler Corp., D. Karrenberg - RIPE NCC, G. J. de Groot - RIPE NCC, E. Lear - Silicon Graphics, Inc., "Address Allocation for Private Internets", RFC 1918, February 1996.

[11] S. Kent - BBN Corp, R. Atkinson - @Home Network, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

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

[13] H.Soliman, C. Castelluccia, K. El-Malki, and L. Bellier, "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)-0," IETF RFC 4140, August 2005.

[14] W. F. Elsadek and M. N. Mikhail, Department of Computer Science and Engineering, the American University in Cairo "Universal Mobility with Global Identity (UMGI) Architecture", Proceedings 2009 International Conference on Wireless Networks and Information Systems (WNIS 2009), December 2009.

 ISBN:978-1-61208-113-7