Comparison and Analysis of Secure Mobile Architecture (SMA) and Evolved Packet System

Jani Pellikka
Centre for Wireless Communications
University of Oulu, P.O. Box 4500,
FI-90014 Oulu, Finland
jani.pellikka@ee.oulu.fi

Marek Skowron
Centre for Wireless Communications
University of Oulu, P.O. Box 4500,
FI-90014 Oulu, Finland
marek.skowron@ee.oulu.fi

Andrei Gurtov
Centre for Wireless Communications
University of Oulu, P.O. Box 4500,
FI-90014 Oulu, Finland
andrei.gurtov@ee.oulu.fi

***Abstract*—In this paper, we analyse and compare two architectures providing an all-IP based connectivity and mobility for mobile devices over heterogeneous access technologies: Evolved Packet System (EPS) as specified by 3GPP and Secure Mobile Architecture (SMA), a standardization effort by The Open Group (TOG). We briefly present each architecture and qualitatively evaluate their advantages and disadvantages in terms of security, mobility, and support for location-based policy enforcement and security zoning. While SMA is capable of providing simultaneous multihoming, cryptographic identity-based packet tracking and ready support for location-based security zoning and policy control, EPS enables legal interception of user traffic and protection of user/host privacy by default.**

***Index Terms*—EPS, SMA, security, mobility, policy enforcement.**

I. Introduction

So as to support advanced real-time and media-rich services in the future mobile telecommunication networks, 3rd Generation Partnership Project (3GPP) has specified a new mobile network standard known as Evolved Packet System, or EPS [1] for short. EPS contains a new high-performance core network, Evolved Packet Core (EPC), to improve network performance through common all-IP network architecture. As all data communications (including voice and video) take place end-to-end over the IP protocol, EPS is able to provide higher scalability and reliability than the previous generation mobile networks.

By realizing a unified IP-based framework for both voice and data, EPS marks an end of circuit-switched voice and is thus a major shift away from the previous mobile networking paradigms. Furthermore, EPS aims not only to provide all-IP based connectivity for mobile devices equipped with heterogeneous access technologies (e.g. WiFi, LTE, and HRPD), but to also support mobility and multihoming between them.

An effort with similar ambitions to those of EPS is Secure Mobile Architecture (SMA) [2], a standardization proposal from The Open Group (TOG), addressing the business requirements of having a secure network access from heterogeneous access network technologies and seamless roaming between them. SMA integrates a variety of emerging standards being developed in the IETF and IEEE forums to provide true end-to-end security and transparent mobility for multimedia sessions. Support for policy enforcement and security zones based upon location is also an integral part of the SMA design.

In this paper, we briefly present the characteristics of the two above mentioned architectures and examine their design principles from the security, mobility, and policy enforcement point of view. This paper is an analysis and comparison of EPS and SMA discussing their strengths and weaknesses against five design principles used as qualitative evaluation criteria.

The paper is organized as follows. In Section II, we present an overview of the EPS architecture as defined by 3GPP, and in Section III, we briefly cover the main traits of SMA. Section IV provides the evaluation and comparison of the two, and finally, Section V concludes the paper and outlines directions for future work.

II. Evolved Packet System

The purpose of EPS is to create a common all-IP network for all access types with shared radio interface [3]. The data flow in EPS, between EPC and different radio access technologies (RATs), is provided by two primary gateways. Serving Gateway (SG-W) is the node through which user data is transmitted from LTE (eNodeBs) to EPC. It is also an anchor point for intra-LTE mobility, as well as between GSM/GPRS, WCDMA/HSPA and LTE. Packet Data Network Gateway (PDN GW) is a user plane node connecting EPC to the external IP networks and non-3GPP services [4]. High-level architecture of EPS is presented in Figure 1.

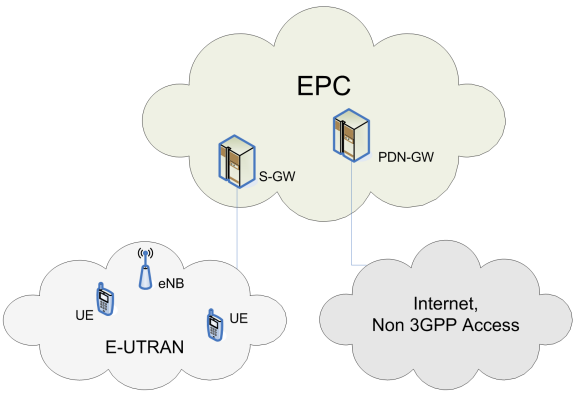

Fig. 1. EPS Network Architecture.

978-1-4244-8329-7/11/$26.00 ©2011 IEEE

A. Services in EPS

1) Voice Services: Voice services in LTE are realized via IP Multimedia Subsystem (IMS), which is a platform offering IP-based multimedia services (most important being VoIP). The concept of IMS is based on Session Initiation Protocol (SIP) [5] developed by IETF as a signalling method via which media sessions can be established and managed.

2) Location Services: Location Services (LCS) in LTE introduce new features to enable innovative location based services. The current position (e.g. in geographical co-ordinates) of the user is available to User Equipment (UE), network operator, service provider, value added providers and for Public Land Mobile Network (PLMN) internal operations. LCS can be used e.g. for charging, lawful interception, emergency calls and positioning services [6].

B. Security Features

Security in EPS can be roughly divided into two domains: network access and network domain security. By network access security we mean the security features that provide a UE with secure access to EPS. This consists of mutual authentication of the UE and the network, and privacy protection. Network domain security, in turn, comprises the features that allow the nodes of EPC such as routers to exchange data securely. The end-to-end path between two network nodes is afforded with hop-by-hop security protection.

3GPP has decided to utilize Authentication and Key Agreement (AKA) protocol, which makes it possible to perform 3GPP-based authentication and authorization with the same credentials shared between a UE and a home network regardless of the access technology. In the 3GPP access, EPS AKA is used to negotiate the keys for ciphering and integrity protection, while in non-3GPP access' case, Extensible Authentication Protocol (EAP) variant of AKA (EAP-AKA) is used. In untrusted non-3GPP accesses, UE and EPS also establish an IPSec tunnel using Internet Key Exchange version 2 (IKEv2) [7] for additional protection.

C. IP Mobility

EPS provides common core network for all current radio accesses i.e. WCDMA, LTE, WiMAX etc. and supports mobility between them. There are two mobility concepts in EPS: host-based and network-based [1]. In the first one UE (host) is involved in mobility signaling and movement detection. The latter one means that the network is responsible for signaling and detection of UE movement.

Every device in EPS is assigned an IP address, which is part of a sub-network. In order to be able to receive packets while being in another network (e.g. when UE switches from 3GPP to WLAN) Mobile IP introduces Home Agent (HA) entity to PDN-GW. The function of HA is to associate the original IP address, Home Address (HoA) and the local address in the foreign network, Care of Address (CoA) and forward packets addressed to HoA to CoA. Route optimization (RO) is not supported in EPS which means that also uplink packets have to be sent via HA.

Mobile IP is specified for both IPv4 (Mobile IPv4 - MIPv4) and IPv6 (MIPv6). There also exists Dual-Stack Mobile IP (DSMIPv6) which supports dual-stack IPv4/IPv6 operation. Those protocols are host-based. An example of network-based protocol is Proxy Mobile IPv6 (PMIPv6). It was created for those UEs which don't have Mobile IP functionality and hence mobility agents in the network (which act as proxies) track the movement of UE and execute signaling of IP mobility instead of UE [1], [8].

D. Policy and Charging Control

The main network node in Policy and Charging Control (PCC) is Policy and Charging Rules Function (PCRF). It forms session-level policy decisions based on combining inputs received from PDN-GW and S-GW and user-specific policies and data from the subscription profile repository (SPR) with the session information from Application Function (AF). AF interacts with applications that require dynamic policy and charging control. For more information about PCC see [9].

III. Secure Mobile Architecture

SMA is an integration architecture defining the basic high-level components for implementing secure IP-based mobile environments and it has already been successfully implemented by The Boeing Company, which has developed an SMA pilot [10], [11] as a part of the company's intranet infrastructure to secure the manufacturing of aircrafts.

A. Host Identity Based Security

The security of networks has so far been based mainly on MAC and IP addresses used as an identity which has made the public Internet inherent to Denial of Service (DoS), Man-In-The-Middle (MitM), and spoofing attacks [11]. SMA intends to resolve this invulnerability in IP-based communications by basing the security on the host identity instead of the address.

In order to provide protection against the above mentioned security hacks, SMA has specified the use of IETF's Host Identity Protocol (HIP) [12] to deliver true end-to-end security and data integrity at the transportation layer. HIP is able to provide a mechanism for host authentication and association of a cryptographic identity with every packet sent across the network. HIP is used as a signaling protocol to negotiate the SAs between communicating parties and to notify IP address changes to the correspondents.

HIP's host identity is a cryptographic public/private key pair represented by a 128-bit long bit string, i.e. Host Identity Tag (HIT). HIT is created by applying a cryptographic hash over the public key and is used by communication peers to identify and authenticate a given host. IP address is used merely as a topological label for locating an endpoint and is not intended for the application layer to use directly.

B. Seamless Mobility

To provide applications with transparent IP address changes, SMA relies on the mobility and multihoming extension of HIP [13], where a HIP control packet is sent to all active

peer hosts to direct the traffic to the new roamed address. Unfortunately, an additional infrastructure to track the IP addresses at which hosts are reachable is also needed.

To enable host tracking and reachability, SMA has specified the use of dynamic Domain Name Service (DDNS) to accept frequent changes to the IP addressing of the hosts. In SMA, the name service is HIP-capable [14] and serves to appropriate domain names to HITs and IP addresses. The motivation to use DDNS is that it can be used to provide real-time tracking and reachability, which is requisite for QoS sensitive applications. From the functioning point of view, SMA requires a roaming host to update its current address to its peers and also to the DDNS by using the HIP address update packets and a separate DNS-specific mechanism, respectively.

SMA also considers integration of HIP and SIP. As SIP is able to provide personal and session mobility at the application layer, and HIP host mobility at the transport layer, combining the two could yield complimentary benefits: SIP would make sure that ongoing sessions are maintained when user moves from one device to another and associate the user with a new host identifier at the roamed device. HIP, in turn, would enable the device to preserve all IP connections in the mobility. The joint use of HIP and SIP is extensively discussed in [15].

The goal of SMA is to support VoIP over WLAN with the capability to transition seamlessly onto cellular networks when not within the range of WLAN access points. So as to establish seamless vertical handovers without interruption in the service, there is a requirement to pass link layer related state information (e.g. L2 security and QoS parameters) to the new roamed domain. To communicate the state information across domain borders, SMA suggests utilizing the CTP proposal from IETF Seamoby Working Group and IEEE's 802.11f Inter-Access Point Protocol (IAPP) [2].

C. Location-Based Security Policy

SMA harnesses location to enable security zones and incorporates policy enforcement based on the host identity and location. The architecture aims to support scenarios where, e.g. roaming and access to the network are restricted when the mobile device is located outside a perimeter such as office building or manufacturing hall.

The architecture describes a policy engine, a policy decision daemon that accesses location-specific policies in a database and is responsible for interpreting and sending them to Policy Decision Points (PDPs) and Policy Enforcement Points (PEPs). The policies may be enforced at either network or application level. In the network level policy enforcement, HIP-aware middleboxes (e.g. routers) identify packet flows using the HITs of communicating hosts, as well as SPI values and IP addresses, and check packets against a set of policies stored in an access policy repository. In application level policy enforcement, the communicating application in an end-host is responsible for checking from the policy repository if its peer is allowed to access its services from the current location.

IV. Comparison of EPS and SMA

Instead of stating hard requirements for secure and mobile IP-based environments, SMA introduces a loosely defined set of principles the mobile environments of the future would be built upon [2]. In this section, we go through these principles as defined by the SMA effort and use them as evaluation criteria to provide qualitative analysis and comparison between the architectures of EPS and SMA. The principles are summarized in Table I.

TABLE I
Principles of the SMA architecture.

Principle	Description
IP-only	Only IP is addressed. The IP protocol is assumed to be the future protocol most data and voice are carried over with in the Internet.
Security	Security is based on the host identity instead of IP and MAC addresses. Authentication, authorization, and encryption are guaranteed between the end points of communication. The security of the user is provided on the basis of communication session.
Mobility	Mobile device is able to seamlessly and transparently migrate across disparate network technologies, while maintaining the ongoing communication sessions and established security parameters. Handovers and transfers must be fast enough for VoIP traffic.
Policy Enforcement	There is a policy engine, which determines policies and employs them based on predefined rules for attributes such as user role and location. Policies can be enforced at network and application level.
Location	Location information is utilized to enable security zones. Host authorization is managed by the policy engine, which decides to deny or grant service to hosts based on their current location.

A. IP-Only

SMA addresses IP only, which implies the use of VoIP as the main streaming application. EPS likewise treats multimedia, including voice, merely as an IP-based network application, which is a major shift away from the previous paradigm where Signaling System 7 (SS7), an ITU-standardized protocol for circuit switched systems, has long managed the voice signaling. Hence, both EPS and SMA are in alignment with the all-IP paradigm where multimedia content is carried over an IP-based transport and connections are allowed with guaranteed bit rates and prioritized treatment over others. More importantly, both architectures acknowledge SIP as a prominent signaling mechanism for managing multimedia sessions.

As the IPv4 and IPv6 protocol families can be expected to co-exist a long time until IPv6 becomes prevalent technology, the IP-only systems need to address them both. EPS and SMA has specified mechanisms to make the protocols to function on the same network and to allow IPv6-based devices to seamlessly communicate with IPv4 applications and vice versa. EPS utilizes here the means provided by DSMIPv6, whereas SMA relies on HIP's built-in feature to simultaneously use the IPv4 and IPv6 addresses bound to single or multiple interfaces. As

HIP effectively separates the roles of a host identifier and an IP address from each other, not just cross-family communication, but also cross-family multihoming is possible in SMA.

B. Security

In EPS, regardless of the access technology, the mutual authentication of a UE and a mobile network is based upon a symmetric key pre-shared by the subscriber and operator and takes place on the link layer through the EAP-AKA or EPS AKA mechanism. SMA does not specify its own link layer authentication method, but expects some method to be in place in the access network. SMA does, however, specify HIP as an additional transport layer mechanism to attach a verifiable (and traceable) identity to every packet and to negotiate the parameters for transport layer ciphering.

Unfortunately, the basic HIP is able to provide only opportunistic security, where the authenticity of a host's identity can not be reliably verified, as opposed to EPS, where the verification is established through mutual possession of IMSI, as well as a pre-shared secret key. As a consequence, SMA needs to incorporate an additional authorization framework, Public Key Infrastructure (PKI), to certify the identities. This unfortunately introduces extra complexity to the system.

In case of unprotected non-3GPP access in EPS, the mobility signaling between the UE and EPC, as well as the user plane data is integrity protected by using an IKEv2-negotiated IPSec tunnel. Thus, EPS utilizes a scheme, where the link layer authentication signaling (i.e. the EAP frames) is carried inside an L3 negotiation protocol, as opposed to SMA, where the HIP BEX is independent from the L2 authentication.

As for similarities between the HIP and IKEv2 protocols, they both use the authenticated Diffie-Hellman protocol for key exchange and contain support for DoS resistance through puzzles and cookies, respectively. However, the main difference between the two protocols is that IKEv2 is able to use any EAP-based authentication method to confirm the identity of a subscriber with the 3GPP AAA backend, while HIP has to rely on, e.g. a PKI infrastructure to confirm the host identities.

The shortcoming of IKEv2 negotiated SAs is that they are bound to IP addresses. When a mobile UE changes its point-of-attachment to a network, the UE is required to negotiate a new IPSec SAs, which leads to latency in handovers and possibly interruption in the ongoing services. EPS alleviates this problem by using the IKEv2 Mobility and Multihoming Protocol (MOBIKE) [16], which allows the IP address bound to an IPSec SA to change freely. The protocol supports also multihomed UEs, but only one pair of IP addresses can be used for an SA at a time. As HIP separates IP address and host's identity from each other (i.e. binds SA to HIT), SMA is able to provide simultaneous multihoming over multiple interfaces with constant SAs, a feature not currently supported in EPS.

In regard to security, the most significant difference between the SMA and EPS architectures is how the user traffic between end-hosts is secured: SMA represents the so called end-to-end scheme, where the data is protected using the SAs negotiated by the end-hosts themselves, while EPS utilizes end-to-middle scheme that protects the packets to and from the hosts only up to the EPC network border. This implies that SMA has no ready support for legal interception (unlike EPS wherein pre-shared keys enable the interception of encrypted packets) as SAs are negotiated in the end-to-end manner and maintained in the end-hosts.

One major security issue SMA needs to overcome is inadequate privacy protection. In the standard HIP, the HIT of a peer host is known, and thus publicly traceable to any third party. However, to solve this issue, a few privacy extensions to HIP are already available, e.g. [17].

C. Mobility

MIP offers an effective mechanism for host mobility in the Internet. However, MIP-based mobility is hindered by several limitations, namely unsuitability for performing handovers fast enough for QoS sensitive applications and inadequate support for security [18]. For these limitations, HIP was selected to handle location updates in SMA. HIP is expected to provide better handover performance than MIP when combined with a separate handover mechanism (e.g. CTP).

Because HIP is dependent on external name resolution and rendezvous infrastructure, SMA specifies DDNS to track hosts and enable reachability in mobility. The viability of DDNS in macro mobility scenarios has been studied in [19] and [20]. The research demonstrates the ability of DDNS to handle IP address updates at rates adequate for QoS sensitive services and thus concludes that DDNS is indeed feasible in supporting real-time mobility. As a downside, however, such a solution is not adequate to solve the issue of simultaneous movement of two peers.

While SMA relies on host-based mobility through HIP, EPS incorporates both host-based and network-based mobility via DSMIPv6 and PMIP, respectively. These protocols represent a mobility scenario, where a PDN GW or other network node near the EPC border acts as an anchor point for both user and control traffic. As pointed out in [21], the 3GPP deployment of MIP, where user traffic always passes HA, leads to scalability issues and therefore the use of a mobility protocol with end-to-end location updates (e.g. SIP and HIP) is preferable. Despite of suboptimal routing, EPS addresses legacy devices with no mobility support, unlike SMA that requires the deployment of HIP in all hosts participating to mobility.

Both SMA and EPS, also support the use of SIP as an application layer solution for keeping ongoing multimedia sessions in terminal and user mobility. SMA, however, suggests combining SIP and HIP for complimentary mobility. Such a joint use of the two protocols and its performance advantages over MIP has been extensively discussed in [22]. The results indicate a hybrid HIP and SIP scheme being substantially more efficient in terms of handover signaling and delay overhead.

D. Policy Enforcement

SMA defines policies on network and network service to be enforceable at the network as well as application level where a policy engine interprets the policies and send them to PDPs

and PEPs. EPS specifies a centralized policy decision entity within EPC, PCRF, which is responsible for subscribing to events and sending corresponding policies to the gateway entities (e.g. PDN GW and SGW) or the eNodeB base stations that enforce them at the network level. PCRF takes the operator-specified service policies and subscription information into account when deciding upon a policy, but to our knowledge, in the current development state it does not consider utilizing the location information available at LCS.

E. Location

SMA emphasizes the importance of location as it enables a plethora of useful industrial applications. EPS aims to address applications that require the location information of UEs through the LCS architecture. There is a server component, an LCS server that serves to accept subscriptions from clients and notify them when a certain event takes place. With a zone transformation function it is possible to perform conversion from geographical coordinates to zone identities, which enables using location for zoning. However, EPS has not explicitly specified interface between PCRF and LCS to make location-based authentication and authorization (i.e. location-based security zoning) possible in the mobile networks.

V. Conclusions and Future Work

In this paper, we compared and analyzed two architectures, Evolved Packet System (EPS) and Secure Mobile Architecture (SMA) in terms of security, mobility, policy enforcement, and support for security zones. Our qualitative review concludes that both all-IP architectures contain support for host mobility and security including authentication and integrity protection of user and control data. As for the location-based security zoning, we further conclude that EPS, as opposed to SMA, has not been constructed such an industrial requirement in mind, and therefore requires architectural changes in that regard. However, EPS already incorporates all required components for realizing security zoning and security zone-based policy enforcement.

In SMA, security and the host mobility features are based on HIP, while EPS incorporates IKEv2-based authentication and negotiation of SAs, coupled with MIP-based schemes for mobility. Where SMA is able to provide parallel maintenance of SAs between two end-hosts and to enable traceability and authentication of each packet through cryptographic identities instead of IP addresses, EPS is able to provide privacy support and allows for legal interception. The two architectures also differ in that SMA relies on end-to-end security and mobility, while EPS utilizes end-to-middle approach. It must be stated here that for large scale systems it may be infeasible to maintain the SMA proposed true end-to-end principle due to the increased number of BEXs between end-hosts and other infrastructure induced signaling. Giving up the design principle of true end-to-end security may also be required to enable support for legal interception.

As future work, we will examine the possibility to integrate SMA and EPS into a converged architecture. Under study will be such topics as to what degree it is possible to maintain the end-to-end security principle, and how to provide support for legal interception and host/user privacy in the architecture.

Acknowledgment

The authors would like to thank the partners of the Celtic MEVICO project for all fruitful discussions and their valuable advice on writing this paper.

References

[1] M. Olsson, S. Sultana, S. Rommer, L. Frid, and C. Mulligan, *SAE and the Evolved Packet Core: Driving the Mobile Broadband Revolution*, 1st ed. Elsevier, 2009.

[2] "Secure mobile architecture (SMA) vision and architecture," The Open Group, Tech. Rep., Feb. 2004.

[3] Pierre Lescuyer, Thierry Lucidarme, *Evolved Packet System (EPS). The LTE and SAE Evolution of 3G UMTS*. John Wiley and Sons, 2008.

[4] Alcatel-Lucent, *Introduction to Evolved Packet Core*, 2009, an Alcatel-Lucent Strategic White Paper.

[5] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol," IETF RFC 3261, Jun. 2002.

[6] 3GPP, *22.071 Technical Specification. Location Services (LCS); Service description; Stage 1, ver 9.0.0 (2009-12)*.

[7] C. Kaufman, "Internet Key Exchange (IKEv2) Protocol," IETF RFC 4306, Dec. 2005.

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

[9] Jose-Javier Pastor Balbas, Stefan Rommer, John Stenfelt, "Policy and Charging Control in the Evolved Packet System," *IEEE Communications Magazine*, pp. 68–74, Feb. 2009.

[10] R. H. Paine, "Secure mobile architecture (SMA) - a way to fix the broken internet," *Information Security Technical Report*, vol. 12, no. 2, pp. 85–89, 2007.

[11] R. Paine, *Beyond HIP: The End of Hacking as We Know It*, 1st ed. BookSurge Publishing, 2009.

[12] P. Nikander, A. Gurtov, and T. Henderson, "Host identity protocol (HIP): Connectivity, mobility, multi-homing, security, and privacy over IPv4 and IPv6 networks," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 2, pp. 186–204, 2010.

[13] P. Nikander, T. Henderson, C. Vogt, and J. Arkko, "End-host mobility and multihoming with the host identity protocol," IETF RFC 5206, Apr. 2008.

[14] P. Nikander and J. Laganier, "Host identity protocol (HIP) domain name system (DNS) extension," IETF RFC 5205, Apr. 2008.

[15] A. Gurtov, *Host Identity Protocol (HIP)*, 1st ed. John Wiley & Sons Ltd, 2008.

[16] P. Eronen, "IKEv2 mobility and multihoming protocol (MOBIKE)," IETF RFC 4555, Jun. 2006.

[17] J. Ylitalo and P. Nikander, "Blind: A complete identity protection framework for end-points," in *The Twelfth International Workshop on Security Protocols*, Apr. 2004.

[18] M. HeidariNezhad, Z. Ahmad Zukarnain, N. Udzir, and M. Othman, "Mobility support across hybrid IP-based wireless environment: review of concepts, solutions, and related issues," *Annals of Telecommunications*, vol. 64, pp. 677–691, 2009.

[19] B. Yahya and J. Ben-Othman, "Achieving host mobility using DNS dynamic updating protocol," in *LCN '08: 33rd IEEE Conference on Local Computer Networks*, Oct. 2008, pp. 634–638.

[20] A. Pappas, S. Hailes, and R. Giaffreda, "Mobile host location tracking through DNS," in *London Communication Symposium*, Sep. 2002.

[21] Z. Faigl, L. Bokor, P. M. Neves, R. A. Pereira, K. Daoud, and P. Herbelin, "Evaluation and comparison of signaling protocol alternatives for the ultra flat architecture," in *ICSNC '10: the Fifth International Conference on Systems and Networks Communications*, Aug. 2010, pp. 1–9.

[22] J. Y. H. So, J. Wang, and D. Jones, "SHIP mobility management hybrid SIP-HIP scheme," in *SNPD-SAWN '05: Proceedings of the Sixth International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing and First ACIS International Workshop on Self-Assembling Wireless Networks*, Washington, DC, USA, 2005, pp. 226–230.