Springer journals manuscript No.
(will be inserted by the editor)

Realization of Mobile Femtocells: Operational and Protocol Requirements

Suneth Namal · Madhusanka Liyanage · Andrei Gurtov

Received: date / Accepted: date

Abstract Femtocells are commissioned in wide range of commercial systems, such as CDMA, GSM, LTE, Wi-Fi, and WiMAX, and offer economically viable solutions to improve network scalability and indoor coverage. The ability to offer multitude of context-aware and value added services, and per-user customization have caught world-wide research interest on femtocells. In this article, we have investigated the feasibility to use femtocells as short-range mobile base stations, and discussed the demanding architectural requirements and challenges. The protocol stack on legacy femtocells must be modified to realize mobility. Mobility introduces new challenges in security and user privacy. Firstly, we analyze several candidate mobility protocols that are deployable on Mobile Femtocells (MFs). Among them, Host Identity Protocol (HIP) was chosen due to enhanced support in flexible mobility, security and end-user privacy. Secondly, we propose the indispensable modifications that enable device mobility, and the suitable transport architecture options based on direct IP links and relay chains. Finally, with the simulation results, the proposal is verified, and the architectural options are evaluated. That, in turn, proves the proposed mobility protocol has low latency in location locking with respect to another competing protocol and low resource utilization as it is depicted from mean round trip time.

Suneth Namal
University of Oulu, P.O. Box 4500, Oulu, FI-90014, Finland
Tel.: +358-41-7282646
Fax: +358-85-532845
E-mail: gkarunar@ee.oulu.fi

Madhusanka Liyanage
University of Oulu, P.O. Box 4500, Oulu, FI-90014, Finland
Tel.: +358-44-9160857
Fax: +358-85-532845
E-mail: madhusanka@ee.oulu.fi

Andrei Gurtov
University of Oulu, P.O. Box 4500, Oulu, FI-90014, Finland
Tel.: +358-85-532847
Fax: +358-85-532845
E-mail: gurtov@ee.oulu.fi

Keywords Mobile femtocells · Location verification · Configuration management · Authentication · Security · OMNeT++

1 Introduction

Femtocells are short-range cellular base-stations that extend the cellular coverage to indoor environments and enhance the user experience by means of the improved flexibility in per-user customization. In business perspective, operators prefer femtocells due to the fact that they exclude the cost that would be borne by the expensive backhaul links and the base stations.

Mobile users generally come-across the regions with no cellular coverage. Sudden drops disconnect the ongoing sessions that critically damages the Quality of Service (QoS). Urban areas with large constructions are highly probable of not having clear line-of-sight. Setting-up additional base stations would not be a solution to overcome this problem due to extremely high equipment and post-maintenance cost and heavy power consumption. As a result, operators prefer to deploy small cells that are economically viable. After all, guaranteed cellular coverage is trivial due to dynamic changes in channel condition. This problem narrows down to network optimization and architecture planning that are highly dependable on the infrastructure budget.

Access to the Internet has now even extended to trains, buses, automobiles and to flights. The increasing number of hand-held devices; smart phones, PDAs and laptops with built-in dual-band access, experience in-vehicle wireless services and gain access to high-speed Internet. Today, free Wi-Fi broadband access is available even in public transport, airports, and shopping malls. The transition between Wi-Fi and cellular access happens to disconnect the ongoing sessions. The significance of the femtocells is the ability to commission all possible services that are provided by macro stations including the session continuity.

In-vehicle Wi-Fi is an approach of subnetwork mobility. Femtocell is far beyond an ordinary base station or an access point in terms of low-cost, power efficiency, flexibility, deployability, and multi-discrepancy services that it can support. Internet, multimedia, and real-time audio and video burgeon in many aspects of today's human life. Certain applications process delay requirements depending on the services that they provide. Session continuity is a manifold research topic in the scope of mobility management. The MFs introduce a new approach to retain the ongoing sessions over cellular access.

Femtocell security and privacy broadly encompass the installation obligations, electromagnetic compatibility, authentication, anti-fraud protection, maintenance of lawful interception and network integrity, and protection from global adversary. The physical protection of the device is also important, since the locations that they are deployed are easily accessible to humans. Besides that, being an open IP device which is well understood by the hackers, possible attacks and threats on the femtocells have greatly increased [2,3]. To protect against them, the backhaul needs confidentiality, integrity, replay protection, support for firewall traversal, common network address and port translation, and etc [4]. Apart from these, location locking, service provisioning, and configuration management are couple of operational requirements in femtocells [5].

In this article, we investigate the theoretical obstacles in implementing MFs and appealing mobility and security requirements. The proposal is simulated on top of the OMNeT++ network simulation framework. This article is organized as follows. In section 2, we briefly describe the related work in this domain. Section 3 presents a feasibility study on this novel concept. Femtocell authentication is described in detail in section 4. In section 5, we present a secure location locking architecture, and in section 6 a configuration management sheme based on our proposal is presented. Section 7, illustrates two MF transport architectures. In section 8, the simulation results are presented, and finally, section 9 concludes the article.

2 Related Work

Dense deployment of small cells introduces co-channel interference between the neighboring cells. This is a critical deployment issue that coexists with MFs. Thus, it is important that they detect the frequency allocation of their neighboring cells and allocate an unoccupied resource block to avoid intercell interference [6]. However, the existing literature mainly focuses on static access of fixed femtocells where the policies do not dynamically change over time. Self organized femtocells were introduced in the recent past that count inter-cell interference, QoS classification and fair utilization of sub-carriers to improve end-user experience [7].

It is mandatory that the MFs intelligently detect and dynamically adjust the frequencies to avoid interference from/to neighboring cells. In [8], the impact of MFs in service outage probability and uplink throughput is presented. The results in [8] demonstrate how significantly they can reduce the outage probability while offering stable and high Signal to Noise and Interference Ratio (SNIR). Legacy femtocells use DSL access to establish the connectivity with the core network. In a typical case, femtocell traffic is tunneled through the Internet if no other service provider is specifically designated for direct delivery.

Because of this nature, femtocell backhaul is vulnerable to attacks. Security consultants with "Trustwave" have uncovered software and hardware vulnerabilities to gain root access to femtocells by sniffing the traffic, guessing passwords, changing IP address range, and investigating hardware printouts [9]. A security research group, "The Hacker's Choice" has reverse-engineered the femtocells operated by a British mobile operator and discovered that it could be used to make illegal calls and to send text messages [10]. Therefore, the current femtocell security mechanisms are inadequate to meet the desired level of protection.

In mobile communication, backhauling is one of the biggest challenge due to non line-of-sight problem and dynamic channel conditions. Operators have already introduced several wireless backhauling technologies, such as satellite, UMTS, HSDPA, and Wi-Fi for stationary and walking mobile users. Fast moving mobile stations mostly use satellite backhaul for high speed data transfer, though it has poor latency and fails in underground tunnels, covered areas and in bad weather conditions [11]. Besides that, modern mobile applications demand stable throughput. IP multihoming is an approach to improve service continuity and to maintain a stable throughput [12]. The results in [12] present throughput, handover latency and drop rate for multihomed MFs based on a simulation model.

3 Feasibility Study: Mobile Femtocells

Network operators prefer femtocell deployment due to low cost and enhanced cellular coverage. However, the problems related to billing, interference management, security, roaming and QoS management yet to be investigated in detail. The emerging user requirements in day-to-day human life introduce new challenges in mobile communication. The limited cellular spectrum generally is a problem in wireless communication. Co-channel interference is a challenge in femtocell deployment due to the interference by neighboring macro cells.

MFs with the proposed mobility suite are an improvement over the legacy 3GPP femtocells. It is important to allocate them a separate spectrum apart from the macro spectrum to reduce the interference. A legacy femtocell may transfer 50 - 100 Mbps of data when it is fully utilized. Thus, the wireless backhauling mechanism must be capable of providing a high bandwidth. When selecting a backhauling technology, it is important to consider cost, capacity, scalability, latency, availability, and installation and commissioning feasibility.

WiMAX, Microwave and E-Band are widely used wireless backhauling solutions that are proposed for distinct and predefined use-cases. MFs can use a similar backhauling mechanism and serve their subscribers with real-time, value-added, and context-aware services offered by operators. Providing guaranteed QoS in mobile communication is a challenge due to the wireless backhaul. Such solutions must also accomplish complete transport architectures for guaranteed traffic delivery. Some operators use satellite backhauls to transfer the traffic aggregated from in-vehicle Wi-Fi access points [11].

Modern multimedia applications insist seamless mobility. Thus, access to media content with automatic switching between environments, networks, and protocols must be enabled. 3GPP femtocell architecture and protocol abstraction are particularly designed for the fixed stations. Therefore, MFs must have own set of protocols to support device mobility. Proxy Mobile IPv6 (PMIPv6) and MOBility extension to Internet Key Exchange (MOBIKE) are the widely used mobility protocols in today's operator networks. But, they explicitly fit in distinct use cases and technologies.

3.1 Proxy Mobile IPv6 Protocol (PMIPv6)

PMIPv6 is one of the widely used and IETF standardized mobility protocol that supports network mobility [13, 14]. PMIPv6 nodes are topologically anchored at a Local Mobility Anchor (LMA) which is responsible for forwarding traffic to the registered mobile nodes and managing their binding states [15]. Protocol also accepts binding registration messages from Mobile Access Gateways (MAGs) that manage mobility related signaling on behalf of the mobile nodes. PMIPv6 nodes do not disconnect the associations even after changing the point of attachment to the network. Instead, mobile nodes use temporary IP addresses that are known as Care-of-Addresses (CoAs) to avoid their identities being changed while moving. Meantime, they share IP tunnels between MAG and LMA with other mobile nodes that are attached to the same MAG.

The CoA information reveals the location information to the core network. An attacker who is eavesdropping the network can observe these messages and track

the location for any harmful action. By eavesdropping the binding updates, an attacker can identify a mobile node by its Home Address (HoA) and also track it based on the granularity of the subnet [13]. Besides that, home agent is a single point of failure due to undesirable dependency on constant reachability. When MIP is used, there is no easy way of defining an alias for others or an identifier for a genuinely different host when two IP addresses are pointing to the same host. Also the malicious nodes can penetrate into the network, if proper authorization checks are not in place and may hijack a legitimate node's mobility session or initiate DoS attack. Thus, only the authorized MAGs in the PMIPv6 domain must be allowed to send binding update messages to LMA on behalf of a mobile node.

The trust between MAG and mobile node can be established in terms of proper authentication and authorization before entering to a network. Authentication attests that the binding between mobile node's identity and link-layer address is secure. Hence, the MAG can identify the legitimate mobile nodes from the packets received on the access links. At the same time, MAG should be trustworthy and may send the binding updates only for the mobile nodes that are presented in the same network. In other words, compromised MAGs are an open problem especially in non-3GPP access, such as WiMax, CDMA or WLAN. PMIP already uses IP Security (IPSec) and establishes Secure Associations (SAs) between MAG and LMA using Internet Key Exchange Protocol version 2 (IKEv2). These SAs are shared by the connected mobile subscribers to protect against replay attack and for integrity check.

MAGs must always be trustworthy and should not send binding updates on behalf of the mobile nodes that are not presented in the PMIP domain. However, the communication between the initiator and the responder is not bounded to end-to-end tunnels. Thus, PMIP communication is not end-to-end secure. Besides that, key exchange between MAG and LMA operates only in static configuration. As a result, the same key exchange protocol cannot be used to establish SAs if the MAG is mobile. MFs have the highest potential to locate the MAG functionality. However, it cannot be realized, since PMIP does not enable MAG mobility. Therefore, a different protocol must be chosen for mobility and key exchange between the MF and the core network.

3.2 Mobility Extension to Internet Key Exchange (MOBIKE)

An extension to Internet Key Exchange version 2 (IKEv2) which is known as MOBIKE provides strong Authentication and Key Management (AKM) for mobile users [16]. It almost replicates the same features of IKEv2 and bounds the associations to the IP addresses. Each time during the handover, the associations must be recreated and the previous sessions must be depreciated. MOBIKE also supports IP multihoming, though it does not support simultaneous movement (rendezvous mechanism) or route optimization [15]. However, it does not improve the resilience against Denial of Service (DoS) or Man-in-the-Middle (MiTM) attack, and does not provide protection for the indications from other parts of the protocol suite. Thus, attackers can spoof the indications from the layers below and confuse the liveness of the addresses.

MOBIKE highly relies on the delivery notifications for IKEv2 messages to determine the route. An attacker who manages to disconnect a communication

link can guide the traffic into a loop or force a particular address to get use. Network Address Translation (NAT) redirection is also possible by modifying the IP header of the NAT detection payloads (dead peer detection messages). Another weakness in MOBIKE is that it discloses the address and the network topology over the address update messages. In a nutshell, MOBIKE supports the mobility requirements that are committed by MFs, but does not provide the expected level of security.

3.3 Host Identity Protocol

HIP provides IP independent mobility and secure AKM for mobile stations. Security and mobility are the biggest challenges in realizing the femtocell mobility. As it was already mentioned, the legacy femtocells demand high bandwidth. Commissioning same services on MFs also requires high bandwidth identical to the legacy femtocells. HIP multihoming allows to establish multiple parallel tunnels between the hosts to improve the overall throughput [17]. HIP is capable of maintaining a stable throughput with flexible support for IP multihoming [12]. Besides that, session continuity is a complicated, but crucial requirement in mobile communication. Delay in handover directly affects the session continuity. For example, handover delay for Voice over IP (VoIP) applications should be less than 150 ms. Smaller the cell size the mobile user will experience frequent handovers that significantly degrades the throughput. Advanced handover techniques, such as Media Independent Handover (MIH) and multihoming can reduce the handover delay between the hosts.

Apart from those, online banking, Internet shopping, and e-channeling are some of the critical applications in terms of security. Therefore, MFs must support strong authentication, authorization, access control, and secure key management prior to deploying these services. Specially, key establishment and exchange must be strong enough to resist against the possible attacks. Femtocells can also be tempted to transfer the personal information over the backhaul. In wireless communication, the unsecure air interface is always accessible to any unauthorized user. Thus, an attacker can eavesdrop the communication and reveal the user confidentiality. Furthermore, impersonated or compromised femtocells can overload the network. As a result, subscribers may experience QoS degradation or even resource unavailability.

An unauthorized user who gains access to the femtocell can also use the services and network infrastructures without any charge. He also can misuse the resources for his own purpose. All security threats for legacy femtocells fall under one of the following category.

- User privacy
- DoS and general service availability
- Fraud and service theft

These vulnerabilities may mostly encounter in the wireless backhaul, Internet or femtocell itself. However, it is certain that secure authentication, message encryption, and access control can reduce these vulnerabilities. Considering the HIP's capabilities in security and flexible mobility, it can be the best potential protocol

among several other candidate protocols to be commissioned in MFs. In application's point of view, HIP is a secure mobility management protocol, though it is a strong AKM scheme in developer's perspective. It introduces a new name space which is statistically globally unique. Base EXchange (BEX) is the core of the HIP that mutually authenticates two hosts.

A host's identity can be represented either by Host Identifier (HI) or Host Identity Tag (HIT). HI is the public key of an asymmetric key-pair. However, HI is not suitable to serve as a packet identifier, since the length of the public keys may vary. The HIT is a 128-bit hashed representation of HI. The Fig. 1 presents HIP-BEX which is a SIGMA-compliant 4-way handshake in order to establish a Diffie-Hellman (DH) key exchange and a pair of IPSec Encrypted Security Payload (ESP) SAs [18]. The SAs are bound to HITs and therefore provide seamless mobility over the dynamic change of attachment. The $I1$ packet which includes the initiator's HIT and optionally the responder's HIT triggers BEX. It is replied with the $R1$ packet that contains the DH key, a cryptographic challenge that must be solved by the responder and the responder's public key. HIP is capable of storing and precalculating the keying materials to reduce the delay in handover.

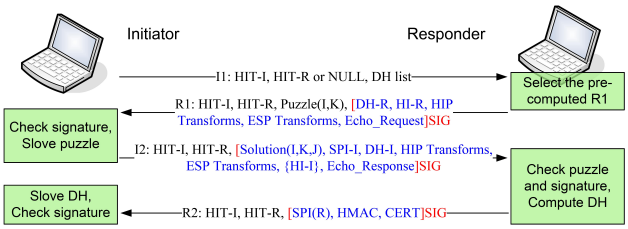


Fig. 1 HIP-BEX 4-way handshake.

Responder also signs the $R1$ packet with its public key before it is sent. This allows the initiator to authenticate the responder at the same time. A cryptographic puzzle is included by the responder to prevent certain types of resource exhaustive attacks. The initiator also computes the DH session key and creates a HIP association using the derived keying materials. Then, initiator concatenates new $I2$ message that includes the solution to the challenge, DH session key and its public key. After receiving $I2$, the responder verifies the puzzle solution and computes the DH session keys, decrypts HI, and verifies the signature on $I2$. The last $R2$ message contains the Security Payload Index (SPI) to establish the SAs between the initiator and the responder, a Hash-based Message Authentication Code (HMAC) computed using the session key, and a signature. Now, the SAs are established. Thus, the traffic flow can be initiated. Since the keys are shared only between the end-hosts, the encryption is possible only by them. Therefore, decryption is not possible even if an attacker intercepts or monitors the traffic in-between. Furthermore, HITs are self-certified by the way that they are generated.

IP multihoming is an extension to HIP that configures multiple IP addresses simultaneously on the same device [17]. The new IP configurations must always be informed to the responders using "LOCATOR" parameter. The UPDATE packet during the handover carries the information of the additional locators over which a node can be reached. To avoid conflicts, HIP recommends to use separate ESP

anti-replay windows for each of the interfaces or addresses to receive packets from the hosts when multiple locators (IPs) are configured. Such a host must indicate its responders of its most preferred locator if more than one is reachable at the same time. Otherwise, multiple locators can be used for load balancing or handover management. It is important to note that HIP does not disconnect the upper layer associations during the handover, since they are built on top of the HITs. Thus, renewing an IP address does not affect the ongoing sessions. Therefore, the sessions can be maintained throughout the whole life of the associations. Besides that, IP addresses become absolute topology anchors that can be used in location locking.

3.4 Mobile Femtocells: User and Control Plane Requirements

Mobile femtocells provide solutions in certain unambiguous use cases in which thousands of mobile users may daily come-across. For example, in-vehicle cellular coverage that makes the time spend on public transport services or personal vehicles usable and entertained. The attraction towards the MF is the multitude of services (context-awareness and ability to per-user customization) that cannot be simply provided with ordinary Wi-Fi access points. Operators are researching on mobile base stations to use them on high speed trains. The current solutions already provide high speed Internet access inside the fast moving trains with Wi-Fi access points located in the carriages. They mostly use expensive satellite connections for backhauling.

LTE femtocells (H(e)NBs) connect to the core network through the S1 interface [19]. The S1 Application Part (S1AP) is responsible for initial context transfer, mobility related signaling, paging, error indication, load balancing, Network Attachment Subsystem (NAS) signaling transport, location reporting, status transfer, and etc [20, 21]. Mobility poses modifications and new challenges in the protocol level. Fig. 2 presents the proposed modifications to the S1 user and control planes that enable mobility. However, it is important to optimize these modifications in order to reduce the impact on the current architecture. The S1 user-plane is modified by introducing HIP that provides flexible IP mobility.

Radio Link Control (RLC) must now use the HIP identities, namely HITs. Thus, RLC methods must be built on top of the HITs but not on top of the IP addresses. Hence, they can support mobility over the S1 interface. In 3GPP, GTP (GPRS Tunneling Protocol) and PMIPv6 (Proxy Mobile IPv6) based interfaces are defined for mobility support. This proposal comes out with new HIP interfaces for mobility support. Accordingly, the whole protocol suite must adopt HIP identifiers by replacing the dynamically changing IP addresses. Theoretically, it is feasible since the new identifiers are almost similar to the IPv6 address format.

GTP is a group of communication protocols that is used to carry General Packet Radio Service (GPRS) within GSM, UMTS, and LTE networks. A GTP tunnel is identified with Tunnel Endpoint IDentifier (TEID), UDP port number, and IP address. While TEID is used to identify the tunnel endpoint in a receiving GTP-U protocol entity, the IP address and the UDP port number is used to establish a connectionless path between two end points. The control-plane RLC layer must also adopt HIP and new identities. Thus, control messages must carry HITs as node identifiers. HITs represent the permanent user identities which are cryptographically verified and globally unique. They are embedded by the operator

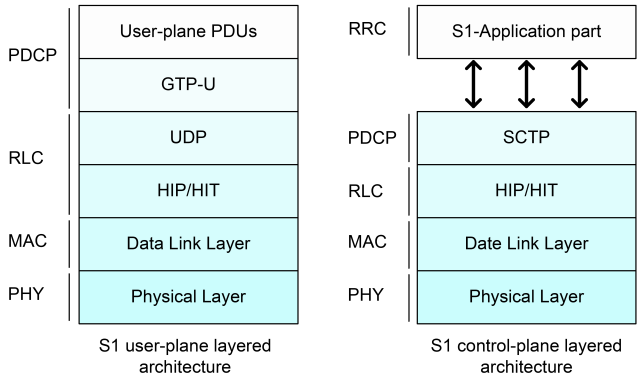


Fig. 2 S1 user-plane and control-plane stack.

or the manufacture. Thus, GTP must now use the HIT and UDP port number to establish the tunnels.

In a nutshell, layers above the network layer must now use the HIP identifiers, namely HITs instead of IPs. Thereby, Stream Control Transmission Protocol (SCTP) and S1 Application Part (S1AP) must replace IPs with HITs. At last, IP addresses will be used only in network layer routing. Decoupling identity/locator functions allows MFs to move freely without disconnecting the ongoing communication sessions that are built on top of the HITs.

4 Femtocell Authentication

This section presents the legacy 3GPP femtocell authentication and MF authentication based on HIP. 3GPP femtocells must mutually authenticate with the Security GateWay (SeGW) using Internet IKEv2 [1]. They use public-keys and signature based authentication with certificates to gain access to the core-network. These certificates are provided by a mobile operator, femtocell manufacturer, vendor or a trusted third party. Similar type of certificate which is provided by an operator trusted Certificate Authority (CA) is configured at the SeGW to authenticate it to the femtocell during the mutual authentication phase. A femtocell stores the security credentials, such as private key of the certificate and other critical cryptographic functions in its Trusted Environment (TrE). TrE is also responsible to perform cryptographic operations during the boot-up and authentication [1].

IKEv2 authentication with certificates is described in the RFC 4306 [22]. Femtocells can be customized to perform mandatory device authentication with or without optional hosting party authentication that is handled by the Hosting Party Module (HPM). HPM is known to be tamper resilient module which contains the credentials for identification and authentication. This module consists of a contractual agreement between the hosting party and the network operator. Thus, it can be replaced or inserted into another femtocell. Hosting party authentication is performed with EAP-AKA (Extendible Authentication Protocol - Authentication and Key Agreement) which is described in [1].

Meanwhile, SeGW operates as an EAP authenticator by forwarding the EAP messages to the AAA (Authentication, Authorization, and Accounting) server in

order to retrieve an authentication vector from AuC (Authentication Centre) via HSS (Home Subscriber Server). As a result of successful authentication, pair of unidirectional IPsec tunnels will be established between the femtocell and the SeGW. During the tunnel setup, supporting ESP authentication and encryption transforms are negotiated over the IKEv2 signaling. Mobility extension to IKEv2 supports IP multihoming, though it does not support simultaneous movement (rendezvous mechanism) and route optimization [16]. Furthermore, IKEv2 does not resist against DoS or MiTM attack during the exchange. Moreover, the operation at the responder is expensive with IKEv2 compared to the puzzle mechanism or cryptographic challenge that the initiator must solve in HIP handshake.

4.1 HIP Authentication with Certificates

Device authentication is an essential preconfiguration of femtocell security. Besides that, authentication must validate the integrity. 3GPP femtocells perform mandatory device authentication and optional hosting party authentication. Fig. 3 presents the network elements that are involved in the authentication phase. During the boot-up, authentication happens only between the SeGW and the femtocell though hosting party authentication extends it towards the AAA and the HSS. Femtocell connects to the core-network over an Internet backhaul which is insecure and prone to attacks. To protect traffic through the Internet backhaul, SAs are established in either direction as a result of successful authentication.

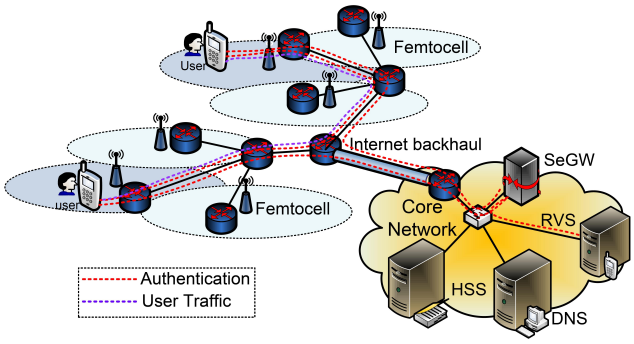


Fig. 3 Femtocell authentication and related network elements.

BEX alone is not sufficient to provide expected level of security. A skillful MiTM attacker can easily manage all the parts of the protocol. Using certificates in third and forth messages during the authentication host identities can be verified. HIP defines "CERT" parameter, which is a container for digital certificates to transport them over the control packets during authentication and handover [23]. Certificate Authority (CA) is responsible for issuing and managing security credentials and public-keys for message encryption. CA issues a certificate as part of a Public-Key Infrastructure (PKI) after checking with Registration Authority (RA) to verify the information that is provided by the requester [23]. The SeGW delivers its certificate in the third packet, whereas the femtocell delivers its certificate

in the forth packet (Fig. 4). With certificates, responders can verify whether the messages are originated at the clamed initiators. Thus, an attacker who is trying to impersonate a legitimate femtocell can be ignored. Moreover, femtocells can also associate with neighboring cells by using the same certificate based authentication.

SeGWs are vulnerable to non-intentional DoS attacks after sudden power cuts in large scale. During the next boot-up, thousands of femtocells may initiate to authenticate at the same time. Thus, it will create a huge I_1 storm towards the SeGW. Therefore, SeGWs must be capable of handing such resource exhaustive attacks. By the design of HIP, cost of setting-up a state at the responder is cheaper compared to it is at the initiator. Moreover, it can be adjusted according to the network conditions and the level of trust. To avoid overloading the SeGW, the same technique can be used. TCP_SYN or "start of transport" packets without prior authentication are rejected by the SeGW and the initiators are requested to authenticate before they transmit. It is known as opportunistic negotiation. By sending a simple pre-made packet which is fixed and easily replayable, SeGWs can be protected from TCP_SYN packet flooding. Besides that, the limited exposure of identities to DoS and MiTM attacks during the authentication is a significant advantage of HIP.

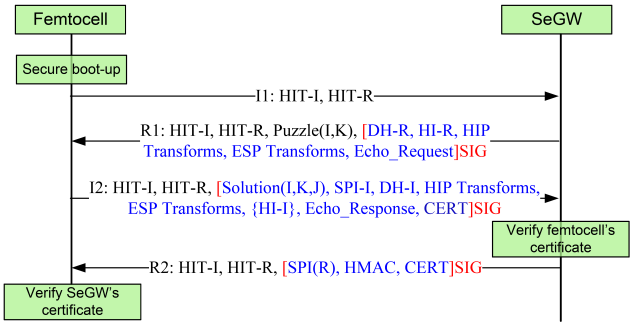


Fig. 4 HIP based authentication with certificates.

5 Secure location locking/relocking

There is a high probability that the subscribers may relocate their femtocells from the original locations. It is a violation of the contractual agreement between the subscriber and the operator. 3GPP femtocells capture the location information from the neighboring cells, subscribers, and the information available within itself for location verification. The drawback is that they must trust their neighbors and subscribers. Besides that, the compromised femtocells can replay the previously stored data that happens to misconfigure the locations. Thus, the misconfigured femtocells may appear to be on manipulated locations.

LTE femtocells use fixed access line end-points, IP addresses, GPS, and radio signatures to obtain the location information [24]. The information is more reliable and secure enough when they use access line identifiers to determine their locations. IP addresses alone are not secure enough to use in location locking,

since compromised femtocells can easily impersonate their addresses by misusing NAT. However, it provides a preliminary verification by denying unauthorized femtocells that are configured with invalid or blacklisted addresses. Location verification function must be carried out within the TrE and protected during the transmission and storing.

Further, TrE must check the integrity of location verification function in bootstrapping and transmission. It is also responsible to protect the information that is obtained during the location verification process. The explained verification methods are secure with location authentication which is intended to protect the femtocell from attackers. Multiple location identification techniques simultaneously can detect the location more preciously. Location verification is a sensitive function in terms of security and must be protected from the malicious acts.

5.1 Location Locking and Security Considerations

Operators bind the IP addresses and the physical ports of the access network with the geographical information in order to verify the location. A network database stores the identification and location information correspond to the IP address and allows to obtain the port number, address and location information in terms of latitude and longitude. This method is not reliable when a femtocell is connected to the Local Area Network (LAN) through a Virtual Private Network (VPN). It is recommended to use this method combined with another method to improve the reliability. Location locking scheme is a combination of location registration and verification.

The registration happens only once when a femtocell connects to the core-network, whereas location verification happens each time it moves to a new location or in continuous time intervals. 3G femtocell triggers this procedure by sending a request message to its Access point Home Register (AHR) which is distinguished from the Home Location Register (HLR) that registers the User Equipment's (UE) location [24]. AHR sends a location information query message to Connectivity session Location and Repository Function (CLF) with the IP address that is received from the previous message. CLF queries its database to obtain the access line identifier, such as NAS port which is represented with an IP address and a port number.

AHR uses this information to determine the location of the femtocell in registration. When a legacy femtocell is deployed, operator agrees on a location for regulatory requirements. Thus, the contract location must be checked and verified by the network each time the femtocell requests to reconnect. Location authentication based on the reports received from the base stations happens according to the IP based approach. Femtocell also scans the neighboring base stations and sends location registration request messages to the AHR with the base-station ID and location area each time when it is powered-up.

Then, AHR can compare the received location information with the information already in the database. The communication paths and the network elements in a location authentication architecture is presented in Fig. 5. However, these methods alone do not meet the accuracy required in constrained applications. Furthermore, location verification using the information received from the GPS enabled handsets introduces a risk of advertising false location information by

an organized set of UEs. When the femtocell has built-in GPS or Assisted-GPS (A-GPS) capability, location information can be sent during the access request. This approach is not always reliable in terms of location identification, since the femtocells can be cleverly manipulated by expertise.

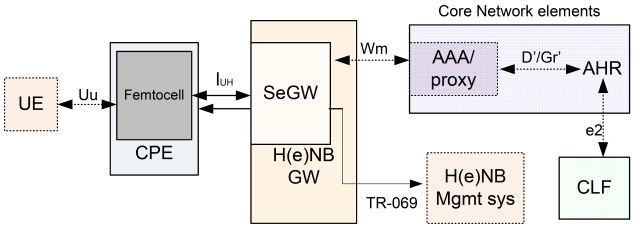


Fig. 5 Femtocell location authentication architecture.

It was proven that a femtocell can obtain an IP address by emulating a VPN over a public network infrastructure [24]. Thereby, a manipulated femtocell can be connected to the core-network from an unregistered location. It is a risk and a violation of the operator agreement. Similar manner, an attacker can impersonate an IP address that belongs to a legitimate femtocell. Besides that, attackers can block or simulate the location information from the neighboring cells and emulate the IP addresses by using VPNs. This could be achieved by using 2G signal jammers, GPS generators or other attenuation methods, such as operating in a covered area or by wrapping with an aluminum foil [24]. Furthermore, an adversary might move his femtocell to avoid being tracked by government agencies or to avoid it being billed for expensive calls.

The current location verification techniques are not secure enough to avoid misuse. Latter discussion demonstrates how VPNs can be manipulated to misuse 3G femtocells during location authentication. The attack vectors that we have discussed so far also affect on the LTE femtocells as well. Since, they are generally connected to the core-network through an access device (DSL modem, router etc.), an attacker on an associated VPN can use them from an unauthorized location in the same VPN or by proxying the connection via a home based network.

Location verification in LTE networks must be performed within the H(e)NB Management System (H(e)MS) as it is defined in TS 33.320 [5]. Similar to the 3G femtocell architecture, TR-069 protocol transfers the location information to the H(e)MS which is capable of verifying the geolocation of the H(e)NB. The architecture relies on the messages from the H(e)NB, but not from the others. When a femtocell is set-up behind a NAT, it is recommended to use a Session Traversal Utilities for NAT server (STUN) which reports the public IP address back to the femtocell.

5.2 Location Locking/Re-locking with HIP

Location locking is important not only for access authorization but also for service provisioning. This section describes how HIP can be utilized to avoid the threats in location locking. First, we analyze the properties of HIP that can be reused in

identifying the host's location. HIP has two representations of identifiers, such as HI and HIT. HI is the public-key that directly represents the pure identity whereas HIT is a fixed 128 bits hash of HI that represents an operational identity. It is a one-way hash which is impossible to reverse in order to obtain the public key. HITs are statically unique and the probability of overlapping them is negligible.

While HIT operates as an identity to the femtocell, IP address operates purely as a locator that depicts only the location. The location verification is considered as a sensitive function which is not necessarily to be carried out within the TrE. During the registration, femtocell sends a request message to AHR or verifying node that queries the CLF database for the access line location identifier. This control packet must also include femtocell's HIT. After receiving the message, verifying node or CLF can confirm that the message is originated at a legitimate femtocell. In addition to the IP address and the access line identifier, we suggest that the CLF database may include the HIT over which the query can be performed to track the movement of the device. This information can be used in provisioning the services based on context awareness.

6 Configuration Management Architecture

Femtocells need concurrent software updates to cope with newly introduced services and applications. In LTE architecture, H(e)MS is the core-network element which is responsible for the software updates. HNB Management System (HMS) is responsible for the same function in a 3G network. The corresponding network elements are specified in 3GPP standards, namely TS 32.593 and TS 32.583 [25, 26]. The H(e)MS may be located within the operator network or outside the network. It is also responsible for configuration management, location verification, file transfer, fault management, and discovery of serving H(e)MS, SeGW, and MME (Mobility Management Entity). H(e)MS has two components within it, namely file server and TR-069 manager. Fig. 6 presents the legacy femtocell management architecture.

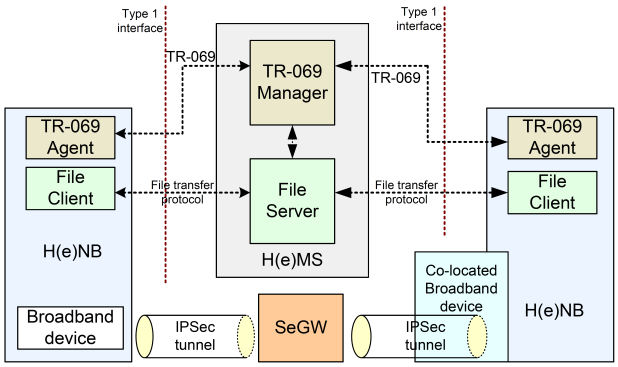


Fig. 6 3GPP Femtocell Management Architecture.

According to their responsibilities, H(e)MSs are divided into two, namely Initial H(e)MS and Serving H(e)MS. The initial configurations, such as location verification, assignment of serving SeGW, MME, and discovery of serving H(e)MS will be handled by the initial H(e)MS. Besides that, identity verification, configuration management, fault management, performance management, and MME discovery are performed by the serving H(e)MS. After acquiring an IP address and establishing a secure IP connection with the initial H(e)MS, the H(e)NB establishes a SA with the serving H(e)MS using discovery procedure. The IP assignment happens during the discovery of serving H(e)MS or during the registration procedure by the serving H(e)MS.

The serving H(e)MS may be located inside the operator network or in the public Internet. Depending on their deployment, the discovery procedure may change. If it is located inside the operator's secure domain, the H(e)NBs may be preprogrammed with the IP address of the initial H(e)MS and the initial SeGW. By using the IP address or the Fully Qualified Domain Name (FQDN), H(e)NB establishes a secure IPSec tunnel with the initial H(e)MS. Then, H(e)NB creates a TR-069 session with the H(e)MS to exchange device ID, location information, and other parameters. According to the information that is received from the initial H(e)MS, the H(e)NB establishes a new association with the serving H(e)MS over the far-end S1 interface address which is delivered during the registration. After establishing an IPSec tunnel with the serving H(e)MS, the previous association with the initial H(e)MS will be depreciated. A modification to this procedure is illustrated in Fig. 8.

This procedure is lengthy and vulnerable to attacks. When the initial H(e)MS is located in the public Internet, femtocells are preprogrammed with H(e)MS's FQDN which is published in a public DNS. The IP connectivity with the initial H(e)MS is established using Secure Sockets Layer/Transport Layer Security (SSL/TLS). Thereupon, the femtocell queries the private DNS to obtain the address of the serving H(e)MS. With the previous information, H(e)NB starts registration with the serving H(e)MS and configures an IP address on the S1 interface and an IPSec usage indicator by invoking the "SetParameterValues" Remote Procedure Call (RPC) method which is defined in the serving H(e)MS. TR-069 describes the methods and parameters of the RPC methods [27].

Followed by the successful registration with the serving H(e)MS, the H(e)NB's TR-069 agent will be triggered by the serving H(e)MS to download the configuration files. This procedure can be initiated at any time when new configurations are readily available. By invoking the "Download" RPC method, H(e)MS triggers the H(e)NB to download the files given the file type, file size, source location, and username and password to the file server. Correspond to the transport protocol which is inferred from the source location URL argument of the Download method, the H(e)NB initiates the download. After, new configurations are completely downloaded and successfully applied on the H(e)NB, it is indicated to the H(e)MS. If the download fails, the configurations that are already downloaded will not be applied. However, latter described configuration management is optional.

TR-069 managers are programmed with mandatory configuration management using TR-069 RPC "SetParameterValues" method. Similar to the previous approach, H(e)NB establishes a TR-069 session with H(e)MS and invokes the "SetParameterValues" RPC method to configure a list of parameters and corresponding values on the H(e)NB. By receiving the list of parameters, H(e)NB configures

the new parameter values and then determines the status argument value which is sent back over the "SetParameterValueResponse" method before the session is torn-down. Note that the mandatory configuration procedure uses the "SetParameterValues" RPC method to configure the parameters. The optional file download procedure uses the "Download" RPC method and a transport protocol, such as FTP, SFTP, HTTP or HTTPS to download the configurations.

Configuration management procedure also includes the management of IPSec tunnels. Thus, the changes in H(e)NB's inner IPSec tunnel addresses must be informed to the H(e)MS using the "Inform" RPC method over a TR-069 session. By acknowledging the "InformRequest" method defined in TR-069, the H(e)MS acknowledges the new IP address before a TR-069 session is torn-down. Besides that, alarm reporting is a part of the configuration management. It uses the same TR-069 session to report the alarms over "SetParameterValues" method and takes "ReportingMechanism" parameter as an argument.

The TR-069 manager initiates this procedure call and H(e)NB acknowledges the completion by triggering the "SetParameterValuesResponse" method. Note that the alarms at H(e)NB are reported to the TR-069 manager using a procedure that depends on the "ReportingMechanism" parameter of an alarm. H(e)NB uses the "Inform" method to report the alarms directly to the TR-069 manager. This procedure call is only applicable to the alarms that are classified as "expedited handling" and "queued handling". After all, a successful reporting is acknowledged by sending an "InformResponse" message back to the H(e)NB.

6.1 Secure Configuration Management in Vehicular Femtocells

TR-069 provides message confidentiality and allows different authentication techniques. It also cooperates with SSL/TLS which provides confidentiality, data integrity, and authentication based on certificates to accomplish the modern security requirements [28]. Other than that, shared secret based authentication is provided at the HTTP layer of the Customer Premises Equipment (CPE). Additionally, SSL can also encrypt the traffic under HTTPS. SSL/TLS transports the TR-069 protocol though it can be used directly over a TCP connection. However, in the second approach, some aspects of security is sacrificed. Thus, H(e)NBs may use shared secrets or certificates to verify their identities.

In a nutshell, SSL or TLS is used to transport the management protocol but not to authenticate the devices. When SSL/LTS is used, the H(e)NB must authenticate the H(e)MS using a network certificate which is provided by the H(e)MS. The H(e)MS may accept a validated device certificate or allow SSL/TLS sessions to be established even without a certificate provided by the H(e)NB. If H(e)NB is not authenticated using SSL/TLS, H(e)MS must authenticate the H(e)NB by digest authentication using HTTP. During the authentication, HTTP uses a password as a shared secret that must be unique and should not be shared with any other H(e)NB. It is important to note that, in this case, the H(e)NB plays the role of a HTTP client while H(e)MS plays the role of a HTTP server.

With SSL/TLS, reusing the passwords significantly degrades the security of an established session and can be vulnerable to replay attack against H(e)MS. Security with TLS and its forerunner SSL are designed to provide security in public Internet. TLS and SSL encrypt network segments over the transport layer

using asymmetric cryptography for key exchange and symmetric cryptography to provide privacy and message authenticity for integrity protection. In terms of security, SSL 3.0 is less desirable compared to TLS 1.0 due to the key derivation process. According to the key derivation, a half of the SSL 3.0 master-key is an output of a fully dependent MD5 hash function which is not resilient to collisions. In other words, TLS 1.0 master-key is a dependent output of both MD5 and SHA-1 which is considered comparatively stronger than SSL 3.0.

Vulnerabilities against TLS 1.0 and all versions of SSL are revealed in 2009 by using plaintext injection. Additionally, protocol defines Simple Object Access Protocol (SOAP) to encode the syntax to transport RPC methods and responses. None of these protocols support mobility and not intended to provide authentication. When a femtocell is mobile, neither SSL nor TLS will perform as it is expected. Thus, MF protocol stack must be modified to enable device mobility. Among several candidate protocols, we identified that HIP has the highest potential to replace SSL/TLS. Fig. 7 presents the proposed modifications. SSL/TLS in abbreviated handshake mode can enable key reuse on top of HIP-DEX or HIP-BEX. However, the certificate exchange in SSL or TLS is not mandatory with HIP since HITs are self-certified.

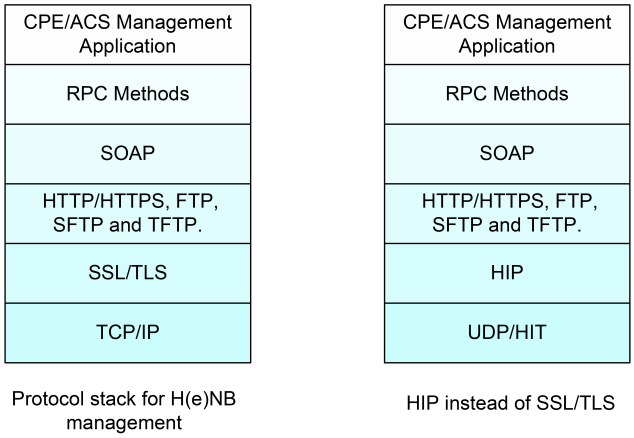


Fig. 7 Mobile femtocell protocols stack.

The communication overhead with HIP is lower than SSL/TLS. During the connection establishment, HIP outperforms SSL/TLS in terms of scalability in large communication networks with centralized H(e)MSs. HIP-DEX is a light protocol compared to SSL/TLS in terms of the dependency on cryptographic hash functions. SSL/TLS uses additional cryptographic functions, such as SHA-256 to improve security whereas HIP-DEX uses Elliptic curve Diffie-Hellman (ECDH) and Advanced Encryption Standard (AES) that are stronger than SHA. Based on our analysis, it is beneficial to use HIP-DEX to communicate OAM (Operation, Administration and Management) data. After all, Fig. 8 depicts the message exchange during the initial set-up when H(e)MS is not in a secure private network domain. Furthermore, DNS queries for the initial SeGW and H(e)MS if it is in a secure domain before the TR-069 exchange is initiated.

The communication with an external H(e)MS which is located in the Internet or inside an insecure domain is prone to security vulnerabilities. Thus, they must implement strong authentication, encryption, and access control to protect them against the security threats and to control exposure of sensitive information. In order to understand the H(e)MS discovery procedure in Fig. 8, assume an IP connectivity is already established during the boot-up between the H(e)NB and Internet or the external insecure domain where the H(e)MS is located. In first place, H(e)NB establishes an IP connectivity with the initial H(e)MS using HIP. It is important to note that the H(e)NB must have a reference to the IP address of the Initial H(e)MS.

If it is necessary, this address can be used to query the public DNS for the IP address which corresponds to the FQDN of the Initial H(e)MS. Thereupon, the H(e)NB establishes a SA and a TR-069 session with the initial H(e)MS. It is initiated by sending an Information request message that includes the device ID and additional parameters if needed. The H(e)MS accepts the session by sending an Information response message over the TR-069 session. The initial H(e)MS invokes the "SetParameterValue" method to configure serving SeGW's and serving H(e)MS's IP addresses and the far-end IP address of the S1 interface. The S1 interface IPs may be provided at this stage or in a later stage during the registration with the serving H(e)MS.

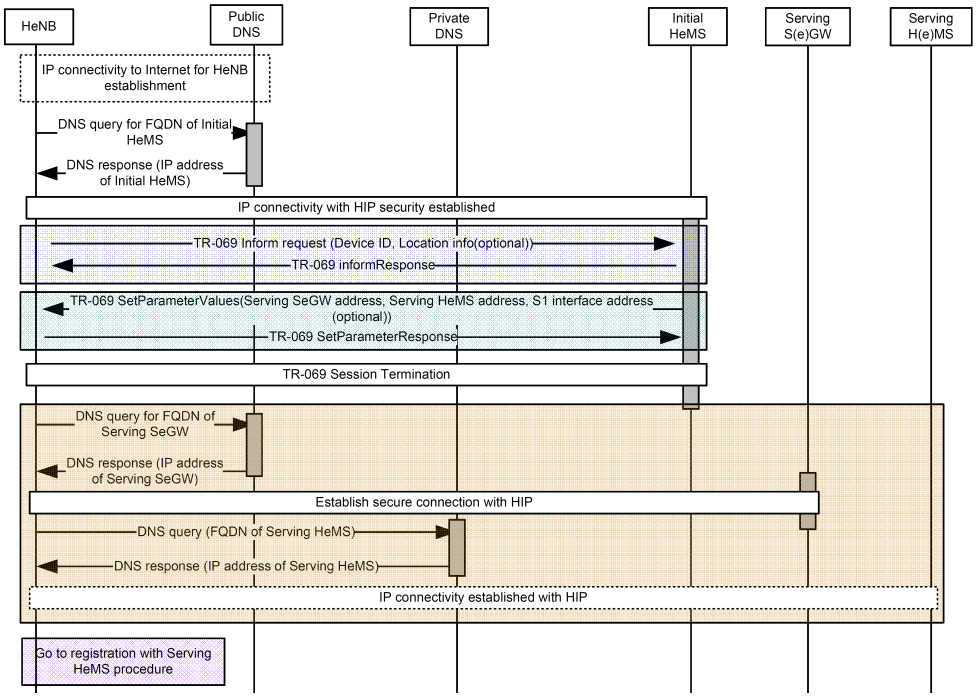


Fig. 8 Serving H(e)MS Discovery via Initial H(e)MS accessible on the public internet.

Then, H(e)NB terminates the TR-069 session with a "SetParameterValuesResponse" message that acknowledges the parameters. The H(e)NB again queries the

public DNS for the IP address of the serving SeGW if it is not provided. Then, they establish a SA using HIP to perform registration and other management functions. Thereby, H(e)NB queries the private DNS to obtain the IP address of the serving H(e)MS, if it is not sent in the previous exchanges with the initial H(e)MS. Then, H(e)NB establishes an IP connectivity with the serving H(e)MS using HIP and initiates the registration. In this approach, communication is protected with HIP and enables flexible device mobility since the associations are built on top of HITs. Using HITs as identifiers, TR-069 can now perform configuration management on mobile femtocells.

7 Mobile Femtocell Backhaul Architectures

This section presents two potential transport architectures that are applicable in MF communication. Core network traffic offloading is one of the main advantages of legacy femtocells. MFs are intended to provide a stable cellular coverage in mobile environments, such as in public transport services and in personal vehicles. LTE subscribers demand comparatively high bandwidth due to multimedia and real-time traffic that they would like to experience. As a result, operators started to deploy small cells to meet the demanding bandwidth requirements. In femtocell technology, operators are not responsible for the operational and maintenance cost of the device. Therefore, deploying small cells is cheaper compared to the cost of deploying large macro cells. However, MF is a novel concept which is not yet discussed within the 3GPP scope.

The MFs must have inbuilt techniques to avoid interference, since they can be affected by the neighboring cells while moving. If the same spectrum is shared with the macro cells, the probability of overlapping the frequencies is even higher. Technically, this can be reduced by assigning a separate frequency range for the MFs or by implementing dynamic frequency adjustment techniques, such as frequency hopping. Since radio spectrum is a scare resource in operators' point of view, assignment of a separate frequency range may be trivial. As a consequence, dynamic frequency adjustment techniques must be embedded to MFs.

Traffic backhauling is a challenge due to constrained applications that demand no packet drops, stable throughput, and minimum delay. Practically, it is impossible to maintain a stable and high bandwidth wireless connection due to non line-of-sight problem. In this section, we have proposed the transport architecture solutions that facilitate the demanding high bandwidth requirements. To address the non line-of-sight problem, wireless relays can be mounted on the street-poles to relay traffic from the MFs to the nearest macro cells. Fig. 9 presents such a transport architecture with wireless relays. The relays in Fig. 9 forward the traffic directly towards the macro cell over direct IP links. This architecture may not fit in a general case due to the maintenance cost and the large constructions beside the roads. Thus, it is preferred to use wired backhauls to transport the traffic from relay stations to the macro cells (ex: telephone lines). However, the direct IP links on clear line-of-sight reduce the backhaul latency.

The second transport architecture option which is presented in Fig. 10 differs from the first architecture by the way that they handle traffic forwarding. This architecture defines relay chains that forward traffic along the chain to a target pole which is on clear line-of-sight with the macro station. The target pole is

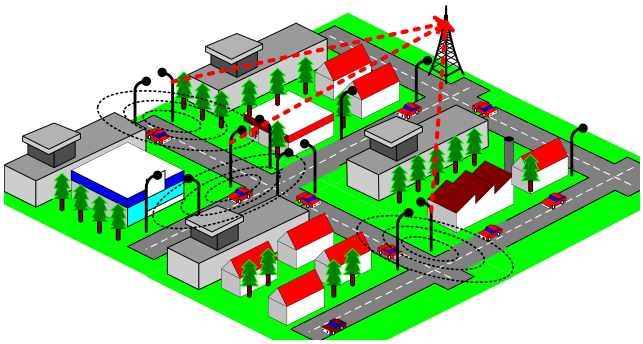


Fig. 9 Direct IP links.

chosen such that it can aggregate the traffic from as many relay chains. Most likely, the target pole can be chosen from a junction or a dense area to improve the Quality of Experience (QoE) on as many subscribers. Compared to the first architecture, the second architecture is cost-effective, since only a selected set of relays with clear line-of-sight forward the traffic to the macro station. However, the first architecture has low latency, since each of the relays is directly connected to a macro station though it incorporates high maintenance cost. In the second architecture subscribers may experience more delay as a result of the relay chains though it incorporates low maintenance cost.

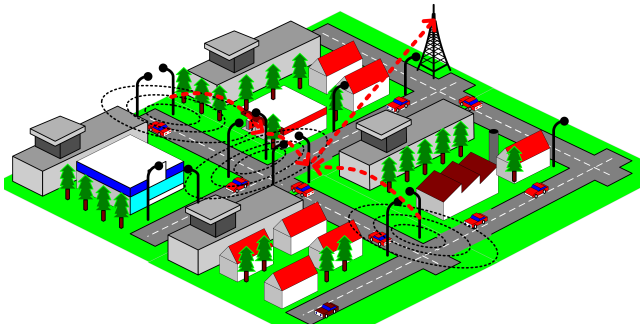


Fig. 10 Relay chains.

However, the efficiency of these transport architecture solutions also depends on the mobility protocols. The wireless backhaul between the relays and the macro cells may not meet the service requirements for certain constrained applications. To comply them, wired connections can be used instead of unstable and error-prone wireless links. This approach can be cost-effective over a long period of time compared to the maintenance cost of wireless backhauls. Thus, it is recommended use over-laying or under-laying telephone lines to establish the relay chains between the poles to deliver traffic.

8 Simulation Results

This section presents the results based on a OMNeT++ simulation model. The OMNeT++ simulation framework is an open source, component-based simulation tool that is designed to model communication networks. We also use HIPSim++ (HIP based simulation framework) and xMIPV6 modules (an accurate and extensible mobile IPv6 simulation model for OMNeT++) that are built on top of INET to evaluate the transport architectures with different mobility protocols [29–31]. The model simulates the transport architecture options which are defined in the previous section and analyze the performance of MIPv6 and HIP mobility protocols on top of them.

The LTE architecture defines default/dedicated bearer activation procedures to send context activation requests that contain the parameters to request a new IPv6 address. In addition, IPv6 must use a Router Solicitation message which is answered with a Router Advertisement from the GGSN (Gateway GPRS Support Node) to finalize the IPv6 address creation over an user data bearer. After an IP address is assigned, MFs must initiate authentication and location verification to comply the requirements that are defined in TS 33.320 [5]. According to the standards, femtocells must use TR-069 protocol to transfer the location information to the H(e)MS. Each time after changing an IP address, H(e)MS must perform location verification. Verifying the geo-IP distribution is the simplest and the fastest preliminary test for location verification. The location updates must be immediately sent to the H(e)MS when an IP is updated or location is changed.

The mobility protocols must complete the initial location registration at the H(e)MS as a result of successful authentication. This simulation models cost-effective Wi-Fi relays that are mounted on the street poles to deliver MF traffic. The poles are located in average of 300m away from each other. The transport architecture may use either direct IP links or relays chains over under-lying or over-laying telephone lines. The MFs must update the detailed location information at the H(e)MS followed by the authentication [5]. The initial location verification test based on IP geo-location can be integrated to the authentication to deny the misconfigured or compromised femtocells with invalid or conflicting IP addresses. Reliable location verification is important in access control and also in services provisioning. We propose that the mobility protocol handles IP authorization at the H(e)MS using the standard registration procedure.

If an invalid assignment is identified, the H(e)MS sends back an error message to deny the connection. When MIPv6 is used, the Binding Update (BU) message type is used to notify the peers of the new CoA that can be used to inform the new IP assignments to the H(e)MS. By sending a Binding Acknowledge (BA) message, the H(e)MS can authorize the new bindings. If the address is blacklisted or does not follow the rules of geo-IP distribution, the location verification must send an error message by denying the connection. Before sending an acknowledgement, H(e)MS must verify the binding address with return routability test. The Home Test Init (HoTI) message initiates the test by requesting a home keygen token from the H(e)MS. The following Care-of-Test-Init (CoTI) message requests a care-of keygen token from the H(e)MS. Furthermore, the return routability test introduces an additional security to the BU messages by using the shared secret key to protect the message integrity.

The initial shared keying materials can be used for identity verification. By sending an acknowledgement message, H(e)MS must accept the new IP addresses if they are not blacklisted or violated the rules of geo-IP distribution. MIPv6 takes comparatively long time to update and authorize the IP assignment due to return routability check. Location verification with MIPv6 also encounters the delay in triangular routing. Besides that, HIP does not need a return routability test. The HIP "UPDATE" message type can be used to trigger the initial location verification with the H(e)MS. Using the source HIT of the message, H(e)MS can easily find and update the correct entries of the database. If MIPv6 is used, the BU messages must carry the previous IP address together with the new link local address to query the correct mapping at the H(e)MS.

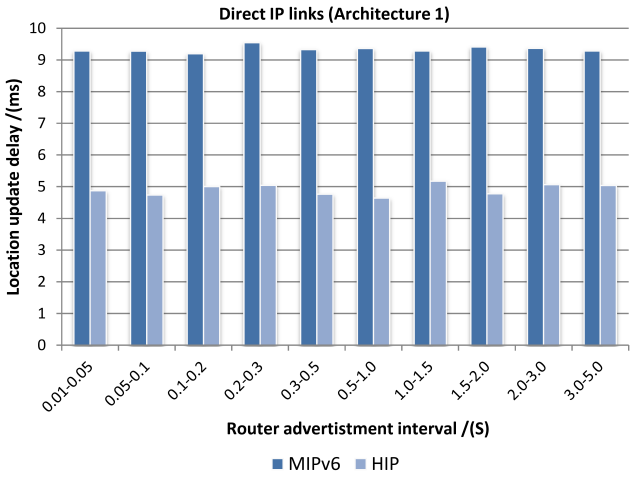


Fig. 11 Location update latency with direct IP links.

Fig. 11 and Fig. 12 compare the location verification latency with the H(e)MS in terms of the delay which is introduced by the indispensable negotiations during the IP authorization process. When considering the transport architecture options defined in the previous section, it was identified that the delay depends on both transport architecture and mobility protocol. Thus, right combination of a mobility protocol with a transport architecture may have an extra advantage. According to the simulation results in Fig. 11 and Fig. 12, the latency with MIPv6 is always higher than the latency with HIP due to the extra overhead which is introduced by the return routability test.

Fig. 13 and Fig. 14 present an indication of network performance by means of Internet Control Message Protocol (ICMP) Round Trip Time (RTT) in between the core-network and a femtocell which is moving at a constant speed. RTT is a signpost of the standing queues and congestions other than the distance between the nodes. When MIPv6 is used, mean RTT significantly differs from direct IP links to relay chains. The first transport architecture option with direct IP links has low RTT than the relay chains. As per the measurements, there is no significant difference between the transport architectures when HIP is used. This behaviour was experienced due to direct IP routing from source to destination despite the

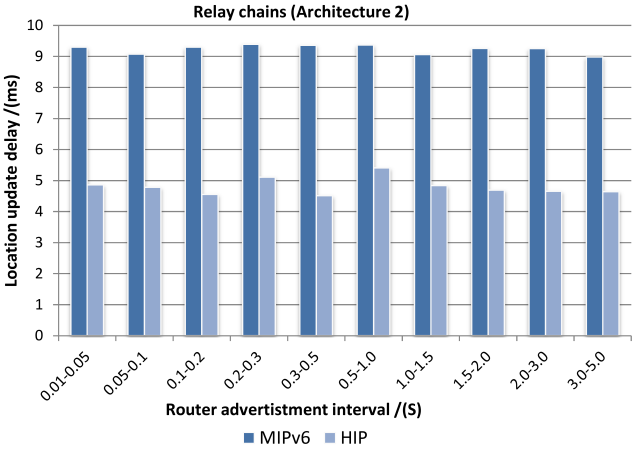


Fig. 12 Location update latency with relay chains.

triangular routing in MIPv6. However, the second architecture introduces more delay when longer the relay chain.

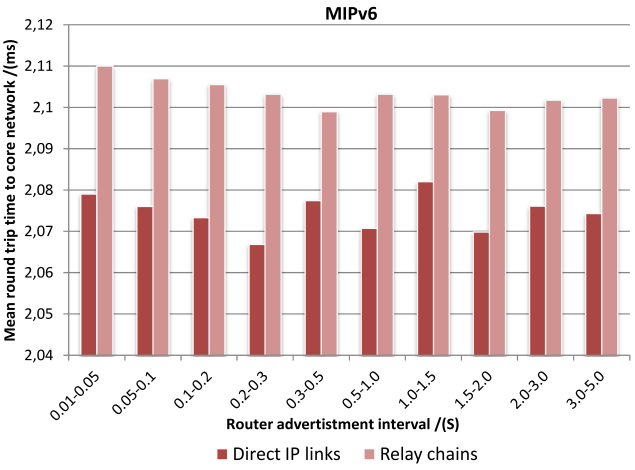


Fig. 13 Mean round trip time with MIPv6.

The modern constrained applications are sensitive to the variance of packet transmission delay which is known as jitter. The real-time audio and video applications are particularly sensitive to jitter. Jitter is typically measured in cooperation with an end-device. Jitter significantly degrades the quality of audio and video services, especially with real-time applications. To overcome this problem, operators must use jitter buffers in their networks. In a nutshell, lower the jitter, the networks can provide better QoE. The Fig. 15 and Fig. 16 present the jitter of ICMP ping requests in different transport architecture options.

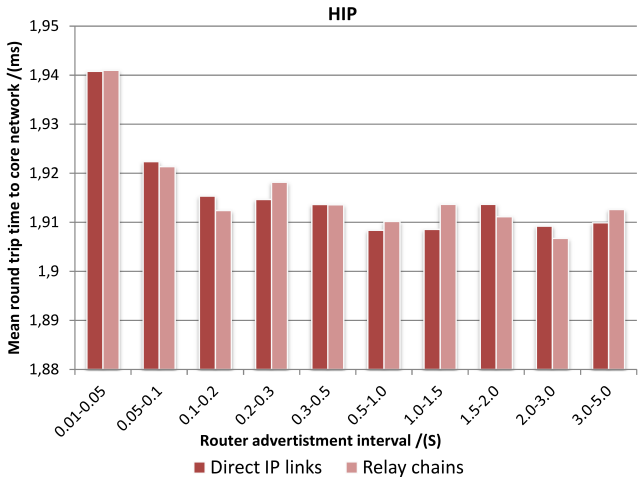


Fig. 14 Mean round trip time with HIP.

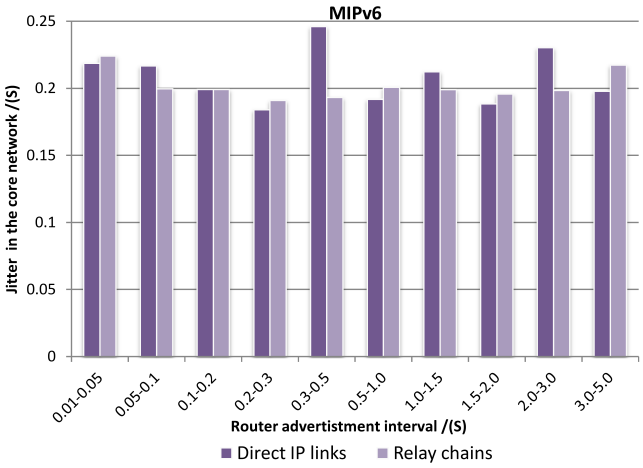


Fig. 15 Jitter in transport architectures (with MIPv6).

Similar to the RTT measurements, we use ICMP Echo requests that are initiated from the MF to the core-network to measure ICMP jitter. According to Fig. 15 and Fig. 16, the ICMP jitter in a MIPv6 network is flat though a high variance was experienced in a HIP network. In certain cases, jitter in the HIP network is lower than it is in the MIPv6 network. But, in most of the cases, jitter in the HIP network is higher than it is in the MIPv6 network. Furthermore, with MIPv6, there was no significant difference in jitter between the architecture options though it was high with HIP. This indicates the utilization of network resources, such as bandwidth and buffers by the mobility protocols. Fig. 16 implies that HIP consumes more network resources compared to MIPv6 though it outperforms in many other perspectives. The simulation uses HIP-BEX that consumes more CPU and memory. But, HIP-DEX which is a light version of BEX is faster and consumes less CPU compared to BEX to provide equivalent level of security

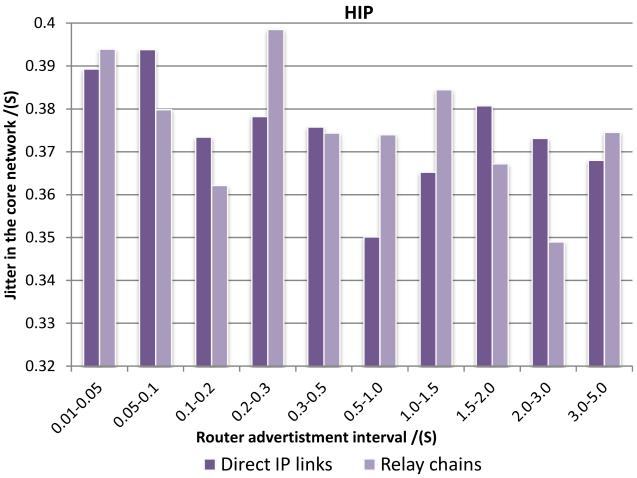


Fig. 16 Jitter in transport architectures (with HIP).

and mobility. Thus, HIP-DEX could be a potential secure mobility protocol for MFs.

9 Conclusion

This paper is an attempt towards the realization of the novel concept of mobile femtocells. We introduce the operational and protocol requirements to enable mobility over MF's S1 interface. Firstly, we discuss the challenges and requirements for realization of this concept. Then, we propose protocol level modifications to make the legacy femtocells mobile. Secondly, the mandatory operational requirements, namely authentication, location verification, configuration management, and advanced security requirements in congestion with femtocell mobility are investigated.

Then, we discuss how beneficial it is to deploy HIP in S1 user and control planes. Thirdly, we introduce two cost-effective transport architecture solutions based on direct IP links and relay chains that backhaul MF traffic. Using the simulation model developed on top of OMNeT++, these transport architectures are evaluated and compared in terms of mean RTT and jitter. The results depict that the location update and network performance depend not only on the architecture but also on the mobility protocols. Therefore, the operators must choose the best combination of a transport architecture with a mobility protocol based on the expected QoS, resource availability, and the implementation/maintenance cost. We also measure the location verification latency which is a critical parameter in terms of service continuity. It was identified that the HIP deployment has notably low latency in location update than the MIPv6 deployment in both transport architecture solutions.

The identity/locator separation in HIP enables MFs to move freely without disconnecting the upper layer associations. Thus, it is not necessary to recreate the associations from the beginning at each time during the handover. This is a

significant advantage compared to PMIPv6, MIPv6, or MOBIKE. HIP effectively supports multihoming, allowing the unique name of a multi-accessible entity to be mapped to multitude of locations where it is reachable. Besides that, multihoming can be used to improve the overall throughput and to reduce handover latency and packet loss. HIP also extends the support for secure signaling delegation. That, in turn, can be used to implement application-level service delegation and subnet mobility. The idea behind the cryptographic delegation is simple but powerful.

Though HIP does not directly address the problems of privacy and accountability, they are provided in other means. The use of cryptographic identities are self certified, thereby provides automatic identity authentication. Separation of identities and locators makes it easy to hide the topological location from the attackers. The privacy extensions to HIP allow to hide the identities from the third party network entities in a commercial network. In a nutshell, when considering the simulation results and the protocol attributes, HIP has very high potential to be commissioned in MFs.

Acknowledgements This work has been performed in the framework of the CELTIC project CP7-011 MEVICO. The authors would like to acknowledge the contributions of their colleagues. This information reflects the consortiums view, but the consortium is not liable for any use that may be made of any of the information contained therein.

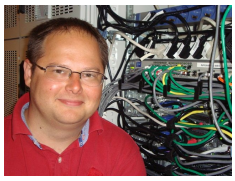
References

1. Technical Specification Group Service and System Aspects; Security of Home Node B (HNB) / Home evolved Node B (HeNB), 3GPP TR 33.820 version 8.3.0 Release 8, December 2009.
2. Nikander P.,Gurtov A. and Henderson T.R., Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks, Communications Surveys & Tutorials, IEEE , vol.12, no.2, pp.186-204, Second Quarter 2010.
3. Gurtov A., Host Identity Protocol (HIP): Towards the Secure Mobile Internet, John Wiley publications, United Kingdom, vol.21, 2008.
4. Namal S. and Gurtov A. and Bennis M., Securing the Backhaul for Mobile and Multihomed Femtocells, in Proceedings of the Future Network & Mobile Summit (FutureNetw) 2011, IEEE, pp.1-15, 15-17 June 2011.
5. Technical Specification Group Service and System Aspects; Security of Home Node B (HNB)/Home evolved Node B (HeNB), 3GPP TR 33.320 version 9.1.0 Release 9, 2010.
6. El-Din N.D. and Sourour E.A. and Ghaleb I.A. and Seddik K.G., Femtocells Interference Avoidance Using Femtocell Identification, in Proceedings of the 28th National Radio Science Conference (NRSC), IEEE, pp.1-9, 26-28 April 2011.
7. Namal S. and Ghaboosi K. and Bennis M. and MacKenzie A.B. and Latva-aho M., Joint Admission Control & Interference Avoidance in Self-organized Femtocells, in Proceedings of the 44th Asilomar Conference on Signals, Systems and Computers (ASILOMAR), IEEE, pp.1067-1071, 2010.
8. Chowdhury, M.Z. and Lee, S.Q. and Ru, B.H. and Park, N. and Jang, Y.M., Service Quality Improvement of Mobile Users in Vehicular Environment by Mobile Femtocell Network Deployment, in Proceedings of the International Conference on ICT Convergence (ICTC), IEEE, pp.194-198, 2011.
9. Ray B., Femtocells Wilt Under Attack, Available: http://www.theregister.co.uk/2010/02/02/femtocell_security/, 2010.
10. Bright P., Insecure Vodafone Femtocells Allow Evesdropping, Call Fraud, Available: http://arstechnica.com/security/news/2011/07/insecure-vodafone-femtocells-allow-eavesdropping-call-fraud.ars, 2011.
11. Nokia Siemens Networks, Thalys High Speed Train Passengers Enjoy Broadband Internet Access, Available: http://www.nokiasiemensnetworks.com/sites/default/files/document/45396726766.pdf, 2008.

12. Namal, S. and Pellikka, J. and Gurtov, A., Secure and Multihomed Vehicular Femtocells, in Proceedings of the 75th Vehicular Technology Conference Vehicular Technology Conference (VTC Spring), IEEE, pp.6-9, May 2012.
13. Dutta A., Lin F.J., Das S., Chee D. and Yokota H., Proxy mobile IP, Google Patents, US Patent App. 12/012,014, 2008.
14. Yan Z., Zhang S., Zhou H., Zhang H. and You I., Network Mobility Support in PMIPv6 Network, in Proceedings of the 6th International Wireless Communications and Mobile Computing Conference, ACM, pp.890-894, 2010.
15. Noriega-Vivas P.,Campo C., Garcia-Rubio C. and Garcia-Lozano E., Supporting L3 Femtocell Mobility Using the MOBIKE Protocol, in Proceedings of the 2nd International Conference on Access Networks, ACCESS, pp.30-35, 2011.
16. Kivinen T. and Tschofenig H., Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol, RFC 4621, Internet Engineering Task Force (IETF), 2006.
17. Nikander P., Henderson T., Vogt, C. and Arkk J.,End-Host Mobility and Multihoming with the Host Identity Protocol, RFC 5206, Internet Engineering Task Force (IETF), 2006.
18. Moskowitz R., HIP Diet EXchange (DEX), draft-moskowitz-hip-rg-dex-06 (work in progress), Internet Engineering Task Force (IETF), 2012.
19. Li, X. and Weerawardane, T. and Zaki, Y. and Timm-Giel, A. and Gorg, C., Recent Advances in Broadband Integrated Network Operations and Services Management, IGI Global Publishing, pp.135-139, 2011.
20. Li Z. and Wilson M.,User Plane and Control Plane Separation Framework for Home Base Stations, Fujitsu Scientific and Technical Journal, vol.46, no.1, pp.79-86, Fujitsu Ltd, 1015 Kamikodanaka Nakahara-ku, Kawasaki-shi, 211, Japan, 2010.
21. Technical Specification Group Radio Access Network;Evolved Universal Terrestrial Radio Access Network (E-UTRAN); S1 Application Protocol (S1AP), 3GPP TR 36.413 version 10.3.0 Release 10, September 2011.
22. Kaufman C. and Hoffman, P. and Nir, Y. and Eronen, P., Internet Key Exchange Protocol Version 2 (IKEv2), RFC 5996, Internet Engineering Task Force (IETF), 2010.
23. Heer T. and Varjonen S., Host Identity Protocol Certificates, RFC 5201, Internet Engineering Task Force (IETF), 2011.
24. Borgaonkar, R. and Redon, K. and Seifert, J.P., Experimental Analysis of the Femtocell Location Verification Techniques, in Proceedings of the 15th Nordic Conference in Secure IT Systems (NordSec) Helsinki, Finland, 2010.
25. LTE: Telecommunication management: Home enhanced Node B (HeNB) Operations, Administration, Maintenance and Provisioning (OAM and P): Procedure flows for Type 1 interface HeNB to HeNB Management System (HeMS), 3GPP TR 32.593 version 11.0.0 release 11, 2011.
26. Telecommunication management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM and P); Procedure flows for Type 1 interface HNB to HNB Management System (HMS), 3GPP TR 32.583 version 10.2.0 release 10, 2011.
27. Bernstein J., Spets T., Bathrick G., Pitsoulakis G., DSL Forum TR-069: CPE WAN Management Protocol, in Proceedings of DSL Forum, 2004.
28. Nie P., Vähä-Herttua J., Aura T. and Gurtov A., Performance Analysis of HIP Diet Exchange for WSN Security Establishment, in Proceedings of the 7th ACM symposium on QoS and security for wireless and mobile networks, ACM, pp.51-56, 2011.
29. Varga A., Modeling and Tools for Network Simulation, Springer-Verlag Berlin Heidelberg, pp.35-59, 2010.
30. Bokor L., Novaczki S., Zeke L.T. and Jeney G., Design and Evaluation of Host Identity Protocol (HIP) Simulation Framework for INET/OMNeT++, in Proceedings of the 12th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems, ACM, pp.124-123, 2009.
31. Yousaf F.Z., Bauer C. and Wietfeld C., An Accurate and Extensible Mobile IPv6 (xMIPV6) Simulation Model for OMNeT++, in Proceedings of the 1st international conference on Simulation tools and techniques for communications, networks and systems & workshops, ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), pp.88, 2008.
32. Technical Specification Group Services and System Aspects; Service requirements for Home Node B (HNB)and Home eNode B (HeNB), 3GPP TS 22.220, vol.9.8.0 release 9, 2011.

Suneth Namal received the B.Sc. degree in computer engineering from the University of Peradeniya, Peradeniya, Sri Lanka in 2007. He completed M.Eng degree in Information and Communication Technologies from the Asian Institute of Technology, Bangkok, Thailand, in 2010 and M.Sc. degree in Communication Network and Services from Telecom SudParis, Paris, France, in 2010. Currently he is a Doctoral student with the Department of Communication Engineering, University of Oulu, Oulu, Finland and a research scientist of Centre of Communications, Oulu, Finland. His research interest includes mobile femtocells, fast initial authentication, load balancing and network security.

Madhusanka Liyanage received the B.Sc. degree in electronics and telecommunication engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2009, the M.Eng. degree from the Asian Institute of Technology, Bangkok, Thailand, in 2011 and the M.Sc. degree from University of Nice Sophia Antipolis, Nice, France in 2011. He is currently a Doctoral Student with the Department of Communications Engineering, University of Oulu, Oulu, Finland. His research interests are mobile and virtual network security.



Andrei Gurtov received M.Sc (2000) and Ph.D. (2004) degrees in Computer Science from the University of Helsinki, Finland and M.Sc. (2001) in Applied Mathematics from Russia. He was appointed a Professor at University of Oulu in the area of Wireless Internet in December 2009. He is also a Principal Scientist (on leave currently) leading the Networking Research group at the Helsinki Institute for Information Technology. He is an adjunct professor at the Aalto University and University of Helsinki. In 2000-2004, he was a senior researcher at Sonera Finland. In 2003-2005, he was a visiting researcher in the International Computer Science Institute at Berkeley, USA. In 2004, he was a consultant at the Ericsson NomadicLab. At Internet Engineering Task Force, Dr. Gurtov co-chaired the Host Identity Protocol Research Group (2005-2012) and co-authored six RFCs. He supervised four PhD and 20 Master's theses. He is a senior member of IEEE and received the best paper award at IEEE Globecom'11. Dr. Gurtov is a co-author of over 100 publications including two books, research papers, and patents. His publications received more than 1000 citations according to Google Scholar. His research interests include network security, peer-to-peer systems, transport protocols, mobile communication systems, and game theory.