Securing the Backhaul for Mobile and Multi-homed Femtocells

Suneth Namal, Andrei Gurtov, Mehdi Bennis
Centre for Wireless Communications
University of Oulu, P.O. Box 4500, FI-90014 Oulu, Finland
Email: [namal, gurtov, bennis]@ee.oulu.fi

***Abstract*—The evolution of femtocells in residential networks expects to accelerate dramatically in next few years. The Femto Access Points (FAPs) connect subscribers to the operator through the residential broadband access or the public Internet. The connectivity between the FAP and the core network has a high risk of being compromised. In this paper, we have discussed, how Host Identity Protocol (HIP) can be adapted in femtocell technology. This research work presents several enhancements to the femtocell technology such as strong authentication, service registration, identity verification and node multi-homing. In addition, Encapsulating Security Payload (ESP) is used to provide confidentiality, data origin authentication, connectionless integrity, anti-replay service and limited traffic flow confidentiality. Moreover, enhanced mobility support by means of locator/identity separation and node multi-homing is discussed in the scope of 3GPP femtocells.**

I. Introduction

The evolved communication technology introduces widespreading residential access points that enable mobile communication through the residential networks. The mobile networks can be widely spanned with the introduction of femtocells extending the operator network to subscriber residence. The home based FAPs enable access to cellular networks over the broadband connectivity. FAPs are 3G hot-spots to which the mobile users can connect over the same Global System for Mobile Communications (GSM) band. Even, FAPs may be WiFi enabled to support WiFi handsets. The Evolved Packet Core (EPC) architecture based on all-IP concept is adapted in femtocell technology.

LTE focuses on the extensive use of subscriber installed FAPs for improved network coverage and high-speed connectivity [1]. FAP establishes IPSec tunnels in either direction through the backhaul to protect the communication from attackers. It is realized that the connectivity between FAP and Secure GateWay (SeGW) is vulnerable to attacks since, both control and data traffic is carried over the unreliable broadband access or public Internet. Thus, protecting femtocell backhaul is a crucial requirement for secure communication.

The open access FAPs are somehow problematic, since the number of subscribers can be served simultaneously is limited [2]. Increasing number of mobile nodes attached to FAP may degrade service quality or prevent desired subscribers accessing operator network. Therefore, access control is a critical requirement in femtocell technology. On the other hand, close access FAPs filter subscribers using Closed Subscriber Groups (CSG), though it may reduce the overall performance of the system [3]. The existing femtocell architecture demands globally unique routable identity to be assigned on each connected device. In case of lacking IP addresses, mobile nodes that demand addresses to configure on it will not be served. For this reason, some operators implement address translation and address mapping in certain devices along the path. When it comes to mobility, IP addresses as identifiers result problems in user mobility. Therefore, identity, locator separation is highly demanded in mobile applications. HIP introduces a new identifier which obligates the rules of Domain Name Service (DNS). Thus, the change in IP address correspond to the point of attachment may not affect transport layer associations.

In this paper, we propose a modification to the existing protocol stack of the 3GPP femtocell architecture. We are more focused into mobility and security issues related to femtocell technology. This research work propose several enhancements to the femtocell technology such as, service registration, identity verification and node multi-homing. Section II describes the background of femtocell security including threats over public network IP backhaul together with an introduction to HIP. The proposed HIP backhaul solution is discussed in Section III. Furthermore, this section introduces the HIP based transport architecture in femtocell technology. Finally, Section IV presents evaluation scheme given the conclusion in Section V.

II. Security Architecture Overview

A. *Femto Access Point Security*

The femtocell security consists of FAP authentication and message encryption across the unreliable public network. Femtocell backhaul is vulnerable to any external attack since, there is no guarantee of security by the network provider. The femtocell security aspects are not yet standardized according to the 3GPP specifications [4]. Thus, there are many ongoing research efforts to enable an end-to-end secure communication in femtocell technology.

FAP authentication is a major consideration in femtocell security. In general, FAP authentication is performed using Extensible Authentication Protocol Method for Authentication and Key Agreement (EAP-AKA), certificate or as a combination of both. The 3GPP standard presumes validation and authentication to be performed sequentially. Thus, during the initial power-up, FAP gets authenticate to the core network. If the certificate based authentication is used, the mutual authentication between the FAP and the core network is performed with X.509 certificate which is already configured at FAP and SeGW. Rather, Universal Integrated Circuit Card (UICC) that defines the identity of the secondary hosting party is used for the authentication [4]. The FAP's Trusted Environment (TrE) [4] holds these credentials that are used to authenticate it to the core network. It is important to protect the certificate and any other data such as certificate revocation list during the operational lifetime and the time it is provisioned. Thus, a malicious user who attempts to manipulate the public key to impersonate the SeGW can be easily isolated. If EAP-AKA based authentication is used, the credential should be provisioned in the TrE of the FAP for non-3GPP access.

However, there is a high risk of compromising the authentication token via a brute force attack or a local physical intrusion. Further, a valid authentication token can be inserted into a manipulated FAP and can be used for harmful actions. The UMTS standard defines security in four domains such as network access security, network domain security, user domain security and application domain security [4], [5]. However, femtocells confront major security problems in locating a mobile user based on UICC and signaling messages, eavesdropping, DoS to User Equipment (UE) and core network and attacks on data integrity [5].

The exposure of the core network to the Internet is the major vulnerability in this architecture. This inspires the intruders to execute Internet-based attack such as, node impersonation, DoS or Distributed DoS (DDoS). The exposure of a public IP to the Internet through which FAPs access the operator network is a potential point of failure in the femtocell architecture. For instance, it is well-known that many large companies have confronted DoS attacks [6], [3]. Distributed security mechanisms are more effective in detection of DDoS attacks since suppression mechanisms are most powerful close to the origin of the attack [5]. However, the protection against such attacks demand the cooperation with Internet Service Provider (ISP) as well as the neighboring ISPs.

B. Femtocells Mobility Issues

In the network layer, mobile nodes are identified by the IP address which is based on the actual topological location. In other words, IP address depicts both location and the identity of a particular mobile device. In general, overload nature of IP is a problem in IP domain. Mobility management becomes more crucial when the active sessions get interrupted by the change of point of attachment to the Internet. If IP addresses are only geographical locators, they identify the location of the mobile node but not the identity. Hence, there should be an additional technique to represent the identifier role which is relied at the transport protocol.

In handover, upper layer protocols such as IPSec guarantees security though, it is only capable of applying and agreeing certain encryption standards between the nodes. This is somehow inefficient and unconvincing since, it does not help to mitigate Denial of Service (DoS) or node impersonation. Deployment of evolved mobile applications need extensive support of security and mobility. But, extended security may increase the communication overhead and processing power. Security a device can promise depends on signaling overhead and processing power of mobile device.

The support of advance mobility and multi-homing scenarios such as simultaneous multi-access, network mobility, application mobility and session mobility together with seamless vertical handover are few challenges in existing femtocell architecture. Certain types of applications such as online games, movies and video calls demand high bit rate over the channel. The smooth handover between the femtocells carries a significant performance indication in terms of quality of service towards the mobile users including pedestrian and vehicular users. However, this handover scenario demands close investigating of the features inevitable to femtocells.

C. 3GPP Specified Backhaul

The validation of FAP demands mutual authentication and initiate secure associations in either direction as a result of the authentication. An IP address is assigned to the FAP as a result of successful authentication and the secure backhaul connections are established in either direction for inbound and outbound traffic. These IPSec tunnels are established based on Internet Key Exchange version 2 (IKEv2). It provides layer-3 security and supports port and Network Address Translation (NAT). The Figure 1 presents the femtocell architecture that consists of several major components such as Security Gateway (SeGW), Home Subscriber System (HSS), evolved NodeB (eNB), Packet Data Network gateway (PDN-GW) and Mobility Management Entity (MME).

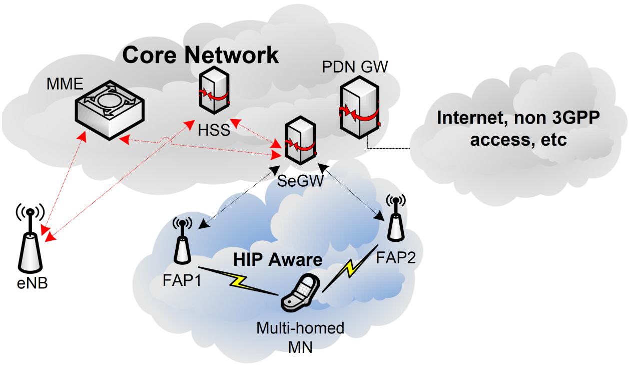

Fig. 1. Architecture model for Home NodeB access network.

Acquiring an IP address FAP creates secure tunnel to SeGW. Separate tunnels through the backhaul can be established to exchange different type of traffics such as Operation Administration and Maintenance (OAM), validation and QoS information while primary tunnel is used to transmit bare traffic and signaling. When the peer node is not behind the same SeGW, the platform integrity should be verified alone the backhaul connection during the validation procedure. Hence, a separate network element should keep track on the state of validation of the platform integrity conjunction in the backhaul connection. Ultimately, this approach dictates an additional complexity keeping track of the states of each device platform integrity over the backhaul connection. Moreover, if a device is validated only at the authentication, the validity of platform integrity must be revised. Thus, an update policy for platform integrity validation procedure is executed in case of modification or termination of a backhaul connection. Further, this information is reflected to other devices which keep track of the platform integrity.

D. An Introduction to HIP

HIP introduces globally unique name space other than the domain name space and IP address which is chosen to be the public key of an asymmetric cryptographic key pair. When the host changes its location, it updates the IP address. For this reason IP address can not be used as an identifier. HIP maintains the separation between location identity and host identity. In HIP, pubic key is a globally unique name and is chosen as the Host Identifier (HI). The Host Identify Tag (HIT) of 128 bits is generated taking a (Secure Hash Algorithm) SHA-1 cryptographic hash over the HI.

HIP introduces a new layer to the TCP/IP suit detaching the transport layer from the network layer. The transport layer accepts the packets with HIT and port address regardless of the IP address. The transport layer identifies the source and destination with the HITs in the HIP packet. The HIT-IP mapping is done at the layer below to enable packet routing towards the destination. Decoupling transport layer from networking layer results a HI to be a pure identifier and an IP to be a pure locator. Entering to new domain, mobile node reconfigure the IP address correspond to the point of attachment to the core network or Internet. However, HIT does not change due to change in location. Thus, mobile node has freedom to change IP address dynamically by DHCP, NAT, PPP or IPv6 prefix assignment [7].

HIP nodes run base protocol to create a secure tunnel as a result of successful mutual authentication. Base protocol defines a four-way handshake between the initiator and the responder [8]. Base protocol performs base exchange [9] as a simple key exchange mechanism for mutual authentication. First, the initiator sends a clear I_1 packet to the responder to convince its desire to attach. Then, the responder replies with a R_1 packet challenging the initiator to solve a puzzle to verify itself with some control data including the Diffie-Hellman (DH) key arrangement parameters. Receiving R_1, the initiator replies with I_2 concatenating the solved puzzle, DH key arrangement parameter and the other requested parameters. Receiving R_2 at the initiator, both initiator and responder will establish secure associations in either direction.

The data transmission in HIP is protected with Encapsulated Security Payload (ESP) which provides a mix of security services. HIP base exchange may establish single or multiple secure associations between the communication parties according to their requirements. If the association is expired, it is revoked and new association is established. Other than that, an association is updated upon changing the IP address due to change in location. Though, mobile host dynamically changes its IP address, it may not affect in the application level since the transport associations are purely built on the HITs that are not changed throughout the lifetime of the associations. In a nutshell, the HIT and the Security Payload Index (SPI) index substitute the role of IP address in the stack except in network layer routing.

The mobile node updates the rendezvous infrastructure which holds the latest IP assignment for the mobile node. In principle, rendezvous server is similar to the home agent in Mobile IP. When the initiator wants to connect to the responder, knowing the responder's HIT initiator forwards the packet to the rendezvous server. On receiving I_1 packet, rendezvous server query the IP address of the responder and forward the packet. For instance, if both mobile nodes move at the same time, HIP readdressing packets will never reach each other since, new assignments are not known each other. Thus, mobile nodes have to trust on the rendezvous mechanism to retrieve the latest HIT-IP mapping.

However, the reachability is checked before sending bulky data since, the fast moving mobile nodes may change location very often. Ultimately, HIP can be defined as a key exchange mechanism and an end-to-end mutual authentication mechanism to be used with security protocols such as ESP IPSec [10].

III. HIP Based Femtocell Backhaul Solution

This section presents a HIP based secure backhaul solution to handle mobility and security issues in 3GPP standardized femtocells technology. With the proposed HIP based solution, the IP addresses are no longer listed as identifies. Ultimately, it denotes the point of attachment of mobile node to the core network. However, IP address still performs network layer routing while seperate name space is proposed to manage identity which does not change once it is configured.

The Home Subscriber Servers (HSS) records the authentication information and subscription data correspond to each FAP and is retrieved whenever it is requested by the Authentication, Authorization and Accounting (AAA) server. The standard defines optional hosting party authentication which is based on the credentials stored in Hosting Party Module (HPM). However, it is out of our focus in this paper. HIP inherits several advanced mobility and security features including extended multi-homing support, middlebox traversal and address translation. In the following subsections we discuss how these features can be adapted in femtocell technology to improve security and to support mobility.

A. HIP-Based Secure Femtocells

The rapid growth of mobile communication revels mobility, not only to the nodes but also to the networks of many connected nodes. We present mobility in terms of node mobility and network mobility. There are three generic approaches of handling mobility signaling. The first approach assumes mobility signaling for each mobile node is handled individually by the node itself. This involves more signaling overhead, processing and long handover reaction time when the number of mobile nodes increase.

The next approach is based on traffic tunneling where signaling traffic generated at the mobile node to the gateway is tunneled to a fixed gateway in the operator network. This approach may not use the optimal path introducing an unexpected delay due to triangular routing. Introduction of IPv6 can resolve the problem of triangular routing which is a common issue with many Mobile IP (MIP) proposals. However, the tunneling overhead in the second approach may increase the packet size which results to lower the throughput. In the third approach, the mobile node delegates rights of mobility signaling to an associated gateway which may further delegate mobility signaling rights to a Local Rendezvous Server (LRVS) located in the core network.

This proposal is a combination of above three approaches. In this approach, mobile devices and core network are assumed to be HIP aware. Moreover, specific Network Address Translation (NAT) machanism which performs SPI mapping (SPINAT- Security Parameter Index multiplexed Network Address Translation) is adapted to hide node identities behind the NAT. SPINAT uses SPI value in ESP packets to demultiplex multiple IP addresses on the same IP address [11]. In the next subsection, we discuss SPINAT in detail. Here onwards, we assume FAPs are authenticated at the initial boot-up using the base exchange defined in HIP.

The mobile node configures an IP address using whatever the available technique in place such as, manual configuration, DHCP or stateless auto-configuration. For instance, in stateless auto-configuration, the mobile node receives one or more prefixes correspond to its domain gateway or the associated FAP. The mobile node randomly selects an address out of the dedicated prefixes. Upon entering to the FAP domain, the mobile node acquires an IP address and triggers Security GateWay (SeGW) to run the base protocol. During the base exchange, the common keying materials are created and exchanged using Diffie-Hellman key exchange mechanism. Thus, the keys drawn from the keying material can be used to protect the signaling and data traffic. For this reason, nobody except the mobile node and the SeGW can decrypt the communication. The Figure 2 presents the node registration and the handover from one femtocell to another. The HIP support over this use case is further explained in the coming paragraphs.

In this case, the SeGW reads the cell information of the target femtocell and performs the access control for the non-CSG mobile nodes. For the CSG-capable mobile nodes, the access control shall be done by the core network and the result will be sent back to SeGW. If the target FAP is allowed access, the SeGW will then send the handover request to it. Since the SeGW only has the information of the connected FAPs, it is applicable only to the intra-GW femtocells. If the source and target femtocells belong to a different SeGW, the core network coordinated handover procedure should be invoked instead. By handling the handover procedure using the SeGW, the handover latency and the load of core network are reduced. However, new functionalities need to be added to the SeGW so that it is able to read and forward the handover request message.

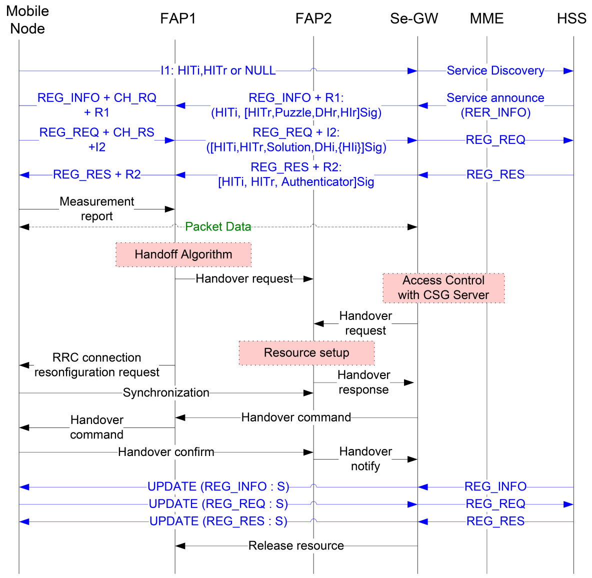

Fig. 2. HIP based call flow in femtocell communication.

By nature, HIP enables end-to-end security. Thus, nobody except the end hosts can encrypt the communication even if the communication is eavesdropped. However, an attacker can still perform replay attack on the HIP hosts. In this proposal, we suggest a challenge, request based replay mitigation procedure which is presented in the Figure 2.

The first step in Figure 2 triggers the base exchange sending an I_1 packet which includes the mobile node's HIT and the SeGW's HIT. The SeGW's IP address can be obtained from the DNS or repository service in place. If the opportunistic mode is used, the responder HIT field is kept null. The I_1 messages always pass by the FAP's associated Local Rendezvous Server (LRVS). This mechanism enables fast route updating when the mobile node moves with the correspond node. The generic DNS mechanism may not be a good solution to handle fast reroute updating in such situations.

This proposal describes, how the HIP based passive service discovery can be used in femtocell technology. The base exchange authorizes the mobile node to exchange the service related information concatenated to the base exchange. The mobile nodes do not want to actively query the services since, it is not feasible to perform FAP discovery each time the nodes move [12]. On receiving the I_1 packet, the SeGW forwards it on upstream to the HSS. The HSS maintains records such as, subscriber profile database, service permissions, and preference settings. The HSS verify the conditions, query the records of the subscriber and services supported by the connected FAP. Finally, the HSS creates a response (a service announcement packet) which includes the services supported by the operator.

The service announcement packet includes the all parameters specified in the R_1 packet. In the service announcement packet, the REG_INFO parameter is mandatory containing the services provided by the core network. In addition to that it contains R1 packet parameters which allows the gateway to continue the base exchange. Thus, the mobile node can perform the service registration directly with I_2 packet. The HIP REG_INFO parameter in service announcement certainly contains the services provided by the operator. Other than that, it contains R_1 parameters such as, SeGW's HIT, mobile node's HIT, cryptographic puzzle and SeGW's public key. The R_1 parameters in the service announcement packet is signed by the SeGW using its public key.

Upon receiving the R_1 packet, the mobile node solves the puzzle and creates an I_2 packet which includes mobile node's HIT, SeGW's HIT, puzzle solution and mobile node's public key. This message is signed by the mobile node using its public key. The REG_REQ parameter in I_2 or UPDATE packet deliver the service(s) the mobile node is eligible. If the REG_REQ parameter is in an UPDATE packet, the SeGW must not modify the content that are not listed in the parameter. On receiving I_2 packet, the SeGW response to the mobile node with a R_2 packet that includes SeGW's HIT, mobile node's HIT and few fields such as HMAC and HIP_SIGNATURE. The HSS includes an REG_RES parameter in its R_2 or UPDATE packet only if a registration has successfully completed. By now, the secure association to the core network is established and the mobile node can start the communication.

The FAP as a middle box has no mechanism to distinguish the legitimate nodes from the malicious nodes since, they are not aware of the encryption and integrity protection keys associated to the ESP secure association. Attackers can eavesdrop the base exchange and grasp the SPI values of an existing association. Thus, fake ESP packets with valid SPI values can easily traverse through the FAP. For this reason, we propose a node authentication mechanism in to the HIP base exchange to enable identity verification of the sending node.

This briefly outlines, additional security measures for HIP-aware FAPs. There is a high risk of compromising a legitimate FAP by an unauthorized external user. Thus, the FAP may need to verify the identity of the mobile node during the base exchange. FAP adds CHALLENGE_REQUEST parameter to R_1 message. Thus, the IP and HIP checksum must recompute once again. This parameter includes an opaque blob of data to the unprotected part of the R_1 packet. The opaque data field serves as nonce and puzzle seed value [13]. The content in the CHALLENGE_REQUEST is to be copied unmodified to the CHALLENGE_RESPONSE parameter of the the corresponding I_2 packet. Otherwise, FAP may deny or degrade the service to the mobile node. The same identity verification procedure can be applied with the UPDATE or NOTIFY messages as well. Apparently, the FAP can be protected from replay based attacks using this mechanism.

After the base exchange, the mobile nodes are in a state to communicate. Upon entering to a new domain, the mobile node acquires an IP address and depreciates the previous address by sending an UPDATE or NOTIFY messages. The HIP associations can be refreshed by the UPDATE procedure when it is required [14]. In the update message, the mobile node sends set of parameters to the SeGW including the LOCATOR parameter which contains the new IP address(es).

However, before updating the association, the SeGW verifies the source address sending an ECHO_REQ which requests to echo back some nonce information. The peer can communicate with unverified address only for a short period of time since, it is controlled by the credit-based authorization. The Figure 2 presents reassociation or the HIP based update procedure. During the update, there is a possibility of an attacker attempting to impersonate the mobile node or the FAP. Thus, we recommend to use the proposed challenge, request based identity verification in femtocell technology.

B. HIP-Based Secure Multi-homed Femtocells

In this section, we discuss the signaling flow of multi-homed FAPs. In other words, this is an attempt to address the network mobility scenario. For instances, in certain scenarios the mobile nodes do not move alone, but, as a part of a small network. Buses, trains, airplanes and Personal Area Networks (PANs) are few examples of network mobility scenarios. In other words, they can be assumed as mobile femtocells.

The mobile nodes change their topological location with the FAP. Entering to a new domain, the FAP renew the IP configuration. And it updates the connected peers, associated LRVS, SeGW and DNS with the UPDATE_PROXY message. Afterwards, the previous set of locators can be depreciated. However, this update can be distinguished from an end-to-end update by the special message type UPDATE_PROXY. In processing perspective, the UPDATE_PROXY exchange is handled similar to the UPDATE exchange [15]. In the Figure 3, we present the discussed network mobility scenario.

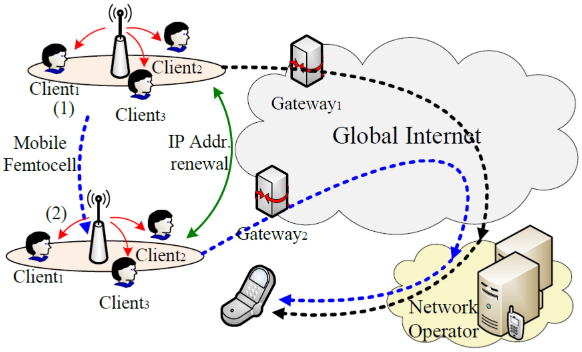

Fig. 3. Mobile femtocell scenario.

It is impractical, the mobile nodes change their IP configuration each time the FAP update the location. Thus, it is possible to use a rewriting mechanisms to rewrite prefixes in the packet headers when they pass by FAP [15]. Thus, the nodes in the mobile femtocell can be configured using link-local subnet prefixes or unique local subnetwork prefixes.

The FAP rewrites it with globally routable prefixes before the packets are forwarded to upstream.

In the nested network case, a FAP moves behind another FAP. Upon changing the attachment to the FAP, the mobile node trigger the UPDATE_PROXY exchange to inform the associated peers, domain LRVS, SeGW and the DNS. On receiving packets at the FAP, it rewrites the packet header with a globally routable address. However, this approach does not allow the FAP to signal on behalf of the mobile node. Moving into a new network, it is recommended to trigger base exchange and generate new keying materials to prevent node impersonation.

C. HIP Enabled WLAN Femtocells

Nowadays many public and private places have wireless access which is standardized and matured over many years. The dual-mode mobile handsets empowered with technology convergence guarantees service continuity over different technology regions. To simplify this scenario, we can think of a mobile user who is entering to his home WLAN. When the mobile node has cellular and WLAN coverage, the user may prefer to use the WLAN since, it is cost effective and provides good coverage in home environment.

Herein, we propose HIP to handle handover between different technologies. The mobile nodes discover FAP by the router advertisements and dynamically configures an IP address on its wireless interface. Thus, the previous address is depreciated. However, the change in IP address does not affect the transport layer associations since, they are purely built on the HITs. The mobile node uses update exchange to inform the address reconfiguration to the peer nodes, LRVS, DNS and the SeGW. Upon completing the update exchange, the SeGW rewrite the packet header with the new address. Thus, the reassociation does not affect the applications above.

In mobile femtocell scenario, the FAP and the SeGW rewrite the packet header before it is forwarded. Otherwise, the packets are decrypted by the SeGW and forwarded upstream over the core network IPSec tunnels. After moving to the home WLAN, the same keying material can be used since, it is shared only between the mobile node and SeGW. If the keying materials are expired, the mobile node has to renew the association. Thus, the same signaling flow in the Figure 2 is applicable to the handover between cellular and WLAN networks assuming the FAP2 is WiFi enabled.

D. HIP Aware Multi-homed Mobile Users

Multi-homing can configure more than a single IP address on a physical interface [16]. Thus, a mobile node with a single air interface can have multiple IP addresses configured on it. Therefore, it can simultaneously communicate over multiple interfaces. Later on, the traffic can be transferred into a stable connection. This concept can be adapted into fast-moving mobile nodes. With multi-homing, mobile nodes experience make-before-break type of handover. For this reason, the packet loss and the handover can be immensely dropped down.

Mobile node acquires an additional IP address upon entering to a new domain, which can be used to attach to the nearest base station. Now on mobile node can use the new configuration and transmit tunnel mode UDP encapsulated packets. Ultimately, this approach can reduce the fault tolerance for high speed mobile users. In other words, the fast moving mobile nodes are reluctant to often handover. The handover delay is a significant parameter in defining the service quality for fast movers. Thus, they certainly demands smooth handover and minimum handover delay. In this proposal, node multi-homing with HIP is proposed for fast moving mobile nodes to reduce the call drop, packet loss, packet reordering and duplication.

E. HIP Based Device Authentication

3GPP standards define mandatory FAP authentication based on certificate or Extensible Authentication Protocol (EAP). To establish a secure association, the identities of the FAP and the core network should be mutually authenticated. The FAP authentication algorithms are stored and executed in the Trusted Environment (TrE). If the authentication algorithm is weak, FAP can be easily compromised. Otherwise, a valid authentication key can be inserted in to a manipulated FAP. Other than that, authentication key can be cloned or compromised by a local physical intrusion. According to Release 8, the hosting party authentication to the core network is made optional. However, the nodes with valid subscription can be directly authenticated to the core network.

The base exchange itself mutually authenticates each other with the packets R_1, I_2 and R_2. The R_2 includes one or two DH keys and the host identity of the responder covered with its signature. Initiator verifies the responder with the signature and computes the session key and establishes a HIP association to encrypt the node identity. Initiator responses with DH key and its host identifier covered with its signature. Responder computes the DH session key to create an association and decrypts initiator's public authentication key. The signature can be verified with the authentication key extracted from the message. Ultimately, applying HIP on FAPs can enable end-to-end authentication and key establishment for ESP and other end-to-end security protocols.

In addition, we have proposed an identity verification approach based on challenge request, response concept. The FAP may use this procedure to ensure only the reliable parties are involved in the communication. This additional verification can protect the FAP from replay attack and node impersonation. HIP defines the authentication as the ability to determine the origin of a received message [16]. Conversely, the plane HIP authentication based on DH key exchange that uses host identifier as the public key may not stand against replay attack. Thus, additional techniques must be integrated to establish a strong authentication techniques in HIP.

F. Performance Enhancement with HIP Aware Femtocells

In this effort, we propose HIP for femtocell networks and describes how it can be utilized to address different practical scenarios. The text mostly emphasis the mobility and security issues in femtocell networks. Introducing a new global address space based on the cryptographic identities guarantees flexibility in underlay protocols. Using HIP, we simplify the complex scenarios in mobility, scalability, security and privacy in femtocell technology. The new global identifications assigned by HIP assures changes in lower hierarchy do not affect the above transport associations. Thus, the transport layer connectivity remains uninterrupted even if the IP addresses are reconfigured in the network layer.

The proposed mobility architecture for mobile FAPs can guarantee service connectivity for fast moving mobile nodes. HIP uses ESP IPSec as the transport protocol. Thus, the nodes may drop the HITs and forward the packets using the SPI value in the packet header. This can reduce the packet overhead significantly. ESP provides confidentiality and integrity by encrypting data to be protected and placing them in the data field of the IP ESP packet. Thus, the attackers those who are trying to eavesdrop the communication may confuse.

The base protocol allows the nodes to concatenate or append several parameters into the base exchange. For this reason, multiple tasks can be completed at the same time. The end-to-end authentication and identity verification over communicating parties protects the femtocell networks from different form of attacks such as replay, DoS, flooding, Man-in-the-Middle and DDoS. The HIP support for interoperability between IPv4/IPv6 and NAT traversal ensures the backward compatibility. In a nutshell, HIP simplifies several complicated problems in femtocell communication related to authentication, security, mobility, address mapping, identity verification and service registration.

IV. Evaluation

A. Plan to Prototype The System

HIPSim++ is a HIP Simulation Framework for INET/OMNeT++ developed to provide a flexible toolset for testing and validation of HIP and its extensions. Our effort is to simulate the HIP based femtocell scenario in WiFi environment. Though, OMNet++ tool does not support 3GPP elements, our objective is to measure the performance indicators. We may use WiFi environment to simulate the proposed architecture using 3GPP femtocell network parameters. Ultimately, we will measure the packet loss, throughput (amount of data received at mobile node per second) and handover latency by means of the time duration between the last packet received from previous association and the first packet received from the new association.

B. Comparison of Header Overhead and RTTs

In the existing femtocell architecture, the FAP establishes a secure IPSec tunnel between the SeGW and the FAP utilizing IKEv2. The Figure 4 presents the generic packet format in the femtocell communication and the HIP control and data packet formats. The local IP is the transport IP received from the access point, DHCP or any available mechanism after successful authentication. IPSec adds a tunnel header which is used to establish a IPSec tunnel utilizing IKEv2. The gateway inserts the remote IP address of the access point in the configuration payload during the IKEv2 exchange and establishes a secure IPSec tunnel with this address.

Data packets are transmitted encapsulating into UDP frames with destination port address set to 500 or 4500. SeGW allows the packets with source address set to FAP's local IP address. Mobile nodes need to perform authentication twice when it is attached to a new service through new FAP. The below action points summarize the typical 3GPP standardized communication flow consequently.

- FAP authentication and authorization.
- Get the Local IP of the access point.
- Query DNS to obtain the gateway address.
- IPSec tunnel establishment.
  - Initiate the establishment of IPSec secure association with IKEV2.
  - Get the Remote IP from the IKEv2 configure payload field.
  - IPSec tunnel establishment.
  - IP in IP tunnel establishment over local IP.

The below action points summarize call flow procedure of the proposed protocol architecture consequently. However, this is already explained in more detail in the previous sections.

- FAP authentication and authorization.
- Query DNS to obtain the mobile node's associated LRVS address.
- Initiate base exchange and service registration.
- IPSec tunnel establishment, service registration and identity verification.
  - Initiate the establishment of secure association by sending an I_1 packet to the peer node.
  - Exchange the common keying material and generate session key.
  - Follow-up base exchange with service registration and identity verification.
  - ESP IPSec tunnel establishment.

Considering the device authentication (FAP authentication to core network) procedure defined in the 3GPP release 8, it was found that the EAP-AKA based authentication spends minimum 4 Round Trip Times (RTTs) between the FAP and the SeGW whereas, the certificate based authentication spends minimum 2 RTTs. Conversely, our approach spends same number of RTTs as certificate based authentication. Thus, compared to EAP-AKA our approach performs much better. Figure 4 presents the control and data packet of 3GPP and HIP based femtocell solution.

The I_1 packet which initiates the base exchange essentially passes through the LRVS. But, the remaining control packets of the base exchange bypass LRVS and establish end-to-end secure associations. After adding a new ESP header field, the data packets are provided confidentiality, data origin authentication, connectionless integrity, anti replay service and limited traffic flow confidentiality. Furthermore, the mobile node does not need to authenticate again and again even if, it reconfigure the association. And the same keying material can

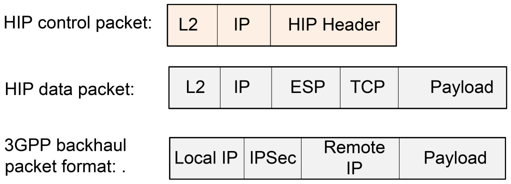

Fig. 4. Proposed control/data packet header format and the 3GPP backhaul packet format.

be used to encrypt the new association whereas, EAP-AKA, certificate-based or combined certificate-based authentication need reauthentication.

V. Conclusion

In this paper, we propose a modification to the existing protocol stack of the 3GPP femtocell architecture. We are more focused into mobility and security issues related to femtocell technology. This research work proposes several enhancements to the femtocell technology such as service registration, identity verification and node multi-homing. Moreover, we could bring down the device authentication to 2 RTTs whereas, EAP-AKA spends 4 RTTs. Our proposal substantially improves the security by means of strong authentication and identity verification. Other than that, the protocol resists to DoS and Man-in-the-Middle attack by nature. The data is encapsulated into ESP packets to guarantee confidentiality, data origin authentication, connectionless integrity, anti-replay service and limited traffic flow confidentiality. In a nutshell, integrating all features above, this proposal can provide strong security and mobility support for femtocell networks.

Acknowledgment

This research has been funded by Academy of Finland grant 128010. Special thanks are due to Prof. Andrei Gurtov and Prof. Matti Latva-aho for the support throughout.

References

[1] T. Chiba and H. Yokota, "Efficient Route Optimization Methods for Femtocell-Based All IP Networks," in *Wireless and Mobile Computing, Networking and Communications, 2009. WIMOB 2009. IEEE International Conference on*. IEEE, 2009, pp. 221–226.

[2] D. Knisely, T. Yoshizawa, and F. Favichia, "Standardization of Femtocells in 3GPP," *Communications Magazine, IEEE*, vol. 47, no. 9, pp. 68–75, 2009.

[3] V. Chandrasekhar, J. Andrews, and A. Gatherer, "Femtocell Networks: a Survey," *Communications Magazine, IEEE*, vol. 4, no. 9, pp. 59–67, 2008.

[4] 3GPP, "Security of H(e)NB," 3GPP, TR 33.820 version 8.3.0 release 8, December 2009.

[5] C. Sankaran, "Network Access Security in Next-Generation 3GPP systems: A Tutorial," *Communications Magazine, IEEE*, vol. 47, no. 2, pp. 84–91, 2009.

[6] I. Bilogrevic, M. Jadliwala, and J. Hubaux, "Security Issues in Next Generation Mobile Networks: LTE and Femtocells," in *2nd International Femtocell Workshop, Luton, UK*. Citeseer, 2010.

[7] J. Laganier and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extension," RFC 5204, April 2008, Tech. Rep.

[8] P. Nikander, A. Gurtov, and T. Henderson, "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, 2010.

[9] T. Aura, A. Nagarajan, and A. Gurtov, "Analysis of the hip base exchange protocol," in *Information Security and Privacy*. Springer, 2005, pp. 481–493.

[10] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "RFC 5201: Host Identity Protocol," *Network Working Group*, 2008.

[11] J. Melen, P. Salmela, and J. Ylitalo, "Security Parameter Index Multiplexed Network Address Translation (SPINAT)," *IETF Draft, April*, 2010.

[12] P. Jokela, J. Melen, and J. Ylitalo, "HIP Service Discovery," *Internet-Draft,work in progress, IETF*, 2006.

[13] T. Heer, M. Komu, and K. Wehrle, "End-Host Authentication for HIP Middleboxes," *draft-heer-hip-middle-auth-00. txt*.

[14] J. Laganier, T. Koponen, and L. Eggert, "Host Identity Protocol (HIP) Registration Extension," *draft-ietf-hip-registration-02 (work in progress)*, 2006.

[15] J. Melén, J. Ylitalo, and P. Salmela, "Host Identity Protocol based Mobile Router (HIPMR)," *IETF Draft, May*, 2009.

[16] A. Gurtov, "Host Identity Protocol (HIP): Towards the Secure Mobile Internet," *Wiley Publishing*, p. 332, 2008.