Lightweight Host and User Authentication Protocol for All-IP Telecom Networks

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

Zoltán Faigl
Mobile Innovation Centre
Bertalan L. u. 2., Z. 301, H-1111 Budapest, Hungary
zfaigl@mik.bme.hu

***Abstract*—Future wireless networks are moving fast towards all-IP network architectures and mobile operators are expanding their services outside traditional cellular networks becoming multi-access operators. This lays stringent requirements on access security, where implementing consistent security policies over disparate radio accesses becomes a challenge. In this paper, we introduce a novel host and user authentication protocol based on a lightweight Host Identity Diet Exchange Protocol that extends the existing 3GPP user authentication architecture and reuses the standard Authentication and Key Agreement scheme. Furthermore, quantitative evaluation of an implementation and real deployment of our proposal along with an extensive analysis of security features is presented. Our measurements and analysis show that the proposal is a feasible lightweight authentication mechanism for mobile network use and it improves the security features of the original Diet Exchange.**

***Index Terms*—Authentication and Key Agreement, Host Identity Protocol, mobile networks, security, user authentication**

I. Introduction

Telecommunication technology is in the advent of mobile broadband and the convergence of Internet and mobile services. This evolution is made possible by the underlying shift from circuit-switched to packet-switched all Internet Protocol (all-IP) network architecture. The all-IP paradigm enables users to enjoy new high-bandwidth services through their mobile devices – anytime and anywhere. The true Mobile Internet is now possible due to the advances in the processing capacity of mobile devices and Radio Access Network (RAN) technology that is able to provide radio interfaces with increased data rates.

So as to provide users with ubiquitous anytime-anywhere connections to mobile services, the providers can be expected to utilize several RANs such as WiFi, E-UTRAN, and WiMAX simultaneously in their mobile network deployments. From the standpoint of mobile network security, this heterogeneity of radio access technologies poses a difficult challenge, as the future mobile networks need to define a consistent security policy identifying objects and trust relationships in access authentication and authorization, as well as security risks and protective measures. Due to RAN technologies having different security considerations and specifying security definitions in separate standards, it is a difficult task to define such a policy, let alone to design consistent security architecture [1].

It is evident that the future mobile networks with heterogeneous RAN accesses require homogenization in regards to security. An approach to tackle the above mentioned problems is to implement the security mechanisms independently from access technology by using a set of overlaid technologies. This approach pushes the security logic to the higher network layers from the link layer (L2). As a consequence, security mechanisms would be implemented by software as part of device's kernel or as separate applications. This approach would allow designing a consistent security policy despite the underlying RAN technologies. Naturally, it implies using the IP protocol as the integrating technology to carry all security signaling over with.

In this paper, we introduce a lightweight Host Identity Protocol (HIP)-based host and user authentication protocol for mobile network use over IP on disparate RAN technologies. Our proposal extends the ongoing 3rd Generation Partnership Project (3GPP) work on access authentication architecture reusing the specified components for compatibility reasons. We present the details of our authentication solution and its real-life deployment in the panOULU network [2], a free municipal WLAN covering the city of Oulu, Finland. The paper also provides an analysis of security features and preliminary quantitative evaluation of our proposal.

The remainder of this paper is organized as follows. In Section II, we provide background information and related work on host and user authentication in a mobile network setting. Section III in turn introduces our proposed mechanism in detail, describes our deployment scenario, and provides qualitative security analysis. The evaluation results are given and discussed in Section IV. Finally, Section V concludes the paper with discussion and directions for future work.

II. Background and Related Work

3GPP has specified the use of Authentication and Key Agreement (AKA) as the common authentication scheme. It allows unified user authentication with the same USIM card-based credentials regardless of the RAN technology. To carry out the AKA process between the User Equipment (UE) and the mobile network two schemes exist: Extensible Authentication Protocol AKA (EAP-AKA') [3] and Evolved Packet System AKA (EPS-AKA). The first scheme is used with non-3GPP accesses such as WiFi and relies on an infrastructure of Authentication, Authorization, and Accounting (AAA) servers,

978-1-4673-1239-4/12/$31.00

while the latter is used with the E-UTRAN access. Unfortunately, the first protocol suffers from various vulnerabilities such as disclosure of the user identity, bandwidth consumption, and vulnerability to Man-in-the-Middle (MitM) attacks [4].

Host Identity Protocol (HIP) [5] is an emerging protocol for host authentication and mobility. It is a signaling protocol to establish security context and to notify of IP address changes between two end-hosts. A complete HIP-based authentication infrastructure for managed networks requires additional components such as Rendezvous servers, Domain Name Servers (DNS), and AAA backends or a Certificate Authority (CA).

An interesting work on utilizing HIP in mobile operator deployments is described in [6]. The authors present their implementation of a HIP-based network attachment protocol and bootstrapping solution over WiFi access. The work incorporates use of a Radius-based AAA backend server as part of HIP Base Exchange (HIP-BEX) for user and access authentication. It is stated that the authentication at the AAA backend is based on the user identifier and required credentials, but no details as to how the credentials are used in the AAA side nor how they are provisioned to the connecting user are elaborated. Furthermore, the work does not address user privacy issues.

Kuptsov et al. have developed distributed authentication architecture for managed Wireless LANs using HIP between UE and a HIP-aware WiFi access points [7]. As a downside, the proposed access control list solution would require drastic changes if deployed in an operator's network due to introduction of new network elements and signaling schemes between base stations and a centralized policy server.

Studies [8] and [9] examine the utilization of HIP in the Internet Multimedia Service (IMS) access authorization and establishment of a secure data channel between mobile client and mobile network. The proposed solution takes advantage of hash functions to bind user identity (i.e. SIP URI) and host identity together to provide non-repudiation support for IMS services. The research provides only theoretical analysis of the feasibility of the proposal.

As discussed in [10], the standard HIP-BEX is too heavy operation for resource constraint devices such as mobile devices and base stations that do not have sufficient CPU power nor memory available. To address constrained devices better, use of elliptic curve cryptography has been proposed to be used with HIP [11]. In fact, HIP Research Group under the IRTF body has already outlined a lightweight version of HIP-BEX called HIP Diet Exchange (HIP-DEX) [12], a variation of HIP using as few cryptographic primitives as possible.

It has already been verified that HIP-DEX indeed is more suitable for resource constrained devices for its lightweight cryptographic properties. In [13] and [14], HIP-DEX is deemed as more suitable for constrained environments such as medical sensor networks where HIP-DEX is deployed in lightweight sensor gateways. A certificate-based method with issuance of short lived membership certificates is proposed for authenticating hosts and users.

An approach described in [15] proposes a lightweight authentication method for HIP by checking the binding between L2 identities and host identities. However, it only covers the trusted non-3GPP access scenario.

Unfortunately, the existing literature discussed above does not yet discuss suitable (user and host) authentication mechanism for operator environments that would be lightweight enough to address resource constrained mobile terminals and handle user authentication in a standard way.

III. Authentication in Mobile Networks

A. Authentication Architecture

Our proposal extends the already existing 3GPP architecture by utilizing HIP-DEX in a novel way that reuses the core components of operator's network, namely the Home Subscriber Service (HSS) backend for EPS-AKA authentication. The architecture removes some of the core network elements involved previously in authentication processes specified by 3GPP, and introduces new and moves old functionality to existing elements. Figure 1 illustrates our architecture proposal.

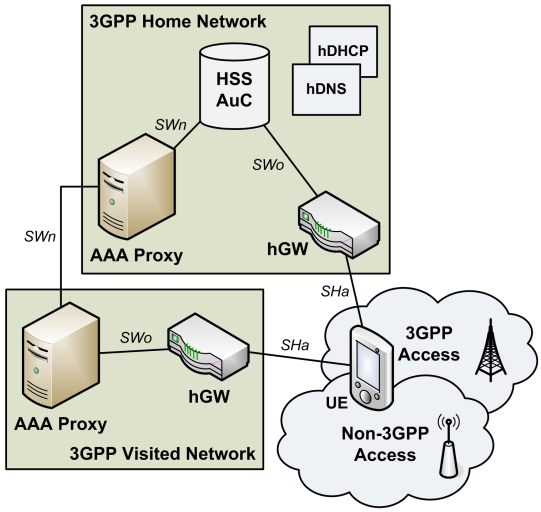

Fig. 1. Authentication architecture proposal.

In our architecture, the serving gateway element at the border of the core network is referred to as hGW. This network element implements a HIP-DEX and Diameter-based application to perform 3GPP-based access authentication between a UE and the mobile network.

While in many operator settings the network access authentication builds on an EAP authentication method - most commonly on the EAP-AKA method - our proposed authentication architecture abandons the EAP protocol altogether and introduces a native support for AKA in HIP-DEX. This allows common USIM-based authentication to take place over any IP-based access on L3. Consequently, the 3GPP AAA server is removed from the architecture as translator for EAP frames is no longer needed. The authenticator role previously served by a AAA server is moved to the serving gateway hGW at the border of the core network.

Our proposal specifies an SWo interface between hGW and HSS. This is identical to the two already defined interfaces

SWx and S6a in the 3GPP Specification Release 11 [16]. These interfaces allow hGW to download Authentication Vectors (AVs) from the HSS server at time of access authentication in order to perform the AKA scheme.

The 3GPP specifications define the use of 3GPP AAA proxy servers for roaming scenarios when the UE resides in a visited network. Our architecture also defines an infrastructure of Diameter-based AAA proxies with interface SWn. The main purpose of the SWn interface is to convey Diameter signaling between home and visited networks in connection with the SWo interface. SWn utilizes the same Diameter applications and extensions as SWo (i.e. SWx and S6a) and thus does not specify a new Diameter application.

B. Authentication Process

In our system, HIP-DEX is used as authenticating protocol between UE and hGW. As specified by HIP-DEX, UE is represented by host identity. The user of the UE, in turn, is represented by International Mobile Subscriber Identity (IMSI) allocated to the subscriber and stored on her USIM card by the operator. While host identity is a self-certifying identity due to its cryptographic properties, IMSI - being only a 15-digit ASCII string - has to be separately verified by proofing access to a secret key shared between the operator and the user. In our system, AKA scheme embedded in HIP-DEX is used to achieve this. This means that our proposed authentication scheme actually performs two authentications in one message exchange: (1) authentication of the user by using the standard AKA mechanism, and (2) authentication of the UE.

The authentication process consists of one HIP-DEX with two extra HIP messages transmitted between the communicating hosts. The main difference with the basic HIP-DEX is that session secrets are not exchanged at all in the 3rd and 4th packets. This is because the AKA mechanism will ultimately produce the session key material for the hosts. The full process of our proposed authentication solution, dubbed as HIP-AKA exchange, is illustrated in Figure 2.

HIP-AKA begins with the UE initiating an I1 packet towards the hGW. The IP address and Host Identity Tag (HIT) of the hGW are assumed to be dynamically learned from the bootstrapping information received during the attachment to the access network through, e.g. a query to a HIP-capable DHCP server. Alternatively, the I1 packet can be sent as an opportunistic broadcast packet without knowing the hGW's HIT or IP address in advance as proposed in [6]. Upon receipt of the I1 packet, the hGW selects a suitable precomputed R1 packet and attaches it with a random nonce I for a puzzle challenge.

Upon receiving the R1 packet, the UE solves the puzzle and adds corresponding solution J to an I2 packet along with the subscriber identity. The identity is represented by a Network Access Identifier (NAI), an ASCII string of form (IMSI)@realm, where the realm part is the name of the serving network the UE has received locally during the bootstrapping process in the access network or statically set in the device. If the UE is configured to use the realm part, it checks that

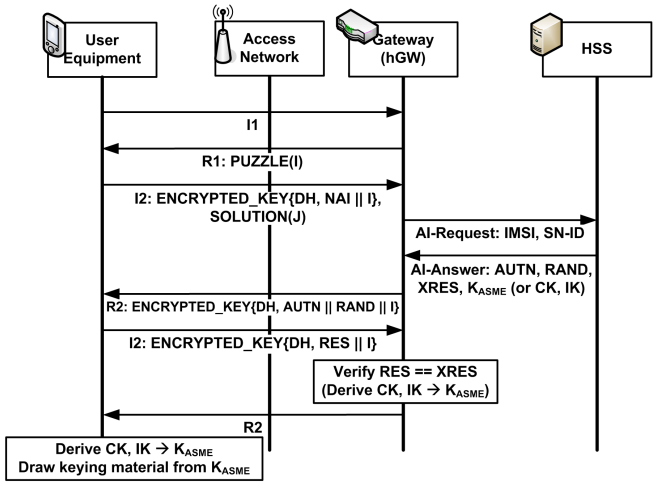

Fig. 2. Message sequence of HIP-AKA protocol.

the realm part received from the hGW is as expected. Because IMSI should not be revealed to third parties, the subscriber's identity is carried encrypted inside the ENCRYPTED_KEY parameter instead of the HOST_ID parameter.

During the HIP-AKA authentication process, hGW communicates directly with an HSS server located in the user's home network. When the hGW receives correct puzzle solution and an IMSI string from the UE in I2 packet, it verifies that the received IMSI (and possible realm part in NAI) is correct and requests AV for the user from the HSS. The communication towards HSS is performed by using a standard Diameter protocol as specified by 3GPP [16]. This message is called Authentication-Info-Request (AI-Request) and it contains the IMSI of the user and Serving Network ID (SN-ID). The HSS constructs the AV including keys and returns them in an Authentication-Info-Answer (AI-Answer) message. The hGW then forwards the RAND and AUTN parameters to the UE inside R2 packet.

Next the UE calculates its own version of the AUTN parameter and compares it with the one received from the hGW. If they are consistent, the UE has successfully authenticated the network and can proceed with the HIP-AKA. The UE generates a response RES using the key K and RAND, and transmits it encrypted to the hGW inside a second I2 packet. Upon receipt of the second I2, the hGW verifies the response by comparing it to the XRES parameter from the HSS. If they match, hGW has authenticated the user and it finalizes the authentication process with a second R2 packet to the UE.

From this point on both UE and hGW are able to generate common session keying material for ciphering and integrity protection as described in [12]. Instead of the secret-x and secret-y keys, $K_{ASME}$is used in the key derivation. Description of the derivation of K_{ASME} itself can be found in [17].

C. Implementation and Experimental Deployment

To determine the feasibility of our proposed authentication scheme, we conducted a case study, where the HIP-AKA protocol was deployed in the IEEE 802.11g-based panOULU WLAN. The panOULU network represented an untrusted

non-3GPP access network without authentication or any L2 security mechanisms (i.e. WEP/WAP). The network topology used in our experiment is illustrated in Figure 3.

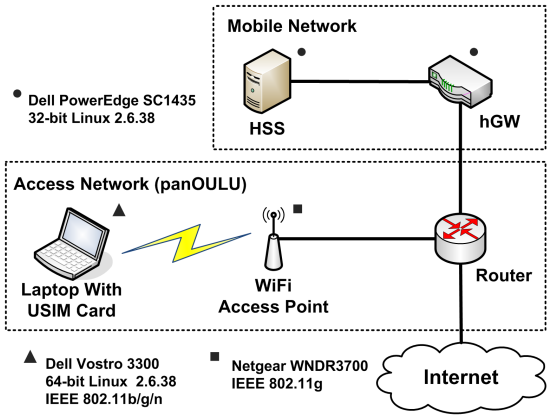

Fig. 3. Network topology for authentication protocol deployment.

The hGW in Figure 3 runs a daemon application responsible for listening and accepting incoming connections from UEs wishing to connect to the mobile network, and performing HIP-AKA as described above. The daemon is written in C++ for the UNIX-based operating systems and takes advantage of the OpenSSL library version 1.0.0d. The same daemon is run in the UE as well but acts in the initiator role and accesses the USIM card during the HIP-AKA exchange.

HSS in turn, runs an emulator server application by Nokia Siemens Networks emulating the HSS functionality and the S6a interface. The application is responsible for accepting connections from the hGW over a Diameter-based interface [16] over the SCTP protocol and generating AVs on request.

D. Identification of Security Attacks

Extending HIP-DEX with the EPS-AKA authentication method has influence on the peer authentication properties of the protocol. Originally HIP-DEX has an extension for password-based user authentication. Using a password the initiator encrypts a challenge obtained from R1, wraps it in an encrypted data block using the static Diffie-Hellman (DH) key, and conveys it to the responder in I2 [12]. AKA replaces password-based authentication option of HIP-DEX. While EPS-AKA mutual authentication method is a strong authentication protocol supporting large-scale deployment in mobile operator environments, one-way password-based authentication has well known limitations with security and scalability. AKA based key derivation also changes the resistance of the protocol against fabrication attacks.

Table I compares the security properties of HIP-AKA with HIP-DEX and HIP-BEX that are further discussed in this section. Mutual authentication of HIP host identities is supported by all schemes. As discussed before, HIP-AKA provides strong user and network authentication as well due to the tunneled AKA protocol. HIP-BEX with certificates (BEX-CERT) [18] can provide the same level of security. Both schemes certify the real user and network identity. User identity, i.e., the IMSI, is transferred in an encrypted block, hence it is not disclosed to other parties. Certificates in BEX-CERT are transferred in clear-text so user identities are disclosed in that case. Host identity protection is supported only by BEX using the BLIND extension [19]. In HIP-DEX and HIP-AKA host identities are transferred in clear-text.

HIT spoofing, Sybil attacks, MitM and network-level wormhole attacks are detected due to strong peer authentication bound to key material in HIP-BEX and AKA. A HIT whitelist based access control was proposed in [13] to strengthen HIP-DEX against Sybil attacks. Due to the lack of identity certification HIP-DEX does not protect against MitM attacks. Password-based authentication protects only the responder against MitM attacks as stated in [13]. Moreover, the key material is not bound to the authentication.

DoS resistance of responder is supported in all schemes by the puzzle-challenge mechanism. This mechanism has, however, practical limitations because the attacker might use high-end devices to solve the puzzle [13]. Blacklisting DoS attackers, whitelisting new legitimate nodes, or cookie-based access authorization could in addition be used to strengthen resistance to DoS attacks.

Resistance against replay attack has been stated strong for HIP-BEX and HIP-DEX [21], [13], however, we have discovered a replay attack against HIP-DEX. Originally, the responder must convey a unique puzzle (I) and may include an R1_COUNTER value in R1. These values are sent back by the initiator in I2 as proof of freshness of I2, i.e., protect the responder against replay attacks. In HIP-BEX, provided that the DH key is always fresh, message authentication codes protect both peers from replay attack. HIP-DEX, however, is vulnerable to the replay of legitimate R1 and R2 messages due to static DH keys and because the initiator does not contribute to the freshness of the integrity keys. That leads to successful HIP host association and IPsec SA pair establishment on the initiator's side by the fake responder. Albeit confidentiality of initiator's communication is not compromised because the key material is not obtained by the attacker, the communication of legitimate initiator can be disrupted. As a countermeasure the initiator should include a nonce with small collision probability in I2. This nonce should be used in key generation process so the MAC value in R2 provides proof of freshness to the initiator.

Perfect forward secrecy is only supported in HIP-BEX due to the ephemeral DH key exchange. In HIP-DEX and HIP-AKA, if long-term secret, such as the private key or the static DH secret established with a given peer, is compromised, previously captured confidential information can be revealed by the attacker.

Non-repudiation of HIP signaling has built-in support in HIP-BEX due to the digital signatures, enabling third parties to authenticate the origin of the messages. The complete support of non-repudiation requires secure logging of HIP packets, verifiable anytime by third parties, as well. Hash-chaining techniques [20], [8] have been proposed to extend non-repudiation and strong authorization to IPsec transport.

TABLE I
SECURITY PROPERTIES.

	HIP-BEX	HIP-DEX	HIP-AKA
Mutual authentication	Strong with certificates [18]	Mid	Strong
User identity protection	Yes with BLIND* [19]	No	Yes
Host identity protection	Yes with BLIND*	No	No
HIT Spoofing/Sybil attack resistance [13]	Strong	Weak	Strong
MitM/network-level wormhole resistance [13]	Strong	Weak	Strong
DoS resistance of responder [13]	Mid	Mid	Mid
Replay attack resistance	Strong	Weak† (only the responder)	Weak† (only the responder)
Perfect Forward Secrecy [12]	Yes	No	No
Non-repudiation support	Strong with [20]	No	No
Signaling protection	Strong	Strong	Strong
Data protection	Strong	Strong	Strong

† For strong protection, responder should prove during the exchange the possession of a fresh nonce conveyed by the initiator.
* Normally HIP-BEX conveys as plaintext HOST_IDs or certificates, revealing user information.

All schemes provide strong signaling protection due to the usage of strong block ciphers, MAC generation methods and digital signature algorithm in case of BEX. All schemes assure that at the end of HIP exchange only the claimed host identities know the good key material for HIP and IPsec protection. Data protection is strong in all alternatives, IPsec ESP provides confidentiality, data origin authentication, connectionless integrity, and anti-replay service.

IV. EXPERIMENTAL EVALUATION

The experimental evaluation of our authentication scheme in the panOULU network concentrated on measuring service times in and memory consumption during the authentication process depicted in Figure 2. The purpose of our measurements was to contrast our proposed authentication mechanism with the standard HIP-DEX and determine its performance overhead in terms of required service times, network traffic overhead, and memory consumption. The used equipment and network topology is described in detail in Section III-C.

A. Division of Service Times

The configuration for our service time measurements is illustrated in Figure 3. The testbed consisted of two separate sub-networks, where the average ping time between the UE and the hGW was around 7 milliseconds and the average ping time between the hGW and HSS was 3 milliseconds. We traced and logged 200 HIP-DEX and HIP-AKA authentication rounds in different hours of day around the campus area of the University of Oulu connecting through several different panOULU access points. The delays were measured by using separate delay logging C++ code compiled into the HIP-DEX and HIP-AKA implementations. The measured service times with detailed descriptions are listed in Table II.

Figure 4 and Table III show our measurement results. From the charts it can be clearly seen that the total service time of one authentication round for initiator is 14.4 and 277.6 milliseconds for HIP-DEX and HIP-AKA, respectively. This means that there is little more than 19 times higher service time overhead involved with HIP-AKA compared with HIP-DEX. This huge difference is due to the AKA process run in the USIM module which takes 157 milliseconds on the average. Other notable service time overhead comes from the retrieval of AVs from the HSS server on the hGW side. In fact, network transmission delay constitutes a great deal of the overall service time overhead (in both UE and hGW) compared to the processing delays in the hosts.

TABLE II
DESCRIPTIONS OF MEASURED SERVICE TIMES.

UE Side

Time	Description
UE_{t1}	RTT between initiating I1 packet and receiving R1 packet
UE_{t2}	Solves puzzle, executes elliptic curve Diffie-Hellman key exchange, derives keying material, and creates I2 packet; HIP-AKA includes encrypted IMSI to the I2 packet
UE_{t3}	RTT between initiating I2 packet and receiving R2 packet
UE_{t4}	Verifies MAC of the received R2 packet; HIP-DEX refreshes keying material with new negotiated shared secret; HIP-AKA runs AKA in USIM module (with received AUTN and RAND parameters) and creates I2 with RES
UE_{t5}	RTT between initiating second I2 packet and receiving second R2 packet
UE_{t6}	Verifies MAC of received second R2 packet, and calculates K_{ASME} and generates keying material from it

GW Side

Time	Description
GW_{t1}	Selects pre-created R1 packet with pre-created puzzle
GW_{t2}	RTT between initiating R1 packet and receiving I2 packet
GW_{t3}	Checks solution, performs elliptic curve Diffie-Hellman key exchange, derives keying material, and verifies MAC; HIP-DEX creates I2 packet; HIP-AKA decrypts IMSI and creates Diameter message towards HSS for AVs
GW_{t4}	RTT between initiating AV query and receiving a new AV from HSS
GW_{t5}	Stores received authentication vector from HSS and creates R2 packet with encrypted AUTN and RAND
GW_{t6}	RTT between initiating R2 packet and receiving second I2 packet
GW_{t7}	Verifies MAC and compares received RES in second I2 with XRES; if match, creates second R2 and draws new keying material from K_{ASME}

B. Network Traffic Overhead

We also measured the induced network traffic overhead between the UE and the hGW in both HIP-DEX and HIP-AKA cases using the Wireshark network analyzer tool. The comparison of network traffic overhead is shown in Table IV. Figures include the size of the IPv4 header (20 bytes).

From Table IV we can notice that our HIP-AKA scheme induces around 53 % (328 bytes) more network traffic compared

TABLE III
AVERAGE SERVICE TIMES IN MILLISECONDS.

HIP-DEX

Time	UE_{t1}	UE_{t2}	UE_{t3}	UE_{t4}	UE_{t5}	UE_{t6}	GW_{t1}	GW_{t2}	GW_{t3}	GW_{t4}	GW_{t5}	GW_{t6}	GW_{t7}	UE_{tot}	GW_{tot}
Average	6.2	2.0	6.2	0.0	-	-	0.0	6.9	1.0	-	-	-	-	14.4	7.9
Std.dev.	8.7	1.2	5.5	0.0	-	-	0.0	4.6	0.2	-	-	-	-	10.7	4.6

HIP-AKA

Time	UE_{t1}	UE_{t2}	UE_{t3}	UE_{t4}	UE_{t5}	UE_{t6}	GW_{t1}	GW_{t2}	GW_{t3}	GW_{t4}	GW_{t5}	GW_{t6}	GW_{t7}	UE_{tot}	GW_{tot}
Average	5.7	2.1	85.3	157.8	26.7	0.0	0.0	7.1	1.0	36.3	0.0	20.8	0.0	277.6	252.3
Std.dev.	9.2	1.2	31.8	0.7	27.8	0.0	0.0	5.7	0.1	13.8	0.0	25.4	0.0	57.4	30.3

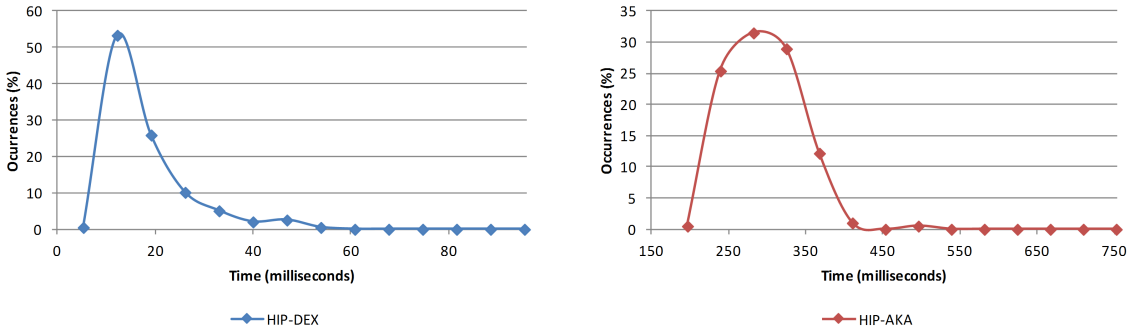

Fig. 4. Probability density function of total service time for UE (initiator).

to the standard HIP-DEX protocol. This is due to the additional exchange of I2 and R2 packets between the hosts. Although not shown in the table, we also measured the network traffic overhead due to an exchange of Diameter messages between the hGW and the HSS server. This was measured to be 612 bytes in total including also the IPv4 and SCTP headers.

TABLE IV
TRANSFERRED BYTES PER HIP PACKET.

	HIP-DEX	HIP-AKA
I1	68	68
R1	172	172
I2	236	236, 220
R2	132	148, 92
Total	608	936

C. Memory Consumption

We measured the amount of heap memory allocated by the HIP-DEX and HIP-AKA implementations on the UE and hGW side in one authentication round. Massif, a heap profiler included in the Valgrind debugging and profiling suite, was used to measure the allocated memory. As embedded and other low-memory footprint applications are generally required to be easy on the amount of memory they use, allocated heap memory was considered as a good performance metric. Allocated heap memory as a function of the number of bytes allocated/deallocated on the heap and stack for responder and initiator can be seen in Figure 5.

The left chart in Figure 5 depicting memory consumption on UE shows that there is no notable difference in memory consumption between HIP-DEX and HIP-AKA. Both curves demonstrate somewhat the same behavior during the authentication round, although the curve of HIP-AKA seems to use slightly more memory than HIP-DEX. This is due to memory allocated for the AKA process run on the USIM. The difference of HIP-DEX and HIP-AKA peaks is only 4.5 % (peak values being 17.7 and 18.7 kilobytes).

For responder the right chart of Figure 5 shows increased memory consumption with HIP-AKA which is due to the Diameter server functionality the HIP-AKA contains. Upon start-up the hGW also performs a capability exchange with the HSS, which shows as increased memory consumption in the figure before authentication takes place. The difference of HIP-DEX and HIP-AKA peaks is 24.4 % (peak values being 17.9 and 22.3 kilobytes).

V. DISCUSSION AND FUTURE WORK

From our experimental evaluation we can conclude that our proposed HIP-AKA authentication scheme is feasible to perform fast initial authentication in mobile networks. However, due to high service time overhead with the AKA process and authentication vector retrieval our protocol requires modifications should it be used in environments where re-authentications take place constantly. To improve the protocol for such environments, GW could fetch several AVs at once or/and UE could be granted with an authenticating ticket or certificate so that time consuming AKA would be run only upon the first attachment. This kind of optimization for re-authentication could improve the performance of subsequent HIP-AKA runs and decrease the signaling overhead.

Memory consumption-wise the HIP-AKA protocol does not induce notable increase on the UE side. On the gateway side, hardware with more memory is required because in addition to the HIP-DEX implementation, the gateway needs to act also as a Diameter application interfacing the backend HSS.

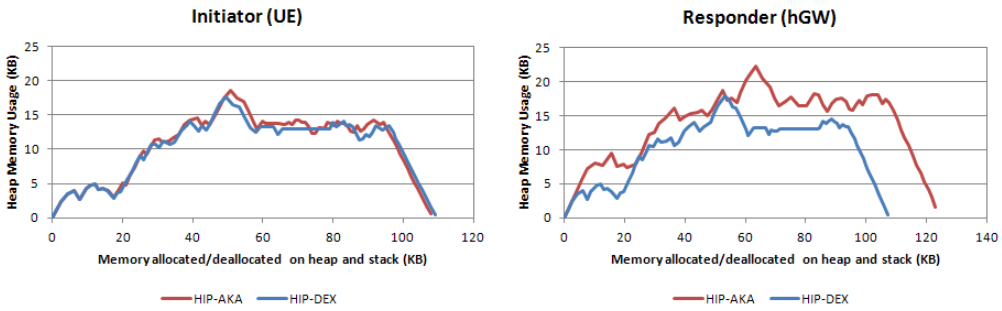

Fig. 5. Heap memory consumption on UE (initiator) and hGW (responder) side.

Security evaluation has shown that HIP-AKA improves the security of HIP-DEX against MitM, HIT spoofing, and Sybil attacks due to the AKA authentication. It, however, inherits the rest of the security features from HIP-DEX, i.e., it does not support perfect forward secrecy, non-repudiation or host identity protection. Hence its security is weaker than that of HIP-BEX.

A special replay attack against the initiator that is valid for the current HIP-DEX draft [12] was also discovered. It is proposed that the initiator must convey a nonce in I2 to the responder and this nonce should be used in the key generation process providing fresh HIP integrity keys. This vulnerability has been introduced to HIP-DEX due to the change of ephemeral DH to static DH. We suggest considering this issue when including static DH exchange to HIP-BEX in the future.

As future work, we will study implementing an optimized re-authentication mechanism to the HIP-AKA scheme. Furthermore, because host privacy remains as a concern in our proposal, we will incorporate a host privacy protection mechanism as part of our implementation. We also plan to make more extensive measurements and comparison between the current 3GPP authentication mechanisms over (E)-UTRAN and WiFi accesses. Other research directions include deploying HIP-AKA closer to the user in WiFi access points and using the scheme to carry bootstrapping information as well.

ACKNOWLEDGEMENT

This work has been carried out in the framework of CELTIC project CP7-011 MEVICO. The authors would like to acknowledge the contributions of their colleagues, although the views expressed are those of the authors and do not necessarily represent the project. This information reflects the consortium's view, but the consortium is not liable for any use that may be made of any of the information contained therein. Special acknowledgement goes to Nokia Siemens Networks for providing us with their LTE emulator software. The second author's work has been supported by the MEVICO.HU project of the Hungarian National Development Agency (EUREKA Hu 08-1-2009-0043).

REFERENCES

[1] A. Hecker, "On Logical System Access Control and the Associated User and Network Management in Future Heterogeneous 4G Wireless Systems," Ph.D. dissertation, l'Ecole Nationale Supérieure des Télécommunications, Paris, France, Feb. 2005.

[2] (2011) The panOULU open wireless internet access. [Online]. Available: http://www.panoulu.net/

[3] J. Arkko, V. Lehtovirta, and P. Eronen, "Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA')," IETF RFC 5448, May 2009, Tech. Rep.

[4] H. Mun, K. Han, and K. Kim, "3G-WLAN interworking: security analysis and new authentication and key agreement based on EAP-AKA," in *"Proc. of WTS'09*, Prague, Czech Republic, Jul. 2009, pp. 309–316.

[5] P. Nikander, A. Gurtov, and T. Henderson, "Host Identity Protocol (HIP): Connectivity, Mobility, Multi-Homing, Security, and Privacy over IPv4 and IPv6 Networks," *IEEE Communications Surveys & Tutorials*, vol. 12, no. 2, pp. 186–204, 2010.

[6] J. Korhonen, A. Mäkelä, and T. Rinta-aho, "HIP based network access protocol in operator network deployments," in *Proc. of M2NM'07*, Sydney, Australia, Oct. 2007.

[7] D. Kuptsov, A. Khurri, and A. Gurtov, "Distributed authentication architecture in Wireless LANs," in *Proc. of WoWMoM'09*, Kos, Greece, Jun. 2009.

[8] S. Heikkinen, "Establishing a Secure Peer Identity Association Using IMS Architecture," in *Proc. of ICIMP'08*, Bucharest, Romania, Jul. 2008.

[9] ——, "Security and Accounting Enhancements for Roaming in IMS," in *Proc. of WWIC'08, Lecture Notes in Computer Science 5031*, Tampere, Finland, May 2008, pp. 127–138.

[10] A. Khurri, E. Vorobyeva, and A. Gurtov, "Performance of host identity protocol on lightweight hardware," in *Proc. of MobiArch'07*, Kyoto, Japan, Aug. 2007, pp. 1–8.

[11] O. Ponomarev, A. Khurri, and A. Gurtov, "Elliptic Curve Cryptography (ECC) for Host Identity Protocol (HIP)," in *Proc. of ICN'10*, Menuires, French Alps, Apr. 2010, pp. 215–219.

[12] R. Moskowitz, "HIP Diet EXchange (DEX)," draft-moskowitz-hip-rg-dex-05 (Work-in-Progress), March 2011, Tech. Rep.

[13] P. Nie, J. Vähä-Herttua, T. Aura, and A. Gurtov, "Performance analysis of HIP diet exchange for WSN security establishment," in *Proc. of Q2SWinet'11*, October 2011, pp. 51–56.

[14] D. Kuptsov, B. Nechaev, and A. Gurtov, "Securing Medical Sensor Network with HIP," in *Proc. of MobiHealth'11*, Kos, Greece, Oct. 2011.

[15] L. Bokor, Z. Faigl, and S. Imre, "A delegation-based HIP signaling scheme for the Ultra Flat Architecture," in *Proc. of IWSCN'10*, Karlstad , Sweden, May 2010, pp. 1–8.

[16] Third generation partnership project (3GPP), "Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol (release 11)," 3GPP, TR 29.272 version 11.0.0, Tech. Rep., September 2011.

[17] ——, "3G System Architecture Evolution (SAE): Security architecture (Release 11)," 3GPP, TR 33.401 version 11.1.0, Tech. Rep., September 2011.

[18] T. Heer and S. Varjonen, "Host Identity Protocol Certificates," IETF RFC 6253, May 2011, Tech. Rep.

[19] D. Zhang and M. Komu, "An Extension of HIP Base Exchange to Support Identity Privacy," IETF Draft, draft-zhang-hip-privacy-protection-03, Tech. Rep., July 2011.

[20] S. Heikkinen, "Non-repudiable service usage with host identities," in *Proc. of ICIMP'07*, july 2007.

[21] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol," IETF RFC 5201, April 2008, Tech. Rep.