HIP Based Network Access Protocol in Operator Network Deployments

Jouni Korhonen
and Antti Mäkelä
TeliaSonera
Finland
Email: {firstname.lastname}@teliasonera.com

Teemu Rinta-aho
NomadicLab
Ericsson Research
Finland
Email: teemu.rinta-aho@ericsson.com

***Abstract*—Wireless mobile operators are expanding their IP networking services outside cellular networks and are increasingly becoming multi-access operators. Increased security requirements, dynamically bootstrapping various IP services and the need for seamless handovers for realtime IP services have become an important problem area to solve in a feasible way. Recent developments on IEEE 802 wireless technologies have addressed most security and management concerns of mobile operators. However, this has been done at a cost of more complex base stations and link layers, and increased control plane signaling between networking nodes. Typically the design is based on the traditional layered networking model, which has caused each networking layer to perform overlapping authentication, authorization and configuration procedures on their own. Clearly, this is inefficient. In this paper we propose a Host Identity Protocol based Network Attachment Protocol, which moves all security features to IP layer, supports bootstrapping of IP configuration as part of the access authentication and supports creation of security associations for authenticating to third party services. Furthermore, the proposed solution has an access technology independent centralized deployment model with minimal requirements on the access network and thus allows deployment of simple lightweight base station. We describe a prototype implementation of the proposed solution using IEEE 802.11 WLAN as the wireless technology. We also show the initial results of our implementation and its performance characteristics.**

I. Introduction

Recent development in numerous wireless networking technologies and multi-radio terminal device capabilities have given operators new alternatives in designing their networks. Traditional cellular mobile operators are also seeking for alternative and cost effective ways to expand their networking coverage and provide IP networking services outside cellular networks. However, security requirements, dynamically bootstrapping various IP services in heterogeneous environments and the need for seamless handovers for realtime IP services have become a pressing problem area to solve in a feasible way. Furthermore, in heterogeneous networks the target network discovery and selection problem [1] rapidly becomes an issue, which also needs to be addressed before the secure seamless mobility requirements can be met.

Larger networking architectures get upgraded incrementally, which means that the legacy and the new functionality need to coexists for a considerable amount of time. This effectively prohibits radical advances in the architecture and protocol design. Networking protocols have traditionally a layered design where each layer is functionally independent. The demand for security in wireless communication and the current layered design has created a situation where, in the worst case, each networking layer executes similar authentication, authorization and configuration steps independently of each other [2] [3]. This is clearly inefficient, especially in managed operator networking environment where all separate authentications, and authorizations tend to end up in the same Authentication, Authorization and Accounting (AAA) backend. Furthermore, each layer typically needs to bootstrap and configure their connectivity services. The same applies to application level services if they also require authentication and authorization each time a new service session gets established. All this combined with the mobile node making frequent handovers between different access networks can greatly impact handover latencies and also increase the load of the AAA backend.

In this paper we concentrate on access authentication in wireless access networks (typically IEEE 802.11 WLANs), and how to secure the communication between a mobile node and an access network. Furthermore, this paper proposes solutions on how to expand the security associations that were created during the network access authentication further to the service level authentication, generic services and IP connectivity bootstrapping. We also investigate centralized wireless access network model where a number of lightweight, simple WLAN base stations are connected to a central controller that takes care of all computationally heavy processing. The solution allows deployment of low cost hardware for WLAN base stations and reduces handover latencies due the network side assistance. All these are based on leveraging the Host Identity Protocol Base Exchange [4] having mobile operator's managed network deployment architecture in mind. We also present general measurement results of the Host Identity Protocol based access authentication.

The rest of this paper is structured as follows: section II describes the basics of Host Identity Protocol and how to apply it into network access authentication. Section III describes the overall solution for the Host Identity Protocol based access authentication, and section IV presents measurement results conducted with our implementation. In section V we discuss about possible enhancements and future work. Finally, the

section VI concludes the paper.

II. Applying HIP Based Network Access into Managed Networks

A. HIP Overview

The Host Identity Protocol (HIP) and the HIP architecture [4] consist at minimum of two nodes: a HIP initiator (HIP-I) and a HIP responder (HIP-R). The complete architecture contains additional components, such as Rendezvous servers, DNS servers and AAA backends. The main goal of the HIP architecture is to add a new namespace to identify hosts, instead of using IP addresses as both host identifier and locator. The locator and identifier split has been identified as a possible way to solve problems of multi-homing, mobility and security in the future Internet architecture.

Each host in the HIP architecture has at least one unique Host Identity (HI), which basically is a public key. A Host Identity Tag (HIT) is a fixed length cryptographic hash of the HI. A HIT is easier to handle at protocol level over the wire. During the HIP Base Exchange, the HIP-I does two request-response transactions with the HIP-R; these messages and their replies are called I1, R1, I2 and R2. The design goal of this 4-way handshake is to make HIP resilient to denial of service attacks. The first response from the HIP-R (R1) contains a puzzle for the HIP-I to solve. Only after a correct answer has been received (in I2), the HIP-R establishes state information regarding the HIP-I. After the Base Exchange is complete, the HIP-I and the HIP-R have a HIP Security Association (SA) and keying material to be used with e.g. a transport layer security protocol, such as Encapsulated Security Payload (ESP) [5].

B. Generic Bootstrapping and Managed Deployment Model

Bootstrapping in networking is defined as the process where a node, without any initial configuration or knowledge of the network, gains enough knowledge to begin communicating. However, since this information can only be delivered by the network itself, bootstrapping relies on some static, globally known constants. In IP networks, for a node to begin communicating outside its local link, it generally has to know: *i) its globally routable IP address including the subnet prefix, ii) the default gateway, and iii) DNS server(s)*.

Our focus in this paper is on extending the HIP Base Exchange to a generic bootstrapping of a HIP capable mobile host in a WLAN environment. The HIP base protocol is easily extendable introducing new Type Length Value (TLV) pairs whenever there is a need to pass new configuration information to the HIP-I. Our reference wireless technology is a 802.11 WLAN deployment, that requires authentication, data security (ciphering) at least over the wireless part of the link, possibly assignment of services level configuration information and services level SAs between the HIP-I and the entity authenticating the HIP-I. The goal of including generic bootstrapping into the HIP Base Exchange is to reduce the amount of signaling required on each layer before the end host is ready to start IP communication. For example, a Mobile IPv6 mobile node in current WLAN networks needs to first run link layer security protocol, where the WLAN base station authenticates the mobile node from a AAA server, then run a protocol to obtain an IP address and other configuration parameters, and only after that send Mobile IPv6 binding update messages to home agent and corresponding nodes. This easily sums up to a dozen or more roundtrips over the radio link before the applications in a mobile node can proceed communication [3]. It is also possible that the HIP-based bootstrapping is the only method for the HIP-I to learn and configure its globally routable IP address.

Managed networks usually have a set of requirements that need to be met before deployments. The management entity may be e.g. a commercial network operator or a community requiring some kind of subscription based participation. Especially in commercial operators' networks these requirements typically include the following: *i) robust accounting and billing functionality, ii) inter-operator roaming capabilities, iii) subscriber traceability, iv) adequate security, v) robust authentication of subscribed user against the subscriber database, vi) interoperability and scalability, and vii) a feasible subscriber and security credential management*. An example of a managed WLAN network architecture is the 3GPP Interworking WLAN [6] architecture that relies on IEEE802.11i [7] and extends 3GPP Release-6 GPRS mobile core [8].

Operators are typically inter-connected via a common roaming backbone network. The purpose of the inter-connection and roaming backbone network is to provide basic but secure IP connectivity and routing services for operators so that end users may gain network access through any access provider that is part of the inter-connection and roaming backbone. These roaming backbone networks may be intentionally separated from public Internet for security and efficiency reasons. GPRS Roaming eXchange (GRX) [9] is an example of such backbone that provides AAA, any IP data inter-connection, and GPRS roaming services for hundreds of GSM operators today. Operators provide subscriber management and AAA services in their home networks.

C. Reference Architecture

Figure 1 illustrates the reference model of our network architecture containing four nodes: *HIP-I* (STA - a node joining to the network), *WLAN base station* (BS), *HIP-R* and a *backend home AAA* (AAAH - for authenticating nodes). The interaction starts with HIP-I joining the WLAN network. After link layer connectivity has been set up, the HIP Base Exchange begins. Normally, HIP messages are only sent after IP connectivity is already up. However, since we are using HIP *for* bootstrapping, HIP messages have to be sent without any knowledge of the network. One possibility is to use well-known link-local address spaces (fe80::/10 for IPv6 and 169.254.0.0/16 for IPv4) or known multicast address spaces (ff00::/8 for IPv6 and 224.0.0.0/4 for IPv4) for HIP-R.

Data traffic between the HIP-I and the HIP-R is protected by ESP at IP layer. The reference model described in this

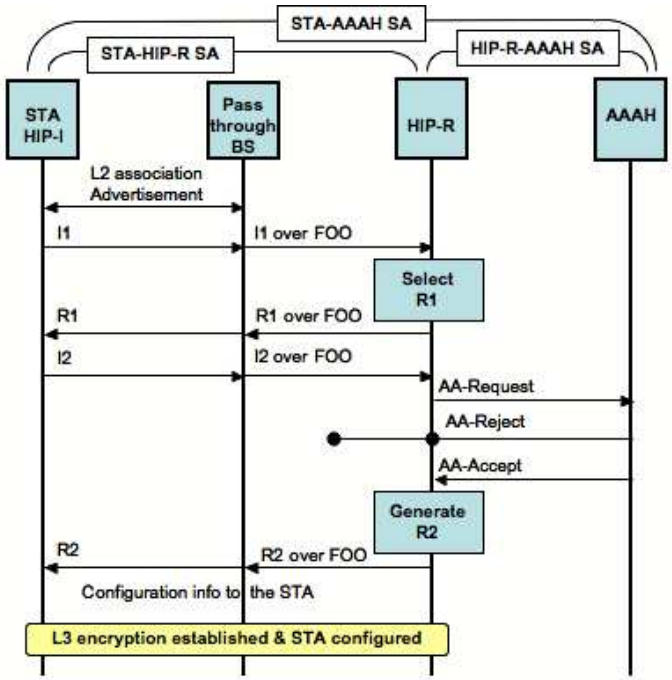

Fig. 1. HIP based network access architecture in an operator like deployment with AAA backend

paper advocates deployments, where one master node (HIP-R) manages a number of simple low-cost pass-through (layer-2 bridge) BSes. In our case these pass-through BSes provide only access to network without any lower layer support for security or any IP layer functionality other than bridging IP packets. HIP related and Network Access Server (NAS) functionality is completely delegated to the central master node (HIP-R) in the access network.

The architecture and deployment model described in this paper has several advantages: *i) use of simple and low-cost 802.11 BS technology without any layer-2 security solution, ii) no need for secure key distribution protocol deployment, iii) fast handovers between BSes are easily made possible* and *iv) only one node (HIP-R) interacts with the AAA backend, which simplifies the access network deployment and management greatly*. The only requirement for BSes is that they act as pass-throughs between HIP-I and HIP-R. Optionally, they may be extended to advertise the HIP Network Access Protocol (NAP) service and the address of the HIP-R. Without the extension, HIP-I could opportunistically send the I1 to a well-known multicast address and try to initiate the HIP NAP exchange.

D. Related Work

Optimizing network attachment for wireless networks has been an active area during past years and various Standards Development Organizations (SDO) have worked on specifications for their access systems. IEEE 802.11r [10] specifies the fast BSS transition system for 802.11 WLANs and IETF HOKEY work [11] addresses the key management and fast re-authentication issues for Extensible Authentication Protocol (EAP) [12]. Multiple 802.11 WLAN hardware vendors have also introduced WLAN switch products that shares ideas of the centralized HIP-R presented in this paper as well as in IETF CAPWAP [13] work. Recent work in IEEE 802.11u [14] includes Generic Advertisement Service (GAS) that allows for example the advertisement of access network capabilities and roaming connections prior authentication. The Mobile WiMAX [15] standardization include both fast BS transition and centralized switch type functionality. Arkko et al were the original proposes of using an integrated HIP-like message exchange for WLAN access authentication and bootstrapping [3]. The service level authentication for 3^{rd} parties has also been addressed in some SDOs. One example is the 3GPP Generic Authentication Architecture (GAA) [16].

III. Solution Overview

A. Capability Advertisement

Our BS implementation consists of FreeBSD 6.1 system in `Host AP` mode, with extended 802.11 beacon frames. We added one additional Information Element (IE) to all beacon frames sent by the BS, which is illustrated in table I. This IE has a tag number 0x63 (reserved), and consists of 8 octets of data. The first 2 octets contain a Service Type. At the moment only two bits are used: Bit 0 ('H') informs that the capability for HIP-based access exists, and Bit 2 ('V') informs about IPv6 capability. Reserved bits are marked as 'r'. The remaining 6 octets contain the MAC address of the HIP-R. When a HIP-I, running our modified `wpa_supplicant`, detects a BS with HIP access capability, the following procedure gets executed:

1) `wpa_supplicant` performs 802.11 open authentication and association
2) `wpa_supplicant` passes the IE to `hip daemon`
3) `hip daemon` constructs the link-local IPv6 address of the HIP-R using EUI-64 address derivation
4) HIP-I's `hip daemon` contacts the HIP-R's `hip daemon`
5) `hip daemons` perform an opportunistic HIP Base Exchange
6) `hip daemons` set up ESP SAs with each other's HITs
7) User plane traffic can flow between HIP nodes

Our solution is actually IP version agnostic. The implementation used IPv6 due to the well-known method for deriving link-local IPv6 addresses from MAC addresses and the simplicity of including HIP-R's MAC address in a beacon. The beacon information could have easily been replaced with, for example, IPv4 address from 169.254.0.0/16 space.

TABLE I
HIP Bootstrapping Information Element in Beacons

Tag	Len	Service Type – bit 0														MAC Address						
0x63	0x08	r	r	r	r	r	r	r	r	r	r	r	r	V	r	H	nn	nn	nn	nn	nn	nn

B. HIP Based Access Protocol

The HIP-based bootstrapping mechanism was briefly described in section II-B. The centralized model of our deployment is shown in figure 2. Each BS advertise the same

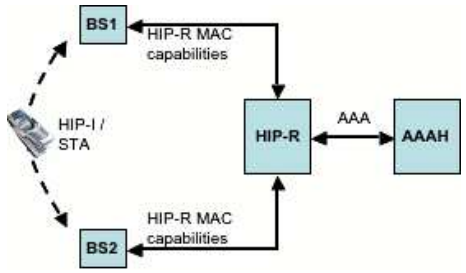

Fig. 2. Centralized management of the access network

HIP access information. A handover between BSes under the management of the same HIP-R does not cause invalidation of the HIP level SA and the associated key material. This is a result of not including any kind of channel binding between HIP peers and the BS into the HIP Base Exchange. As a result a new HIP Base Exchange is only required when the HIP-I roams to a BS under another HIP-R.

After initiating the opportunistic HIP Base Exchange (I1 and R1 message exchange) the HIP-I continues by sending the I2 message. The I2 message contains a HOST_ID field [4] that is used to convey HIP_I's domain identifier in a NAI [17] form (*user@realm*). After receiving I2 message, HIP-R forwards the identifier and the required credentials to the AAA backend. The routing of AAA traffic makes use of realm-based routing. The HIP-R is considered as a trusted party by the AAA infrastructure. The AAA returns either Access-Reject or Access-Accept with possible additional bootstrapping information. Upon receiving an Accept, the HIP-R completes the Base Exchange by sending the R2 message including any additional received bootstrapping information. Once the the HIP Base Exchange has completed there are SAs between the HIP-I and the HIP-R.

Two STAs under the same HIP-R may well communicate directly with each other using link local addressing. The centralized model does not restrict that in any way. This is beneficial in a sense that a local traffic within the access network does not load the HIP-R or the AAA backend unnecessarily. Only when a STA needs to communicate outside the local access network (e.g. in order to access certain services) the HIP-based access needs to be run.

Our HIP-I and HIP-R implementations were based on FreeBSD 6.1 with modified `hip4bsd`[1] HIP distribution. The HIP-R and the AAAH used standard RADIUS [18] as the AAA protocol. The RADIUS client in the HIP-R was based on FreeRADIUS[2].

C. Security Associations and Keying Material

Section II-B described the general managed AAA framework for the HIP-based network access protocol solution. From figure 1 we can see that a number of SAs are required between different entities. Firstly the terminal (referred as HIP-I or STA) and the home network AAA (referred as AAAH) share a long lived SA and credentials. We call this the STA-AAAH SA. The STA and the AAAH use this SA for mutual authentication. The authentication procedure is conveyed over the HIP and AAA protocols between the STA and the AAAH. As a result of a successful authentication both the STA and the AAAH are able to create a master session key (MSK) material that can be used for subsequent service level authentications for 3^{rd} parties. The service level authentication is discussed in section V. Secondly the HIP-I and the HIP-R will dynamically create SAs after a successful HIP Base Exchange. We call this the STA-HIP-R SA. Thirdly the HIP-R and the AAAH must also share a long lived SA and required credentials. We call this the HIP-R-AAAH SA.

The details of the STA-AAAH and HIP-R-AAAH SAs are out of scope of this paper. The required provisioning of the security related data is also out of scope of this paper but could be done out-of-band between the STA and the AAAH, and between the HIP-R and the AAAH. In mobile operator deployment scenarios it is highly probable that the STA also contains some secure tamper proof smart card media such as a UICC [19]. This media could be used to store *HIP HI*, *corresponding private key*, *HIP-I identities*, and the credentials needed for the *STA-AAAH SA*.

IV. Experimentation Results and Analysis

A. Experimentation Setup

Our experimentation setup is similar to the topology illustrated in figure 2. All nodes were Compaq Armada laptops with 500MHz Pentium II CPUs running FreeBSD 6.1. For WLAN access we used D-LINK's 802.11bg PCMCIA cards. The AAAH was TeliaSonera's commercially used RADIUS server. The BSes were set to the same channel because that allowed easier monitoring of WLAN traffic over the air. The experimentation premises had 22 other discoverable active WLAN networks on random channels.

We ran three series of experimentations aiming to measure how well our implementation performs in a deployment scenario it has been designed for and also how it compares to other deployments with and without security. The first one included the HIP-based access, selection of the BS, running the HIP Base Exchange, authentication to the RADIUS server and a series of 30 script generated handovers between BSes. The second experimentation was essentially the same as the first one but only using a basic IEEE 802.11 open authentication without any security or RADIUS backend involvement. The third experimentation was again the same as the earlier ones but this time the security was based on WPA2 and EAP-TLS [20] authentication. EAP-TLS authentication was terminated to the same RADIUS server as in the first experimentation. The PMKSA caching feature of IEEE 802.11i was enabled. In all our experiments the background traffic was normal once a second initiated `ping` echo request-reply. `ping` traffic was considered good enough for initial testing of our implementation, although we realize that it does not represent any realistic application or user traffic scenario.

[1]Available at: http://www.hip4inter.net
[2]Available at: http://www.freeradius.org

B. Results and Analysis

The results of the first handover experiment are shown in table II. We measured handover (HO) latencies in both downlink (DL) and uplink (UL) directions. In the table the Probe delay means the time it takes for the STA to realize it has lost the connectivity to the previous BS and done the probing of BSes it knows. The Probe+Association means the time the STA broadcasts a Probe to find any new BS that supports the HIP-based network access, receives replies, selects the BS that advertises the support for HIP-based network access and completes the 802.11 authentication and association to the new BS. The Hi means highest value in the whole test set and respectively the Lo means the lowest value. We also show the 80% percentile of the measurements. The initial attachment took a total of *1,45s* out of which 802.11 association contributed *0.61s*, the HIP Base Exchange processing *0.82s* and the RADIUS negotiation *0.01s*. The HIP Base Exchange is run only during the initial attaching to a HIP-R or when there is a need to rekey an existing HIP SA. The units in all tables are seconds.

TABLE II
EXPERIMENTATION 1) RESULTS WITH PING BACKGROUND LOAD AND HIP BASED SECURITY AND AUTHENTICATION

	Handover Latency DL	Handover Latency UL	Probe delay	Probe + Association
Hi	7.01	3.62	3.21	0.62
Lo	2.70	2.66	2.25	0.21
80%	4.71	3.48	3.05	0.41
avg	3.93	3.17	2.74	0.43

The table III shows the results of the IEEE 802.11 open authentication tests without any security or authentication involving the AAA backend. We can see that the open authentication does not do much better than our HIP-based solution, which indicates that the overhead of our approach is neglible.

TABLE III
EXPERIMENTATION 2) RESULTS WITH PING BACKGROUND LOAD AND IEEE 802.11 OPEN AUTHENTICATION WITHOUT ANY SECURITY

	Handover Latency DL	Handover Latency UL	Probe delay	Probe + Association
Hi	3.63	4.5	3.22	0.61
Lo	2.67	2.67	2.05	0.21
80%	3.38	3.49	2.90	0.61
avg	3.12	3.19	2.59	0.53

The table IV shows the results of tests using WPA2 security and EAP-TLS authentication. The initial authentication to a new BS includes also RADIUS negotiation with the AAA backend. The RADIUS negotiation with the first BS took 0.39 seconds and with the second one 0.48 seconds respectively. The subsequent authentications made use of the IEEE 802.11i Pairwise Master Key SA (PMKSA) caching functionality, thus the authentication was completely local and between the STA and a BS. The functionality of the PMKSA caching resembles our HIP-based solution in a sense of reducing the AAA backend load. However, attaching to a new BS requires involving the AAA backend even if BSes were in the same administrative domain, where as the HIP-based solution requires only involvement of the AAA backend when crossing administrative domains.

From the results in the table IV we can see that our HIP-based solution competes evenly with a state of the art industry solution and even outperforms it time to time. However, IEEE 802.11i requires extensive software, layer-2 security and hardware ciphering support for WPA2 security and PMKSA caching feature, where as our HIP-based solution operates on top simple low-cost and inherently insecure IEEE 802.11 system. When extending the measurement setup to include all necessary functions to support inter-domain mobility, the benefit of the HIP NAP should be more visible. We believe that the current layer-2 security+IP configuration+IP mobility sequence can be replaced with a single HIP Base Exchange, thus shortening the messaging sequence considerably. Also, if in the future internetworking nodes have HIP or similar protocol installed anyway, then using it for several layers and purposes could reduce the complexity (amount of code) of the nodes, e.g. layer-2 can be kept simpler.

TABLE IV
EXPERIMENTATION 3) RESULTS WITH PING BACKGROUND LOAD WITH WPA2 SECURITY AND EAP-TLS AUTHENTICATION

	Handover Latency DL	Handover Latency UL	Probe delay	Probe + Association
Hi	7	7	4.22	3.31
Lo	3	3	2.06	0.23
80%	5.2	5.2	2.93	0.63
avg	3.93	3.93	2.67	0.72

In our HIP-based implementation the access authentication does not contribute to the handover latencies after the initial authentication. As long as the STA stays under the same HIP-R there is no need to re-establish the IP level security association.

Considerable amount of handover latency originates from the scanning and probing phase when the STA discovers it has lost the connectivity to the previous BS and tries to find a new target BS [21]. For example, in the experiment 1 approximately 74% of the downlink direction handover latency was contributed by the scanning and probing. It turned out that the real source of the latency in our case were the WLAN driver and the wpa_supplicant implementations for FreeBSD. The handover latency could possibly be significantly reduced by dropping the wpa_supplicant from the handover decision process and leaving all that to the WLAN driver implementation. Also the impact of modifying the WLAN driver aggressiveness on handovers should be investigated but is out of scope of this work. The current implementation was notably conservative on initiating a handover.

V. FUTURE WORK

One of the topics that was left out of this paper is the handovers between HIP-Rs. Most likely a single HIP-R serves dozens or hundreds of BSes, and one or more IP subnets.

Therefore the handover not only involves HIP and AAA, but also IP mobility. Besides IP mobility, handovers between HIP-Rs of different operators present yet another problem field, for example if we need to deploy context transfer between HIP-Rs. We need to study further, how current standardized HIP IP mobility solution [22] fits to our proposed architecture.

Our implementation does not yet include mutual authentication between the STA and the AAAH. Subsequently the support for service level authentication and the generation of the associated MSK is not completed. The value of service level authentication is that a STA can authenticate towards 3^{rd} party services without preset SAs and 3^{rd} party services can also authenticate the STA towards the AAAH without knowing the STA beforehand. The details of the solution are left for further study.

The third possible future work item is the layer-2 encryption support, i.e. how could the existing layer-2 encryption protocols be fed with the keying material generated during the HIP Base Exchange. This would require a protocol between the BS and the HIP-R. We also plan to verify whether the centralized approach actually scales better price/performance wise when the security in implemented at IP layer or at layer-2.

TABLE V
SUMMARY OF EXPERIMENTATIONS AND COMPARISON OF TECHNOLOGIES

Technology	**Security**	**AAA Backend**	**Capability Advert.**	**Avg. HO Latency**
HIP-based	Auth+encr at IP layer, STA-HIP-R	Once per each HIP-R	IP config options	3.93s (DL) 3.17s (UL)
802.11 open	none	none	none	3.12s (DL) 3.19s (UL)
WPA2 + EAP-TLS	Auth+encr at layer-2, STA-BS	once per each new BS	Security + QoS options	3.93s (DL) 3.93s (UL)

VI. CONCLUSIONS

This paper described our implementation of an enhanced HIP-based Network Attachment Protocol and bootstrapping solution using IEEE 802.11 WLAN as the example wireless technology. We showed that its centralized deployment model with AAA backend subscriber management has potential in managed operator WLAN networks. Our IP layer approach allows deploying notably low cost base station hardware solutions with minimal management overhead and AAA backend load. The HIP-based solution itself is access technology agnostic except for the capability advertisement that our implementation used, for example, to discover the central HIP-R node. The capability advertisement also helps a STA to find and select quickly a target network that supports our HIP-based solution. The table V shows the summary of the HIP-based Network Attachment Protocol compared to IEEE 802.11 with open authentication and WPA2 based security.

The handover experiments showed that our implementation does not at its current state meet realtime applications' requirements. The latencies are just too big. However, the experiments also showed that the handover latencies are not caused by our HIP-based Network Attachment Protocol and its security solution but rather due the used WLAN driver implementation. Our HIP-based solution has no additional overhead to handover latency as long as the STA stays connected to the same central HIP-R node.

ACKNOWLEDGMENT

This work was conducted under the TEKES funded MERCoNe project (http://www.tekes.fi/eng/giga).

REFERENCES

[1] J. Arkko, B. Aboba, J. Korhonen, and B. Fari, "Network Discovery and Selection Problem," draft-ietf-eap-netsel-problem-08.txt, June 2007.
[2] J. korhonen, "Performance implications of the multi layer mobility in a wireless operator networks," *Fourth Berkeley-Helsinki Ph.D. Student Workshop on Telecommunication Software Architectures*, June 2004.
[3] J. Arkko, P. Eronen, H. Tschofenig, S. Heikkinen, and A. Prasad, "Quick NAP - Secure and Efficient Network Access Protocol," *In Proceedings of the 6th International Workshop on Applications and Services in Wireless Networks (ASWN 2006)*, pp. 163–170, May 2006.
[4] R. Moskowitz, P. Nikander, P. Jokela, and T. Henderson, "Host Identity Protocol," draft-ietf-hip-base-08.txt, June 2007.
[5] S. Kent, "IP Encapsulating Security Payload (ESP)," RFC 4303 (Proposed Standard), Dec. 2005.
[6] 3GPP, "3GPP system to Wireless Local Area Network (WLAN) interworking; System description (Release 6)," 3GPP TS 23.234 6.10.0, Sept. 2006.
[7] IEEE, "IEEE Standard for Information Technology - information Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements," IEEE P802.11i-2004, July 2004.
[8] 3GPP, "Technical Specification Group Services and Systems Aspects; Network architecture (Release 6); Stage 2," 3GPP TS 23.002 6.10.0, Dec. 2005.
[9] GSMA, "Inter-PLMN backbone guidelines; version 3.7," GSM Associations, Official Document PRD IR.34, Apr. 2006.
[10] IEEE, "Draft Amendment to STANDARD FOR Information Technology - Local and Metropolitan Area Networks; Amendment 2: Fast BSS Transition," IEEE P802.11r/D4.00, Nov. 2006.
[11] T. Clancy, "Handover Key Management and Re-authentication Problem Statement," draft-ietf-hokey-reauth-ps-02.txt, July 2007.
[12] B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, "Extensible Authentication Protocol (EAP)," RFC 3748 (Proposed Standard), June 2004.
[13] L. Yang, P. Zerfos, and E. Sadot, "Architecture Taxonomy for Control and Provisioning of Wireless Access Points (CAPWAP)," RFC 4118 (Informational), June 2005.
[14] IEEE, "Draft Amendment to STANDARD FOR Information Technology - LAN/MAN Specific Requirements - Part 11: Interworking with External Networks," IEEE P802.11u/D0.02, Nov. 2006.
[15] WiMAX Forum, "WiMAX end-to-end network systems architecture (stage 3: Detailed protocols and procedures)," Work-in-progress draft, subject to change. 2006 Release 1 V&V DRAFT, Aug. 2006.
[16] 3GPP, "Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic bootstrapping architecture (Release 7)," 3GPP TS 32.220 7.6.0, Dec. 2006.
[17] B. Aboba, M. Beadles, J. Arkko, and P. Eronen, "The Network Access Identifier," RFC 4282 (Proposed Standard), Dec. 2005.
[18] C. Rigney, S. Willens, A. Rubens, and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)," RFC 2865 (Draft Standard), June 2000, updated by RFCs 2868, 3575.
[19] 3GPP, "Characteristics of the Universal Subscriber Identity Module (USIM) application (Release 6)," 3GPP TS 31.102, Mar. 2007.
[20] B. Aboba and D. Simon, "PPP EAP TLS Authentication Protocol," RFC 2716 (Experimental), Oct. 1999.
[21] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process." [Online]. Available: citeseer.ist.psu.edu/541775.html
[22] T. Henderson, "End-Host Mobility and Multihoming with the Host Identity Protocol," draft-ietf-hip-mm-05.txt, Mar. 2007.