Location Privacy Extensions for the Host Identity Protocol

Alfredo Matos, Justino Santos, João Girão[†], Marco Liebsch[†], Rui Aguiar

[†] NEC Europe Ltd, Network Laboratories

Abstract – **Privacy and security are key aspects on future communication networks. The Host Identity (HIP) aims to provide identity based security in new networks. In this document we propose an aditional framework based on the Host Identity Protocol that provides location privacy to registered attendents.**

Keywords – **Location, privacy, Host Identity Protocol, architecture.**

I. INTRODUCTION

The future of communications in the Internet is evolving to something where concepts such as mobility and global reachability are very common. Nowadays we can already see an increasing number of access technologies (e.g. wireless, WiMax, GPRS), user equipments with multiple network interfaces and new popular kinds of services (e.g. VoIP) that require mobility support. However, when the current Internet architecture was designed, mobility and multihoming where not taken in consideration. In the current Internet architecture, IP addresses are used simultaneously as locators and identifiers for a host, mainly because in the late 1970's no one would imagine that computers would be multihomed or even mobile. Nodes were basically static and trusted, reasons by which IP addresses could be used as identifiers and locators. Solutions such as the Host Identity Protocol (HIP) [1], [2] and FARA [3] try to address the IP address dual role problematic.

Another great concern of today's networks is closely related to security and privacy. Specifically, location privacy has a big role in new mobile networks. Users don't wish to be tracked either by the network provider or by third parties. In [4] location privacy is defined as the capability of preventing other parties from learning one's previous or current location. Location mainly pertains to the topological position of a node, and not its geographical position, although frequently the topological location can give a very accurate geographical position.

For a node to obtain location privacy, there must be no relation between its identifiers and locators. Location privacy concepts [5] clearly state that the problem is not limited to a single layer. In fact, it concerns all identifiers associated with a node, including MAC and IP addresses. Thus another important problem is the identifier interdependency, where, for instance, a mobile device moving through foreign networks always carries the same unique MAC address. However, location privacy problems concerning the MAC Layer are considered out of scope for this document. The threat model also discusses the location privacy problems at the network layer. Using the IP address as identity and locator, the way it's currently done in the Internet, makes this relation almost impossible to conceal. In the IPv6 context, a Mobile Node (MN) performing address auto-configuration is implicitly disclosing its MAC address, allowing a direct mapping between MAC address and IPv6 address. Furthermore, the usage of Mobile IPv6 [6], discloses location and associates it with the node identifier.

The Host Identity Protocol [1], [2] is receiving a lot of attention for identifier/locator separation, but currently it does not support location privacy considerations. In our work, we try to address location privacy issues through a HIP based generic framework with support for mobility, allowing users to successfully attach to a new network without leaking location information. In Section II we present a survey of related work. In Section III, we introduce the HIP protocol, and the necessary location privacy consideration that we try to address with this novel solution. In Section IV we explain the proposed framework. Section V shows the protocol operations for registration, packet delivery and mobility of endpoints. In Section VII we summarize the advantages of this framework and proposed future work.

II. RELATED WORK

The current work in this area is focused on new network architectures or mechanisms that are able to cope with location privacy issues. IP2 [7], Turfnet [8] and I3 [9], while not focusing on location privacy, are able to address some issues.

IP2 [7] is able to hide the user location through the use anchor point in the network that handles mobility issues. This resembles what happens in HMIPv6 [10] (with MAPs) and our proposed framework (with RVAs).

Overlay networks provide also good approaches to hide location information. In I3 [9], a new realm for routing is defined, based on names. Using a rendezvous point for the communicating partners, it is possible to achieve some degree of location privacy. In Turfnet [8], location privacy is achieved implicitly mainly due to a innovative method of routing and usage of Turfnet Gateways connecting each Turf. However it is difficult to achieve optimal routing.

Onion routing [11] is particularly interesting: it prevents the transport medium from knowing who is communicating with whom by using multiple onion routers, where each router is responsible for one layer of encryption, added by the Onion Routing Proxy. Even though this procedure hides location from transport elements, it presents several drawbacks: the high processing overhead at each router; the user's identity is not protected from the first proxy, and the path to that proxy; endpoints are aware of the location information.

In [12] a complete identity protection framework for endpoints is presented. This paper proposes a Diffie-Hellman authenticated agreement for identity exchange. Regarding location privacy, a solution based on identity aware NATs is proposed. When an endpoint tries to initiate communication with the other end point, it uses a Forwarding Agent that selects a virtual IP address for it. The peers are able to see only the virtual address, not the real address of the endpoint. Although very similar to our approach, security between endpoint and Forwarding Agent is not considered, neither how mobility is supported.

The presented approaches can achieve a certain degree of location privacy, but either lack on performance or do not offer a high degree of location privacy. Our privacy framework based on HIP tries to address these issues.

III. HOST IDENTITY PROTOCOL

The Host Identity Protocol (HIP) [1], [2] introduces a new cryptographic namespace for identification that eliminates the dual role of IP addresses, providing added flexibility for solutions that provide location privacy (fig. 1). In addition to this separation, in HIP protocol is defined to negotiate security associations between HIP capable nodes.

A. Separation Between Identity and Location

HIP provides a solution for decoupling the location from the identity. When used, each host has one or more identities, long or short-term, that can identify it in the network. A cryptographic public key, of an asymmetric key pair, the Host Identity (HI), is used and acts as the host's unique identifier. The host private key can prove that it actually owns the identity that the public key represents. In comparison to real life, it resembles showing an ID-card.

The identifier - HIP Host Identity (HI) - in form of a public key, is not practical to use on the wire due to its length. The HI can be represented by a 128-bit long Host Identity Tag (HIT), that is a hash of the HI. Thus, the HIT pertains to an HI. Since the HIT is 128-bits long, it can be used seamlessly by IPv6 applications because it has the same length as IPv6 addresses. When HIP is used, the upper layers, including the applications, are not aware of the IP Address used for routing.

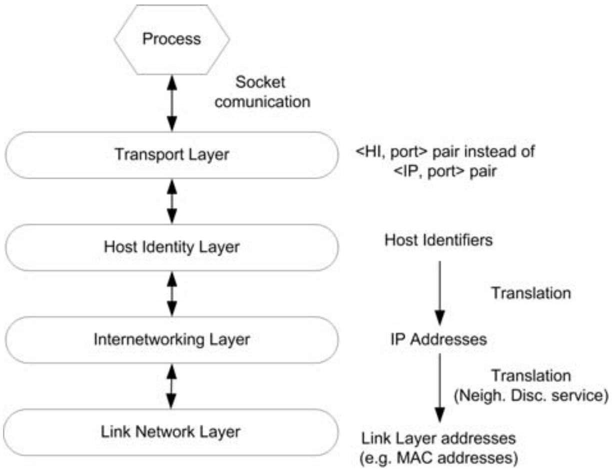

Fig. 1 - HIP proposed architecture

B. Base Exchange

The HIP base protocol defines a base exchange (BE) which is an authenticated Diffie-Hellman four-way handshake. The BE provides means for two nodes to prove their identity to each other. The BE establishes cryptographic material that is later used to establish IPSec Security Associations, enabling a secure communication channel between two nodes. These security associations between the hosts are bound to the Host Identities. However, the packets travelling in the network do not contain the actual HI information, but the inbound packets are identified and mapped to the correct SA using the Security Parameter Index (SPI) value in the IPsec header.

C. Mobility and Multihoming

With HIP, the separation between the location and identity information makes it clear that packet identification and routing can be decoupled. The host receiving a packet identifies the sender by first getting the correct key and then decrypting the packet. Thus, the actual IP addresses that were used for routing the packet are irrelevant, providing implicit mobility, since changing IP addresses (roaming) does not break ongoing sessions. Mechanisms have been defined for end-host mobility and multihoming signalling [13], allowing a host to securely inform a corresponding peer of the set of IP addresses in use, while maintaining upper layer sessions. This is done through a generalized locator parameter for use in HIP messages. The locator parameter allows a HIP host to notify a peer about alternate addresses at which it is reachable.

D. Rendezvous

A rendezvous mechanism was also designed in [14] allowing hosts to be reached if they are mobile without using dynamic DNS updates.

E. HIP Location Privacy Issues

The current HIP architecture does not take into account location privacy issues. The support for mobility in HIP [13] requires a node to send its locator to every correspondent node it is connected to. In the base exchange this accomplished by including the locator parameter in R1 and I2 messages. In case of a L3 handover occurs, explicit update messages with the locator parameter must be sent. This procedure is comparable to the Binding Update messages exchanged between MIPv6 [6] enabled Mobile Nodes (MN) and Correspondent Nodes (CN) when performing route optimization. One can learn the current location of a mobile node by simply inspecting the base exchange and update messages, which means a complete loss of location privacy.

Even if we consider the presence of an rendezvous server (RVS), the Initiator does not immediately reveal the current locator of the Responder. However, that information is disclosed in the R1 packet.

In both approaches an end-to-end addressing mechanism is used. This means that both Initiator and Responder will always learn each other's current IP address once the BE is completed, since the resolution, Identifier to Locator, is done at the end hosts. Furthermore, capturing the HIP base exchange enables an eavesdropper to learn the HITs and IPv6 addresses of both participants, consequently forfeiting the location privacy of the peers. HIP ultimately suffers from the same location privacy issues as MIPv6 described in [5]. If the target HIP node of a DNS query is not registered in an RVS then the DNS resolves to the current IPv6 address of the node.

In an architecture that supports location privacy, the HIP nodes should never be able to map the identifier to the real locator of the node. In [15] some considerations and network elements are introduced to shield a HIP node's location. Our proposal is to use the current HIP architecture and introduce new functional units and enhanced protocol operations that solve the above mentioned problems, providing location privacy to attendants [16].

IV. HIP LOCATION PRIVACY ARCHITECTURE

As suggested in [15], location privacy is provided by delegating the HIT to IP resolution into a network entity called the Rendezvous Agent (RVA). Moving the resolution upwards in the network topology, from the HIP Mobile Node (HMN) to the RVA, has the benefit that locators can eventually be omitted within the Access Network. The core feature of the proposed solution is the concept of RVA protected areas, which are Access networks, where locators are concealed or not used at all. Instead, HITs are used to identity the traffic path. RVAs are also responsible for local mobility under their protected areas. We do not assume any transport layer, as long as it can support HIP. Currently, HIP is defined only for IPv4 and IPv6. In this document, for simplicity, we provide examples assuming the presence of IPv6.

Rather than defining a specific transport layer for our approach, we base ourselves in some basic assumptions that allow the specified mechanisms to work in generic way, independent of the technology used. The only assumption made is that the core network is IP based. In RVA protected areas, the technology used may differ and the solution is closely related to this. Basically, we propose some instantiations based on direct IPv6 address translations, tunnels and semantical adaptations (replacing IPv6 addresses with HITs). In principle all approaches are valid and one should just keep in mind that, when a specific approach is chosen, optimizations might be possible. For example, if a tunnel mechanism is used between RVAs, there is no need for a global locator attribution per HMN. In Section VI an IPv6 based solution is described.

An example of the proposed topology has been illustrated in figure 2. The scenario consists of two RVA protected areas connected to the Internet. An RVA protected area is composed by multiple ARs which are directly connected to an RVA. There are no assumptions on the number of RVA protected areas, although it is reasonable to think that an RVA covers a large number of ARs. A wider coverage of area, geographical or topological, limits the amount of location information revealed to an external eavesdropper. The RVS and DNS servers are located in the core. Note that several RVS's may exist in this architecture. The AR and the RVA are functional entities, thus they can also be collocated in the same machine. As stated in Sect. III-E, due to the area coverage of such an RVA, this option has consequences in the amount of the location privacy provided to the HMNs in that RVA protected area.

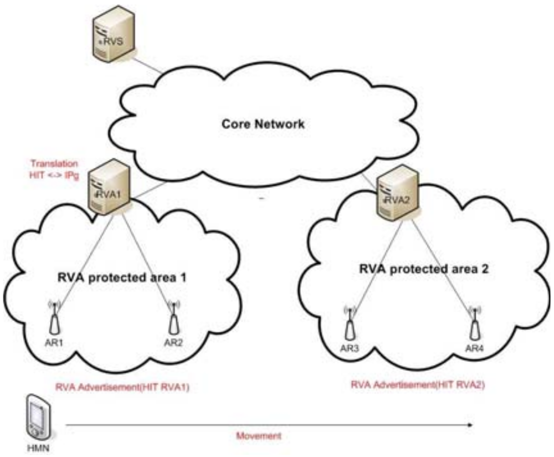

Fig. 2 - Basic architecture topology example

In order to provide location privacy, we introduce a new network entity - the RVA - and modify some of the existing entities in HIP archicteture and behaviour:

A. HIP Mobile Node

The HMN is meant to deal with intra and inter RVA mobility, signalling the RVA and RVS respectively. The HMN has to perform movement detection, based on the advertisements it receives from the ARs. There are no requirements in what concerns address auto-configuration, as the HMN does not use real IP addresses for communication in RVA protected areas. However, it is required to maintain a communication path to the AR by some undefined mean.

B. Access Router

The AR is responsible for forwarding the packets to/from the RVA or the AN edge router. It keeps a HIT based neighbor list of all the HMNs under it. Each entry of the HIT neighbor list contains a HIT based route to forward the packets from the RVA to the MN and vice- versa. The AR sustains the advertisement protocol by broadcasting RVA advertisement messages. This enables the HMN to learn the HIT of the local RVA and to perform movement intra and inter RVA area handover.

C. Rendezvous Agent

As described in [15], the RVA is an enhanced RVS that performs the IP-HIT address resolution function. This functionality split provides location privacy to the HMNs behind it. This is done by readdressing packets flowing between RVA protected areas and the core network. To forward packets to a destination HIT outside an RVA protected area, the RVA addresses a globally routable IPv6 address previously assigned by another RVA to the destination host. When an RVA receives packets from the outside network to a host belonging to its RVA protected area, it re-addresses them to HITs and forwards the packet to the destination. Note that the RVA is the entity which assigns globally routable IP addresses to the hosts under it, and the only one to map between HITs and global IP addresses. The RVA is capable of forwarding packets based on HITs because it maintains a table mapping for every HMN in the protected area to its point of attachment, which is the AR. The RVA is responsible for handling mobility for the HMNs in the protected area. This means that the RVA might have to signal other RVAs or HCNs on behalf of the HMNs for location updates.

D. Rendezvous Server

The Rendezvous Server (RVS) is a network entity which serves as the initial contact point for registered HIP nodes. The RVS provides a relaying service of incoming I1 packets to a Responder. A Responder uses the registration mechanisms defined in [14] to previously register with the RVS. After the first packet is relayed, all communication occurs directly without the assistance of the RVS. The proposed architecture implies that a Responder registers the HIT of his designated RVA, instead of normally using it's locators. When the initial I1 packet, sent by the Initiator, arrives at an RVS, the RVS resolves the identity of the Responder to the identity of a corresponding RVA, and finally obtains the locator of the RVA, effectively forwarding the I1 packet.

V. PROTOCOL OPERATION

In order for the privacy location scenario to work it is necessary to alter the basic HIP mechanisms. This includes changes in the base exchanges with both the RVA and RVS, mobility signaling, network readdressing of outgoing packets from the RVA protected areas and signaling between RVAs.

A. Base Exchange with RVA

When a HMN first arrives on a protected area is has to register with the responsible RVA. The RVA HIT is learnt from the Advertisement messages sent by the AR. Upon receiving an advertisement message, the HMN register with the announced RVA by means of a base exchange using the registration extensions defined in [17]. Note that no packet forwarding for the HMN is done until the BE is completed to avoid DoS attacks. After the BE is completed, the RVA learns the HIT-AR mapping for further packet forwarding.

The HMN can uses the BE to cross-certify his assigned RVA. This procedure can later be explored for mobility delegation and other explicit signaling from the RVA to the RVS on behalf of the HMN.

B. Base Exchange with RVS

After arriving on a new RVA protected area and performing the BE with the RVA described above, the HMN has to register with his RVS or update it. If the HMN is not yet registered in an RVS, it begins the registration process. This registration procedure consists in an enhanced base exchange which contains the identifier of the designated RVA for the node. The I1, R1 and R2 packets are the same as described for a standard base exchange with an RVS in [14].

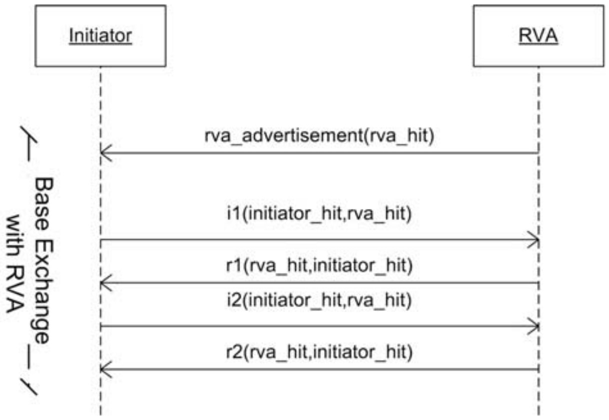
Initiator
RVA
Base Exchange with RVA
rva_advertisement(rva_hit)
i1(initiator_hit,rva_hit)
r1(rva_hit,initiator_hit)
i2(initiator_hit,rva_hit)
r2(rva_hit,initiator_hit)

Fig. 3 - Base exchange with Rendezvous Agent

The I2 packet contains an extra HIP parameter which carries the newly discovered RVA identifier. This parameter - RVA Parameter - is used to inform the RVS of the RVA identifier this HMN is currently using. This enables the HMN to register with the RVS not with a locator but with an identity.

In a RVA protected area, packets are routed using a transport mechanism (eg. point-to-point IPsec) that does not use the locators in the core network. For this reason, packets coming from a RVA protected area are processed and given the correct locators for routing in the core network. Packets arriving from the outside network need to be forwarded correctly to the current assigned AR for destination HIT. Until the base exchange is completed, no globally routable address is assigned to the HMN. Therefore, in the outside network, packets concerning signalling to a RVS use the locator of the HMN's assigned RVA.

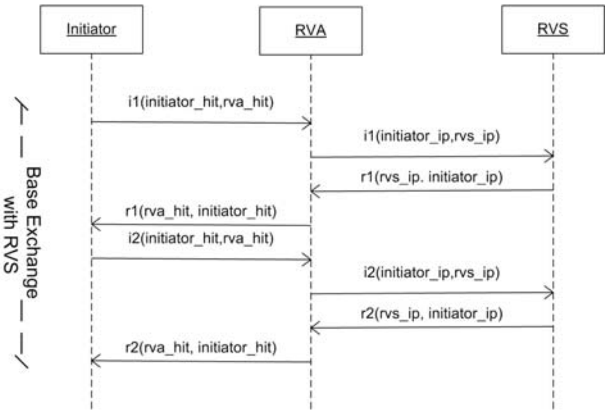

Fig. 4 - Base Exchange with Rendezvous Server

C. Base Exchange with HCN

The HIP base exchange between an Initiator and a Responder remains unchanged from HIP base protocol at the HIP layer. Key differences are at the network layer. The Initiator's RVA performs readdressing of outgoing packets to globally routable IP addresses. If the RVA does not know the Responder's HIT, it queries the DNS for its IP address. The DNS server then returns the IP address of the Responder's RVS. The RVS then relays I1 packet to the IP address of the Responder's RVA. This is done based on the two step mapping previously discussed where the Responder's HIT is translated to the RVA HIT, and then RVA HIT is finally translated to the RVA IP address. Also, the FROM and VIA Parameters are included as described in [14]. Upon receiving the I1, the Responder's RVA forwards the packet to the destination HIT's currently. The RVA also needs to store the newly learnt HIT I - IPg I mapping for further packet forwarding.

Afterwards, the HMN receives the packet and replies with a R1 packet. The R1 packet is then relayed in RVA, which performs its normal operation, readdressing the packet based on the on the learnt mapping. In the base exchanges remaining packets (I2 and R2) the globally assigned IP addresses of both I and R are used between RVAs.

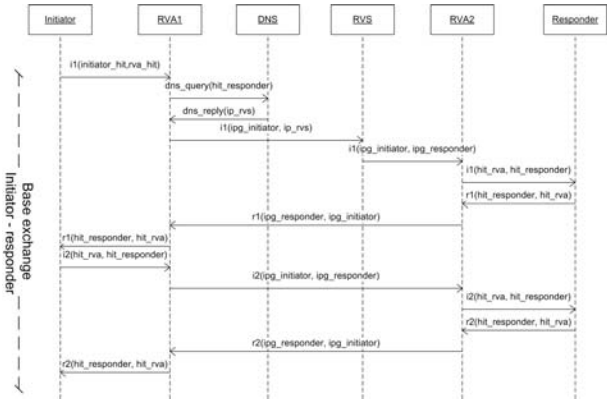
Initiator
RVA1
DNS
RVS
RVA2
Responder
i1(initiator_hit,rva_hit)
dns_query(hit_responder)
dns_reply(ip_rvs)
i1(ipg_initiator, ip_rvs)
i1(ipg_initiator, ipg_responder)
i1(hit_rva, hit_responder)
r1(hit_responder, hit_rva)
r1(ipg_responder, ipg_initiator)
r1(hit_responder, hit_rva)
i2(hit_rva, hit_responder)
i2(ipg_initiator, ipg_responder)
i2(hit_rva, hit_responder)
r2(hit_responder, hit_rva)
r2(ipg_responder, ipg_initiator)
r2(hit_responder, hit_rva)
Base exchange
Initiator - responder

Fig. 5 - Base Exchange with HIP Correspondent Node

D. Intra-RVA Handover

When a HMN detects that it has changed AR, though, without changing RVA protected area, it performs an intra RVA handover. Since the AR is in the same RVA protected area there is no need to update the RVS. The HMN updates its binding to the RVA directly, performing a normal HIP update procedure without a locator. This update message is used by the RVA to learn the new HMN - AR mapping. Note that the globally assigned IP for the node performing the handover remains the same. This location change is transparent to the RVS since the HMN remains in the same area. It is also transparent to other RVAs because the global assigned IP address for that node does not change.

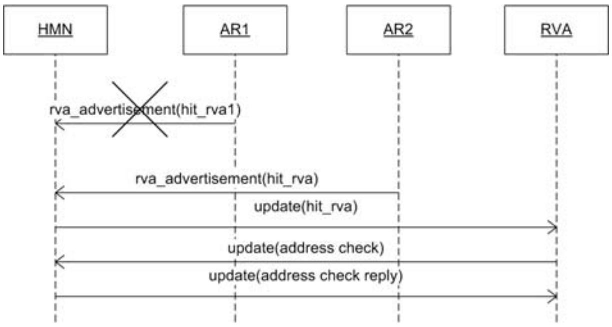
HMN
AR1
AR2
RVA
rva_advertisement(hit_rva1)
rva_advertisement(hit_rva)
update(hit_rva)
update(address check)
update(address check reply)

Fig. 6 - Intra RVA Handover

E. Inter-RVA Handover

The inter-RVA handover occurs when a HMN detects it has changed RVA protected area after receiving a RVA Advertisement message. The HMN then registers with the RVA by means of a base exchange. Then the HMN performs a normal Update to the RVS and to the old RVA. To the RVS, the HMN sends a HIP Update packet including the RVA HIT on a RVA parameter, in the same way it is done for the I2 packet mentioned before. The RVS updates the HMN entry according to this parameter, changing the responsible entity for the HMN to the new announced RVA. To the old RVA, the HMN sends an update packet with an RVA parameter. This packet is used to inform the old RVA that HMN as changed RVA protected area.

After the update procedure is completed, the old RVA needs to forward the data packets destined to the HMN to the new RVA. When the new RVA receives the forwarded packets, it updates the location to the HCNs RVA's.

It is possible to perform an inter-RVA handover without signalling the RVS. The advantage of this approach is the reduced overhead of the handover, but it requires the RVAs to act as RVSs (forwarding de I1 packet) for every registered HMN. This forms a cascading chain of RVSs that could be desirable if the geographical area covered by one RVA is considerably big. This matter requires further study.

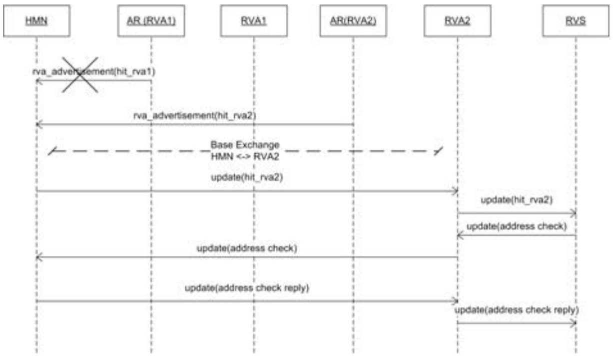

Fig. 7 - Inter RVA Handover

F. RVA to RVA Update

When the new RVA receives the forwarded packets from another RVA, it updates the location to the HCNs RVA's. The forwarded packets need to be differentiated from the normal traffic, allowing a RVA to decide when mobility updates are needed or not.

G. Packet Forwarding

For packet forwarding, the RVAs use the same mechanisms already described for base exchange and update packets. The RVAs perform the required readdressing, concealing the globally routable IP addresses assigned to the HIP nodes from RVA protected areas. In the RVA protected areas, the transport mechanism defined, based on HITs, is used to deliver the packets to the destination.

VI. AN EXAMPLE IPV6 INSTANCIATION

The framework definition, as it exists in [16], does not make assumptions on packet relaying mechanisms within the RVA protected area. Only IPv6 is assumed in the core network. The most logical solution is that the RVA protected area should be an IPv6 Access Network (AN). Communication between nodes within RVA protected area is done by using the HIT's of the attendants in the IPv6 source and destination fields. The main advantage of this solution is that it requires no changes to packet formats since both IPv6 addresses and HIT's are 128 bits long. Also, the routing based on identities is facilitated by using the HIT's as IPv6 addresses, thus enabling the identity based routing, not disclosing any information about the location of the nodes. With the IPv6 access network, deploying the RVA advertisement system consists in enhancing the Router Advertisement [18] messages to carry HIP parameters as options. Just like a HIP parameter, a neighbor discovery option has a type/length/value (TLV) format, allowing a clean integration of the new options. The new HIP parameter - called RVA_INFO - is a TLV that advertises both RVA and AR HITs and the advertisement lifetime.

With the advertisement mechanism in place, the HMN can detect AR's and RVA's. When a HMN first arrives to an AN it acquires both AR and RVA HITs from the newly defined RVA advertisement messages. The registration procedure with the RVA is as described earlier in Section V-A and the RVA assigns a global IPv6 address to the HMN upon registration completion. After these procedures complete, the HMN register with the RVA HIT in the RVS. Detecting Intra-RVA mobility is done by watching the RVA advertisements. When the AR HIT changes then the HMN performs an update to the RVA allowing it to update the routing entry for that particular HMN. The update procedure does not require any extensions to the base draft definition. Inter-RVA mobility is detected when a newly received RVA HIT, from the RVA advertisement messages, differs from the one where the HMN is currently registered. When this occurs, a new registration is performed with the new RVA, as described in Section V-E. Upon registration the HMN updates it's current RVA with the RVS, with a normal HIP Update procedure, but signaling the new RVA HIT. It is important to understand the usage of the IP header, specially the source and destination fields, to fully understand how the IP address are concealed from a RVA protected area. The framework also describes that RVA-to-RVA signalling is required. Since both RVA's have global IPv6 addresses, to communicate between each other they perform a normal HIP Base Exchange, allowing secure communication and authentication. Depending on the required scenario, the trust relation between the RVAs may be different. For instance in a network operator scenario, all RVAs may be certified by a common CA, allowing only trusted RVAs to signal each other. A more flexible solution resides on the HMN giving a certificate to the RVA during the registration process, thus enabling them to prove to each other that they are acting on behalf of the HMN.

VII. CONCLUSION

Our proposed framework is able to conceal the IP address of a HIP Mobile Node from a HIP Correspondent Node and vice-versa, if both are under RVA protected areas. The communication in the RVA protected areas is based on HITs and therefore no locators are necessary. In case the transport in the AN requires locators for routing, the scope of these names are deemed as local and are never leaked outside the AN.

The attacker is only able to learn a HMN's location if it is in the same AN. In this case, the attacker can track HITs, MACs and possibly other AN transport information by simply eavesdropping on the physical medium. We believe that this architecture can be extended or combined with other mechanisms to also cover this case.

The globally assigned IPv6 addresses limits the amount of location information an eavesdropper in the core network obtains from mapping HITs to global addresses used in the routing process. This factor can even be reduced if an encrypted tunnel is used between the different RVAs. If the eavesdropper is on the path and able to intercept all messages received by the HCN outside the HCN's protected area, it does not learn of local mobility and can only track movement between different RVA protected areas. The size of RVA protected areas determines how much geographical location information an attacker can obtain by using this method.

An attacker tracking the base exchange can learn the SPIs of IPsec SAs and afterwards map the SPIs to the assigned IPv6 addresses. Once again, the attacker is limited to the location of the RVAs information and the SPIs used.

REFERENCES

[1] R. Moskowitz, "Host Identity Protocol", Internet Draft (Work in Progress), February 2005.
URL: *http://www.ietf.org/internet-drafts/draft-ietf-hip-base-02.txt*

[2] R. Moskowitz, "Host Identity Protocol Architecture", Internet Draft (Work in Progress), January 2005.
URL: *http://www.ietf.org/internet-drafts/draft-ietf-hip-arch-02.txt*

[3] A. Falk D. Clark, R. Braden and V. Pingali, "Fara: reorganizing addressing architecture", *Proceedings of ACM SIGCOMM workshop on future directions in network architecture*, pp. 313–321, 2003.

[4] W. Haddad, "Privacy for Mobile and Multi-homed Nodes: MoMiPriv Problem Statement", Internet Draft (Work in Progress), February 2005.

[5] W. Haddad, "Privacy for Mobile and Multi-homed Nodes: Formalizing the Threat Model", Internet Draft (Work in Progress), February 2005.

[6] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6", RFC 3775 (Proposed Standard), June 2004.
URL: *http://www.ietf.org/rfc/rfc3775.txt*

[7] T. Okagawa, M. Jo, K. Nishida, and A. Miura, "Ip packet routing mechanism based on mobility management in a ip based network", *8th International Conference on Intelligence in next generation networks*, 2003.

[8] M. Brunner S. Schmid, L. Eggert and J. Quittek, "Turfnet: An Architecture for dynamically composable networks", *Proceedings in*

1st IFIP TC6 WG6.6 Workshop on Autonomic Communication (WAC 2004), 2004.

[9] I. Stoica, D. Adkins, S. Zhuang, S. Shenker, and S. Surana, "Internet indirection infrastructure", *Proceedings in ACM SIGCOMM Conference (SIGCOMM'02)*, pp. 73–88, August 2002.

[10] H. Soliman, C. Castellucia, K. El Malki, and L. Ballier, "Mobility Support in IPv6", RFC 4140 (Proposed Standard), June 2004.
URL: *http://www.ietf.org/rfc/rfc4140.txt*

[11] N. Mathewson R. Dingledine and P. Syverson, "TOR: The second-generation onion router", *Proceedings of 13th USENIX Security Symposyum*, 2004.

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

[13] P. Nikander, "End-Host Mobility and Multi-Homing with Host Identity Protocol", Internet Draft (Work in Progress), February 2005.
URL: *http://www.ietf.org/internet-drafts/draft-ietf-hip-mm-01.txt*

[14] J. Laganier and L. Eggert, "Host Identity Protocol (HIP) Rendezvous Extensions", Internet Draft (Work in Progress), February 2005.
URL: *http://www.ietf.org/internet-drafts/draft-ietf-hip-rvs-01.txt*

[15] L. Eggert and M. Liebsch, "Host Identity Protocol (HIP) Rendezvous Mechanisms", Internet Draft (Work in Progress), July 2004.

[16] A. Matos, "Host Identity Protocol Location Privacy Extensions", Internet Draft (Work in Progress), June 2005.
URL: *http://tools.ietf.org/wg/hip/draft-matos-hip-privacy-extensions-00.txt*

[17] T. Koponen and L. Eggert, "Host Identity Protocol (HIP) Registration Extension", Internet Draft (Work in Progress), February 2005.
URL: *http://www.ietf.org/internet-drafts/draft-koponen-hip-registration-00.txt*

[18] W. Simpson T. Narten, E. Nordmark, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.