# Mobility and Multihoming Solutions with Host Identity Layer - Introduction and Comparison

Essi Vehmersalo
Helsinki University of Technology
Telecommunications Software and Multimedia Laboratory
Internetworking Seminar Course
Essi.Vehmersalo@hut.fi

## Abstract

Mobility and multihoming (or multiaddressing) are becoming more and more common in the Internet. Still one of the most problematic issues is the relation between locations and identities of mobile hosts. Currently the IP address is used to represent both; end-point in the transport layer connections and location for routing in the network level. This paper discusses the need for separating the concepts of location and identity and evaluates proposed solutions for that. The proposals define an intermediate host identity sublayer between the existing network and transport layers, for separating identifiers and locators and for providing mapping between them. KEYWORDS: Mobility, Multihoming, HIP,

LIN6, MAST

## 1 Introduction

The fundamental purpose of organising networking as a protocol stack is to separate functionalities and related data and therefore make the architecture more modular and accessible. Still, probably the most common example of shared data between two layers is the IP address used also by the transport layer protocols. The IP address has also been considered a static identification of a host, eventhough it is very often dynamically allocated and dependent on location in the network topology, something that hosts increasingly are not. As pointed out by Saltzer [16], there is an ambiguity of network objects and their locations, more generally refering to service and node providing it, node and its network attachment point, network attachment point and the route to get to it. In the past this may have been an efficient choice of not making things more complicated than the current environment requires. However, in the current circumstances, as the locations of hosts change but transport connection end points should not, it makes continuous transport connections problematic. After all, as defined by Abley et al. [1] one of the objectives of multihoming solutions, is keeping the transport level connections intact during address changes.

This fundamental IP mobility problem is also considered by Bhagwat et al. [2] noting that the IP address actually has two meanings. On network level, it identifies a location on the network topology but transport layer protocols use it to identify a host. In effect, mobility could be coped either by explicitly changing IP addresses or by virtually preserving addresses and using forwarding mechanisms to deliver packets to mobile hosts, which was the approach chosen by [2]. The first approach would essentially redefine IP address as only a location and as layers above network layer could no longer rely on a simple IP address as a host identifier, possibly encourage steering the architecture towards removing this inter-layer dependency.

The second approach would be concealing the change of location, as the current Mobile IP does. This way an IP address, or *home address*, in this case actually is bound to a certain node and the network layer sees to it that the traffic for this mobile endpoint is routed to the actual IP address or *care-of-address*. The problem here is that the inter-layer dependency remains but information an IP address would provide to the transport layer is taken away. Furthermore, as pointed out by Clark et al. [3], binding location identifiers to moving entities is a fundamental problem, since the very purpose of IP addresses is to present hierarchical location information in the network topology. After all, effective routing is based on the hierarchy of networks and their addresses.

### 1.1 Internet Mobility Currently - Mobile IP

Mobile IP is the currently proposed solution for mobility handling in IP networks. It is based on the use of *home address* and using a *home agent* to forward traffic to the temporary *care-of-address* the mobile node has. The functionality can be made more effective by using IP-in-IP encapsulation to tunnel traffic directly from corresponding node (CN) to mobile node (MN) in its current location. In any case, despite location, the home address is used to refer the mobile node. The problem is that the forwarding mode of operation is simply ineffective and in a sense creates a separate deviating model of routing in the network layer on top of the IP routing logic. As pointed out by Crocker [4], also with the tunneling mode there exists a conceptual anomaly as an IP address expressing location is used to refer to location it does not actually represent. From the point of view of the transport layer protocols, this creates an illusion that the location of other end-point could be deduced from the available home address. Therefore, some transport layer functionalities monitoring the path qualities to the other end-point (such as the congestion control mechanisms) will be fooled into believing that the static home address actually provides topological information.

The strong dependence on home address may also be difficult when anticipating the future needs for networking capabilities [10]; The new embedded mobile devices are becoming more and more common and even the currently known devices are becoming increasingly more mobile. Therefore, it is questionable whether specific home network can be defined for all of them or if defining an artificial home network, more importantly, makes sense in this environment, as noted by Nikander [10]. Furthermore, Mobile IP does not enable the use of multiple care-of-addresses simultaneously wich would be necessary to support multihoming.

Altogether, it seems to be a commonly shared view of several writers that mobility and multihoming are not treated as an integral part of network environment even in the upcoming IPv6 architecture, which had the chance of renewing the network architecture along with solving the current problems. The Mobile IP seems to be designed as an add-on to the existing architecture that would cover up mobility and keep up the impression of a static networking setting. These shortcomings were noticed by some already in the early days of IPv6 as presented in coming chapters.

## 1.2 Host Identity Sublayer and Separating Locators and Identifiers

In general, multiaddressing enabling proposals have been presented for several parts in the IP layering. The common thing for the proposals covered in this paper is that instead of using directly any of the existing layers, a new layer or a sublayer would be created between network and transport layers. In essence, the function of the new layer is to separate the concepts of location and identity of a network entity to eliminate the interlayer dependence.

Another viable solution might be the mobility-aware transport level protocols that are able to handle multiple endpoint identifiers simultaneously. However, these solutions also have security problems, inherently relating to not having a specific identifiable end-point to bind the connections, as noted by Ohta [15].

Adding a new layer to the well-established TCP/IP stack appears as rather bold proposition. However, as pointed out in previous chapters, there are fundamental shortcomings in the way the existing architecture serves the current and emerging needs of networking. Furthermore, separating a new concept, the end-point identifier, that is mapped to the lower network layer identifiers and used by the upper transport layer, calls for an additional layer of abstraction.

In general, a characteristic feature of the sublayer is that it can not be completely defined as part of neither, the network layer or the transport layer. Architecturally there is quite clear functional distinction between network and transport layers. The transport layer is the lowest layer with end-to-end communication, where as network layer to an extent operates between intermediate nodes as it routes packets towards the destination. The host identity sublayer is conceptually a component of network layer that maps the upper layer identifiers to network layer IP addresses. It also creates an abstraction to the above transport layer that enables it to refer the other end-point with the end-point identifier. Still, with many proposals the sublayer includes some end-to-end signaling to update current valid addresses and therefore also has transport layer characteristics.

What would then be the offerings of the host identity sublayer to the existing architecture? From the point of view of the network layer, it takes of the burden of twisting routing or forwarding mechanisms to manage mobility in a way that is invisible to the layer above it. To the transport layer it would offer an identifier truly representing the other endpoint that transport associations need to be bound. Also as the meaning of security, both for inner workings of protocols as well as protecting the user payload data, increases there needs to be a definite instance to which the security associations can be bound. As pointed out by Ylitalo et al. [19] especially the security associations as well as transport level connections should be bound to actual identifiers. Introducing explicit host identifier does finally remove the topological information from transport level identifiers. As pointed out with Mobile IP, the same problems of for example congestion control exist here. However, what a host identifier can accomplish is to eliminate the confusion between IP addresses that represent location of a node and addresses that represent the identity.

## 1.3 Security Problems with Mobility and Multihoming

Besides the general security risks in the current network infrastructure, there are some security vulnerabilities caused inherently by mobility and multihoming. As location updates must be an essential part of mobile communication, the problems relate to verifying that the host claiming to be reachable at some address is indeed the host claimed and is indeed at the address claimed. The introduction of these problems is based on [12] by Nikander et al.

The first issue, *address stealing*, is caused when a malicious host sends a false location update to a communicating peer to redirect the traffic to an address, where the true communicating host is not reachable. The attack may be used as denial-of-service or man-in-the-middle attack. The defense would be proper authentication of the location update messaging to ensure that the host sending the location update is actually the host claimed. Most proposals for mobility solutions do consider this problem by using for example IPSec, but the initial establishing of the security associations is not always fully covered. Address stealing attack is presented in (Fig. 1).

The other way around, the problem may be ensuring that location update coming from the verified other end-point is actually true. In the case of *address flooding*, the malicious host does not claim to be someone else, but somewhere else and by redirecting possibly a considerable amount of traffic to some address tries to cause an address flooding attack. Because of this, it should be first made sure that the other host is actually reachable at the address claimed before fully redirecting the traffic to that address. With reachability checking the problem of IP spoofing may still remain if the malicious host can still intercept the reachability messages and further answer to them supposedly from the checked address. Address flooding attack is presented in (Fig. 2).

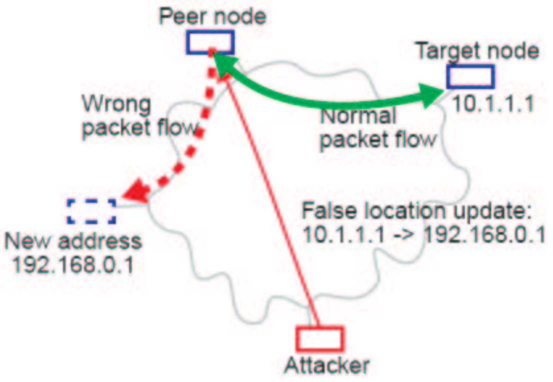

Figure 1: "Address stealing attack. The peer believes that 10.1.1.1 is now at 192.168.0.1". Figure borrowed from [12]

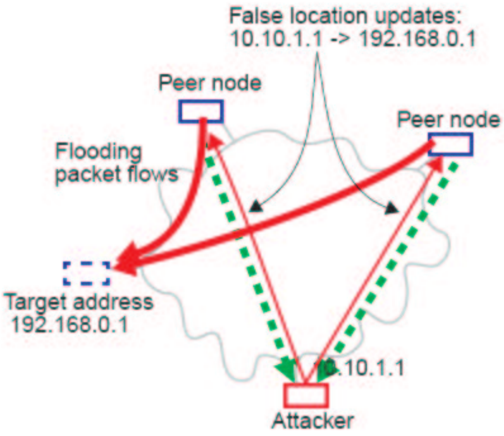
False location updates: 10.10.1.1 -> 192.168.0.1
Peer node
Peer node
Flooding packet flows
Target address 192.168.0.1
10.10.1.1
Attacker

Figure 2: "Address flooding attack". Figure borrowed from [12]

# 2 Host Identity Layer Solutions

This section presents proposals that define some form of sublayer between transport layer and network layer for enabling mobility and multihoming. The sublayer is here generally called host identity sublayer, but each proposal seems to have its own terminology.

## 2.1 Earlier Proposals

The idea of separating identifiers from locators has come up already at the time the new IPv6 protocol was being developed. Already then some people felt that mobility should be considered more carefully in the new protocol and not implemented as an add-on to the architecture. Also separating the concept of host location and host identifier was not only noticed, but actually proposed. One example of this is presented in the next chapter.

### 2.1.1 Virtual Internet Protocol (VIP)

Virtual Internet Protocol (VIP) was proposed by Teraoka et al. [18] already when the IPv6 was being developed. It suggested that the problematic binding between locators and identifiers of host should be eliminated so that transport and higher layers could refer to end-points with an immutable identifier. The address resolution by identifiers should exist in a sublayer of network layer. The entire model seems quite similar to the newer proposals made almost ten years later, as can be seen from following chapters. Only the location update mechanisms of VIP are more modest and bit more unorganized. Only the home network and the previous network are explicitly informed of location change. Still any node has an own Address Mapping Table and may update its bindings when information of a new binding happens to be available. VIP also includes some consideration of security, but the solutions for authentication are somewhat incomplete and at very least poorly scalable.

## 2.2 Host Identity Payload and Protocol (HIP)

Host Identity Payload and Protocol (HIP) proposes a solution with a new name space of Host Identifiers (HI) that can be dynamically bound to IP addresses to enable mobility and multihoming. The distinct feature of HIP is the cryptographical nature of Host Identifier, which makes the security tightly embedded into the solution. This HIP introduction is based on [8] and [9] by Moskowitz and [12] and [11] by Nikander et al.

### 2.2.1 Host Identifier HI

The basis of HIP is the separation of host identity from host location so that a network host could be referred independent of its current location. A new Host Identity Layer takes care of mapping the HI to current valid IP address. Furthermore, the host identifier is the public key of a public-private key pair associated to the host. This way not only the security associations can be automatically bound to a static host identifier, but the establishing of security associations is done based on the existing public keys. This eliminates the verification of the identity public key binding that would otherwise require a complicated and poorly scalable Public Key Infrastructure (PKI). Host Identifier can also be used to create IPv6 address compatible host Identity Tag (HIT) by applying a hash function to the Host Identifier. Therefore, HIT can be used by upper layer protocols along with common IPv6 addresses.

### 2.2.2 Architecture

HIP defines the Host Layer Protocol (HLP) to be used between the end-points for signalling location updates and other information about current available addresses. With the initial handshake, also mutual authentication and IPSec security association are established for further communication of payload data as well as signalling messages. For initial host discovery, HIP uses a directory service such as DNS to locate a specific *rendezvous server* that is then used to forward the initial packet to its destination. HIP operation also considers the double-jump situation by defining packet forwarding agent. In double-jump problem, both end-points move simultaneously and miss each other's location updates. In case of this, a host can ask the packet forwarding agent to present a virtual interface of the host, by forwarding the packets sent to the old address to the host's current location. For the packet forwarding it is essential that the forwarding agent knows that the host indeed has been assigned the address in question or that the address is available to be assigned to the host. In practise packet forwarding may be done by a network access router or by a node acting as a virtual access router, used especially for forwarding purposes.

The reachability or return routability is also considered with normal location updates as well as with packet forwarding and the host of forwarding agent must first check the reachability before using the address. Another security consideration is the privacy of hosts, which might be problematic in an environment with explicit globally unique identities of hosts. HIP provides anonymity for hosts with the possibility of having more than one Host Identifier associated with the host. This way some HIs can be used as temporary identifiers.

## 2.3 Location Independent Network Architecture (LINA) and LIN6

Location Independent Network Architecture (LINA) is yet another proposal to solve mobility and multihoming problems by separating the host identifier from the network interface location. LINA has been adapted to IPv6 with a protocol specification called LIN6. LIN6 is presented in the following chapters based on LIN6 proposals by Teraoka et al. [17], Kunishi et al. [7] and Ishiyama et al. [6].

### 2.3.1 Addressing

With LIN6, a specific unique *LIN6 ID* is used to identify a mobile node, which can be used by layers above network layer to refer to a node instead of a network attachment point. As the IPv6 addresses currently use the Aggregateable Global Unicast Address (AGUA) format, where the address is basically divided into 64 bit network prefix and 64 bit host part, the LIN6 addressing conforms to this by having the 64 bit LIN6 ID that can be embedded into IPv6 address. This way the host part of the IPv6 address is replaced with the LIN6 ID to form a *LIN6 address*, which must be also recognized by the node's network interface. Forming of LIN6 address is presented in (Fig. 3). In addition, a *generalized identifier* can be formed by combining a fixed value *dedicated locator*, as the network part, with LIN6 ID. This generalized identifier is particularly the address that transport and application layers can use as an immutable node identifier, but which still follows the regular IPv6 address format. This provides backward compatibility with the existing IPv6 implementation and this way the transport and application layers are also able to use the actual interface locator for communication.

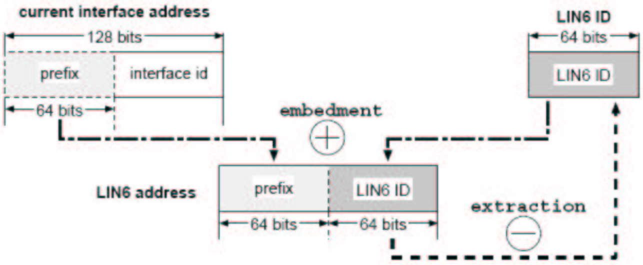

Figure 3: LIN6 address format. Figure borrowed from [6]

### 2.3.2 Architecture

The network layer is in LIN6 divided into two sublayers; *Identification sublayer*, which performs the mapping from node identifier to locator and the other way around and the *Delivering sublayer*, which performs the traditional packet forwarding functions of network layer. The mapping in identification sublayer is done by extracting the LIN6 ID of the generalized address and fetching the current valid interface address of the node from mapping table. After the mapping, the LIN6 ID is again embedded into the IPv6 address to form the LIN6 address. The mapping is obviously not done if the address does not have the LIN6 dedicated locator and is already an interface address. A reverse procedure that creates a LIN6 generalized ID out of the LIN6 address is done with received packets.

LIN6 uses DNS and Mapping Agents (MA) for initial host discovery. A DNS query is used to find out the dedicated MAs of a node with a certain generalized LIN6 address. These MAs hold the current address of the node at each time and are registered to DNS. Because the use of DNS the nature of node MAs binding is intended to be relatively static, but basing the solution to already globally functional DNS system also makes it more scalable. To acquire the actual current interface address of a node one of the MAs must be then queried. The binding of node to current address in MAs is maintained by *mapping updates* sent by the mobile node. As the mapping updates are also sent to corresponding nodes that the mobile node is communicating with, the communication can be kept up as the node moves.

## 2.4 Multiple Address Service for Transport (MAST)

Multiple Address Service for Transport (MAST) is a proposal partially based on HIP and LIN6, but still presents slightly different approach. It avoids creating new namespace, but defines a layer between network and transport layers that hides the multiple locations (IP addresses) from the transport layer. In fact MAST accomplishes roughly the same functionality as LIN6 and HIP, but using the existing IP addresses. It only maps different IP addresses to a single IP address that may be initially visible to the transport layer. The introduction of MAST is based on MAST proposal by Crocker [5]

#### 2.4.1 Operation

MAST functionality is based on *MAST association* that is maintained with simple request/response messaging. Messages are used to initially establish the MAST association, to update the set of valid IP addresses, query association status, convey error information and to terminate the association. MAST reliability is based on response messages and retransmission of the requests, when necessary. The association information, shared between the hosts, consists of endpoint identifiers (domain names) for both hosts, endpoint association label and sequence label used as sequence number for detecting missing, duplicate data and correlating responses. MAST exchange may be initiated both before and during an existing transport association. When initiated during transport association, the address initially visible to transport layer must continue to be visible to transport layer and all other addresses are mapped to that address.

The initial rendezvous is accomplished in the same manner as with LIN6 and HIP. DNS is used to provide the information of dynamic presence service relating to a specific mobile host. The DNS lookup is done by the domain name of the host. As with the other solutions, the mobile host registers its current address with dynamic presence service, which in the case of MAST is defined to be The Extensible Messaging and Presence Protocol (XMPP).

#### 2.4.2 Security Considerations

Plain MAST would be quite vulnerable to, for example, spoofing and redirection attacks, so the messaging must be done in more secure manner. MAST suggests exchange of protection keys in the beginning of the association, before any address updates occur. In addition, use of IPSec or TLS is suggested, when more stronger protection is needed. In essence, MAST may be no worse than the current generally used level of security, but it does not increase the security either.

### 2.5 Site Multihoming Solutions

This chapter presents two proposals that are closely related and architecturally quite similar to previously presented host identity sublayer proposals. They have however different and more limited goals as they only provide solution to infrequent site multihoming.

#### 2.5.1 Strong Identity Multihoming (SIB)

Strong Identity Multihoming (SIB) is proposed by Nordmark [14]. SIB presents a solution for multihoming where a special M6 layer is inserted between IP and transport layers to hide the change of IP locator from the transport layer protocol. The solution uses a three-way handshake to create a host-pair context in the M6 layer in the both end-points upon establishing the transport connection. As with previously presented solutions, M6 sublayer with the host-pair context is used to keep up a state and to convert end-point identifiers used with transport layer protocols to IP addresses marking location. In addition, SIB uses Cryptographically-based Identifiers that are hashes produced from public keys of public-private key pairs. This is the same approach as with HIP and provides much the same advantages as HIP.

What clearly differs from other proposals is the location updating between the communicating end-points. No explicit location updates are used, but with each received packet, the recipient registers the used address as the one preferred (possibly among other possible addresses). In addition, border routers may rewrite the source addresses of some out-bound packets. This is done to convey information about the prefered address of the network to peers of communicating hosts inside the site. When receiving these packets, the recipient will take note of that address as the preferred one.

#### 2.5.2 Multihoming without IP Identifiers

Multihoming without IP identifiers is very similar solution to SIB also proposed by Nordmark [13]. Multihoming without IP Identifiers has the same M6 layer that it uses to establish the host-pair context.

As opposed to SIB, the transport layer identifier is one of the valid IP addresses, which is a similar solution as MAST. For verification of the valid end-point addresses Multihoming without IP identifiers uses DNS lookups.

Both solutions, SIB and Multihoming without IP Identifiers, rely heavily on use of DNS for destination discovery and Multihoming without IP Identifiers also uses DNS with verification of each end-point address. As also defined in the proposals, the scope covers only cases where address changes are infrequent enough to be manageable with DNS.

## 3 Comparison and analysis

This chapter evaluates the different proposals for mobility and multihoming. HIP, MAST and LIN6 are refered as the three main proposals. The site multihoming solutions are also considered, but not as thoroughly as they clearly address a slightly different problem than the main proposals.

### 3.1 Architecture and Operation

The central concept in all of these solutions is identifying hosts independent of their location. Therefore one significant architectural choice is whether there should be a new name space for host identifiers. Explicitly defining a new identifier might make the network architecture more complex and of course bringing a completely new component to a system may in general cause unanticipated complications. Therefore, a solution like MAST could be considered more easily approachable. However, the host identifier is not entirely new concept, but one that has been previously modelled with IP address, which in turn has had a duplicate meaning. Having an explicit host identifier is not just logically more pleasing solution, but also reflects the real world more accurately. In general, a big problem with the current Internet is that things, such as IP addresses, are not always what they appear to be. Therefore creating an explicit identifier for end-point might provide something to bind the much needed security associations as well as transport level connection.

Another issue is how the allocation of the identifiers is done and in what scope the identifiers need to be unique. MAST of course uses the already allocated and managed IP addresses. With LIN6 the LIN6 generalized ID needs to be unique in order for DNS to be able to provide mapping between the LIN6 generalized ID and the mapping agents associated with the host. This would require some form of organized allocation of the 64 bit LIN6 IDs. Also HIP Host Identity Tags should be unique. HIP, however, provides a way to delegate the address allocation, as the different types of HITs are marked with the first two bits of the HIT. The first 62 bits of the HIT can be used to express two levels of delegation. On the other hand also the collision propabilities of the 128 bit hash are very small even with relatively big number of hosts. HIP therefore seems to provide more easily approachable methods of host identifier allocation as also pointed out by Moskowitz [8]. Furthermore HIP host identifier inherently provides the proof that the instance using the identifier is entitled to doing so. With MAST and LIN6 there needs to be an additional method to authenticate an instance to prevent a kind of host identifier spoofing.

From the point of view of the transport layer the presentation of the host identifiers is also quite significant. As proposals operate in the current environment, one especially problematic issue may be that in some cases the transport layer protocols are not able to tell if the identifier they are using describes a location or host identity. With LIN6 host identifiers always have the dedicated locator as the network prefix and with HIP the firs bits of the Host Identity Tag can also be used to mark the IPv6 address. However, with MAST, the end-point identifiers actually are IP address.

### 3.1.1 Scope of Solution

The scope of solutions also varies. Some proposals set out to solve only site multihoming, some concentrate only on hosts. There are also differences in how frequent changes in addresses solutions are prepared to handle. However it is essential that a new host identity sublayer and possibly new namespace of identifiers will not be introduced just because of one specific case of the problem. The solution must be able to cover as many of the foreseeable needs concerning multiaddressing as possible. Solutions such as SIB and Multihoming without IP identifiers are greatly limited by the time DNS data takes to propagate and thus would not be suitable for host mobility. Then again, as the major site rehoming problem is the ownership of IP addresses, MAST, which uses an ordinary IP address as host identifier could hardly solve that problem. Still even though HIP and LIN6 are focused on host mobility and multihoming, they should be able to be usable also with site address changes, at least to ensure the transport level connection survivability.

## 3.2 Ease of Adoption

One crucial thing with new network technologies is how much effort is required to adopt the technology. Naturally, bigger changes to current infrastructure also require more work to adopt. In addition, the solution must be backward compatible with the existing technologies so that it can be taken into use gradually. With all the main solutions, IPv6 addresses may be used by the applications and transport level protocols side by side with the new identifiers. In addition, all of them implement the required changes in the end systems and the IP routing system is not affected by the solutions. Keeping the complexity in the end systems is essential in keeping the entire networking architecture modular and clear. With this in mind, the site multihoming solutions, with address rewriting at border routers, seem to put more burden on the routers than would be necessary.

Another important issue are the possible new network components or services the solutions require or additional requirements they pose on existing network services. All the main solutions use DNS in the process of initial host discovery, which does not require too much additional effort. DNS is already used and available globally and proved to be relatively established solution. The limitations of DNS have also been taken into account by all main proposals. All of them also require an additional rendezvous entity that provides the current address of the host or as with HIP, forwards the initial packet to the host. This should not be unreasonable demand, since rendezvous service, staticly related to a host, can be organized with some administrative work. In addition to static rendezvous server, HIP also includes forwarding agents that can be dynamically taken into use. It should be expected that especially in the early stages of possible adoption this might not be available in all networks. However, the forwarding agent is only necessary in case of so-called double jump situation and then again HIP seems to be the only solution to consider this problem.

## 3.3 Security

All of the main solutions take security into account, as they should. Still HIP (and SIB) with the direct use of a public key to represent the identity of a host positively stand out. This way, external security mechanisms are not just used to protect the solution, but the solution actually becomes part of the public key cryptography system that can be used to protect network traffic. As the PKI systems often are difficult to manage and very poorly scalable HIP might prove to be useful already because it to some extent eliminates the need for external PKI.

In addition, essential security problems for these solutions are the address stealing and address flooding problems presented earlier. All of the solutions must, by their very nature, include some location update mechanisms and therefore need some forms of protection agains those problems. The verification of the host in location updates seems to be taken into account in all the main proposals. Some mechanism is used or is available for use in all solutions. Still the initial establishment of the security context is likely to be the weak point of LIN6 and MAST. However, with LIN6 also choices of the level of security used are available, which gives a change for more lightweight use of the technology. The return routability for preventing address flooding attacks seems to be explicitly considered only with HIP. Still a similar mechanism of reachability checking as used with HIP could be easily added to LIN6 and MAST as well since they already have the authentication mechanisms necessary for challenge-response functionality.

# 4 Future challenges

This paper has mostly analysed the suitability of host identity model in the context of the central TCP/IP architecture. Still the purpose of the entire protocol stack is however to provide service to the upper most layer, the applications. One of the most visible changes between mobile and static environment will be the varying and at times non-existent quality of service. Previously the applications could assume some reasonable level and even more so assume the continuation of service. The applications adapted to the mobile world need to have some guarantees of the quality and continuation of the service, or more realistically means to receive information about those things and built-in mechanisms to adapt to them.

Furthermore, as noted before the host identity model would deprive the transport layer of the topological information of the connection end-points. Currently for example TCP optimizes its operation based on the path qualities it deduces from how the network seems to be working at that time. If the mobility would be handled with a mobility-aware transport protocol that could handle multiple end-point addresses, the protocol would receive quite a lot of information just by observing the changes in, and maybe also occasional lack of, end-point identifiers.

However, the path between end-point is hardly defined by only the locations of its end-points. Especially in dynamic world of future, where not only processes and hosts, but also entire networks may be mobile and have multiple simultaneous access points. Also, as a single host may constantly have available multiple network access points with different costs and qualities of service, the currently used access may want to chosen to optimize cost or available bandwidth. In this case, the mere IP address will not convey much information about the qualities of the connection medium.

Therefore, in the future there needs to be some efficient way to relay information about availble quality of service, available network acceess points and their qualities.

# 5 Conclusions

There appears to be obvious problems with the way an end-point is currently represented in the mobile networking environment. Using IP address for this purpose seems to have negative effects on both the transport level functions as well as the network level functions. Therefore there should be a clear distiction between the identifiers of these two layers. This distinction could be provided by an intermediate layer of abstraction that would provide mapping between the identifiers of the two layers.

The paper presented different proposed solutions as host identity layer architectures. One of the most significant differences in approaches was whether a new end-point identifier namespace should be created, as HIP and LIN6 suggest. Creating a new end-point identifier does however have advantages not only as a mobility enabling technique, but as more profound security solution, as seen from HIP.

Some of the different qualities of the proposals were also compared. The three main proposals HIP, LIN6 and MAST are architecturally and functionally relatively similar. However, the cryptographic nature of the HIP host identifier distiguishes it from the others as it may provide solutions to not just mobility, but also network security.

# References

[1] J. Abley, B. Blac, and V. Gill. Goals for ipv6 site-multihoming architectures. RFC 3582, IETF, August 2003.

[2] P. Bhagwat, C. Perkins, and S. Tripathi. Network layer mobility: an architecture and survey. *Personal Communications, IEEE*, 3:54–64, June 1996.

[3] D. Clark, K. Sollins, J. Wroclawski, and T. Faber. Addressing reality: An architectural response to real-world demands on the evolving internet. In *ACM SIGCOMM 2003 FDNA Workshop*, August 2003.

[4] D. Crocker. Choices for multiaddressing. Internet draft draft-crocker-mast-analysis-01.txt, IETF, October 2003.

[5] D. Crocker. MULTIPLE ADDRESS SERVICE FOR TRANSPORT (MAST): AN EXTENDED PROPOSAL. Internet draft draft-crocker-mast-proposal-01.txt, IETF, September 2003.

[6] M. Ishiyama, M. Kunishi, and F. Teraoka. An analysis of mobility handling in LIN6. In *International Symposium on Wireless Personal Multimedia Communication*, 2001.

[7] M. Kunishi, M. Ishiyama, K. Uehara, HiroshiEsaki, and F. Teraoka. LIN6: A new approach to mobility support in IPv6. In *International Symposium on Wireless Personal Multimedia Communication*, 2000.

[8] R. Moskowitz. Host identity payload and protocol. Internet draft draft-moskowitz-hip-05.txt, IETF, October 2001.

[9] R. Moskowitz. Host identity payload architecture. Internet draft draft-moskowitz-hip-arch-02.txt, IETF, February 2001.

[10] P. Nikander. TCP and UDP in the mobile world, or what is wrong with mobile IP version 6, and how to fix it. In *Proceedings of NordU'2001*, Stockholm, Sweden, February 2001.

[11] P. Nikander and J. Arkko. End-host mobility and multihoming with host identity protocol. Internet draft draft-nikander-hip-mm-01.txt, Ericsson Research Nomadic Lab, December 2003.

[12] P. Nikander, J. Ylitalo, and J. Wall. Integrating security, mobility, and multi-homing in a hip way. In *Proceedings of Network and Distributed Systems Security Symposium (NDSS'03)*, pages 87–99. Ericsson Research NomadicLab, February 2003.

[13] E. Nordmark. Multihoming without IP identifiers. Internet draft draft-nordmark-multi6-noid-01.txt, Sun Microsystems, October 2003.

[14] E. Nordmark. Strong identity multihoming using 128 bit identifiers (SIM/CBID128). Internet draft draft-nordmark-multi6-sim-01.txt, Sun Microsystems, October 2003.

[15] M. Ohta. Threats relating to transport layer protocols handling multiple addresses. Internet draft draft-ohta-multi6-threats-00.txt, IETF, February 2004.

[16] J. Saltzer. On the naming and binding of network destinations. RFC 1498, IETF, ftp://ftp.rfc-editor.org/in-notes/rfc1498.txt, 1993.

[17] F. Teraoka, M. Ishiyama, and M. Kunishi. LIN6: A solution to multihoming and mobility in IPv6. Internet draft draft-teraoka-multi6-lin6-00.txt, IETF, January 2004.

[18] F. Teraoka, K. Uehara, H. Sunahara, and J. Murai. VIP: a protocol providing host mobility. *Communications of the ACM*, 37, August 1994.

[19] J. Ylitalo, P. Jokela, J. Wall, and P. Nikander. End-point identifiers in secure multi-homed mobility. In *Proceedings of OPODIS'02*, pages 17–28, Reims, France, December 2002. Universite de Reims Champagne-Ardenne.