INVITED PAPER *Special Section on Technologies and Architectures for Improving Scalability, Reliability, and Robustness for Future Information Networks*

Empowering Security and Mobility in Future Networks with an Identity-Based Control Plane

Pedro MARTINEZ-JULIA[†a)] ***and*** **Antonio F. SKARMETA**[†]**,** ***Nonmembers***

SUMMARY Current network technologies, mainly represented by the Internet, have demonstrated little capacity to evolve because of the strict binding of communications to identifiers and locators. While locator namespaces represent the position of communication participants in the graph of a specific protocol, unstructured/plain identifiers represent the position of communications participants in the global network graph. Although they are valid for forwarding packets along communication paths, both views fail to fully represent the actual entities behind communications beyond a simple vertex. In this paper we introduce and evaluate an identity-based control plane that resolves these problems by abstracting communications from identifiers and locators and by using identities to achieve enhanced security, and mobility management operations. This identity-based control plane can then be integrated into different network architectures in order to incorporate the features it provides. This facilitates the evolution capacity of those architectures that separate the information transmission concerns (networking, routing), from end-to-end aspects like security and mobility management.

key words: *future network, identity, overlay, security, mobility*

1. Introduction

The Internet has become the central infrastructure that supports our day-to-day communications, the virtual place where we meet, and the bottleneck of our digital lives. More and more devices and objects of many kinds (things) are connected to the Internet. But the original design of the Internet did not contemplate this evolution, so several problems have arisen, both at networking and internetworking levels [1]. These problems are becoming even worse with the current explosion of mobile devices and newly required functionality, as these represent the critical mass of current and future networks.

A new and huge area of services, devices, and information has exposed many flaws of the original design of the Internet. In this paper we focus on security and mobility management issues because, among other flaws, the need for comprehensive security and integrated mobility management are essential for the Future Internet (FI). It is widely accepted that one of the key problems found in the design of the current Internet is that networked entities are treated just as *hosts*, which are identified and located by network addresses that change with the point of attachment of those entities to the network.

Manuscript received April 3, 2014.
Manuscript revised July 10, 2014.

[†]The authors are with the Department of Communication and Information Engineering, University of Murcia, 30100, Murcia, Spain.
a) E-mail: pedromj@um.es

DOI: 10.1587/transcom.E97.B.2571

The direct answer from the research community to overcome these problems has been to separate identifiers and locators [2] (widely called locator/identifier separation). But this scheme is not complete enough to cover the requirements to support mobile elements in the same way static elements (hosts) are supported.

Another problem is that current mobility management schemes do not offer enough protection of security and privacy. When a device moves from one network to another (handover), its security and privacy contexts should be maintained regardless of the place, location, or point of attachment to the network. Moreover, security and privacy contexts should be transparently preserved during the handover process, so when an entity moves from one network to another, some infrastructure element should be in charge to maintain its security and privacy, and this element should be trusted. Moving entities will change their properties dynamically, so their virtual identities change.

Apart from the context, when devices can move from network to network it is hard to unequivocally identify them or the entities they represent (persons, services, etc.). As we advanced in previous work [3]–[5], we propose to use digital identities to represent the entities behind communications to identify them securely and privately. As defined by ITU-T X.1250 [6], an identity is a collection of attributes about an entity. Here, entities can be people, software (services), hardware (machines), things, etc. Thus, identities can act as communication endpoints, like when a person *talks* to a service.

Therefore, the need for preserving security and privacy contexts and their application regardless of the location, together with the secure identification of network entities, has led us to design a control plane that offers enhanced security and mobility management functions for other underlying network architectures to permit their entities to communicate in an *identity-to-identity* manner. Mapping identity attributes among entities and applying them to different security contexts is a complex problem we aim to resolve by means of a network model based on an overlay network that also builds a Distributed Hash Table (DHT) using a variation of the Kademlia [7] overlay routing algorithm.

In summary, the approach we propose provides three main innovations not present in current security and mobility management solutions. First, the management of identity information makes extensive use of ontologies and semantic techniques to allow entities to be represented in a natural way. This facilitates retaining strong security and mobility

management schemes. Second, using *Bloom Filters* [8] to translate identities (attribute sets) into identifiers for referencing identities along the overlay network provides a feasible and efficient mechanism. Third, our approach integrates the functions in a control plane that will be attached to the network layer of other network architectures, so benefiting the separation of concerns and allowing those architectures to evolve, while keeping backwards compatibility.

To demonstrate our claims, we have analyzed the proposed approach from three different views. We have compared it to a well-known protocol with similar capabilities to our proposal, demonstrating the key differences. We have also performed a security analysis to demonstrate that the proposed mobility management protocol is secure. Finally, we have performed a detailed performance analysis by modeling our mobility management approach and weighing it against well-known identifier/locator separation protocols and by executing extensive experiments with the identity lookup mechanism used by our overlay network. Thus we have obtained strong evidence for its feasibility and for the assertions above.

The remainder of this paper is organized as follows. First, in Sect. 2 we discuss the related work regarding locator/identifier separation. Then, in Sect. 3 we describe the details of the identity-based control plane and how it can be used to achieve the objectives discussed above. In Sect. 4 we evaluate the proposed approach and demonstrate the feasibility of our claims. Finally, in Sect. 5 we conclude the paper and give some indications of future work.

2. Related Work

Many proposals have been designed to overcome the problems of current networks, but they lack some important aspects for future networks. Below we introduce the most representative solutions and their problems.

The Locator-Identifier Separation Protocol (LISP) [9] seeks to achieve effective separation of locators and identifiers with a map-and-encapsulate scheme. It incorporates special border gateways (ingress and egress tunnel router) that will resolve identifiers (EIDs) to locators (RLOCs) using the Mapping System (MS), a distributed database with EID/RLOC mapping entries. Although this is a fairly accepted solution, it is tied to IP and does not deal with heterogeneous networks, does not provide specific mobility support, and does not cover network security or privacy because EIDs/RLOCs are not protected.

The Host Identity Protocol (HIP) [10] proposes the use of cryptographic host identifiers (HITs) on top of location-bound IP addresses. It uses a public key security infrastructure to disseminate the HIT and focus on secure identification of hosts. However, it does not protect privacy because HITs unequivocally represent entities, and it does not provide dynamic negotiation of communication parameters or support for heterogeneous underlying networks.

Other proposals go beyond state-of-art HIP/LISP and define a completely new network models, some coupling with existing models while others propose a complete revamp (clean-slate approaches). From the former, we find BLIND [11] which is a derivation of HIP centered in security, but it lacks support for negotiating security aspects and needs forwarding agents to get privacy protection.

Conceived within the AKARI project [12], the HIMALIS architecture [13], [14] provides identifier/locator separation with less footprint than the solutions mentioned above, so it is suitable to be used in low power devices, like in sensor networks [15]. However, it identifies entities by their devices and does not include privacy protection or mutual end-to-end authentication and authorization.

Being *clean-slate* proposals, MILSA [16] and Enhanced MILSA [17] have covered most requirements for future networks. However, they are host-oriented, do not provide clear abstraction of endpoints, and require current networks to be jettisoned before being deployed.

We consider that an evolutionary migration approach has greater expectations of success than *clean-slate* approaches, so in this paper we address the location/identifier separation in an integrated manner, with special attention to security and privacy. This approach, as discussed in the following sections, has some things in common with HIP, so we have chosen this to be compared with our proposal.

3. Identity-Based Control Plane

In order to overcome the complexity of maintaining security and privacy contexts, while providing secure identification, we propose to build a control plane that addresses entities by their digital identities instead of their point of attachment to the network. This will complement any current and future network architecture, allowing them to incorporate its qualities by just using it to initiate and manage communications. This benefits the separation of concerns so that the network architecture can be concentrated, among other things, on network traffic routing and underlying mobility management, while the identity-based control plane will resolve the security issues, such as access control, privacy protection, authentication, authorization, etc. Hence, this proposal permits the creation of new architectures with security as a central aspect.

The core element of the identity-based control plane is the Domain Trusted Entity Infrastructure (DTEi). The objective of such infrastructure is to have a trusted overlay network in which each element is responsible for managing the identities of its own domain but offers restricted operations to other domains. This way, when an entity wants to contact with another entity from other domain, it will use the DTEi node from its own domain, which the entity can directly reach. Thus, the *contact* operation is performed in a trusted, private, and totally secure manner. This functionality is included in the identity-based control plane, so the actual entities do not need to contact their DTEi nodes directly; their network protocols will do this for them.

Once the DTEi is built, it will use its inherent trusted and secure features to offer a set of network services that are

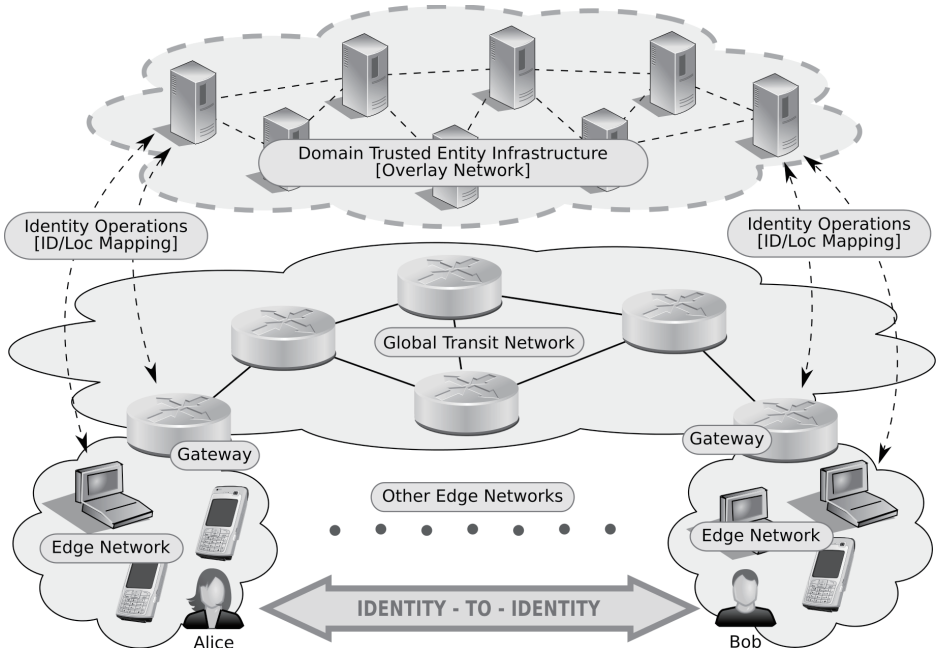


Fig. 1 Architecture overview.

part of the identity-based control plane. The main services are security negotiations and mobility management. Addressing security and privacy issues from the beginning of communications is a prospective requirement for all future network communications, so it should be offered from the same perspective as other communication operations. Furthermore, mobility has security implications beyond the inner security of the mobility mechanisms because the new network to which a node has moved may not enforce the security policies set by the communication parties.

3.1 Domain Trusted Entity Infrastructure (DTEi)

As introduced above, the DTEi is responsible for managing the identities of network entities but it will also manage the security associations they establish for their communication, as well as their privacy contexts. All this functionality is achieved by interconnecting all DTEi nodes to build an overlay network that permits nodes to communicate each other in a trusted and secure way without requiring external resolution mechanisms or even addresses. The overlay network is built with the routing algorithm found in Kademlia [7], which is based on Chord [18], the well known overlay network algorithm.

To achieve proper indexing of identities in the overlay network we represent them as sets of attribute/value pairs. Then, we use the *Bloom Filters* [8] mechanism to get an indexing key for each identity, so similar identities will have close keys (using XOR metric). As attribute/value pairs cannot be derived from the keys, DTEi nodes are able to reference identities without revealing any attribute.

Each DTEi node or instance manages identities and dynamic identifiers for an administrative or network domain. While identities are used to identify networked entities, dynamic identifiers are just used to identify communication sessions. Identifiers can change over time without breaking communications because the DTEi will be used to inform the entities involved which identifier corresponds to which session. Moreover, the DTEi permits entities to validate those identifiers so they can be sure that they are *talking* to *who* they want without revealing their actual identities.

The DTEi will protect the privacy of networked entities but, if permitted by policies, it will be able to provide some attributes to other entities. For instance, when tied to address-based networks, the current location of an entity can be revealed to the underlying elements, so they can deliver network traffic to the entity.

3.2 Abstracting Endpoints from Identifiers and Locators

One key aspect of the identity-based control plane is that it emphasizes the differentiation of *identity* and *identifier*. It follows the ITU-T X.1250 definition of identity as "the representation of an entity in the form of one or more information elements which allow the entity(s) to be sufficiently distinguished within context". On the other hand an identifier is a piece of fixed-size data that identify something.

Identities are therefore used to identify entities. They are the endpoints, so underlying identifiers and locators may change during communications. The identity-based control plane will be in charge of negotiating and reporting all changes required to manage communications.

3.3 Secure Communications

In general, entities participating in communications are au-

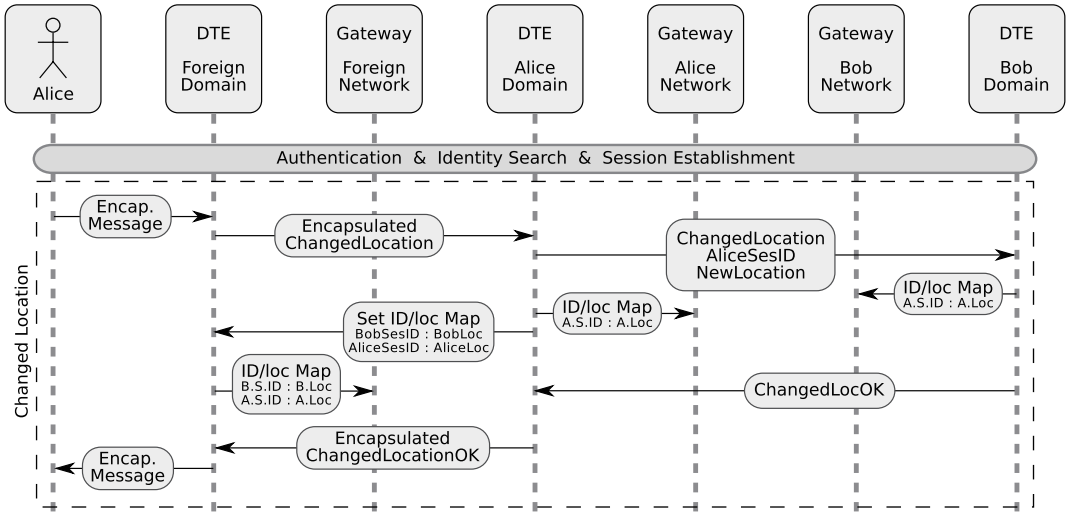


Fig. 2 Mobility management: message exchanges after moving to another network (handover).

thenticated with their digital identity. This is performed by the DTEi while mediating in session management. But entities are in full control of what they want to reveal and they can use virtual identities to achieve anonymity. Moreover, the DTEi can reveal identity attributes, but it is totally regulated by the policies set by the entities.

Apart from authentication, the DTEi can provide attribute-based authorization. It supports negotiating access to any resource, even to identity attributes, by means of the value of the attributes of another identity. For example, an identity can have a policy to *talk* only with other identities pertaining to the same domain. The DTEi negotiates this and, if it succeeds, permits the communication, reserves a session identifier, and reveals the locator in the underlying network.

With this mechanism, instead of hiding the identity information of an entity, the identity-based control plane offers other entities a controlled access to such information. Thus, the DTEi validates identities against specific entities, so other entities may ask it to ensure that an entity is "who" it is claiming to be. Also, we can consider that an entity is *authenticated* just by validating the identifier (or identifiers) it is using and the integrity of the messages exchanged with it, which is achieved by a signature field included in the messages. Therefore, when another architecture integrates the identity-based control plane, it will provide integrated authentication and authorization of communications.

In order to prevent educated guesses of the identity that is behind a host, the architecture permits arbitrary changes of session identifiers. Existing sessions are not affected by the identifier change because they are bound to session identifiers. New session identifiers are negotiated through the DTEi, which is a totally secure and trusted channel, so attackers can not follow the data flow to guess the identity associated to an identifier.

Finally, our approach proposes an asymmetric encryption mechanism to get confidentiality when needed. For instance, Identity Based Encryption (IBE) [19] provides strong security and fits perfectly with our proposal. Those mechanisms have obvious benefits over weaker encryption methods: 1) Transmitted information will be kept secret for longer; 2) They fit and perform much better in publisher/-subscriber underlying networks. In the future, processor performance improvements may make those methods much more feasible.

3.4 Mobility Management

Mobility operations are sensible to environment changes, both from a functional and security points of view. Therefore, the identity-based control plane, through the DTEi, includes a mobility management mechanism. This is used to achieve full mobility support in other network architectures or just to complement them to ensure the security in their mobility schemes.

As the identity-based control plane promotes the use of identifiers to deliver messages without using network addresses or any other location information, entities are able to keep the identifiers they are using even when they change from one underlying network to another. However, the underlying network infrastructures need to know how to deal with the messages exchanged by the entities, so they have to update the mapping between an identifier and the locator of the entity it represents.

When the control plane is integrated into an address-based underlying network, it introduces a *gateway* on each network domain, like in Proxy Mobile IPv6 (PMIPv6) [20] or Hierarchical Mobile IPv6 (HMIPv6) [21]. Behind the gateway there may be one or more entities, so their actual addresses are protected.

As shown in Fig. 2, once an entity (Alice) has moved to a new domain (Foreign Domain), it reports its new location for the current session identifier to the DTEi node of its identity domain (Alice Domain) by sending an encapsulated message to the DTEi node of the foreign domain. Then, the DTEi node of Alice Domain will report the new location to

the DTEi node of the corresponding entity (Bob Domain) and both send a *ID/loc Map* message to the gateways involved in the communication. As the DTEi node of Alice Domain does not have rights to set the mapping into the foreign gateway, it will send such message to the DTEi node of the foreign domain and this node will send the mapping to the foreign gateway. Finally, a confirmation is sent back to the entity. As we demonstrate in the following sections, this procedure does not add a big overhead to the network because it only requires to update the gateways of the entities with which the mobile node has opened sessions.

4. Evaluation

In this section we evaluate the approach proposed in this paper. We first compare the capabilities of our approach with HIP, as both have some common mechanisms. Then we analyze the security of our mobility approach to demonstrate the security advantages of our approach. After that we analyze the mobility operation of the DTEi in comparison with HIP and LISP to show the performance of our approach. Finally, we discuss the experimentation results we have obtained to demonstrate the performance of the lookup approach used by the DTEi.

4.1 Comparison with HIP

As introduced in Sect. 2, HIP provides a mechanism to achieve locator/identifier separation by defining the Host Identity Tag (HIT) as the identifiers and network addresses (normally IP addresses) as locators. It also provides a mobility solution as described in [22]. It states that when a host moves to a new network and obtains a new address, it must send an *HIP UPDATE* packet with a *LOCATOR* parameter indicating the new address to any other party to which it is communicating. Then, this packet is acknowledged and the handover process is finished.

When the communication is established in a secure way through, for example, an ESP tunnel, keys must be negotiated again. Moreover, to support the simultaneous mobility of two hosts that are communicating, HIP proposes its Rendezvous Extension [23]. It states that a rendezvous server (RVS) intermediates in the first message exchanges, so a host that move will update the RVS with its current locator. The RVS will send the message to the destination and then the entities will communicate directly.

In comparison to our proposal, while HIP requires the RVS to globally know all HIT/address mappings, in our architecture, each node of the DTEi knows only the identifier/locator mappings of its domain. When entities from different domains communicate, the DTEi nodes of those domains interact to establish the communication and to exchange the necessary identifier/locator mappings. Also, when a host moves to a new network, instead of trusting in peers to directly communicate locator changes to each other, our architecture uses the DTEi that provides a trusted path to communicate the updated identifier/location mappings.

When our architecture is instantiated together with an address-based network, gateways are used to deal with the identifier/locator resolution, like in Proxy Mobile IPv6 (PMIPv6) [20], so the mobility support in them is also transparent to the entities. In addition, when it is instantiated together with an overlay network, it does not need to update real identifier/locator mappings to the infrastructure, because it is location independent.

That said, our architecture introduces intermediate elements and more message exchanges to provide mobility support but with the great benefit of enhanced trust, privacy, and overall security. Moreover, our architecture provides other advantages over HIP:

- HIP relays on DNS to resolve names to HITs, HITs to addresses, and to obtain the RVS address when it is used. Instead, our architecture moves the need for a hierarchical DNS infrastructure to a local element (DTEi node). This enhances security and trust.
- Instead of name/address resolutions, our architecture is based on queries to (one or more) identity attributes to resolve the locator. This adds enormous flexibility to entity identification.
- HIP identifiers (HITs) are unique for each host. Our architecture permits to dynamically change identifiers. This prevents traceability and increases privacy by changing identifiers between sessions.
- HIP lacks support for identity or identifier negotiations, so any entity can resolve and try to contact any other entity. Our architecture provides identity-based negotiations to enhance security by preventing unauthorized entities to obtain the identifier/locator mapping.
- Finally, the RVS in HIP is outside the control of the identifier/locator mapping owner. Our architecture stores identifier/locator mappings in the DTEi nodes managing the identity domain of their respective owners. This increases security and improves scalability.

Apart from these differences, as discussed above, our architecture offers other interesting capabilities, such as the consideration of digital identities instead of hosts as communication endpoints.

4.2 Security Analysis

Security is an essential aspect of our proposal and we want to be sure that the mobility management scheme we propose is secure. Thus, we have analyzed the security of the mobility protocol. We opted for the AVISPA automated security validation tool [24] because of its simplicity and strength in analyzing network protocols.

AVISPA requires an input file in the High-Level Protocol Specification Language (HLPSL) so we need to formalize our mobility protocol using Alice-Bob (A-B) notation. As shown in Fig. 3, we first represent the entities taking part in the protocol. They are: Alice, represented as A; the nodes of the DTEi corresponding to three domains (home domain as DTE1, correspondent domain as DTE2,

```
 1  A    -> DTE3 : {{TkADTE1.AsID.Aloc}_inv(KA)}_KDTE1
 2  DTE3 -> DTE1 : {{TkDTE13.{{TkADTE1.AsID.Aloc}_inv(KA)}_KDTE1}_inv(KDTE3)}_KDTE1
 3  DTE1 -> DTE2 : {{TkDTE12.AsID.Aloc}_inv(KDTE1)}_KDTE2
 4  DTE2 -> GW2  : {{AsID.Aloc}_inv(KDTE2)}_KGW2
 5  DTE1 -> GW1  : {{AsID.Aloc}_inv(KDTE1)}_KGW1
 6  DTE1 -> DTE3 : {{H(TkDTE13).AsID.Aloc.BsID.Bloc}_inv(KDTE1)}_KDTE3
 7  DTE3 -> GW3  : {{AsID.Aloc.BsID.Bloc}_inv(KDTE3)}_KGW3
 8  DTE2 -> DTE1 : {{H(TkDTE12).OK}_inv(KDTE2)}_KDTE1
 9  DTE1 -> DTE3 : {{H(TkDTE13).{{H(TkADTE1).OK}_inv(KDTE1)}_KA}_inv(KDTE1)}_KDTE3
10  DTE3 -> A    : {{H(TkADTE1).OK}_inv(KDTE1)}_KA
```

Fig. 3 Protocol for mobility support in *Alice and Bob* notation.

and foreign domain as DTE3); and their gateways, represented as GW1/2/3. The function H represents a hash and the *inv* function gets a cryptographic private key from a public key. The variables KA, KDTE1, KDTE2, KDTE3, KGW1, KGW2, and KGW3 are the corresponding public keys of the entities. The variables named Tk* are the authentication tokens obtained during the authentication process and H(Tk*) are hashed tokens used to authenticate answers. Finally, AsID.Aloc and BsID.Aloc represent the session identifiers and locators of Alice and Bob.

With this A-B notation we create the HLPSL file, assigning a different role to each entity and indicating that the analyzer tool should check the secrecy of all tokens (Tk*), which can be known only by the pair of entities that communicate. We also indicate that the analyzer should use those tokens to authenticate the senders. To keep the simplicity of the process we do not test for replay attacks and we do not include the sequence numbers in the protocol notation, but urge the tool to run two parallel sessions to see if there is any problem with it.

The resulting HLPSL file is used as input for AVISPA to generate the Intermediate Format (IF) that is, in turn, used by the actual analyzers (backends). To strengthen the analysis we run different backends: the On-the-Fly Model Checker (OFMC), the CL-based Attack Searcher (CL-AtSe), the SAT-based Model-Checker (SATMC), and the Tree Automata-based Protocol Analyser (TA4SP). All backends gave a SAFE result except the TA4SP, which gave an INCONCLUSIVE result due to the nature of the rules. These results demonstrate that the protocol is secure.

4.3 Mobility Performance Analysis

In this section we analyze the performance of the mobility management approach included in the identity-based control plane and compare it with the mobility approaches from HIP and LISP. To perform this analysis we have built a mathematical model for each approach. Such models represent the cost in milliseconds (ms) of sending a message/packet from one endpoint to another during and after a handover. We have to notice that, from the beginning, we expect our approach to offer less performance than HIP or LISP because it adds extra security operations to ensure the security advantages discussed throughout the paper.

To build proper mathematical models, as shown in Fig. 4, we have defined a common scenario that maps the same elements to specific elements of each approach. Therefore, we have a scenario with five elements: Initiator Node (IN), Responder Node (RN), Initiator Gateway (IGW), Responder Gateway (RGW), and Rendezvous Infrastructure (RI). These elements have direct mapping to HIP and LISP elements, including the RI, which is mapped to the RVS of HIP and the Mapping System (MS) of LISP.

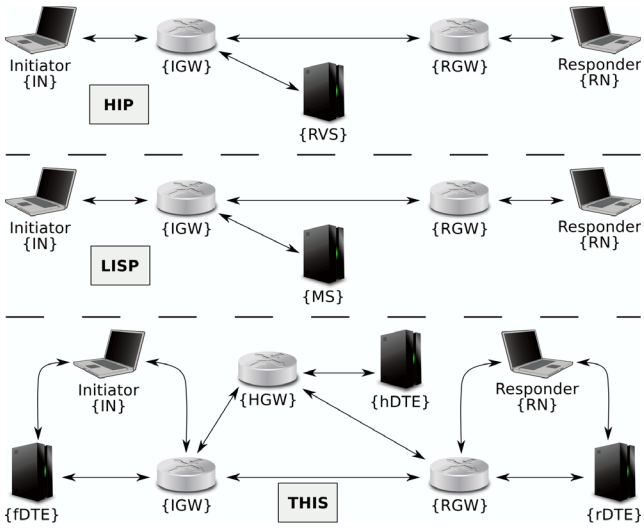


Fig. 4 Scenarios used to build the mobility analysis models for the comparison of HIP, LISP, and our approach (THIS).

In our approach (labeled THIS), the RI is mapped to the whole DTEi but since the operations inside it are complex we decided to represent the different DTEi nodes. Therefore, the RI is replaced by the hDTE (home domain), the fDTE (foreign domain), and the rDTE (responder domain). To better represent our approach, we also included the Home Gateway (HGW) into this representation.

Once we have defined the common scenario, we proceed with the definition of the base parameters used to construct the mathematical models as follows:

- $T_{a\to b}$: Time (ms) spent to transmit a message/packet from a to b, where a/b can be any of the elements defined above. We consider that $T_{a\to b} = T_{b\to a}$.
- N_d: Number of network/administrative domains.
- N_h: Average number of hosts per domain.
- α: Time (ms) spent finding an entry in a hash table per

entry in the table.

Using these parameters we have built the equations that represent the intended mathematical models, which are used to calculate the cost (in milliseconds) of the handover and a following message/packet exchange between two nodes of different domains (IN and RN) for HIP (Eq. (1)), LISP (Eq. (2)), and the approach proposed in this paper (Eq. (3)).

First we define the equation used for HIP. The handover starts when IN sends an id/loc update message to RN, going through IGW and RGW. Then, RN sends an acknowledgement to IN. To update the RVS, IN sends another id/loc update message to it through the IGW, and the RVS updates the corresponding record and sends an ACK to IN through the IGW. Finally, IN sends the message to RN through IGW and RGW, and RN sends its response to IN through RGW and IGW. The equation results as follows:

$$\begin{aligned} C_{\text{HIP}} =& T_{IN\to IGW} + T_{IGW\to RGW} + T_{RGW\to RN} \\ &+ T_{RN\to RGW} + T_{RGW\to IGW} + T_{IGW\to IN} \\ &+ T_{IN\to IGW} + T_{IGW\to RVS} + \alpha * N_h * N_d \\ &+ T_{RVS\to IGW} + T_{IGW\to IN} \\ &+ T_{IN\to IGW} + T_{IGW\to RGW} + T_{RGW\to RN} \\ &+ T_{RN\to RGW} + T_{RGW\to IGW} + T_{IGW\to IN} \end{aligned} \tag{1}$$

The handover in LISP requires updating the mappings in the MS so IN sends an id/loc update message to MS through IGW and the MS sends an acknowledgement, also through IGW. To communicate with RN, IN sends a message to IGW. This asks the MS to find the mapping entry and it sends the response to IGW. Then, IGW sends the message to the corresponding RGW which, in turn, sends it to RN. Now, RN sends its response to RGW and this again asks the MS to resolve the locator of IN. Finally, RGW receives the locator of IN and sends it the response message through IGW. The resulting equation is as follows:

$$\begin{aligned} C_{\text{LISP}} =& T_{IN\to IGW} + T_{IGW\to MS} + \alpha * N_h * N_d \\ &+ T_{MS\to IGW} + T_{IGW\to IN} \\ &+ T_{IN\to IGW} + T_{IGW\to MS} + \alpha * N_h * N_d \\ &+ T_{MS\to IGW} + T_{IGW\to RGW} + T_{RGW\to RN} \\ &+ T_{RN\to RGW} + T_{RGW\to MS} + \alpha * N_h * N_d \\ &+ T_{MS\to RGW} + T_{RGW\to IGW} + T_{IGW\to IN} \end{aligned} \tag{2}$$

The handover process of the approach proposed in this paper, as depicted in Fig. 2, begins with the initiator node (IN) that has moved to a foreign network and uses the foreign DTEi node (fDTE) and foreign gateway (IGW) to send an encapsulated message to its home DTEi node (hDTE) with the new location for its session ID. The home DTEi node (hDTE) sends the new location to the DTEi node assigned to the responder node (RN) and both of them send in parallel an update loc/id map to the gateways. The home DTEi node (hDTE) also sends the foreign DTEi node (fDTE) an update loc/id map with both IN and RN entries, which in turn sends it to its gateway. Finally, the home DTEi node (hDTE) sends a confirmation to IN through fDTE and the corresponding gateways (HGW and RGW). The process is translated to an equation with the same parameters used above and results in the following equation:

$$\begin{aligned} C_{\text{THIS}} =& T_{IN\to fDTE} + T_{fDTE\to IGW} \\ &+ T_{IGW\to HGW} + T_{HGW\to hDTE} + \alpha * N_h \\ &+ T_{hDTE\to HGW} + T_{HGW\to RGW} \\ &+ T_{RGW\to rDTE} + \alpha * N_h \\ &+ T_{rDTE\to RGW} + T_{RGW\to HGW} \\ &+ T_{HGW\to hDTE} \\ &+ T_{hDTE\to HGW} + T_{HGW\to IGW} \\ &+ T_{IGW\to fDTE} + T_{fDTE\to IN} \\ &+ T_{IN\to IGW} + T_{IGW\to RGW} + T_{RGW\to RN} \\ &+ T_{RN\to RGW} + T_{RGW\to IGW} + T_{IGW\to IN} \end{aligned} \tag{3}$$

To facilitate the handling of the models we simplify them, generalizing all gateways (IGW, RGW, HGW) to GW, both endpoints (IN, RN) to N, and all nodes from the DTEi (fDTE, hDTE, rDTE) to a specific DTEi node. Thus, the simplified models are as follows:

$$\begin{aligned} C_{\text{HIP}} =& 10 * T_{N\to GW} + 4 * T_{GW\to GW} \\ &+ 2 * T_{GW\to RVS} + \alpha * N_h * N_d \end{aligned} \tag{4}$$

$$\begin{aligned} C_{\text{LISP}} =& 6 * T_{N\to GW} + 6 * T_{GW\to MS} \\ &+ 3 * \alpha * N_h * N_d + 2 * T_{GW\to GW} \end{aligned} \tag{5}$$

$$\begin{aligned} C_{\text{THIS}} =& 2 * T_{N\to DTE} + 8 * T_{DTE\to GW} \\ &+ 6 * T_{GW\to GW} + 2 * \alpha * N_h + 4 * T_{N\to GW} \end{aligned} \tag{6}$$

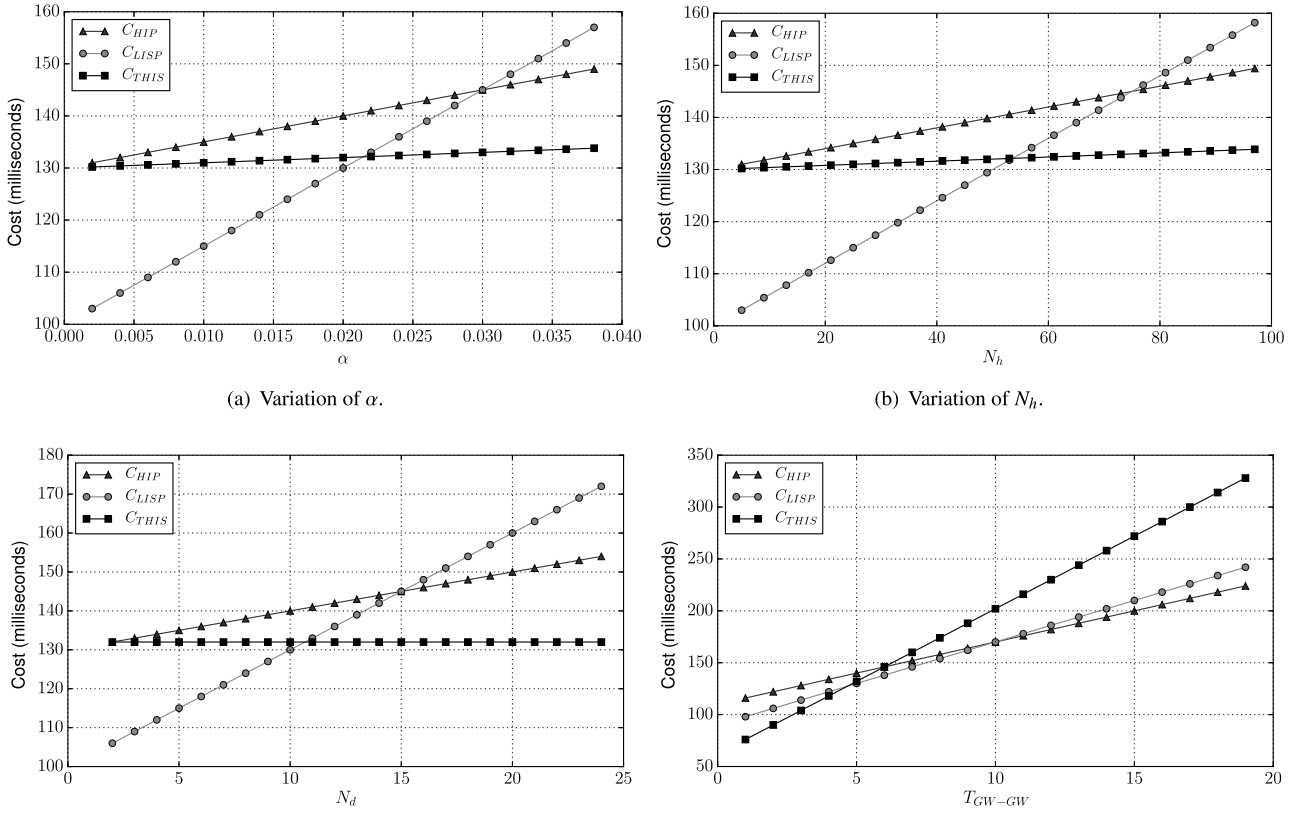
Once the models have been defined, we run them by using the values and ranges shown in Table 1 to assign their variables. Default values are set from experience from previous experiments in real networks but in order to obtain valid results we decided to use wide intervals (from *min* to *max*) that include as much real cases as possible. Thus we have a wide spectrum of values for the parameters.

For instance, we set transmission times for each hop to vary from 1 ms, which is very low and is typically found in wired links (1 hop), to 20 ms, which is somewhat high and is typically found in wide networks (10–15 hops). Moreover, these wide intervals emphasize the points where the plots intersect, which are the points of interest from the results, together with the slope of each plot.

With the outputs from the models we have built the plots shown in Fig. 5. First, Fig. 5(a) shows the results for the three approaches when varying the α parameter between

Table 1 Parameter values and ranges.

Parameter	Default	Min	Max
α	0.02	0.002	0.04
N_h	50	5	100
N_d	10	2	25
$T_{GW\to GW} \mid T_{DTE\to GW}$	5	1	20
$T_{GW\to MS} \mid T_{GW\to RVS}$	5	1	20
$T_{N\to GW} \mid T_{N\to DTE}$	10	-	-



(a) Variation of α.

(b) Variation of N_h.

(c) Variation of N_d.

(d) Variation of $T_{GW\rightarrow GW}$, $T_{DTE\rightarrow GW}$, $T_{GW\rightarrow MS}$, and $T_{GW\rightarrow RVS}$.

Fig. 5 Analysis results for Eqs. (1), (2), and (3) with the parameters taken from Table 1.

the defined range boundaries. It shows that LISP is much better than HIP and our approach for lower values of α, but for $\alpha > 0.025$, our approach improves on the others. Next, Fig. 5(b) shows that, for the variation of the average number of hosts per domain, our approach improves on the others from 60 average hosts per domain onwards. Figure 5(c) shows the results for the variation of the number of network or administrative domains, and also shows that our architecture improves on the others when there are more than 12 domains.

As discussed above, the first three architectures have a similar behavior when varying α, N_h, or N_d. In contrast, Fig. 5(d), which represents the variation of elapsed time to contact a gateway from other gateway or from a DTEi node, shows a very different picture. It shows that the overhead of our approach over HIP or LISP increases with $T_{GW\rightarrow GW}$. This is the main drawback of our approach for the selected parameters, but it is not a big problem, since the time between GWs is not expected to grow over 5 ms but rather to decrease in the future. However it is something we have to analyze in future iterations of our apporach.

4.4 Overlay Network Lookup Performance

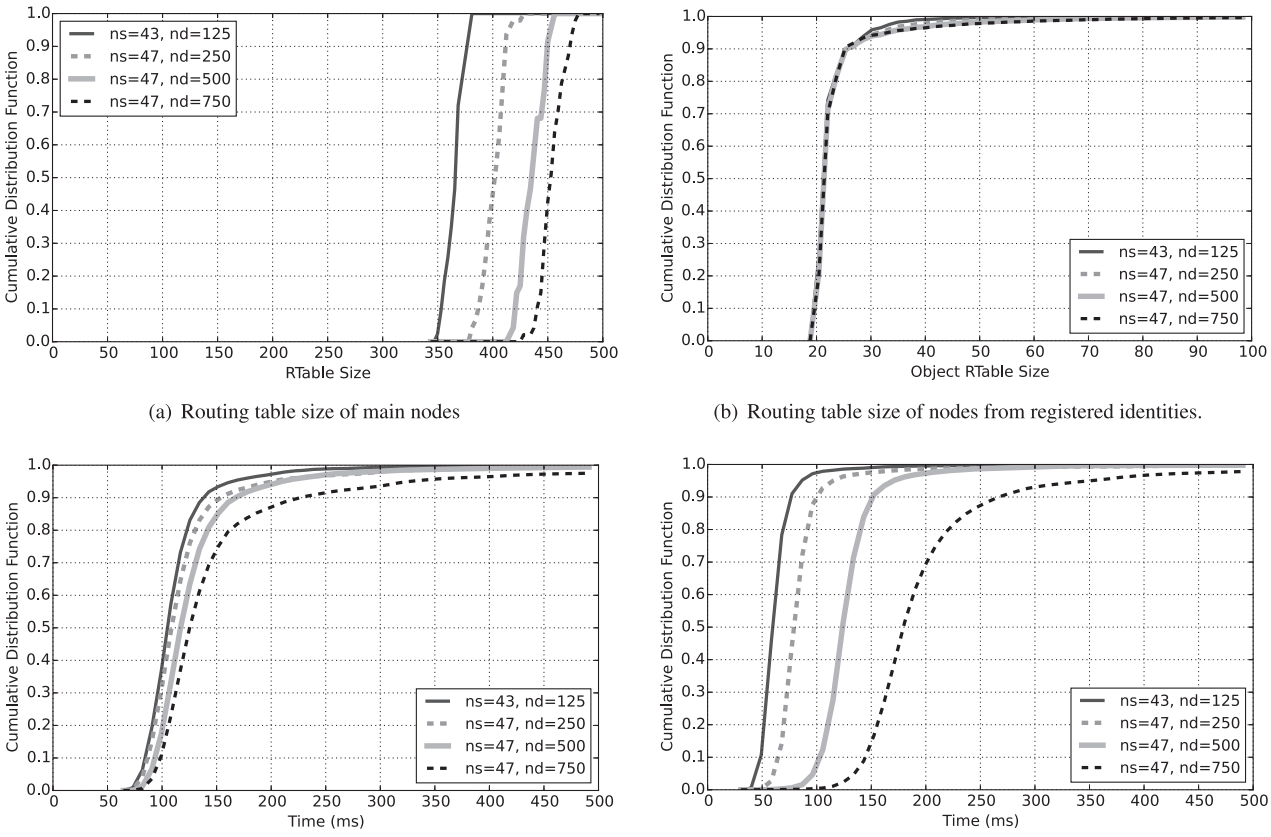
In order to get a running view of the behavior of the proposed solution, we built a prototype implementation of the DTEi to perform some experiments. The main objective of these experiments is to demonstrate the performance of the overlay network lookup approach, which is the key point in the DTEi because it has to find the DTEi of other identities. It is based on non-complete identities (partial identities), with a different number of attributes in each search.

4.4.1 Experimentation Scenario

To prepare the experimentation scenario, we deployed as many DTEi nodes as computing nodes available in the target experimentation infrastructure (43 and 47 respectively). Then, we deployed one more overlay network node for each registered identity. These nodes run in different threads, so they do not interfere each other in their operation.

In each execution of our experiments we set the number of registered identities (also instantiating new and lightweight overlay network nodes) to 125, 250, 500, and 750. Therefore, we get different sizes for the overlay network (number of nodes), correspondingly 5375, 11750, 23500, and 35250. In this way we are sure we stress the overlay network approach of the DTEi.

Within this scenario, we have launched 10 different searches for each DTEi node and for each number of attributes in the partial identity (from 1 to 9), with 5 iterations of each operation. Next, for each execution, we obtained four different measurements: the time spent in identity registration, the time spent in identity lookup, the size of the



(a) Routing table size of main nodes

(b) Routing table size of nodes from registered identities.

(c) Time spent in identity registration.

(d) Time spent in identity lookups.

Fig. 6 Overlay routing table sizes and lookup/registration times.

routing table of each node (differentiating main and identity nodes), and the precision of the lookup operations (differentiating those that find the desired identity as first result, those that find the desired identity as non-first result, and those that do not find the desired identty).

The testbed we have used to run the experiment is the GAIA experimentation infrastructure [25]. From it we have used 47 computation nodes which dedicated 1 GiB of RAM and 2 GHz of CPU to the experiment. Those nodes are interconnected through Ethernet links (100 Mbit/s) by a high-end switch (Cisco Catalyst 2950, 48 ports). These resources are typically found in server environment, so the results we obtained from the experiment reflect the real world behavior of the proposed architecture with high confidence degree. Each node of the testbed holds a main DTEi node and as many lightweight overlay network nodes, as indicated in the experiment configuration described above.

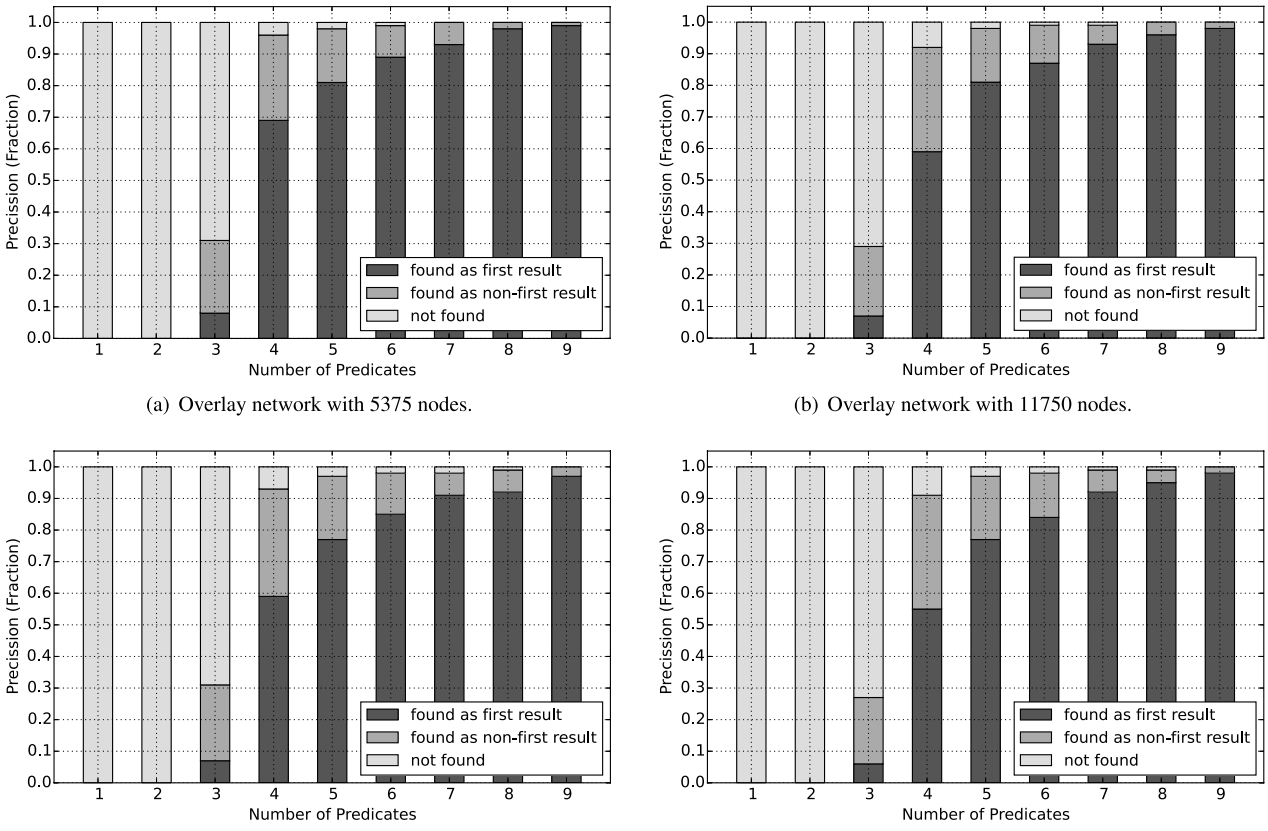
4.4.2 Results

Once we have executed the experiments and obtained the measurements we have proceeded to interpret and analyze them. As shown in Fig. 6, for each different size of the overlay network we compared the routing table size of the DTEi nodes, the routing table size of the nodes that manage identities, the time spent in identity registration, and the time spent in identity lookups. Each plot shows the CDF (cumulative distribution function) of the measured values for the number of physical servers (*ns*) and the number of deployed nodes per physical server (*nd*).

Regarding the size of the routing table, as shown in Fig. 6(a), the routing table sizes of the main nodes increase with the number of nodes in the overlay network but the increase of the number of main nodes is negligible. This is because, since they act as access point for the secondary nodes (identity nodes) they have the opportunity to know more identities. However, as the maximum number of nodes in the table is 3200, resulting from the 160 buckets [†] and 20 nodes per bucket, the average size of the tables is very low, not exceeding 450 nodes per table on average.

In contrast with the results discussed above, the routing table size of the nodes corresponding to the identities registered, as shown in Fig. 6(b), is very similar, regardless of the number of nodes registered. This is because these nodes are bootstrapped to the main nodes, their access points, and they only know other nodes when they interact with them. On average, this size is kept around 20, which is the selected bucket size in the experiments. This is because, during the bootstrap, the nodes select k (= 20) other nodes to be in-

[†]Buckets are used by the Kademlia algorithm to structure the overlay routing table.



(a) Overlay network with 5375 nodes.

(b) Overlay network with 11750 nodes.

(c) Overlay network with 23500 nodes.

(d) Overlay network with 35250 nodes.

Fig. 7 Lookup precision for different overlay network sizes.

cluded in their tables. From this result we can again confirm that it is very far from the maximum number of nodes (3200), so the overlay network can still grow while improving its operation. This reduced table size does not affect lookups because of their iterative method.

Regarding the time spent in registering identities, as shown in Fig. 6(c), there is a slight difference when the overlay network size changes. This difference is because of the lookup operation that each node performs during the bootstrap in the overlay network. Although the median grows from around 100 ms to around 125 ms, the average time grows from around 100 ms to around 170 ms. This difference is mainly affected by those operations with extreme times, which had errors (packet losses). However, both are reasonable times considering all the operations to be performed to bootstrap a new node and register the identity in the α-closest nodes of the DHT. Indeed, this demonstrates that the registration time depends on the size of the network, but the time is very low and demonstrates the validity of the proposed solution.

Regarding the time spent on the lookup operation, as shown in Fig. 6(d), the size of the overlay network has more impact on the lookup than the register operation. This operation is very quick for small networks, with an average of 63 ms and a Q3 (third quartile) of 66 ms for the smallest network, but it is also kept within small times when the network grows, having an average of 207 ms and a Q3 of 209 ms when the overlay network is almost 7 times bigger. As expected, the overlay network size affects this time because DHT operations have to contact many nodes, having a maximum complexity order of *O(log n)* nodes, where *n* is the size of the network. This is correlated with the measurements obtained, because the network size has grown 7 times but the lookup time grows slightly more than 3 times. This result is another indicator of the feasibility and scalability of the proposed solution.

We have also measured the number of lookups that responded with the desired identity for each number of predicates used in the lookup operation. This way, in Fig. 7 we show box plots indicating the proportion of lookups of lookups that did not respond with the requested identity, the proportion of lookups that responded with the requested identity as non first result, and the proportion of lookups that responded with the desired identity as first result.

In Fig. 7(a) we show the results regarding the precision of the identity lookup approach included within the DTEi. It depicts that when using only 1 or 2 attributes in the partial identity introduced to the lookup, the system does not retrieve the desired identity. However, starting from just 3 attributes, 30% of the lookup operations return the desired identity, of which less than 10% have it as first result. As expected, the precision grows exponentially with the num-

ber of attributes included in the partial identity. From 4 attributes onwards, almost 100% of the lookups return the desired identity, most of them as the first result.

When increasing the number of nodes forming the overlay network, as shown in Fig. 7(b), the precision of the lookup method is almost the same, with the exception found in the reduced proportion of identities found using partial identities with 3 and 4 predicates. The same behavior can be observed in the following increments of the number of nodes forming the overlay network, as shown in Fig. 7(c) and Fig. 7(d).

From the precision results we can obviously determine that using a very low number of attributes/predicates is not adequate to obtain the requested identity from the DTEi. However, from 4 predicates onwards, the results are impressive because more than 90% of lookups found the searched identity for all the different network sizes used in the experiments. This result, together with the performance results discussed above, demonstrates the suitability, and hence the feasibility, of the proposed approach.

5. Conclusions and Future Work

This paper has shown how to build an identity-based control plane that provides comprehensive security and integrated mobility management to future networks by using an identity-based overlay network to place digital identities in the middle of communications.

To demonstrate the qualities of the proposed approach, we compared it with HIP, a popular security-centric solution to locator/identifier separation. Both approaches may look similar, but they differ in how they deal with communication endpoints and how they address privacy. In summary, our proposal improves HIP in the following points:

- Identities are used as endpoints, which are derived to dynamic identifiers, instead of static identifiers.
- Entity resolutions are performed in a natural way by representing queries as partial identities instead of strict domain-names.
- Endpoint identifiers can be changed securely and dynamically, improving traceability avoidance.
- Communication sessions are negotiated using participant identities and their authorization policies are enforced, so general security is enhanced.
- Scalability is improved because the identifier/locator mappings are distributed across the overlay network and DHT built by the DTEi.

We have also analyzed the security of the proposed mobility management scheme with AVISPA [24], an automated protocol security analysis tool. It demonstrates that the handover protocol addressed by the proposed identity-based control plane is secure.

After confirming the security of the proposed approach, we demonstrated the performance of the proposed mobility management approach, comparing it with HIP and LISP. Although in principle we expected our approach to add significant overhead to HIP and LISP because of its extra security capabilities, the analysis has demonstrated the opposite. The only drawback in our approach appears when message transmission time between gateways increases, which is something we have to study deeply in future work.

Therefore, the results discussed in Sect. 4 demonstrate the claims we stated at the beginning of the paper, so it is feasible to use an identity-based overlay network and DHT mechanism to build an identity-based control plane that can be used to provide comprehensive security and mobility management to current and future network architectures. Also, we have demonstrated the benefits of using *Bloom Filters* to index and find identities through the Kademlia-based overlay network and DHT.

As future work, we plan to investigate the decentralization of identity validation to gain certain level of independence from the DTEi. This may accelerate the transactions involving only a few messages. Also, we plan to study how the identity-based control plane we proposed here behaves when instantiated within other architectures, such as current IP-based networks, different overlay network approaches, and architecture proposals for the FI such as HIMALIS [14] and different Information Centric Networking (ICN) schemes. Finally, as identities provide a proper way to describe networked entities, we will investigate the possibility of using the information managed by the DTEi to provide a secure discovery mechanism to the control plane, so network architectures will also gain integrated discovery support.

Acknowledgments

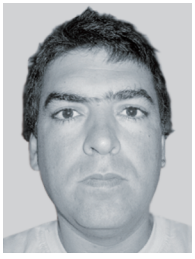
This work is partially supported by the European Commission's Seventh Framework Programme (FP7/2007-2013) project GN3, by the Ministry of Education of Spain under the FPU program grant AP2010-0576, by the Ministry of Economy and Competitiveness of Spain under the grant TIN2013-50477-EXP, and by the Program for Research Groups of Excellence of the Séneca Foundation under grant 04552/GERM/06.

References

[1] R. Jain, "Internet 3.0: Ten problems with current internet architecture and solutions for the next generation," Proc. Military Communications Conference, pp.1–9, Los Alamitos, CA, USA, 2006.
[2] T. Li, "Design goals for scalable Internet routing," 2011. http://www.ietf.org/rfc/rfc6227.txt
[3] P. Martinez-Julia, A.F. Gomez-Skarmeta, J. Girao, and A. Sarma, "Protecting digital identities in future networks," Proc. Future Network and Mobile Summit 2011, pp.1–8, 2011.
[4] P. Martinez-Julia and A.F. Gomez-Skarmeta, "Using identities to achieve enhanced privacy in future content delivery networks," Computers and Electrical Engineering, vol.38, no.2, pp.346–355, 2012.
[5] P. Martinez-Julia and A.F. Gomez-Skarmeta, "A novel identity-based network architecture for next generation internet," J. Universal Computer Science, vol.18, no.12, pp.1643–1661, 2012.
[6] ITU-T, "Series X: Data Networks, Open system communications and security. Cyberspace security — Identity management. Baseline

capabilities for enhancing global identity management and interoperability," Recommendation ITU-T X.1250," 2009.
[7] P. Maymounkov and D. Mazières, "Kademlia: A peer-to-peer information system based on the xor metric," Proc. First International Workshop on Peer-to-Peer Systems, pp.53–65, London, UK, 2002.
[8] D.E. Knuth, The Art of Computer Programming, Addison-Wesley, 2006.
[9] D. Meyer, "The locator identifier separation protocol (LISP)," The Internet Protocol Journal, vol.11, no.1, pp.23–36, 2008.
[10] R. Moskowitz and P. Nikander, "Host identity protocol (HIP) architecture," 2006. http://www.ietf.org/rfc/rfc4423.txt
[11] J. Ylitalo and P. Nikander, "BLIND: A complete identity protection framework for end-points," Lect. Notes Comput. Sci., vol.3957, pp.163–176, 2006.
[12] National Institute of Information and Communications Technology, "AKARI" Architecture Design Project for New Generation Network, 2010. http://akari-project.nict.go.jp
[13] V.P. Kafle and M. Inoue, "HIMALIS: Heterogeneity inclusion and mobility adaptation through locator id separation in new generation network," IEICE Trans. Commun., vol.E93-B, no.3, pp.478–489, March 2010.
[14] P. Martinez-Julia, A.F. Gomez-Skarmeta, V.P. Kafle, and M. Inoue, "Secure and robust framework for id/locator mapping system," IEICE Trans. Inf. & Syst., vol.E95-D, no.1, pp.108–116, Jan. 2012.
[15] V.P. Kafle, H. Otsuki, and M. Inoue, "An id/locator split architecture for future networks," IEEE Commun. Mag., vol.48, no.2, pp.138–144, 2010.
[16] J. Pan, S. Paul, R. Jain, and M. Bowman, "Milsa: A mobility and multihoming supporting identifier locator split architecture for naming in the next generation internet," Proc. Global Communications Conference, pp.2264–2269, Washington, DC, USA, 2008.
[17] J. Pan, R. Jain, S. Paul, M. Bowman, X. Xu, and S. Chen, "Enhanced milsa architecture for naming, addressing, routing and security issues in the next generation internet," Proc. International Conference on Communications, pp.14–18, Washington, DC, USA, 2009.
[18] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," Proc. 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, pp.149–160, New York, NY, USA, 2001.
[19] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM J. Comput., vol.32, no.3, pp.586–615, 2003.
[20] S. Gundavelli, et al., "Proxy Mobile IPv6," 2008. http://www.ietf.org/rfc/rfc5213.txt
[21] H. Soliman, et al., "Hierarchicaly Mobile IPv6 (HMIPv6) Mobility Management," 2008. http://www.ietf.org/rfc/rfc5380.txt
[22] P. Nikander, et al., "End-Host Mobility and Multihoming with the Host Identity Protocol," 2008. http://www.ietf.org/rfc/rfc5206.txt
[23] J. Laganier, et al., "Host Identity Protocol (HIP) Rendezvous Extension," 2008. http://www.ietf.org/rfc/rfc5204.txt
[24] L. Viganò, "Automated security protocol analysis with the AVISPA tool," Electronic Notes in Theoretical Computer Science, vol.155, pp.61–86, 2006.
[25] P. Martinez-Julia, A.J. Jara, and A.F. Skarmeta, "Gaia extended research infrastructure: Sensing, connecting, and processing the real world," Proc. TridentCom 2012, pp.3–4, 2012.

Pedro Martinez-Julia received the B.S. degree in Computer Science from the Open University of Catalonia in 2009 and the M.S. degree in Advanced Information Technology and Telematics from the University of Murcia in 2010. He is currently a Ph.D. candidate at the University of Murcia. Since 2009 he is a research fellow in the Department of Communication and Information Engineering at the University of Murcia, Spain. He has been part of the research staff working in JRA3-T3 of the GN3 project under the European Commission's Seventh Framework Programme (FP7-2007–2013). His main interests are the overlay networks, the security protocols, and the distributed systems and services. He is an associate member of ACM and IEEE.



Antonio F. Skarmeta received the M.S. degree in Computer Science from the University of Granada, and B.S. (Hons.) and the Ph.D. degrees in Computer Science from the University of Murcia, Spain. Since 2009 he is Full Professor at the same department and University. Antonio F. Skarmeta has worked on different research projects in the national and international area, such as Euro6IX, 6Power, Positif, Seinit, Deserec, Enable, and Daidalos. His main interests are the integration of security services at different layers like networking, management, and web services. He is associate editor of the IEEE SMC-Part B and reviewer of several international journals. He has published over 90 international papers and he is member of several program committees.