Future Network & Mobile Summit 2012

4 - 6 July 2012, Berlin, Germany

Username: Pas

General Information
- Welcome
- Mailing List
- Committees
- Contact Us

Programme
Plenary Speakers
Registration
Call for Papers
Online Submission
Exhibition
Sponsors
Paper Repository
Showcase
ICT-MobileSummit 2008
ICT-MobileSummit 2009
Future Network & MobileSummit 2010
Future Network & MobileSummit 2011

Welcome

Future Network and MobileSummit 2012 takes place in the Estrel Berlin, Germany, 04 - 06 July 2012. This is the twenty-first in a series of Annual Conferences supported by the European Commission, which regularly attracts over 500 delegates from industry and research to share experiences and research results, identify future trends, discuss business opportunities and identify opportunities for international research collaboration under the ICT Theme of Framework Programme 7 (FP7). It will thus contribute to showcasing European research in the field, and position it within the multiplicity of related initiatives supported in other regions of the world.

In the context of convergence and innovation, the 21st Future Network and MobileSummit will address the challenges of building the Future Internet Infrastructures, based on mobile, wireless and fixed broadband communications technologies.

Net!Works Video Blog - Published each day during event

Net!Works, through the NetWorld CA project, is supporting FutureNetworkSummit 2012 and is publishing a series of video blog clips during the event. Please go to http://www.networks-etp.eu/ to view short interviews with speakers and participants as they are published.

Programme

The Scientific Programme for Future Network and MobileSummit 2012 is based on an open Call for Papers which closed in December 2011. The Final Programme consists of four plenary sessions and 38 parallel sessions featuring different aspects of Radio Access and Spectrum, Converged and Optical Networks, Integrated Satellite Communications and Future Internet Technologies.

Plenary speakers confirmed to date include:

- Mario Campolargo, Director, Net Futures, DG Communications Networks, Content and Technology, European Commission
- Hossein Moiin, Chief Technology and Strategy Officer, Nokia Siemens Networks
- Prof Hans-Joachim Grallert, Director, Fraunhofer Heinrich-Hertz Institut
- Reiner Liebler, BnetzA, Germany
- Peter Meissner, NGMN Alliance
- Ruprecht Niepold, Adviser Radio Spectrum Policy, DG Information Society and Media, European Commission
- Dr Lutz Stobbe, Fraunhofer-Institut für Zuverlässigkeit und Mikrointegration IZM, Germany
- Mark Daly, ESB, Ireland
- Didier Bourse, Alcatel Lucent Bell Labs
- Prof. Paul Müller, University of Kaiserslautern, Germany
- Radoslaw Krzywania, Poznan Supercomputing and Networking Center, Poland
- Dai Davies, Dante, UK
- Rolf Sperber, Alcatel-Lucent

Exhibitors

Future Network Summit 2012 Agenda

Updated: 2012-07-02

To view the full programme for each day, click on the day link. To view the papers within a session, click on the session title (WS = workshop session).
To print the full programme, click Printable version.

Day 1:	04 July 2012
08:00	Registration
09:00	**Plenary: Opening Plenary** Prof Klaus David, University of Kassel, Germany (TPC Chair) Mario Campolargo, Director, Net Futures, DG Communications Networks, Content and Technology, European Commission Hossein Moiin, Chief Technology and Strategy Officer, Nokia Siemens Networks Prof Hans-Joachim Grallert, Director, Fraunhofer Heinrich-Hertz Institut
11:00	Coffee Break
11:30	6 Parallel Sessions Next-generation Radio System Architectures and Protocols **WS:** Cognitive Radio/Cognitive Networks **WS:** Optical Networks Standardization in FP7 projects Future Internet Architecture Quality in Future Internet FI Poster Session
13:15	Lunch Communications LTE Advanced Systems: PHY Layer Issues Optical Access Networks **WS:** Cloud Networking – Technical and Business Challenges I **WS:** Green Communications and Networks I RAS Poster Session
16:00	Coffee Break
16:30	6 Parallel Sessions Session 4a LTE Advanced Systems - Future Challenges and Way ahead Optical Technologies and Networking **WS:** Cloud Networking – Technical and

Day 2:	05 July 2012
09:00	**Plenary: Plenary II - Radio Spectrum Policy: Strategic Aspects and the link to R&D on Wireless** Peter Meissner, NGMN Alliance Reiner Liebler, BnetzA, Germany Ruprecht Niepold, Adviser Radio Spectrum Policy, DG Information Society and Media, European Commission Chris Woolford, Director of Spectrum and International Policy, OFCOM UK
11:00	Coffee Break
11:30	5 Parallel Sessions Enabling technologies for flexible spectrum usage Integrated Satellite Communications Optical Network Control Self Management Future Internet Experimental Facilities
13:15	Lunch
14:15	**Plenary: Plenary III - Sustainability** Green IT Evolution - From Energy Didier Bourse, Alcatel Lucent Bell Labs Prof. Klaus David, University of Kassel, Germany
16:15	Coffee Break
16:45	5 Parallel Sessions Cognitive and Reconfigurable Radio Systems I Content Distribution **WS:** FINSENY – Defining the Opportunities for ICT in Smart Energy Scalable Architectures for the Real World Internet Network Overlay, Virtualization and Federation

Day 3:	06 July 2012
09:00	5 Parallel Sessions Cognitive and Reconfigurable Radio Systems II **WS:** Network Federation I - Architecture **WS:** Machine to Machine Communications: Maintaining User Capacity and Pursuing Energy Efficiency in the Internet of Things I **WS:** Future Network Stability: Threats and Challenges I **WS:** Fostering Programmability of Wireless Networks I
10:45	Coffee Break
11:15	5 Parallel Sessions Novel radio network technologies, including energy-efficiency **WS:** Network Federation II - Algorithms & Proof of Concept **WS:** Machine to Machine Communications: Maintaining User Capacity and Pursuing Energy Efficiency in the Internet of Things II **WS:** Future Network Stability: Threats and Challenges II **WS:** Fostering Programmability of Wireless Networks II **Beyond Bandwidth** Introduction G-Lab: A Software Defined Networking Perspective PL-LAB: Polish Distributed Laboratory for Testing Future Internet Solutions Bandwidth on Demand- The next Internet Innovation Federation of Data sets for Multinational Research Projects
16:00	**Plenary: Closing Plenary**
16:30	Conference ends

11:30 **Session 2d: Future Internet Architecture**

Chair: David Kennedy, Eurescom, Germany

A New Inter-networking Architecture for Mobile Oriented Internet Environment
Heeyoung Jung, Electronics and Telecommunications Research Institute (ETRI), Korea, Republic Of

On Converged Multidomain Management of Connectivity in Heterogeneous Networks
Michael Soellner, Alcatel-Lucent Deutschland AG, Germany

Research and Experimentation With the HIMALIS Network Architecture for Future Internet
Pedro Martinez-Julia, University of Murcia, Spain

Socioeconomic Tussles Analysis of the ETICS Approach for Providing QoS-enabled Inter-domain Services
Costas Kalogiros, AUEB-RC, Greece

11:30 **Session 2e: Quality in Future Internet**

Chair: Uwe Herzog, EURESCOM, Germany

Internet Interconnection Assured Quality Services: Issues and Strategic Impact
Manos Dramitinos, Athens University of Economics and Business, Greece

A Global Customer Experience Management Architecture
Jukka-Pekka Laulajainen, VTT Technical Research Centre of Finland, Finland

Service Level Management Convergence for Future Network Enterprise Platforms
Philip Robinson, SAP UK Ltd, United Kingdom

Modelling Quality of Experience in Future Internet Networks
Antonio Pietrabissa, Univ. Rome Sapienza, Italy

11:30 **Poster Session 2f: FI Poster Session**

Chair: Rui Aguiar, Instituto de Telecomunicacoes, Portugal

Supporting an Architecture for Cross-Layer Optimization
Gianmarco Panza, CEFRIEL, Italy

Design and Implementation of a Service Discovery and Composition Framework for Security, Privacy and Dependability Control
Antonio Pietrabissa, Univ. Rome Sapienza, Italy

Evaluating Secure Identification in the Mobile Oriented Future Internet (MOFI) Architecture
Pedro Martinez-Julia, University of Murcia, Spain

Virtualization of Real-world Objects for a full realization of the Internet of Things
Vera Stavroulaki, University of Piraeus, Greece

Managing Customer Experience through Service Quality Monitoring
Anderson Morais, Telecom SudParis, France

Network Architectures for End-to-End Business and Traffic Collaborations Among Carriers
Nicolas Le Sauze, Alcatel-Lucent Bell Labs France, France

13:15

Lunch : Lunch

Cooperative Radio Communications over Correlated Shadowing: Outage Analysis
Athanasios D. Panagopoulos, National Technical University of Athens, Greece

A Wireless Transceiver Power Consumption Model and Two-hop vs. Single-hop Energy Efficiency Ratio
Goran Dimic, Institute Mihajlo Pupin, Univ. of Belgrade, Serbia

Future Network and MobileSummit 2012 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2012
ISBN: 978-1-905824-29-8

Poster Paper

Evaluating Secure Identification in the Mobile Oriented Future Internet (MOFI) Architecture

Pedro MARTINEZ-JULIA[1], Antonio F. SKARMETA[1],
Hee Young JUNG[2], Seok Joo KOH[3]
[1]*Department of Communication and Information Engineering, University of Murcia, 30100, Murcia, Spain*
Email: {pedromj,skarmeta}@um.es
[2]*ETRI, 138 Gajeongno, Yuseong-Gu, Daejeon, 305-700, South Korea*
Email: hyjung@etri.re.kr
[3]*Kyungpook National University, Daegu, 702-700, South Korea*
Email: sjkoh@knu.ac.kr

Abstract: With the recent growth of smart phone services, it is envisioned that *mobile* will be the key driver toward Future Internet (FI). In this paper we present a security enhancement for the Mobile-Oriented Future Internet (MOFI) architecture, which considers mobile nodes as default nodes in FI. The security enhancement proposed here is introduced as a new functional block that extends the architecture with secure identification (SEID) of communication participants. We also analyze the behavior of SEID in terms of the binding update and packet delivery costs.

Keywords: Future Internet, Architecture, Mobility, Security, MOFI

1. Introduction

With the wide popularity of smart phones and general mobile devices (sensor networks), the Internet has rapidly changed from fixed-based to mobile-based. This trend is going to dominate the future, with more than 1.6 billion of 2014, exceeding the number of desktop users [1]. The current Internet model, and its patch-on extensions, is fixed-host centric, so the mobile-based environment is a primary factor to be incorporated to the Future Internet (FI).

Being tightly integrated to the current Internet, the Mobile IP (MIP) [2] and its variants does not fit with this mobile-centric view because they still relay on a fixed-host environment. However, some approaches that provide decoupling of identifier and locator (aka. ID/LOC split) are defined to mitigate this problem. Both the Host Identity Protocol (HIP) [3] and the Locator-Identifier Separation Protocol (LISP) [4], propose to decouple identifiers from locators and provide some handover mechanisms to support mobility but they still consider the network nodes as fixed hosts.

The limitations of the approaches introduced above have caused the appearance of some *clean-slate* approaches. For instance, the AKARI project [5] of the NICT of Japan has defined the HIMALIS architecture [6], which provides ID/LOC split with less footprint than LISP or HIP. However, this proposal also lacks in the specific consideration of mobile nodes by default and in the definition of security and privacy protection, which is starting to be addressed in [7].

On the contrary, as deeply commented in Section 2., the architecture proposed by MOFI [8] is centered around mobile devices, considering mobility the default behavior

of the FI. It is primarily built with three functional blocks: 1) host ID and network LOC, 2) global ID-based communication with local LOC-based delivery in the data plane, and 3) search-based distributed mobility control in the control plane. With them, it builds a architecture with complete separation of control and data planes and integrated mobility and multihoming support. The main limitation we find in this approach is the lack of security. In this paper, we propose to enhance this architecture by the introduction of the secure identification functional block (SEID) that enhances MOFI with identity-based negotiations of networking security aspects, primarily the identification of communication participants (entities), as previously addressed in [9].

The remainder of this article is organized as follows. First, in Section 2. we describe the MOFI architecture. In Section 3. we discuss the integration of SEID over MOFI. In Section 4. we analyze the behavior of SEID, and in Section 5. we conclude the paper and discuss some points about the future work.

2. MOFI Architecture

As commented above, MOFI is designed with three functional blocks. First, the ID-LOC separation with Host Identifier and Network Locator (HINLO) [10] functional block meets with the separation of host identifier from network locator, an essential requirement for FI. In the data plane, the packet delivery is accomplished by Global ID-based communication and Local LOC-based delivery (GIC-LLD) which separates the delivery mechanism of access network (AN) and backbone network. For mobility control, MOFI uses the Search-based Distributed Mobility Control (SDMC) [11] in the control plane, which meets with the FI requirements of separation of control and data delivery functions and the distribution of mobility control.

MOFI basically assumes the host-based communication that is already adopted in current Internet. The Host Identifier and Network Locator (HINLO) functional block is used to support ID/LOC split, in which independent host ID (HID) is employed and separated from locator (LOC).

The mobility control is performed by the Search-based Distributed Mobility Control (SDMC) functional block, which provides search-based and distributed signaling operations based on the distributed mobility management presented in [12]. It naturally implies the separation of control plane from data plane. This search-based mobility control may induce a certain amount of delay for LOC query signaling. However, such an initial signaling delay may be negligible in the session setup phase. In case of handover, the LOC binding will be updated directly between the two concerned ARs for route optimization.

The Global ID Communications and Local LOC Delivery (GIC-LLD) functional block provides the possibility for each host to have a global HID with several LOCs used for packet delivery in each network. Each LOC is used locally in the networks, without any assumption on global uniqueness. In GIC-LLD, the packet delivery operations have two stages, i.e. access networks and backbone. On it, communication between two hosts is performed with HIDs, whereas LOCs are used for packet delivery inside the Access Network (AN) and through the Internet backbone. The SDMC control operation is used to find appropriate LOC for each HID in each network.

3. Secure Identification (SEID) over MOFI

Due to the security limitations we find in MOFI we propose to integrate it a new functional block, the secure identification (SEID). It is responsible to securely mediate in the resolution of HIDs from host names (or identities) and the resolution of LOCs from HIDs. With it, networked entities can be securely identified by means of their digital identity but, if specified in their security policies, entities can communicate without revealing any information about their true identity, not even their activities, so they cannot be traceable. This is the normal operation of SEID, so even when communications are not encrypted, it prevents the traceability and provides attribute-based negotiation of sessions to enhance privacy. Also, when desired, an entity may change its HID to prevent session linkability.

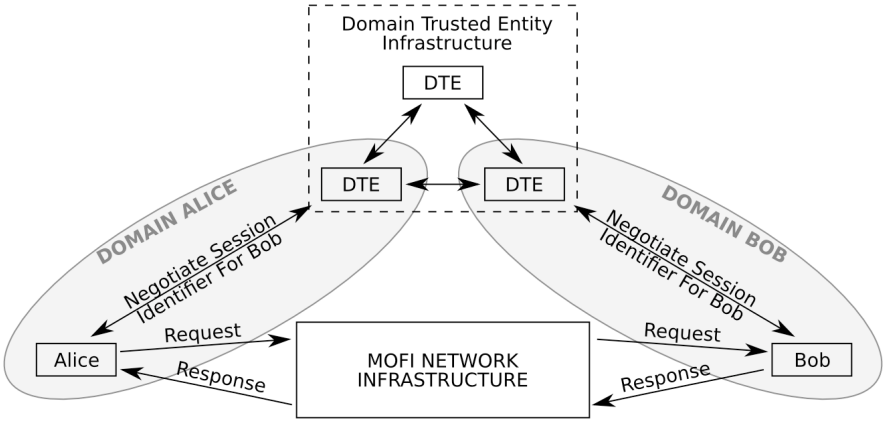

Figure 1: Domain Trusted Entity Infrastructure for secure identification

The basic mechanism behind SEID is the identity plane, a security-oriented and identity-based control plane, which, as shown in Figure 1, is built with the Domain Trusted Entity Infrastructure (DTEi) [13, 14] described below. It can be used by any network entity, both communication participants and infrastructure elements to negotiate network security parameters while protecting their identities.

The DTEi is a network infrastructure that keeps and protects the identities of communication participants while allowing the identity-based negotiations of the security aspects of communications. In order to get a full coverage of the identity space, we propose to deploy a different element in each administrative (identity) or network domain, connected to the distributed overlay network that forms the DTEi. In summary, the DTEi is therefore a completely distributed system to securely and privately manage the identity information of the several entities taking part of the communications.

The functionality provided by the DTEi is then used to define a new control plane, the identity plane, to negotiate many aspects of the network, such as the permissions of a communications to cross a network, the establishment of security associations, etc. Figure 2 shows the shape of the DTEi and its interactions. On the left it depicts how DTEi is formed from different elements connected in a overlay ring to form the infrastructure and indicates how to connect it with other architectures, such as MOFI, the architecture we are considering in this paper. On the right side it shows the basic

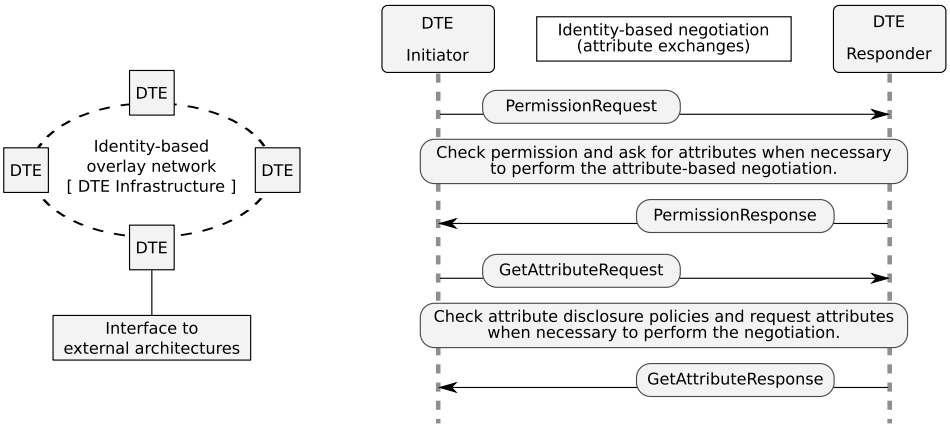

Figure 2: Overview of Domain Trusted Entity Infrastructure (DTEi) and message exchanges

message exchanges used in security negotiations. Below we describe the most important aspects of the DTEi.

3.0.1 Overlay Network

As commented above, the DTE infrastructure is composed by many DTE instances connected to form an overlay network. This way, the whole infrastructure is totally distributed and the instances can reach each other without even knowing their underlying identifiers or addresses. There are many ways to build the overlay network, we decided to use the routing algorithm found in Chord [15], because its simplicity, and improved with LPRS [16].

3.0.2 Operations

The main operations supported by the DTE infrastructure are, as commented above, the identity-based negotiations. We support two types of negotiations: the permission request to access a resource and the attribute request to obtain the value of an attribute from an entity. Both operations can use the attribute query when required by policies, that is, attribute requests from a responder to an initiator can be used anytime during a negotiation. The permission request operation is used to perform an attribute-based authorization procedure and get access to a resource that is represented by an identity while the attribute request is used to perform a plain attribute-based negotiation.

3.0.3 Authentication and Security

The negotiations performed by the DTEs are delicate and they must be conducted in a secure way and under mutual authentication of the parties taking part of the negotiation, so they can be sure that those parties are who claim to be and no other entity can see any exchange of their negotiations.

In order to achieve the mutual authentication in a fast and reliable way we propose to use only one exchange (round-trip) and be based on digital (public key) certificates of the DTEs that communicate. To be sure this is performed in a trusted manner, we propose to trust only in the entities that hold the private key of certificates issued/signed by a trusted certification authority (CA), like in X.509 used by Private Key Infrastructures (PKIs), or certificates signed by itself or by N trusted entities, like in the Web of Trust concept used by PGP. The two models denote the centralized and decentralized (distributed) trust models.

4. Analysis

To analyze the performance of the Secure Identification (SEID) approach, we compare the behavior of the MOFI architecture with SEID over MOFI. In order to facilitate the analysis we build a mathematical model of both approaches. As the mobility is an essential part of the architecture, the model includes the binding update cost (BUC) together with the packet delivery cost (PDC), so the total cost (TC) is represented as $TC = BUC + PDC$. The importance of the comparison is because, in SEID over MOFI, the ARs need to also update the DTE infrastructure, so the BUC is of the SEID approach is slightly increased. It adds a new control exchange that logarithmically depends on the number of ARs deployed in the network.

To build the equations of the model we use the following parameters: 1) P_k is the processing cost for binding update or location lookup at node k, which is proportional to the number of active hosts in the domain. This can apply to P_{AR} and P_{HA}; 2) $T_{\text{a-b}}$ is the transmission cost of a packet between two nodes (a and b) in the network, which is proportional to the number of hops between the concerned two nodes. This can apply to $T_{\text{MN-AR}}$, $T_{\text{AR-HA}}$, and $T_{\text{AR-AR}}$; 3) α is the unit cost of packet transmission per hop; 4) β is the unit cost of location binding or lookup per database entry; 5) $H_{\text{a-b}}$ is the hop count between nodes a and b in the network; 6) N_{AR} is the number of ARs in the network; 7) $N_{\text{Host/AR}}$ is the number of hosts per AR; 8) S_{control} is the size of a control packet; 9) Finally, S_{data} is the size of a data packet.

The SEID functional block differentiates between host DTE and visited DTE. So, there are two different variables to measure: local BUC and remote BUC, whose equations are as follows:

$$\begin{aligned} &BUC_{\text{MOFI+SEID-local}} = \\ &= S_{\text{control}} \times 2T_{\text{MN-AR}} + S_{\text{control}} \times 2T_{\text{AR-DTE}} + P_{\text{DTE}} \\ &= S_{\text{control}} \times 2\alpha(H_{\text{MN-AR}} + H_{\text{AR-DTE}}) + \beta(N_{\text{Host/AR}}). \end{aligned} \tag{1}$$

$$\begin{aligned} &BUC_{\text{MOFI+SEID-remote}} = \\ &= S_{\text{control}} \times 2T_{\text{MN-AR}} + S_{\text{control}} \times 2T_{\text{AR-DTE}} + S_{\text{control}} \times 4T_{\text{DTE-DTE}} + 2P_{\text{DTE}} \\ &= S_{\text{control}} \times 2\alpha(H_{\text{MN-AR}} + H_{\text{AR-DTE}} + 2[H_{\text{DTE-DTE}} \times log_2(H_{\text{AR}})]) + 2\beta(N_{\text{Host/AR}}). \end{aligned} \tag{2}$$

The packet delivery cost of SEID over MOFI also involves the communication through DTEi to perform the attribute-based negotiation, which is necessary to enhance privacy and security requirements to the communication, as well as to reveal the actual locator (LOC) of a node. It also differentiates between local and remove operations. Thus, the PDC can be obtained as follows:

$$\begin{aligned} &PDC_{\text{MOFI+SEID-local}} = \\ &= S_{\text{data}} \times T_{\text{CN-AR}} + S_{\text{control}} \times 2T_{\text{AR-DTE}} + S_{\text{control}} \times 4T_{\text{DTE-DTE}} + 2P_{\text{DTE}} + \\ &+ S_{\text{control}} \times 2T_{\text{AR-DTE}} + S_{\text{data}} \times T_{\text{AR-AR}} + S_{\text{data}} \times T_{\text{MN-AR}} \\ &= S_{\text{data}} \times \alpha H_{\text{CN-AR}} + S_{\text{control}} \times 2\alpha H_{\text{AR-DTE}} + S_{\text{control}} \times 4\alpha H_{\text{DTE-DTE}} \times log_2(N_{\text{AR}}) + \\ &+ 2\beta(N_{\text{Host/AR}}) + S_{\text{control}} \times 2\alpha H_{\text{AR-DTE}} + S_{\text{data}} \times \alpha H_{\text{AR-AR}} + S_{\text{data}} \times \alpha H_{\text{MN-AR}}. \end{aligned} \tag{3}$$

$$
\begin{aligned}
&PDC_{\text{MOFI+SEID-remote}} = \\
&= S_{\text{data}} \times T_{\text{CN-AR}} + S_{\text{control}} \times 2T_{\text{AR-DTE}} + S_{\text{control}} \times 4T_{\text{DTE-DTE}} + 2P_{\text{DTE}} + \\
&+ S_{\text{control}} \times 2T_{\text{DTE-DTE}} + P_{\text{DTE}} + S_{\text{control}} \times 2T_{\text{AR-DTE}} + S_{\text{data}} \times T_{\text{AR-AR}} + S_{\text{data}} \times T_{\text{MN-AR}} \\
&= S_{\text{data}} \times \alpha H_{\text{CN-AR}} + S_{\text{control}} \times 2\alpha H_{\text{AR-DTE}} + S_{\text{control}} \times 4\alpha H_{\text{DTE-DTE}} \times log_2(N_{\text{AR}}) + \\
&+ 2\beta(N_{\text{Host/AR}}) + S_{\text{control}} \times 2\alpha H_{\text{DTE-DTE}} \times log_2(N_{\text{AR}}) + \beta(N_{\text{Host/AR}}) + \\
&+ S_{\text{control}} \times 2\alpha H_{\text{AR-DTE}} + S_{\text{data}} \times \alpha H_{\text{AR-AR}} + S_{\text{data}} \times \alpha H_{\text{MN-AR}}.
\end{aligned}
\tag{4}
$$

Based on the above equations, we have two different variables for the total cost of the security enhancements (SEID) of MOFI, they are:

$$
\begin{aligned}
TC_{\text{MOFI+SEID-local}} &= BUC_{\text{MOFI+SEID-local}} + PDC_{\text{MOFI+SEID-local}} \\
TC_{\text{MOFI+SEID-remote}} &= BUC_{\text{MOFI+SEID-remote}} + PDC_{\text{MOFI+SEID-remote}}
\end{aligned}
\tag{5}
$$

Once the above equations are formulated, we set the parameters to typical values, as used in [10], which are as follows: $N_{\text{Host/AR}} = 100$ (range from 10 to 1000), $N_{\text{AR}} = 10$ (range from 10 to 100), $H_{\text{AR-AR}} = 3$, $H_{\text{DTE-DTE}} = 3$, $\alpha = 0.5ms$, $\beta = 0.2ms$, $H_{\text{MN-AR}} = 1$, $H_{\text{CN-AR}} = 1$, $H_{\text{AR-DTE}} = 1$, $S_{\text{data}} = 1024$ (bytes), and $S_{\text{control}} = 1024$ (bytes).

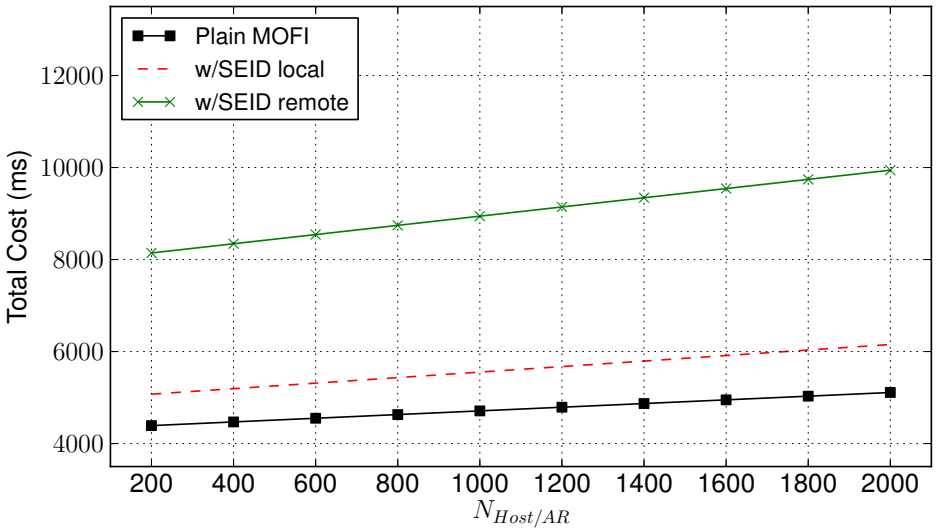

Figure 3: Analysis results for the variation of $N_{\text{Host/AR}}$ for the equations of SEID over MOFI in comparison with MOFI.

In Figure 3 we can see that SEID approach adds a little overhead to MOFI and remains constant, independently of the value of the number of hosts per AR. In contrast, in Figure 4 we see that SEID over MOFI grows logarithmically because it only involves the necessary ARs to build the DTE overlay network.

5. Conclusions and Future Work

The *mobility* is the most envisioned feature in Future Internet (FI) but the current Internet was originally designed for fixed networks. In this paper we presented the

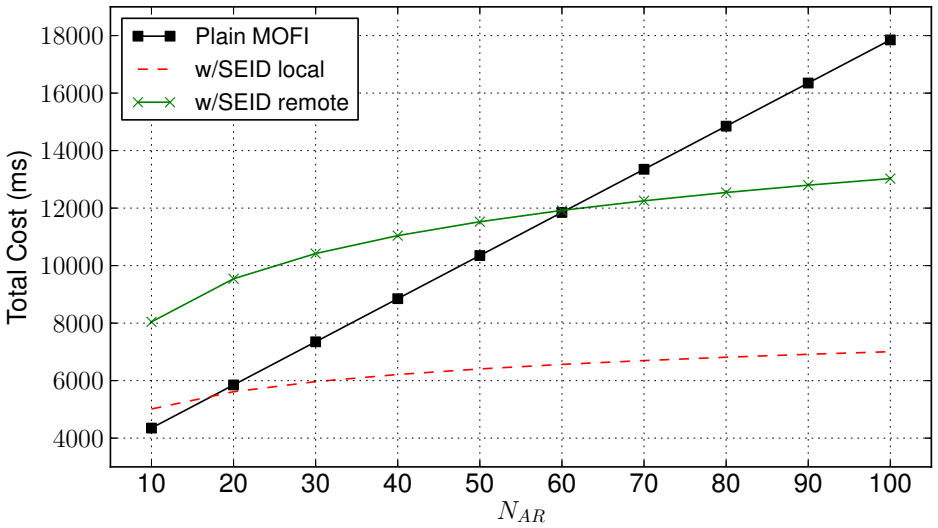

Figure 4: Analysis results for the variation of N_{AR} for the equations of SEID over MOFI in comparison with MOFI.

security enhancement of MOFI, a new architecture for FI that considers mobile nodes as the default case and which provides a set of distinctive features. However, it is difficult to achieve many security requirements in the current Internet because security was not considered at design time. Thus, we propose to enhance MOFI with the SEID functional block built with the DTE infrastructure [13, 14], a security oriented infrastructure that provides the identity-based negotiation of security aspects. We also analyzed the impact of the secure identification functional component to show its performance behavior and found it feasible for a FI architecture.

For future work, we propose to continue with the security integration, as shown in [14] and the interaction with other network architectures for FI, as shown in [7].

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, and by the Program for Research Groups of Excellence of the Sneca Foundation under grant 04552/GERM/06.

References

[1] M. Stanley, "Report on Internet Trends," 2010. `http://www.morganstanley.com/institutional/techresearch/pdfs/Internet_Trends_041210.pdf`.

[2] C. Perkins *et al.*, "IP Mobility Support for IPv4," 2002. `http://www.ietf.org/rfc/rfc3344.txt`.

[3] J. Laganier *et al.*, "Host Identity Protocol (HIP) Rendezvous Extension," 2008. `http://www.ietf.org/rfc/rfc5204.txt`.

[4] D. Farinacci, V. Fuller, D. Meyer, and D. Lewis, "Locator/id separation protocol (LISP)," internet-draft, IETF, 2011.

[5] National Institute of Information and Communications Technology, ""AKARI" Architecture Design Project for New Generation Network," 2010. `http://akari-project.nict.go.jp`.

[6] V. P. Kafle and M. Inoue, "HIMALIS: Heterogeneity inclusion and mobility adaptation through locator id separation in new generation network," *IEICE Transactions on Communications*, vol. E93-B, no. 3, pp. 478–489, 2010.

[7] P. Martinez-Julia, A. F. Gomez-Skarmeta, V. P. Kafle, and M. Inoue, "Secure and robust framework for id/locator mapping system," *IEICE Transactions on Information and Systems*, vol. E95-D, no. 1, pp. 108–116, 2012.

[8] "Mobile Oriented Future Internet (MOFI)," 2011. `http://www.mofi.re.kr`.

[9] 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.

[10] H. JUNG and S. J. KOH, "Hinlo: An id/loc split scheme for mobile oriented future internet," in *Proceedings of the Future Network and Mobile Summit 2011*, pp. 1–8, International Information Management Corporation, 2011.

[11] H. Jung, M. Gohar, J.-I. Kim, and S. J. Koh, "Distributed mobility control in proxy mobile ipv6 networks," *IEICE Transactions on Communications*, vol. E94-B, no. 8, pp. 2216–2224, 2011.

[12] H. Chan *et al.*, "Problem statement for distributed and dynamic mobility management," internet-draft, IETF, 2011.

[13] P. Martinez-Julia and A. F. Gomez-Skarmeta, "Secure identity-to-identity communications over content-centric networking," in *Proceedings of the 4th IEEE International Conference on Internet Multimedia Systems Architecture and Applications*, (Washington, DC, USA), pp. 1–6, IEEE, 2010.

[14] P. Martinez-Julia, A. F. Gomez-Skarmeta, J. Girao, and A. Sarma, "Protecting digital identities in future networks," in *Proceedings of the Future Network and Mobile Summit 2011*, pp. 1–8, International Information Management Corporation, 2011.

[15] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in *Proceedings of the 2001 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, (New York, NY, USA), pp. 149–160, ACM, 2001.

[16] H. Zhang, A. Goel, and R. Govindan, "Incrementally improving lookup latency in distributed hash table systems," in *Proceedings of the 2003 ACM SIGMETRICS International Conference on Measurement and Modeling of Computer Systems*, (New York, NY, USA), pp. 114–125, ACM, 2003.