Mobile Information Systems 10 (2014) 37–77
DOI 10.3233/MIS-130171
IOS Press

Lightweight MIPv6 with IPSec support

A mobility protocol for enabling transparent IPv6 mobility in the Internet of Things with support to the security

Antonio J. Jara*, David Fernandez, Pablo Lopez, Miguel A. Zamora and Antonio F. Skarmeta
Clinical Technology Lab (CLITech), Research Institute for Oriented Information and Communications Technologies, Computer Sciences Faculty, University of Murcia, Regional Campus of International Excellence Campus Mare Nostrum, Murcia, Spain

Abstract. Mobility management is a desired feature for the emerging Internet of Things (IoT). Mobility aware solutions increase the connectivity and enhance adaptability to changes of the location and infrastructure. IoT is enabling a new generation of dynamic ecosystems in environments such as smart cities and hospitals. Dynamic ecosystems require ubiquitous access to Internet, seamless handover, flexible roaming policies, and an interoperable mobility protocol with existing Internet infrastructure. These features are challenges for IoT devices, which are usually constrained devices with low memory, processing, communication and energy capabilities. This work presents an analysis of the requirements and desirable features for the mobility support in the IoT, and proposes an efficient solution for constrained environments based on Mobile IPv6 and IPSec. Compatibility with IPv6-existing protocols has been considered a major requirement in order to offer scalable and inter-domain solutions that were not limited to specific application domains in order to enable a new generation of application and services over Internet-enabled dynamic ecosystems, and security support based on IPSec has been also considered, since dynamic ecosystems present several challenges in terms of security and privacy. This work has, on the one hand, analysed suitability of Mobile IPv6 and IPSec for constrained devices, and on the other hand, analysed, designed, developed and evaluated a lightweight version of Mobile IPv6 and IPSec. The proposed solution of lightweight Mobile IPv6 with IPSec is aware of the requirements of the IoT and presents the best solution for dynamic ecosystems in terms of efficiency and security adapted to IoT-devices capabilities. This presents concerns in terms of higher overhead and memory requirements. But, it is proofed and concluded that even when higher memory is required and major overhead is presented, the integration of Mobile IPv6 and IPSec for constrained devices is feasible.

Keywords: Internet of Things. mobility, IPv6, Mobile IPv6, IPSec, lightweight, smart cities, hospital wireless sensor networks, handover

1. Introduction

Future Internet presents a more ubiquitous and mobile Internet. Mobility support is increasing the applicability of Future Internet to new areas. Mobile platforms such as smart phones and tablets are enabling a tremendous range of applications based on ubiquitous location, context awareness, social networking, and interaction with the environment [3].

The potential of the Future Internet is not limited to smart phones. *Internet of Things* (IoT) is another emerging area of the Future Internet, which is offering a higher integration of the cybernetic and

*Corresponding author: Antonio J. Jara, Clinical Technology Lab (CLITech), Research Institute for Oriented Information and Communications Technologies, Computer Sciences Faculty, University of Murcia, Regional Campus of International Excellence Campus Mare Nostrum, Murcia, Spain. Tel.: +34 868 88 87 71; Fax: +34 868 88 41 51; E-mail: jara@um.es.

physical world. The main goals from the IoT is to collect data from the real-world entities and events. Many entities may move around in a real world environment, thus making the IoT devices attached to them mobile. Thus, handling mobility and dynamic systems is a key requirement for IoT solutions and consequently adequate support needs to be provided.

Specifically, the challenge is the provisioning of adequate mobility management to control and exploit realistic mobility of both IoT devices and real world entities. Some dynamic ecosystem where mobility management is required are the *Smart Cities* [7] and *Hospital Wireless Sensor Networks (HWSN)* [5,6], which are being extended with the integration of sensors and smart devices.

Smart cities present infrastructure that is being enabled with Internet connectivity, such as street lights [30], parking lots, smart banners, and traffic lights. Mobility management is required since citizens and transport are dynamic. Therefore, services based on geo-location and context awareness require a continuous connectivity through the existing metropolitan WiFi networks and emerging IEEE 802.15.4 networks from the mentioned infrastructure. For example, some projects such as *SmartSantander* in Spain have deployed a IEEE 802.15.4 infrastructure to empower transport and citizens [2]. Another example of *Smart Mobility* in smart cities is being developed by the project *BUTLER* [1], this optimizes the travel time based on external information from the public transport system and the personal location and information integrated into mobile applications. This kind of solutions are enabling new ways to interact, plan, and live in a smart life ecosystem.

Mobility management in hospitals is required since clinical devices can be connected through wireless technologies. Mobility offers highly valuable features such as higher quality of experiences for the patients, since it allows to the patients move freely, continuous monitoring through portable and wearable sensors, extends the coverage to all the hospital, and finally a higher fault tolerance since the mobility management allows to adapt dynamically the connection to different access points. Therefore, HWSNs is one of the main scenarios where the mobility for the IoT-based applications exploit these capabilities. On the one hand, fault tolerance influences directly in the life support. On the other hand, continuous monitoring influences in the quantity of data available which is required for real-time diagnostic with algorithms such as YOAPY [12].

Such as described, both scenarios present different requirements since, on the one hand, smart cities are offering an inter-domain mobility scenario where the Wireless Internet Service Providers (WISP) will be heterogeneous and consequently the addressing spaces will be distributed, and on the other hand, HWSNs present an inter-domain scenario where even when multiple access points are deployed in the hospital campus, it is defined a single domain. Therefore, the addressing space is common.

Finally, in a smart life environment, it could be addressed scenarios that mix the smart cities with the HWSNs, one example of use case is the extension to the ambulances, where the ambulance is a mobile network dependent on the gateways available around the city, and finally when the ambulance arrives to the hospital, then patient's sensors are connected to the hospital wireless network and re-assigned to the hospital domain.

IoT capabilities enable this evolution of the ecosystems to dynamic and connected environments in order to offer new high level services such as continuous monitoring. Finally, it could be considered end-to-end scenarios such as a H2H (Home to Hospital) solution where the patients are monitored in their home domain with a set wearable sensors, they continue connected in the ambulance and finally they are monitored in the hospital.

This kind of scenarios are desirable for the capabilities of the Future Internet and IoT in an horizon 2020. The challenges to reach this wide scenario that cover multiple domains and require interoperability among different entities can be distinguished into two families, on the one hand, the requirements based on governance and policies management which are out of the scope from the scientific point of view, and on the other hand, the requirements based on technical aspects to reach a common addressing space, inter-domain handover method, and finally satisfies the constraints from the IoT devices in terms of power consumption, computation, communication, memory footprint, and number of messages.

The proposed solution has taken into account the mentioned constrains of the IoT environments, for integrating Mobile IPv6 (MIPv6) [13], since Mobile IPv6 is not initially feasible for the constraints of the IoT devices [14], this solution has proposed a lightweight version of MIPv6. Lightweight MIPv6 has been properly integrated into constrained devices and has been evaluated its compatible with the Mobile IPv6 (MIPv6) protocol.

The compatibility with the existing Mobile IPv6 implementation has been considered the main major requirement, since IPv6 provides the basis for Future Internet and IoT, due to its homogeneous and large address space, the huge leverage in existing protocols and support by the current hardware, platforms and operating systems to support IPv6. For that reason, IPv6 compatibility has been considered for the design and development of the proposed protocol in order to build dynamic ecosystems with the same flexibility, scalability and potential of Internet.

Mobility management brings several vulnerabilities, since this requires the validation of a mobile node from an unknown network with an unknown IPv6 address (the new IPv6 address in the visited network). Therefore, the validation of the mobile node identity, the management of security associations between the mobile node and the base station, and finally the protection of the mobility control messages are also major requirements to build the mentioned dynamic ecosystems. For that reason, this work has also addressed the support for the security.

Mobile IPv6 relies on IP Security (IPSec) security protocol to protect the communication between the mobile node and the base station (called in the MIPv6 protocol Home Agent). IPSec was considered unsuitable for constrained devices in [17], for that reason, this works has also carried out a lightweight implementation and integration of IPSec in order to make it feasible for constrained devices and compatible with existing IPSec implementations.

Mobile IPv6 and IPSec have been analysed, implemented a lightweight version for constrained devices, and finally evaluated in terms of memory footprint, overhead, handover latency, and communications costs.

This work is structured as follows. Section 2 presents the integration of IPv6 technologies to build the IoT. This analyses he background in mobility protocols for Wireless Sensor Networks (WSNs) in Section 3. Section 4 analyses the requirements and design issues for the mobility management in the IoT. Section 5 analyses the MIPv6 protocol and its requirements. Sections 6 and 7 describe the lightweight approach of MIPv6 and IPSec proposed in this work to support dynamic ecosystems. Section 8 evaluates the solution with an experimental analysis, we have focused on an empiric approach instead of simulations/emulations, since they are most suitable for the analysis, of the impact, performance and memory footprint, over constrained devices and light. Section 9 analyses the other approaches to offer mobility support in IPv6 networks. Finally, Section 10 concludes this paper.

2. Internet of Things and IPv6

The number of devices that are connected to the Internet is growing exponentially. This has led to define a new conception of Internet, the commonly called Future Internet, which started with a new version of the Internet Protocol (IPv6) that extends the addressing space in order to support all the emerging Internet-enabled devices.

IPv6 has been designed to provide secure communications to users and mobility for all the devices attached to the user; thereby users can be always connected.

IPv6 features are what have made possible to think about to connect all the objects and build the IoT. The objective of IoT is the integration and unification of all communications systems that surround us. Hence, the systems can get a control and access total to the other systems for leading to provide ubiquitous communication and computing with the purpose of defining a new generation of services.

IoT is enabled by tiny and highly constrained devices, so-called smart objects. These devices have low-performance properties due to their constraints in terms of memory capacity, computation capability and energy autonomy. In addition, their communication capabilities present a low bandwidth, limited reachability because the usage of hard duty cycles and consequently unstable connectivity for solution with a very low duty cycle and high power constraint.

These devices with constrained connectivity and communication capacity are what we can find, since some years ago, in the Low-power Wireless Personal Area Networks (LoWPANs).

Recently, the IETF working group has defined IPv6 over that LoWPANs (6LoWPAN) to extend Internet to smart devices. 6LoWPAN offers to the LoWPANs all the advantages from IP such as scalability, flexibility, tested, extended, ubiquitous, open, and end-to-end connectivity.

It could be considered that 6LoWPAN devices are also empowered with IP protocols, i.e., protocol for mobility such as MIPv6, and management such as SNMP, security such as IPSec. However, it is not feasible for the 6LoWPAN devices to be associated with host based protocols because 6LoWPAN nodes are energy and resource constrained; host based protocols require most of the signalling on end nodes and because the design features of 6LoWPAN network were not considered in the design issues of the host based protocols. For example, a 6LoWPAN node may run out of energy causing a fault in the network, this has restriction in size packets and this presents aggressive techniques to conserve energy by using of sleep schedules with long sleep periods (e.g., the node just wake up to receive IPv6 signalling messages). These features introduce delays in the reception of messages because they are not attended until that the node wakes up. Therefore, these delays, power restrictions, packet size restrictions, etc., are not considered in the current host based IPv6 protocols.

For the mentioned differences between IPv6 design issues and IoT-devices capabilities is what has led during the last years to empower these constrained devices with the protocols and functions of Internet-enabled devices.

Table 1 presents the mapping to lightweight implementations and versions of the existing protocols, that continue being interoperable/translatable to the full implementations. For that purpose, it has been developed lightweight implementations of the IP stack such as uIP and header compression through the 6LoWPAN protocol [32] in order to reach Internet connectivity, Web Services through RESTFul architecture with also lightweight and compressed protocols such as the Constrained Application Protocol (CoAP) [20], and recently the management of constrained networks and devices (COMAN) [31] as an alternative to the Simple Network Management Protocol (SNMP).

This work is focused on provide mobility management with security support for the IoT, in order to continue evolving the integration of the IoT in Internet. Mobility has been chosen for our research, since it is one of the most important issues in the Future Internet.

3. Mobility protocol trends

Mobility is one of the major issues of the Future Internet. Mobility is solved in different ways, they are split into two trends, one the one hand, a trend based on an evolutionary research following the

Table 1
Lightweight protocols implemented for the IoT.

Protocol	Full version	Lightweight	Description
IPv6	IPv6 (RFC 2460)	uIP (Contiki OS) 6LoWPAN (RFC 6282) GLoWBAL IPv6 [28]	Internet prot ocol
Neighbor discovery	ND (RFC 2461)	ND for 6LoWPAN (RFC 6775)	Auto-configuration
RESTFul	HTTP (RFC 2616)	CoAP [20,33]	Web services
SNMP	SNMP (RFC 5590)	COMAN [31]	Network management
DNS	DNS / mDNS [39]	CoAP Service Discovery [27] lmDNS [40]	Service Discovery

IPv6-based approach and current Internet architecture, and on the other hand, a clean-slate trend, where new architectures that require major changes in the existing protocols and networking philosophy are proposed.

The clean-slate trend is based on new concepts such as identifier and locator split architectures such as the presented in [18]. This kind of architectures presents the advantage that mobility is directly supported by the separation of the session identification with the locator of the device, which is the problem of the current Internet architecture. Previous works for the IoT has been focused on this approach, the main issue is that the overhead for 6LoWPAN devices increase since the need to transport one additional header for the identification layer. This type of solutions are very relevant from the research point of view, but they present the main inconvenient that they are not feasible in a sort term, since the current deployed hardware and infrastructure is not ready for this kind of approach.

For that reason, this work is focused on the evolutionary research approach. This follows the current Internet architecture for the management of the identification and location, i.e. IPv6 continues being used for *Identification* of the session in the transport and application layers, and *Locator* of the devices for routing in the network layer. These solutions allow to continue using the existing infrastructure and overcome the problem using a similar concept to the identifier/locator split but in an implicit way. Specifically, the main protocol following the evolutionary approach is Mobile IPv6 (MIPv6). MIPv6 uses two IPv6 addresses, on the one hand, the initial address of the device, commonly denominated Home Address is used as identifier, and the new address in the visited network, commonly called care-of address, is used as locator.

MIPv6 protocol provides the signalling messages and IPv6 headers extensions to manage the binding between these two addresses. In addition, this defines the security mechanisms and networking requirements in order to avoid the identity supplantation and man in the middle attacks. Specifically, this defines return routability mechanism to carry out route optimization in order to avoid triangle routing and IPSec tunnelling between the mobile node and the home agent. Thereby, security and authentication of the mobile node for the binding updates, when the node needs to register a new care of address, is ensured.

The main functions of MIPv6 are covered by the home agent, which is the entity in charge of manage the identifier, cache packets when the mobile node is in transit, and demonstrate the authenticity of the mobile node when the mobile node claim its identity from a visited network.

In previous works, we have evaluated the feasibility of Mobile IPv6 for constrained devices such as the considered for the IoT [14]. These works concluded that MIPv6 presents a high overhead for the data packets when the mobile node is in roaming, since this needs to include the destination option to specify its home address in case of route optimization applied or build an IPv6 tunnel which requires an additional IPv6 header. Both cases require a high overhead.

The second problem with Mobile IPv6 is that IPSec is mandatory in order to protect the communications between the mobile node and the home agent. Such as mentioned, the trust relationship between the mobile node and the home agent is a fundamental requirement of MIPv6, since all the security of the binding update for the mapping between the care-of address and home address, and additional security processes such as the return routability for the route optimization are based on this trust relationship.

Therefore, the lightweight implementation of MIPv6 for the IoT is not so simple as carry out a header compression and reduction of the size for the signalling control messages as previously defined for other protocols such as IPv6 with 6LoWPAN and HTTP with CoAP. Important changes are required to solve the challenges from the emerging infrastructure deployed for the IoT. Specifically, this change of infrastructure for the IoT is the mentioned introduction of highly constrained devices in Internet in the level where usually were deployed nodes with high capabilities such as laptops, PCs and servers. Therefore, the evolution from a current infrastructure of end hosts with high capabilities, and gateways/routers with also high capabilities, to an infrastructure where the end nodes are a large number of constrained devices, and border routers with high capabilities. In addition, these emerging Internet-enabled devices require additional self-* properties in order to support the required scalability and autonomy to support dynamic environments.

The next sections present the design issues for the lightweight version of MIPv6 and the proposed solution to offer a secure and efficient mobility management for the IoT.

4. Design issues

The following items present the requirements for the design of a mobility management protocol that satisfies the requirements from dynamic ecosystems and that is aware of the constraints from the devices used to build the IoT ecosystems.

Each scenario presents different requirements and challenges. But all of them present the common goal of reaching a seamless handover ensuring the security and a suitable efficiency.

These design issues have been defined considering the requirements from emerging scenarios such as smart cities, HWSNs and health monitoring in critical environments from previous works [4,54].

- *Global identifier:* End devices need to be reachable globally by any other entity connected to Internet. Thereby, end-to-end connectivity can be offered, which is a foundation of IPv6, Future Internet and IoT [35,54].
- *IPv6-based protocol:* Mobility management for IoT needs to be built over Internet protocols, such as Mobile IPv6 (MIPv6). Even when they are not implementing all the functions of the host-based IPv6 protocol. Thereby, it is offered an evolutive approach for the IoT that can be integrated with the existing Internet-based software and infrastructure.
- *Lightweight protocol:* Mobility management protocol needs to consider similar lightweight considerations and implementation guidelines that have been already taking into account for 6LoWPAN and CoAP. Thereby, mobility management can be integrated into constrained devices with low memory capabilities [19]. Anyway, such as it has been mentioned the requirements from MIPv6 are higher that 6LoWPAN and CoAP, since MIPv6 is presenting additional security requirements and an overhead for all the data packets during the roaming.
- *Communication cost:* Mobility headers and related signalling must be optimized to reduce the impact in the power consumption and overhead ratio. Specifically, signalling messages should fit within a single frame to avoid fragmentation [54]. In addition, broadcast and multicast usage should be reduced since smart objects have a low duty cycle, and consequently the impact in power consumption of these kind of communications arise additional challenges.

The overhead impact needs to be reduced mainly for the data communication which needs to include an additional IPv6 header (tunnelled packets through the home agent) or the destination option (when route optimization is applied and the communication can be directly established with the correspondent node).

Regarding the other binding-related messages, they are not presenting a major challenge, since they require less than a frame. The unique issue that could cause fragmentation for these messages is the usage of piggyback payload packets on the binding-related messages, but this technique is not usually applied in the mobility signalling.

- *Packet encapsulation:* Packet encapsulation used by Mobile IPv6 (when tunnelling packets between a mobile node and its home agent) reduces the frame size left for data and thus may generate fragmentation. For that reason, new challenges arise for enabling mobility management in this kind of devices in order to reduce the overhead from Mobile IPv6 for data packets.
- *Security:* Node authentication and authorization must be supported to offer security capability, ensure protection of the resources, integrity and confidentiality of the information.

  Many security challenges exist in dynamic IoT ecosystems, mainly due to the resource constraints of mobile users, the authentication delay constraint, and the demanding security requirements of applications when the nodes are in roaming, i.e. visiting foreign networks.
- *Movement detection:* Mobile IPv6 relies on neighbour discovery for movement detection and care-of address creation. This movement detection, based on neighbour discovery, is very slow since it depends on the router advertisement frequency. Therefore, it is not effective in wireless networks when different channels is used for different LoWPANS.

  Solutions for movement detection can be optimized for specific use cases, for example in HWSNs where continuous monitoring generates continuous and periodical traffic. These traffic can be used for the RSSI evolution analysis and consequently avoid the usage of extra signalling messages, some example of this kind of movement detection techniques has been presented in [4].

5. Mobility management for the internet of things

The proposed mobility management protocol needs to offer a high efficiency in terms of low computation complexity and communication cost, but at the same time, this needs to be compatible with the existing IPv6 infrastructure and offer a suitable security level. Figure 1 presents the main metrics for the mobility management protocol for the IoT and its relation with the solutions proposed and evaluated in this work.

The integration and interoperability with the existing infrastructure is one of main requirements for mobility management in dynamic ecosystems, since mobile nodes require the capability to use other networks during the roaming, i.e., during the time that they are out of the home network. For that reason, it is important to offer a solution compatible with the available access points and routers.

The security is a high requirement for mobility, since this offers the capability to redirect traffic to a new address (the care-of address), and claim the identity of a node. Therefore, these both features open a high number of vulnerabilities for man in the middle attacks, identity supplantation, and data integrity. In order to avoid these vulnerabilities, it is required the authentication of the mobile node. In Mobile IPv6, it is carried out with the trust relationship between the mobile node and its home agent.

Efficiency is always a desirable feature, but in the IoT is a mandatory feature, since this marks the difference between solutions suitable for the constrained capabilities of the devices of the IoT solutions, and solutions not suitable.

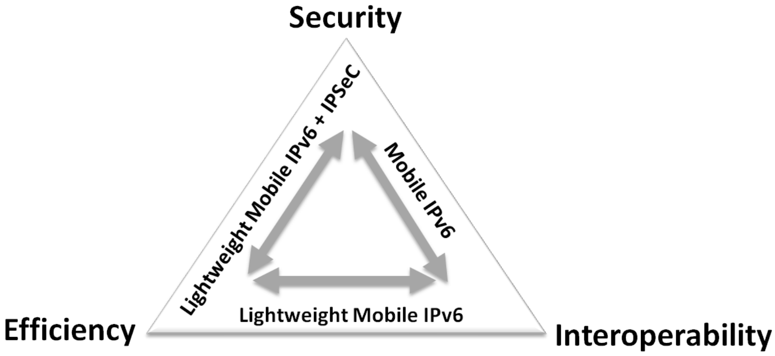


Fig. 1. Metrics triangle for the different mobility support solutions over 6LoWPAN.

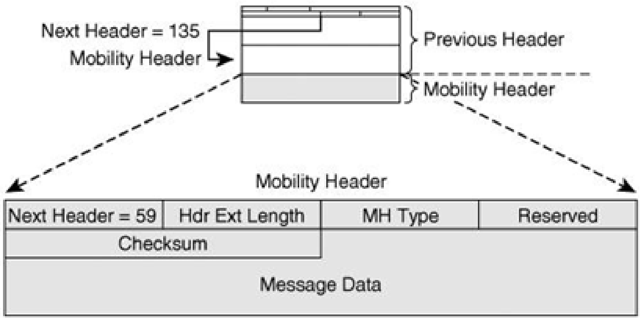


Fig. 2. Mobile IPv6 packet format.

An optimal solution satisfying the three described metrics cannot be defined for IoT environments with the existing solutions and protocols, since the unsuitability of the full Mobile IPv6 protocol and the lack of standardization for new proposals. For that reason, this work analyses the three approaches and discusses each one in function of the scenario requirements.

The following subsections present the approaches evaluated in this work. First, it is analysed Mobile IPv6 since this offers a high integration. The main problem of Mobile IPv6 is that presents requirements which make it unsuitable for constrained devices. For that reason, it is presented a lightweight version of Mobile IPv6, which presents a higher efficiency for IoT environments and maintains the interoperability with the original Mobile IPv6 protocol. Finally, lightweight Mobility support with security support (i.e., IPSec) is analysed, following the requirements and design considerations of Mobile IPv6.

5.1. Mobile IPv6

Mobile IPv6 offers an extension header for the IPv6 protocol to support the binding management. Figure 2 presents the integration of the mobility header as an option of the IPv6 header.

5.1.1. Mobile IPv6 requirements

The main problems of Mobile IPv6 over 6LoWPAN are, on the one hand, the overhead due to the mobility options, home agent address specification in all the data packets, and the tunnelling costs for the communications through the home agent, and on the other hand, the viability of the required security for the communication between the mobile node (MN) and its Home Agent (HA).

Mobile IPv6 requires a set of mandatory capabilities or the MN, which are not feasible for the constrained devices used in the IoT. Specifically the requirements of Mobile IPv6 for MNs are as follows:

1. The MN must be able to process Mobility Headers.
2. The MN must maintain a Binding Update List.
3. The MN must be able to send Binding Updates, and receive Binding Acknowledgement and Binding Refresh Request.
4. The MN must support receiving Mobile Prefix Advertisements (*Router Advertisements*) and reconfiguring its home address based on the prefix information contained therein.
5. The MN must support movement detection and care-of address formation.
6. The MN must support the *Destination Option header* to include the Home Address in the Binding Updates.
7. The MN must perform IPv6 encapsulation and decapsulation for the communications based on triangle routing through the HA.
8. The MN must support IPSec, since the communication between the MN and the HA needs to be protected.
9. The MN must support the return routability procedure.
10. The MN must be able to process type 2 routing header in order to receive packets directly from the Correspondent Node (CN) and include the Home Address option to send the packets directly to the CN, both options when the Route Optimization procedure is carried out

All the presented requirements are mandatory following the RFC 6275 [23], therefore they need to be supported in order to be interoperable and full compliant with the existing Mobile IPv6 implementations.

5.1.2. Mobile IPv6 analysis

The initial seven requirements are based on the basic functionality of Mobile IPv6 in order to perform the binding management, set-up of the care-of address, and exchange of data with the correspondent node when the MN is in roaming. Specifically, Destination option is required to indicate the home address during the binding management when the source address is the care-of address instead of the home address, and the encapsulation/decapsulation is required to continue using the home address as source address during the roaming.

The last three requirements, even when they are mandatory, a Mobile IPv6 scenario can be established without them. These requirements are related with security aspects, first IPSec for the communication between the MN and the HA, and second the return routability procedure used to exchange binding key, ensure the reachability of the CN from the MN and authenticate the MN for the route optimization, in order to avoid the triangle routing through the HA.

The communications in Mobile IPv6 with the correspondent nodes can be carried out in two different ways, on the one hand, with suboptimal traffic flow in the case that the CN does not support MIPv6, and on the other hand, directly with the CN in the case that the route optimization process can be performed.

The route optimization and consequently return routability process are only carried out when the CN supports Mobile IPv6. For that reason, it can be established a mobility scenario without these two functions and ignore when the MN supports Mobile IPv6, since it should be required to carry out triangle routing.

Therefore, IPSec requirement presents the main concerns about the feasibility of Mobile IPv6 over 6LoWPAN, since IPSec was not initially considered suitable for constrained devices, due to its high overhead and processing requirements [17].

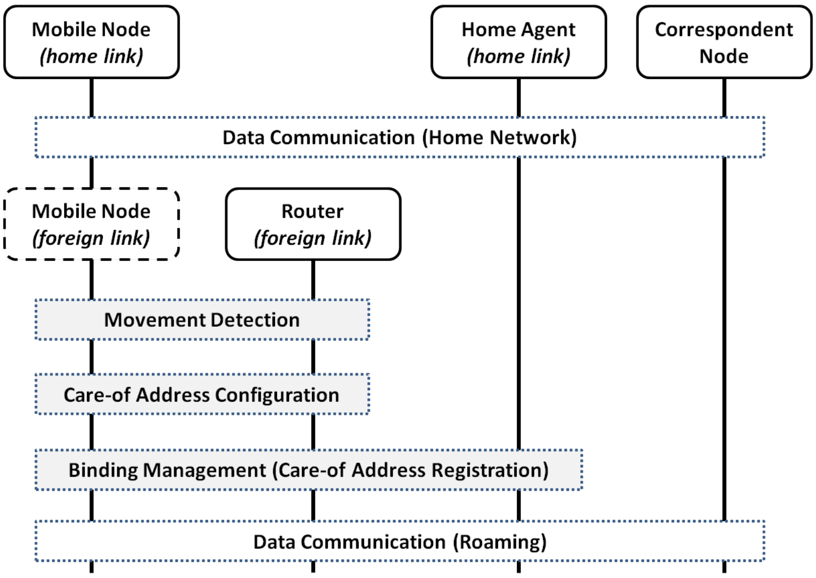

Mobile Node
(home link)
Home Agent
(home link)
Correspondent
Node
Data Communication (Home Network)
Mobile Node
(foreign link)
Router
(foreign link)
Movement Detection
Care-of Address Configuration
Binding Management (Care-of Address Registration)
Data Communication (Roaming)

Fig. 3. Sequence of phases in Lightweight Mobile IPv6.

This work analyses the feasibility to integrate IPSec and its limitations. In details, this work proposes, on the one hand, a lightweight version of Mobile IPv6 without security support, where are satisfied the initial seven requirements, and consequently it is compatible and functional with the existing Mobile IPv6 solutions, on the other hand, IPSec is analysed and integrated in the lightweight version of Mobile IPv6, thereby it is offered a solution with security support satisfying the requirement number eight.

The next two subsections present both the proposed lightweight Mobile IPv6 and the IPsec support in the lightweight Mobile IPv6.

6. Lightweight Mobile IPv6

Lightweight Mobile IPv6 is a lightweight version of Mobile IPv6, since this does not support route optimization, return routability, and IPSec. In addition, it has been optimized its implementation to be integrated into constrained devices with a low capacity in terms of memory and communication capabilities.

Figure 3 presents the sequence of phases in Lightweight Mobile IPv6, the main difference with respect to full Mobile IPv6 is that *Return Routability Procedure* and *Correspondent Binding Procedure* are not carried out, consequently it is not supported Route Optimization.

The phases are described are described in more details in the following subsections.

6.1. Movement detection

Movement detection in Mobile IPv6 is based on Neighbour Discovery. Neighbour Discovery has been redefined for 6LoWPAN in the RFC6775 [25]. The revision of Neighbour Discovery for 6LoWPAN presents serious inconvenient for the Mobile IPv6, since the router advertisements are only sent upon reception of router solicitation, therefore the movement detection cannot be based on the router advertisement frequency or appearance of router advertisements with a different prefix.

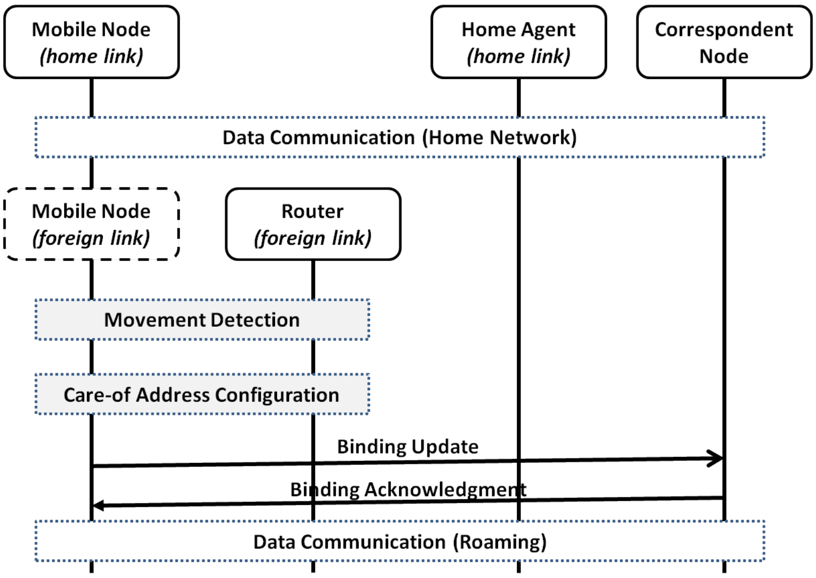


Fig. 4. Care-of address registration.

The revised Neighbour Discovery is also removing the duplicated address detection procedure but the mobile node continues requiring to register its new care-of address on the router. This registration only consists in exchanging neighbour solicitation and neighbour advertisement messages between the mobile node and the router.

For that reason for 6LoWPAN, it has been proposed several solutions for movement detection based on cross-layer movement detection through values from the link layer, such as RSSI, and additional signalling packets such as keep alive [8].

Signalling for the movement detection should be based on passive overhearing of messages from other protocols instead of active keep alive for the movement detection, since it needs to be reduced as much as possible the number of messages dependent from the mobility protocol in order to ensure the low power features from the IoT. Passive overhearing analysis to trigger the movement detection dependent on each solution.

Particularly, for the evaluation in this work is considered, first, active scan to associate to the new network, and after standard neighbour discovery, such as defined in the standard. As an alternative, an approach based on direction determination and RSSI evolution have been presented in our previous works for critical environments and hospital wireless sensor networks [5,6].

6.2. *Care-of address configuration and binding management*

Care-of address configuration is based on state-less auto-configuration. State-less auto-configuration is one of the advantages from neighbour discovery through the router advertisement, where is announce the prefix of the new network.

Care-of address registration uses the mobility headers defined by the MIPv6 protocol. Specifically, care-of address registration is carried out through the Binding Update message and its respective Binding Acknowledgement, such as presented in the Fig. 4.

6.2.1. Binding Update (BU)

BU message is used when the MN is at the home network in order to indicate to the Home Agent that needs to take care of its home address. This process is denominated as Home Agent Registration process. Second, BU is used by the MN to notify to the Home Agent of a new care-of address assigned in the visited network for itself. Thereby, the Home Agent is able to map and forward the messages from the active communications.

The main difference between the registration and update is in the flags enabled over the mobility header. For that purpose, we will analyse in more details the Mobile IPv6 header for the BU.

BU is composed of two IPv6 header extensions such as presented in the Fig. 6.2.1. First, it is used the *Destination Options for IPv6 header* to indicate its Home Address. Thereby, the Home Agent can link the new care-of address with its home address. Then it is sent the mobility header, in this case is the mobility header 5 which is the BU. The fields as described as follows:

- *Sequence Number:* The sequence number is used to avoid duplicate packets and match the binding update with the binding acknowledgement.
- *A:* The bit A is set to request to an acknowledge from the Home Agent.
- *H:* The bit H is set to indicates to the received node that it should act as its Home Agent, i.e., it is presenting the home agent registration process. For that reason, when this packet is sent the MN needs to be in the same network (included subnet prefix) that the Home Agent.
- *L:* The bit L is set to indicate that the home address is the same to its link local address, it is mainly for the Home Agent registration process.
- *K:* The bit K is set to indicate that the dynamic key management for IPSec is supported. Otherwise, if IPSec is established static or non-security is defined for the communications with the Home Agent then it needs to be cleared.
- *Lifetime:* The lifetime of the binding update indicates when can be considered expired the update from the MN.
- *Options:* Some mobility options such as alternative care-of address can be added.

For the Lightweight Mobile IPv6 the Binding Update is equivalent but with the usage of the 6LoWPAN and the extension header format proposed by the RFC6282.

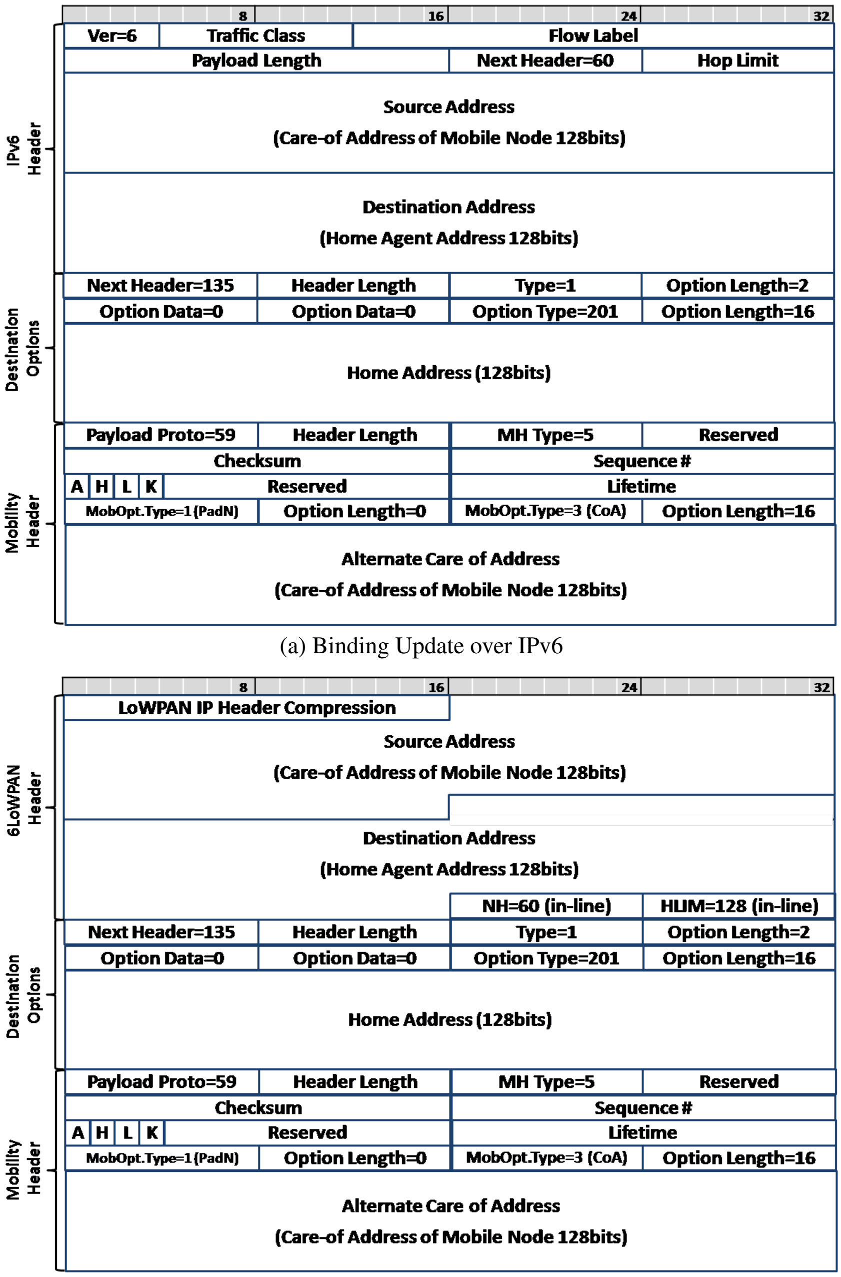
Figure 5(b) is presenting the BU for the 6LoWPAN version available in the Contiki implementation of 6LoWPAN, which is neither supporting the next header compression for the destination option nor for the mobility header. For that reason, this carries out the original next header value of the destination option in-line (i.e., next header with value 60), and this also requires to carry out the hop limit field, since this values is equal to 128 and the header compression to elide this value is only considering 1, 64 and 255 values.

Figure 6 presents the proposed version of the BU with the compression mechanism for the IPv6 Next Header (NHC), this work has considered as a novelty the first implementation of the 6LoWPAN NHC for the destination option and the Mobile IPv6 headers.

The NHC for the IPv6 Destination Options Header has the value reserved in the RFC6282 [32], *1110011N*, where N indicates if it one additional header with the NHC format is present, in this case since this is also added the IPv6 Mobility Header the value of N is 1, and this presents the NHC=0xE7.

The fields included for the compressed version of the IPv6 Destination Options Header are:

- Header Length: This field indicates the length of this header, at the same way that in the original IPv6 Destination Options Header. This is required since several options can be included, and consequently the length is variable.



(a) Binding Update over IPv6

(b) Binding Update over 6LoWPAN

Fig. 5. (a) Binding Update Message in Mobile IPv6. (b) Binding Update Message in Mobile IPv6 with 6LoWPAN header with the original Contiki OS implementation.

- Option Type: This field indicates the option type, at the same way that the original IPv6 Destination Options Header. For example, the value 201 means the Home Address Options, which is required to indicate to the Home Agent to which MN belongs this BU.
- Option Length: This field indicates the length of the option, since each option has a different value.

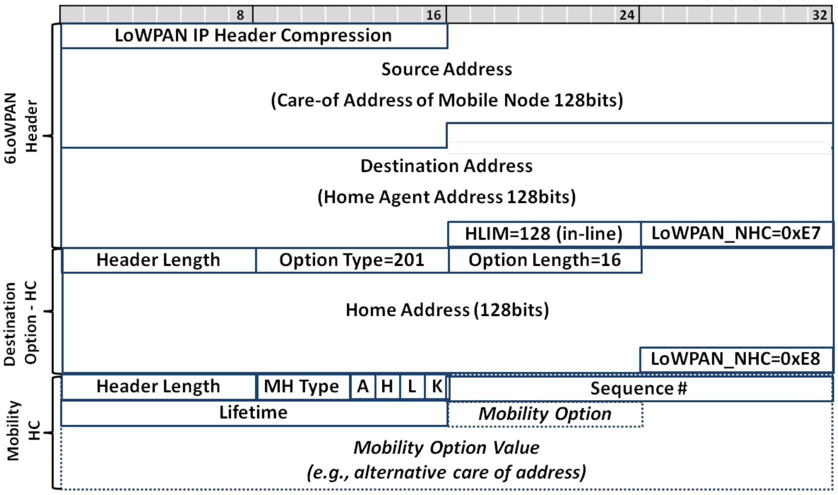


Fig. 6. Binding Update Message proposed for the Lightweight Mobile IPv6 with 6LoWPAN header and next header compressed for the destination option and the mobility headers.

The NHC for the IPv6 Mobility Header has the value reserved in the RFC6282 [32], *1110100N*, in this case since this N is 0, and this presents the NHC = 0xE8.

The fields included for the compressed version of the IPv6 Mobility Header are:

- Header Length: This field indicates the length of this header at the same way that in the original IPv6 Mobility Header. This is required since several mobility header types are defined.
- Mobility Header Type (MH): This field indicates the MH type. This has been reduces from 8 to 4 bits, since the MH Types considered are under 16, and this allows to re-use the reserved 4 bits after the flags.
- Flags (A, H, L, and K): The flags keep the same semantic that the original one.
- Sequence Number: This field has the same semantic that in the original mobility header.
- Lifetime: This field has the same semantic that in the original mobility header.
- Mobility options: This offers at the same way that original Mobile IPv6 header the option to add mobility options such as the alternative care-of address option.

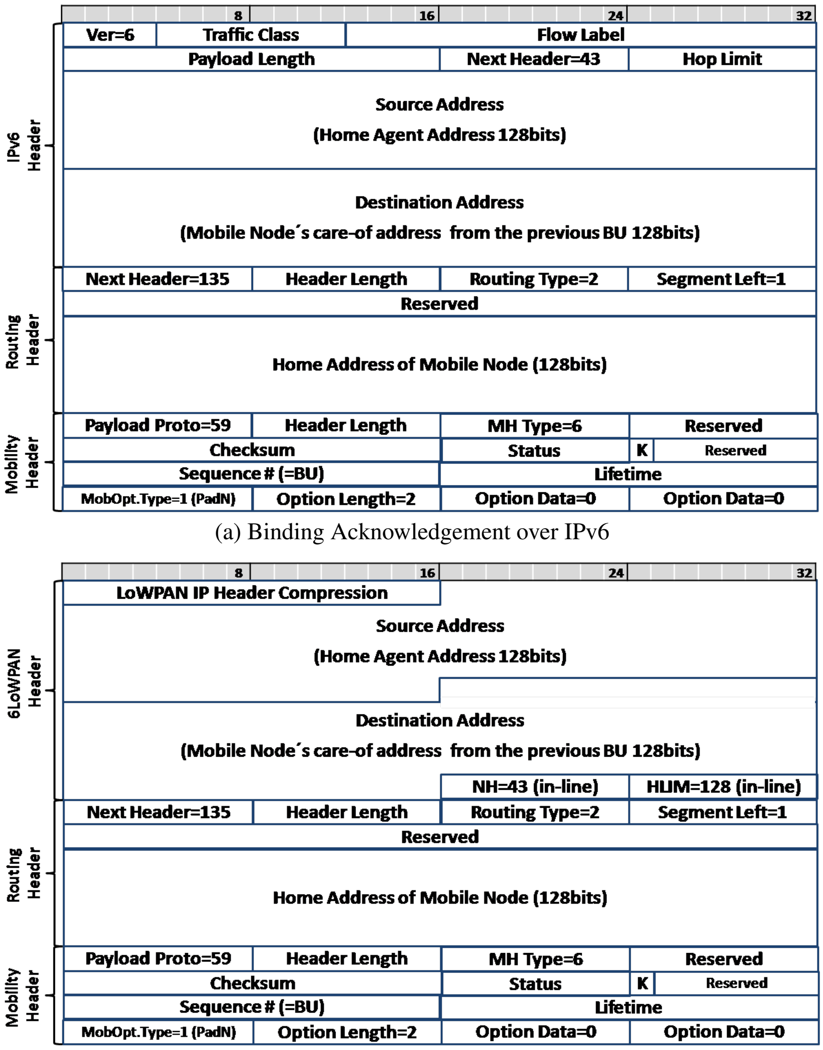
The compressed version of the BU presented in the Fig. 6 is converted to the version presented in the Fig. 5(a), when this goes through the 6LoWPAN Border Router. Thereby, making it totally interoperable with Mobile IPv6.

6.2.2. Binding Acknowledgement (BA)

BA presented in the Fig. 7(a). BA is very similar to the BU but with the difference of the inclusion of the Routing Header type 2 to hold the Home Address of the MN and the field *Status* to indicate if the BU has been accepted or not.

At the same way that for the Binding Update, the Fig. 6.2.2 presents the version of the Binding Acknowledgement with the usage of the 6LoWPAN, which is offered by the current Contiki OS implementation of 6LoWPAN. Since, it should be used the extension header format proposed by the RFC6282, Fig. 8 presents the version proposed with the implementation of the IPv6 Routing Header Type 2 using the NHC.

The NHC for the IPv6 Routing Header has the value reserved in the RFC6282 [32], *1110001N*, where N is equal to 1, since the IPv6 Mobility Header is added. The value is NHC = 0xE4.



(a) Binding Acknowledgement over IPv6

(b) Binding Acknowledgement over 6LoWPAN

Fig. 7. (a) Binding Acknowledgement Message in Mobile IPv6. (b) Binding Acknowledgement Message in Mobile IPv6 with 6LoWPAN header with the original Contiki OS implementation.

The fields included for the compressed version of the IPv6 Routing Header are:

- Header Length: This field indicates the length of this header, at the same way that in the original IPv6 Routing Header.
- Routing Type: This field indicates the type of the routing header, in this case it is used the routing header type 2, which is the reserved for the mobility purpose. The other options of mobility are being deprecated because security issues. Therefore, this field could be elided in the future.
- Segment left: The field indicates the number of hosts that this message still has to visit before reaching its final destination. This value is equal to 1 in the case of mobility purpose, since this is only used to identify the MN Home Address, at the same way that the destination option identified to the MN Home Address in the BU message. Therefore, since it will be always equal to 1, this field can be elided in the future.

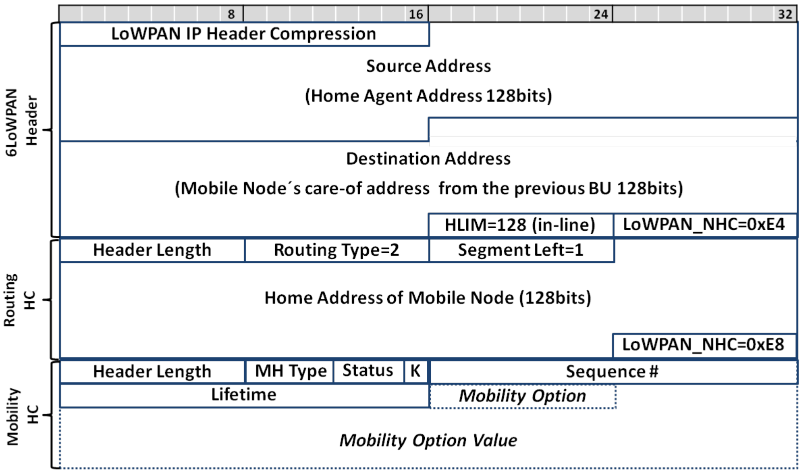


Fig. 8. Binding Acknowledgement Message proposed for the Lightweight Mobile IPv6 with 6LoWPAN header and next header compressed for the routing and the mobility headers.

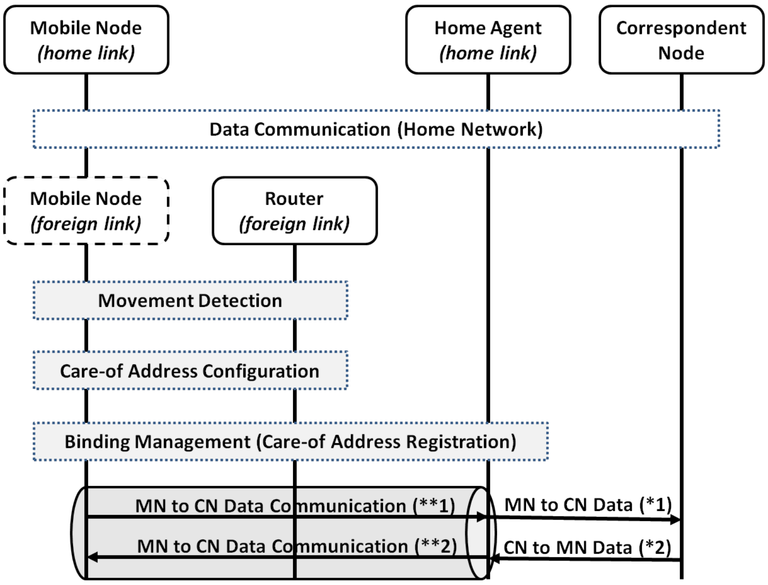
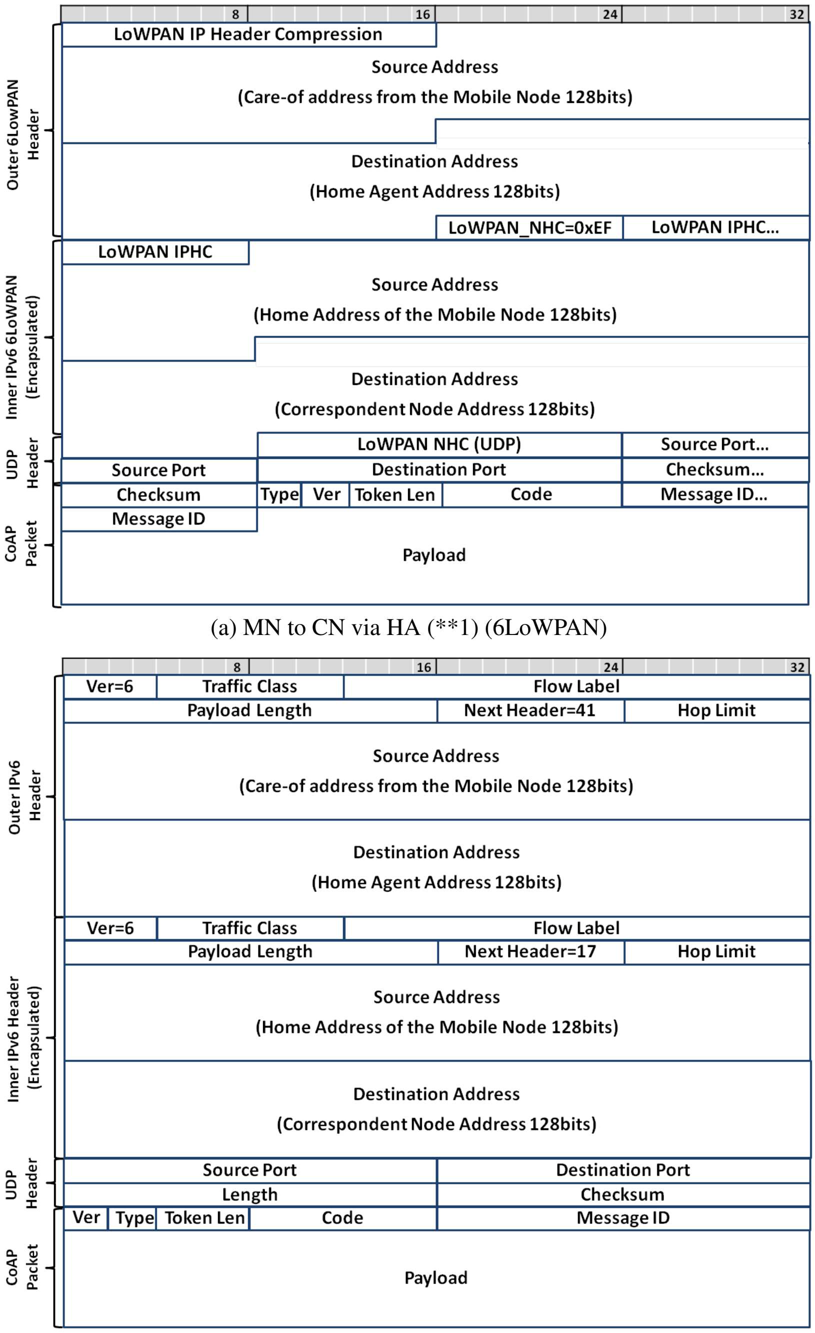

Mobile Node (home link)
Home Agent (home link)
Correspondent Node
Data Communication (Home Network)
Mobile Node (foreign link)
Router (foreign link)
Movement Detection
Care-of Address Configuration
Binding Management (Care-of Address Registration)
MN to CN Data Communication (**1)
MN to CN Data (*1)
MN to CN Data Communication (**2)
CN to MN Data (*2)

Fig. 9. Data communication exchange tunneled via the HA.

The NHC for the IPv6 Mobility Header for the BA changes with respect to the BU. Specifically, this has changed the A, H and L flags to the status field. This change has been applied for the Lightweight version presented in the Fig. 8.

6.3. Data communication

The traffic generated for the data communication is tunnelled via the HA such as presented in the Fig. 9. This shows the triangle routing through the HA is required when the CN is not supporting Mobile IPv6, and in particular for Lightweight Mobile IPv6 since it has not been considered the support of Route Optimization.



(a) MN to CN via HA (**1) (6LoWPAN)

(b) MN to CN via HA (**1)

Fig. 10. (a) Packet from the MN to the CN via the HA (**1) based on 6LoWPAN header compression. (b) Packet from the MN to the CN via the HA (**1) based on IPv6.

The encapsulation is from the MN to the HA and vice versa. For that reason, it is defined two versions of the same packet. First, it is presented the "**" version of the packet for the encapsulated and the "*" version for the desencapsulated.

The Fig. 10(a) presents the format of a CoAP packet when is sent from the MN to the CN via the HA. This includes the outer 6LoWPAN header with the source address of the current address of the MN (care-of address) and destination address set to the HA address. The inner 6LoWPAN headers with the source address the home address of the MN and destination address of the CN address. Finally, this includes the useful data with the CoAP packet or the transport/application protocol used.

This uses the NHC defined for IPv6 packets in the RFC6282, where such as presented, the NHC value for the tunneled IPv6 packet uses the reserved value *1110111N*. N is 1 since this requires the UDP next header. Therefore, the value is NHC = 0xEF.

This packet based on 6LoWPAN is translated to the IPv6 version presented in the Fig. 10(b) after that this is decompressed by the 6LoWPAN Border Router.

This compression of both the outer and inner headers from IPv6 to 6LoWPAN has been one of the optimizations carried out by the Lightweight Mobile IPv6, since the original implementation such as the found in the Contiki OS just compresses the outer header and carries out the inner header with the full IPv6 header.

CoAP has been optimized for the integration of the REST architecture in constrained networks, such as it is present just requires 4 bytes to specify version (Ver), Type to indicate if this message is of Confirmable (CON), Non-Confirmable (NON), Acknowledgement (ACK) or Reset (RST), Token Length in case that some option is added, Code similar to HTTP in terms of GET, PUT, POST and DELETE, and finally the message ID for the detection of message duplication, and to match messages of type ACK/RST to messages of type CON/NON. More details about CoAP can be found in [20].

Then, the presented packet in the Fig. 10(b) is desencapsulated by the HA and then it is only sent the packet as if the MN was in its home address. This packet is presented in the Fig. 11(a), where this is removed the outer IPv6 header.

At the same way, the traffic generated by the CN is sent to the MN via the HA. The Fig. 11(b) presents the packet transmitted from the CN to the MN, which is not encapsulated. This packet arrives to the HA encapsulated such as presented in the Fig. 12(a), and finally the 6LoWPAN Border Router adapts the outer and inner header to 6LoWPAN instead of IPv6, see Fig. 12(b).

Therefore, the MN always needs to encapsulate and desencapsulate all the packets, what means an extra overhead due to the encapsulated IPv6 header. The presented tunneling is assuming IPv6 headers and it is not taking into account security. Figure 13 presents the different options to implement the tunnel between the MN and the HA. Mainly, two modes are defined, on the one hand, encapsulation without security such as the presented, and on the other hand, encapsulation with IPSec ESP.

The Lightweight Mobile IPv6 implementation can consider IPv6 header compression instead of full IPv6 such as 6LoWPAN. For that reason, it is presented in all the presented figures the version based on the 6LoWPAN header.

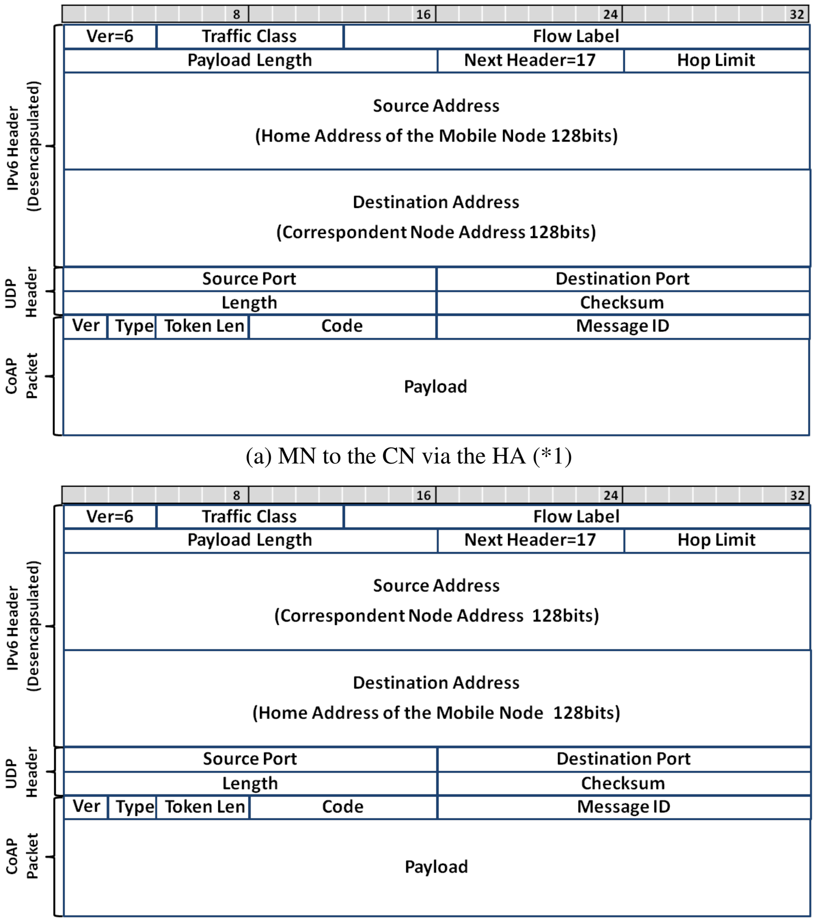
The next section presents the case that there is an IPSec tunnel between the MN and HA.

7. IPSec support in lightweight Mobile IPv6

7.1. IPSec analysis

IPSec is mandatory with IPv6, making it available in the majority of operating systems and networking hardware.

IPsec is not one protocol but rather three: Authentication Header (AH) and Encapsulating Security Payload (ESP) are used for traffic security and Internet Key Exchange (IKE) is used for the establishment



(a) MN to the CN via the HA (*1)

(b) CN to the MN via the HA (*2)

Fig. 11. (a) Packet from the MN to the CN via the HA (*1). (b) Packet from the CN to the MN via the HA (*2).

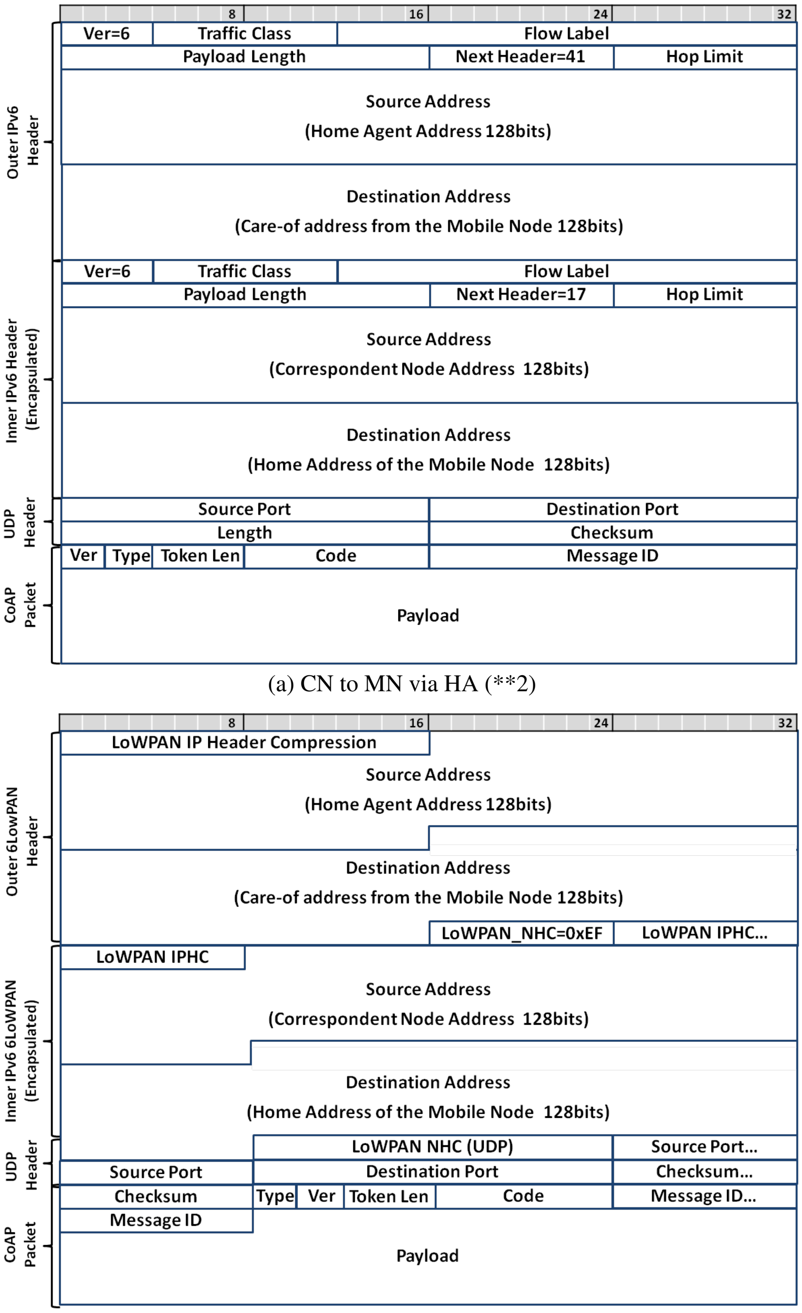
of keying material and other traffic security parameters. AH and ESP are usually supported by the kernel as part of the IP stack, while IKE is implemented as a user daemon.

IPSec offers end-to-end security in the network layer. It was expected to be a suitable security protocol for datagram traffic generated by client-server applications, but at the end it has not been exploited as much as expected since its difficult to suit for Web-based client-server application models, since this needs to be managed in the kernel. For that reason, protocols such as DTLS has gained attention for its application in the datagram traffics. In particular for the IoT, DTLS 1.2 has been considered the security protocol for CoAP [20].

IPSec is mainly used to build tunnels between hosts such as the used for MIPv6. The traffic exchanged between the MN and its HA is IPsec protected (tunnel mode). In all cases, its signalling traffic is protected using transport mode (ESP).

IPsec has to be used for traffic through the Home Agent tunnel, this solves most of the security challenges introduced by mobility such as MIPv6 introduces no new security threats.

The main problem of IPSec is its overhead and extra memory requirements for its integration in the communication stack.



(a) CN to MN via HA (**2)

(b) CN to MN via HA (**2) (6LoWPAN)

Fig. 12. (a) Packet from the CN to the MN via the HA (**2). (b) Packet from the CN to the MN via the HA (**2) based on 6LoWPAN header compression.

The integration of IPSec over constrained devices can be carried out, on the one hand, through the usage of specific cryptosuites such as AES-CCM that are directly supported by hardware in the majority of the transceivers used in IoT solutions such as IEEE 802.15.4 and 6LoWPAN. Thereby, the impact

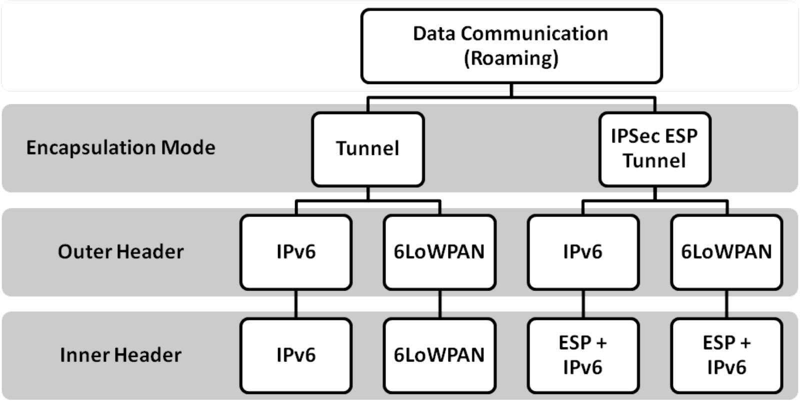


Fig. 13. Encapsulation modes for data communication during roaming.

coming from the cryptographic primitives is elided. On the other hand, it can be used more common and supported cryptosuites such as AES-CBC, which offers encryption and can be used in conjunction with other authentication mechanisms, in case that authentication can be also provided.

Both of them continue presenting the inconvenient of the overhead for the communications.

The next subsection presents the new formats including the IPSec ESP header and trailer.

7.2. IPSec integration in Mobile IPv6

Mobile IPv6 considers IPSec as the security protocol to protect the binding management, the communications between the MN and the HA, and the communications with the CN send via the HA.

Binding management requires the use of IPSec ESP in transport mode to provide data origin authentication, connectionless integrity, and optional anti-replay protection.

Regarding the data communication with the CN via the HA, it is used IPSec ESP in tunnel mode to protect the inner IPv6 address. Thereby, intruders between the MN and the HA cannot figure out which is the real destination address of the packet.

One inconvenient of IPSec for Mobile IPv6 is that Route Optimization is not compatible with IPSec Tunnel payload (i.e., ESP), since it is not established the Security Association (SA) with all the CNs. The SA is established mainly between the MN and its HA. For that reason, when Route Optimization is applied the security is carried out through Return Routability procedure. In the case of lightweight Mobile IPv6, it is not used Route Optimization with the CN and consequently the IPsec protection is not lost for traffic leaving/entering the foreign network.

7.3. Crytosuites support for IPSec in lightweight Mobile IPv6

The cryptosuites considered for the IPSec integration with Mobile IPv6 can be based on different approaches. IPSec defines as mandatory AES-CBC for encryption and HMAC-SHA1-96 for authentication [34], although it has been defined the AES-CCM support in the RFC6275 [23].

AES-CCM can be considered highly relevant for the IoT, since the majority of the transceivers support this functions by hardware. For example, IEEE 802.15.4 standard includes support for AES-CTR for encryption, AES-CBC-MAC for message authentication and AES-CCM which combines encryption and message authentication. This offers blocks of 32, 64 or 128 bits, it can be also found some implementations supporting 96 bits. The mandatory mode by the standard is AES-CCM. For that reason, this work is focused on AES-CCM.

CCM is an authenticate-and-encrypt block cipher mode for the Advanced Encryption Standard (AES) block cipher available in the majority of the hardware used to build the IoT devices such as IEEE 802.15.4 and IEEE 802.11 transceivers.

AES CCM is used as an IPSec ESP mechanism, such as required to build the IPSec tunnel between the MN and the HA. AES CCM provides data integrity and data origin authentication for the payload and for additional information included in the Additional Authentication Data (AAD) section of the ESP payload. Thereby, the ESP payload is the composition of the initialization vector (IV), encrypted payload and the authentication data.

AES CCM requires a different IV for each encryption in order to avoid vulnerabilities. IV needs to be generated by the encryptor and be transferred to the decryptor. Since, IV collision can lead to obtain plain-text information from both packets. For that reason, it is suggested the dynamic change of keys through the Internet Key Exchange (IKE) offered by IPSec or other solutions such as the temporal key integrity protocol (TKIP) used in IEEE 802.11.

7.4. IPSec format

Figure 14 presents the total headers integrated in an Lightweight Mobile IPv6 packets. This is assumed that the outer IPv6 header is 6LoWPAN, but this could be also considered IPv6.

Such as presented in the Fig. 14 the overhead of ESP in mode tunnel depends of the crypto algorithm used. The overhead introduced by AES-CCM mode is at least 18 bytes. 16 bytes from ESP Header (SPI, Sequence number and IV), 2 bytes from ESP trailer (Pad length and next header) when the block alignment is perfect and consequently padding is not required. The use of AES-CBC introduces at least 26 bytes. 24 bytes from ESP Header (SPI, Sequence number and IV) and 2 bytes from ESP Trailer (Pad length and next header) following the mentioned conditions before.

The difference resides on the IV vector, since AES-CBC [21] introduces the full IV vector length (16 bytes) and AES-CCM [22] the half length of the IV (8 bytes). AES-CCM requires less bytes for the IV due to the use of the counter mode to generate the key stream. Therefore, AES-CCM uses 1 byte for CCM flags, 4 bytes for the block counter, and the remaining bytes are composed of 3 bytes of salt assigned at the beginning of the security association and the 8 bytes transmitted in the packet.

AES-CCM provides confidentiality, optionally could be introduced the ESP Authentication Header in order to provide integrity. AES-CCM algorithm is prepared to provide integrity but no AES-CBC that need the use of an additional algorithm such as HMAC-SHA1.

However, the mentioned fields could be compressed such as described in [24] in case that ESP Authentication Data is not included. The main motivation is that ESP Authentication Data considers the ESP header for its calculation, therefore in case of use a compressed version of the ESP header this ICV field will be corrupt in the 6LoWPAN network. Otherwise, it could be considered a compressed version of the ESP header, which is uncompressed in the border router, at the same way that 6LoWPAN header is decompressed.

The ESP fields meaning is as follows:

- Security Parameter Index (SPI): This identifies the Security Association (SA) used in IPSec. This requires 4 bytes. SPI field can be elided in case that the SA for a host (IP address) is well-known by the border router, e.g., it has been learned by the border router by a previous usage. Other option

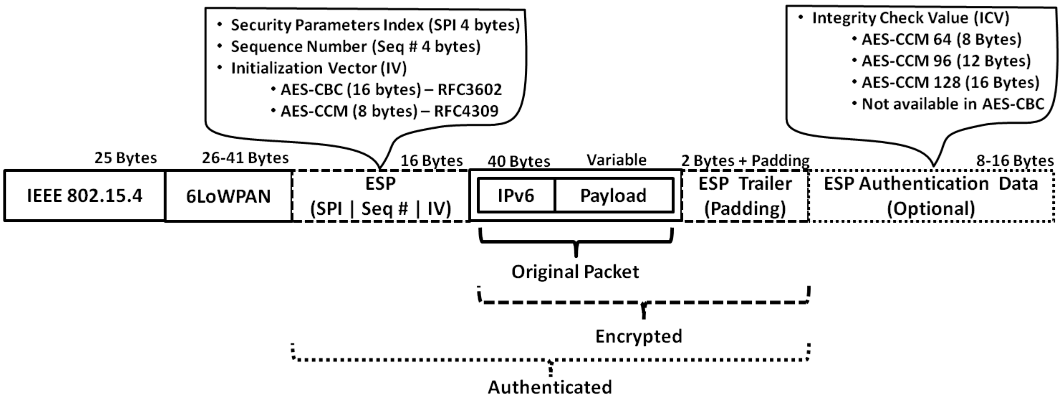

• Security Parameters Index (SPI 4 bytes)
• Sequence Number (Seq # 4 bytes)
• Initialization Vector (IV)
• AES-CBC (16 bytes) – RFC3602
• AES-CCM (8 bytes) – RFC4309
• Integrity Check Value (ICV)
• AES-CCM 64 (8 Bytes)
• AES-CCM 96 (12 Bytes)
• AES-CCM 128 (16 Bytes)
• Not available in AES-CBC
25 Bytes
26-41 Bytes
16 Bytes
40 Bytes
Variable
2 Bytes + Padding
8-16 Bytes
IEEE 802.15.4
6LoWPAN
ESP (SPI | Seq # | IV)
IPv6
Payload
ESP Trailer (Padding)
ESP Authentication Data (Optional)
Original Packet
Encrypted
Authenticated

Fig. 14. IPSec packet format.

is to reduce it to 4 bits in order to support 16 different SPIs assuming that the IoT devices will not keep multiple SAs since its constrained capabilities. Thereby, the border router does not keep an status, else just extend from 4 bits to 32 bits adding zeros.

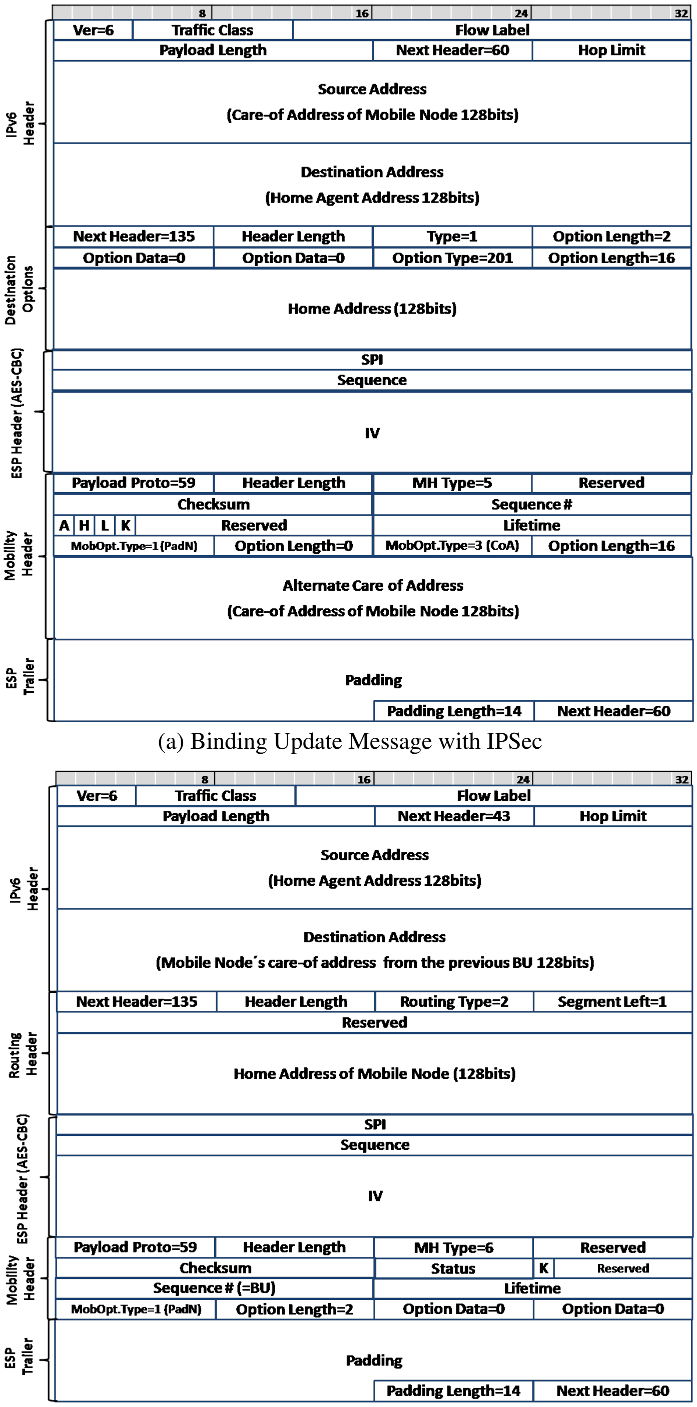
- Sequence Number: The sequence number is used to prevent replay attacks. This can be learned by the border router or reduced to a lower number of bits. The main problem of the reduction of bits is the coherence with the home agent, which can set sequence numbers of until 32 bits. For that reason, the options for this field are include the 32 bits, include only the last 4 bits and assume that the border router is tracking and storing the initial 28 bits of the sequence number. But, since this can bring additional issues in terms of aliasing and status synchronization in the Border Router, this optimization is not applied.
- Initialization Vector (IV): These 8 bytes need to be include, since the initialization vector is used for the decoding of the packet, and this is changed for each transmission in order to avoid the vulnerabilities of block ciphering when the IV is re-used.
- Padding Length: This field indicates the number of bytes added in the ESP trailer to align the payload block to the multiple of the AES-CCM, in our case align it to blocks of 16 bytes (128 bits).
- Next header: This field indicates the next IPv6 header option.

The overhead with IPSec ESP in mode tunnel is excessive since this does not allow to compress the inner IPv6 header. The reason because the inner header cannot be compressed is because the HA does not need to be aware of the 6LoWPAN header compression. Therefore, even when the ESP header is compressed, it continue requiring to carry 40 bytes of the inner IPv6 header. The Section 8 presents the evaluation of the overhead of IPSec for its different configurations. But, it can be seen in advance that for the presented configuration with outer header based on 6LoWPAN, the final available payload is 20 bytes out of the original 127 Bytes, which makes it with an efficiency under the 16%.

Therefore, since the main overhead of Mobile IPv6 is coming by the tunnel, i.e. the inner IPv6 header, it can be considered two options. First, the non-usage of security and consequently the header compression such as 6LoWPAN or GLoWBAL IPv6 [28] for both the outer and inner headers.

7.5. Binding management with IPSec

The format of the IPsec-protected Binding Update (BU) message is presented in the Fig. 15(a). This message is sent by the MN to its HA from a foreign network to register its new CoA. The BU message is



(a) Binding Update Message with IPSec

(b) Binding Acknowledgement Message with IPSec

Fig. 15. (a) Binding Update Message in Mobile IPv6 protected with ESP. (b) Binding Acknowledgement Message in Mobile IPv6 protected with ESP.

Table 2
Binding Update overhead analysis considered along this document

Packet	Headers (Bytes)	Total bytes	IPsec overhead	Fragmentation required?
Binding Update Figure 5(a)	LL (25) + IPv6 (40) + Dest. Opt. (24) + Mob Header: BU (32)	121	N/A	NO
Binding Update Contiki Figure 5(b)	LL (25) + 6LoWPAN (35) + Dest. Opt. (24) + Mob Header: BU (32)	116	N/A	NO
Binding Update Contiki UMU Figure 6	LL (25) + 6LoWPAN (35) + Dest. Opt. HC (20) + + Mob. Header HC: BU (26) + ESP Trailer	106	N/A	NO
Binding Update ESP Figure 15(a)	LL (25) + IPv6 (40) + Dest. Opt. (24) + ESP Header (24) + Mob. Header: BU (32) + ESP Trailer (16)	161	24.8%	YES
Binding Update Contiki ESP No Image	LL (25) + 6LoWPAN (35) + Dest. Opt. (24) + ESP Header (24) + Mob. Header: BU (32) + ESP Trailer (16)	156	25.6%	YES
Binding Update Contiki ESP UMU No Image	LL (25) + 6LoWPAN (35) + Dest. Opt. HC (20) + ESP Header HC (18) + Mob. Header: BU (32) + ESP Trailer (16)	146	23.3%	YES

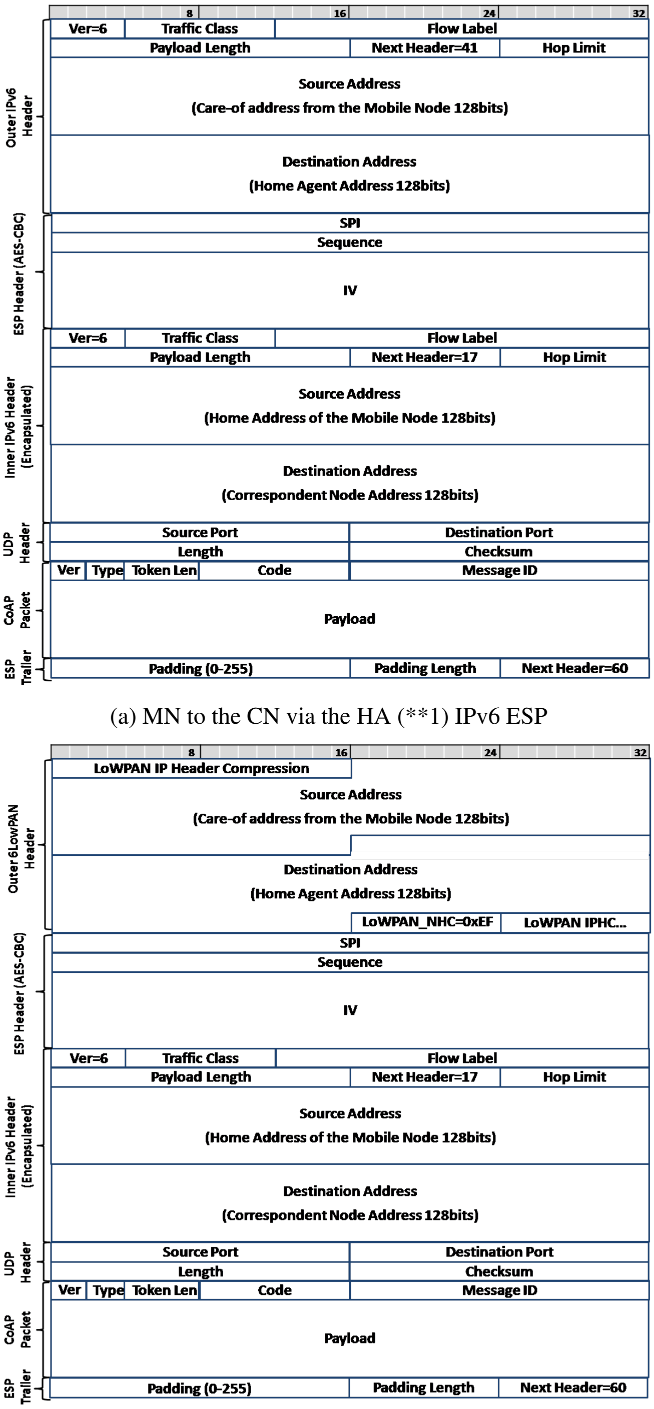
Table 3
Binding Acknowledgement overhead analysis considered along this document

Packet	Headers (Bytes)	Total bytes	IPsec overhead	Fragmentation required?
Binding ACK Figure 7(a)	LL (25) + IPv6 (40) + Routing Header (24) + Mob Header: BA (16)	105	N/A	NO
Binding ACK Contiki Figure 6.2.2	LL (25) + 6LoWPAN (35) + Routing Header (24) + Mob Header: BA (16)	100	N/A	NO
Binding ACK Contiki UMU Figure 8	LL (25) + 6LoWPAN (35) + Routing Header HC (20) + Mob. Header HC: BA (10)	79	N/A	NO
Binding ACK ESP Figure 15(b)	LL (25) + IPv6 (40) + Routing Header (24) + ESP Header (24) + Mob. Header: BA (16) + ESP Trailer(16)	145	27.6%	YES
Binding ACK Contiki ESP No Image	LL (25) + 6LoWPAN (35) + Routing Header (24) + ESP Header (24) + Mob. Header: BA (16) + ESP Trailer(16)	140	28.6%	YES
Binding ACK Contiki ESP UMU No Image	LL (25) + 6LoWPAN (35) + Routing Header HC (20) + ESP Header HC (18) + Mob. Header: BA (16) + ESP Trailer(16)	130	26.1%	YES

sent using the current CoA of MN (address in source address field of the IPv6 header). The HoA is found in the *Home Address Option* in the *Destination Option Header* extensions following the IPv6 header. The BU message (Mobility Header type 5) is IPsec-protected. It contains an *AltCoA* option which provides the current CoA of the MN.

When the HA receives the BU, the HA replies with an IPSec protected Binding Acknowledgement (BA) message. The format of the message is presented in the Fig. 15(b). The Routing Header Type 2 contains the final destination of the packet, i.e. the HoA. The destination address of the packet (outer IPv6 header) is the MN's CoA.

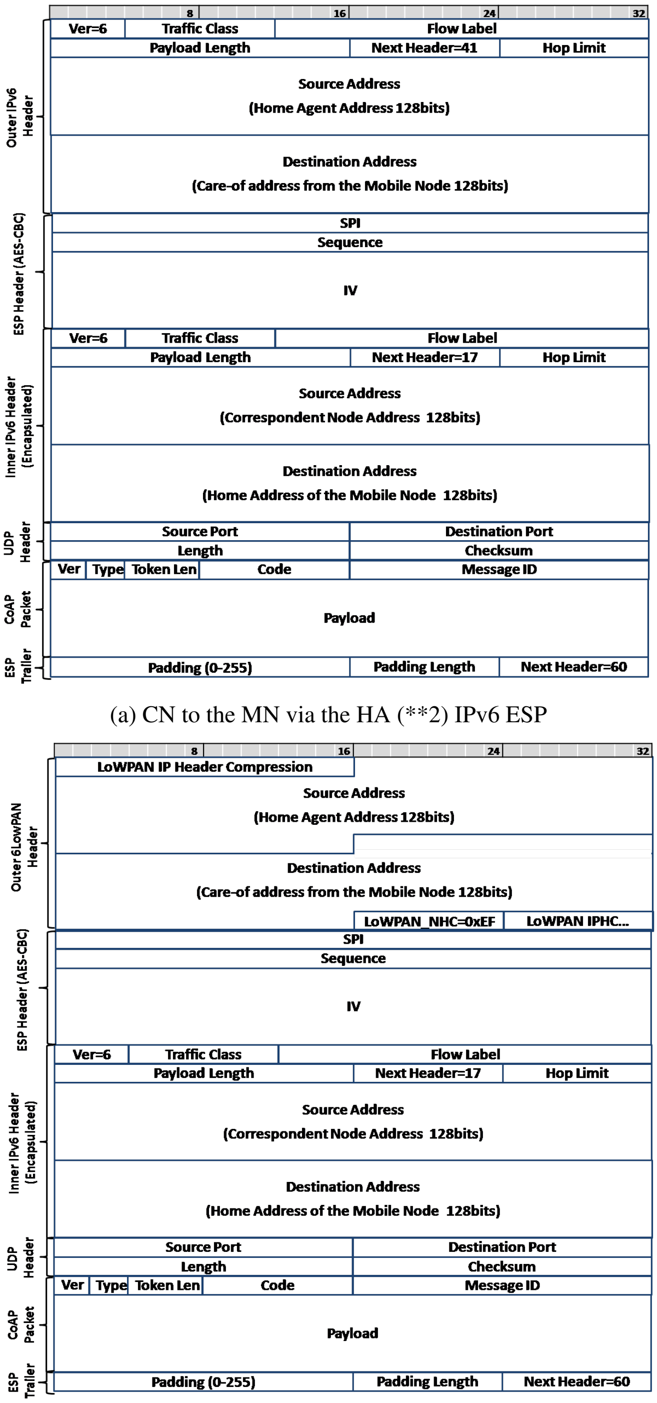
Tables 2 and 3 make a comparative about the size, security overhead, and need of fragmentation for the BU and BA messages in the different versions described. These results present that the overhead



(a) MN to the CN via the HA (**1) IPv6 ESP

(b) MN to the CN via the HA (**1) 6LoWPAN ESP

Fig. 16. (a) Packet from the MN to the CN via the HA (**1) based on IPv6 using ESP tunnel. (b) Packet from the MN to the CN via the HA (**1) based on 6LoWPAN header compression using ESP tunnel.



(a) CN to the MN via the HA (**2) IPv6 ESP

(b) CN to the MN via the HA (**2) 6LoWPAN ESP

Fig. 17. (a) Packet from the CN to the MN via the HA (**2) based on IPv6 using ESP tunnel. (b) Packet from the CN to the MN via the HA (**2) based on 6LoWPAN header compression using ESP tunnel.

Table 4
UDP CoAP communication overhead analysis considered along this document

Packet	Headers (Bytes)	Total bytes	Payload size	IPsec overhead	Fragmentation required?
*1 and *2 Figure 11(a) and Figure 11(b)	LL (25) + IPv6 (40) + UDP (8) + CoAP (4)	77	50	N/A	NO
**1 and **2 Contiki 10(a)	LL (25) + 6LoWPAN (35) + 6LoWPAN (35) + UDP (8) + CoAP (4)	107	20	N/A	NO
**1 and **2 IPv6 10(b)	LL (25) + IPv6 (40) + IPv6 (40) + UDP (8) + CoAP (4)	117	10	N/A	NO
**1 and **2 IPv6 ESP 16(a)	LL (25) + IPv6 (40) + ESP Header (24) + IPv6 (40) + UDP (8) + CoAP (4) + ESP Trailer (16)	157		25.5%	YES
**1 and **2 Contiki ESP 16(b)	LL (25) + 6LoWPAN (35) + ESP Header (24) + IPv6 (40) + UDP (8) + CoAP (4) + ESP Trailer (16)	152		26.3%	YES
**1 and **2 Contiki ESP UMU No image	LL (25) + 6LoWPAN (35) + ESP Header (18) + IPv6 (40) + UDP (8) + CoAP (4) + ESP Trailer (16)	146		23.3%	YES

caused by the use of IPSec for the BU and BA represents between 23.3% and 28.6% of overhead for these messages. In addition, the use of IPSec requires fragmentation, since the sizes are bigger than the maximum frame size for 802.15.4 (i.e., 127 bytes).

7.6. Data communication with IPSec

IPSec security using ESP tunnel mode was used in order to avoid vulnerabilities related with the mobility protocol. The use of security includes 2 new headers in the packet, the ESP Header and the ESP Trailer; both headers has been discussed before. Following the data communication example previously presented in the Fig. 9, Figs 16(a) and 17(a) present the version "**" of the packet using ESP tunnel mode when the packet is sent from the MN to the CN via HA and viceversa. Figures 16(b) and 17(b) presents the version "**" of the packet using ESP tunnel mode when they are sent from the MN to the CN via HA and vice-versa using 6LoWPAN Header Compression. These figures present a ESP tunnel mode encrypted using AES-CBC algorithm. Desencapsulated version ("*") is presented in the Figs 11(a) and 11(b).

These example packets contains UDP-CoAP communications. Table 4 shows the different options for the data communication (based on UCP-CoAP packets). The different configurations in terms of security and tunnelling are presented and analysed.

8. Evaluation

8.1. Evaluation testbed

The evaluation testbed is presented in the Fig. 18. The testbed is composed of a HA, a MN, a CN and two 6LoWPAN Border Routers announcing two different networks.

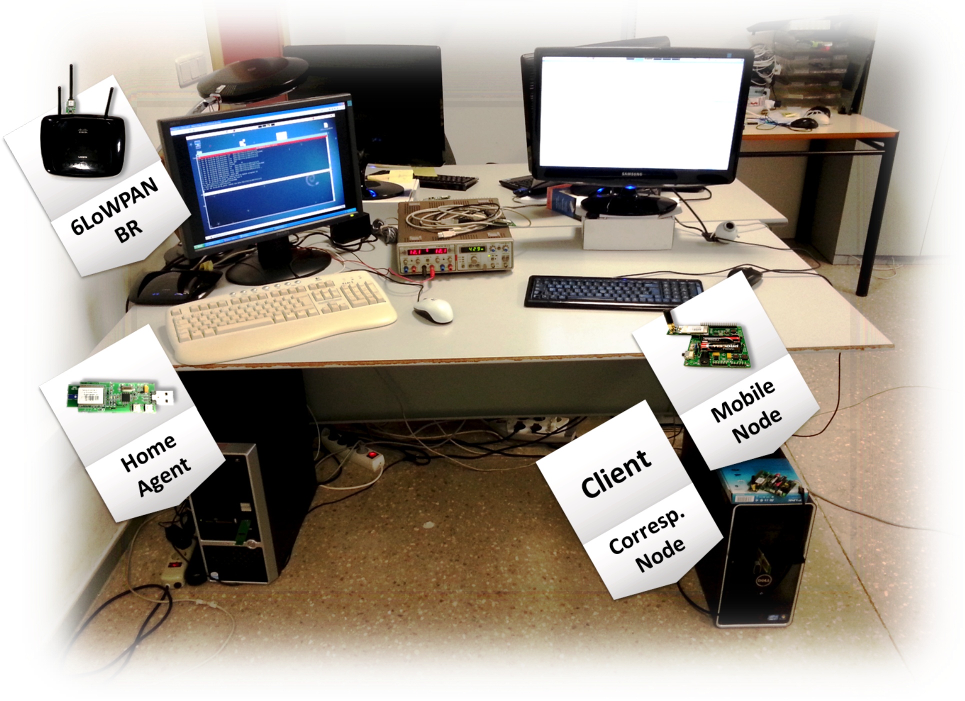


Fig. 18. Testbed for mobility evaluation.

The HA implementation is based on Mobile IPv6 in order to be compatible with the IPv6-enabled backbone. Specifically, it is based on the UMIP implementation of Mobile IPv6 [55]. UMIP is an open-source Mobile IPv6 stack for the GNU/Linux Operating System.

The HA has integrated a 6LoWPAN Ethernet bridge presented in the Fig. 18. This networking device builds a virtual network interface (tun/tap) for the 6LoWPAN network.

The 6LoWPAN Border Router for the foreign network (visited network) has been developed with a Cisco Router enabled with OpenWRT. OpenWRT has been extended to support the previously mentioned 6LoWPAN Ethernet bridge in order to enable with 6LoWPAN connectivity.

The Mobile Node is a sensor board powered with batteries in order to make it mobile.

Finally, the Correspondent Node is a Server with Linux OS.

8.2. *Memory footprint*

Current Lightweight Mobile IPv6 implementation has been developed under Contiki OS 2.4 version. Specifically, this has been developed extending the Jennic port branch for JN51XX chipsets. The movement detection is based on a simple energy scan on all frequencies along 2 seconds, this could be improved with some technique on next versions. Signalling packets and tunnel mode works in both modes, with and without ESP security. The footprint of this implementation is 7,4 KBytes with AES-CCM (hardware supported) and 15.5 KBytes with AES-CBC (software implemented).

8.3. *Overhead*

The encapsulated packet for the data communication during the roaming has a size of 92 bytes plus the payload of the CoAP Packet such as presented in the Fig. 10(b). This packet is encapsulated into a

Table 5
Overhead analysis when using ESP Security ciphered with AES-CBC or AES-CCM mode

Packet	Headers (Bytes)	Total bytes	Payload size	IPsec overhead	Fragmentation required?
IPv6 ESP (AES-CBC)	LL (25) + IPv6 (40) ESP Header (24) + IPv6 (40) + ESP Trailer(16)	145		27.6%	YES
Contiki ESP (AES-CBC)	LL (25) + 6LoWPAN (35) ESP Header (24) + IPv6 (40) + ESP Trailer(16)	140		28.5%	YES
Contiki UMU ESP (AES-CBC)	LL (25) + 6LoWPAN (35) ESP Header HC (18) + IPv6 (40) + ESP Trailer(16)	134		25.2%	YES
IPv6 ESP (AES-CCM)	LL (25) + IPv6 (40) ESP Header (16) + IPv6 (40) + ESP Trailer(16)	137		23.3%	YES
Contiki ESP (AES-CCM)	LL (25) + 6LoWPAN (35) ESP Header (16) + IPv6 (40) + ESP Trailer(16)	132		24.2%	YES
Contiki UMU ESP (AES-CCM)	LL (25) + 6LoWPAN (35) ESP Header HC (10) + IPv6 (40) + ESP Trailer(16)	126	1	20.6%	YES

IEEE 802.15.4 frame, which introduces 25 bytes of the IEEE 802.15.4 header. Therefore, the total size is 117 bytes out of the 127 bytes of the MAC frame size. This means that when the CoAP payload is over 10 bytes fragmentation is required.

For the version based on the 6LoWPAN headers, the reduction is 10 bytes, i.e., the size is 82 bytes plus the payload of the CoAP Packet such as presented in the Fig. 10(a). The reduction is very low since the global addressing requires to carry in-line the source and destination addresses for both IPv6 headers, in addition, since the ports considered for the UDP header are not in the rage of the compressed ones, this requires also to carry them in-line. Consequently, the reduction is very limited. For that reason, the future work is going to be focused on analyse the feasibility of new techniques such as GLoWBAL IPv6 for the header compression of IPv6 and UDP, instead of 6LoWPAN.

Table 5 compares the overhead introduced by IPSec security in both encryption modes (AES-CCM and AES-CBC).

It has been concluded, that the use of secure communications imposes the fragmentation at link layer in 802.15.4 for all the secure communications.

8.4. Movement detection

Movement detection has been described in the Section 6.1. The ideal movement detection is based on passive overhearing but this solution is not realistic since in real environments it will be used different channels between the home network and the visited ones. For example, smart cities use an extended range of channels in order to avoid interference with other 6LoWPAN networks and existing WiFi networks working in the 2.4 Ghz frequency.

This work analyses the scan time that is required for movement detection, since this is schedule a periodic scan with energy sensing to discover new networks and measure the current link quality [29].

The total scan time depends on the number of channels to be scanned and the time spend for listening to a specific channel. The scan time per channel is an important value, which needs to be synchronized with the beacon frequency in order to detect the networks.

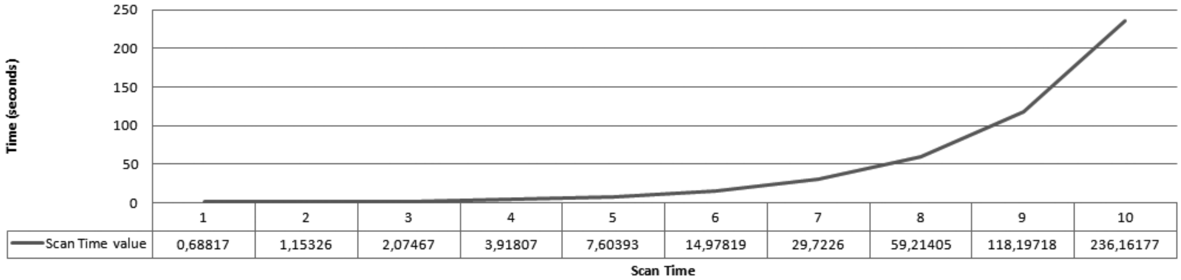


Fig. 19. Time for the different scan times considering all the channels.

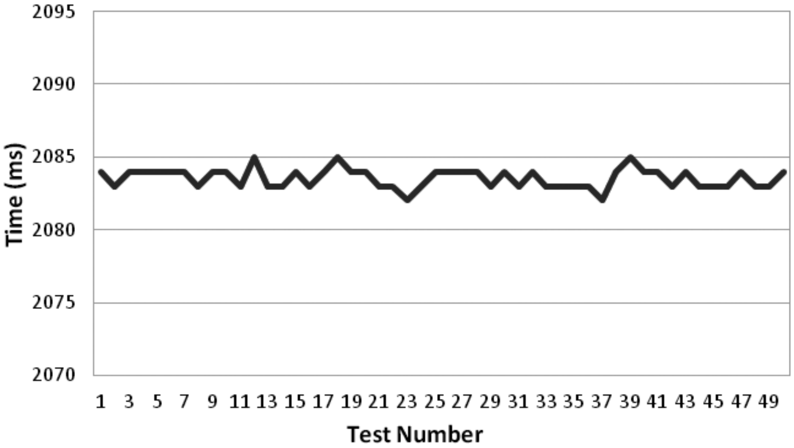


Fig. 20. Scan time with energy sensing to detect if the MN is moving and discover new networks.

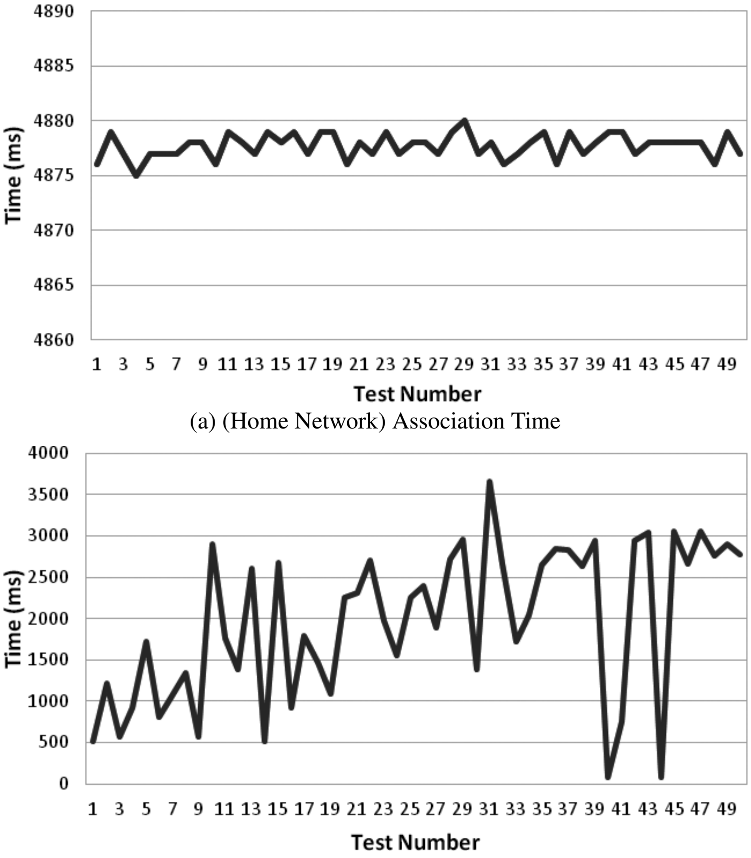
Figure 19 presents the time spend with the different scan times for scanning all the channels. For example, Contiki OS brings the scan time set to 4 by default, which means around 4 seconds. Since, for the mobility purpose scan is not only used the first time when joining to the network, else it is used periodically, this value should be reduced, in our case for the lightweight Mobile IPv6, it has been used a scan time of 3, which is a time of around 2 seconds, such as presented in the Fig. 20 for the 50 evaluation tests carried out.

The scan during the connection time cause some concerns in terms of reachability and power consumption. Specifically, the node is unreachable during the 2 seconds that the node is scanning, and the power consumption of active listening during 2 seconds for each scan.

8.5. *Handover latency*

The handover latency depends on multiple phases. First, movement detection is carried out through the active scan, since the other techniques are not feasible when multiple channels are used in an ecosystem. Second, the MN requires to associate to the new network in the link layer, i.e., link to the IEEE 802.15.4 network. Third, the MN requires to set-up the new CoA after that this receives the Router Advertisement (RA) from the visited network, and finally, the MN requires to send the BU to the Home Agent and waits for the BA.

Figure 21 presents the association time to the link layer and the time for the network layer configuration for the first connection of the MN to its Home Network. These values are presented as a reference.



(a) (Home Network) Association Time

(b) (Home Network) Router Advertisement Time

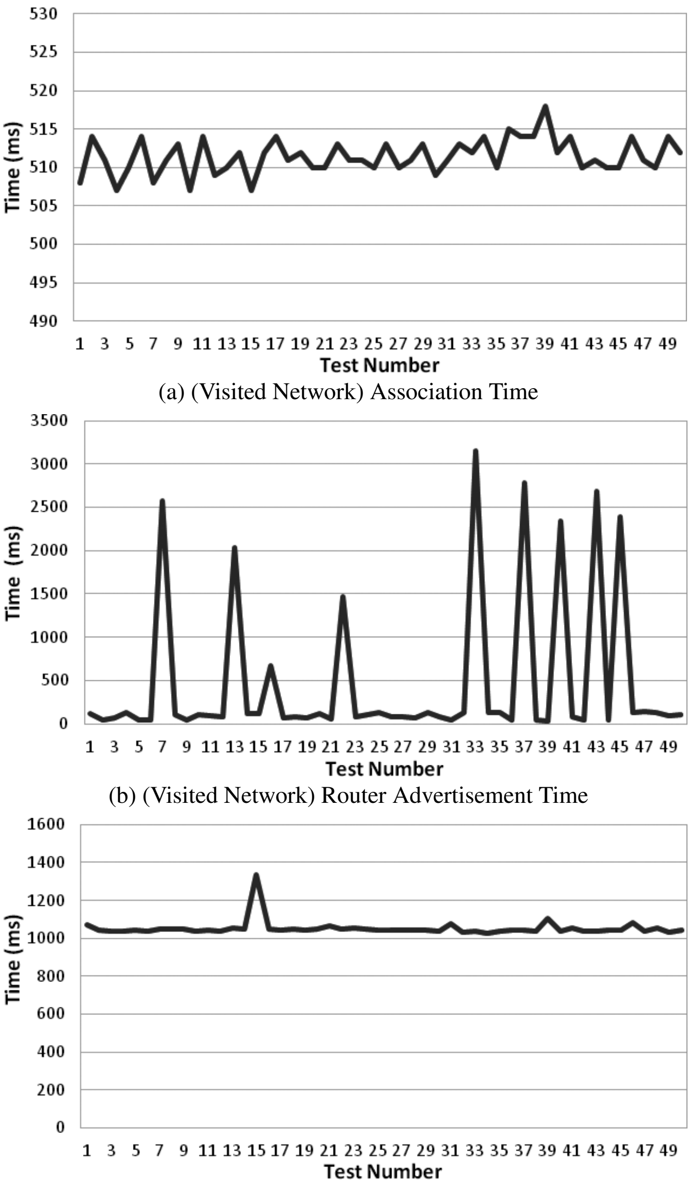
Fig. 21. Time to establish the first association in the home network and time to receive the first router advertisement in the home network.

Note, as the home association spends over 4 seconds due to that the scan time is set with the value equal to 4. The network configuration time is very random, this goes from 78 milliseconds because has received the RA just 78 milliseconds after joining, to 3,658 seconds because the RA was sent 300 milliseconds before joining to the network.

Regarding the scan time during the mobility, the scan time is presented in the Fig. 20 with a time around 2,083 seconds. When a movement change is detected, and this is considered to change the network, this spends an average of 511ms to associate at link layer with the new Border Router. The results are presented in the Fig. 22(a).

Once the link layer connection has been established. The MN waits to receive the RA in order to obtain the network layer configuration. This time is around 100ms since after the link layer association, a Router Solicitation is sent in order to improve the time to receive the network layer configuration. The time to receive the Router Advertisement is from 36 milliseconds with some random high picks of 3,151 seconds that set the average time to receive the Router Advertisement in 473 milliseconds. Figure 22(b) presents the time for receiving the RA after joining to the visited network.

Finally, the MN needs to send the BU and wait for the BA. Figure 8.5 presents the time spent for the Round Trip Time spend to send the BU and receive the BA, it is around 1 seconds with a minimum of 1,028 seconds and a maximum of 1,338 seconds.



(a) (Visited Network) Association Time

(b) (Visited Network) Router Advertisement Time

(c) (Visited Network) Binding Update to Binding Acknowledgement time

Fig. 22. a) Time to establish the association after scan in the visited network. b) Time to receive the router advertisement in the visited network. c) Time to send the BU and receive the BA.

Therefore, the handover time without considering the scan phase, since the scan phase has been part of the movement detection is presented in the Fig. 23. This presents a minimum time of 1,592 seconds, and a maximum of 4,700 seconds with an average of 2,037 seconds.

This result is very close to the handover times from other works such as the found in the softhand [15, 16], which presents a value of 2.1047 seconds.

This result shows that some state of the art results such as the 13,7 seconds mentioned in the work found in [10] for its comparative of Mobile IPv6 with respect to their MOBINET proposal can be reduced following the design issues and the optimization carried out with Lightweight Mobile IPv6.

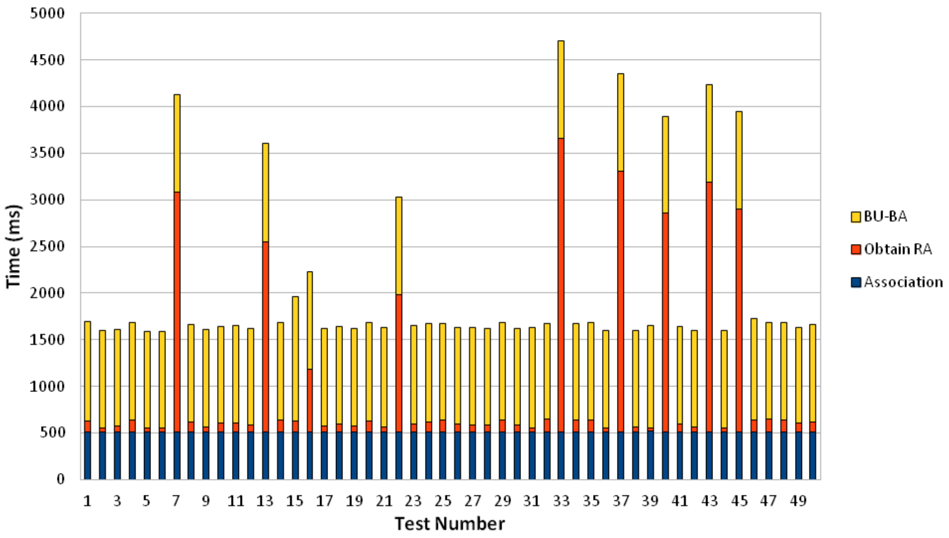


Fig. 23. Handover time for the Lightweight Mobile IPv6 protocol without scan phase.

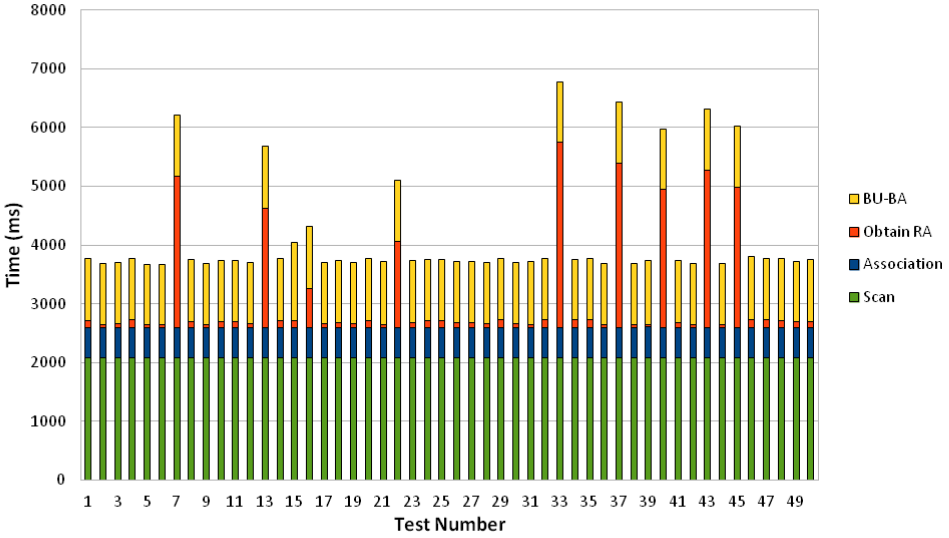
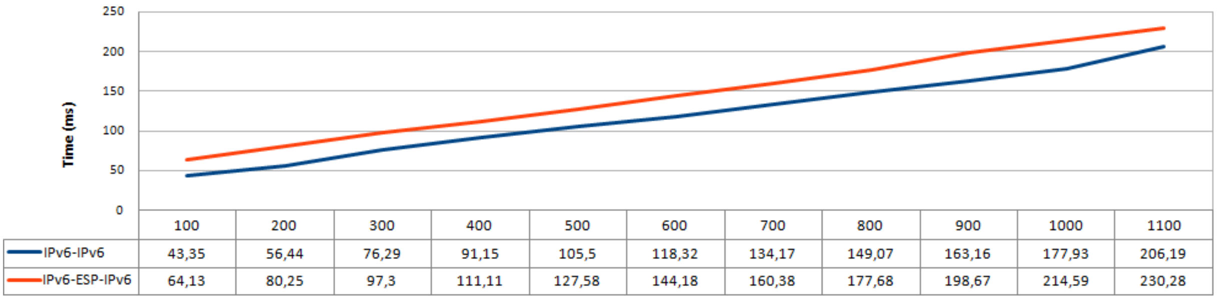


Fig. 24. Full handover time for the Lightweight Mobile IPv6 protocol.

Finally, Figure 24 presents the value also considering the scan time.

A final remark about the evaluation is that the handover latency depends on very issues related with the implementation, platform or operating system, since all these issues are ignored in simulators [11]. For that reason, this work has carried out all the evaluation with a implementation over real nodes using the Contiki OS.

The handover latency to start the process in Mobile IPv6 is influenced by the RA frequency, since the MN needs to wait for the expiration of the default router lifetime before sending new router solicitations, or wait for the router advertisement from the 6LoWPAN Border Router, which used to be very low in order to optimize lifetime from the sensors, since this packet needs to be treated by all the nodes, even after that they have already being connected.



	100	200	300	400	500	600	700	800	900	1000	1100
IPv6-IPv6	43,35	56,44	76,29	91,15	105,5	118,32	134,17	149,07	163,16	177,93	206,19
IPv6-ESP-IPv6	64,13	80,25	97,3	111,11	127,58	144,18	160,38	177,68	198,67	214,59	230,28

Fig. 25. Time impact when using ESP security during UDP transmissions of several payload lengths.

In our implementation, the measure is taking into account the association time which is the union of the RA reception and the auto-configuration from the MN. Therefore, this also introduces an extra time.

The main factor is the movement detection, the best case could be that all the networks were working in the same channel in order to be able to see other RAs from networks located at the neighbourhood. Thereby, it can be evaluated other networks without requiring an active scan.

8.6. Transmissions

The use of a triangle routing presents an impact on downstream and upstream time transmissions, since there is an intermediate routing the packets to the foreign network. But, in addition, the use of security have also an impact not only in the packet size, also in the time. This increased time is related with the time spent by the HA and the MN to include/remove ESP headers and encrypt/decrypt the packet. Home Agent and Mobile Node must include/remove 24 bytes from ESP Header (SPI, sequence and nonce using AES-CBC) and 16 bytes from ESP Trailer (Padding, Padding length and Next Header).

In order to demonstrate the impact of the security during transmissions, a set of tests has been carried out. These tests take measures from Round Trip time of UDP packets with several lengths, up to 1100 bytes of payload since when headers (outer IPv6, ESP Header, inner IPv6 and ESP Trailer) are added, the length of the packets is near to the IPv6 MTU.

Figure 25 shows RTT times measured from the test, these reflect the increased time when ESP security is used to avoid attackers along the mobility. The increased time along the several payload length goes from 19.9 ms as minimum up to 36.6 ms with an average of 25,8 ms.

9. Related works

Wireless Sensor Networks (WSN) was one of the basis areas for the IoT. Nowadays, several of IoT resources are based on wireless devices designed over protocols such as IEEE 802.15.4, which is the main protocol to develop WSN.

Mobility for WSN was addressed in the previous works. However, the majority of these proposals were defined from a point of view where IP integration was not considered. The IP integration is the main difference between the previous WSN solutions and the current IoT.

These related works are focused on the IP-based solutions. For this purpose, this section analyses, on the one hand, the different solutions for mobility supporting IPv6 from a general point of view, i.e. not considering the features and constraints of the IoT resources. On the other hand, the first approaches for mobility support with consideration of the specific features, requirements and constrains of IoT resources are analysed.

MIPV6 protocol is the most studied and well-known protocol to provide mobility in IPv6 networks. It was considered not suitable for 6LoWPAN nodes, since this presents an enormous overload for MN, because MN is involved during all the handover processes, with very weighty messages, and high processing requirements [47]. For that reason, this work has carried out a lightweight version of Mobile IPv6 in order to make it suitable for IoT resources such as 6LoWPAN nodes.

Hierarchical Mobile IPv6 (HMIPv6) [48] is an optimization of the MIPv6 regarding the subject of micro-mobility in a well-known architecture that is composed of a Home Agent (HA), gateways and several access routers to increase coverage. When MN changes access point, it only needs to update its local short 16 bit address with the gateway. Its IPv6 Care of Address (CoA) remains the same. Short addresses are managed by the topology control algorithm.

Mobile IP Fast Authentication Protocol (MIFA) [49] introduces a very simple concept on how to support macro-mobility with authentication. It defines a group known as L3-FHR (Layer 3 Frequent Handover Region) composed of the neighbours of a network, where a mobile device is able to move. This protocol also increases the functionality of the mobility entities in the visited networks, making them responsible for the authentication of the mobile nodes.

Fast Handover for Mobile IPv6 (FMIPv6) [50] is characterized by the MN being able, through the use of link layer specific mechanisms, to find available access points to request subnet information. Thereby, MN is capable of configuring its CoA while it is still located in its current network. This considerably reduces the handover latency.

The solution proposed in this work has been focused on the main protocol, i.e., Mobile IPv6, for 6LoWPAN networks.

Initial approaches have been defined to support mobility in 6LoWPAN. For mobility based on node, we defined a solution based on 6LoWPAN Neighbour Discovery [52,53], which supports micro-mobility, since it supports Extended 6LoWPANs, i.e., a group of 6LoWPAN networks interconnected through a backbone.

Regarding Mobile IPv6, a lightweight version of the Mobile IPv6 messages was suggested in [54]. This approach was similar to the idea of header compression used for IPv6 messages over IEEE 802.15.4 [32].

Finally, other approaches can be found based on Network Mobility (NEMO) [6,36–38] to reduce overload in MN, and Proxy Mobile IPv6 (PMIPv6) [6,51], where MN does not require mobile functionality in its IPv6 stack, because exchange of messages between MN and HA are delegated to a new network device, which acts as Proxy between them. These protocols are specifically appropriate for 6LoWPAN, because this avoids the involvement of MN in mobility-related signalling, but they are not applied in our approach since we are focused on en device mobility.

10. Conclusions and future work

Smart Objects are highly capable of integrating and transferring enriched data from environmental sensors, parking, activities, behaviours, home automation, intelligent transportation systems, clinical devices from mobile health, and Ambient Assisted Living (AAL) environments [6].

Wireless Sensor Networks (WSNs) are usually appointed as the missing extension to connect the virtual to the real world. Constituted by low power and low cost small nodes, WSNs have been projected for thousands of applications in several areas, such as military, healthcare, education, environment, transport, and industrial automation. Although the number of uses is increasing daily, the existent WSNs do not cover the half of them. Such situations happen because the technology evolution is not following the theoretical WSNs potential. The network technology should not limit the application; instead, it should adequately respond to its requirements. Therefore, independent of people's activity within a specific scenario, WSNs must be able and ready to support it and to provide the required reliability. In real-time monitoring scenarios such as the above, high latencies and packet losses might signify failure to detect a critical anomaly, potentially leading to disaster and/or casualties. In this context, there is a strong motivation to develop solutions for mobility support [42], since WSNs are seen as linking the virtual to the real world, and consequently it is natural that the probability of monitoring mobile bodies is truly a high one.

Mobility is one of the most important issues in next generation networks. Mobility based communication increases the fault tolerance capacity of the network, increases the connectivity between nodes and clusters, and deployment of multiple controlled mobile elements can be used to provide load balancing and gathering data.

Mobility is a requirement for continuous monitoring of vital signs in HWSN, and also for offering a suitable reachability and ubiquitous services in Smart Cities.

The HWSN and Smart City scenarios have two characteristics in common. The first one is that the application requires the highest reliability level, meaning that network failures, packet losses or delays should not occur under any situation. It is important because reaching continuous monitoring in real time makes possible the detection of health anomalies [43,44] in the case of HWSN, and a proper service and usability for Smart Cities. The second common characteristic is that the application requires user mobility, which, in turn, means the mobility of sensor nodes. For instance, patients and citizens should be able to move freely while they are connected.

Wireless Sensor Networks used for our research are IP-based in order to provide features from Internet to WSN such as global connectivity, flexibility, open standards and end-to-end communication with other systems. Particularly, it is based on IPv6 Low-Power Personal Area Networks (6LoWPANs), which are low cost communication networks that allow wireless connectivity in applications with limited power and relaxed throughput requirements. 6LoWPAN networks are constrained by their link layer technology i.e. IEEE 802.15.4, which is characterized as lossy, low-power, low bit-rate, short range and with many nodes saving energy which means long deep sleep periods. Moreover, IEEE 802.15.4 links are asymmetric and non-transitive in nature, and finally they do not define a common domain broadcast; a 6LoWPAN network is potentially composed of a large amount of overlapping radio ranges, eventually federated by either a backbone or a backhaul link.

For the mentioned constrains for 6LoWPAN, the use of classic IPv6 protocols such as Neighbor Discovery (ND) [45], IP Security (IPSec) [46], and Mobile IPv6 (MIPv6) [47] encounter several problems. For example, ND was not designed for non-transitive wireless links, the assumption of traditional IPv6 link concept i.e. a single domain broadcast and heavy use of multicast makes it infeasible [52].

Mobile IPv6 was originally not considered feasible because the overhead and requirements of security based on IPSec, but this work has presented a Lightweight Mobile IPv6 version of the problem that is an optimized version with both minimal yet sufficient for IoT nodes constraints and use cases requirements.

At the same way, IPSec was not considered feasible, since IPSec requires cryptographic primitives, which are very expensive in relation to the number of CPU cycles and memory. But, it has been presented how to make it feasible with the AES-CBC and AES-CCM cryptosuites, since they are supported by HW or presenting a low memory footprint.

In this context, this paper has presented a lightweight implementation of Mobile IPv6 with header compression, reduced footprint requirements, and the support for IPSec. Lightweight Mobile IPv6 has been implemented over the Contiki OS and evaluated successfully offering mobility with a handover under 2 seconds and an integral compatibility with the existing Mobile IPv6 implementations such as MIPV6. For the evaluation of the compatibility with the standard MIPv6, it has been validated with the tests defined by TAHI [41].

In conclusion, protocols such as MIPv6 and IPSec have presented a big challenge for its integration in constrained devices, but this work has presented that it is feasible with a memory footprint around 7,4KB for MIPv6 and 15.5KB for IPSec. The support and comparability with the existing Internet-based protocols is a major requirement in order to reach a proper IoT convergence. The link layer MUST fragment packets in 802.15.4 when IPSec security is used. At same time, IPSec introduces a brief latency due to the added time to encrypt and to send the over headed packet.

Future work is focused on evaluate the capabilities of GLoWBAL IPv6 to reduce the overhead presented by the encapsulation of the data communication and apart, the study and implementation about Next Header Compression for the several headers such as Routing Header, Destination Options Header, and ESP Header.

Acknowledgments

This work has been made possible by the means of the Excellence Researching Group Program (04552/GERM/06) from Foundation Seneca, the FP7 European Project IoT6 (grant agreement no: 288445), and the grant from the Spanish ministry for education under the FPU program (AP2009-3981).

References

[1] R. Kistler, R. Andrushevic, Y. Gasto, E. Joubert, V. Verdot and S. Chevillard, BUTLER: uBiquitous, secUre inTernet-of-things with Location and contEx-awaReness, *European Project* **287901**, IERC European Research Cluster (2013).

[2] L. Sanchez, J.A. Galache, V. Gutierrez, J.M. Hernandez, J. Bernat, A. Gluhak and T. Garcia, SmartSantander: The meeting point between Future Internet research and experimentation and the smart cities, *Future Network and Mobile Summit (FutureNetw)* (2011), 1–8.

[3] D. Siewiorek, Generation SmartPhone, *IEEE Spectrum*, http://spectrum.ieee.org/consumer-electronics/gadgets/generation-smartphone/, September, (2012).

[4] A.J. Jara, R.M. Silva, J.S. Silva, Mi.A. Zamora and A.F. Skarmeta, Mobile IP-Based Protocol for Wireless Personal Area Networks in Critical Environments, *Wireless Personal Communications* **61**(4) (2011), 711–737.

[5] A.J. Jara, M.A. Zamora and A.F. Skarmeta, HWSN6: Hospital wireless sensor networks based on 6LoWPAN technology: Mobility and fault tolerance management, *In Computational Science and Engineering, 2009. CSE'09. International Conference on*, vol. 2, *IEEE*, (2009), 879–884.

[6] A.J. Jara, M.A. Zamora and A.F. Skarmeta, An Initial Approach to Support Mobility in Hospital Wireless Sensor Networks based on 6LoWPAN (HWSN6), *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)* **1**(2/3) (2010).

[7] A.J. Jara, P. Lopez, D. Fernandez, J.F. Castillo, M.A. Zamora and A.F. Skarmeta, Mobile Digcovery: Discovering and Interacting with the World through the Internet of Things, Personal and Ubiquitous Computing, 10.1007/s00779-013-0648-0, *Springer-Verlag London*, (2013).

[8] J. Rodrigues, Performance Assessment of a New Intra-Mobility Solution for Healthcare Wireless Sensor Networks. *International Journal of Ad Hoc and Ubiquitous Computing (IJAHUC)*, (2013).

[9] T.K. Hoey, G.R. Sinniah, R. Khoshdelniat, A. Abdullah and S. Subramaniam, Mobility management schemes and mobility issues in low power Wireless Sensor Network, *In Telecommunication Technologies (ISTT), International Symposium on, IEEE*, (2012), 65–70.

[10] D. Roth, J. Montavont and T. Noel, MOBINET: Mobility Management Across Different Wireless Sensor Networks. *In: Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC'11)* (2011), 351–356.

[11] D. Roth, J. Montavont and T. Noel, Performance Evaluation of Mobile IPv6 Over 6LoWPAN. *In: Proceedings of the 9th ACM International Symposium on Performance Evaluation of Wireless Ad hoc, Sensor, and Ubiquitous Networks (PE-WASUN'12)*. ACM, New York, NY, USA (2012).

[12] A.J. Jara, D. Fernandez, P. Lopez, M.A. Zamora, L. Marin and A.F.G. Skarmeta, YOAPY: A data aggregation and pre-processing module for enabling continuous healthcare monitoring in the internet of things, *In Ambient Assisted Living and Home Care*, Springer Berlin Heidelberg, (2012), 248–255.

[13] H. Soliman, Mobile IPv6: mobility in a wireless Internet. Reading: Addison-Wesley, 2004.

[14] A.J. Jara, R.M. Silva, J. Silva, M.A. Zamora and A.F.G. Skarmeta, Mobile IPv6 over Wireless Sensor Networks (6LoWPAN): Issues and feasibility, 7th IEEE European Wireless Sensor Networks (EWSN2010), Coimbra, Portugal, 2010.

[15] R. Mendao, J. Sa Silva and F. Boavida, MIPv6 Soft Hand-off for Multi-Sink Wireless Sensor Networks, *Smart Wireless Sensor Networks, Yen Kheng Tan (Ed.),* ISBN: 978-953-307-261-6, InTech, DOI: 10.5772/13654, (2010).

[16] R. Silva, J.S. Silva and F. Boavida. Towards Mobility Support in Wireless Sensor Networks, *CRC2010-10th Portuguese Conference on Computer Networks*, 2010.

[17] J. Granjal, R. Silva, E. Monteiro, J. Sa Silva and F. Boavida, Why is IPSec a viable option for wireless sensor networks, *Wireless and Sensor Networks Security*, 2008.

[18] A.J. Jara, V. Kafle and A.F. Skarmeta, Secure and Scalable Mobility Management Scheme for the Internet of Things Integration in the Future Internet Architecture, *International Journal of Ad Hoc and Ubiquitous Computing*, Inderscience Publishers, **12**, (2013).

[19] C. Bormann, Guidance for Light-Weight Implementations of the Internet Protocol Suite, Lightweight Implementation Guidelines(LWIG) Working Group, *Internet Engineering Task Force (IETF)*, work in progress, draft-ietf-lwig-guidance-02 (2012).

[20] Z. Shelby, K. Hartke, C. Bormann and B. Frank, Constrained Application Protocol (CoAP), Constrained Resources (CoRE) Working Group, *Internet Engineering Task Force (IETF)*, work in progress, http://tools.ietf.org/html/draft-ietf-core-coap-15, (2013).

[21] S. Frankel, The AES-CBC Cipher Algorithm and Its Use with IPsec, *Internet Engineering Task Force (IETF)*, RFC 3602, (2003).

[22] R. Housley, Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP), *Internet Engineering Task Force (IETF)*, RFC 4309, (2005).

[23] C. Perkins, D. Johnson and J. Arkko, Mobility Support in IPv6, ISSN: 2070–1721, *Internet Engineering Task Force (IETF)*, (2011).

[24] S. Raza, S. Duquennoy, J. Hglund, U. Roedig and T. Voigt, Secure communication for the Internet of Thingsa comparison of link layer security and IPsec for 6LoWPAN, *Security and Communication Networks* (2012).

[25] Z. Shelby, S. Chakrabarti, E. Nordmark and C. Bormann, Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN), *IETF Request for Comments*, RFC6775, (2012).

[26] O.S. Contiki, The Operating System for Embedded Smart Objects, 2010.

[27] Z. Shelby, RFC6690 – Constrained RESTful Environments (CoRE) Link Format, *IETF Standards*, CoRE Working Group, (2012).

[28] A.J. Jara, M.A. Zamora and A. Skarmeta, GLoWBAL IP: An adaptive and transparent IPv6 integration in the Internet of Things, *Mobile Information Systems*, IOS Press, ISSN: 1574-017x, (2012).

[29] Jennic, JN-AN-1014 Checking for channel activity using the Site Survey Tool and JN-SW-4022 Jennic Production Test API, (2010).

[30] M. Castro, A.J. Jara and A.F. Skarmeta, Smart Lighting solutions for Smart Cities, *International Workshop on Pervasive Internet of Things and Smart Cities (PITSaC)*, Barcelona, Spain, (2013).

[31] M. Ersue, D. Romascanu and J. Schoenwaelder, Management of Networks with Constrained Devices: Problem Statement, Use Cases and Requirements, http://tools.ietf.org/html/draft-ersue-constrained-mgmt-03, Internet Engineering Task Force (IETF), work in progress, (2013).

[32] J. Hui and P. Thubert, Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, RFC 6282, *Internet Engineering Task Force (IETF)*, ISSN: 2070-1721 (2011)

[33] Z. Shelby, Embedded web services, *Wireless Communications, IEEE* **17**(6) doi: 10.1109/MWC.2010.5675778, (2010), 52–57.

[34] National Security Agency, Internet Protocol Security (IPsec) Minimum Essential Interoperability Requirements, v1.0.0, Core, (2010).

[35] G. Bag, M.T. Raza, H. Mukhtar, A.H. Akbar, S.M.S. Shams, K.-H. Kim, Y. Seung-wha and K. Donghwa, Energy-aware and bandwidth-efficient mobility architecture for 6LoWPAN, *Military Communications Conference 2008* **32** (2008).

[36] G. Bag, S.M.S. Shams, A.H. Akbar, H.M.M.T. Raza, K.-H. Kim and S.-W. Yoo, Network Assisted Mobility Support for 6LoWPAN, *IEEE Consumer Communications and Networking Conference*, (2009).

[37] J. Ho Kim, C. Seon Hong and T. Shon, A Lightweight NEMO Protocol to Support 6LoWPAN, *ETRI Journal* **30**(5) (2008), 685–695.

[38] Z. Yan, H. Zhou and I. You, N-NEMO: A Comprehensive Network Mobility Solution in Proxy Mobile IPv6 Network, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)* **1**(2–3) (2010).

[39] S. Cheshire, M. Krochmal and D.N.S. Multicast, RFC 6762, ISSN: 2070-1721, *Internet Engineering Task Force (IETF)*, (2013).

[40] A.J. Jara, P. Martinez-Julia and A. Skarmeta, Light-Weight Multicast DNS and DNS-SD (lmDNS-SD): IPv6-Based Resource and Service Discovery for the Web of Things, Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012 Sixth International Conference on, doi: 10.1109/IMIS.2012.200, (2012), 731–738.

[41] TAHI, Mobile IPv6 Test Profile ver. 2.0, http://www.tahi.org/mipv6/doc-2.0/MIPv6_Profile_v2_0-4.pdf (2013).

[42] S. Dixit, Wireless IP and Its Challenges for the Heterogeneous Environment, *Wireless Personal Communications* **55**(2) (2002), 261–273.

[43] A.J. Jara, F.J. Blaya, M.A. Zamora and A.F.G. Skarmeta, An Ontology and Rule Based Intelligent System to Detect and Predict Myocardial Diseases, *9Th IEEE EMBS International Conference on Information Technology and Applications in Biomedicine*. Cyprus, (2009).

[44] A.J. Jara, M.A. Zamora and A.F.G. Skarmeta, An ambient assisted living system for Telemedicine with detection of symptoms, *Bioinspired Applications in Artificial and Natural Computation Third International Work-Conference on the Interplay Between Natural and Artificial Computation.* Lecture Notes, (2009), 75–84.

[45] T. Narten, E. Nordmark, E. Simpson and H. Soliman, IPv6 Neighbor Discovery RFC4861, (2007).

[46] J. Arkko, V. Devarapalli and F. Dupont, Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents RFC 3776, (2004).

[47] D. Johnson, C. Perkins and J. Arkko, Mobility Support in IPv6 RFC 3775, (2004).

[48] H. Soliman, C. Castelluccia, K. ElMalki and L. Bellier, Hierarchical Mobile IPv6 (HMIPv6) Mobility Management, RFC 5380, (2008).

[49] A. Diab, A. Mitschele, E. Al-Nasouri, R. Boringer and J. Xu, Mobile IP Fast Authentication Protocol, Technische Universitat Ilmenau, Fachgebiet Integrierte HW/SW-Systeme, (2005).

[50] R. Koodli, Fast Handovers for Mobile IPv6, RFC 4068, (2005).

[51] C.J. Bernardos, M. Gramaglia, L.M. Contreras, M. Calderon and I. Soto, Network-based Localized IP mobility Management: Proxy Mobile IPv6 and Current Trends in Standardization, *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)* **1**(2–3) (2010).

[52] Z. Shelby, P. Thurbert, J. Hui, S. Chakrabarti, C. Bormann and E. Nordmark, 6LoWPAN Neighbor Discovery, draft-ietf-6lowpan-nd-07, Internet-Draft, *IETF*, work in progress, (2010).

[53] A.J. Jara, M.A. Zamora and A.F.G. Skarmeta, Intra-mobility for Hospital Wireless Sensor Networks based on 6LoWPAN, *The Sixth International Conference on Wireless and Mobile Communications (ICWMC2010)*, Valencia, Spain, (2010),

[54] M.-K. Shin, T. Camilo, J. Silva and D. Kaspar, Mobility Support in 6LoWPAN, *IETF*, Internet Draft draft-shin-6lowpan-mobility-01.txt, work in progress, (2009).

[55] UMIP: Mobile IPv6 and NEMO for Linux, http://www.umip.org/ (2013).

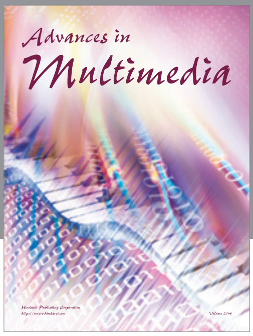
Antonio J. Jara-Valera received the B.S. (Hons. – valedictorian) degrees in Computer Science from the University of Murcia (UMU), Murcia, Spain, in 2007. M.S. Computer Science degree from the University of Murcia (UMU), Murcia, Spain, in 2009, where his Master Thesis was about "Internet of things in clinical environments". A second M.S. Computer Science degree about advanced networks and artificial intelligence from the University of Murcia (UMU), Murcia, Spain, in 2010, where his Master Thesis was about "Mobility protocols for 6LoWPAN". He is with the Department of Information and Communication Engineering, UMU, since 2007, where he is working on several projects related to the ZigBee/6LoWPAN and RFID applications in Intelligent Transport Systems (ITS), home automation and mainly healthcare. He is especially focused on security and mobility for Future Internet and its applications in healthcare, which is the topic of his Ph.D. He has published over 70 international papers.

David Fernández Ros is a MSc student at CLITech Technology group within University of Murcia, Spain. He received his BSc in Computer Engineering in Febrary 2012 at the same University. In September 2011 he started as an intern researcher in the Department of Information and Communication Engineering at the University of Murcia. He participated in the spanish AIR e-Health (AIRe) project and currently in the FP7 EU project, Internet of Things and IPv6 (IoT6). His interests are related to Internet of Things, Ubiquitous Computing, Networks and Smart everyday objects.

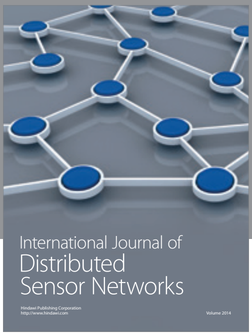
Pablo López Martínez is a Master student at CLITech group within University of Murcia, Spain. He received his BSc in Computer Engineering in July 2012 from University of Murcia, Spain. In 2012 joined CLITech within Department of Information and Communication, Faculty of Computer Sciences, University of Murcia, Spain. He participated in the spanish AIR e-Health (AIRe) project and currently in the FP7 EU project, Internet of Things and IPv6 (IoT6). His interests are related to Internet of Things, networks and ubiquitous systems.

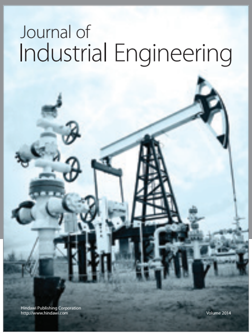
Miguel A. Zamora-Izquierdo received the M.S. degree in automation and electronics and the Ph.D. degree in computer science from the University of Murcia, Spain, in 1997 and 2003, respectively. Since 1999, he has been an Associate Professor with the Department of Information and Communication Engineering, UMU, where he works on several projects related to the remote monitoring and control with a focus on sensors system and embedded system.

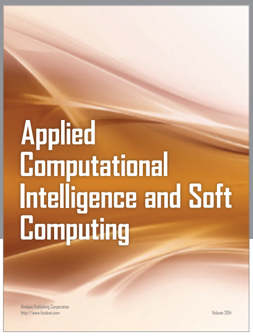
Antonio F. Skarmeta-Gomez received the M.S. degree in Computer Science from the University of Granada and B.S. (Hons.) and the Ph.D. degrees in Computer Science from the University of Murcia Spain. Since 2009 he is Full Professor at the same department and University. Antonio F. Gómez-Skarmeta has worked on different research projects in the national and international area, like Euro6IX, 6Power, Positif, Seinit, Deserec, Enable, Daidalos, ITSS6, and IoT6. His main interested is in the integration of security services at different layers like networking, management and web services. Associate editor of the IEEE SMC-Part B and reviewer of several international journals, he has published over 90 international papers and is member of several program committees.

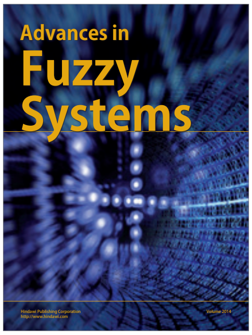

Advances in
Multimedia

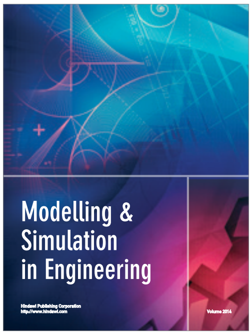
The Scientific
World Journal

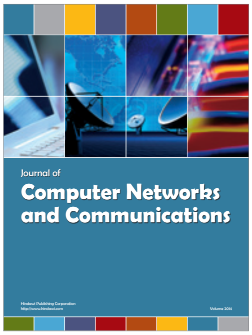

International Journal of
Distributed
Sensor Networks

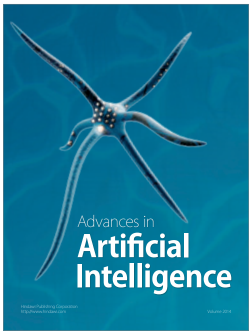

Journal of
Industrial Engineering

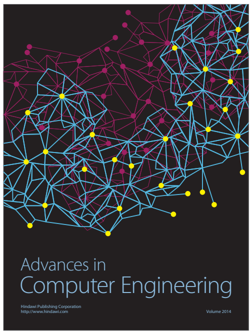

Applied
Computational
Intelligence and Soft
Computing


Advances in
Fuzzy
Systems

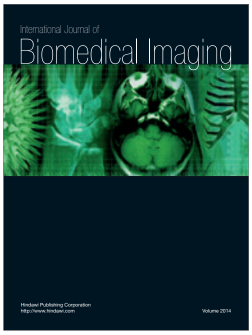

Modelling &
Simulation
in Engineering

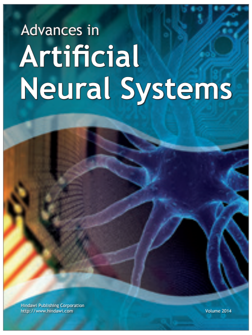

Journal of
Computer Networks
and Communications

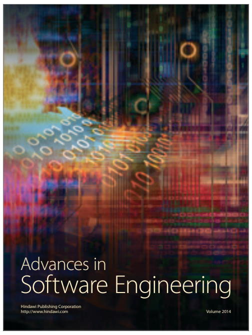

Advances in
Artificial
Intelligence


Advances in
Computer Engineering

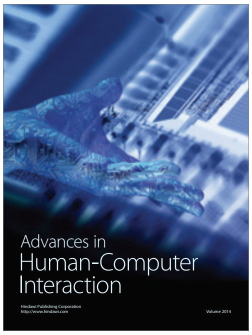
International Journal of
Computer Games
Technology

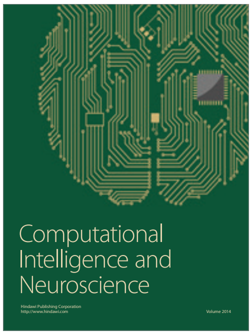

International Journal of
Biomedical Imaging


Advances in
Artificial
Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer
Interaction


Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering