Wireless Personal Communications manuscript No.
(will be inserted by the editor)

Mobile IP-based Protocol for Wireless Personal Area Networks in Critical Environments

Antonio J. Jara · Ricardo M. Silva · Jorge S. Silva · Miguel A. Zamora · Antonio F. G. Skarmeta

Received: date / Accepted: date

Abstract Low-power Wireless Personal Area Networks (LoWPANs) are still in their early stage of development, but the range of conceivable usage scenarios and applications is tremendous. That range is extended by its inclusion in Internet with IPv6 Low-Power Personal Area Networks (6LoWPANs). This makes it obvious that multi-technology topologies, security and mobility support will be prevalent in 6LoWPAN. Mobility based communication increases the connectivity, and allows extending and adapting LoWPANs to changes in their location and environment infrastructure. However, the required mobility is heavily dependent on the individual service scenario and the LoWPAN architecture. In this context, an optimized solution is proposed for critical applications, such as military, fire rescue or healthcare, where people need to frequently change their position. Our scenario is health monitoring in an oil refinery where many obstacles have been found to the effective use of LoWPANs in these scenarios, mainly due to transmission medium features i.e. high losses, high latency and low reliability. Therefore, it is very difficult to provide continuous health monitoring with such stringent requirements on mobility. In this paper, a paradigm is proposed for mobility over 6LoWPAN for critical environments. On the one hand the intra-mobility is supported by GinMAC, which is an extension of IEEE 802.15.4 to support a topology control algorithm, which offers intra-mobility transparently, and Movement Direction Determination (MDD) of the Mobile Node (MN). On the other hand, the inter-mobility is based on pre-set-up of the network parameters in the visited networks, such as Care of Address and channel, to reach a fast and smooth handoff. Pre-set-up is reached since MDD allows discovering the next 6LoWPAN network towards which MN is moving. The proposed approach has been simulated, prototyped, evaluated, and is being studied in a scenario of wearable physiological monitoring in hazardous industrial areas, specifically oil refineries, in the scope of the GinSeng European project.

Keywords 6LoWPAN · Mobility · Topology Control · Wireless Sensor Networks

---

Antonio J. Jara · Miguel A. Zamora · Antonio F. G. Skarmeta
Department of Information and Communications Engineering Computer Science Faculty, University of Murcia, Murcia, Spain E-mail: {jara, mzamora, skarmeta}@um.es

Ricardo M. Silva · Pedro Lopes · Jorge S. Silva
Departamento de Engenharia Informática, Faculty of Sciences and Technology, University of Coimbra, Coimbra, Portugal E-mail: {rnsilva,. sasilva}@dei.uc.pt

1 Introduction

Wireless Sensor Networks (WSNs) are usually appointed as the missing extension to connect the virtual to the real world [1]. 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 [2], 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. This is necessary to allow the monitoring of employees within hazardous areas such as oil refineries, chemistry and petro-chemistry industries among others. In such places employees can be under difficult and unhealthy conditions and therefore suffer hard consequences. Hence, it is highly demanded that employees are being monitored in real time, regarding for instance, common vital signs such as heart rate, SPo2 and breathing rate. Mobile WSNs allow employees to carry out their work while they are sure that if any uncommon situation in their health state is detected, an alarm will be triggered in real time. Apart from hazardous areas, within industrial environments, healthcare environments [3,4], and military areas also demand such monitoring [5].

Scenarios where WSNs are used for monitoring vital signs 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 [3,6,7]. The second common characteristic is that the application requires user mobility, which, in turn, means the mobility of sensor nodes. For instance, workers in hazardous areas should be able to move freely while they are being monitored. The same is true for firemen, soldiers and patients at hospitals.

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) [8], IP Security (IPSec) [9], and Mobile IPv6 (MIPv6) [10] 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 [18]. Another example is IPSec, which is based on cryptographic primitives [11], which are very expensive in relation to the number of CPU cycles and memory. Finally, MIPv6 which introduces overhead and requirements of security based on IPSec are not feasible either [24,12]. Therefore, the definition of optimized protocols both minimal yet sufficient for 6LoWPAN operation is required.

In this context, the objective of this paper is to propose a paradigm for 6LoWPAN mobility to satisfy the requirements for wearable physiological monitoring in hazardous industrial areas. The critical scenario considered in our research is an oil refinery. Oil refinement is a complex and dangerous process, during which any small failure can lead to disaster, with serious consequences on human lives, the environment and also the economy. Currently, the refinery, where our solution is being deployed, is equipped with thousands of wired sensors, capable of detecting all of the main potential problems. In addition, worker physiology is monitored in order to detect the possible existence of a highly polluted environment in some sections within the refinery. During the oil refinement process harmful gases are produced, and in some sections of the refinery relatively high concentrations of these gases can occur, threatening the safety and lives of the workers. Therefore, the solution proposed is to equip each worker with sensors that monitor in real-time in order to keep track of the health condition of each worker who is performing hazardous tasks, and detect problems even before they occur. In case of accident, the control center has precious information and can immediately activate emergency response teams. To detect the mentioned anomalies knowledge-based systems are used [6,7], which need continuous information from workers. Consequently, message lossy and delay can have severe consequences and can even be fatal. As such, connectivity is the most precious good, which must independent of the environmental condition and the workers' mobility be guaranteed. The proposed approach has been prototyped and is being studied in a scenario in the scope of the GinSeng European project [13], whose main objective is the monitoring of several scenarios to develop solutions for performance controlled WSNs.

The remaining sections here are organized as follows. Section 2 presents the related works. Section 3 presents the design issues of the mobility protocol. Section 4 presents the method with which the mobility protocol is supported by MAC layer. Section 5 presents the mobility protocol. Section 6 evaluates the mobility protocol. Finally, Section 7 concludes the paper.

2 Related works

Mobility in WSNs is a highly mentioned topic in the WSN literature, where different solutions have been defined in function of whether the domain has changed or not, inter-mobility and intra-mobility respectively. Other mobility classifications can be considered in function of what is moving i.e. node or network, and whether it is assisted by a proxy or not. However, the majority of these proposals are defined from a point of view where IP support is not considered. For this reason, these approaches are not suitable for WSNs based on IP such as 6LoWPAN networks. In this related work, we analysed, on the one hand, the different solutions for mobility supporting IPv6 from a general point of view, i.e. not considering the features of the end node. On the other hand, we analysed the first approaches for mobility support with consideration of the specific features, requirements and constrains of 6LoWPAN nodes. From this related work, we discovered the opportunities, limitations and possibilities to move from the current IPv6 mobility protocols towards the future 6LoWPAN mobile networks. The design issues and the basis used to define our mobility proposal are presented in the next section.

MIPV6 protocol is the most studied and well-known protocol to provide mobility in IPv6 networks, but it is not suitable for 6LoWPAN nodes, since it brings an enormous overload for MN, because MN is involved during all handoff processes, with very weighty messages, and high processing requirements [10]. Other approaches of mobility for IPv6 optimize some aspects with respect to MIPv6. They are analysed to extract optimizations, which are interesting to define a suitable mobility solution for 6LoWPAN.

Hierarchical Mobile IPv6 (HMIPv6) [14] 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) [15] introduces a very simple concept on how to support macro-mobility with authentication. It defines a group known as L3-FHR (Layer 3 Frequent Handoff Region) composed of the neighbors 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) [16] 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 handoff latency.

The solution proposed in this work is partially based on these protocols. A comparative among the different proposals, and what we have considered and enhanced from each of these IPv6 mobility protocols is presented in the Table 1. The comparative has been defined considering aspects such as the functionality of the mobility entity in the visited network, how the micro mobility is supported, whether it has defined a neighborhood map, in order to know which are the networks in its area, whether this considers pre-set-up of parameters, such as previous CoA configuration, and finally how long is the handoff, in order to determinate the handoff latency. Our design issues and proposal are focused on optimizing the mentioned aspects.

It is worth mentioning, that some initial approaches have been defined to support mobility in 6LoWPAN. For mobility based on node, we defined a solution based on 6LoWPAN Neighbour Discovery [18,19], which supports micro-mobility, since it supports Extended 6LoWPANs, i.e. a group of 6LoWPAN networks interconnected through a backbone. Functionality of mobility is delegated to Border Routers, since these check with the other routers whether a MN is accessible from other Border Routers linked to the same Backbone or not. Other initial proposals for micro-mobility are found in [29,30]. Remark, that this kind of mobility is just with nodes which are in the same subnet and does not change its IPv6 address. Furthermore, mobility is supported by a solution based on lightweight message versions of Mobile IPv6 [20]. This approach is similar to the idea of header compression used for IPv6 messages over IEEE 802.15.4 [22]. That approach is not suitable since security extensions cannot be supported, and MN receives a high overload [24].

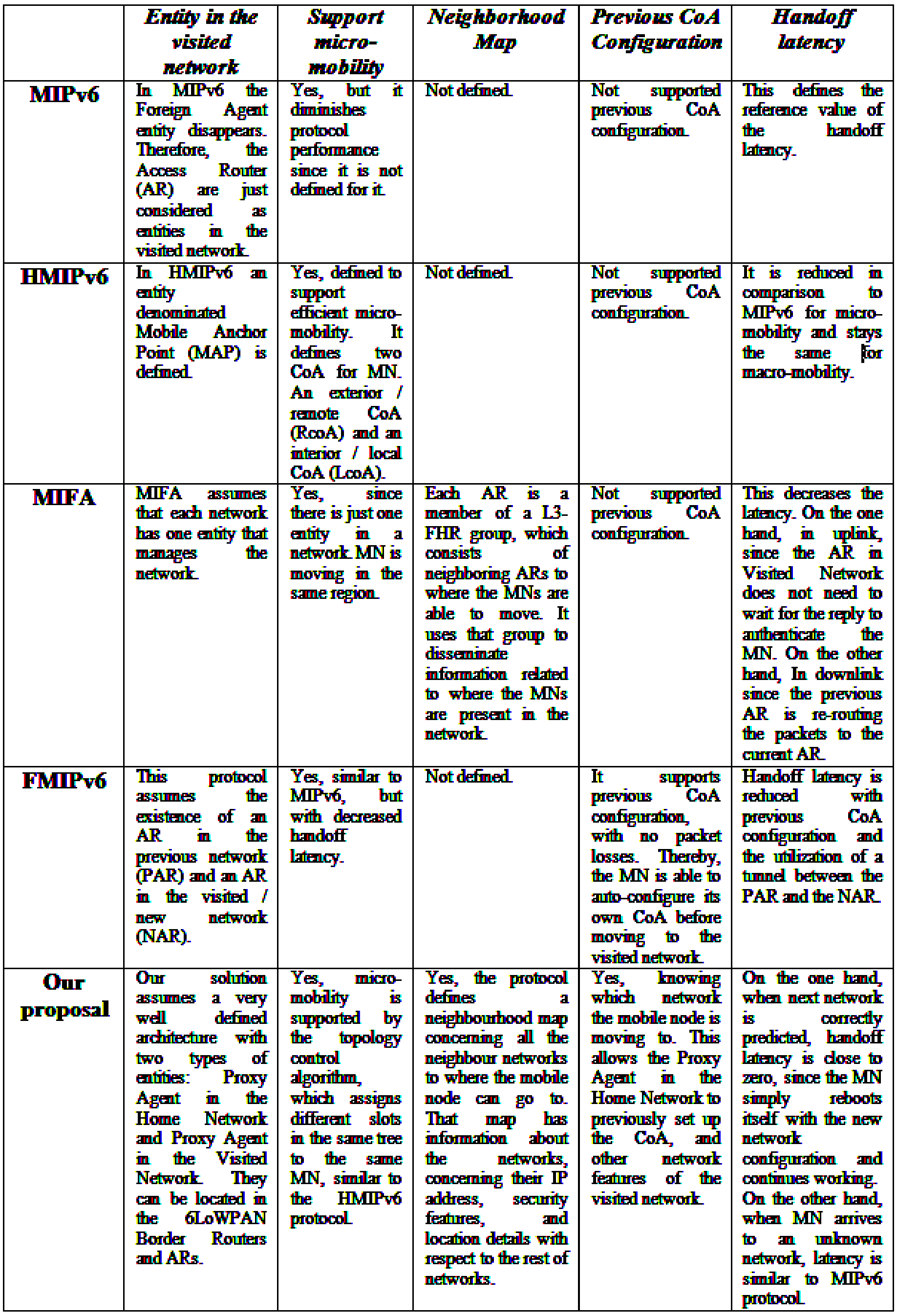
In addition, other approaches can be found based on Network Mobility (NEMO) [4, 25–27] to reduce overload in MN, and Proxy Mobile IPv6 (PMIPv6) [4,17,28], where MN does not require mobile functionality in its IPv6 stack, because exchange of messages between MN and HA are delegated to a new network device, 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. Finally, other works related to the mobility are found in [31] and [32]. On the one hand, in [31] three different paradigms are described how mobility in sensor nodes could be supported. On the other hand, in [32] a link layer specific mechanisms, which is needed between the sink node and the MN to help it perform multi-hop with communication with the gateway, is described.

3 Mobility protocol design issues

Given the low-performance properties of 6LoWPAN, new challenges arise of enabling mobility support to devices with reduced memory and power. In this section, the design issues for the 6LoWPAN mobility protocol are described. They have been defined considering our scenario requirements, the optimizations mentioned in the related works, and the results of the previous analysis that we have carried out about 6LoWPAN requirements and goals to support mobility, which can be found in [12,20].

1. Global addressing. 6LoWPAN nodes must be addressable by any corresponding node, independent of its current whereabouts. It is necessary to reach a global end-to-end connectivity with the devices through the current Internet infrastructure [20,32].
2. Mobility solutions should be compatible and based on current IPv6 protocols [12].
3. Interconnect 6LoWPANs with backbone links seamlessly. Thereby, errors and delays are not added to intra-domain handover (micro-mobility) [18].
4. Micro-mobility needs to be supported by the topology control algorithm in a local level, i.e. simple by changing short 16 bits local address, similar to the HMIPv6 protocol [12,19].
5. Reduction of related mobility signalling messages to reduce overload, specifically removing the use of multicast/broadcast flooding, which has a high cost, and signalling where Reduced Function Devices (RFDs) are involved, such as MN [21].
6. Fast mobility detection is required in order to avoid delays, high jitter and/or interruptions of the communication during handoff process. 6LoWPAN node should be able to keep continuous connectivity during handover process, or to reduce disconnection time as much as possible [20]. Therefore, node mobility needs to be detected as soon as possible so as to pre-set-up its configuration in the visited network while it is still located in its current network, similar to the pre-set-up of CoA in FMIPv6 protocol.

Table 1 Summary of different mobility protocols for IPv6 and their relation with our proposal.



	Entity in the visited network	*Support micro-mobility*	*Neighborhood Map*	*Previous CoA Configuration*	*Handoff latency*
MIPv6	In MIPv6 the Foreign Agent entity disappears. Therefore, the Access Router (AR) are just considered as entities in the visited network.	Yes, but it diminishes protocol performance since it is not defined for it.	Not defined.	Not supported previous CoA configuration.	This defines the reference value of the handoff latency.
HMIPv6	In HMIPv6 an entity denominated Mobile Anchor Point (MAP) is defined.	Yes, defined to support efficient micro-mobility. It defines two CoA for MN. An exterior / remote CoA (RcoA) and an interior / local CoA (LcoA).	Not defined.	Not supported previous CoA configuration.	It is reduced in comparison to MIPv6 for micro-mobility and stays the same for macro-mobility.
MIFA	MIFA assumes that each network has one entity that manages the network.	Yes, since there is just one entity in a network. MN is moving in the same region.	Each AR is a member of a L3-FHR group, which consists of neighboring ARs to where the MNs are able to move. It uses that group to disseminate information related to where the MNs are present in the network.	Not supported previous CoA configuration.	This decreases the latency. On the one hand, in uplink, since the AR in Visited Network does not need to wait for the reply to authenticate the MN. On the other hand, In downlink since the previous AR is re-routing the packets to the current AR.
FMIPv6	This protocol assumes the existence of an AR in the previous network (PAR) and an AR in the visited / new network (NAR).	Yes, similar to MIPv6, but with decreased handoff latency.	Not defined.	It supports previous CoA configuration, with no packet losses. Thereby, the MN is able to auto-configure its own CoA before moving to the visited network.	Handoff latency is reduced with previous CoA configuration and the utilization of a tunnel between the PAR and the NAR.
Our proposal	Our solution assumes a very well defined architecture with two types of entities: Proxy Agent in the Home Network and Proxy Agent in the Visited Network. They can be located in the 6LoWPAN Border Routers and ARs.	Yes, micro-mobility is supported by the topology control algorithm, which assigns different slots in the same tree to the same MN, similar to the HMIPv6 protocol.	Yes, the protocol defines a neighbourhood map concerning all the neighbour networks to where the mobile node can go to. That map has information about the networks, concerning their IP address, security features, and location details with respect to the rest of networks.	Yes, knowing which network the mobile node is moving to. This allows the Proxy Agent in the Home Network to previously set up the CoA, and other network features of the visited network.	On the one hand, when next network is correctly predicted, handoff latency is close to zero, since the MN simply reboots itself with the new network configuration and continues working. On the other hand, when MN arrives to an unknown network, latency is similar to MIPv6 protocol.

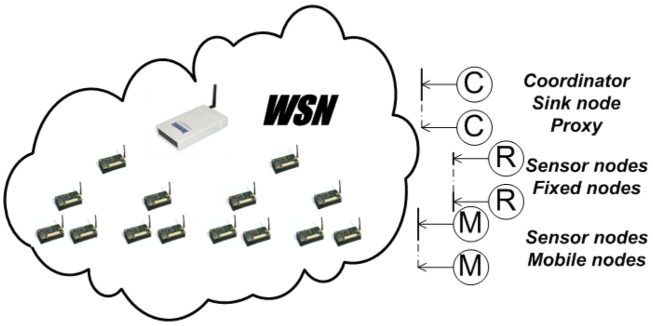


Fig. 1 Tree topology and type of nodes in the topology.

7. 6LoWPAN Border Router should act as Proxy to assist the MN in tasks such as notification to the Home Agent about the presence and movement of a MN, i.e. Binding Update may be performed by Border Router/Proxy instead of MN [4].
8. Node authentication and authorization must be supported so as to offer security capability, ensure protection of the resources, integrity and confidentiality of the information. It should be assisted by Border Routers, similar to MIFA protocol [12].
9. The mobility protocol should be based on distributed storage of information [18], rather than conventional central repository due to support fault tolerance.
10. Mobility and options header message must be optimized as much as possible to reduce the overhead for data messages in roaming. Thereby, payload can be optimized and consequently reducing the fragmentation. Messages exchanged with MN should fit within a single IEEE 802.15.4 frame to avoid fragmentation [20].

4 MAC layer support for Intra-mobility and direction determination

An extension of the IEEE 802.15.4 has been developed to fulfill the design issues imposed by the critical environments considered under the European Project GinSeng [13]. This is based on Time Division Multiple Access (TDMA), and is designed to support small networks with planned deployment. This extension of IEEE 802.15.4 has been denominated GinMAC [23]. In this section, we present those extensions, which specifically are a topology control algorithm with intra-mobility support, and movement direction determination for the inter-mobility protocol presented in the Section 5.

4.1 GinMAC topology

GinMAC topology is presented in Figure 1, it is based on a tree topology, where root node is the Coordinator, which has functionality of sink node and proxy, internal nodes, which have router functionality, and leaf nodes, which are able to be mobile nodes.

1. **Coordinator / Sink node :** This controls the network set up, and is going to be the gateway to the rest of the network. This is usually located in the Border Router.

2. **Internal router nodes / Sensor nodes:** These are located as internal nodes in the network, which function as routers. These devices are Full Function Devices (FFD). Thus, their power comes from either power line or powerful batteries, and their position is going to be fixed. For example, these can be sensors with fixed position such as motion sensor.
3. **Mobile nodes / Sensors nodes:** These are located as leaf nodes in the network, which are able to be mobile nodes. These devices are Reduced Function Devices (RFD), hence their power is based on batteries, our scenario is for workers, where their health status is monitored through wireless body sensors such as a pulse oximeter. Topology only considers mobility for lead nodes. Firstly, because it is simpler to add and remove nodes from the tree topology for the topology control algorithm, and secondly, in order to improve the lifetime of the mobile nodes, since they are not involved in tasks such as routing and message forwarding, when they are in the middle of a route in a multi-hop network.

4.2 Topology control algorithm

Topology control algorithm defined by GinMAC supports intra-mobility and determines movement direction. It has the following features to support intra-mobility:

- The tree position acquired by the MN is strongly dependent on the physical location of the MN. Inside each 6LoWPAN network, the nodes use 16-bit tree address, instead of using the IPv6 address. The coordinator is responsible for mapping this 16-bit address to the global IPv6 address in case there is a need for communicating with a corresponding node, which is located outside of the intra-domain. That 16-bit tree address is also used for routing inside the tree.
- The MN receives one of the free positions in the tree. Therefore, one of the functionalities of the topology control algorithm is to inform the MN of tree positions that it should obtain. The requirement is to always have free positions to which to attach the arriving MNs. Figure 2 presents free slots in the bottom level of the topology tree.
- A node can be attached to more than one tree position inside the same tree. This option will be helpful in case of micro-mobility where mobility occurs within the tree network domain. Figure 2 displays how a node changes its slots. As a result, the MN can have two 16-bit tree addresses at the same time. Topology control and routing will handle this situation, since the node changes its attachment points and consequently also changes its 16-bit tree address. The coordinator, which has a role very similar to the Home Agent must be notified about this change. This notification is carried out with a binding update, which is sent to the coordinator, in order to update its mapping table. In addition, the routing protocol will be responsible for updating its routing table and forwarding the data to the new location (slot in the tree) of the MN. The node can identify that it is still moving inside the same WSN by a fall in link quality below a certain threshold. That analysis of the link quality, based on Received Signal Strength Indication (RSSI) values, is explained in the next subsection.

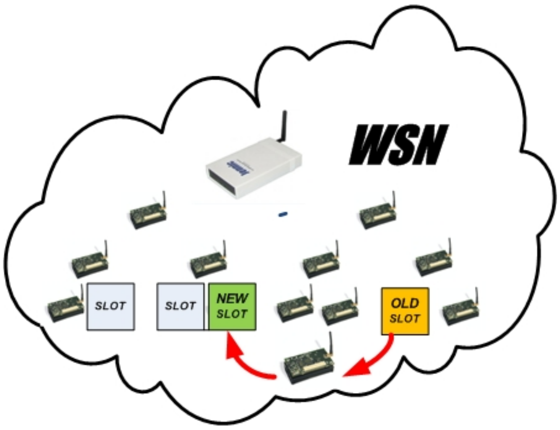


Fig. 2 Intra-mobility based on GinMAC.

4.3 Analysis of the link quality

In the GinSeng project, the GinMAC aims is to maintain good links of each node with at least other three nodes, in order to satisfy that requirement, the router nodes need to monitor a set of parameters in real time such as RSSI values to detect movement and determine movement direction. During movement the node may be in a state where it is actively communicating or it might be completely silent. In the first case the application allows to detect the movement of the node without using any extra features. However, in the second case, i.e. when the node is not communicating, additional mechanisms are defined to make sure that mobility is detected in time and the handoff disconnection time remains under a predefined maximum value. To overcome this problem topology control algorithm uses the KEEP-ALIVE and NODE-ALIVE messages [28]. The KEEP-ALIVE message is sent by the parent every X seconds where $X \in \mathbb{N}$. Consequently, the MN is aware of the time to receive the KEEP-ALIVE message. when MN does not receive the KEEP-ALIVE message, then it transmits the NODE-ALIVE message, and waits for the acknowledgement. Finally, if the acknowledgement is not received then the MN sets the mode to scan.

This solution allows to ensure a specific maximum disconnection time during handoff. However, it is also improved with the following method to detect critical zones. Thereby, it can detect when change of network is going to happen. Figure 3 presents the situation when a KEEP-ALIVE is received, whose RSSI value is in the critical zone. The critical zone is the interval between the threshold and the rupture point. This zone is obtained dynamically based on node direction, velocity and noise. In the GinSeng project a predefined threshold value was established, and therefore the critical zone [28]. Since the current RSSI is within the critical zone, nodes are automatically entering the scan mode searching for a new attachment point (parent). Topology control algorithm will be responsible to find a new attachment point for the MN.

Another possible situation is shown in Figure 4, when the received RSSI value of KEEP-ALIVE is on the left side, i.e. the RSSI is not in the critical zone, but with high probability that it will enter the critical zone soon. Since there is no further message sent in the next X seconds, the MN will be disconnected and it will not be possible to detect this, neither to localize it. Therefore, NODE-ALIVE message is included to be

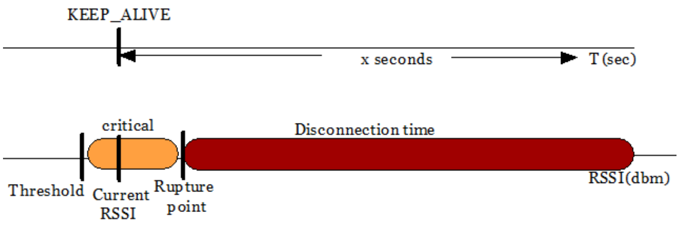


Fig. 3 RSSI and KEEP-ALIVE relationship in critical zone.

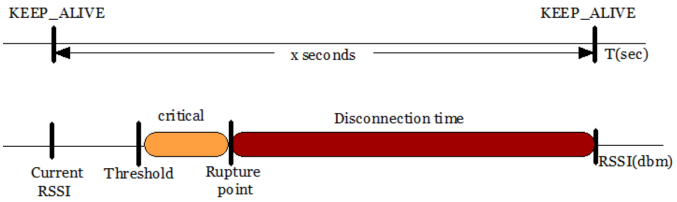
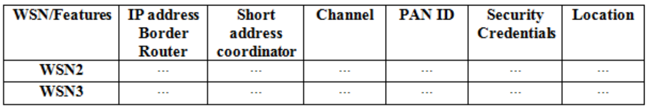


Fig. 4 RSSI and KEEP-ALIVE relationship out of critical zone.



WSN/Features	IP address Border Router	Short address coordinator	Channel	PAN ID	Security Credentials	Location
WSN2	...	...	...	...	...	...
WSN3	...	...	...	...	...	...

Fig. 5 Neighborhood Map located in WSN1's Proxy Agent.

sent after the expected KEEP-ALIVE message. For instance, if the KEEP-ALIVE interval is set to 30 seconds, at the end of the interval the MN will send a NODE-ALIVE message if no further messages have been received. After sending NODE-ALIVE, MN must receive an acknowledgement. If not, it will enter the scan mode searching for a new attachment point. As mentioned before, topology control will take care of that. The MN will then switch to scan mode in order to receive an advertisement of a new position.

4.4 Direction movement determination

Direction movement determination is used to estimate the next network, i.e. WSN where the MN is moving. It is based on RSSI values from router nodes, which are deployed in fixed positions. A special structure of information has been defined in the Proxy Agents, *Neighborhood Map*, where the information is stored about the rest of WSNs of the neighborhood, it is used to communicate with the Proxy Agent of the visited network, and pre-set-up the network configuration in the visited network of the MN. An example of *Neighborhood Map* is presented in Figure 5.

Following Figure 6, RSSI table has references for the MN from routers R1 to R6, where all RSSI values are stored in the Proxy Agent (located in the Border Router). Once the information about RSSI is available, localization method determines movement direction. Localization methods in WSNs have played an important role within of the scientific community. Recently, with the popularity of WSNs, wireless localization becomes even more desired. Designed to detect events while monitoring specific

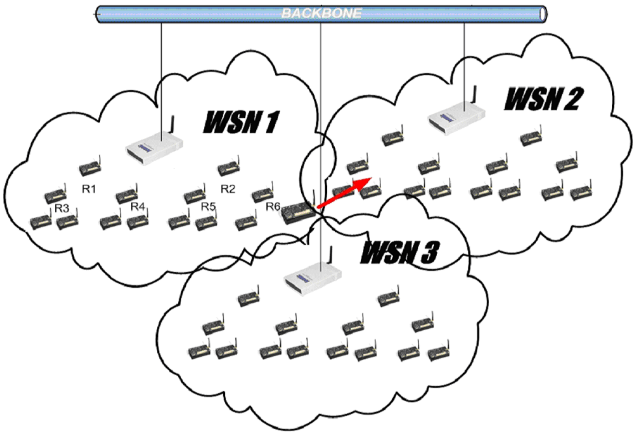


Fig. 6 Extended 6LoWPAN and inter-mobility scenario.

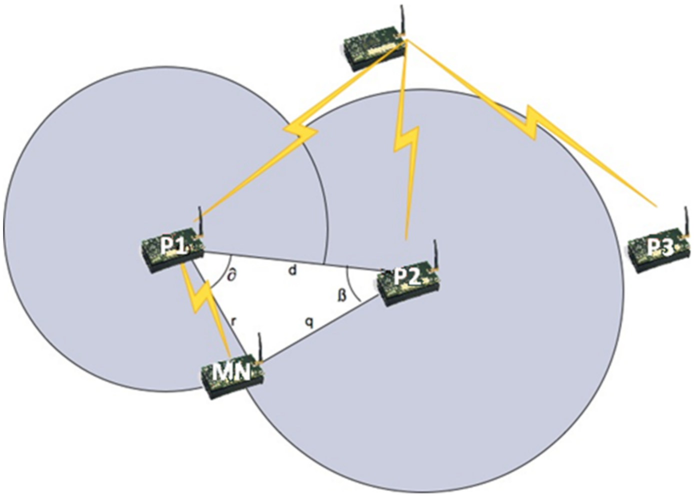


Fig. 7 Direction movement determination in an Extended 6LoWPAN for inter-mobility.

parameters, node localization is a requirement to accurately determine where the event occurs. In addition, these methods have been previously used in cellular networks to reach smooth handoff [33], where it is reachable, since cellular networks have fixed infrastructure, well-known antenna location and mainly directional antennas, which make movement direction easier to detect. Our approach is based on omnidirectional antennas and devices with very constrained capacity to estimate movement direction. For these constrains, mobility protocol is based on movement direction determination instead of accurate location.
There are three common techniques to get a node localization [34]. The first type is based on knowing the distance and direction from a known point (x, y). The second type is based on previously knowing the direction from two known points (x_1, y_1) and (x_2, y_2). Finally, the third type is based on knowing the distance from three known

points (x_1, y_1), (x_2, y_2) and (x_3, y_3). From these three methods, the two firsts require directional antennas. Otherwise, it would not be possible to get direction; the most well known example is the Angle of Arrival (AoA) algorithm [35]. The third method, based on the three well-known points can be easily used with ordinary omnidirectional antennas and therefore is more suitable for common wireless networks, including WSNs. Those algorithms get such parameters from signal propagation. Some calculate the distance based on signal delay, while others calculate it based on signal strength i.e. RSSI. Time of Arrival (ToA) [35] and Time Difference of Arrival (TDoA) [36] are popular examples of signal delay based solutions. The first requires node synchronization in order to accurately achieve the three distances. The second does not require synchronization since it uses a signal correlation to compute distances. Knowing the signal strength in the sender and comparing it in the receiver, makes signal strength also a valuable and widely used tool to compute distances.

Our mobility protocol does not need to get the accurate node position, but it needs to determine the node movement direction. To carry it out with the common omnidirectional antennas available in wireless sensor nodes, we aim to estimate distances between existent fixed nodes with well-known positions, accomplishing this with the third described method. As a result, we are able to determine towards which network the MN is moving, in order to speed up the handoff and registration in visited network process.

Based on the case study in the oil refinery, the network is previously configured and deployed following a tree topology with the maximum of 3 levels and no more than 25 nodes. Although the leaf nodes are able to be MN, the positions of all router nodes (internal nodes) are well-known. Hence, it is possible to determine movement direction of the MN based on the position of the internal routers of its neighborhood. The method proposed is based on angles between relative vectors constituted by the routers and MN locations. Figure 7 displays the scenario.

Let P1 and P2 be static internal routers, and MN be a leaf node. All of them with relative coordinates (x, y). Our goal is to establish a virtual triangle defined by those 3 points ($\triangle$), and calculate the angles $\delta = P1MN \wedge P1P2$ and $\beta = P2MN \wedge P2P1$. The first step is to get the MN coordinates. it is possible to obtain the distance between two nodes [37] based on RSSI. For that purpose, communication among at least 3 nodes periodically is necessary to reach an accurately monitor direction.

In addition, knowing distance between P1-MN and P2-MN from RSSI values, it can be assumed that these distances are radius circle (r and q) in which MN is one intersection point (see Figure 7). Through δ and β the MN movement direction is determined by comparing the previous measurement, relative to P1 and P2, with the current measurement. This is a purely geometric method, where uncertainty models to avoid additional computational cost in the node processors have not been considered, taking into account that we are looking only for a thick direction towards the next network. This method is evaluated in Section 6.

5 Mobility protocol for inter-mobility

GinMAC supports intra-mobility. Therefore, the next step to reach a full mobility solution is to support smooth handoff in inter-pan mobility, but it is not possible, since GinMAC is based on TDMA, such as mentioned in Section 4, and for TDMA and Frequency Division Multiple Access (FDMA), where different frequency ranges are used

in adjacent WSNs in order to minimize channel interference, only hard handoff is possible. Therefore, it is feasible with brief disconnections in order to switch the radio to reconfigure channel, AES 128-bit key of the MAC security, 16-bit short address etc. Consequently, in inter-mobility our challenge is to reduce time for handoff, i.e. reduce the latency which adds mobility protocol during handoff process. Time handoff latency is what is being optimized with our mobility paradigm.
Figure 6 presents an inter-mobility scenario, which is also known as Extended 6LoWPAN. Extended 6LoWPAN scenarios are a set of WSN connected through a backbone, which is an Ethernet network, WiFi, 868Mhz, GPRS or for more extended deployments it may be the Internet. Particularly, we are deploying it with Jennic Border Routers, which offers Ethernet network interface for backbone communication.
The mobility paradigm proposed is based on movement direction determination, and handoff assisted by Proxy Agent in home and visited network. As such, movement direction determination defines which is the next WSN, and Proxy Agents pre-set-up the configuration, such as FMIPv6. In addition to support security, authentication steps are also carried out by Proxy Agents. They optionally are able to communicate with a AAA server to authenticate to the other Proxy Agents. Credentials for authentication are also located in neighborhood map (see Figure 5). Thereby, it can carry authentication out before change of network, such as MIFA. The relation of our proposal with the mentioned mobility protocols is summarized in Table 1.
Therefore, on the one hand, movement direction determination of the next WSN allows to carry out authentication and MN configuration before the MN change of network, and on the other hand, authentication of MN is carried out by Proxy Agents.

The pre-set-up of the MN configuration follows the next steps:

1. Firstly, Proxy Agent of the home network detects that the MN is moving, and notifies the Proxy Agent of the visited network.
2. Proxy Agent of the home network sends authentication information about its MN.
3. Proxy Agent of the visited network replies to the Proxy Agent of the home network with the configuration information for the MN in its network, such as short address, IPv6 address, AES 128-bit key etc.
4. Proxy Agent of the home network notifies MN that is leaving its network and provides MN its configuration in the visited network.
5. MN changes its configuration, when its connection goes down by the defined threshold (MAC layer notification, see section 4.3).
6. Set up new configuration and send *Arrived Confirmation* to Proxy Agent in visited network. Finally, Proxy Agent in visited network informs about this to Proxy Agent in home network.

The pre-set-up of the MN configuration steps, information about the protocol and the role for each entity involved during mobility are presented in the flowcharts in Figure 8, Figure 9, and Figure 10.

Figure 11 presents the exchange of messages when movement direction determination is right. Firstly, Proxy Agent of the home network detects that the MN is moving out of its domain. As such, it calculates, with the RSSI table and the Neighborhood Map, the next visited network. Home Agent sends *Node Registration* messages to the Proxy Agent of the visited network, *Node Registration* is composed of the credentials of the MN, which may be checked with the AAA server. If credentials are correct, Proxy Agent of the visited network replies to the Proxy Agent of the home network with the

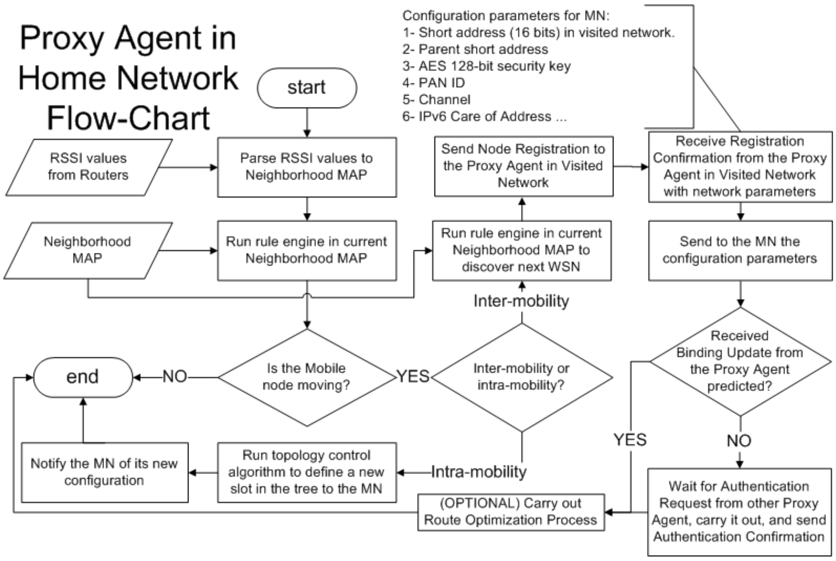


Fig. 8 Proxy Agent in the Home Network Flowchart.

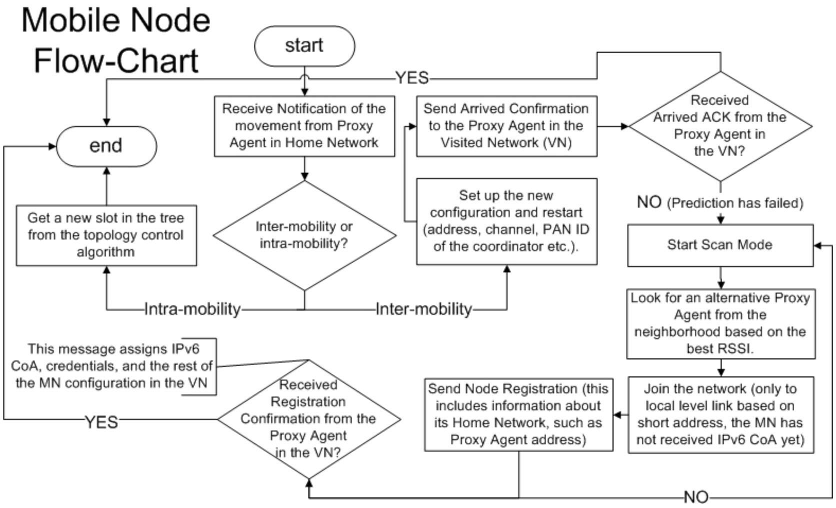


Fig. 9 Mobile Node Flowchart.

Node Confirmation message, which includes the information presented in Figure 8, e.g. CoA, short address, security key, etc. Proxy Agent of the home network notifies the MN with *Mobility Notification* message. It includes the configuration information in the visited network in the same way is *Node Confirmation*. MN will use that information to change its configuration when GinMAC detects that signal level is under the critical zone. MN in the visited network announces its presence with *Arrived Confirmation* message, which is confirmed with *Arrived ACK* message to the MN from Proxy Agent of the visited network, while it is also notified to the Proxy Agent of the home network

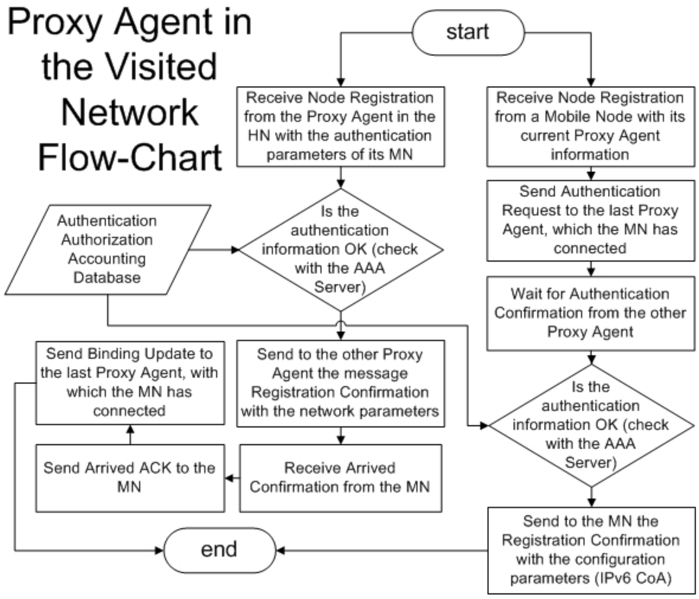


Fig. 10 Proxy Agent in the visited network Flowchart.

Table 2 Angles obtained during the evaluation iterations with Cooja and Bonnmotion.

Iteration	∂	ß
1	66.4º	25.8º
2	53.1º	25.8º
3	25.8º	25.8º
4	25.8º	45.6º
5	25.8º	60.0º
6	25.8º	70.1º
7	25.8º	74.3º
8	24.6º	74.3º
9	24.6º	80.6º
10	20.2º	80.6º
11	17.7º	80.6º
12	17.7º	70.1º
13	17.7º	63.3º
14	17.7º	50.0º
15	17.7º	44.8º
16	20.3º	47.6º
17	46.9º	25.8º
18	66.4º	25.8º
19	74.3º	25.8º
20	80.6º	24.6º

with the *Binding Update* message.

Figure 12 presents the case when movement direction determination is wrong, and consequently MN cannot join the visited network. In that case it starts to scan networks, and when it detects a network, it joins and sends *Node Registration* messages with its security credentials. Proxy Agent of the visited network sends *Authentication Request* to the Proxy Agent of the home network to confirm that MN credentials are correct, Proxy Agent of the home network checks the credentials of the Proxy Agent in the visited network, and if they are valid, it confirms to the Proxy Agent of the visited network with *Authentication Confirmation* message. Finally, Proxy Agent of the visited network checks credentials, and sends *Registration Confirmation* message to the Mobile Node to finish handoff and authentication process.

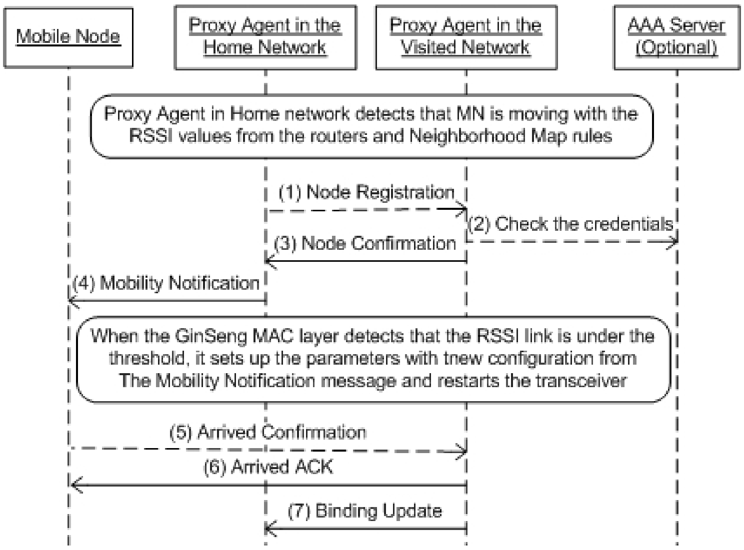


Fig. 11 Exchange of messages when the prediction is right

Table 3 parameters used by Bonnmotion.

Number of nodes	100 nodes.
Simulation time	900 seconds.
Initial period phase	3600 seconds, this period is discarded, since that the nodes are initially distributed randomly, they take some time until reach a stationary distribution.
Velocity and pause periods	They are uniformly distributed from a minimum to a maximum value chosen randomly by the simulator.

6 Results and evaluation

The evaluation is divided into three parts. Firstly, we evaluate the accuracy of mobility direction determinations based on Cooja simulator. Secondly, we evaluate the handoff latency and overload for MN based on Omnet++ simulator. Finally, we evaluate the full process in a real deployment based on Jennic 6LoWPAN solution.

6.1 Movement direction determination

Movement direction determination has been simulated and tested with the ContikiOS simulator [37], i.e. Cooja. The simulation scenario is shown in Figure 13, this displays one Proxy Agent (localized in the top), two internal router nodes (localized in the middle) and one MN (localized above in green color). Mobility has been simulated with Boonmotion [39] and the RandomWaypoint model. The simulated motes were based on the Tmote sky platform, which is equipped with the MSP430 and Intel 8051 processor, where math functionality is highly constrained, to implement our movement direction determination algorithm. Thus, some accuracy is lost due to the lack of floating points support, and the reduced precision of the integers. However, positive results were archived.

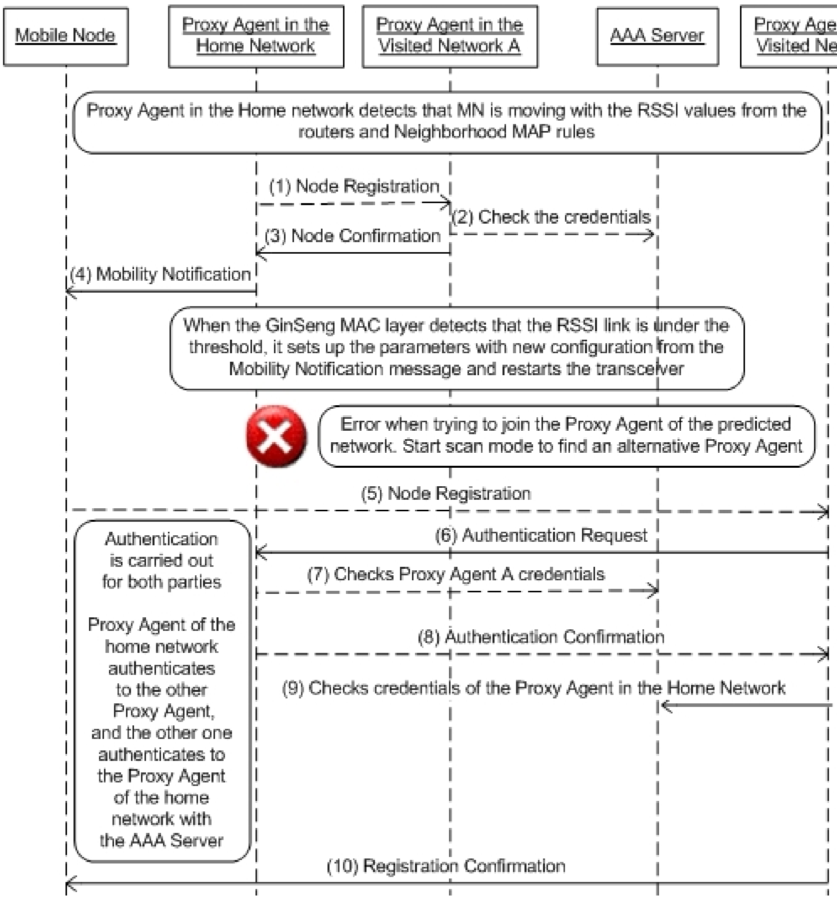


Fig. 12 Exchange of messages when the prediction is wrong.

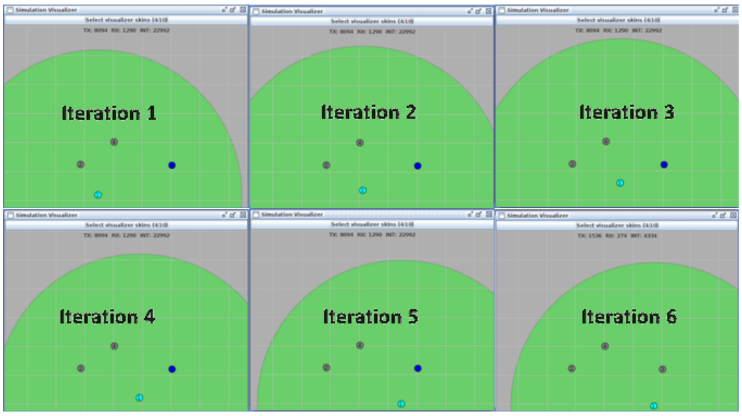


Fig. 13 Tested scenario in Cooja simulator.

The Proxy Agent calculates the direction of the MN, based on the reports received from each internal router node. Considering that parents can be any other mote present in the network range in a specific time or period, it is not critical to require them in the targeted scenario.

The evaluation has been carried out for 20 movements followed during a simulation time of 900 seconds, the δ and β values are presented in Table 2. Figure 13 displays the first 6 movements. The path followed by the MN is based on the RandomWaypoint mobile model from Bonnmotion tool. Table 3 presents the Bonnmotion parameters.

The speed and the periodicity of the mobile nodes movement are defined in a trace file, which was randomly generated using Bonnmotion. Therefore, it is a random mobile pattern using different speeds and different periodicities.

In the presence of these values, movement direction can quickly be obtained for each iteration. For instance, by calculating the difference between the first and the second iteration, we know that the MN moved 13.3° to the right, maintaining the 25.8° of β, which means that it was moving in direction to P2. Then, in iteration 3 the MN continues straight to P2 and in iteration 4 it suddenly changed direction, continuing movement to the right, but now in the opposite direction to P1, at least until iteration 6. Following this method, the time spent for the movement direction determination by Tmote Sky mote is around 31 milliseconds (this depends on the RSSI values for the complexity of each power and square operation); this time is equivalent to 248000 cycles considering the CPU speed of the Tmote Sky (8 Mhz). Therefore, direction can be effectively obtained and the next network determined in time.

In the 20 presented simulations, in different positions, we concluded that our method was ***95.4% accurate*** when compared to the theoretical results. This difference is mainly caused by the implementation of the method without floating points, which are not supported by mspgcc, and the errors in the measurement (simulated errors in order to reach more realist result). However, 4.6% error in the achievement of the MN direction should not be critical in a real scenario, where the number of existent adjacent networks is not so big.

6.2 Mobile node overload and handoff latency

The aim of this evaluation is to determine, on the one hand, node overload, and on the other hand, handoff latency. This part of the evaluation has been carried out with Omnet++ [38], where the messages exchanged in our protocol, nodes involved, and medium features for inter-mobility have been defined. The messages length have been estimated defining the required fields for each message, and the medium features defined for IEEE 802.15.4 link are based on the performance results of [40].

Firstly, an usual MN handoff process is explained, in order to show from this our optimizations. The first step, in order to access an MN to a visited network, is to scan for medium as such to discover an alternative Border Router which connect to. This time is defined as T_{scan}, which depends on the channel which is the next network, and medium status. In addition, we need to consider a time to join, which is T_{join}, to the IEEE 802.15.4 network (MAC layer). Then, the negotiation process starts to carry out some task, such as to get CoA and to announce to HA about the mobility (Binding Update). Finally, we need to add time to authenticate the MN and the access router in the visited network. This time is $T_{authentication}$. Therefore, handoff latency can be reduced with some of these four measures of time. The total handoff time is presented in Equation 1.

Our proposal is to remove from the handoff time, the time spent in the Scan, Negotiation and Authentication steps. In order to reach this goal, we propose to carry out these steps previous to the change of the network, such as FMIPv6 for CoA negotiation, and MIFA for authentication. Therefore, the handoff time is, when movement direction determination is correct, equal to that presented in Equation 2. Otherwise, when the prediction is wrong, it is equal to that presented in Equation 1.

On the one hand, Figure 14 presents the messages exchanged, scenario simulated and latency times, when movement direction determination is right. On the other hand, Figure 15 presents when it is wrong.

The table from Figure 14 presents a summary of the latency time added by each one of the steps from the handoff process, when movement direction determination is right. Notice that MN is just involved for 2 messages. As much, overload in MN is highly reduced with respect to MIPv6, where MN is involved for all the mobility control messages. Negotiation and Authentication steps are supported by Proxy Agents. Scan and Join steps are removed, since configuration is defined before arriving to the visited network, consequently time offline is close to zero, because MN only needs to restart transceiver with the new configuration.

Table from Figure 15 presents a summary of the latency added by each one of the steps from the handoff process when movement direction determination is wrong. MN is only involved for 2 messages, in the same way as when prediction is correct. Therefore, overload in MN continues being low. Negotiation and Authentication steps are supported by Proxy Agents. Time offline is increased with the time used to solve the problem because of the wrong prediction, i.e. $T_{scan-join}$, and the time to authenticate and register with Proxy Agent in the visited network. Specifically, the offline period starts when trying to join the Proxy Agent of the next determined network, followed by $T_{scan-join}$ of an alternative Proxy Agent, and then the protocol for this special case, which starts with *Node Registration* message to the new Proxy Agent, and finishes with *Registration Confirmation*. Therefore, time offline in this case is high with respect to when prediction is correct. Proxy Agents will keep messages while MN is offline. Finally, remark that approximate 58% handoff time (without $T_{scan-join}$) is used for authentication, thus one possible solution to reduce handoff time is based on decrease security level, but this option only should be considered in extreme cases such as real-time applications.

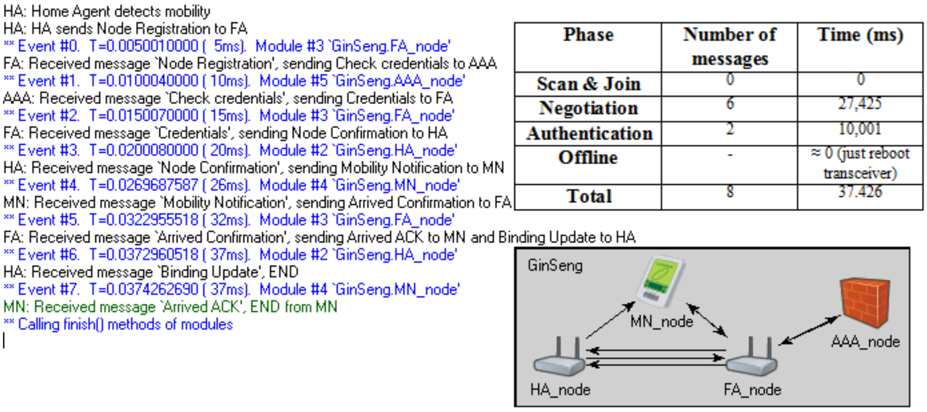
$$T_{handoffpredictionwrong} = T_{scan} + T_{join} + T_{negociation} + T_{authentication} \tag{1}$$

$$T_{handoffpredictionright} = T_{join} \tag{2}$$

6.3 Evaluation in a real deployment based on the Jennic 6LoWPAN solution

An evaluation of the protocol has been carried out over the 6LoWPAN solution from Jennic, which has been one of the first vendors offering 6LoWPAN Border Routers with Ethernet interface in order to connect to the Backbone. Figure 16 displays the deployment carried out on the first floor of the Computer Science Faculty at the University of Murcia. This deployment is composed of 3 Border Routers, 9 internal routers and a MN.

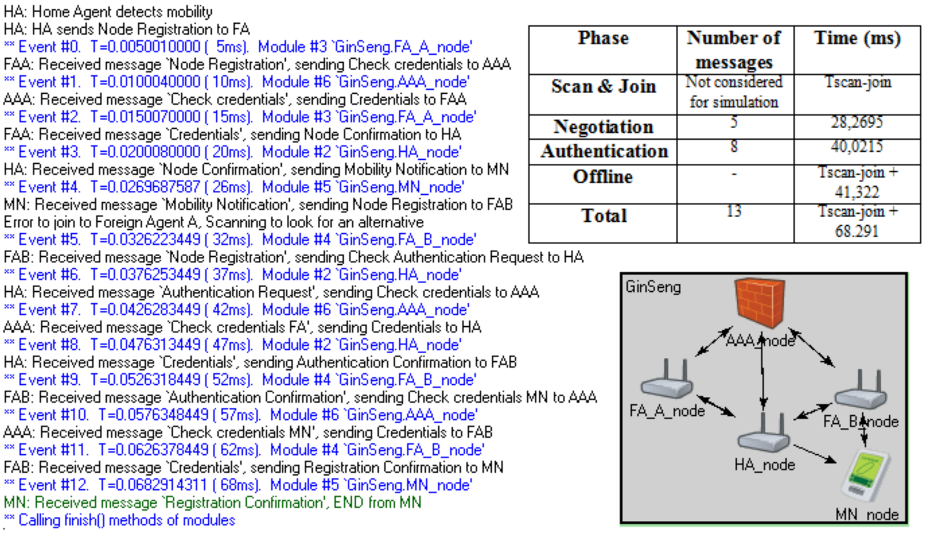
For this evaluation, we have found the problem that Border Routers from Jennic are



```
HA: Home Agent detects mobility
HA: HA sends Node Registration to FA
** Event #0.  T=0.0050010000 (  5ms).  Module #3 `GinSeng.FA_node'
FA: Received message `Node Registration', sending Check credentials to AAA
** Event #1.  T=0.0100040000 ( 10ms).  Module #5 `GinSeng.AAA_node'
AAA: Received message `Check credentials', sending Credentials to FA
** Event #2.  T=0.0150070000 ( 15ms).  Module #3 `GinSeng.FA_node'
FA: Received message `Credentials', sending Node Confirmation to HA
** Event #3.  T=0.0200080000 ( 20ms).  Module #2 `GinSeng.HA_node'
HA: Received message `Node Confirmation', sending Mobility Notification to MN
** Event #4.  T=0.0269687587 ( 26ms).  Module #4 `GinSeng.MN_node'
MN: Received message `Mobility Notification', sending Arrived Confirmation to FA
** Event #5.  T=0.0322955518 ( 32ms).  Module #3 `GinSeng.FA_node'
FA: Received message `Arrived Confirmation', sending Arrived ACK to MN and Binding Update to HA
** Event #6.  T=0.0372960518 ( 37ms).  Module #2 `GinSeng.HA_node'
HA: Received message `Binding Update', END
** Event #7.  T=0.0374262690 ( 37ms).  Module #4 `GinSeng.MN_node'
MN: Received message `Arrived ACK', END from MN
** Calling finish() methods of modules
|
```

Phase	Number of messages	Time (ms)
Scan & Join	0	0
Negotiation	6	27,425
Authentication	2	10,001
Offline	-	≈ 0 (just reboot transceiver)
Total	8	37.426

Fig. 14 Tested scenario in Omnet++ when prediction is right (see Figure 11). MN-node is the Mobile Node, AAA-node is the AAA server, FA-node is the Proxy Agent in the visited network, and HA-node is the Proxy Agent in the home network.



```
HA: Home Agent detects mobility
HA: HA sends Node Registration to FA
** Event #0.  T=0.0050010000 (  5ms).  Module #3 `GinSeng.FA_A_node'
FAA: Received message `Node Registration', sending Check credentials to AAA
** Event #1.  T=0.0100040000 ( 10ms).  Module #6 `GinSeng.AAA_node'
AAA: Received message `Check credentials', sending Credentials to FAA
** Event #2.  T=0.0150070000 ( 15ms).  Module #3 `GinSeng.FA_A_node'
FAA: Received message `Credentials', sending Node Confirmation to HA
** Event #3.  T=0.0200080000 ( 20ms).  Module #2 `GinSeng.HA_node'
HA: Received message `Node Confirmation', sending Mobility Notification to MN
** Event #4.  T=0.0269687587 ( 26ms).  Module #5 `GinSeng.MN_node'
MN: Received message `Mobility Notification', sending Node Registration to FAB
Error to join to Foreign Agent A, Scanning to look for an alternative
** Event #5.  T=0.0326223449 ( 32ms).  Module #4 `GinSeng.FA_B_node'
FAB: Received message `Node Registration', sending Check Authentication Request to HA
** Event #6.  T=0.0376253449 ( 37ms).  Module #2 `GinSeng.HA_node'
HA: Received message `Authentication Request', sending Check credentials to AAA
** Event #7.  T=0.0426283449 ( 42ms).  Module #6 `GinSeng.AAA_node'
AAA: Received message `Check credentials FA', sending Credentials to HA
** Event #8.  T=0.0476313449 ( 47ms).  Module #2 `GinSeng.HA_node'
HA: Received message `Credentials', sending Authentication Confirmation to FAB
** Event #9.  T=0.0526318449 ( 52ms).  Module #4 `GinSeng.FA_B_node'
FAB: Received message `Authentication Confirmation', sending Check credentials MN to AAA
** Event #10.  T=0.0576348449 ( 57ms).  Module #6 `GinSeng.AAA_node'
AAA: Received message `Check credentials MN', sending Credentials to FAB
** Event #11.  T=0.0626378449 ( 62ms).  Module #4 `GinSeng.FA_B_node'
FAB: Received message `Credentials', sending Registration Confirmation to MN
** Event #12.  T=0.0682914311 ( 68ms).  Module #5 `GinSeng.MN_node'
MN: Received message `Registration Confirmation', END from MN
** Calling finish() methods of modules
```

Phase	Number of messages	Time (ms)
Scan & Join	Not considered for simulation	Tscan-join
Negotiation	5	28,2695
Authentication	8	40,0215
Offline	-	Tscan-join + 41,322
Total	13	Tscan-join + 68.291

Fig. 15 Tested scenario in Omnet++ when prediction is wrong (see Figure 12). MN-node is the Mobile Node, AAA-node is the AAA server, FA-A-node and FA-B-node are Proxy Agents of networks from the visited neighborhood, and HA-node is the Proxy Agent in the home network.

not open to define a customized version of the firmware. For that reason, Proxy Agent functionality and Border Router have been defined separately. The pictures of the deployed Border Router show how the Border Routers are connected to the same Ethernet network of a PC/laptop, which carry out the Proxy Agent tasks.

The Proxy Agents are being prototyped with a Java application which is always listening in a port and well-known IPv6 address. This periodically receives from the internal router a report, which contains the signal quality of the medium. The movement direction determination process in this scenario is deterministic, since physically the options of movement are limited by the corridors. Consequently, the results are that e.g. Proxy

Agent from network 1 always assigns network 2 when it detects a drop in the MN signal quality under the threshold. Our goal for future work is to reach the unification of the Border Router and the Proxy Agent in just one entity. For that reason, our future works are focused on changing to Sensinode solution, since it offers a platform based on ARM9 microprocessor, which is empowered with Linux OS and consequently is more flexible to define new protocols.

The internal routers are based on the demo sensor board from the Jennic development kit (see Figure 16). They carry out active scan of the medium in order to periodically send reports about the signal quality to the Proxy Agent. This active scan is based on the Jennic Production Test API [42], which allows to check the channel activity of the MN.

The MN is based on a specific board developed in our lab, in order to offer interfaces to connect clinical sensors such as the previously mentioned pulse oximeter for the oil refinery. The pulse oximeter connected to the MN is also presented in Figure 16.

The log with times of the MN is presented in Listing 1, such as can be seen, the handoff time is 5407 milliseconds (since restarted MAC layer, until joined to the visited network), which higher than the handoff time simulated in Omnet++, it is because the Border Router is not united to the Proxy Agent, and consequently the join process is conditioned by Jennet, the network layer from Jennic, which is between IEEE 802.15.4 and 6LoWPAN network layer. Therefore, some additional time is spent in order to join the network defined by the Jennet Coordinator. Such as mentioned, this issue is going to be solved in ongoing works, with the Sensinode solution, which offers a solution of 6LoWPAN based on Contiki OS, which is not including additional network layers above 6LoWPAN.

Listing 1 Log carried out through the Serial port of the MN. Time measures have been logged by a Java application which prints the milliseconds spent since the first message is received

```
Time -> Start timer, MSG: Joined to Network with IPv6 address: 0x2002 0x0 0x0 0x1
0x215 0x8d00 0xb 0x6156
Time -> 9593, MSG: Received Mobility Notificion from Proxy Agent, starting to reboot
Time -> 9593, MSG: stack mode set to E_STATE_JOINING and redefine tsStackInitData
with information from Mobility Notificion
Time -> 9593, MSG: Restart MAC layer and call to iJIP_InitStack
Time -> 15000, MSG: Joined to Network with IPv6 address: 0x2002 0x0 0x0 0x2 0x215
0x8d00 0xb 0x6156
Time -> 15109, MSG: Send Arrived Confirmation
Time -> 15312, MSG: Received Arrived ACK
```

7 Conclusions and Future Works

In this paper we have proposed and demonstrated the use of a paradigm for the support of mobility in critical wireless sensor network applications. The paradigm relies on the use of Proxy Agents, which perform all the mobility and authentication related operations on behalf of the Mobile Nodes, in order to provide soft handoffs and guarantee low latency during the whole handoff process.

The proposed mobility paradigm supports intra-mobility and inter-mobility. On the one hand, intra-mobility is directly supported by topology control algorithm from the MAC layer defined under this research (GinMAC), and on the other hand, inter-mobility is also supported by GinMAC to determine movement direction, which is used to carry out fast handoff and previous authentication and MN configuration.

The proposed paradigm satisfies the requirements and goals defined in the design issues. First, this supports global IPv6 addressing, such as presented in the evaluation

Fig. 16 Evaluation in a real deployment carried out in the Computer Science Faculty.

carried out with the Jennic nodes, where global IPv6 addressing has been used. Second, the proposal is based on the optimizations of the current IPv6 protocols, such as presented in comparative Table 1. Third, this supports intra-mobility directly with the topology control algorithm. Next, deployment is based on a set of 6LoWPAN networks interconnected through a backbone. After, the related mobility signalling messages exchanged with the Mobile Node are reduced to 2 messages for inter-mobility. Next, fast mobility is supported with movement direction determination and pre-set-up configuration, which allows to carry out part of the handoff process assisted by the Proxy Agents. After, security and authentication with an AAA server is supported. Then, the information is distributed among all the Proxy Agents from the neighborhood. And finally, the mobility control messages are limited to the size of one IEEE 802.15.4 frame. Therefore, the design issues defined have been followed and fulfilled.

The results reached are 95,4% of correct predictions for the movement direction determination algorithm for inter-mobility. Handoff latency is 37.426 milliseconds during handoff process when prediction is correct, with practically 0 milliseconds of offline time. It is 68.291 milliseconds when prediction is wrong with 41.322 milliseconds of offline time. The extension of this simulation to the evaluation in real nodes has presented an increment of the handoff time, bringing the total handoff time to 5,407 milliseconds, since the time for connection to the Border Router has depended on the coordinator join protocol, which is predefined by Jennet (a network layer from Jennic), which is located between IEEE 802.15.4 and 6LoWPAN.

For that reason, ongoing work is to consider evaluating this solution with Sensinode Border Routers, which offer the possibility to define Proxy Agents in the Border Router platform. In addition, the evaluation of the protocol is going to be carried out in the GALP oil refinery in Sines (Portugal). Finally, our research continues exploring the following guidelines: optimization of the proxies tasks, evaluation of the load delegated to the proxies, and overload in the backbone.

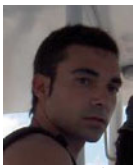
Acknowledgements The work presented in this paper was partially financed by the IST FP7 0384239 Ginseng - Performance Control in Wireless Sensor Networks. As well, this work has been carried out under the Spanish Program: "Programa de Ayuda a los Grupos de Excelencia" from the "Fundacin Séneca" 04552/GERM/06. Finally, the authors would like to thank the Spanish "Ministerio de Educación y Ciencia" for sponsoring the research activities under the grant AP2009-3981, under the FPU program.

References

1. Akyildiz, W., Su Y., Sankarasubramaniam, E., Cayirci: A survey on sensor networks, IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, (2002)
2. Dixit, S.: Wireless IP and Its Challenges for the Heterogeneous Environment, Wireless Personal Communications, Vol. 55, No. 2, Issue. 2, pp. 261-273, (2002)
3. Huan-Bang, L., Takashi, T., Masahiro, T., Yasuyuki, M., Ryuji, K.: Wireless Body Area Network Combined with Satellite Communication for Remote Medical and Healthcare Applications, Wireless Personal Communications, Vol. 51, No. 51, Issue. 4, pp. 697-709, (2010)
4. Jara, A.J., Zamora, M.A, Skarmeta, A.F.G.: HWSN6: Hospital Wireless Sensor Networks based on 6LoWPAN Technology: Mobility Fault Tolerance Management, IEEE International Conference on Computational Science and Engineering, Vancouver (Canada), (2009)
5. Sung, M., DeVaul, R.,; Jimenez, S., Gips, J., Pentland, A.: Shiver Motion and Core Body Temperature Classification for Wearable Soldier Health Monitoring Systems, Eighth IEEE International Symposium on Wearable Computers, pp. 192-193, (2004)
6. Jara, A.J., Blaya F.J., Zamora, M.A., Skarmeta, A.F.G.: 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)
7. Jara, A.J., Zamora, M.A., Skarmeta, A.F.G.: 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, pp.75-84, (2009)
8. Narten, T., Nordmark, E., Simpson, E., Soliman, H.: IPv6 Neighbor Discovery RFC4861, (2007)
9. Arkko, J., Devarapalli, V., Dupont, F.: Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents RFC 3776, (2004)
10. Johnson, D., Perkins, C., Arkko, J.: Mobility Support in IPv6 RFC 3775, 2004.
11. Ayuso, J., Marin, L., Jara, A.J., Skarmeta, A.F.G.: Optimization of Public Key Cryptography (RSA and ECC) for 16-bits Devices based on 6LoWPAN, 1st Workshop on the Security of the Internet of Things (SecIoT 2010). Tokyo, Japan (2010)
12. Jara, A.J., Silva, R.M., Silva, J., Zamora, M.A., Skarmeta, A.F.G.: Mobile IPv6 over Wireless Sensor Networks (6LoWPAN): Issues and feasibility, 7th IEEE European Wireless Sensor Networks (EWSN2010), Coimbra, Portugal, (2010)
13. GinSeng European Project, http://www.ict-ginseng.eu/, (2010)
14. Soliman, H., Castelluccia, C., ElMalki, K., Bellier, L.: Hierarchical Mobile IPv6 (HMIPv6) Mobility Management, RFC 5380, (2008)
15. Diab, A., Mitschele, A., Al-Nasouri, E., Boringer, R., Xu, J.: Mobile IP Fast Authentication Protocol, Technische Universitat Ilmenau, Fachgebiet Integrierte HW/SW-Systeme, (2005)
16. Koodli, R., : Fast Handovers for Mobile IPv6, RFC 4068, (2005)

17. Bernardos, C.J., Gramaglia, M., Contreras, L.M., Calderon, M., Soto, I.: 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), Vol 1., No.2-3, (2010)
18. Shelby, Z., Thurbert, P., Hui, J., Chakrabarti, S., Bormann, C., Nordmark, E.: 6LoWPAN Neighbor Discovery, draft-ietf-6lowpan-nd-07, Internet-Draft IETF, work in progress, (2010)
19. Jara, A.J., Zamora, M.A., Skarmeta, A.F.G.: Intra-mobility for Hospital Wireless Sensor Networks based on 6LoWPAN, The Sixth International Conference on Wireless and Mobile Communications (ICWMC2010), Valencia, Spain, (2010)
20. Shin, M-K., Camilo, T., Silva, J., Kaspar, D.: Mobility Support in 6LoWPAN, IETF Internet Draft draft-shin-6lowpan-mobility-01.txt, work in progress, (2009)
21. Chakrabarti, S., Park, S.D.: LowPan Mobility Requirements and Goals, draft-chakrabarti-mobopts-lowpan-req-01, Internet-Draft IETF, work in progress, (2010)
22. Kushalnagar, N., Montenegro, G., Shumacher, C.: IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN), RFC 4919, (2004)
23. Suriyachai, P., Brown, P., Roedig, P.: A MAC Protocol for Industrial Process Automation and Control. 7th IEEE European Workshop on Wireless Sensor Networks (EWSN2010), Coimbra, Portugal, (2010)
24. Granjal, J., Silva, R., Monteiro, E., Sa Silva, J., Boavida, F.: Why is IPSec a viable option for wireless sensor networks, Wireless and Sensor Networks Security, (2008)
25. Bag, G., Shams, S.M.S., Akbar, A.H., Raza, H.M.M.T., Ki-Hyung Kim, Seung-Wha Yoo: Network Assisted Mobility Support for 6LoWPAN, IEEE Consumer Communications and Networking Conference, pp. 1-5, (2009)
26. Ho Kim, J., Seon Hong, C., Shon, T.: A Lightweight NEMO Protocol to Support 6LoWPAN, ETRI Journal, vol.30, no.5, pp.685-695, (2008)
27. Yan, Z., Zhou, H., You, I.: N-NEMO: A Comprehensive Network Mobility Solution in Proxy Mobile IPv6 Network, Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol 1., No.2-3, (2010)
28. Silva, R., Zinonas, Z., Sa Silva, J., Vassiliou, V., Lopes, P., Brandao, J.: Mobility in WSN for Critical Applications, ICC, Kyoto, Ïn Press, (2011)
29. Singh, D., Kim, D.: MMSP: Design a Novel Micro Mobility Sensor Protocol for Ubiquitous Communication, The Fourth International Conference on Mobile Ubiquitous Computing, Systems, Services and Technologies (UBICOMM2010), Florence, Italy, (2010)
30. Bag, G., Mukhtar, H., Shams, S.M.S., Ki Hyung Kim, Seung-wha Yoo: Inter-PAN Mobility Support for 6LoWPAN, Convergence and Hybrid Information Technology, ICCIT '08, Volume 1, 11-13, pp. 787-792, (2008)
31. Camilo, T., Pinto, P., Rodrigues, A., Sa Silva, J, Boavida, F.: Mobility management in IP-based Wireless Sensor Networks, WoWMoM 2008, pp. 1-8, (2008)
32. Bag, G., Raza, M.T., Mukhtar, H., Akbar, A.H., Shams, S.M.S., Kim, K-H., Seung-wha Y., Donghwa K.,: Energy-aware and bandwidth-efficient mobility architecture for 6LoWPAN, Military Communications Conference 2008, pp.1-7, 32, (2008)
33. Stojmenovic, I.: Handbook of Wireless Networks and Mobile Computing, John Wiley & Sons, Inc, ISBN: 0-471-41902-8, (2002)
34. Chaczko, Z., Klempous, R., Nikodem, J., Nikodem, M.: Methods of Sensors Localization in Wireless Sensor Networks, 14th Annual IEEE international Conference and Workshops on the Engineering of Computer-Based Systems, (2007)
35. Chen, R.T.Y., Chiu, C.C., Tu, T.C.,: Mixing and Combining with AOA and TOA for Enhanced Accuracy of Mobile Location, IEE, Michael Faraday House, Stevenage, (2003)
36. Gustafsson, F.: Positioning Using Time-Difference of Arrival Measurements, Acoustics, Speech, and Signal Processing, Proceedings. (ICASSP '03), (2003)
37. ContikiOS. The Operating System for Embedded Smart Objects, (2010)
38. OMNeT++. The discrete event simulation environment. www.omnetpp.org, (2010)
39. Aschenbruck, N., Ernst, R., Gerhards-Padilla, E., Schwamborn, M.: BonnMotion - A mobility scenario generation and analysis tool, University of Bonn, (2010)
40. Jin-Shyan, L.: Performance Evaluation of IEEE 802.15.4 for Low-Rate Wireless Personal Area Networks, IEEE Transactions on Consumer Electronics, Vol. 52, No. 3 (2006)
41. Wang, X., Bischoff, O., Laur, R., Paul, S.: Localization in Wireless Ad-hoc Sensor Networks using Multilateration with RSSI for Logistic Applications. Proceedings of the Eurosensors XXIII conference. 2009, pp. 461-464, (2009)
42. Jennic, JN-AN-1014 Checking for channel activity using the Site Survey Tool and JN-SW-4022 Jennic Production Test API, (2010)

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



Ricardo Silva is currently a PhD Student of the doctoral program in Sciences and Information Technology at the University of Coimbra. He received his BSc in Informatics Engineering in 2006 from the Polytecnic Institute of Leiria and his MSc degree in Network Communication Engineering in 2008 from the University of Coimbra. Ricardo is a Researcher in the Laboratory of Communication and Telematics in the Centre of Informatics Engineering of University of Coimbra, Portugal. He is currently participating in the FP7 GINSENG Project. IPv6, Neighbor Discovery and Mobility in Wireless Sensor Networks are his main interests.

Jorge Sá Silva received his PhD in Informatics Engineering in 2001 from the University of Coimbra, where is a Professor at the Department of Informatics Engineering of the Faculty of Sciences and Technology, and a Senior Researcher in the Laboratory of Communication and Telematics of Centre of Informatics Engineering of University of Coimbra, Portugal. His main research interests are Mobility, IPv6, Network Protocols and Wireless Sensor Networks. His publications include 2 book chapters and over 50 papers in refereed national and international conferences and magazines. He participated in European initiatives and projects such as FP5 E-NET, FP6 NoE E-NEXT, FP6 IP EuQoS, FP6 IP WEIRD and FP7 Ginseng. He actively participated in the organization of several international conferences, (e.g. he was the Chair of IFIP Networking2006, Publicity Chair of EWSN2009, General Co-Chair of EWSN2010). He is a member of IEEE, and he is a licensed Professional Engineer.

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 (UMU), Murcia, Spain, in 1997 and 2003, respectively. In 1997, he was with the Department of Engineering and Systems, Technical University of Valencia (UPV), Valencia, Spain. 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 ITS field and is especially focused on navigation systems for road vehicles.

Antonio F. Gómez-Skarmeta received the M.S. degree in Computer Science from the University of Granada, Spain, and the B.S. (Hons.) and the Ph.D. degrees in Computer Science from the University of Murcia. Since 1993, he has been an Assistant Professor with the Department of Information and Communications Engineering at UMU. Research interests include mobile communications, and Future Internet Network Model. He has published over 100 international papers.