An Initial Approach to Support Mobility in Hospital Wireless Sensor Networks based on 6LoWPAN (HWSN6)

Antonio J. Jara, Miguel A. Zamora and Antonio F. G. Skarmeta
University of Murcia
Murcia, Spain
{*jara, mzamora, skarmeta*}*@um.es*

Abstract

Low-power personal area networks (LoWPANs) are still in its early stage of development, but the range of conceivable usage scenarios is tremendous. The numerous possible applications of Wireless Sensor Networks (WSNs) make obvious that mesh and multi-technology topologies will be prevalent in LoWPAN environments and mobility is one of the most important issues in the Future Networks. Mobility based communication can prolong the lifetime of devices, increase the connectivity between nodes and clusters, and support fault tolerance. Using distributed LoWPANs is possible to sculpt the devices density to cluster around areas of interest, cover large areas, and work more efficiently. The required mobility is heavily dependent on the individual service scenario and the LoWPAN architecture. For that reason in this paper is presented a mobility protocol oriented to clinical environments. This protocol is based on our monitoring architecture oriented for continuous vital signs monitoring. Thereby, it has been defined and optimized to exploit the other elements of the architecture with high capacity and resources (6LoWPAN Border Router and gateways) to reduce latency and node's overload with respect to other IPv6 mobility solutions such as Mobile IPv6 (MIPv6).

1 Introduction

Wireless sensor networks (WSNs) have recently been proposed for a large range of applications in several areas, such as home and industrial automation, environmental monitoring, and healthcare [28]. Particularly solutions based on IEEE 802.15.4 [2] are the most widely used. IEEE 802.15.4 specifies a wireless link for low-power personal area networks (LoWPANs). These kinds of networks are characterized by their more limited capabilities than other WPANs and WLANs. Specifically, IEEE 802.15.4 has smaller frame size, lower data rate, lower bandwidth and lower transmit power to reach a low power consumption and low cost [13].

A set of new manifold options is arriving to the WSN based on IEEE 802.15.4 networks (LoWPAN) with the connectivity to the Internet, with the solution 6LoWPAN [21], which provides IP network layer to IEEE 802.15.4, defined by the Internet Engineering Task Force (IETF) [9].

6LoWPAN offers to the WSN all the advantages from IP such as scalability, flexibility, tested, extended, ubiquitous, open, end-to-end connectivity, etc. In addition, we could consider that WSN nodes are also empowered with IP protocols, e.g. protocol for mobility such as MIPv6, management such as SNMP, and security such as IPSec. However, these protocols are not feasible for the 6LoWPAN devices. These devices features satisfy the minimum requirements to be associated with host based mobility, management, and security protocols, since 6LoWPAN nodes are, firstly, energy and resource constrained, secondly, host based protocols require most of the signalling on node's end [24], thirdly, the design features of 6LoWPAN network were not considered in the design issues of the host based protocols, e.g. a 6LoWPAN node may run out of energy causing a fault in the network, fourthly, they have restriction in size packets, and finally, this presents aggressive techniques to conserve energy by using of sleep schedules with long sleep periods, e.g. 6LoWPAN nodes just wake up to receive IPv6 signalling messages, this feature introduces delays in the reception of messages because they are not attended until

---

Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, volume: 1, number: 2/3, pp. 107-122

that the node wakes up. Therefore, these delays, power restrictions, packet size restrictions etc. are not considered in the current IPv6 protocols, and they need to be considered to define a suitable protocol for networks based on 6LoWPAN. Some additional studies about the low performance of the IPv6 protocols over 6LoWPAN can be found for specific protocols such as MIPv6 and HMIPv6 for mobility solutions, and SNMP for management solutions on 6LoWPAN networks in [6, 3, 4, 5].

For this reason we must redefine these kinds of protocols to satisfy the new design features [11]. For example we can find the adaptation of SNMP for 6LoWPAN networks in [25] and some mobility approaches in [27, 6, 3, 4, 5]. Furthermore, we must consider that WSNs present a large scope of applicability and, with the conjunction of the variety of case scenarios it is difficult to produce a standard mobility scenario [6].

Particularly, this paper is going to define a solution for mobility over 6LoWPAN to satisfy the new design features which has been defined from the analysis of MIPv6 [15] and the before work of mobility for 6LoWPAN [17, 6, 3, 4, 5, 11, 27, 12, 10]. Mobility has been chosen for our research, because it is one of the most important issues in next generation networks, mobility based communication increase the fault tolerance capacity of the network and prolong the lifetime of devices and increase the connectivity between nodes and clusters. Using distributed LoWPANs is possible to sculpt the devices density to cluster around areas of interest, cover large areas, and work more efficiently by filtering local data at the node level before it is transmitted. Furthermore, multiple controlled mobile elements can be used to provide load balancing and gathering data.

The mobility protocol presented is optimized for Hospital Wireless Sensor Networks since healthcare patients' monitoring is highly desired; heart rate, SPo2, ECG, breath rate, blood pressure and weight are common factors, which should be constantly monitored. Therefore, using portable monitoring systems based on WSNs make possible, besides a most efficient medical service, to provide a new freedom of the patients. For example, mobility allows that the patient is able to go for a walk around the corridor while he is monitored; mobility also allows that the patient can be changed of room for tests without lost the continuous monitoring, e.g. change the patient to the X-ray room. The goal of this continuous monitoring in Hospitals is to reach an extended quantity of data from the patient to, on one hand, increased the information stored in the Hospital Information System (HIS), and on the other hand, enhanced the Knowledge Based System (KBS) to detect symptoms and predict illness such as myocardial infarction [16, 14].

In this paper, we present a protocol to carry out intra-WSN mobility based on the architecture, which has been defined for hospitals. This protocol shows how to exploit the other elements of the architecture (sink nodes and gateways) with high capacity, high resources, and not so constrained with power consumption to carry out the moving signalling. Thereby, mobile nodes decrease their overload and number of messages necessaries to support mobility.

The rest of the paper is organized as follows. Section 2 presents the related works about mobility protocols for IPv6 and 6LoWPAN. Section 3 presents the design issues that have been considered to develop this mobility solution. Section 4 describes the architecture that we can find at the hospital, describing the characteristics of each element. Section 5 presents the mobility protocol. Section 6 evaluates the mobility protocol. Finally, Section 7 concludes this paper.

2 Related works

Mobility in Wireless Sensor Networks is a topic highly mentioned in the WSN literature, where different solutions have been defined in function whether the domain is changed or not, inter-mobility and intra-mobility respectively, other type of mobility can be considered in function what is moving i.e. node or network, and whether it is assisted by a proxy. But, these proposals are usually defined from a point of view where IP was not considered. For this reason, these approaches are not suitable for WSNs based on IP such as 6LoWPAN. In this related work are analysed the different solutions for mobility supporting IPv6, and the first approaches for 6LoWPAN, to define the basis to discover the opportunities, limitations and possibilities to adapt the IPv6 mobility protocols to 6LoWPAN, all these design issues are summarized in the next section.

MIPV6 protocol is the most studied and well-know 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 process, with very weighty messages, and high processing requirements [18]. 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) [29] is an optimization of the MIPv6 regarding the subject of micro-mobility, in a well known architecture that is composed by a gateway, Home Agent (HA), Foreign Agent (FA) 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. Their IPv6 Care of Address (CoA) remains the same. Short addresses are managed by the topology algorithm control.

Mobile IP Fast Authentication Protocol (MIFA) [7] introduces a very simple concept about how to support macro-mobility with authentication. It defines a group called L3-FHR (Layer 3 Frequent Handoff Region) composed by the neighbours of a network, where a mobile device is able to move. This protocol also increases the functionality of the FA entity, making them responsible for the authentication of the mobile nodes.

Fast Handover for Mobile IPv6 (FMIPv6) [19] main characteristic concerns the MN being able, through the use of link layer specific mechanisms, to find available access points to request subnet information. Thereby, MN is able to configure its CoA while is still located in its current network. This reduces considerably the handoff latency.

Some initial approaches have been defined to support mobility in 6LoWPAN. On one hand, 6LoWPAN Neighbour Discovery [26] supports micro-mobility, since it Extended 6LoWPANs, i.e. a group of 6LoWPAN networks interconnected trough a backbone. Functionality of mobility is delegated to Border Routers, since they check with the other ones whether a Mobile Node is accessible from other of the Border Routers linked to the same Backbone. On other hand, mobility is supported by a solution based on lightweight messages version of Mobile IPv6 [27], which is similar to the idea of header compression used for IPv6 messages over IEEE 802.15.4 [20]. That approach is not suitable since security extensions cannot be supported, and MN receives a high overload [10]. Other approaches have been considered based on Network Mobility (NEMO) [17, 5, 12] to reduce overload in MN, and Proxy Mobile IPv6 (PMIPv6), 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. Finally, other heterogeneous approaches are found in [3, 4, 6].

3 Design Issues

Given the unique low-performance properties of 6LoWPANs, as seen in the introduction, new challenges arise of enabling mobility and support to devices with highly reduced memory and power. It is therefore crucial to reduce the additional mobility related signalling overhead, optimize the payload size to reduce fragmentation in the 6LoWPAN network and optimize use of MAC layer characteristics to increase devices life-time.

Hence in 6LoWPAN mobility protocol we must consider a set of design issues in order to face these restrictions. These design issues are being defined from the analysis of MIPv6 protocol over 6LoWPAN

[15]. They are organized into two groups. On one hand, it is defined the design issues which are interesting to reach, which are referred as ”goals” for the mobility protocol, on other hand, it is defined the design issues which are mandatory to reach, which are referred as ”requirements” for the mobility protocol. The next subsections present it both.

3.1 Mobility protocol goals

In this section are enumerated the goals proposed for mobile IPv6 protocol over 6LoWPAN with the proposal of optimizing power consumption and optimize use of MAC layer characteristics to increase devices life-time.

- Global addressing must be supported; 6LoWPAN nodes must be addressable by any corresponding node, independent of the current whereabouts. It is necessary to reach a global connectivity with the devices using the current Internet infrastructure.
- Minimize signalling by removing the use of multicast/broadcast flooding and reducing the frequency of link scope multicast/broadcast messages inside the LoWPANs.
- Mobile protocol must be supported in star topology as well as mesh topology where is needed multi-hop routing to reach a desired destination. Mesh networks are typically formed by nodes with a high degree of mobility.
- Reduction of related mobility signalling messages to reduce the overhead.
- End devices such as Reduced Function Devices (RFDs) should not be involved in mobility signalling due to the low performance characteristics of 6LoWPAN devices.
- Fast mobility detection is required to avoid delays, high jitter and/or interruptions of the communication during handover process. It needs to be considered that a LoWPAN node might even change its location while being in state of hibernation (sleep mode).
- Mobility solutions should be compatible and based on current IPv6 protocols such as ICMPv6 and MIPv6.
- Interconnect LoWPANs with backbone links seamlessly, thereby not additional errors and delays are added for intra-domain handover.
- Mobility and options header for data messages must be optimized as much as possible to reduce the overhead for data messages in roaming, thereby can be optimized payload and consequently reduced the fragmentation.
- A LoWPAN node which participates in forwarding packets from its neighbour, i.e., router node, may no longer be available to forward packet if it moves away from its neighbour’s coverage. Thus the sender needs to find an alternate router to ensure connectivity and fault tolerance.
- A 6LoWPAN node should be reachable by another 6LoWPAN node or a global network node even if it moves from a LoWPAN to other one, i.e., support mobility inter-domain.
- A 6LoWPAN node may be able to keep continuous connectivity during handover process.
- The mobility protocol should be based on distributed storage of information rather than conventional central repository due to the nature of instability in 6LoWPANs and to support fault tolerance.

- Node authentication and authorization must be supported to offer security capability, ensure protection of the resources, integrity and confidentiality of the information.

3.2 Mobility protocol requirements

In this section are enumerated the requirements proposed for mobile IPv6 protocol over 6LoWPAN to reach a suitable mobility protocol for the features and constrains of 6LoWPAN.

- LoWPAN node has assigned a link local IPv6 address as well as IEEE 802.15.4 MAC address. In addition is recommendable to assign for each node a global IPv6 address to support global communication but if the 6LoWPAN network is isolated then it is not recommendable the use of global addressing, because the overhead of messages sent using global addressing is higher, for the reason that 6LoWPAN header compression is worse for global addressing than for link local one.
- The signalling messages must fit within a single IEEE 802.15.4 frame, i.e., fragmentation must be avoided for signalling messages.
- 6LoWPAN Border Router must notify to the Home Agent about the presence of a mobile node from its domain, i.e., binding update must be performed by 6LoWPAN Border Router instead of Mobile Node in order to reduce overload for mobile node.
- The original IPv6 gateway (6LoWPAN Border Router), i.e., home agent is responsible for buffering and forwarding packets to the mobile node.
- If the mobile node is a router in its home network it is no longer router for its home network during the roaming time.
- The movement of a 6LoWPAN node with an IPv6 address must be transparent to a correspondent IPv6 node external to the 6LoWPAN network if is not being used route optimization technique.
- Authentication of the mobile node is required by the 6LoWPAN Border Router of the visited network, i.e., Foreign Agent, before than 6LoWPAN Border Router updates location information.
- Security support must be provided, e.g. Hospital Wireless Sensor Networks require assuring the protection of the patient's information. Security support can be reached by AES security mechanism, which is provided in link layer, but it is relatively loose, therefore it must be limited to the 6LoWPAN network, and for the rest of the elements from the architecture must implement strong mechanisms for privacy, security, integrity and authentication such as IPSec.

4 System Architecture

The system architecture is made up of a local gateway (Monere System), deployed at each room of the hospital, such as operating rooms and patient rooms. This local gateway (6LoWPAN Border Router) is connected to the Internet, other rooms, and the Hospital Information System (HIS) trough the hospital backbone.

The architecture deployed at the Hospital is presented in the Fig. 1. Where each room system is a Monere System, and it is connected to the HIS, users (physicians, surgeons and nurses) trough and Internet.

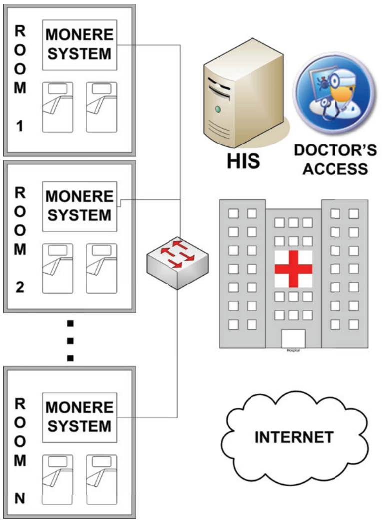


Figure 1: Hospital Architecture Diagram

4.1 Hospital Information System

Hospital Information System (HIS) is a system based on Open Services Gateway Initiative (OSGi) technology for the management of all the other systems from the hospital.

Hospital Information System is the gateway with networks going out of the hospital and the place to get information and access to the services of the other systems from the hospital. Some of these services are:

1. **Directory service:** we can obtain the IPv6 address of sensor nodes and Monere system for each patient.
2. **Localization service:** we can obtain the localization of each patient in the hospital from the mobility information.
3. **Health status:** All the information related to the patient from the medical sensors.
4. **Electronic Health Record (EHR):** It can provide information from the EHR of the patient.
5. **Management of alarms from the Monere Systems:** It provides communication to the Doctors in cases of some alarm from the Monere system about the health status (detection of symptoms or unusual values from some sensor).

4.2 Monere system (sink node - local gateway

Monere system is the 6LoWPAN Border Router in the hospital rooms and it is also the mobile data collector (MDC) from the Patient sensors. This gateway is responsible to establish and manage the connection between other networks. It is equipped with several interfaces that allow it to contact other networks using (Ethernet, cellular, 6LoWPAN or Bluetooth). It is presented in the Fig. 2.

It is equipped with technologies to control home automation (EIB, X10 and ZigBee) and standard (CANBus, Ethernet and Serial) [23]. Hence, we can connect it to the current sensors from the hospital, which do not work over 6LoWPAN. Finally, it supports the security requirements defined in Section3.

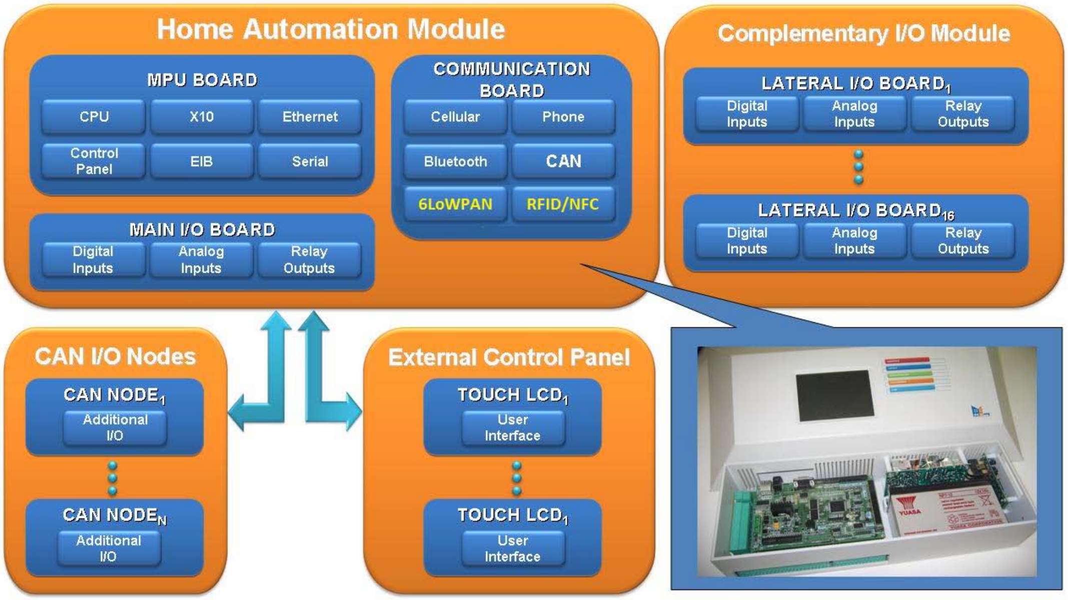


Figure 2: Logical diagram of the Monere System

1. **Privacy and security.** It can cipher the communications with AES-CBC cryptography (256bits key).
2. **Integrity.** It can do hashing using SHA256 and CRC using CRC16-ITT.
3. **Authentication.** It is carried out using hashing ciphered with the shared key.

4.3 Patient node (mobile node)

A set of sensors are been 6LoWPAN powered for continuously transmitting healthcare data such as heart rate, SpO2, peripheral and core body temperature, glucose etc. Fig. 3 presents the glucometer and SPo2 sensors connected trough 6LoWPAN.

Figure 3: Mobile sensors connected trough 6LoWPAN

5 Mobility Protocol

WSNs present a large scope of applicability and, with the conjunction of the variety of case scenarios make it difficult to produce a standard mobility scenario. For this reason we are defining a specific mobility protocol for Hospital Wireless Sensor Networks, where are fulfil the requirements from this scenario i.e., continuous monitoring, low latency, no loose of packets and low signalling.

Fig. 4 presents a scenario, where a patient node moves from its base network to other networks (visited networks) until it returns to the base network. We can consider this kind of scenario at the hospital when patients wander through the hospital or they are moved to other room to do some medical tests (e.g. radiography).

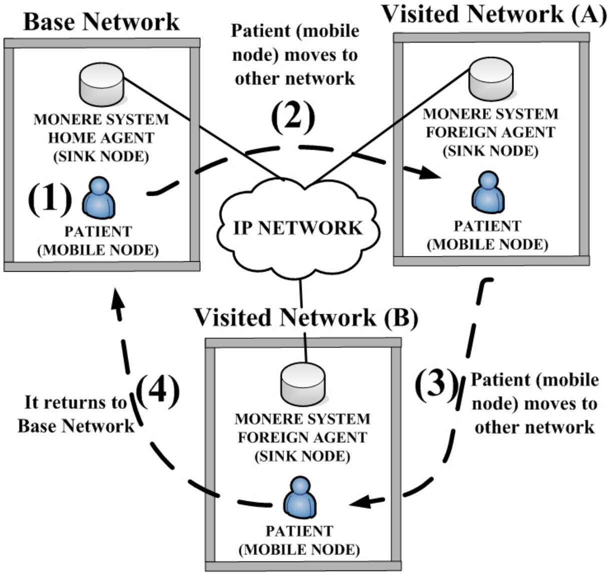


Figure 4: Mobility scenario

Phase 1 from Fig. 4 shows an initial state of the patient node in his room, where it is connected to its assigned Monere system, which is monitoring vital constants of the patient. Afterwards, in phase 2 and 3, it moves to other networks of the hospital. Finally in phase 4, it returns to the base network.

Fig. 5 presents a diagram with the messages exchanged in order to carry out the changes of networks shown in Fig. 4.

1. **Exchange of messages in the Base Network:** The messages between 1 and 7 as seen Fig. 5, show the usual data frames, requests, responses and acknowledgements of the transmission of information between sensor node and the Monere system. Data frames contain monitoring information such as EKG values or SPo2 level. Request messages are queries to the patients either to change a value of configuration or to obtain some value. Response messages are the replies to the request messages, where we get the result of the operation. Specifically, for this simulation a data packet from a pulsioximeter (SPo2 level) is sent each 5 seconds, and a request from the doctor is attended by the patient node, with its respective response message (messages 4 and 5).

2. **Movement detection time:** Patient node observes that its link quality has degraded beyond a certain threshold; it assumes that the patient node is moving [4]. Moreover in the patient node the current router is no longer reachable, and a new and different access router is available [8].

3. **Entering to the visited network (Router discovery):** 6LoWPAN coordinator (Monere system) periodically transmits beacon packets (message 8 in Fig. 5), which contain PAN ID and information to access the network. When a patient node enters the network it sends an Association Request (message 9) with the information of its home agent (Monere system in the base network). Remark

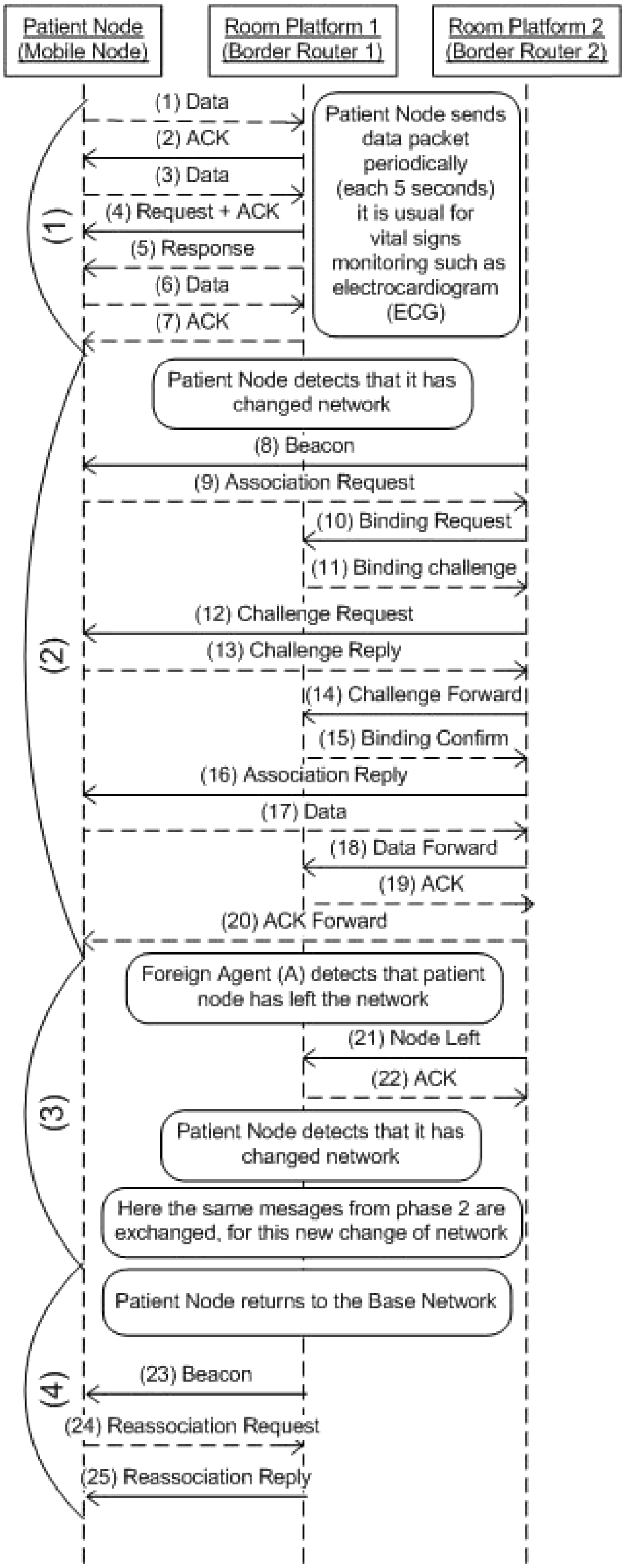


Figure 5: Messages exchanged for mobility

that in this step, as we are using fixed IPv6 addressing, 6LoWPAN coordinator must only assign a short address (16 bits) [5], but it does not need set up the IPv6 address. Monere system detects a new node in its network, hence it initiates the process to authenticate the node.

4. **Authentication of mobile node in visited network:** To confirm that the new mobile node is from the hospital, we need to authenticate it. In first place, foreign agent (Monere system from the visited network) sends a message to the home agent (Monere system from the base network). This message informs relative to the presence of home agent network node in its network (message 10). Home agent replies with a challenge for the mobile network (message 11), hence it can confirm that it is a real node from its network, because each 6LoWPAN network has a different AES key in 802.15.4 link layer. Foreign agent makes a forward of this challenge to the patient node (message 12). Patient node ciphers the challenge and sends it to the foreign agent (message 13). Foreign agent makes a forward of this challenge ciphered to the home agent (message 14). Home agent checks the challenge, if it is right, it sends a confirm message to the foreign agent (message 15). In other case it sends a deny message to avoid that the unauthenticated patient node receives or sends confidential information. Finally home agent sends a location update to the HIS of the patient node. HIS is only going to use this information to locate patients within the hospital. HIS is going to continue sending messages to this node to the home agent instead of the foreign agent, because home agent needs to know all the information related to the patient in order to detect anomalies and symptoms.

5. **Exchange of messages in the Visited Network:** The messages between 17 and 20 show how a data frame and its acknowledgements are carried out. It shows how all the messages arrive to the foreign agent from the home agent and it forwards it to the mobile node.

6. **Changing from a visited network to another one:** When a patient leaves a visited network, foreign agent sends a message to the home agent (messages 21-22).

7. **Returning to the Base Network:** When the patient node returns to the base network it sends a re-association request to inform the home agent of its new location (messages 23-25).

6 Results and evaluation

The aim of this evaluation is to determinate nodes overload and handoff latency. This evaluation has been carried out with Omnet++ [1], where has been defined the messages exchanged in our protocol (see Fig. 5), nodes involved, and medium features for the intra-mobility scenario presented in the Fig. 4. The messages length has 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 [22].

As we have already seen, the objective of this protocol is to reduce to the maximum the interaction of the patient node in the mobility protocol, through the assistance of the other elements of the architecture. This type scenario can be close to the concept of mobility assisted by the network but without the restrictions placed in the 6LoWPAN network by mesh topologies multi-hop [27].

In first place, we achieve this reduction using fixed addresses, therefore this avoid the stages of ”care of address configuration”, ”duplicate address detection” and ”CoA Registration with HA” with respect to Mobile IPv6 [8]. Thereby, we remove time for addressing. We can see that all this communication is with mobile node, hence by removing these messages we reduce overload in the 6LoWPAN network.

Secondly, all the stages related to the binding update are carried out by the Monere system in the ”binding” stage, having only the mobile node presenting an interchange of messages in order to carry out the authentication of the patient node challenge.

Thirdly, as the algorithm is defined, route optimization is not carried out. Although at first this appears as an inconvenience for general solutions, in our case it does not cause any problem, since in our system design was defined that all the communications must go through the Monere system (home agent) in order to carry out the constant monitoring of the patient and additionally it allows us to simplify even more the mobility protocol, by eliminating the ”routeability CN” stage.

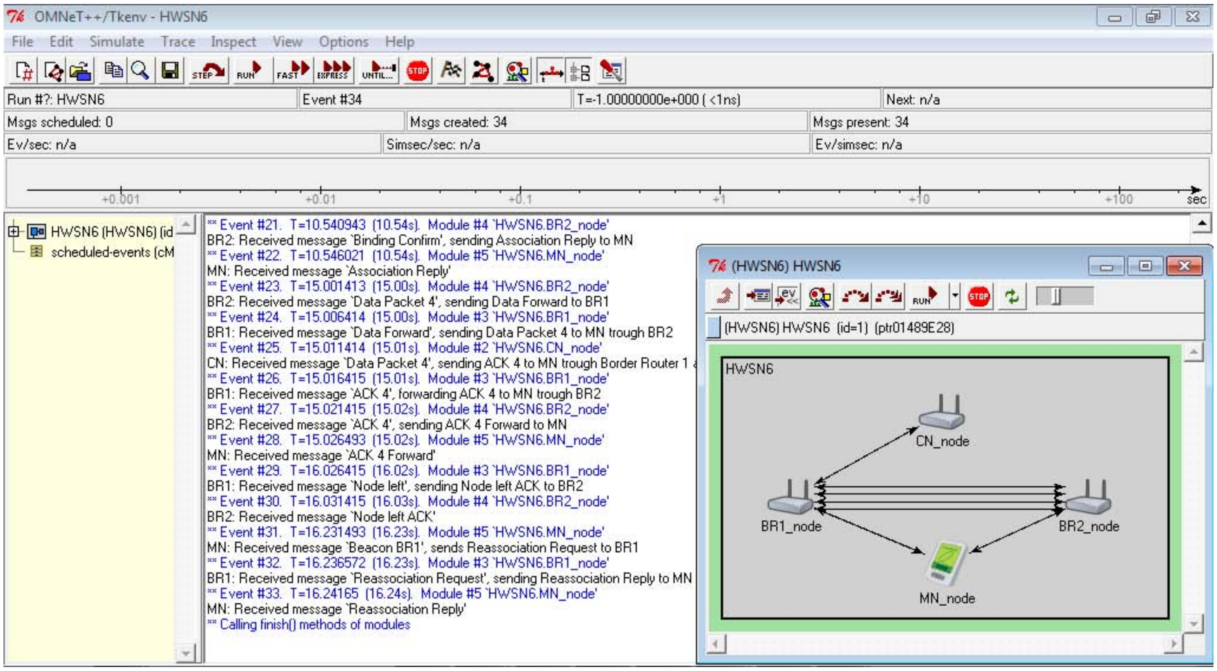
Therefore the handoff time from MIPv6 (see equation 1 and Fig. 9) is reduced with respect to the handoff time from our proposal, which is presented in the equation2.

$$\begin{aligned} T_{handoff-MIPv6} &= T_{movement-detection} + T_{addressing} + T_{routability-CN} + T_{binding-update} + T_{authentication} \\ &\qquad where, T_{addressing} = T_{CoA-configuration} + T_{DAD} + T_{COA-Register} \end{aligned} \tag{1}$$

$$T_{handoff-new} = T_{movement-detection} + T_{binding} + T_{challenge} \tag{2}$$

The messages exchanged (see Fig. 5) in the scenario presented in the Fig. 4 has been simulated in the platform Omnet++. Fig. 6 presents the Omnet++ environment with the evaluation which has been carried out. Fig. 7 presents the Omnet++ scenario, which is equivalent to the scenario from Fig. 5. Finally, the Fig. 8 presents the results of the simulation, where is described as the messages has been exchanged and the time when is sent and received each one.

The exchange of messages simulated (see Fig. 8), presents that the Data messages sent periodically each 5 seconds from a pulsioximeter simulated (SPo2 values) have not received any delay because handoff process.



Run #?: HWSN6
Event #34
T=1.00000000e+000 (<1ns)
Next: n/a
Msgs scheduled: 0
Msgs created: 34
Msgs present: 34
Ev/sec: n/a
Simsec/sec: n/a
Ev/simsec: n/a

```
** Event #21.  T=10.540943  (10.54s).  Module #4 `HWSN6.BR2_node'
BR2: Received message `Binding Confirm', sending Association Reply to MN
** Event #22.  T=10.546021  (10.54s).  Module #5 `HWSN6.MN_node'
MN: Received message `Association Reply'
** Event #23.  T=15.001413  (15.00s).  Module #4 `HWSN6.BR2_node'
BR2: Received message `Data Packet 4', sending Data Forward to BR1
** Event #24.  T=15.006414  (15.00s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Data Forward', sending Data Packet 4 to MN trough BR2
** Event #25.  T=15.011414  (15.01s).  Module #2 `HWSN6.CN_node'
CN: Received message `Data Packet 4', sending ACK 4 to MN trough Border Router 1 
** Event #26.  T=15.016415  (15.01s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `ACK 4', forwarding ACK 4 to MN trough BR2
** Event #27.  T=15.021415  (15.02s).  Module #4 `HWSN6.BR2_node'
BR2: Received message `ACK 4', sending ACK 4 Forward to MN
** Event #28.  T=15.026493  (15.02s).  Module #5 `HWSN6.MN_node'
MN: Received message `ACK 4 Forward'
** Event #29.  T=16.026415  (16.02s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Node left', sending Node left ACK to BR2
** Event #30.  T=16.031415  (16.03s).  Module #4 `HWSN6.BR2_node'
BR2: Received message `Node left ACK'
** Event #31.  T=16.231493  (16.23s).  Module #5 `HWSN6.MN_node'
MN: Received message `Beacon BR1', sends Reassociation Request to BR1
** Event #32.  T=16.236572  (16.23s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Reassociation Request', sending Reassociation Reply to MN
** Event #33.  T=16.24165  (16.24s).  Module #5 `HWSN6.MN_node'
MN: Received message `Reassociation Reply'
** Calling finish() methods of modules
```

Figure 6: Omnet++ environment

Table 1 presents a summary of the latency and time added by each one of the steps from the handoff process.

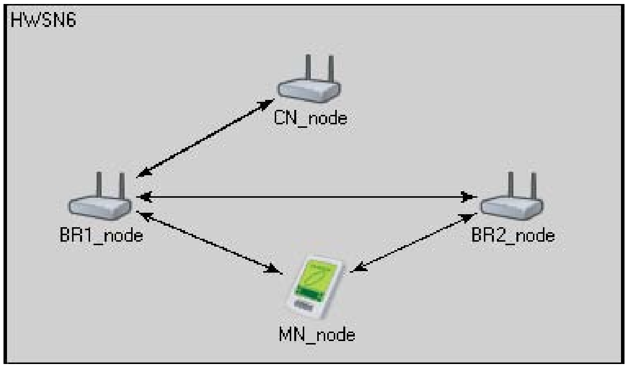


Figure 7: Scenario simulated in Omnet++

Table 1: Handoff times summary (details in Fig. 8)

Phase	Stage	Number of messages	Time (ms)
1	Data	8 (Considering communications with Correspondent Node)	41,5709
	Data Control	6 (Considering communications with Correspondent Node)	30,2619
2	Network Control	1 (Beacon, it is sent periodically each 0.5 seconds)	5,0507
	Negotiation	4 (Association Request and Reply, Binding Request and Confirm)	20,158
	Authentication	4 (Binding Challenge, Challenge Request, Reply and Forward)	20,785
	Data	3 (Data goes trough Home Agent, since it is necessary for KBS)	15,3931
	Data Control	3	15,079
3	Mobility Control	2 (Node left and ACK, it is sent 1 second later node left)	10,000
	The rest of messages from this phase are equivalent to phase 2		
4	Network Control	1 (Beacon)	5,0507
	Negotiation	2 (Reassociation Request and Reply)	10,157

Finally, remark that the proposed mobility protocol satisfies the requirements and goals defined in the section 3. Specifically, this supports security and authenticate MN with a challenge based on AES 128 bits when the MN changes its Border Router (Monere System), supports global IPv6 addressing, supports intra-mobility among the Monere systems deployed at the hospital, reduces overload in Mobile Nodes with respect to Mobile IPv6 (see Fig. 9, mobility protocol is assisted by Border Routers/Proxies (Monere Systems), distributed storage of the information among all the Monere Systems and mobility control messages with MN has been defined to avoid fragmentation, i.e. they are limited to one IEEE 802.15.4 frame.

7 Conclusion

Continuous vital sign monitoring in Hospitals is defining a new evolution in the Hospital Information Systems, the information from continuous monitoring allows the deployment of Knowledge Based Systems for detection of symptoms and prediction of illness. This paper has presented an architecture to support continuous monitoring; the most important challenge for this architecture, to ensure the continuous monitoring is to support mobility. Supporting mobility makes possible: provide a new freedom of the patients, allows to the patients go for a walk around the corridor, and change room for testing without

```
MN: MN sends a data package periodically each 5 seconds
** Event #0.  T=0.0053921517 (  5ms).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Data Packet 1', forwarding Data Packet 1 to CN
** Event #1.  T=0.0103927517 ( 10ms).  Module #2 `HWSN6.CN_node'
CN: Received message `Data Packet 1', sending ACK 1 to MN trough Border Router 1
** Event #2.  T=0.0153928717 ( 15ms).  Module #3 `HWSN6.BR1_node'
BR1: Received message `ACK 1', forwarding ACK 1 to MN
** Event #3.  T=0.0204713021 ( 20ms).  Module #5 `HWSN6.MN_node'
MN: Received message `ACK 1'
** Event #4.  T=5.0053922  ( 5.00s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Data Packet 2', forwarding Data Packet 2 to CN
** Event #5.  T=5.0103928  ( 5.01s).  Module #2 `HWSN6.CN_node'
CN: Received message `Data Packet 2', sending Request and ACK 2 to MN trough Border Router 1
** Event #6.  T=5.0153929  ( 5.01s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Request and ACK 2', forwarding Request and ACK 2 to MN
** Event #7.  T=5.0204975  ( 5.02s).  Module #5 `HWSN6.MN_node'
MN: Received message `Request and ACK 2', sends Response to CN
** Event #8.  T=5.0258896  ( 5.02s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Response', forwarding Response to CN
** Event #9.  T=5.0308902  ( 5.03s).  Module #2 `HWSN6.CN_node'
CN: Received message `Response'
** Event #10.  T=10.00589  (10.00s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Data Packet 3', forwarding Data Packet 3 to CN
** Event #11.  T=10.01089  (10.01s).  Module #2 `HWSN6.CN_node'
CN: Received message `Data Packet 3', sending ACK 3 to MN trough Border Router 1
** Event #12.  T=10.01589  (10.01s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `ACK 3', forwarding ACK 3 to MN
** Event #13.  T=10.020969  (10.02s).  Module #5 `HWSN6.MN_node'
MN: Received message `ACK 3'
** Event #14.  T=10.505078  (10.50s).  Module #5 `HWSN6.MN_node'
MN: Received message `Beacon', sends Association Request to new Border Router
** Event #15.  T=10.510157  (10.51s).  Module #4 `HWSN6.BR2_node'
BR2: Received message `Association Request', sending Binding Request to BR1 (usual patient room)
** Event #16.  T=10.515157  (10.51s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Binding Request', sending Binding Challenge to MN trough BR2
** Event #17.  T=10.520158  (10.52s).  Module #4 `HWSN6.BR2_node'
BR2: Received message `Binding Challenge', sending Challenge Request to MN
** Event #18.  T=10.52555  (10.52s).  Module #5 `HWSN6.MN_node'
MN: Received message `Challenge Request', sends Challenge Reply to BR1 trough BR2
** Event #19.  T=10.530942  (10.53s).  Module #4 `HWSN6.BR2_node'
BR2: Received message `Challenge Reply', sending Challenge Forward to BR1
** Event #20.  T=10.535942  (10.53s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Challenge Forward', sending Binding Confirm to BR2
** Event #21.  T=10.540943  (10.54s).  Module #4 `HWSN6.BR2_node'
BR2: Received message `Binding Confirm', sending Association Reply to MN
** Event #22.  T=10.546021  (10.54s).  Module #5 `HWSN6.MN_node'
MN: Received message `Association Reply'
** Event #23.  T=15.001413  (15.00s).  Module #4 `HWSN6.BR2_node'
BR2: Received message `Data Packet 4', sending Data Forward to BR1
** Event #24.  T=15.006414  (15.00s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Data Forward', sending Data Packet 4 to MN trough BR2
** Event #25.  T=15.011414  (15.01s).  Module #2 `HWSN6.CN_node'
CN: Received message `Data Packet 4', sending ACK 4 to MN trough Border Router 1 and 2
** Event #26.  T=15.016415  (15.01s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `ACK 4', forwarding ACK 4 to MN trough BR2
** Event #27.  T=15.021415  (15.02s).  Module #4 `HWSN6.BR2_node'
BR2: Received message `ACK 4', sending ACK 4 Forward to MN
** Event #28.  T=15.026493  (15.02s).  Module #5 `HWSN6.MN_node'
MN: Received message `ACK 4 Forward'
** Event #29.  T=16.026415  (16.02s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Node left', sending Node left ACK to BR2
** Event #30.  T=16.031415  (16.03s).  Module #4 `HWSN6.BR2_node'
BR2: Received message `Node left ACK'
** Event #31.  T=16.231493  (16.23s).  Module #5 `HWSN6.MN_node'
MN: Received message `Beacon BR1', sends Reassociation Request to BR1
** Event #32.  T=16.236572  (16.23s).  Module #3 `HWSN6.BR1_node'
BR1: Received message `Reassociation Request', sending Reassociation Reply to MN
** Event #33.  T=16.24165  (16.24s).  Module #5 `HWSN6.MN_node'
MN: Received message `Reassociation Reply'
** Calling finish() methods of modules
```

Figure 8: Messages exchanged for mobility in Omnet++

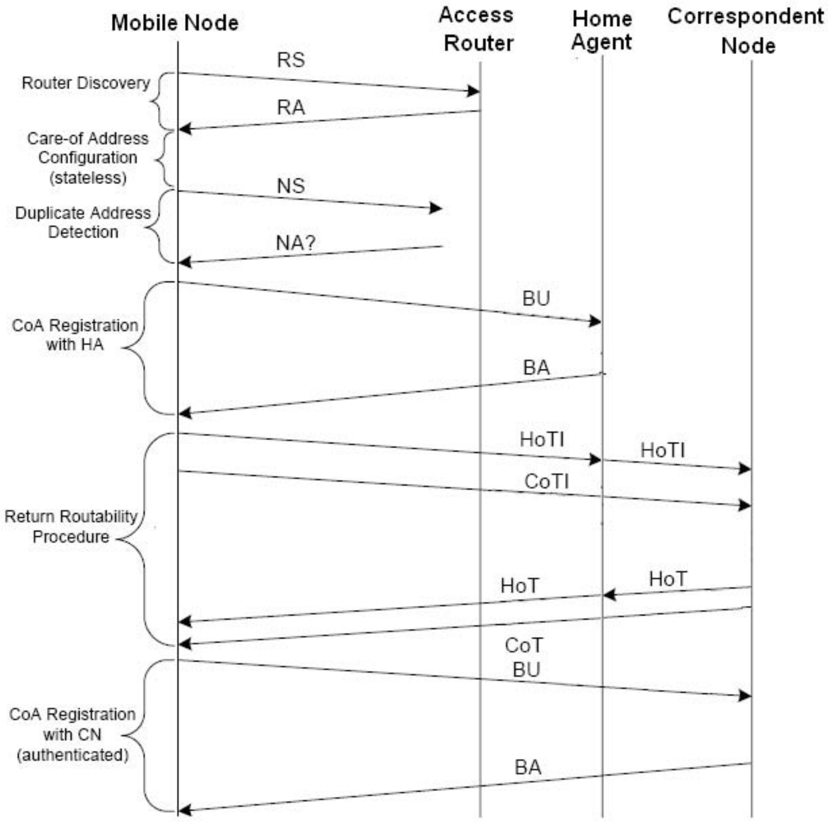


Figure 9: Messages exchanged for MIPv6 handoff

lost the continuous monitoring.

This paper has shown a mobility protocol. This protocol carefully considers the features of the architecture deployed in a hospital in order to define a solution that reduces the amount of messages and overload in 6LoWPAN network. These features are, on one hand, the use of fixed IPv6 addressing to avoid reconfiguring IP addresses when patient nodes change networks. On the other hand, patient node delegates the management of the mobility to the Monere system. Hence, we reduce the amount of messages exchanged with the patient node, we reduce from 6 stages (12 messages exchanged) from Mobile IPv6 to 3 stages (6 messages exchanged) with the mobile node. Finally, this protocol considers the features of the architecture deployed in the hospital in order to define a solution that exploits the other elements of the architecture i.e., border router and backbone to carry out the mobility. Thus, the requirements and goals defined for the mobility protocol are partially fulfilled. For example, smooth handover is not fulfilled because connection is lost during handoff process. We can conclude that with a mobility protocol with support of this architecture, it is more feasible in a WSN based on 6LoWPAN.

7.1 Future Work

Ongoing work is oriented to, on one hand, optimization of the protocol to reduce handoff latency with techniques based on movement direction determination to carry out a fast handoff, which is based on pre-configuration of the mobile node configuration in the visited network. On other hand, evaluation of the protocol is going to be carried out in a real deployment, specifically in our Computer Science Faculty building, where a set of Monere systems are going to be deployed.

7.2 Acknowledgments

- This work has been carried out in frames of the Spanish Program: ”Programa de Ayuda a los Grupos de Excelencia de la Fundación Séneca 04552/GERM/06”.
- The authors would like to thank the University of Murcia by the scholarship ”Becas/Contrato Predoctorales”.

References

[1] Omnet++. the discrete event simulation environment. `www.omnetpp.org`, 2010.

[2] IEEE Standard 802.15.4-2003. Wireless medium access control and physical layer specifications for low-rate wireless personal area networks, 2003.

[3] Mukhtar H. Shams-S.M.S. Ki Hyung Kim Bag, G. and Seung wha Yoo. Inter-pan mobility support for 6lowpan. Convergence and Hybrid Information Technology, ICCIT 08, Volume 1, pp. 787-792, 2008.

[4] Raza M.T. Mukhtar-H. Akbar A.H. Shams-S.M.S. Kim K-H. Seung-wha Y. Bag, G. and Donghwa K. Energy-aware and bandwidth-efficient mobility architecture for 6lowpan. Military Communications Conference 2008, pp.1-7, 2008.

[5] Shams S.M.S. Akbar-A.H. Raza H.M.M.T. Ki-Hyung Kim Bag, G. and Seung-Wha Yoo. Network assisted mobility support for 6lowpan. Consumer Communications and Networking Conference, 2009. pp. 1-5, 2009.

[6] Pinto P. Rodrigues-A. Sa Silva J. Camilo, T. and F. Boavida. Mobility management in ip-based wireless sensor networks. World of Wireless, Mobile and Multimedia Networks, 2008. WoWMoM 2008, 23-26 June 2008, pp. 1-8, 2008.

[7] Mitschele A. Al-Nasouri E. Boringer R. Diab, A. and J. Xu. Mobile ip fast authentication protocol. Technische Universitat Ilmenau, Fachgebiet Integrierte HW/SW-Systeme, 2005.

[8] M. Dunmore and T. Pagtzis. Mobile ipv6 handovers: Performance analysis and evaluation. 6net project, 2004.

[9] Internet Engineering Task Force. `http://www.ietf.org/`, 2010.

[10] R. Monteiro-E. Sa Silva J. Granjal, J. Silva and F. Boavida. Why is ipsec a viable option for wireless sensor networks, wireless and sensor networks security. , 2008.

[11] C. Gungor and P. Hancke. Industrial wireless sensor networks: Challenges, design principles, and technical approaches. Industrial Electronics, Forthcoming, 2009.

[12] Seon Hong-C. Ho Kim, J. and T. Shon. A lightweight nemo protocol to support 6lowpan. ETRI Journal, vol.30, no.5, pp.685-695, 2008.

[13] J.W. Hui and D.E. Culler. Extending ip to low-power, wireless personal area networks. Internet Computing, IEEE, Volume 12, Issue 4, pp. 37-45, July-Aug. 2008.

[14] Blaya F. J. Zamora M. A. Jara, A. J. and A. F. G. Skarmeta. An ontology and rule based intelligent information system to detect and predict myocardial diseases. The 9th IEEE International Conference on Information Technology and Applications in Biomedicine, Cyprus, 2009.

[15] R. M. Sa Silva J.-Zamora M. A.. Jara, A. J. Silva and A.F.G. Skarmeta. Mobile ipv6 over wireless sensor networks (6lowpan) issues and feasibility. European Wireless Sensor Networks, 2010.

[16] Zamora M. A. Jara, A. J. and A. F. G. Skarmeta. An ambient assisted living system for telemedicine with detection of symptoms. Lecture Notes in Computer Science. Editorial: Springer Verlag. Volume: 5602 pp 75-84. 0302-9743, 2009.

[17] Zamora M.A. Jara, A.J. and A.F.G. Skarmeta. Hwsn6: Hospital wireless sensor networks based on 6lowpan technology: Mobility fault tolerance management. IEEE International Conference on Computational Science and Engineering, Vancouver (Canada), 2009.

[18] Perkins C. Johnson, D. and J. Arkko. Mobility support in ipv6 rfc 3775. , 2004.

[19] R. Koodli. Fast handovers for mobile ipv6, rfc 4068. , 2005.

[20] Montenegro G. Kushalnagar, N. and C. Shumacher. Ipv6 over low power wireless personal area networks (6lowpan), rfc 4919, 2004.

[21] Montenegro G. Hui J. Kushalnagar, N. and D. Culler. 6lowpan: Transmission of ipv6 packets over ieee 802.15.4 networks - rfc 4944, 2007.

[22] Jin-Shyan Lee. Performance evaluation of ieee 802.15.4 for low-rate wireless personal area networks. IEEE Transactions on Consumer Electronics, Vol. 52, No. 3, 2006.

[23] J. Santa M. A. Zamora and A. F. G. Skarmeta. Integral and networked home automation solution towards indoor ambient intelligence. Pervasive Computing, 2010, accepted for publication.

[24] Xin Ma and Wei Luo. The analysis of 6lowpan technology. Computational Intelligence and Industrial Application, PACIIA 08. Volume 1, pp. 963 966, 2008.

[25] Kim Kang-Myo Chaudhry S.A. Akbar A.H.-Kim Ki-Hyung Mukhtar, H. and Seung-Wha Yoo. Lnmp- management architecture for ipv6 based low-power wireless personal area networks (6lowpan). Network Operations and Management Symposium, 2008. NOMS 2008, pp. 417-424, 2008.

[26] Thurbert P.-Hui J. Chakrabarti S. Bormann-C. Shelby, Z. and E. Nordmark. 6lowpan neighbor discovery. draft-ietf-6lowpan-nd-12, Internet-Draft IETF, work in progress, 2010.

[27] Camilo-T. Silva J. Shin, M-K. and D. Kaspar. Mobility support in 6lowpan. IETF Internet Draft draft-shin-6lowpan-mobility-01.txt, work in progress., 2009.

[28] A. Sleman and R. Moeller. Integration of wireless sensor network services into other home and industrial networks; using device profile for web services (dpws). Information and Communication Technologies: From Theory to Applications. ICTTA 2008, pp. 1 - 5, 2008.

[29] Castelluccia C.-ElMalki K. Soliman, H. and L. Bellier. Hierarchical mobile ipv6 (hmipv6) mobility management, rfc 5380, 2008.

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. He is with the Department of Information and Communication Engineering, UMU, since 2007, where he works on several projects related to the RFID applications in Intelligent Transport Systems (ITS) and healthcare. He is especially focused on security and mobility for Internet of things and its applications in healthcare, ITS and home automation.

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 Va-lencia (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 ve-hicles and RFID applications in ITS and medical envi-ronments.

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 Univer-sity of Murcia. Since 1993, he is Assistant Professor with Department of Information and Communications Engi-neering at the same university. Research interests include mobile communications, GNSS location-based services and RFID applications in ITS and medical environments. He has published over 100 international papers.