This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2010 proceedings

# An architecture based on Internet of Things to support mobility and security in medical environments

Antonio J. Jara, Miguel A. Zamora and Antonio F. G. Skarmeta *IEEE Member*
University of Murcia, Computer Science Faculty, Murcia, Spain. jara@um.es

***Abstract*— Recently the problem of providing effective and appropriate healthcare to elderly and disable people is an important field in relative to the aging of population problems. The objective of information and communication technologies (ICT) is to focus on the new technologies the medical environments, so that it can provide management to accelerate and improve the clinical process. Our contribution is to introduce an approach based on Internet of things (IoT) in medical environments to achieve a global connectivity with the patient, sensors and everything around it. The main goal of this globality feature is to provide a context awareness to make the patient's life easier and the clinical process more effective. To achieve this approach, firstly has been developed an architecture which has been designed to offer great potential and flexibility of communications, monitoring and control. This architecture includes several advanced communication technologies; among them are 6LoWPAN and RFID/NFC, which are the basis of the IoT. Moreover the research deal with the problems related to the mobility and security that happens when IoT is applied in medical environments. The mobility issue requires developing a protocol over 6LoWPAN network to be carried out in sensor networks with high specification related with low power consumption and capacity. While in the RFID/NFC technologies need to support secure communications, our proposal is to introduce a set of security techniques and cryptographic SIM card to authenticate, encrypt and sign the communications with medical devices. The preliminary results showed a reduction of time in the handover process with the protocol for mobility defined, by omitting the stages of addressing and simplifying the MIPv6 protocol. In addition to increase the security in the communications carried out by NFC devices enhanced with the inclusion of cryptographic SIM card.**

***Keywords*— Internet of things, Ambient Assisted Living, 6LoWPAN, RFID, NFC, mobility, security, hospital.**

## I. Introduction

NEW problems are arising with aging of the population, as a result of increased life expectancy and declining birth rate. Today there are around 600 million persons aged 60 in the world. The number will be doubled by 2025 and will reach almost 2000 million by 2050 [1]. Therefore, the demand of healthcare services is increasing in Europe and now we have a problem; we are not able to react to the demand of healthcare services because of the lack of personnel, old people's home and nursing homes. For this reason, it is well known that the information and communication technology (ICT) must provide an answer to problems arisen in the field of healthcare.

ICTs evolution has led to wireless personal devices like cellular phone, personal computer, PDA etc. These devices have in common that are designed to operate over IP Networks. Hence, the number of devices that are connected to the Internet has grown exponentially. This increase of devices has led to a new version of Internet (IPv6), which is characterized by increasing address space, to support all the existing and new devices. Furthermore, IPv6 has been designed to provide at all times secure communications to users, so there is no place any intrusion into their lives. In addition, IPv6 also provides mobility for all the devices attached to the user; thereby users can be always connected. IPv6's features is what has made possible to think about to connect all the objects that surround us to Internet, it is Internet of things (IoT). The objective of IoT is the integration and unification of all communications systems that surround us. Hence, the systems can get a control and access total to the other systems for leading to provide ubiquitous communication and computing with the purpose of defining a new generation of assistance services.

IoT is complemented by the application of artificial intelligence, to learn user behavior patterns, gain knowledge of the context, define action rules for each scenario in relation with the user's behavior etc. Specifically, the field from artificial intelligence that works with the Internet of things to define services for the assistance of people is ambient intelligence and particularly when dealing with healthcare of elderly and disabled people is Ambient Assisted Living (AAL). The goal of AAL aims to prolong the time that elderly people can live independent in decent way in their own home [2]. It can be achieved increasing their autonomy and confidence, knowing that if any problem happens, they are not really alone, doing activities of daily living easier with IoT and AAL solutions.

The main goal of this paper is to define an architecture based on IoT to offer AAL services for elderly people in medical environments. The problem is that the IoT's technologies, in order to make large deployments and integrate them into all the objects that surround us, have been designed to be low cost, consumption and size, which means that they cannot offer enough capacity to handle the mobility and security as defined in IPv6. Hence a set of challenges arise and consequently the objectives of our research.

Our proposal for the Internet of things in medical

978-1-4244-5176-0/10/$26.00 ©2010 IEEE

Authorized licensed use limited to: University of Melbourne. Downloaded on September 19,2020 at 09:25:25 UTC from IEEE Xplore. Restrictions apply.

environments is based on three pillars:

Firstly, to provide connectivity to devices such as sockets, lights etc. an architecture has been built to offer services of home automation, security, control and communication, it provides great flexibility and scalability, to be able to offer solutions in very wide scenarios [3-4].

Secondly and thirdly are used the technologies which are the basis for the Internet of things, for active communications is used 6LoWPAN (IPv6 based Low-Power Personal Area Networks) and for passive communications is used RFID (Radio Frequency Identification) and NFC (Near Field Communication).

The problems from these technologies are that they cannot offer enough capacity to handle the mobility and security as defined in IPv6. On one hand, 6LoWPAN does not support the mobility protocol Mobile IP (MIPv6) devices defined for IPv6 [5]. But we need to support mobility in 6LoWPAN, so that in order to give mobility support, we had defined a mobility protocol that can be adapted to the limitations and requirements of 6LoWPAN devices [6]. On the other hand, with respect to RFID/NFC appears the problem that these technologies are not secures [7]. This raises some society concerns because they can be traced or can be accessed private information without their consent. That is why we need to protect and restrict access to data from RFID tags. In addition to the inclusion of RFID in cellular phones with NFC services like payment, identification and now for management of clinical information (electronic health records) make the issue of security even more important and therefore should be treated [8-9].

In conclusion, this goal of this paper is to offer a proposal to solve the problems that appears in the technologies that enable Internet of things, to provide a consistent, secure and robust technology to make the Internet of things might become a reality in medical environments. For that proposal, on one hand for RFID/NFC, we include cryptographic SIM card [15] to support security and on the other hand, for 6LoWPAN, we have developed a mobility protocol, which is based on the architecture built to support IoT. Thus we define a set of proposals to solve the challenges found in the integration of the Internet of things in medical environments.

## II. An architecture for AAL based on IoT

We have developed a modular architecture to be scalable, secure, effective and affordable. Its last feature is very important, because we are defining a very complex, flexible and with a lot of possibilities system. Usually a user does not need all the technologies that system provides, so that each client can define an ad-hoc solution from his needs [11-12].

One of the most important parts of a system that works with users is the user interface. We can find a lot of literature about Human Machine Interface (HMI) and the need of simple and intuitive interfaces, especially in this case, where a very simple interface is needed because it works with elder people who are not fully adapted to the world of new technologies (ICT), have vision problems or cannot learn to use the system (e.g. Alzheimer patients). That is why the proposal is that the user does not need to communicate with the system. However, we offer an intuitive LCD touch and Web interface with a 3D (360 degree cylindrical panoramas) home/hospital representation to access and control the system for hospital personal, old people's home personal, management personal or patients if they are able to use it. It is shown in figure 1. Where, in the left picture is shown a control panel with touch screen and touchpad interfaces. In the middle picture is shown a screenshot of the house setting-up software. Finally, in the right picture is shown the Flash application with 3D HMI for local and remote management.

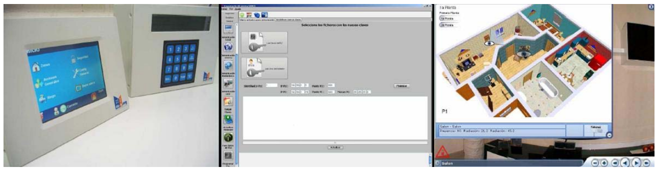

**Figure 1. Users interface of the system**

The communication layer provides privacy, integrity and authentication during process of exchanging information between agents. This system ciphers all the communications with AES cryptography to get privacy and security. It uses hashing with MD5 to get integrity, and user and password to get authentication.

This system has been designed to work with sensors for medical purpose from different vendors. Therefore, this system has a very flexible and open connectivity support.

The system has the next communication interfaces (see figure 2):

***1) External communications*****:** Ethernet connection for UDP/IP communications (Internet), modem GPRS (Internet) and Contact ID using PSTN.

***2) Local communications:*** X10 home automation protocol, EIB/KNX (European Installation Bus), Bluetooth, Serial, CAN (Control Area Network), wire communications using digital or analog input/output and for Internet of things are included 6LoWPAN and RFID.

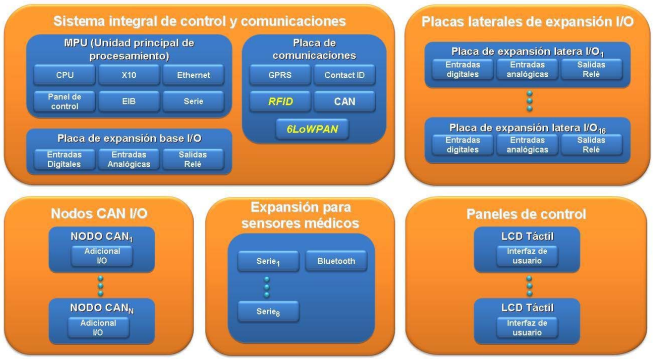

**Figure 2. Communications diagram.**

Hence, this architecture serves as a framework to deliver healthcare services to elderly and disable people. This

Authorized licensed use limited to: University of Melbourne. Downloaded on September 19,2020 at 09:25:25 UTC from IEEE Xplore. Restrictions apply.

framework is used as a basis to deploy specialized services, coverings aspects such as:

***1) Home automation:*** This service is going to do easier the home facilities. This system was originally designed as a system that integrates multiple technologies for home automation, adding a high-capacity and heterogeneous communications layer to interact with other systems.

***2) Security:*** It is very usual to find security solutions together with home automation ones. For this reason, it is able to be used like a security system too, and for that purpose, it implements the standard protocol used nowadays in security systems to send alarms to a central security, i.e. contacted over Public Switched Telephone Network (PSTN).

***3) Ambient Intelligence:*** Ambient intelligence is used to increase the easiness of use of home facilities provided by the home automation and to adapt home to the Activities of Daily Living (ADL). ADL refers to the basic task of everyday life, such as eating, bathing, dressing, toileting and transferring [13]. If a person can do his ADL, then we can talk of independence. These kinds of tasks are very difficult in elderly people. Thus learning behaviors using Ambient Intelligence, ADL is going to be easier for these persons.

***4) Telemedicine****:* The last service is health condition monitoring for healthcare of elderly and disable people who live in their homes. For that purpose, a set of biometric sensors are located in the environment of the patient, which transmit, via the central module, information about his/her health status to the hospital, so that, the information from the patient can be accessed by qualified professionals to evaluate their health status. Hence, Doctors can carry out a remote diagnosis. Furthermore, the architecture installed at the patient's home could raise alarms in case of abnormal values.

## III. RFID/NFC: Challenges and proposals in security

This section examines the challenges of RFID and NFC in security, for each one of the security problems found, we make a proposal to solve it [7-10]. The security problems in RFID/NFC and possible solutions are:

***1) Only one ID:*** Each tag has only one ID, it is used for identification and in the anticollision algorithm. Therefore, it can be read and used to supplant the owner.

**Solution:** A random generation algorithm could be used to generate a different ID. This ID can be used in the anticollision algorithm, so that real ID is just given when reader or tag is authenticated.

***2) Denegation of Service:*** The reader is working even with wrong and white cards, sending error messages. Hence, if reader is using a battery as in cellular phones, it is going to wear out and reader will stop of working.

**Solution:** We can use a button to activate the device under demand, this problem could be solved.

***3) Eavesdropping in card emulation:*** Data from the card can be read even with the device turned off, it is because card emulation mode does not need battery to work.

**Solution:** Similarly, a button could be used to activate the card emulation mode, avoiding the possible reading of the card when the user does not wish it.

***4) Eavesdropping in peer to peer:*** The communications are not ciphered, so they could be intercepted.

**Solution:** The solution to this requires a cipher. We can define two kinds of ciphers:

1- **Symmetric ciphers:** It needs that tag and reader share a key, so that data is ciphered with the shared key. It is a suitable solution for environments where we have control over all the devices, so we can define the shared key before of communications. We can find this solution in RFID with the DESFare tags.

2- **Asymmetric ciphers:** It can carry out secure communications without that reader and tag share any key. Asymmetric cipher is more interesting on mobile phones, because we could interact with a lot of different devices that have not shared any key. But it is not defined in RFID solutions; therefore we are going to use an element to asymmetric cipher. We call to this element "secure element".

***5) Privacy of the device contents:*** Malicious applications in our mobile could sniff the NFC index of applications existent in some cards (NXP in Mifare, JCOP …).

**Solution:** We just allow access to application index to applications with a digital signature (for authentication that it is not a malicious application), so we need to add digital certificates management to our devices. One more time, it is not available in NFC solutions, so we are going to add an element to digital certificates management.

We realized that it needs a secure element to cover the needs of asymmetric cipher and digital certificate management. The best secure element for a mobile phone is a cryptographic SIM card [15], with the capabilities of a normal SIM card plus asymmetric cipher, digital certificate management and safe storage for data and applications.

## IV. 6LoWPAN: Challenges and proposals in mobility

6LoWPAN devices could be considered that are empowered with IP protocols, for mobility (e.g. MIPv6), management (e.g. SNMP) etc. However it is not feasible for these devices that are energy and resource constrained.

Some studies can be found about the low performance of MIPv6 like HMIPv6 for mobility [16, 18-19] and SNMP like LNMP for management on 6LoWPAN networks [20].

We present a protocol to carry out inter-WSN mobility inside of the architecture that has been defined at a hospital. This protocol shows how we exploit the elements of the architecture with high capacity and resources to carry out the moving signalling; therefore mobile nodes decrease the number of interchanged messages [6].

The protocol defined includes a suitable security support to assure the protection of the patient's information.

Figure 3 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

Authorized licensed use limited to: University of Melbourne. Downloaded on September 19,2020 at 09:25:25 UTC from IEEE Xplore. Restrictions apply.

through the hospital or they are moved to other room to do some medical tests (e.g. radiography).

In the figure 3, phase 1 shows an initial state of the patient node in his room, 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.

In the figure 4 is illustrated a diagram with the exchange of messages in order to carry out the changes of networks shown in figure 3.

1- **Exchange of messages in the Base Network:** The messages between 1 and 7 as seen in the figure 4, shows the usual data frames, requests, responses and acknowledgments of the transmission of information between sensor node and architecture. Data frames contain monitoring information such (EKG wake values, SPo2 level, blood pressure values …). Request messages are queries to the patient's node either to obtain values or to change configuration. Response messages are the replies to the request messages.

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 [16]. Moreover in the patient node the current router is no longer reachable, and a new access router is available [17].

3- **Entering to the visited network (Router discovery):** 6LoWPAN coordinator (architecture) periodically transmits beacon packets (message 8 in figure 4), 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 (architecture from the base network). Remark that in this step, as fixed IPv6 addressing is used, 6LoWPAN coordinator must only assign a short address (16 bits) [18]. Architecture detects a new node in its network, thus it initiates the authentication process.

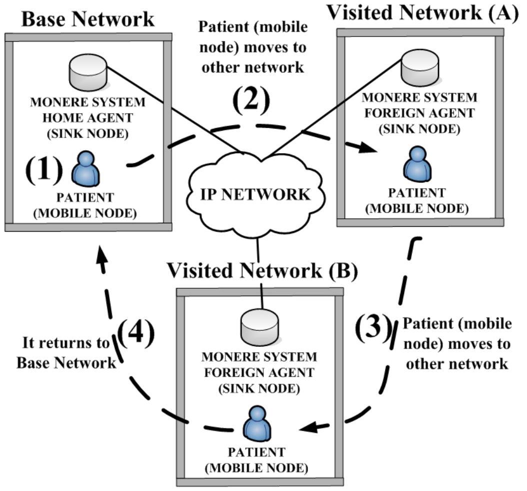
Base Network
Patient (mobile node) moves to other network
Visited Network (A)
MONERE SYSTEM HOME AGENT (SINK NODE)
(2)
MONERE SYSTEM FOREIGN AGENT (SINK NODE)
(1)
PATIENT (MOBILE NODE)
IP NETWORK
PATIENT (MOBILE NODE)
Visited Network (B)
It returns to Base Network
(4)
(3)
Patient (mobile node) moves to other network
MONERE SYSTEM FOREIGN AGENT (SINK NODE)
PATIENT (MOBILE NODE)

**Figure 3. Mobility scenario**

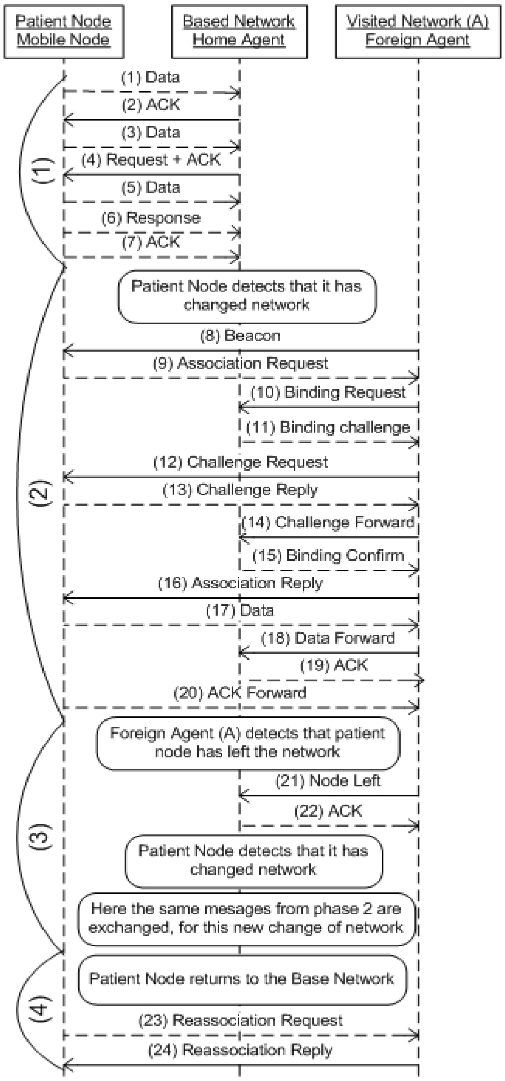

**Figure 4. Messages exchanged for mobility**

4- **Authentication of mobile node in visited network:** To confirm that the new mobile node is from the hospital, it is authenticated. In first place, foreign agent sends a message to the home agent. This message informs relative to the presence of patient 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 to the home agent (message 14). Home agent checks it, if it is right sends a confirm message to the foreign agent (message 15). In other case it sends a deny message.

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

Authorized licensed use limited to: University of Melbourne. Downloaded on September 19,2020 at 09:25:25 UTC from IEEE Xplore. Restrictions apply.

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 reassociation request to inform of its new location (messages 23- 24).

## V. NEW SERVICES IN MEDICAL ENVIRONMENTS FROM IOT

In this section is going to be shown the services from Internet of things for each one of the actors in the hospital:

***1) Patient:*** Patients can move in the hospital facilities when they are being monitored, they are not wired to a set of machines, because he is monitored at all times by an wireless and wearable system [14], further this wearable system is connected to the architecture defined in section 2, which assures that if an anomaly happens it will be detected.

***2) Nurse and clinical assistant:*** They capture the information from medical systems with a NFC based mobile device; thereby, data from the patient is sent directly to the electronic health record (EHR), hence it reduces error. Further, they can check medicines (RFID tagged) with the EHR before before providing to the patient. Other common use of RFID in hospitals is for tracking of hospital resources.

***3) Doctor****:* He can access remotely to patient monitoring information (EHR), therefore, he can add instructions for the patient remotely, consult patient information and even these solutions can include a decision support system to help to the doctor in the diagnosis of the patient (see future work).

## VI. CONCLUSION AND FUTURE WORK

Internet of Things and Ambient Assisted Living are the research lines from ICT to alleviate the problems posed by the aging population. The problem that arises when IoT and AAL solutions are applied in medical environments is that these environments define a set of requirements for which IoT technologies were not originally designed. In particular, RFID and NFC were not designed to carry out secure communications, therefore, when its use is extended beyond what is prescribed arises security problems. On the other hand, LoWPAN networks were not designed to handle the IP stack, therefore, a set of security and mobility problems arises with 6LoWPAN.

Our contribution has been to build an architecture to support IoT in medical environments. Hence, the problems mentioned are solved. For NFC has been explained how to carry out secure communications, therefore this technology can be applied in hospitals without violating the privacy of the patient's information. With respect to 6LoWPAN has been proposed a mobility protocol based on the architecture defined, thereby it can cover their weaknesses and allow it to perform the mobility without the overhead of MIPv6.

As future work, on one hand, we are going to analyze the power consumption of the 6LoWPAN sensors to check whether the introduction of the mobility protocols maintains the principles of low power consumption from LoWPAN. On the other hand, we are going to introduce algorithms for detection symptoms in the architecture applying medical knowledge and chronobiology algorithms. Finally, we are going to integrate the standard CEN/ISO 13606 for Electronic Health Record to export clinical information and exchange data between hospital and patient's residence.

## ACKNOWLEDGMENT

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 and the project: TSI-020302-2009-89.

## REFERENCES

[1] United Nations.: "World Population Ageing 2007", www.un.org/esa/population/publications/WPA2007/wpp2007.htm (2007).

[2] Steg, H. et al.: Europe Is Facing a Demographic Challenge - Ambient Assisted Living Offers Solutions.VDI/VDE/IT, Germany (2006).

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

[4] A. J. Jara; M. A. Zamora and A. F. G. Skarmeta. An architecture for ambient assisted living and health environments. Distributed Computing, Artificial Intelligence, Bioinformatics, Soft Computing and Ambient Assisted Living,, Lecture Notes, pp. 882-889 (2009).

[5] J. Granjal; R. Silva; J et al. Why is IPSEC a viable option for wireless sensor networks. In Wireless and Sensor Networks Security, (2008).

[6] A. J. Jara; M. A. Zamora and A. F. G. Skarmeta. (HWSN6) hospital wireless sensor networks based on 6LoWPAN technology: mobility and fault tolerance management. The 7th IEEE IFIP International Conference on Embedded and Ubiquitous Computing, (2009).

[7] Klaus Finkenzeller. Known attacks on RFID systems, possible countermeasures and upcoming standardisation activities. In 5th European Workshop on RFID Systems and Technologies, (2009).

[8] A. J. Jara; M. A. Zamora and A. F. G. Skarmeta. NFC/RFID applications in medicine: security challenges and solutions. 5th International Conference on Intelligent Environments - IE'09 (2009).

[9] A. J. Jara; M. A. Zamora and A. F. G. Skarmeta. Secure use of NFC in medical environments. 5th European Workshop on RFID Systems and Technologies, (2009).

[10] Gerald Madlmayr. NFC devices: Security & privacy. 3$^{a}$ Internacional Conference on Availability, Reliability and Security (2008).

[11] Alsinet, T. et al.: Automated monitoring of medical protocols: a secure and distributed architecture, Artificial Intelligence in Medicine, Volume: 27, pp. 367-392. (2003).

[12] Magrabi, Farah et al.: Home telecare: system architecture to support chronic disease management. Engineering in Medicine and Biology Society. Proceedings of the 23rd Annual International Conference of the IEEE, Volume 4, 25-28, pp. 3559 - 3562 (2001).

[13] Cortes, Ulises et al.: Intelligent Healthcare Managing: An assistive Technology Approach, IWANN 2007, LNCS, pp. 1045-1051 (2007).

[14] A. J. Jara; M. A. Zamora and A. F. G. Skarmeta. A wearable system for Tele-monitoring and Tele-assistance of patients with integration of solutions from chronobiology for prediction of illness. Ambient Intelligence Perspectives: Selected Papers from the First International Ambient Intelligence Forum 2008, pp. 221-228. IOSPress, (2008).

[15] György Calman et al. SIM as secure key storage in communication networks. Proceedings of the third international conference on wireless and mobile communications - ICWMC'07 (2007).

[16] Bag, G., Raza, M.T et al., "Energy-aware and bandwidth-efficient mobility architecture for 6LoWPAN", Military Communications Conference 2008, pp.1-7 (2008).

[17] Dunmore, M. and Pagtzis, T., 6net project, "Mobile IPv6 Handovers: Performance Analysis and Evaluation" (2004).

[18] Bag, G., Shams, S.M.S et al "Network Assisted Mobility Support for 6LoWPAN", Consumer Communications and Networking Conference, 2009. pp. 1-5. (2009).

[19] Camilo, T., Pinto, P., Rodrigues, A. et al, "Mobility management in IP-based Wireless Sensor Networks", World of Wireless, Mobile and Multimedia Networks, pp. 1-8. (2008).

[20] Mukhtar, H., Kim Kang-Myo et al, "LNMP- Management architecture for IPv6 based low-power wireless Personal Area Networks (6LoWPAN)", Network Operations and Management Symposium, 2008, (2008).

Authorized licensed use limited to: University of Melbourne. Downloaded on September 19,2020 at 09:25:25 UTC from IEEE Xplore. Restrictions apply.