A group-based wireless body sensors network using energy harvesting for soccer team monitoring

Jaime Lloret*

Integrated Management Coastal Research Institute,
Universidad Politécnica de Valencia,
Valencia 46022, Spain
Email: jlloret@dcom.upv.es
*Corresponding author

Miguel Garcia

Departamento de Informática,
Universidad de Valencia,
Valencia 46100, Spain
Email: miguel.garcia-pineda@uv.es

Angel Catala

Integrated Management Coastal Research Institute,
Universidad Politécnica de Valencia,
Valencia 46022, Spain
Email: acatala@moliprimer.com

Joel J.P.C. Rodrigues

Instituto de Telecomunicações,
University of Beira Interior,
Covilhã 6201-001, Portugal

and

University ITMO,
St. Petersburg 197101, Russia
Email: joeljr@ieee.org

Abstract: In team-based sports, it is difficult to monitor physical state of each athlete during the match. Wearable body sensors with wireless connections allow having low-power and low-size devices, that may use energy harvesting, but with low radio coverage area but the main issue comes from the mobility. This paper presents a wireless body sensors network for soccer team players' monitoring. Each player has a body sensor network that use energy harvesting and each player will be a node in the wireless sensor network. This proposal is based on the zone mobility of the players and their dynamism. It allows knowing the physical state of each player during the whole match. Having fast updates and larger connection times to the gateways, the information can be routed through players of both teams, thus a secure system has been added. Simulations show that the proposed system has very good performance in high mobility.

Keywords: group-based wireless sensor network; WSN; wireless body sensor network; mobility; soccer.

Reference to this paper should be made as follows: Lloret, J., Garcia, M., Catala, A. and Rodrigues, J.J.P.C. (2016) 'A group-based wireless body sensors network using energy harvesting for soccer team monitoring', *Int. J. Sensor Networks*, Vol. 21, No. 4, pp.208–225.

Biographical notes: Jaime Lloret is an Associate Professor at Universitat Politecnica de Valencia. He is the Head of research group 'communications and remote sensing' of the Integrated Management Coastal Research Institute. He is the director of Master degree 'Digital Post Production'. He is currently Chair of Internet Technical Committee. He has authored 12 books and has more than 240 research papers published in conferences and international journals. He has been the co-editor of 15 conference proceedings and guest editor of several international books and journals. He is Editor-in-Chief of the international journal 'Networks Protocols and Algorithms'. He is currently the chair of the Working Group of the Standard IEEE 1907.1. He has been general chair (or co-chair) of 19 International workshops and conferences.

Miguel Garcia, PhD, is an Assistant Professor in the Department of Computer Science at the University of Valencia, Valencia, Spain and a researcher of the same department. His work is focused on the area of wireless sensor networks, multimedia networks, computer networks and cloud computing, where he has more than 45 scientific papers published in international conferences and more than 30 papers published in international journals. He has been technical committee member in several conferences and journals; also, he has been in the organisation committee of several conferences. He is an Associate Editor of several journals.

Angel Catala is currently a PhD student of the doctoral programme in Telecommunications at Universitat Politecnica de Valencia. He received his BS in Computer Science and his MS in Telecommunications Engineering at the same university. He has mainly developed his professional career in private sector. Nowadays, he is working as Software Engineer in the Public Health System of Spain. His knowledge areas are network and software engineering.

Joel J.P.C. Rodrigues is a Professor in the Department of Informatics of the University of Beira Interior, Covilhã, Portugal, and a Researcher at the Instituto de Telecomunicações, Portugal. His main research interests include sensor networks, delay-tolerant networks, e-health, e-learning, and mobile and ubiquitous computing. He is the Editor-in-Chief of IJEHMC and Recent Patents on Telecommunications journals, has served as Chair and TPC Member for many international conferences, and several editorial review boards. He has authored or co-authored over 150 publications. He is a licensed professional engineer (as senior member), and he is Member of ACM SIGCOMM, ISOC, an IARIA Fellow, and a Senior Member of IEEE.

This paper is a revised and expanded version of a paper entitled 'A wireless sensor network for soccer team monitoring' presented at *International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, Barcelona, Spain, 27–29 June, 2011.

1 Introduction

The number real deployments of wireless sensor networks (WSNs) has increased enormously in the last years (Bri et al., 2009; Garcia et al., 2010a). Body area networks (BANs) and wireless body area networks (WBANs) have emerged as a technology for health monitoring because of their huge benefits (Xiang and Zhu, 2009). Their main uses are focused on sensing biometrical parameters, by means of wearable devices, from target individuals for both monitoring actual medical episodes and preventing further complications. Some of these biometrical parameters are hearth rate, temperature, blood pressure, walking biometric parameters, etc. Furthermore, BANs and WBANs can be used to collect athletes' data for performance assessment and/or improvement. Both technologies can be accomplished by means of off-line processing of the data collected from the athlete sensing system. Several works in the literature give us an overview of the wide range of applications (Glaros and Fotiadis, 2005). For example, how to monitor foetal movement during a woman's pregnancy is shown in Borges et al. (2008).

Many different types of sensors and actuators are used in a WBAN (Latré et al., 2011). The main use of all these devices is found in the area of health applications. The number of nodes in a WBAN is limited by the nature of the network. Smaller integrated circuits and embedded devices, new technological advances in miniature bio-sensing devices, small physiological sensors, transmission modules and processing capabilities, made possible the appearance of new wearable sensor systems for health, mental and activity status monitoring. WBANs have several requirements and challenges. They are shown as follows:

- *Size*: They must be very small (often < 1 cm^3 (Gyselinckx et al., 2006), and easy to wear, in order to disturb the human as less as possible. Moreover, non-invasive sensors are desired in order to automatically monitor the human body.
- *Deployment and density*: BAN/WBAN nodes are placed strategically on the human body, or are hidden under clothing. They do not form a dense network.
- *Availability*: There are no redundant devices. All devices are equally important. Each device is added for a specific purpose and it is only added when they are needed.
- *Mobility*: The devices are located on the human body that can be in motion. BANs/WBANs should therefore be robust against frequent changes in the network topology. Although BANs/WBANs nodes share the same mobility pattern.
- *Reliability and delay*: Gathered data consists of medical information. Thus, BAN/WBAN should provide high reliability and low delay. This requirement is dictated by the medical applications.
- *Data rate*: BANs/WBANs data streams may occur in a periodic manner, and have relatively stable rates. Owing to strong heterogeneity of applications, data rates will vary strongly, ranging from simple data at a few kbps to video streams of several Mbps. Common rates are around 50–200 kbps.
- *Energy*: Energy consumption can be divided into three domains: sensing, wireless communication and data

processing. The wireless communication is likely to be the most power consuming. In most devices it is not possible to recharge or change the batteries for the lifetime of the device is wanted. For this reason, a correct WBAN should transmit information only when it is necessary, but with enough power because the waves could be attenuated considerably before they reach the receiver (Jovanov, 2008). Moreover, an extremely low transmit power per node is needed to minimise interference with health concerns (IEEE Std. C95.1b-2004, 2004).

- *Quality of service (QoS)*: Proper QoS handling is an important part in the framework of risk management of medical applications. A crucial issue is the reliability of the transmission in order to guarantee that the monitored data are received correctly by the healthcare professionals.
- *Usability*: In most cases, a WBAN will be set up in a hospital by medical staff, not by ICT-engineers. Consequently, the network should be capable of configuring and maintaining itself automatically, i.e. self-organisation and self-maintenance should be supported.
- *Security and privacy*: The communication of health-related information between BAN/WBAN nodes, and over the internet to servers, is strictly private and confidential and medical data should be encrypted to protect the patient's privacy.

Zigbee is the commonly used wireless technology in WBANs. It was developed to address the needs of small, low-cost and low-power wireless networks. Its standard is specified in IEEE 802.15.4-2006 (2006) and it operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz. It is a packet-based radio protocol that allows devices to communicate in a variety of network topologies and can have a long live battery (even for several years, depending on the quantity of data that is transmitted).

WBAN systems have to ensure seamless data transfer across ZigBee to promote information exchange and plug and play device interaction. Furthermore, the systems should be scalable, reliable and secure, ensure efficient migration across networks, and offer uninterrupted connectivity for personal and individual healthcare.

In this paper, we make use of WBANs and propose a WSN that allows the interconnection of WBANs placed en each soccer player. The major issues to be solved with this approach are:

- The radio coverage distance of each soccer player must not be longer than 2, 3 or 4 metres in order to avoid eavesdropping from any place of the stands. Any person trying to hack the system, should have a very big satellite dish, thus it will be detectable.
- The transmission power between soccer players will be very low, so wireless sensor nodes will have very low power consumption, and an energy harvesting system can be used to provide energy.
- The mobility of the soccer players will permit to transmit their physical state while they are playing.
- Bearing in mind that there are two teams playing the soccer game and the radio coverage of each player is very short, we take profit of all players playing in the game for transmission purposes.
- All players must be able to send the information health to the trainer of its team. The information should be sent encrypted, but only those players from the same team will be able to decrypt it.

This paper is an extension of our paper presented in Garcia et al. (2011). In this extension paper, we have added the proposed body sensors to for the soccer players, the energy harvesting system and detailed the security system used in our proposal. Moreover, we have improved the mobility model and increased the number of simulations of our proposal in order to show in depth the performance of the system. As far as we know there is not any group-based system for soccer teams such as the one presented in this paper.

The paper is organised as follows. Section 2 details some related work from three perspectives: group-based topologies and mobility models, biosensor systems for athletes, and group-based security systems. The body sensors used for our proposal are introduced in Section 3. Energy harvesting system is detailed in Section 4. Section 5 presents the proposed system architecture. In Section 6, we explain the security system used in our proposal. The mobility model, the analytical assumptions and the routing protocols used in our proposal is described in Section 7. Section 8 provides the simulation results. Finally, our conclusion and future work are shown in Section 9.

This section is divided into three main parts. The first one is focused on group-based topologies and mobility models, the second part shows some important works on security systems for ad hoc and sensor network groups and the third part is focused on the research on biosensor systems for athletes or for any sportsman or sportswoman. In this last case, athletes, sportsmen or sportswomen become ad hoc network nodes that need to transmit and relay information from their own sensors or from other players to the sink nodes. Our proposal requires new mobility models, which follow accurately the paths of the players in the field during the match, as well as reliable routing protocols.

2 Related work

When several teams or groups of people should be monitored at the same time, a group-based topology must be used. Moreover, each group could have different topology (Lloret et al., 2008). In this paper, we consider that groups are located in the same place and a node can only belong to one group. An example of how groups can be created and could coexist in the same place is shown in Lloret et al. (2009).

Camp et al. (2002) present a survey of mobility models that are used in ad hoc network simulations. They describe individual mobility models and group mobility models. The models are classified in traces and synthetic, and they focused their work in the second type. Their results show the importance of choosing a mobility model when an ad hoc protocol is simulated. Most of these group models could be a reference-point for modelling soccer player's behaviour.

One of the most well known routing protocols that consider moving groups in Wireless Ad Hoc Networks is Landmark Routing Protocol (LANMAR) (Pei et al., 2000). Pei et al. presented an approach where the set of nodes move as a group, so the group can enlarge or diminish with the motion of the members. The fact of considering nodes moving as a group lets the system to reduce routing update overhead. LANMAR combines the features of link state and distance vector routing protocols, which exploits and adapts to the wireless ad hoc environment. Nodes exchange link state only with their neighbours. Routes within links state scope are accurate, while routes to remote groups of nodes are 'summarised' by the corresponding landmarks. The proposal is a 'proactive' routing scheme.

Several works propose group-based security systems. The main problem is how to secure a single group (or several groups) when the network is formed by groups of nodes.

In Wong et al. (2000) was proposed a system using key graphs to specify secure groups. They focused the problem from a group/multicast key management problem perspective. They investigated three rekeying strategies, user-oriented, key-oriented and group-oriented, and specified join/leave protocols for them. The system was based on a hierarchy of keys.

To avoid the dependency on sensors' expected locations to help pre-distributing keying materials (Liu et al., 2008) propose a group-based key pre-distribution deployment model where sensor nodes are deployed in groups. They assumed that nodes in the same group are close to each other after the deployment.

Kashif Kifayat et al. proposed a structure and density independent group-based key management protocol in Kifayat et al. (2007). Their aim was to develop a protocol in order to provide better secure communication, secure data aggregation, data confidentiality and resilience against node capture and replication attacks using reduced resources in group-based networks.

We also proposed a security system for group-based WSNs in Garcia et al. (2010b). The paper explained the methods of key creation management. Moreover, we took into account a secure communication between groups. In this case, we estimated the energy consumption given by each operation in the group-based security protocol.

There are some works related to the sensing of physiological and health data from professional sport practitioners, but most of them rely on off-line data analysis. Next works show how some systems allow real-time monitoring. There are also some experiences where athletes and soccer players are monitored. In Pantelopoulos and Bourbakis (2010), they present a survey on wearable biosensor systems for health monitoring. They compare a variety of system implementations and approaches. They study a set of significant features and identify their technological shortcomings.

A body area sensor network for monitoring soccer players in a soccer field is presented in Dhamdhere et al. (2010). They show their design and discuss the choices taken for their proposal. Because of the high delays for direct transmissions from the soccer players to the base stations, they propose a multi-hop routing protocol that balances between the competing objectives of resource consumption and the delay.

A group mobility model (called DynaMo) that takes into account the interactions between players and the expected trajectories of players during a soccer match, is presented in De Nardis et al. (2010). Each player wears a BAN that collects and transfers data to a sink node by means of inter-BAN multi-hop routing. The impact of the mobility on the network performance is analysed in terms of throughput and delay. Moreover, the model is compared with existing solutions (such as the Reference Point Group Mobility model) by analysing the generated mobility patterns.

In Sivaraman et al. (2010), the authors conduct several field experiments with sensor devices to record the inter-connectivity of soccer players during a real game. They show that the wireless topology in the soccer field is in general sparse, with short encounters and power-law distributed inter-encounters. Coordinated movement of players gives significant correlations amongst links, which could be exploited by real-time routing algorithms.

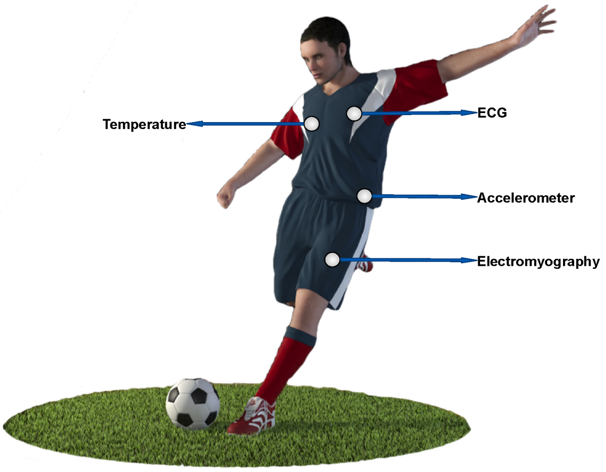
In this paper, we present a proposal that takes into account the mobility of the soccer players, the topology of the nodes in the WSN, which is given by the team formation system, and the a security system which is based on groups. As far as we know, all the works in the related literature published till today tackle the problem as there were only one soccer team, and our WSN proposal is designed to work using both teams simultaneously.

3 Proposed body sensors

This section focuses on the presentation of a body sensor network solution for data collection on the soccer team during a game. Taking into account the available technology, SHIMMER (Sensing Health with Intelligence Modularity, Mobility and Experimental Reusability) platform (Kuris and Dishongh, 2006) was chosen taking into account its easy interconnection among different sensors and uniform (real-time) data collection, storage, and processing (Burns et al., 2010). Shimmer is a wireless sensor platform designed by the Intel Digital Health Group and is used as the processor unit of the biosensor. The platform includes the following components: an 8 MHz Texas InstrumentsTM MSP430 CPU, a class 2 Bluetooth® radio communication, a 2.4 GHz IEEE 802.15.4 ChipconTM wireless transceiver (with ZigBee compatibility). A 3-Axis FreescaleTM accelerometer, a MicroSDTM slot for up to 2 Gbytes, an integrated Li-Ion battery management and some extension boards (internal and external) that increase the potential of SHIMMER platform with new features and functionalities. All these features are compacted in a very small form factor (2.0 × 4.5 cm) no larger to a thumb (Burns et al., 2010).

Illustration of the proposed BSN solution for biofeedback monitoring and corresponding sensors is presented in Figure 1. As it is shown, an accelerometer, an electrocardiogram (ECG), electromyography (EMG) and temperature sensors are considered. Accelerometer is used to measure the player movements and directions. This sensor may be tied at the waist. ECG is considered for cardiac rhythm monitoring and it is performed with the corresponded ECG leads connected to the platform and easily fixed with a chest strap. Temperature sensor can also be fixed on body using the same chest strap. EMG sensor measures and records data about all activity of the whole muscle. Depending on number of muscles to be monitored, different types of sensors (and platforms) should be considered. These sensors can be tied close to each monitored muscle over an arm/abdominal/thigh/leg strap.

Figure 1 Illustration of sensors placed on a football player, considering accelerometer, electrocardiogram (ECG), electromyography (EMG), and temperature sensors (see online version for colours)



The communication among wireless sensors and between sensors and the network infrastructure that allows data collection and monitoring in real time is performed through the standard IEEE 802.15.4 (Latré et al., 2011; Baronti et al., 2007). In this proposed solution, the above-mentioned ZigBee technology is used over IEEE 802.15.4. In SHIMMER, IEEE 802.15.4 ChipconTM wireless transceiver has a maximum data rate of 250 Kbps.

Even though the SHIMMER platform has most of the required features for our design, in terms of integrated sensors, it only includes an accelerometer. Then, in order to create the BSN depicted in Figure 1, we also include a temperature sensor, an ECG sensor, and an EMG sensor per SHIMMER platform. This SHIMMER platform collects raw data that is stored in a microSD card in real time. This feature offers the possibility of working in a stand-alone mode and collecting sensed data for a long period. After a game, all sensed measurements gathered in the SHIMMER's microSD card might be transferred to a computer for analysis, using a Bluetooth connection.

4 Energy harvesting system

New advances in energy harvesting have increased the efficiency gathering energy from the environment and its conversion to electrical power in order to run low-size and low-power devices and let them be self-sufficient. Moreover, power requirements of microcontrollers have been reduced considerably in last years. Furthermore, the way to acquire electrical power from different energy sources is increasing daily. Systems based on energy harvesting can be even more secure that those based on batteries (mainly because are not able to provide high amount of energy), but they are generally used to complement a primary energy source in order to increase the system reliability and lifetime. Currently, many systems are using multiple energy sources in order to increase amount of energy to be harvested. The most comment energy harvesting sources are:

- *Mechanic energy*: It is based on vibrations and on mechanic tensions.
- *Thermal energy*: It is based on the difference of temperature.
- *Photovoltaic energy*: It is taken from the sun or artificial light by using light sensors, photodiodes or solar panels.
- *Electromagnetic energy*: It comes from inductors, transformers, etc.
- *Wind energy*: It is obtained from the wind. Wind currents generate kinetic energy.
- *Hydropower*: It is the energy obtained by the force of a stream of water.
- *Human energy*: It is the combination of the mechanic and thermal energy that is generated from the human body through its actions such as walking, running, body heat, etc.

The amount of energy that can be harvested from the human body and its regular environment (compared with other sources) is given in Table 1 (Sáez and Loreto, 2009; Vullers et al., 2010). Our system proposal combines several energy sources. We have used Kinetic, Photovoltaic and Heat because they are the ones that harvest more energy.

Table 1 Typical values of harvested energy

Type of energy	*Energy source*	*Harvested energy*
Kinetic (using vibrations)	Human	4 μW/cm^2
	Industry	100 μW/cm^2
Photovoltaic (Light)	Indoor	10 μW/cm^2
	Outdoor	10 mW/cm^2
Heat (temperature difference)	Human	30 μW/cm^2

4.1 Kinetic

Commercial energy harvesting systems are able to collect up to 1 mW/cm^3 from walking (Romero et al., 2009a). They use a swing pendulum. However, also other systems harvest electrostatic energy from piezoelectric cells or flexible elastomers. Piezoelectricity is a property given in several types of crystal materials, such as natural crystals and manufactured ceramics. Crystalline structure produces a voltage that is proportional to the applied pressure. In the same manner, when a voltage is applied to the piezoelectric material, it is stretched or shrunk, in the direction of the applied voltage. Crystal materials are not deformed in this process. In Romero et al. (2009b), authors state that the power generated in kinetic energy harvesters is proportional to the proof mass, the acceleration squared, and the quality factor and inversely proportional to the driving frequency for a system where the driving frequency matches its resonant frequency. Then, larger ratios of acceleration-squared-to-frequency and larger Q factors are related to a higher available power. An explanation of a deployment, which uses the human motion to power wireless electronic devices is shown in Mitcheson et al. (2008). This paper shows human parts that provide more motion and therefore more energy are ankles and knees.

4.2 Photovoltaic

Photovoltaic energy sources are the most developed systems in the last years. Photovoltaic effect is directly related with the photoelectric effect, which consists on giving off electrons when a material is exposed to the light energy during a period of time. In the photovoltaic effect, a semiconductor is exposed to the light, which takes up the energy of the photons. This energy is used by the electrons to get out from their regular positions, and thus creating holes. These electrons form the current flow for the electric circuit. A photovoltaic cell forces the electrons and holes to move forward the opposite direction of the material, so it generates a voltage and a current between both parts, like in a battery.

Typically, around 1 mW can be harvested by each 1 cm^2 photovoltaic cell. There is a typical efficiency of 10%, and the capacity factor is between 15% and 20%. It has high performance until 25 years, then the generated power decreases. An example of a wireless sensor system that uses energy harvesting taken from indoor light using a photovoltaic cell is shown in Wang et al. (2009). We can also see a circuit development for a WBAN that uses solar energy harvesting in Tan et al. (2012). In our system, the energy is harvested using solar micropanels placed in the shirts tissue. Depending on the country, the soccer game may be played during the daylight or at the beginning of the night (where the light is obtained from the floodlights.

4.3 Thermal

Thermal energy produces electricity from the dissipated calorific energy. Thermal energy harvesting is based on Seebeck's theory (Luste and Anatychuk, 2005). Seebeck's effect states that when there is a temperature difference across two dissimilar materials, an electric voltage is generated. It is used as the energy converter to transform the thermal energy into electrical energy. In our design, thermoelectric generator is fabricated using aluminium and Teflon. Aluminium is used to act as the hot plate designed with a small surface area in order to collect heat fast and cold plate designed in a shape to act as a good heat diffuser. Teflon is used as the insulator sandwiched between the hot and the cold plate so as to effectively reduce the convection and radiation of heat from the hot plate and the cold plate, preventing it from warming up which is highly undesirable as it reduces the thermal gradient between the plates thus affecting the heat flow and power output.

We can see several real values obtained for people running and walking in Hoang et al. (2009). In this paper, it is also shown that it depends on the weight of the people.

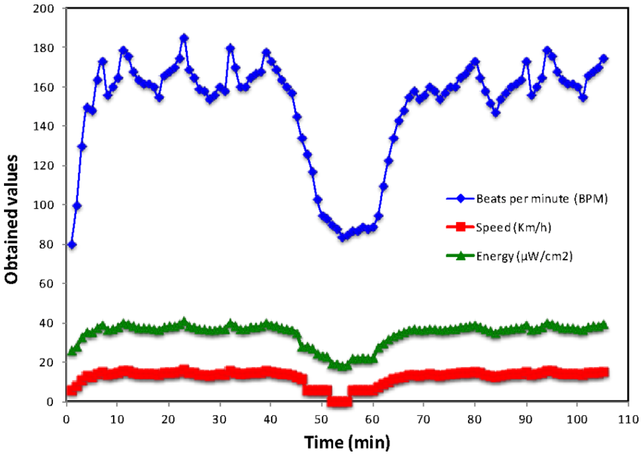
Last researchers in this in thermal energy harvesting are focused on producing energy from the difference between the environmental and the body temperature. We can see that more energy will be obtained in countries where the soccer game is played in winter, because the environmental temperature will be quite lower.

4.4 Energy harvesting in a soccer match

In this subsection, we are going to calculate the average harvested energy produced by a soccer player when previously presented energy harvesting system is being used. In order to evaluate this parameter, firstly we have studied the behaviour of a player. Following the study presented in University of Texas (2000), developed by some researchers of the University of Texas, we can know if a soccer player is walking, running or sprinting and we are able predict how much time each player is doing each one of these activities. Every data presented in University of Texas (2000) is related with the mean heart rate of a player. When a player is doing some activity stronger than another, their heart rate increases and when he is doing a more relaxed activity (for example walking in a soccer match) his beats per minute (BPM) decreases.

To carry on this study we have monitored several soccer players in a soccer match. Then, we estimated the average BPM of a player in each minute. We have accepted that soccer player behaviour is not constant and depends on its movement in each moment. This effect can be shown in Figure 2. The blue line is the average BPM for a soccer player. There are several peaks, which could be produced by two situations: when the soccer player attacks or defends. Moreover, we can see that heart rate decreases at 45 min down to 60 BPM. This happens because in this period there is a break in the soccer match. Following the relations shown in University of Texas (2000), we can calculate the average speed of a player. It is represented in red in our Figure 2. This graph is quite constant because we have estimated the mean of the speed in order to know the average harvested energy in a soccer match. It is represented in Figure 2 with the green line. We have estimated the harvested energy using typical values (Table 1). The harvested energy is directly proportional to the speed and light inside soccer stadium. Our system takes energy from the kinetic energy, which is directly related to the speed of a player. It will produce less energy when this player is walking. On the other hand, the gathered photovoltaic energy will be less when players go inside the locker room, because a stadium has a good illumination in field.

Figure 2 Energy harvesting produced by a soccer player (see online version for colours)



Finally, the energy produced by the thermal change of a soccer player is associated to the heart rate. Generally, when a soccer player has a high heart rate it means that he has run, which produces a heat rising in his body. These relations could be seen in the graph of the energy harvested shown in Figure 2.

5 System architecture

Our goal is to get biometrical, physiological, or in a broader sense, general health data from soccer players during a match, or a workout, in order to know which the physical state of each one is during the entire match. It will allow the soccer coach to see if a soccer player is tired, and lets the coach to monitor remotely each player. To achieve our goal, each player has a wireless body sensor and each player will act as a sensor node in the WSN. How the data are taken from the body and the way used to gather, them are described in the previous section.

It is important for the athletes that both the sensing and the transmission system should be non-intrusive and light-weighted because in high-level sport competitions every simple detail can make a big difference. This requirement leads us to use low power radio devices that implies low transmission range.

In our approach, every single player on the field is a WBAN that can generate data to transmit or relay data from other nodes in the WSN. To provide communication between WSN nodes we have decided to use ZigBee.

ZigBee uses the standard IEEE 802.15.4 physical and Medium Access Control (MAC) layers to provide a robust and reliable wireless data transfer. It adds network structure, routing, and security to complete the communications suite. ZigBee defines the upper layers of the protocol stack, providing target applications with the interoperability and intercompatibility required to allow similar products from different manufacturers to work seamless.

To provide reliable data delivery, ZigBee uses 27 channels in three separate frequency bands through several mechanisms at multiple layers. The 2.4 GHz band has 16 channels and a maximum over-the-air data rate of 250 Kbps. Lower frequency bands are different in several world zone regions. America and much of the Pacific Rim use the 902–928 MHz band, with 10 channels and a burst rate of 40 Kbps. Europe applications use one channel in the 868–870 MHz band, which provides 20 Kbps burst rate.

To ensure reliable data transmission on a specific channel, the 802.15.4 radio relies on a number of mechanisms. First, the PHY layer uses binary phase shift keying (BPSK) in the 868/915 MHz bands and offset quadrature phase shift keying (O-QPSK) at 2.4 GHz. The information is coded onto the carrier with direct sequence spread spectrum (DSSS). The size of the data payload ranges from 0 to 104 bytes, more than enough to meet body sensors needs. The information is sent performing a 16-bit cyclic redundancy check (CRC), which will be used by the receiver to verify if the packet was corrupted in transmission. The receiver automatically transmits an acknowledgement packet when the received packet has a good CRC. If the CRC indicates the packet was corrupt, then the packet is dropped and no acknowledgement is transmitted.

The Medium Access Control used in our system proposal has been slotted CSMA/CA (Ha et al., 2007). Slotted CSMA/CA algorithm is implemented using units of time called back-off periods. Each time a device wishes to transmit data or command frames during the Contention Access Period (CAP), it locates the boundary of the next back-off period. Each device maintains three variables for CSMA/CA algorithm for each transmission attempt: NB, CW and BE (Fruth, 2006).

- NB is the number of back-off periods used by the CSMA/CA algorithm while attempting the current transmission. It is initialised to 0 before each new transmission. If the channel is assessed to be busy the

MAC layer increments NB by one. When NB reaches a maximum value, it declares channel access failure.

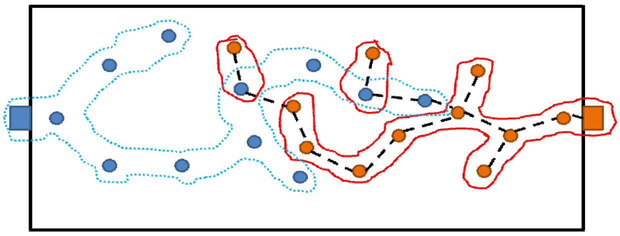
- BE is the back-off exponent. It is related to the number of back-off periods a device shall wait before attempting to assess the channel. BE are initialised and the boundary of the next back-off period is located. Before a station attempts to send a frame, it waits for a random integer number between 0 and 2BE-1 complete back-off periods, then requests the PHY to perform a clear channel assessment (CCA). If the channel is assessed to be busy the MAC layer increments NE by one.
- CW is the contention window length. It defines the number of back-off periods needed to be clear of activity before starting the transmission. It is initialised to 2 before each transmission attempt and reset to 2 each time the channel is assessed to be busy. If the channel is assessed to be idle, then the MAC sublayer ensures the CW is expired before starting transmission. For this, CW is decremented by one first. If CW is not equal to 0, CCA is performed on back-off boundary. Otherwise, it starts transmission on the boundary of the next back-off period.

From the network layer point of view, the most appropriate route is always a route where the nodes are from the same team. If all the nodes within the path are from the same team, a weak encryption is needed, but, otherwise, if there are nodes from different teams, a hard encryption is needed when the data goes through a node from a different team. Thus, every node (player) is a next-hop candidate, and both teams use the same infrastructure in order to receive data from their players.

The information can be routed through any node, but the data must not be merged and any information transmitted to the network belongs to the source node's team and must only be understood by that team. The way that data are encrypted is explained in next section.

The proposed architecture is based on inter-WBAN data communication, where each WBAN is placed in each player. Hence, we have mobility in the WBAN sensors and between WBANs, which are grouped in two groups. The sensed data will be routed from a mobile source node to a fixed sink located outside the game field. There is no preferred place to fix these sink nodes, although we have placed them behind the goals. The rationale behind this choice is that some team players are likely close to one of the goals most of the time (at least the goal keepers), so they will be under the coverage area of the sink nodes. Figure 3 shows a network with 22 WBANs in a moment of the game, 11 WBANs (in blue) belong to one team and the other 11 ones (in orange) belong to the other team. Each WBAN is represented by a circle and the sink node by a square. We can see which the path is in a specific moment for the orange team. We can also see how two nodes of one team (orange team) send information through the nodes of the blue team in order to reach its sink node.

Figure 3 WSN example with 2 teams (see online version for colours)



The soccer player's formation and the way each player moves on the field determine the effectiveness of the whole system. Hence, it is important the use of an accurate topology and mobility model. WE have used the soccer game features in order to model our system more accurately.

The size of the field can vary from 100 m to 110 m long and from 64 m to 75 m wide (it depends on the country and the world zone). There are two teams with 11 players. Their formation and the number of players in each line depend on the strategy of the coach. Some formation is better when the coach pretends to attack during the game and others are better to have a defensive structure. Every location is known as a position. Positions are grouped by lines. These lines are named as: goalkeeper, defenders, midfielders and forwards. Except goalkeeper line that is formed by a single player, the rest can be formed by a number of players that can vary between matches or during a single match due to tactical variations. From our research perspective, this formation will determine the topology of our WSN. Figure 4 shows the most common team formations, which will be our base WSN topology. They are named 1-4-4-2 rhombus, 1-4-4-2 line, 1-4-4-2 square, 1-4-3-3, 1-4-2-4 and 1-3-5-2 formation, respectively. There are others such as 1-5-3-2 and 1-3-3-4 which are not so shown. These topologies provide us the most probably location where each node will be placed and we can also can estimate the area where they will most probably be moving during the match. The zone range of each player and the probability of finding the player are discussed later in the next section.

The first issue we should address is the radio coverage of the player to connect with other players. The most common model used to estimate the radio coverage of a node is the disk model, which assumes that the radio region is a circular area centred on it. Any node placed closer than the radio coverage d will be a neighbour. d is determined by the transmitter and receiver power and the antenna gains.

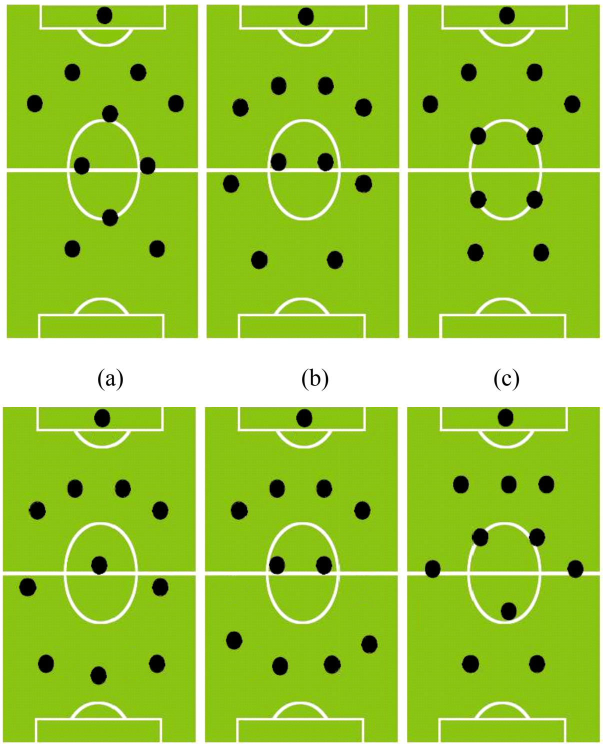
When the node only covers an area (not the whole circle), because of the type of antenna or because a part is hidden by the body of the soccer, the receiver must be located inside the angle of the transmitter's coverage area. The area inside a partial circle bounded by a radius r and an arc α is provided by equation (1).

$$\text{Area} = 0.5 \cdot d^2 \cdot \left(\pi \cdot \alpha / 180 \cdot sin\alpha\right) \tag{1}$$

where *d* is the circle radius and α is the angle (in degrees). Figure 5 shows the partial circle area covered by a soccer player.

To know the percentage of the football field that is covered by the players when they are playing, we will use a football field with a size of 110×70 m^2. Let us suppose that the wireless sensor node has a sectorial antenna and its angle is 180º. If there is no overlapping area between the 22 players, then we can see in Figure 6 the percentage of covered football field depending on the distance from the soccer.

Figure 4 Possible WSN topologies: (a) 1-4-4-2 rhombus; (b) 1-4-4-2 line; (c) 1-4-4-2 square; (d) 1-4-3-3; (e) 1-4-2-4 and (f) 1-3-5-2 (see online version for colours)



(a) (b) (c)

(d) (e) (f)

Figure 5 Radio coverage of each player

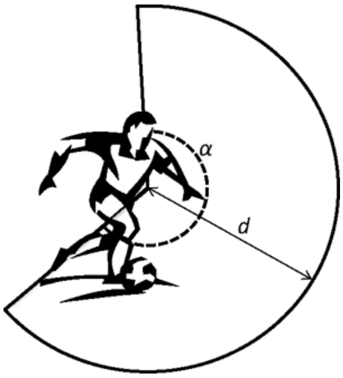
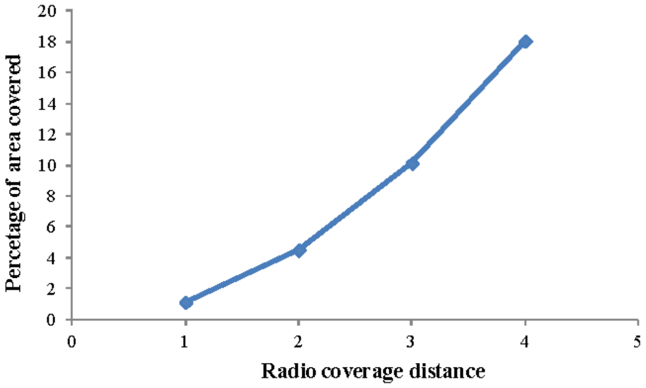


Figure 6 Percentage of area covered as a function of the radio coverage distance of the soccer (see online version for colours)



6 System security

To provide security to our system, we should add data encryption and user authentication for privacy. This section describes our security proposal to provide both features in our system.

First, because of the dynamic nature of the ad hoc network, the keys in the groups must be distributed efficiently without the need of a group manager or a trusted third party (Noack and Spitz, 2009). To achieve this goal, we have chosen a hybrid solution based on asymmetric and symmetric cryptography. Each team has a pair of team keys (a public team key and a private team key), which is shared by all players of the same team. It must not be ever discovered by the other team, and a shared game key that is the same for both teams, which will enhance the security level to prevent intruders from outside of the game. For the pair of team keys, we use asymmetric encryption, while for the game key we use symmetric encryption.

The shared game key is shared before starting the game and any message sent to the network uses the shared secret game key in any communication during the game. Given M, the message with the sensed information, and K, a shared game key, we use AES-256 (Federal Information Processing Standards Publication 197, 2001) in order to encrypt the message sent from one player to another. Equation (2) provides the cipher C.

$$C = AES - 256(M,\ K.) \tag{2}$$

Thus, the receiver will obtain the message by using the inverse cipher as it is shown in

$$M = C^{-1}\left(\text{AES} - 256(M,\ K),\ K'\right) \tag{3}$$

where *K′* is the inverse shared game key.

But the message M is encrypted using the public key infrastructure if the message is sent to a node which does not belong to the same team to the source node. That is, only when the message goes through the nodes belonging to the same team of the source node, will remain the message unencrypted. But when the message is sent to a node of the other team, first, this message is encrypted using its private key and only when it arrives to a node that belongs to the same team, will be able to decrypt and forward to the nodes of its team. To do that, each node stores the public keys of the rest of the nodes in its team, so it is able to decrypt any message sent by a node of its team. So, before starting the game, e.g., in the soccer team's dressing room, each player generates its pair keys (priK, pubK), its private and public keys, and sends its public keys with the others members of the team jointly with the modular value of two large primes at random (n). Equation (4) shows what is kept and published of the private and public key.

$$\begin{cases} \text{Keeping secret private encryption key} = \{priK, n\} \\ \text{Publishing their public decryption key} = \{pubK, n\} \end{cases}. \quad (4)$$

Thus, the sensed data of the player (plaindata) is encrypted (M) by the source following:

$$M = (\text{plaindata})^{privK} \bmod n. \quad (5)$$

The receiver belonging to the same team will be able to decrypt the data knowing the source node and taking its public key. It is shown in

$$\text{plaindata} = M^{pubK} \bmod n. \quad (6)$$

We have studied the energy consumption of asymmetric and symmetric encryption algorithms in low power consumption devices. Thus, the energy and computational costs due to security issues are detailed in depth in Lacuesta et al. (2011). Bearing in mind that study, we can state that the combination of both systems is optimal to provide high security while having low power consumption.

To provide authentication in our system, every time a new player joins the game, it has to authenticate with the first player of his team he finds. In the authentication process, the new player sends the shared game key encrypted with his private key. Only the players of the same team will be able to decrypt it (because all players have stored the public keys of its team players, as we have aforementioned) with the new player's public key and he will be able to check if they have the same shared game key. If they have the same key the new player is authenticated and will be able to join the wireless network. Now every time a node sends information to the sink node, it follows the aforementioned security procedure and routes it to the appropriate sink node (to its sink node if it is from a player of its team or to the sink node of the contrary if it is from a player of the other team).

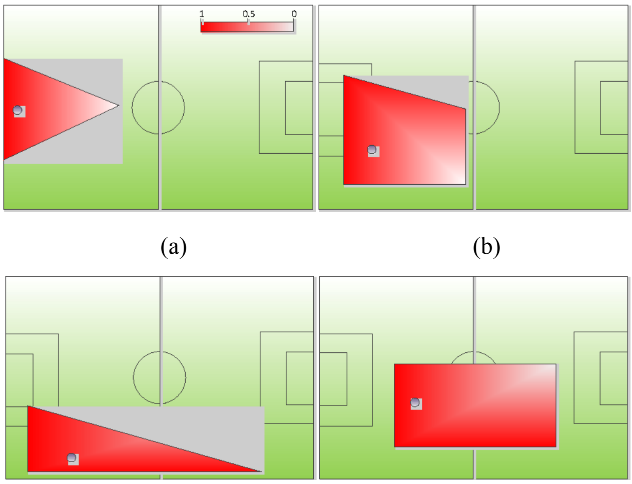
7 Mobility model

In this section, we are going to explain the mobility model of our proposal. It has been divided in three parts. The first one explains the zone model, which is the zone in which each player is moving, the second one explains the group mobility model, which let us know that players try to move behind the ball, and the third one which explains the routing protocol used in our proposal.

7.1 Zone model

We define a probabilistic model for the players' position formation and their motion. In steady state, at the beginning or after a defensive withdrawal, the players draw the team topology on the field (Figure 4). On the basis of the initial position of 1-4-4-2 square, we have plotted the most probable zone where every player will be more time during a match (Figure 7). Every player will move on the field inside an area that will depend on his position. The likely movement of the goalkeeper is represented in Figure 7(a). We can see that near the goal, the goalkeeper spends more time than around of the centre, this player will be near of the centre when his team is near than the opposite goal. Moreover, he will be very few times at the side of the soccer goal, only when the contrary comes from that side. Central defenders will be more time near their goal than in the midfield, because of their condition, but they cover more area (Figure 7(b)). On the other hand, a midfielder spend more time in the midfield (Figure 7(d)), this is because the function of these players. These players distribute the game, and they are the liaison between the defenders and forwards. Players on the side of the field spend most of the time in their side. In this case, there is a clear difference between defensive players and offensive players. In defensive players, the probability of being close to their goal is increased compared with offensive players (Figure 7(c) and (e)). Finally, forwards will be more time near the opponent's goal than elsewhere, if they are offensive players (Figure 7(f)). This is because they should score a goal for their team, in order to win the match.

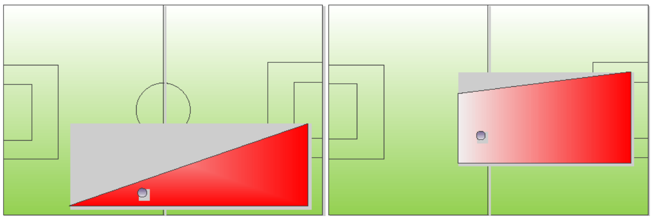
Figure 7 High probabilistic position on 1-4-4-2 square: (a) goalkeeper's high probabilistic position; (b) central defender's high probabilistic position; (c) right defender's high probabilistic position; (d) midfield's high probabilistic position; (e) right side's high probabilistic position and (f) forward's high probabilistic position (see online version for colours)



(a) (b)

(c) (d)

Figure 7 High probabilistic position on 1-4-4-2 square: (a) goalkeeper's high probabilistic position; (b) central defender's high probabilistic position; (c) right defender's high probabilistic position; (d) midfield's high probabilistic position; (e) right side's high probabilistic position and (f) forward's high probabilistic position (see online version for colours) (continued)



(e) (f)

For each player, we define a two dimension probability density function (PDF) which depends in the player's position. We will call this function 'the locator'. Given a couple of coordinates x and y, a position locator returns the probability of finding the player associated to the position in a specific moment of the game. Equation (7) shows the PDF function.

$$P\left[a \le X \le b, c \le Y \le d\right] = \iint f_{x,y}\left(x,y\right)\mathrm{d}x\mathrm{d}y. \qquad (7)$$

A default locator's library is created, and every entry in the library will be assigned to a position. New positions will be added to the library as needed, and we can add more than one entry for a given position.

7.2 Group mobility model

Our group mobility model is based on Persecution Mobility Model (Camp et al., 2002). It shows players tracking a ball. The target can have its own individual mobility model, but in our case, it acts as a gravity centre for each player, but they keep moving in their zone.

In both cases, a team is attacking or defending, the players will pursue the ball working in a collaborative manner. We can distinguish two types of players in each team, the attackers and the defenders. When a team is defending, the players usually keep in their zone and pursue the ball. However, when a defender takes the ball, usually the attackers run to the opposite goal in order to find clear zones and increase the probability of making a goal, so these players do not pursue the ball in that cases, only the one that has it. Thus, we can consider two types of groups which behaviour will be different depending on the case (if they are attacking or defending).

Our model uses update location formula for each player, which depends on the position of the ball. Using a persecution model, the new position can be obtained from the previous ones as it is shown in equation (8).

$$p_l = p_{ol} + acceleration\left(b_l - b_{ol}\right) + random\_vector \qquad (8)$$

where p_l is the player new location, p_{ol} is the player old location, b_l is the ball new location, b_{ol} is the ball old location, $acceleration(b_l - b_{ol})$ is needed to follow the movements of the ball, and, finally, *random_vector* is calculated from an individual player mobility model.

Our proposal adds the estimation of the *random_vector* out of the locator from our zone model, because in real soccer games, the movements of the players are ball position dependent combined with the player position in the team topology. The ball may have its own mobility model, independent of the rest of the players (e.g., random walk), or a model influenced by attack structures. Its model affects to the mobility model of the players.

Now, we add a gravitational model to our system. The closer is a player to a ball, the more attracted will be by it. This addition let us model the action of a defending player over an attacker that is driving the ball. The acceleration vector used in our model follows the regular gravity model, which depends on the inverse of the square of the distance between two nodes. Equation 9 shows the acceleration vector.

$$\overrightarrow{a_{x,y}} = \frac{G}{\left(b_l - p_l, b_{ol} - p_{ol}\right)^2}(x,y) \qquad (9)$$

where, G is a constant that depends on the state of the players (if they are tired or not), their animation, liveliness and energy. G must be adjusted empirically in order to provide accurate movements.

7.3 Zigbee routing

To provide routing in the WSN formed by the soccer players, we used the ZigBee Routing Protocol, which is defined in the standard (Cuomo et al., 2007). It is based on algorithm is based on the notion of 'Distance Vector' (DV) routing, concretely it uses a modified AODV (Ad hoc On Demand distance Vector) routing protocol (Perkins et al., 2003).

It is a reactive routing protocol by default and Hierarchical Tree Routing protocol as last resort. Reactive protocols establish paths only upon request (e.g., when there is an event, in response to a query, etc.); meanwhile, sensors remain idle in terms of routing behaviour. It makes this protocol ideal when nodes have frequent mobility. Nodes forward each routing request to peers until it arrives at a sink. In Nefzi and Q. (2007), there is a performance analysis of ZigBee Routing Protocol. It shows that Hierarchical Tree Routing provides shorter average end-to-end delay but performs poorly in terms of energy consumption. Therefore, in our case, for supporting real time communication, it is desirable to choose Hierarchical Tree Routing. We can see proposed in the related literature some enhancements on the hierarchical tree routing protocol used in ZigBee (Ha et al., 2007). Moreover, some researchers have been working on providing enhancements to ZigBee in order to improve the scalability issues (Lee et al., 2007), but our proposal lacks of scalability problems.

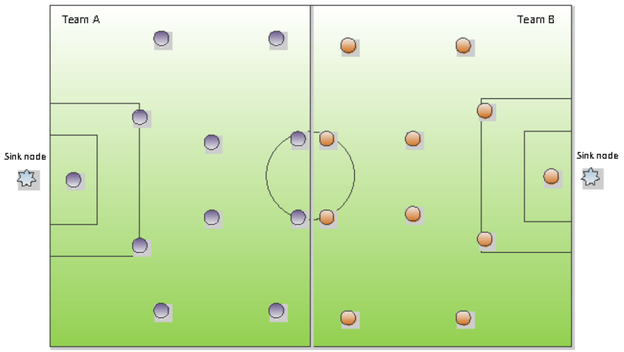
8 Simulations

In this section, we present the simulations performed in our proposed system.

8.1 Test bench

The simulations presented below were performed using the OPNET simulator (Riverbed, 2014). We have created an environment with the characteristics of a football field. The football field has a size of 110×70 m^2. Players of each team are placed in the initial position shown in Figure 8. From this initial topology, we have made three simulations, one when players are not moving (NM), this case has been added for comparison purposes, another one when the players have low mobility (LM), and, finally, a simulation where players have high mobility (HM).

Figure 8 Test bench topology (see online version for colours)



In our simulations, we have located two sinks, one behind each goal. We thought that it is the best situation, because the goalkeeper can always serve as a liaison between the players and the sink. The information comes from sensors located at players, besides they send information to the sink. The sink will collect this information, which will send it by using another wireless or wired technology to the team bench in order to let the coach and the trainers know how the physiological state of the players is. It will allow them to have updated information about the players in the field.

In our simulation, nodes communicate using Zigbee in the 915 MHz frequency band. The traffic injected into the WSN follows an exponential distribution with an average packet size of 1024 bits and an inter-arrival time of 10 seconds. We believe that to use an average of 10 seconds is appropriate because there is no need of monitoring these events with higher accuracy.

8.2 Load of each team

In Figures 9 and 10, we can see the instantaneous load of the network per team. Figure 9 shows the instantaneous load of the A team. In this figure, we can see that the behaviour of the traffic is quite variable. There is greater variability of the load when we have a topology with a high mobility. This variability decreases when our topologies have less mobility. On the other hand, Figure 10 shows the same parameter of Figure 8, but in this case, it is from B team. Figure 9 is different of Figure 10 due to the movement of the players. In this second case, when the players have a high mobility, the load of the network is around 26 Kbps, this load increases until 50 Kbps when the mobility is low, and, finally, the load is 58 Kbps when the players are static. Thus, we observed that there is higher load in the network when the mobility is lower.

Figure 9 Load (bits/sec) of the team A (see online version for colours)

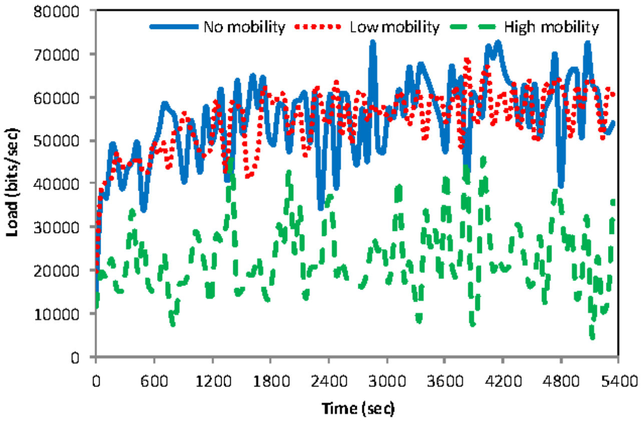


Figure 10 Load (bits/sec) of the team B (see online version for colours)

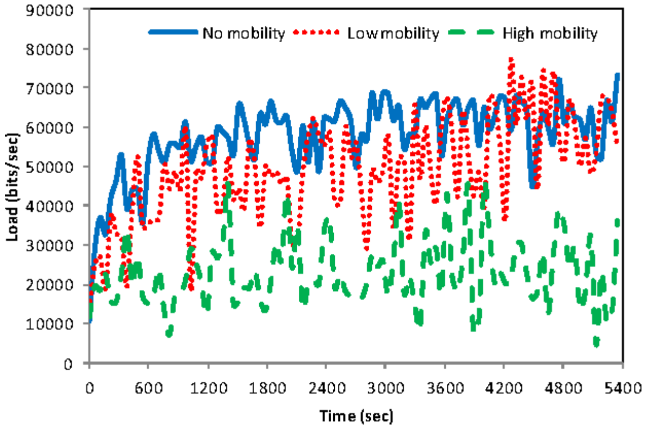
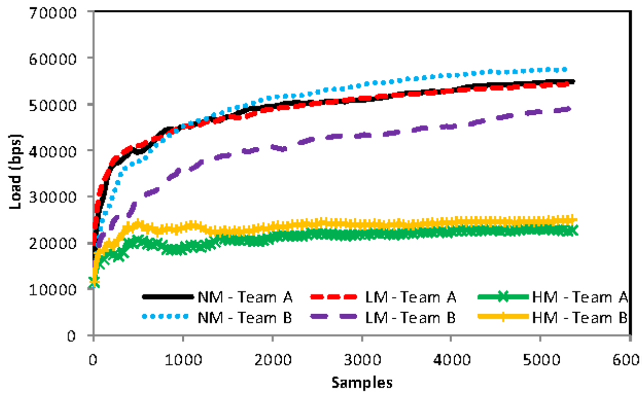


Figure 11 shows the average network load of each team on the MAC layer. When analysing team A, the load is very similar for NM and LM cases, ~53 Kbps when the network converges. Nevertheless, on team B, NM and LM cases have a difference of 10 Kbps. NM case has a load of 56 Kbps and 46 Kbps on LM case. This is due to the movements of the nodes from the initial stage to the convergence of the network proximity of sensor nodes to a sink node is different if a team attacks and the other one defends. However, when the topologies have a high mobility (HM – Team A and HM – Team B) this difference is small, and the load of each team is around 20 Kbps.

Figure 11 Average load of 2 teams on IEEE 802.14.5 MAC layer (see online version for colours)



According to these figures, we can say that our proposal works better when the topology has high mobility because the network load is lower. This happens because our proposal is designed to work in high mobility scenarios. Our system is focused on downloading the information of a player when a node is near to a sink. Therefore, if the players have high mobility, our system will download data to the sinks constantly, which means that our network has less data on the network and therefore less load. Thus, if the soccer game is active, sensor nodes will have less energy consumption, because they will transmit fewer frames.

8.3 Control and management traffic

In this subsection, we are going to analyse control and management traffic introduced on IEEE 802.14.5 MAC layer in our system when football players are in action using several mobility models.

Figure 12 shows the average control traffic received (in bps) received by all network nodes on IEEE 802.14.5 MAC layer, sent from the sink nodes, in the three cases. We can observe that the NM case introduces more control traffic (280 bps when the network converges, which is around 1000 samples) than any other case. Using the presented mobility model this traffic decreases when the mobility of nodes decreases, we have 120 bps in the LM case and 40 bps in the HM case. It is due to the facility of finding a node to transmit information when their mobility is high.

Figure 12 Average control traffic received on IEEE 802.14.5 MAC layer (see online version for colours)

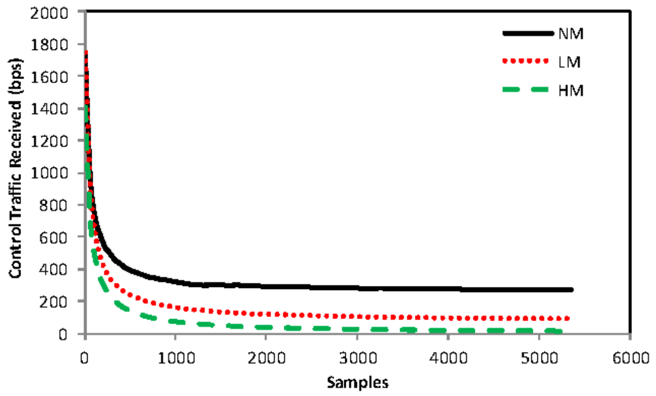
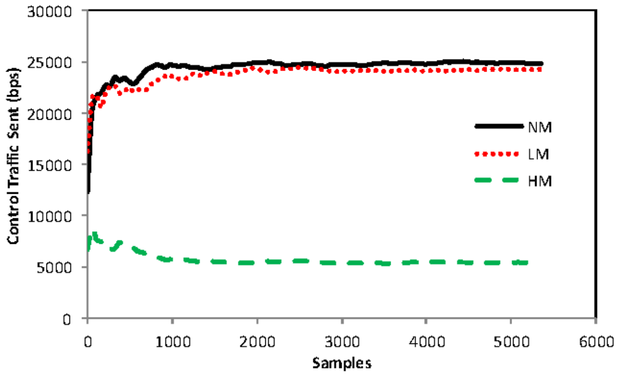


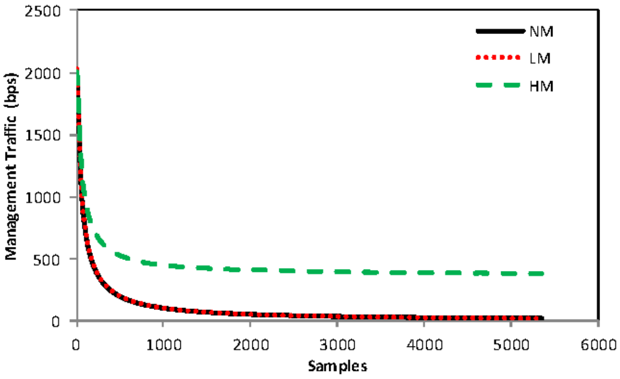
Figure 13 shows the average control traffic (bps) sent from sensor nodes to the sink nodes on IEEE 802.14.5 MAC layer. In this case, we see that the amount of control traffic is higher. This happens because the nodes placed on the soccer field have to send more control traffic to meet neighbours and nearby sink nodes. As it happened in Figure 12, the NM case introduces more traffic (close to the 25 Kbps). This traffic decreased slightly (about 24 Kbps) in the LM case, but the big difference comes in the HM case. In this simulation case, the control traffic drops to 5.6 Kbps when the network converges.

Figure 13 Average control traffic sent on IEEE 802.14.5 MAC layer (see online version for colours)



In Figure 14, the average management traffic on the MAC layer is represented. Here, we can see that NM and LM cases follow similar patterns. In these two cases, the management traffic is high at the first samples, but then, it is very small (53 bps) when network converges, this is due to the low mobility of the nodes. However, when sensor nodes have a high mobility, this traffic increases up to 500 bps. This amount of traffic is small, but it is enough to manage the network nodes when they have high mobility. In the initial stages of all cases greater control is required because the network is discovered, so the management traffic increases.

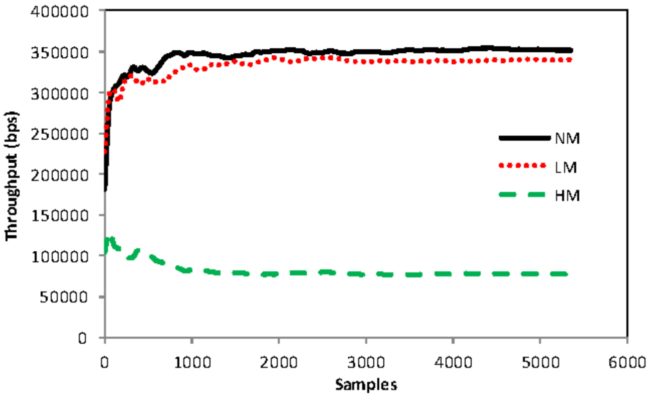
Figure 14 Average management traffic on IEEE 802.14.5 MAC layer (see online version for colours)



8.4 Throughput of the network

Figure 15 shows the throughput of the network. Throughput or network throughput is the rate of successful message delivery over a communication channel. The highest throughput is introduced in the NM case. It introduces ~350 Kbps when the network converges.

Figure 15 Average throughput on IEEE 802.14.5 MAC layer (see online version for colours)



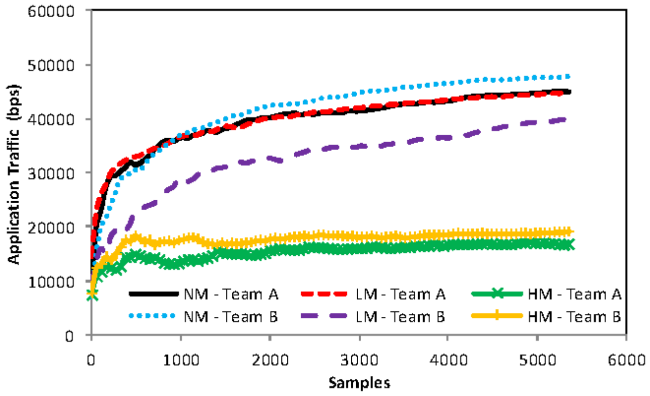
However, when mobility is low (LM) this throughput decreases 20 Kbps (compared with the NM case). However, the biggest change occurs when nodes have a higher mobility. In this case the throughput is increased around 100 Kbps. This result was expected according to the behaviour of previous figures.

8.5 *Application traffic*

In this subsection, we are going to focus in data sent by our system. This information will be all parameters collected by body sensors used in every football player.

In Figure 16, we show the application-level traffic handled by each team in the simulated cases. The graph shows that all cases present similar behaviour of Figure 9, but with a smaller number of bits. In this case, we are talking about traffic at the application level and Figure 12 shows the MAC level traffic. The worst cases have been NM for both teams and the A team LM case.

Figure 16 Average application traffic (see online version for colours)



8.6 *Hops needed in each team*

In Figures 17 and 18, we analyse the probability dense function of the average number of hops needed by teams A and B. Figure 17 shows the probability for the A team. In this case, the probability of needing four hops to reach the sink is 0.7 when there is low mobility, but this probability decreases when there is higher mobility. That is, with higher mobility this probability increases according to the number of hops, so it is more probable to need more hops to reach the sink. It happens because the network is changing continuously. Thus, it is more difficult to find a good path to arrive to the destination. In the high mobility of the A team the most probable will be 16 hops per route.

Figure 17 Probability density function of the No. of hops (team A) (see online version for colours)

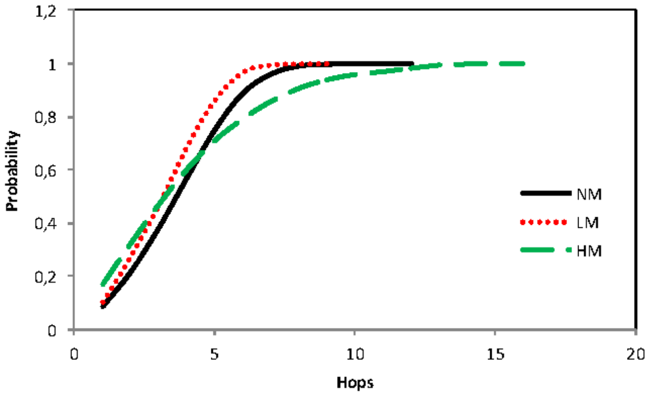
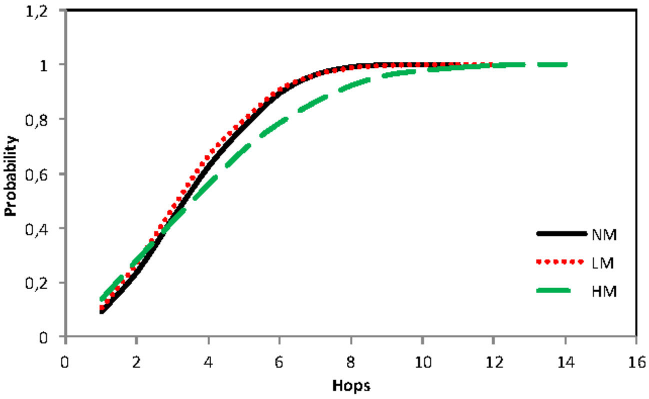


Figure 18 Probability density function of the No. of hops (team B) (see online version for colours)

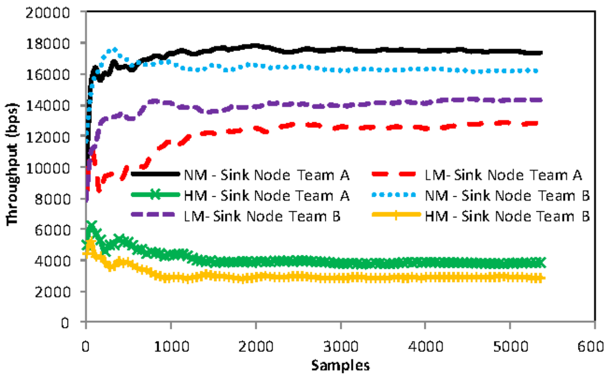


The same behaviour occurs with the B team (see Figure 18). In this case, the static and the low mobility case have a similar behaviour. In both cases it is most probable to need more than nine hops to arrive to the sink. When the network has high mobility, it is most probable to have between 11 and 14 hops per route. According to this behaviour, we can say that our proposed system is feasible and performs well even when there is high mobility. However, it needs more hops to reach the sink node when there is high mobility.

8.7 *Throughput in every sink node*

Figure 19 shows the throughput at every sink node for the simulated cases. ML cases of both teams are the ones that introduce most throughputs. The sink located on the B team area has 16 Kbps of throughput, and the sink node of the A team area has 17.5 Kbps. When nodes have a higher mobility the throughput decreases to 14 Kbps in the sink node located in the B team area and to 12.5 Kbps in the A team area. Finally, the lowest throughput is obtained when there is high mobility (the throughput is around 3 and 4 Kbps). These small differences between the sink nodes located in different areas occur because one team is performing more attacks, while the other team is defending more time.

Figure 19 Average throughput on IEEE 802.14.5 MAC layer per each sink node (see online version for colours)

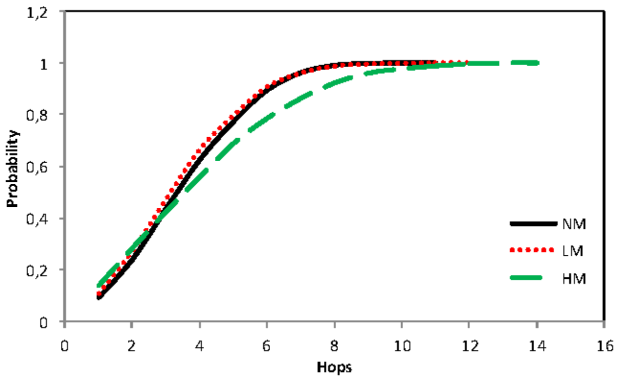


8.8 *Control traffic in every sink node*

In this case, we analyse the control traffic processed by every node in our network.

In Figure 20, we observe the data related to traffic control on the sink nodes for the simulated cases. When there is no mobility, the control traffic is between 1.25 Kbps and 1.35 Kbps. This traffic decreases with the mobility and it is between 1 Kbps and 0.95 Kbps for LM cases. In the case where the nodes have high mobility, the control traffic is around 0.2 Kbps and 0.3 Kbps. As it happened in Figure 12, when the nodes have less mobility, there is greater amount of control traffic.

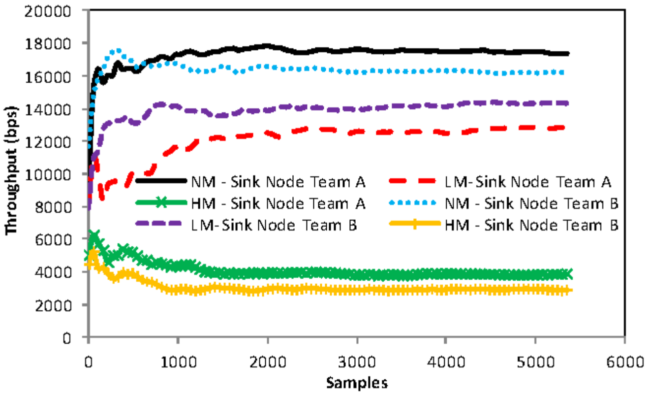
Figure 20 Probability density function of the No. of hops (team B) (see online version for colours)



8.9 *Application traffic in every sink node*

Finally, the application layer traffic in every node is analysed too. Figure 21 shows the application-level traffic processed by each sink node in the simulated cases. It shows that the traffic pattern is very similar for all cases, but the number of bits is smaller according to the nodes' mobility. The sink nodes perceive an application traffic around 4 Kbps in the LM case. This traffic flow decreases when nodes have low mobility. However, when the nodes have a high mobility, the application traffic decreases over than 57%, being 1.4 Kbps on the sink node located at the B team area.

Figure 21 Average throughput on IEEE 802.14.5 MAC layer per each sink node (see online version for colours)



9 Sport monitoring systems comparison

This section compares our proposal with other systems used for monitoring sport activities. Javier Vales-Alonso et al. propose a system in Vales-Alonso et al. (2010), which takes data from the athletes in several sink points. Their architecture is based on WSNs, but the communication is directly performed between sensor nodes and sinks. In Le Sage et al. (2010), they propose a real-time system for monitoring of swimming performance, which uses WiFi technology. Llosa et al. (2009) shows a sensor network-based application that provides a detailed picture of a boat movement, individual rower performance, or his or her performance compared with other crewmembers. Finally, Zulkifli et al. (2012) presents a wireless sensor node to send the heart rate through the WSN using ZigBee technology.

Table 2 shows the comparison of our proposal with other sport monitoring systems. Our proposal stands out because each player has a body sensor network that uses energy harvesting and each player will be a wireless sensor node in the WSN. Information could be routed through any player by using a secure mechanism.

Table 2 Comparison between several sports' monitoring systems

	Vales-Alonso et al. (2010)	*Le Sage et al. (2010)*	*Llosa et al. (2009)*	*Zulkifli et al. (2012)*	*Our proposal*
Team's sport oriented	No	No	Yes	Yes	Yes
Using of WSN (technology)	Yes (ZigBee)	Yes (Wi-Fi)	Yes (ZigBee)	Yes (ZigBee)	Yes (ZigBee)
Energy harvesting	No	No	No	No	Yes
Security included	In future works	No	No	No	Yes
Using other nodes (no sinks) to send information	No	No	No	No	Yes
Monitoring based on …	Heart rate and laps	Laps	Velocity, acceleration and location	Heart rate	Heart rate, acceleration, temperature and EMC

10 Conclusions

In this paper, we have presented a new way to transmit the information gathered from the wireless body sensors placed in the football players. The information can be routed though the nodes of the same team or through the nodes of the other team, but the information can be only decrypted by players (and the coach) of the same team. The radio coverage area of each soccer player is no longer than 4 m in order to avoid eavesdropping from any place of the stands.

We have proposed an energy harvesting system that is able to provide enough energy for that very low transmission range.

A soccer match is 90 min long and the players could move more or less depending on the dynamic of the soccer game (fast or slow) and on the place where the ball have been rolling (which affects more to some users than to others). In order to study the performance of our proposal, we have simulated the load in each team, the control and management traffic, the throughput of the network, the application traffic, the number of hops needed in each team, and the throughput, control traffic and application traffic in every sink node. Our simulations show that the network load is lower when the players have high mobility, but it needs more hops when there is high mobility. In both situations, low mobility and high mobility, the management traffic is low, and in all cases below 250 Kbps, which is the maximum transmission data rate of the SHIMMER IEEE 802.15.4 ChipconTM wireless transceiver. Finally, we have compared our proposal with other systems and we have shown that our system has more and better features than others.

Although the system has been developed to inform the coach the physiological state of the players, we must highlight that the security system allows implementing a receiver in each player to let him know the physiological state of his partners, and, hence, plan an attack or not.

We are now developing the devices in order to measure our proposal in a real soccer game. In future works, we will add intelligent localisation systems in order to improve the accuracy of our proposal (Lu and Demirbas, 2011; Gui et al., 2011).

Acknowledgements

This work has been partially supported by the Instituto de Telecomunicações, Next Generation Networks and Applications Group (NetGNA), Portugal, by Government of Russian Federation, Grant 074-U01, by National Funding from the FCT – Fundação para a Ciência e a Tecnologia through the PEst-OE/EEI/LA0008/2013 Project.

References

Baronti, P., Pillai, P., Chook, V.W.C., Chessa, S., Gotta, A. and Fun Hu, Y. (2007) 'Wireless sensor networks: a survey on the state of the art and the 802.15. 4 and ZigBee standards', *Computer communications*, Vol. 30, No. 7, pp.1655–1695.

Borges, L.M., Rente, A., Velez, F.J., Salvado, L.R., Lebres, A.S., Oliveira, J.M., Araujo, P. and Ferro, J. (2008) *Overview of Progress in Smart-Clothing Project for Health Monitoring and Sport Applications*, IEEE Digital Library, Aalborg.

Bri, D., Garcia, M., Lloret, J. and Dini, P. (2009) *Real Deployments of Wireless Sensor Networks*, IEEE Computer Society, Athens, Greece.

Burns, A., Doheny, E.P., Greene, B.R., Foran, T., Leahy, D., O'Donovan, K. and McGrath, M.J. (2010) *SHIMMER™: An Extensible Platform for Physiological Signal Capture*, IEEE Press, Buenos Aires, Argentina.

Camp, T., Boleng, J. and Davies, V. (2002) 'A survey of mobility models for ad hoc network research', *Wireless Communications & Mobile Computing*, Vol. 2, No. 5, pp.483–502.

Cuomo, F., Della Luna, S., Monaco, U. and Melodia, T. (2007) *Routing in ZigBee: Benefits from Exploiting the IEEE 802.15. 4 Association Tree*, IEEE Press, Glasgow, Scotland, pp.3271–3276.

De Nardis, L., Domenicali, D. and Di Benedetto, M. (2010) *Mobility model for Body Area Networks of soccer players*, IEEE Press, Paris, France, pp.65–68.

Dhamdhere, A., Chen, H., Kurusingal, A., Sivaraman, V. and Burdett, A. (2010) *Experiments with Wireless Sensor Networks for Real-Time Athlete Monitoring*, Denver, Colorado, USA, IEEE Press, pp.938–945.

Federal Information Processing Standards Publication 197 (2001) *Advanced Encryption Standard (AES)*, FIPS PUB 197, s.l.

Fruth, M. (2006) *Probabilistic Model Checking of Contention Resolution in the IEEE 802.15. 4 Low-Rate Wireless Personal Area Network Protocol*, IEEE Press, Paphos, Cyprus, pp.290–297.

Garcia, M., Bri, D., Sendra, S. and Lloret, J. (2010a) 'Practical deployments of wireless sensor networks: a survey', *International Journal on Advances in Networks and Services*, Vol. 3, Nos. 1–2, pp.170–185.

Garcia, M., Catala, A., Lloret, J. and Rodrigues, J. (2011) *A Wireless Sensor Network for Soccer Team Monitoring*, IEEE Digital Library, Barcelona, Spain.

Garcia, M., Lloret, J., Sendra, S. and Lacuesta, R. (2010b) 'Secure communications in group-based wireless sensor networks', *International Journal of Communication Networks & Information Security*, Vol. 2, No. 1, pp.8–14.

Glaros, C. and Fotiadis, D.I. (2005) *Wearable Devices in Healthcare. En: Intelligent Paradigms for Healthcare Enterprises*, Heidelberg: Springer Berlin Heidelberg, pp.237–264.

Gui, L., Val, T. and Wei, A. (2011) 'A novel two-class localization algorithm in wireless sensor networks', *Network Protocols & Algorithms*, Vol. 3, No. 3, pp.1–16.

Gyselinckx, B., Vullers, R.J., Van Hoof, C., Ryckaert, J., Yazicioglu, R.F., Fiorini, P. and Leonov, V. (2006) *Human++: Emerging Technology for Body Area Networks*. IEEE Digital Library, Nice, France.

Ha, J.Y., Kim, T.H., Park, H.S., Choi, S. and Kwon, W.H. (2007) 'An enhanced csma-ca algorithm for ieee 802.15. 4 LR-WPANs', *IEEE Communications Letters*, Vol. 11, No. 5, pp.461–463.

Ha, J.Y., Park, H.S., Choi, S. and Kwon, W.H. (2007) 'EHRP: enhanced hierarchical routing protocol for zigbee mesh networks', *IEEE Communications Letters*, Vol. 11, No. 12, pp.1028–1030.

Hoang, D.C., Tan, Y.K., Chng, H.B. and Panda, S.K. (2009) *Thermal Energy Harvesting from Human Warmth for Wireless Body Area Network in Medical Healthcare System*, IEEE Press, Tapei, pp.1277–1282.

IEEE 802.15.4-2006 (2006) *IEEE Standard for Information technology – Telecommunications and Information Exchange Between Systems – Local and Metropolitan Area Networks – Specific Requirements Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications*, s.l.: IEEE, USA.

IEEE Std. C95.1b-2004 (2004) *IEEE Standard for Safety Levels With Respect to Human Exposure to Radio Frequency Electromagnetic Fields*, 3 kHz to 300 GHz Amendment 2: Specific Absorption Rate (SAR) Limits for the Pinna, s.l.: IEEE, USA.

Jovanov, E. (2008) *A Survey of Power Efficient Technologies for Wireless Body Area Networks*, IEEE digital library, Vancouver, Canada.

Kifayat, K., Merabti, M., Shi, Q. and Llewellyn-Jones, D. (2007) 'Group based secure communication for large-scale wireless sensor networks', *Journal of Information Assurance and Security*, Vol. 2, No. 2, pp.139–149.

Kuris, B. and Dishongh, T. (2006) *SHIMMER Hardware Guide Rev 1.3.*, SHIMMER – Sensing Health with Intelligence, Modularity, Mobility, and Experimental Reusability, USA.

Lacuesta, R., Lloret, J., Garcia, M. and Peñalver, L. (2011) 'Two secure and energy-saving spontaneous ad-hoc protocol for wireless mesh client networks', *Journal of Network and Computer Applications*, Vol. 34, No. 2, pp.492–505.

Latré, B., Braem, B., Moerman, I., Blondia, C. and Demeester, P. (2011) 'A survey on wireless body area networks', *Journal Wireless Networks*, Vol. 17, No. 1, pp.1–18.

Le Sage, T., Bindel, A., Conway, P., Justham, L., Slawson, S. and West, A. (2010) 'Development of a real time system for monitoring of swimming performance', *Procedia Engineering*, Vol. 2, No. 2, pp.2707–2712.

Lee, K.K., Kim, S.H. and Park, H.S. (2007) *Cluster Label-based ZigBee Routing Protocol with High Scalability*, IEEE Press, Cap Esterel, France.

Liu, D., Ning, P. and Du, W. (2008) 'Group-based key predistribution for wireless sensor networks', *ACM Transactions on Sensor Networks (TOSN)*, Vol. 4, No. 2, pp.11.

Lloret, J., Garcia, M., Bri, D. and Diaz, J. (2009) 'A cluster-based architecture to structure the topology of parallel wireless sensor networks', *Sensors*, Vol. 9, No. 12, pp.10513–10544.

Lloret, J., Garcia, M., Tomas, J. and Boronat, F. (2008) 'GPB-WAHSN: a group-based protocol for large wireless ad hoc and sensing networks', *Journal of Computer Science and Technology*, Vol. 23, No. 3, pp.461–480.

Llosa, J., Vilajosana, I., Vilajosana, X., Navarro, N., Suriñach, E. and Marquès, J.M. (2009) 'REMOTE, a wireless sensor network based system to monitor rowing performance', *Sensors*, Vol. 9, No. 9, pp.7069–7082.

Lu, X. and Demirbas, M. (2011) 'Model-based tracking for mobile ad hoc networks', *Network Protocols & Algorithms*, Vol. 3, No. 2, pp.1–23.

Luste, O.J. and Anatychuk, L.I. (2005) 'Modern thermodynamic theory of thermoelectricity', in Rowe, D.M. (Ed.): *Thermoelectrics Handbook*, CRC Press, USA, pp.2.1–2.14.

Mitcheson, P.D., Yeatman, E.M., Rao, G.K., Holmes, A.S. and Green, T.C. (2008) 'Energy harvesting from human and machine motion for wireless electronic devices', *Proceedings of the IEEE*, Vol. 96, No. 9, pp.1457–1486.

Nefzi, B. and Q., S.Y. (2007) *Performance Analysis and Improvement of ZigBee Routing Protocol*, Toulousse, France.

Noack, A. and Spitz, S. (2009) 'Dynamic threshold cryptosystem without group manager', *Network Protocols and Algorithms*, Vol. 1, No. 1, pp.108–121.

Pantelopoulos, A. and Bourbakis, N.G. (2010) 'A survey on wearable sensor-based systems for health monitoring and prognosis', *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, Vol. 40, No. 1, pp.1–12.

Pei, G., Gerla, M. and Hong, X. (2000) *LANMAR: Landmark Routing for Large Scale Wireless Ad Hoc Networks with Group Mobility*, IEEE Press, Boston, MA, USA, pp.11–18.

Perkins, C., Belding-Royer, E. and Das, S. (2003) *RFC 3561 – Ad Hoc on-Demand Distance Vector (AODV) Routing*, Internet RFCs, s.l.

Riverbed (2014). *OPNET Network Simulator.* [On line] Available at: http://es.riverbed.com/products-solutions/products/network-performance-management/network-planning-simulation/Network-Simulation.html [Last Access: February, 2014].

Romero, E., Warrington, R.O. and Neuman, M.R. (2009a) 'Energy scavenging sources for biomedical sensors', *Physiological Measurement*, Vol. 30, No. 9, p.R35.

Romero, E., Warrington, R.O. and Neuman, M.R. (2009b) *Body Motion for Powering Biomedical Devices*, IEEE Press, Minnesota, USA, pp.2752–2755.

Sáez, M. and Loreto, M. (2009) *Energy Harvesting from Human Passive Power*, TDX (Tesis Doctorals en Xarxa), Barcelona, Spain.

Sivaraman, V., Grover, S., Kurusingal, A., Dhamdhere, A. and Burdett, A. (2010) *Experimental Study of Mobility in the Soccer Field with Application to Real-Time Athlete Monitoring*, IEEE Press, Niagara Falls, Canada, pp.337–345.

Tan, Y.K., Zheng, Y. and Foong, H.C. (2012) 'Ultralow power management circuit for optimal energy harvesting in wireless body area network', in Iniewski, K. (Ed.): *Advanced Circuits for Emerging Technologies*, Wiley, USA, pp.147–173.

University of Texas (2000) *Design of a Soccer Training Session Based Upon the Physiological Match Demands of Competitive Soccer*, University of Texas, KIN 395, Texas, USA.

Vales-Alonso, J., López-Matencio, P., Gonzalez-Castaño, F.J., Navarro-Hellín, H., Baños-Guirao, P.J., Pérez-Martínez, F.J., Martínez-Álvarez, R.P., González-Jiménez, D., Gil-Castiñeira, F. and Duro-Fernández, R. (2010) 'Ambient intelligence systems for personalized sport training', *Sensors*, Vol. 10, No. 3, pp.2359–2385.

Vullers, R.J., Schaijk, R.V., Visser, H.J., Penders, J. and Hoof, C.V. (2010) 'Energy harvesting for autonomous wireless sensor networks', *IEEE Solid-State Circuits Magazine*, Vol. 2, No. 2, pp.29–38.

Wang, W.S., O'Donnell, T., Ribetto, L., O'Flynn, B., Hayes, M. and O'Mathuna, C. (2009) *Energy Harvesting Embedded Wireless Sensor System for Building Environment Applications*, IEEE Press, Aalborg, Denmark, pp.36–41.

Wong, C.K., Gouda, M. and Lam, S.S. (2000) 'Secure group communications using key graphs', *IEEE/ACM Transactions on Networking*, Vol. 8, No. 1, pp.16–30.

Xiang, J. and Zhu, Y. (2009) *A Survey on Body Area Network*, Beijing, China.

Zulkifli, N.S.A., Harun, F.C. and Azahar, N.S. (2012) *XBee Wireless Sensor Networks for Heart Rate Monitoring in Sport Training*, IEEE Press, Penang, Malaysia, pp.441–444.