# Technological Solutions for Smart Homes

Jeedella S. Y. Jeedella and Mahmoud Al-Qutayri

## Contents



**Abstract**

The combination of ubiquitous computing and wireless communication has provided the opportunities to create novel solutions to realize smart environment. The application of smart environments in the field of health care and assisted living is accelerating at a high pace. These systems can provide cost-effective solutions that will improve the quality of life of humans, particularly those regarded as senior citizens or have some form of disability. The realization of smart environments with real-time monitoring will enable such people to lead independent lives in the comfort of their normal homes. This chapter focuses on highlighting the major components and systems that are currently available to deliver reliable technological solutions for smart homes, health care, and well-being. The key sensing devices that form the basis of smart environments are

J.S.Y. Jeedella (✉)
Fontys University of Applied Sciences, Eindhoven, The Netherlands
e-mail: j.jeedella@Fontys.nl

M. Al-Qutayri
Khalifa University of Science, Technology, and Research, Abu Dhabi, UAE
e-mail: mqutayri@kustar.ac.ae



J. van Hoof et al. (eds.), *Handbook of Smart Homes, Health Care and Well-Being*,
DOI 10.1007/978-3-319-01583-5_47

discussed. The integration of these devices into wireless sensor networks (WSNs) that can be spread over an area to build smart health and assisted living environments is investigated. The role of power line communication technologies, which complements wireless communications, and the new reliable solutions is also highlighted. Wireless communication technologies and the various options and standards available are discussed. Target localization plays a key role in many of the services supported by smart environments. The various fundamental localization techniques are investigated. The major security and privacy issues related to WSNs and wearable body area networks (WBANs) and their impact on the trust in using such systems are addressed. A case study that demonstrates the integration of various WSNs elements to deploy a guiding system for blind persons is described.

**Keywords**
Ubiquitous computing • Context-aware • Smart homes • Sensors

## Introduction

The world's population, particularly in developed countries, is aging, and the health care costs are increasing at a high pace. Therefore, there is a real need to create opportunities for senior citizens, people with disabilities, as well as those that suffer from health problems that require long-term health care, such as diabetes and certain cardiovascular conditions, to live independently in their preferred environment. This will inevitably have a positive impact on the concerned persons, as they will be able to have control on their environment and activities, live autonomously without burdening their caregivers, and have the feeling of dignity and overall well-being. This will obviously reduce the cost of health care provisions and will enable the redeployment of resources to support other services.

Advances in technological solutions currently make it possible to realize smart environments and homes that will enable older adults, persons with disabilities, and those with chronic health conditions to lead independent lives. Smart homes are ones that are augmented with sensors that sense and observe the environment, communicate the sensed information, and have actuators or devices that can react in a proactive manner. The sensing and the other aspects of a smart environment are becoming highly pervasive, due to the phenomenal advances in integrated circuit technologies and other aspects of ICT (information communication technology), and include wearable devices that can be attached or even embedded in the body of say an older adult whose condition is to be continuously monitored. This enables the formation of a wireless body sensor network, which includes accelerometer sensors for motion, ECG sensor, etc., that will facilitate the acquisition of a person's vital signs information and diagnosis of their state of health remotely (Viani et al. 2013).

The devices and technologies that enable the realization of smart environments are becoming even more sophisticated in their sensing/actuation capabilities, embedded computational power, and wireless connectivity. All these modern devices require very low power, which means internal batteries, where they exist, can run for a long time without having to be replaced. In fact, in some cases the devices are self-powered through their energy-harvesting capabilities. The energy-harvesting/scavenging aspect can be from the surrounding environment or even the body of the person being monitored. Context awareness is an important property of the modern devices used to realize smart environments. Fusion of the device context, the environment context, and the person context will enable all better understanding of the situation and hence improve the decision-making process.

The realization of smart environments for older adults and others in need of monitoring and health care provision is expected to become of a plug-and-play nature. This is driven by the fact that a smart home or ambient will take advantage of the Internet of Things (IoT) world that is starting to take shape. In the IoT world objects with unique identifiers will be interconnected, and information can be transferred between them seamlessly. A person with a wearable ECG monitor or a motion sensor that has connectivity to existing Internet infrastructure is considered an object. This means that billions of ubiquitous objects will be connected to the Internet. This will as stated earlier make the realization of smart homes at a large scale feasible and affordable. Some work on smart environments for persons with disability using IoT architecture has been recently reported in the literature (Domingo 2012).

Therefore, with the advent of IoT and the availability of sophisticated sensors that can monitor a myriad of health as well as other parameters, persons will not need to move from the comfort of their homes when they become senior citizens. Delivering real-time health monitoring and general care while an older adult is at his/her normal home is becoming a reality. Given the vast amount of information that can be gathered and processed, the smart environment systems will even have the capability of predicting some health conditions, such as heart attacks, before they actually occur. These types of capabilities will enable to attend to emergencies much faster than otherwise.

This chapter is organized in eight sections. The first section describes the key sensing devices that can form the basis of smart environments. The integration of these devices into wireless sensor networks (WSNs) is investigated in "Wireless Sensors Networks" section. The role of power line communication technologies, which complements wireless communications, is highlighted in PLC section. The "Wireless Communication Technologies" section discusses the various options and standards available that can influence smart environments. Localization plays a key role in many of the services supported by smart environments; accordingly it is presented in the "Target Localization" section. The "Security" section addresses the major security and privacy issues related to WSNs and wearable body area networks (WBANs). Finally, this chapter ends by describing a case study that demonstrates the integration of various WSN elements to deploy a guiding system for blind persons.

## Sensing Devices

Ambient intelligence can be provided to smart home users by making use of a heterogeneous network of smart sensors that actively monitors and collects important information about the home facilities and its users. The type of services provided using this smart home sensors network can be as simple as controlling the environmental condition within its premises. The remote monitoring of health conditions of senior citizens living alone in their home is one of the advanced challenges that could be integrated in this network. Different types of sensors and actuators can be used to implement the different services provided to users of smart home. For example, the integration of temperature, humidity sensors, location-based sensors, and information processing can be used to control the air conditioning and heating systems not only to optimize energy usage but also to adapt the same atmospheric condition to its user based on his/her location inside the home.

For health care monitoring, sensors can be from simple biosensors such as heartbeat, respiration, blood pressure, etc. to more advanced ones such as location, postures, and emotion sensors. Information processing is an important component in the smart home sensors network where data collected from different sources can be combined together to create a confidence about the whereabouts of the smart home resident. The location of the smart home resident for example can be inferred based on the data acquired from his/her location sensor, and by processing the audio data stream from his/her voice, some confidence can be created about his/her current activity. By combining the aforementioned data streams with the face analysis of the video stream monitoring of the smart home user, some judgement can be formed about the well being and emotional state of the person being monitored.

In the future, both wearable smart sensors and implantable medical devices (IMD) can be used to provide remote health care monitoring. For example, pacemaker, implantable cardiac defibrillators (ICDs), drug delivery systems, neurostimulators, etc. are some of the IMDs that can be connected to the smart home networks to provide the constant monitoring of the smart home user. With the advances in flexible sensors, miniaturization technology, low power design, wireless networks, and smart textile, wearable health-monitoring systems (WHMS) (Pantelopoulos and Bourbakis 2010; Kim et al. 2011) can be developed. A senior citizen who needs to be monitored can wear WHMS most of the time. The WHMS is embedding or integrating different types of sensors such as electrocardiogram (ECG), electromyogram (EMG), blood pressure, respiration, heartbeat, etc. (Chen et al. 2011). The collected measurements are transmitted via wires or wirelessly to an information processing unit which produces the information that are displayed on the user interface and transmits the vital signs data to the medical center. Figure 1 shows a possible architecture of a WHMA.

The information processing unit could be a PDA, a smartphone, a pocket PC, or any specialized microcontroller-based device. Thus, it will allow the real-time monitoring of the vital signs of a senior citizen living alone. The collected information can provide feedback information about the user's health condition to the medical center or directly to the professional physician and in some situation alert

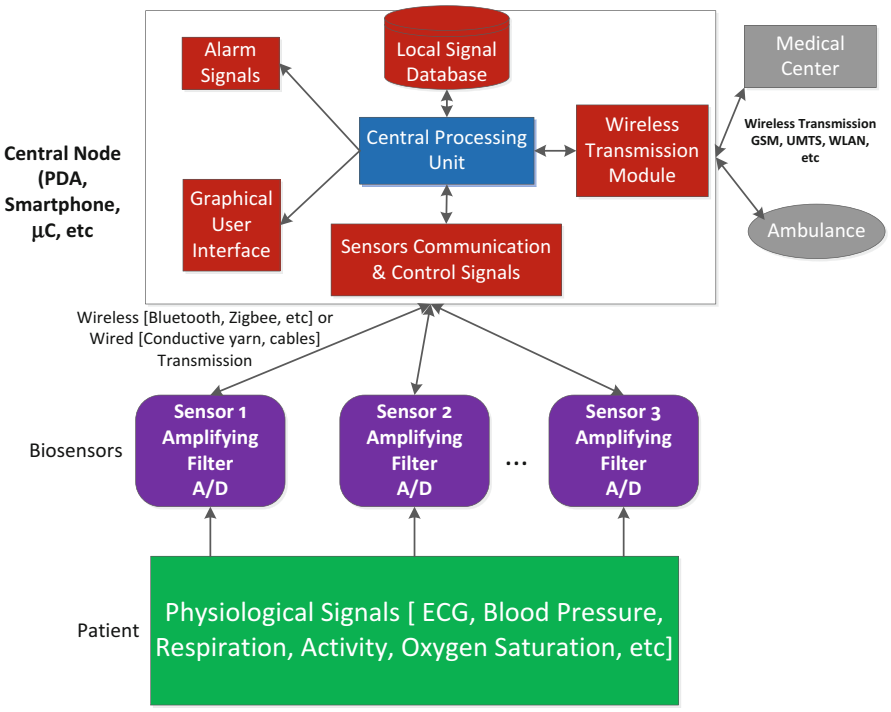


**Fig. 1** Architecture of a wearable health-monitoring system (Pantelopoulos and Bourbakis 2010)

the concerned individuals in case of emergency health-threatening conditions. The authors (Pantelopoulos and Bourbakis 2010) reviewed several of the state-of-the-art wearable sensor-based systems for health monitoring that are as research prototypes and also commercially available products.

## Wireless Sensor Networks

Wireless sensor networks (WSNs) are the main elements of smart environments. They are the key to gathering sensory information and communicating it for subsequent processing for a myriad of applications that include health monitoring, security, localization, seismic sensing, and many others. A WSN is basically a network of a large number of distributed autonomous tiny devices that are deployed over a geographical area to sense particular physical phenomena such as those stated earlier. Each sensor node in a WSN typically consists of three components: (1) sensing and data acquisition subsystem, (2) processing component, and (3) wireless communication transceiver module.

In addition to the above components, each WSN node normally gets powered from a battery to provide a small amount of energy. In general the battery is not

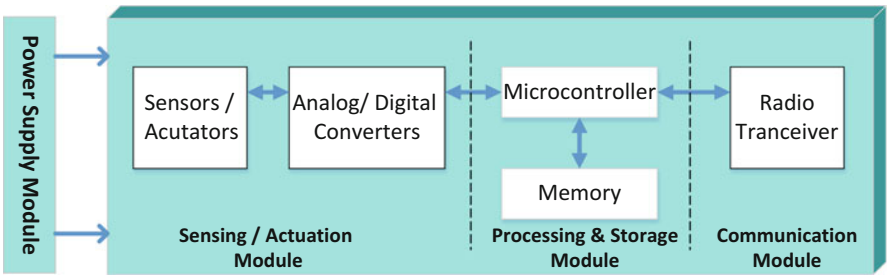


**Fig. 2** Wireless sensor node general architecture

expected to be replaced as the sensor node could be deployed in a remote hazardous environment. This requirement puts severe constraints on the design of WSN components and its functionality. The components must have very low power consumption. This has led to many innovative power management designs including those that utilize energy scavenging techniques. Given the limited energy supply, WSNs have severely constrained communication bandwidth and range as well as information processing and local storage capacity. The general architecture of a wireless sensor node is shown in Fig. 2. Wireless sensor nodes are available from a variety of suppliers with various features that depend on the application being targeted.

To build a network, sensors typically get grouped in clusters, with each cluster having a cluster head. The nodes within a cluster forward their data through the cluster head. The routing of the various cluster heads traffic is done using multi-hop wireless communication through a special node called a sink node, which basically acts as the base station. A number of wireless communication standards are used in wireless sensor networks including IEEE 802.15.1 (Bluetooth) and 802.15.4 (widely known as Zigbee).

The use of WSN in health monitoring and assisted living are among the prominent applications of this increasingly pervasive technology. In the field of health, wearable body area networks (WBANs) have been deployed as part of the general WSNs in a number of studies. WBANs include both wearable and implanted devices. The wearable ones enable monitoring temperature, heart rate, blood pressure, etc. The implantable devices get inserted inside the body, and they include cardiac arrhythmia monitor, brain liquid pressure sensor, etc. The range of both types of devices is expanding with advances in materials, MEMS (microelectromechanical systems), and integrated circuit design. A typical architecture of WSNs in health care applications is shown in Fig. 3 (Al Ameen et al. 2012).

In Chipara et al. (2010), the authors presented the design, deployment, and empirical study of a WSN clinical monitoring system that collects pulse and oxygen saturation readings from patients. According to the study, monitoring these vital signs enables early detection of clinical deterioration so that clinicians can intervene before the patient's condition deteriorates. The choice of monitoring the said vital

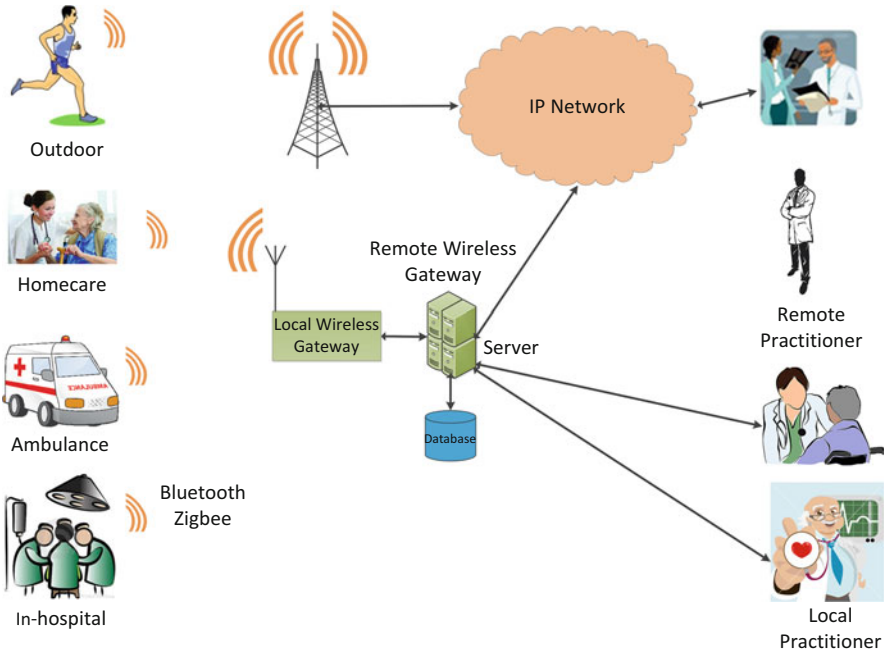


**Fig. 3** Typical architecture of WSNs in health care applications (Chipara et al. 2010)

signs is driven by the fact that these parameters do not need high data rates and hence can be easily supported by energy efficient IEEE 802.15.4 enabled WSNs.

In Wood et al. (2008), a WSN-based system called AlarmNet for assisted living and residential monitoring is presented. The system combines many of the features of predecessors including PlaceLab (Intille et al. 2005) and CodeBlue (Malan et al. 2004). AlarmNet is a heterogeneous scalable network that has the ability to integrate new technologies as they become available. The architecture of the AlarmNet system, shown in Fig. 4, includes the following main elements:

- Mobile body networks are wireless sensors that can be worn by the patient or senior citizen being monitored. The devices can sense and transmit physiological and activity parameters such as pulse rate and acceleration.
- Emplaced sensors are used to sense the quality of the environment, such as temperature and dust levels, the person is living in. They can also be used to monitor a person's activities and provide location information that can be integrated for context awareness features of the AlarmNet system.
- Alarm-Gate is an embedded platform to run various applications.
- At the back end of this is a set of programs that perform online analysis of sensory data and use it along with profile information to aid context awareness.

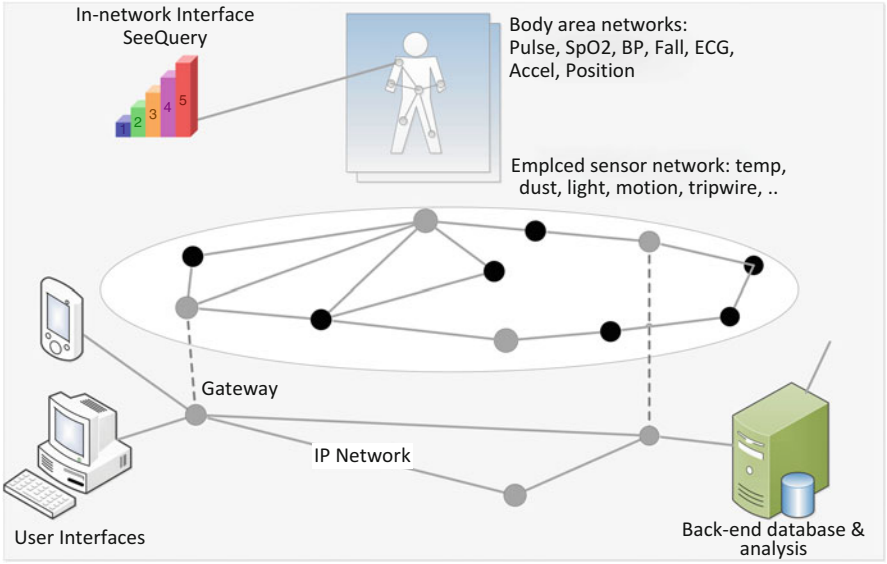


**Fig. 4** AlarmNet architecture (Wood et al. 2008)

## Power Line Communication Technologies

This technology uses existing power line wires for home communication purposes. Several power line communication (PLC) commercial products are used for home automation and networking such as X10 which is a proprietary technology. It provides low data rate and poor reliability in noisy environment (Nunes 2003). Some of PLC products use LonWorks technology (Jeon 2002). The Consumer Electronics Bus (CEBUS) is meant to define a local area network to exchange control and services among home appliances. Even though it is meant to revolutionize home automation, it has not yet gained much popularity (Jeon 2002).

The HomePlug Alliance released a set of standards for in-home PLC networks with the intention to provide platform to foster the creation of products and services in a cost-effective and interoperable with each other's (Home Plug Alliance). HomePlug 1.0 with data rate of 14 Mb/s intends to provide networking using home PL wiring. Also for high speed Internet, HomePlug BPL was defined. This can provide an alternative to wired network protocols such as Ethernet. HomePlug AV with data rate of theoretically 200 Mb/s intends to support multimedia applications in homes. HomePlug C&C (Command & Control) is intended for home automation since it provides a low data rate at low cost networking. PLC is shared channel such as Wi-Fi; accordingly encryption is required to improve its security. HomePlug uses DES encryption with a 56-bit key. However, it suffers from intrusion and interference from adjacent subnets such as apartments. Since it uses the existing

infrastructure, it has tremendous potential; accordingly many companies and researchers are interested to find solutions for the challenges related to technology.

## Wireless Communication Technologies

The ultimate goal for wireless communication is to communicate with all types of information, audio, video, data, and control, with anyone and any system, at any time and from everywhere. The emergence of wireless communication standards such as Wi-Fi, cellular technologies, Bluetooth, Zigbee, RFID, and MICS can help in realizing this goal. With the aid of a combination of these standards, smart homes can be constructed. Basically, any wireless communication technology supporting some form of sensing, data transfer, and control can be a candidate to realize some of the smart home requirements.

Wireless Fidelity (Wi-Fi) is a technology that refers to wireless networks; however, it uses the IEEE 802.11 wireless communication standard. This standard defines the standard for wireless local area networks (WLAN) where 2.4, 3.6, 5, and 60 GHz frequency bands are used. Wi-Fi technology allows network users to move around to different locations while they can still access the network from almost anywhere. It can provide an alternative solution for providing network services for old buildings. The Wi-Fi standard defines an access point (AP) and a wireless client as shown in Fig. 5. The Wi-Fi client could be a laptop or a smartphone equipped with a wireless network interface.

Transferring the information between the wireless network and the wired network is the responsibility of the AP, and it can service up to 30 wireless devices. The coverage range of an AP is between 33 and 50 m in indoor situation and can be up to 100 m in outdoor situation. Wi-Fi devices can form together a network using ad hoc infrastructure where a Wi-Fi node can operate as both an AP and a client.

The mobile communication systems have gone through extensive developments since their introduction. This has culminated in the current 4th generation and heading toward Long-Term Evolution (LTE) systems (Astely et al. 2013). The

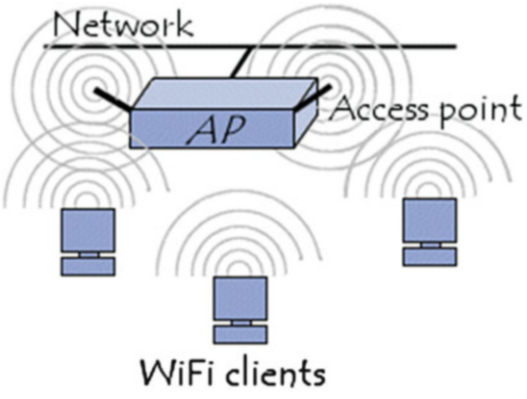


**Fig. 5** Wi-Fi standard network architecture

developments brought about an increase in bandwidths and a rich set of services. With the supported data rate, it is possible to provide mobile TV, video conferencing, and fast Internet.

Bluetooth technology uses a short-range universal radio interface to replace the wired communication between various electronic devices, such as mobile phones, headsets, and sensors (Blueooth). The development of many Bluetooth-enabled devices and sensors enabled the formation of personal area networks ubiquitously. Furthermore, many applications were developed based on this technology. It uses 79 channels of 1 MHz in the 2.4 GHz band and it can provide data rates up to 2.1 Mbit/s. It can support a maximum range of 100 m in case class 1 devices are used. Encryption is optional and provided using a 64 or 128 bits SAFER + algorithm; however, Bluetooth is often designated as vulnerable to attacks. Bluetooth SIG announced the addition of two stacks: the Bluetooth low power targeting devices with limited battery sources such as health care devices and sport/wellness devices. The second stack is Bluetooth 3.0 specification that uses Wi-Fi physical/MAC layer for higher data throughput.

Zigbee is a technological standard created for control and sensor networks based on the IEEE 802.15.4 standard (Zigbee Alliance). It is defined for low cost, low data rate, low power, wireless personal area network (WPAN). It can use 868 MHz in Europe, 915 MHz in the USA and Australia, and 2.4 GHz in most jurisdictions worldwide. It can support data rate of 20 (868 MHz), 40 (915 MHz), and 250 kbit/s (2.4 GHz). This technology provides a communication standard for low power, battery-operated sensors and low cost application by providing a compromise between these parameters and the supported date rate. It uses advanced encryption standard (AES) to perform authentication to guarantee communication privacy. The operating frequency, data rate, and network size are all defined by the standard. Zigbee devices operating in the 2.4 GHz band are more often used since it is available worldwide and the supported data rate is higher than other bands. The size of the network is limited to 64,000 devices; however, by using multiple coordinators connected together, large networks can be made.

Radio frequency identification (RFID) is a system where an object can be wirelessly scanned; accordingly it will transmit its identity. This technology defines an RFID tag that holds information about the object carrying it and an RFID reader. The RFID tag will only transmit its data when it is scanned by the reader. In case that the RFID tag is passive, then it will have no battery, and it will be powered by the reader's magnetic field; accordingly it is cheap to manufacture. The passive RFID tag has a low range when compared to an active RFID tag that does have battery powering its circuitry.

The Medical Implantable Communication Services (MICS) technology is an ultralow power, low data rate, and short-range communication for therapeutic or diagnostic functions related to medical devices. This technology uses the 402–405 MHz frequency band with 300 kHz channels. It targets devices such as pacemakers and implantable cardiac defibrillators (ICDs) with limited radiated power to 25 μW. Even though this technology has interesting characteristics, it was not used by many researchers in their prototypes due to the limited commercially available MICS solutions (Pantelopoulos and Bourbakis 2010).

## Target Localization

Target localization is an important feature of WSNs. This is particularly the case for WSNs that are used for assisted living, senior citizen monitoring, target tracking, and other tasks in smart environments. In general target localizations enable the computation of the position of a node within some fixed coordinates. By doing so, many applications can be developed. For example, a WSN can be installed in the home of a senior citizen, and a sensor node can be attached to the person. The movement of the concerned senior citizen can then be tracked, and an alarm can, for example, be raised if the person's activity behavior changes from the norm. Node localization can also be used in hospitals to track equipment, patients, and medical staff. This ability to localize a node within a smart environment opens many other possibilities for a multitude of applications and services. For example, the fusion of a target node location with other sensory information and a profile database enables building context aware systems with various degrees of sophistication.

Localization can be achieved in wireless systems using a variety of techniques. A straightforward one is the use of GPS (global positioning system) that requires satellite line of sight. However, such systems are only suitable for outdoor environments and consume relatively high amount of energy. Given these constraints and the fact that nearly all WSN operate with small batteries that are supposed to last for a long time, the use of GPS for localization is precluded in such systems. Many node localization techniques have been proposed in the literature that do not depend on GPS.

Generally location discovering techniques consist of two computational phases: (1) distance estimation and (2) location combining. Depending on the parameter used to calculate the relative position of a target node, distance (or angle) estimation techniques can be classified as: angle of arrival (AoA), time of arrival (ToA), time difference of arrival (TDoA), and the received signal strength indicator (RSSI).

The AoA technique calculates the position of a node by estimating the angle at which signals are received. AoA can give accurate results; however, it requires an array of directional antenna elements which increases the complexity of the hardware. ToA computes the time at which a signal first arrives at a receiver. Distance can then be calculated by multiplying the measured propagation time (be it one way or round trip) by the radio signal velocity. In ToA the nodes have to be synchronized and the signals time stamped. The TDoA technique uses either multi-node or multi-signal to compute the location of a node. The former is based on the difference in time at which a single signal from the target node arrives at the at least three receiving nodes, while the latter uses two signals that have different propagation speeds (e.g., radio frequency and acoustic) generated by the target node and compares their delay. TDoA gives accurate results under line-of-sight conditions. However, the accuracy gets highly reduced in indoor environments due to multiple reflections of radio signals.

RSSI localization technique measures the received signal power, and given that the transmit power is known, the propagation loss can be calculated. This information can be combined with a channel model to translate the loss of transmitted signal power into a distance estimate. RSSI is very popular in target

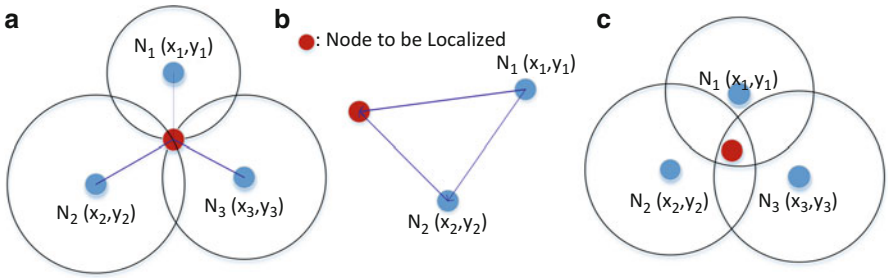


**Fig. 6** Localization techniques: (**a**) trilateration (**b**) triangulation (**c**) maximum likelihood

localization in WSNs because the received power indicator is available at no cost at the physical layer of the WSN nodes. However, RSSI technique does not provide accurate ranging estimation, compared with AoA, ToA, and TDoA, due to the multipath propagation effect of radio signal. The accuracy of RSSI can be improved by having more accurate radio propagation path loss models and the use of adaptive computational algorithms (Kupershtein et al. 2013).

The location discovery combining phase normally uses trilateration, triangulation, or maximum likelihood estimation techniques. These techniques are depicted in Fig. 6. Trilateration or lateration, shown in Fig. 6a, is an intuitive geometrical technique that uses the intersection of at least three circles; each represents the aperture distance between an anchor node and the node to be localized. The radius of the circle is equal to the distance measurement. The triangulation method, depicted in Fig. 6b, uses basic trigonometry to find the location of a node. In doing so, it uses angles instead of distance information. The node to be localized estimates its angle to each of the three reference nodes then uses this and the known positions of the reference nodes to calculate its own position by applying trigonometric properties. The maximum likelihood (ML), shown in Fig. 6c, is a probabilistic technique that attempts to mitigate the uncertainty in distance estimation. ML uses distance measurements from multiple reference nodes to estimate a node position. When the unknown node receives a signal from a reference node, it assumes it to be at any place around the reference node with equal probability. The same process gets repeated for other neighboring reference nodes. This results in identifying the probable position of the unknown node. The major drawbacks of ML are the high computational cost and information storage requirement.

## Security

The security and privacy in WBANs as well as WSNs in general are of major concern. Both types of networks use wireless communications, and that exposes them to all the security and privacy vulnerabilities associated with such technologies. However, security and privacy issues are much more critical for WBANs as they may affect the lives of the persons involved. In WBANs sensors collect data about

the various physiological parameters of a person; however, those devices are severely constrained in their resources and available power, and hence incorporating traditional security schemes is not feasible (Al Ameen et al. 2012; Li et al. 2010; Kaseva et al. 2011).

Malicious attackers can compromise the security of WBANs by gaining access to the data collected by the sensors. This can then be used to launch passive or active attacks at the system and information security levels in ways that could pose serious problems to the concerned individual. An attacker may, for example, change the destination of a data packet containing critical vital signs information, such as blood pressure, and hence deprive the person from receiving appropriate medical attention leading to possible loss of life. Generating routing inconsistencies which leads to identity deception is another possible type of attacks. In such cases the adversary can cause selective forwarding and wormhole and sinkhole attacks (Zhu et al. 2011; Krontiris et al. 2009).

Through eavesdropping to the WBANs or WSNs, an attacker can steal health data about an individual and use it to blackmail or compromise the person. Security attacks on node location information in WBANs/WSNs are critical ones. An attacker may intercept location packets and replay them in different locations. It may also manipulate the intercepted information and use it to distribute incorrect locations for malicious reasons. These forms of attacks may threaten the life of the individual. For example, in an assisted living smart environment node, location is used for context awareness so having the wrong information will lead to incorrect inferences about the state of the person being monitored (Al Ameen et al. 2012; Li et al. 2010; Zhu et al. 2011; Krontiris et al. 2009).

A summary of the security risks in WBANs and their corresponding security requirements are listed in Table 1 (Al Ameen et al. 2012). Security associated with WBANs/WSNs is an active research area, and various solutions are continually proposed in the literature to address new challenges as the technology evolves (Kaseva et al. 2011; Zhu et al. 2011; Hu et al. 2009; Rohokale et al. 2013; Matyas et al. 2013).

Privacy and measures of preserving it are a major concern for individuals as well as organizations that deploy WBANs and WSNs in general. Privacy threats include attacks on content where the meaning of the information being exchanged is understood by the adversary, identity theft which results from revealing the identities of the communicating entities, and location privacy threat which results in identifying the physical location of a node. All privacy oriented attacks, be it in WBANs or WSNs, lead to unauthorized access to information that may be of critical nature such

**Table 1** WBAN security risks and requirements (Al Ameen et al. 2012)

| Attack assumptions | Risks to WBAN | Security requirements |
|---|---|---|
| **Computational capabilities** | Data modification | Data integrality |
| | Impersonation | Authentication |
| **Listening capabilities** | Eavesdropping | Encryption |
| **Broadcasting capabilities** | Replay | Freshness protection |

as medical records and hence compromise trust in the system. Depending on the nature of the privacy attack, the life and well-being of the affected person may be threatened. Solutions to overcome privacy threat at all levels of WBANs/WSNs continue to be proposed in the literature. However, the ever increasing complexity of these systems, particularly their distributed nature that extends to the computing clouds, means that the issue of privacy will need to be continually addressed in order to keep an acceptable level of trust in the systems (Al Ameen et al. 2012; Li et al. 2010; Krontiris et al. 2009; Di Pietro and Viejo 2011; Matyas et al. 2013).

## Case Study

This section provides a system architecture of a smart home that integrates wireless sensor networks with different types of sensors to help blind or visually impaired person to navigate independently inside his/her home. It is based on a Zigbee network that calculates the location of its user and a digital compass that help to infer his/her orientation. The localization and navigation algorithm is running partially on a remote server and partially on a mobile node carried by its user. This mobile node is a Zigbee end device that requires relatively low power. The server receives the audio command from its user regarding his/her target destination. Accordingly, the system will calculate the optimal path to the requested target using the current user's location and the internally stored virtual map of the house. The required audio commands to help the user navigate to his/her target destination will be generated by the server and received and played back on the mobile node. Figure 7 shows the global system architecture of the prototype system. The system will receive the various input signals and continuously adapt the navigation commands based on the current location and the target destination in real-time.

Based on this architecture, a demonstrator was developed and tested, and its accuracy is highly dependent on the localization engine in Zigbee mobile node.

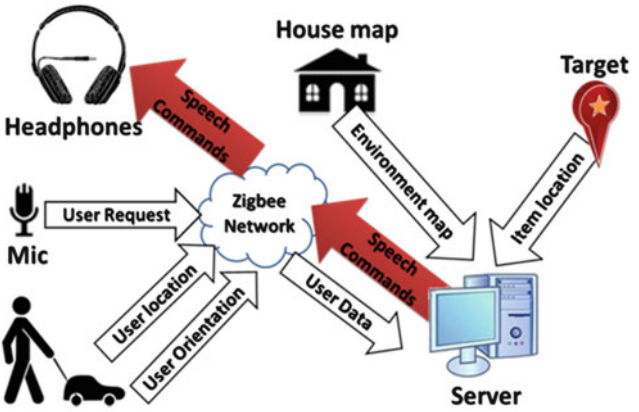


**Fig. 7** System architecture (Al-Qutayri et al. 2011)

Furthermore, the system was not fully autonomous, and it relies on the user to do local obstacle avoidance since the household situation can continuously change. With the advances in indoor localization algorithm, we believe that the localization accuracy of this demonstrator can be improved by using better localization engine as was discussed in the "Target Localization" section.

## References


Al Ameen M, Liu J, Kw K (2012) Security and privacy issues in wireless sensor networks for healthcare applications. J Med Syst 36(1):93–101

Al-Qutayri M, Jeedella J, Al-Shamsi M (2011) An integrated wireless indoor navigation system for visually impaired. In: Systems conference (SysCon), 2011 I.E. international, Montreal

Astely D, Dahlman E, Fodor G, Parkvall S, Sachs J (2013) LTE release 12 and beyond [Accepted from open call]. IEEE Commun Mag 51(7):154–160

Blueooth [Online]. Available: http://www.bluetooth.com. Geopend 8 Dec 2013

Chen M et al (2011) Body area networks: a survey. Mob Netw Appl 16(2):171–193

Chipara O, Lu C, Bailey TC, Roman G-C (2010) Reliable clinical monitoring using wireless sensor networks: experiences in a step-down hospital unit. In: Proceedings of the 8th ACM conference on embedded networked sensor systems, New York

Di Pietro R, Viejo A (2011) Location privacy and resilience in wireless sensor networks querying. Comput Commun 34(3):515–523

Domingo MC (2012) An overview of the Internet of Things for people with disabilities. J Netw Comput Appl 35(2):584–596

Home Plug Alliance [Online]. Available: https://www.homeplug.org/home/. Accessed 12 Nov 2013

Hu W et al (2009) Secfleck: a public key technology platform for wireless sensor networks. In: Wireless sensor networks. Springer-Verlag, Berlin/Heidelberg, pp 296–311

Intille SS, Larson K, Beaud JS, Tapia M, Kaushik P, Nawyn J, McLeish TJ (2005) The PLACELAB: alive-in laboratory for pervasive computing research (VIDEO). In: Pervasive computing, third international conference, Munich, Germany PERVASIVE 2005

Jeon J (2002) A survey on protocols for home networks based on power line communication. In: Proceedings on the 15th CISL winter workshop, Kushu

Kaseva V, Hämäläine TD, Hännikäinen M (2011) A wireless sensor network for hospital security: from user requirements to pilot deployment. EURASIP J Wirel Commun Netw 17 http://dx.doi.org/10.1155/2011/920141

Kim H-C, Meng Y, Chung G-S (2011) Health Care with Wellness Wear, Health Management - Different Approaches and Solutions, Dr. Krzysztof Smigorski (Ed.), ISBN: 978-953-307-296-8, InTech, DOI: 10.5772/19875. Available from: http://www.intechopen.com/books/health-management-different-approaches-and-solutions/health-care-with-wellness-wear

Krontiris I, Benenson Z, Giannetsos T, Freiling FC, Dimitriou T (2009) Cooperative intrusion detection n wireless sensor networks. In: EWSN '09 proceedings of the 6th European conference on wireless sensor networks, Berlin

Kupershtein E, Wax M, Cohen I (2013) Single-site emitter localization via multipath fingerprinting. IEEE Trans Signal Process 61(1):10–21

Li M, Lou W, Ren K (2010) Data security and privacy in wireless body area networks. IEEE Wirel Commun 17(1):51–58

Malan D, Fulford-Jones T, Welsh M, Moulton S (2004) CodeBlue: an ad hoc sensor network infrastructure for emergency medical care (2004). In: International workshop on wearable and implantable body sensor networks

Matyas V, Kur J (2013) Conflicts between intrusion detection and privacy mechanisms for wireless sensor networks. IEEE Secur Priv 11(5):73–76

Nunes RJC (2003) Home automation – a step towards better energy management. In: International conference on renewable energies and power quality (ICREPQ03), Vigo

Pantelopoulos A, Bourbakis NG (2010) A survey on wearable sensor-based systems for health monitoring and prognosis. IEEE Trans Syst Man Cybern Part C Appl Rev 4(1):1–12

Rohokale VM, Prasad NR, Prasad R (2013) Reliable and secure cooperative communication for wireless sensor networks making use of cooperative jamming with physical layer security. Wirel Pers Commun 73:595–610

Viani F, Robol F, Polo A, Rocca P, Oliveri G, Massa A (2013) Wireless architectures for heterogeneous sensing in smart home applications: concepts and real implementation. Proc IEEE 101 (11):2381–2396

Wood AD, Stankovic JA et al (2008) Context-aware wireless sensor networks for assisted living and residential monitoring. IEEE Netw 22(4):26–33

Zhu WT, Xiang Y, Zhou J, Deng RH, Bao F (2011) Secure localization with attack detection in wireless sensor. Int J Inf Secur 10:155–171

Zigbee Alliance [Online]. Available: http://www.zigbee.org. Geopend 8 Dec 2013