Body Area Networks and Body Sensor Networks

David J. Ruprecht
University of Minnesota, Morris
600 East 4th Street
Morris, MN 56267
rupre009@morris.umn.edu

ABSTRACT

Recent advances in wireless communication technologies, batteries, and sensors have enabled a new wireless network sensor research and development area. This new area of research and development has brought forward many applications such as medical patient monitoring, recreational gaming control, as well as athletic body monitoring. This paper discusses body area networks, their implications on society, challenges involved, and common solutions to those challenges. We will look at network communication architectures, hardware challenges, and network security specific to body area networks.

Categories and Subject Descriptors

C.2.1 [**Network Architecture and Design**]: Network communications

General Terms

Security

Keywords

access point, body area network, body sensor network, medium access control, personal server, radio frequency, wireless sensor network

1. INTRODUCTION

With recent advancements in technology, devices and sensors are getting smaller. These tiny sensors have allowed doctors, trainers, and even gamers to implant sensors in or wear sensors on or near the body. These recent advancements have made it possible to build entire wireless networks inside the human body. For example sensors can even be as small as 1 micrometer [1]. Pacemakers and heart monitors are two examples of devices possibly enhanced by this new technology [4].

Recently interest has increased in research and development of Body Area Networks (BANs) and Body Sensor Networks (BSNs), fueled by advances in wearable sensors that are both lightweight and physically small. BSNs are a subset of BSNs and each will be used in this paper when appropriate. Traditional deployment methods and features of well known wireless sensors networks are not well adapted to this unique type of network.

One of most prominent development was the advancement of the IEEE 802.15.4 standard. The IEEE 802.15.4 supports wireless communication between nodes with low power consumption [3].

In this paper we will first discuss possible uses of Body Area Networks and Body Sensor Networks. Next we will investigate Body Area Network communication technology, architecture, and related hardware. To finished we will talk about specific security challenges involved in Body Area Networks and Body Sensor Networks.

2. APPLICATIONS OF BODY AREA NETWORKS

Sensor Networks implanted within the body can have many benefits in the medical, military, and automotive.

2.1 Medical

BSNs have a considerable potential in the medical field. In the case of a routine exam an individual might be fitted with a temporary sensor to read information such as pulse, blood pressure, blood sugar, or hormone level. The very size of these sensors in most cases make them less invasive than the traditional methods of gathering information.

Another medical scenario could be in the case of an emergency, where the patient is not in the hospital, information could be gathered by sensors placed in or on the body in the field before the patient is transported to the hospital. The information collected could be immediately sent to the hospital where the emergency room technician, doctors and other staff could review it. Also, “the data obtained during a large time interval in the patient’s natural environment offers a clearer view to the doctors than data obtained during short stays at the hospital” or emergency room [4].

Alternatively an emergency situation might be avoided by “continuous monitoring” sensors and alerts. Much like a pacemaker continuously monitors a patient’s heart rhythm, it could be possible for an entire BSN with many types of sensors to identify issues before they cause an emergency situation. It could even be possible in some cases for medical technicians to contact the patient fitted with a BSN to

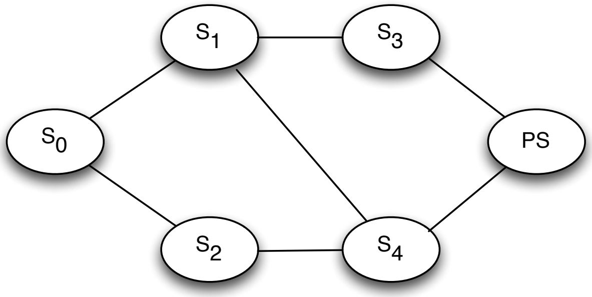

Figure 1: A simple example of a mesh network.

address issues without the patient physically traveling to a clinic. Not only could this reduce costs to both the clinic and the patient, it could also allow patients to have better medical care than previously possible. The patient might also feel more comfortable by having the ability to freely move around while still receiving the medical monitoring they only previously could have received in the clinic. [4]

2.2 Athletics

Body sensor networks also have implications beyond the medical setting. BSNs could play a huge role in non-competitive and competitive athletics through continuous monitoring would provide huge advantages to athletes and trainers.

The first advantage BSN nodes would provide is tuning. By simply reading the information gathered by the sensors, athletes or trainers could adjust levels of sugar, water, oxygen, and even chemicals such as caffeine in the body. The same might occur in competition setting where simple tuning could be adjusted mid-competition to account for different aspects of the event. In the case of the running, it would be possible to monitor lactic acid output and water input. Another example summarized in [1] fits BAN sensors to a golfer and club. Readings of the golfers hips and club position provide instant feedback allowing the golfer to adjust his power and movement. This would in turn allow the golfer to adapt to varying conditions on the course.

2.3 Military

Body Area Networks can also be used by the military to monitor aspects of the soldier's condition in the field. First, sensors can determine if adequate water is being consumed to protect the soldier from heat stroke. In this situation the solider's BSN would transmit signals to a database. The information could then be used to better plan troops movements. [1]

2.4 Intelligent Biosensor System

BANs and BSNs can also be integrated into an intelligent vehicle system allowing for the collection of blink-rate, yawning, eyebrow raise, and head movements. This information can be analyzed to determine the alertness of the operator possibly providing a warning to the operator if necessary. The system could even be completely installed in the vehicle as opposed to the person's body, to read the users physiological signs. [1]

3. ZIGBEE MESH NETWORKS

There are many integral devices involved in wireless networks like BANs and BSNs. A Zigbee network is one of the many different communication technologies used in these networks. Although Zigbee is not directly related to BANs or BSNs it is important to mention because Zigbee may be used to bridge between a local network and a global Internet connected BAN or BSN.

Zigbee is a mesh network standard based on the radio standard IEEE 802.15.4 [6]. A simple example of a mesh network is shown in Figure 1 where each node is labeled with a letter "S" and the server is labeled "PS". IEEE 802.15.4 was developed to support low data rates, simple connectivity, as well as battery powered nodes. IEEE 802.15.4 has also become one of the most commonly accepted radio platforms in the BAN/BSN field. Bluetooth is also a platform that is generally used although when compared to IEEE 802.15.4, Bluetooth is found to be less energy efficient. Zigbee allows for communication between wireless nodes with minimal range that might only be able to communicate with a small subset of others nodes in the network. The Zigbee protocol also takes responsibility for data message routing. Acknowledgements are messages sent in response to verify another signal was received. Because the Zigbee network is a "self meshing" network the network will automatically self-heal if one or more nodes are damaged, greatly increasing network reliability [6]. The term self healing means if a link fails in the network the network will attempt to use another path if one exists. For example in Figure 1 if the link between S_3 and PS were to fail, traffic would take a different path to the PS. In this particular example S_3 would be able to communicate to PS via S_1 and S_4.

The availability and relatively low cost of Zigbee compatible networks makes it a very popular solution to many situations where small low-power networks are required. Also, due to Zigbee's low power consumption and mesh design it is perfect for deployment in a BSN/BAN setting. Power can be conserved by only requiring sensors in the network to communicate to a few others nodes as opposed to requiring wireless communication over large distances [6]. Although the largest distance between two nodes may only be a few feet in a BAN, it is much easier to determine the body tissue resistance between two nodes that are closer together than requiring a node to communicate through tissue that might be constantly changing.

4. COMMUNICATION ARCHITECTURES

Wireless Local Area Networks is one common communication technology used in BANs. BANs can be broken into three component tiers: Intra-BAN communication, Inter-BAN communication, and Beyond-BAN communication. [1]

4.1 Intra-BAN communication

Intra-BAN-Communication, also called Tier-1-Communication is defined as radio communication between two nodes [1]. This communication can be between two sensors or between a sensor and another portable device like a cellular phone or dedicated personal server (PS). A basic example of this can be seen in Figure 2. Tier-1-Communication design is highly difficult due to battery operated nodes are incapable of sending large amounts of information over large distance. One possible solution to this issue is a hard wired

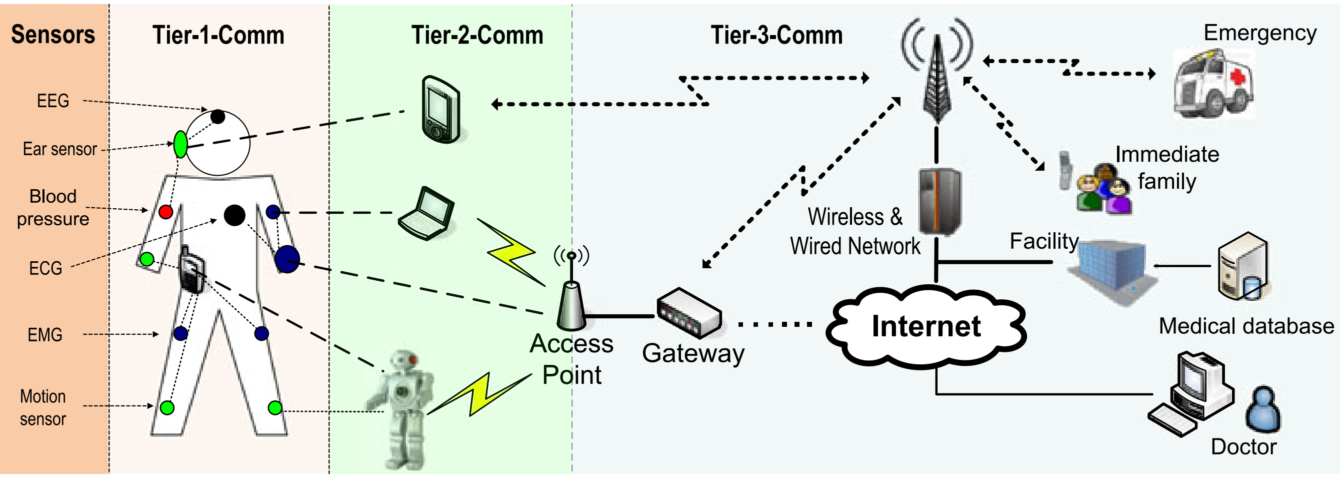

Figure 2: An example of a 3 tier BAN system. Taken from [1].

link between sensors and the PS device. Another option is to eliminate the battery operated PS altogether. In this case, body sensors would be directly communicating with an Access Point (AP) if the access point is within the range of the sensor network. [1]

4.2 Inter-BAN communication

Inter-BAN communication, also called Tier-2-Communication involves another layer of technology, involving access points, cell phones, PDAs, and computers allows us to deal with certain issues. One issue can be a lack of power at the PS. In order to process all of the raw data the PS needs to use elevated levels of power. An advanced method to deal with the PS bottleneck is the use of a central processor. In this model all sensor nodes communicate wired or wirelessly directly with a central processor. The central processor will pull together the data before transmitting it to the AP. A central processor can be a device like a computer or smartphone. This can be seen in Figure 2.

In contrast to common wireless sensor networks BANs rarely work autonomously meaning they very likely work with a user or database. An AP will allow the BAN sensors to communicate with easily accessible external networks. These networks can include the Internet or possibly another device like a cellular phone [1].

Two sub-categories of Tier-2-Communication are defined in [1], infrastructure-based architecture and ad hoc-based architecture.

Infrastructure based architecture is the most common among current BAN applications. Infrastructure based architecture assumes a limited space environment such as an office space, home, or waiting room. Centralized management and security control via the AP are key features of infrastructure based networks. The predominant disadvantage with infrastructure based networks is the constraint on physical space [1].

An ad hoc based network uses multiple APs to allow a larger network area. While BAN networks typically have a range of two meters an ad hoc based architecture allows the network to extend over considerably greater distance. The APs in an ad hoc network form a mesh structure that allows flexible wireless deployment that can be rapidly installed. An example is the immediate deployment of APs along a emergency hallway. APs can be added whenever and wherever needed without affecting the other parts of the network. This allows coverage to be added where needed at any time. [1, 5]

4.3 Beyond-BAN communication

Beyond-BAN communication, also called Tier-3-Communication extends even further. Beyond-BAN communications requires a device that bridges between the Inter-BAN and external network. This "gateway device" can be a dedicated device, or we can use a smartphone to provide a wireless, nearly uninterrupted link to the external network [1]. A nearly uninterrupted link such as this would allow several advantages. With an uninterrupted link medical personnel would have the ability to quickly and easily view the recent history alongside the current status of the patient in an emergency. This history could include up to the minute information on the condition of the patient. Emergency technicians could also gather information about the patient before the patient's arrival in the emergency room. It is also possible the medical event could have been avoided altogether by constant monitoring of the patient's condition and automated alerts.

5. HARDWARE

BANs and BSNs have two main hardware components. The first is the data collection sensors and the second is the radio platform through which the sensors connect.

The sensors in a BSN network are integral because the sensors are the data sources of the system. They typically are directly placed on the surface or under the surface of the skin, so their size is of particular interest. The physical size is one of the key aspects that allow sensors to be much less invasive than the traditional methods of gathering information. These deployment methods could help lower medical and health costs associated with data collection. [1]

5.1 Types of Sensors

Some commonly available BAN sensors include blood glucose, blood pressure, carbon dioxide (CO_2) gas sensor, electrocardiography (ECG), electroencephalography (EEG), electromyography (EMG), gyroscope, and pulse oximetry. [1]

Possibly one of the most common sensors is an ECG sensor for monitoring heart rhythm; typically being applied over the skin. In most cases electrodes will be made of silver chloride (AgCl) and can only be used for short periods of time; long-term use of these sensors may cause skin problems as well as possible sensor failure. One of the most recent developments in ECG sensors is integrating them in textiles. These electrodes can be placed in fibers and can be woven into clothes. Because this type of electrode forms to the shape of the body and skin they are much better suited for long-term monitoring. This same approach can be used for EEGs and EMGs. [1]

5.2 Challenges and Limitations

There are many hardware challenges unique to BANs and BSNs. Some of these include antenna design, power, and medium access control management.

5.2.1 Power

Power is a concern and challenge in Body Area Networks. Power is affected by the size and location of sensors within the body. The power required by a sensor can also be impacted by how the sensor is being used. A sensor that is required to constantly read and send data across the body will consume much more power than a sensor that is only required to gather data once a day.

The maximum power is also governed by specific national and international regulations. An example is the FCC's strict caps on the maximum power output of body area radio devices.

Sensors placed in the body tend to have very limited battery capacity. Operating on this low power availability is mainly achieved through low duty cycles, meaning the sensors only wake up at predetermined times. Also to increase lifespans of implanted power sources energy-efficient medium access control (MAC) protocols play an important role. [1]

5.2.2 Antenna Design

Antenna design is a problem when it comes to BANs and BSNs. Issues include physical complications like user's posture, weight loss/gain, and aging skin. Posture and weight change both affect the distance between nodes. With variable distance it becomes hard to tune the network for power and range. A good antenna design should incorporate these aspects and adapt appropriately.

Another challenge comes from implanting an antenna inside the body. All materials used must be non-corrosive and bio-compatible. The usual materials for medical implants are platinum or titanium, but these materials exhibit poor range performance when compared to a standard antenna made of copper. Another challenge when implanting an antenna in the body is shape and size, both of which are dictated by the location inside the body of the user. For example, an antenna implanted in a user's leg could be longer and less flexible than an antenna implanted in the trunk of the body, although a device implanted in the trunk of the body might be larger in surface area. This limits much of the design freedom non-BAN antennas might have.

A third major issue that must be taken into consideration is heating of fat, muscle, and skin due to the electric field of the antenna. [1]. By using low power devices and devices that only operate at certain intervals this issue can be addressed.

5.2.3 Medium Access Control

In an attempt to reduce the energy used by implanted sensors, MAC plays an integral role. It is the MAC layer that assists with addressing of devices, some aspects of security, and power saving. One method to save power involves turning off radios when sensors are not in use [1].

Another method of power conservation used in some MAC protocols is low-power listening (LPL). This is the use of channel polling to check nodes for activity. In channelling polling the node would start listening for traffic for a specified amount of time. If nothing is received during that amount of time the node will go to sleep for a different specified amount of time, saving power during the sleep period.

Recently some BAN specific MAC protocols have been proposed. Cascading Information retrieval by Controlling Access with Distributed slot Assignment (CICADA) is a low-power, wireless protocol specifically designed for high traffic BANs. Power is saved by enabling sensors to send data often instead of spending time and power buffering the data locally [1]. Instead the buffering and all processes other than reading and sending the information are moved to a remote device such as a personal server or access point.

Body sensor network MAC (BAN-MAC) is a protocol developed for BAN using a star topology. A star topology network involves a central hub which other nodes connect to. This type of network is very common and allows the unrelated nodes in the network to conserve power by preventing any information from passing through them unnecessarily. BAN-MAC allows connection using IEEE 802.15.4 and also connects to biosensors. BAN-MAC dynamically adjusts protocols to achieve the best power usage. [1]

6. SECURITY

Security of BANs and BSNs is broken into two parts. First is security at the lower wireless level. This involves encryption of information passing from one node to another. The second piece of security is at the user level. This involves passwords and methods of access to the BAN. In this section we will first look at general wireless security goals, followed by wireless communication security using IEEE 802.15.4 and then user level security.

6.1 General Wireless Security Goals

Security of BAN and BSN depend on what radio platform is used. In this discussion we will see features that can also be applied to many wireless radio platforms.

The first essential feature is message integrity. Message integrity means a message must make it from the sender to receiver without tampering. If the message is indeed tampered with the receiver should be able to detect this and reject the message. Another feature is confidentiality. Having confidentiality means preventing unauthorized parties from gaining even partial information about the contents of the message being sent. Confidentiality is usually achieved with encryption. A third feature is called replay protection. Some attacks come from an unauthorized party re-sending a mes-

1 byte	2 bytes	1 byte	0/2/4/10 bytes	0/2/4/10 bytes	variable	2 bytes
Len.	Flags	Seq. No	Dest. Address	Source Address	Data payload	CRC

(a) Data packet format

1 byte	2 bytes	1 byte	2 bytes
Len.	Flags	Seq. No	CRC

(b) Acknowledgment packet format

Figure 3: 802.15.4 data and acknowledgment packet formats. Taken from [7].

sage that was sent on the network previously. This message will have the correct encryption information because it is a copy. A network that has replay protection will recognize these repeat messages and reject them. Repeat protection can be achieved by assigning each message a monotonically increasing sequence number. If a message is received with sequence number not greater than the sequence number of the previous messages will be rejected. [7]

6.2 Important IEEE 802.15.4 Security Features

The IEEE 802.15.4 protocol has a few specific security features such as packets, security suites, and keying models used by the suites are three of the major features.

6.2.1 Packets

Two packet types are important in 802.15.4 security: data packets and acknowledgement packages. A data packet, as seen in Figure 3, can have a variable length. A node uses data packets to pass messages to one or more other nodes. Each data packet has a fields to indicate type, security, and checksum. We can also see there is a one byte sequence number serving as an identifier if the sender requests acknowledgment. A two byte Cyclic Redundancy Check (CRC) checksum serves to protect against transmission errors [7]. The sending device calculates the check value based on what is included in the packet. When the packet is received by the intended node the node will calculate the check value of the packet it receives. The node will then check to see if the two values are the same. Identical values would indicate the packet of information received is likely the same as what was sent.

The acknowledgment packet, also shown in Figure 3, is returned to the sender by the recipient of the data packet only if acknowledgment flag in the data packet was true. An acknowledgment packet structure is much simpler than the data packet. The packet has two bytes for flags much like the data packet, a one byte sequence number, and a two byte checksum. [7]

6.2.2 Security Suites

The 802.15.4 protocol provides various security suite options. The choice of security suite will be made at the application level in the BAN or BSN. Each suite has an option for a 4, 8, or 16 byte long message integrity code (MIC), used to provide authentication and integrity. The sending node would include the MIC in the packet and the receiving node would check the MIC to ensure it matches the expected code. The longer this code, the harder it is to forge a correct integrity code. Even with an 8 byte MIC the chance of correctly guessing is 2^{-64}. The tradeoff for more security is increased packet size. [7]

An application is able to decide what security will be used based on the sender address and receiving address. 802.15.4 radio chips all have access control lists that are used to store security policies and keying information. If the security flag is true, the destination address is looked up in the access control list ACL table. Upon receiving a packet the media access control layer checks the security flag to determine if any type of security has been applied to the packet. [7]

6.2.3 Keying Models

A keying model determines the correct key a node will use when it transmits a message to another node. In this section we will list and briefly explain a few keying models that might be used with 802.15.4.

The first keying model we will look at is called network shared key. In this model a single network-wide key is held by each node. Here key management is easy because all nodes have the same key. Having easy key management makes this model attractive, but if one node is compromised, the entire network is in turn compromised.

A slightly more secure method is called pairwise keying. This method limits the scope of a compromise. In pairwise keying each pair of nodes shares a different key. This means a compromise will only affect the past and future messages between the compromised pair of nodes. The overhead here is key management. If a nodes communicates securely with many other nodes, the node will need to store security information for each of those nodes. This can be restrictive when nodes have minimal storage resources to work with. [7]

Group keying can also be used. Group keying allows a tradeoff between network shared keying and pairwise keying. Group keying simply allows multiple nodes in a group to have a shared key that can be used when communicating with each other. This creates groups that can be compromised but limits the scope of the compromise only to that small subset of the network.

In the end "The keying model that is most appropriate for an application depends on the threat model that an application faces and what types of resources it is willing to expend for key management." [7] Many situations are different and require different wireless communication security.

6.3 User Level Security

Security challenges become even more prominent in a medical BSN application, where clinical, emergency, and unauthorized access are all very important. During a clinic visit a patient's doctor must be able to access the sensors in the BSN to gain information or adjust the settings of the network. In an emergency it is very important for medical personnel to gain access to any sensors or devices implanted in the body. Especially in the medical BSN, unauthorized access is very undesirable and could possible be threatening to a patient's health.

6.3.1 Passwords

Passwords are traditionally used to protect access to tools or information. This creates a natural tendency to use this form of security. It is well known that many individuals forget their passwords, especially when the individual does not consistently use them. Users often write their password in an easy to remember place. Both of these issues pose huge risks in a BSN. Having users that are unable to produce their password could potentially be life threatening. This problem could be seen in an emergency where the individual is physically unresponsive. It is at this point a password approach might fail.

One solution to this issue is to alter the body of the patient. This might include a tattoo with the password key. This approach however makes it very hard to revoke and otherwise change passwords. Another challenge is the perception of tattoos by some patients. A statement in [2] indicated that the patient, "objected that having a tattoo would present a persona to others that would be inconsistent with the one that she wished to project."

Another solution would be to require the use of a medical alert bracelet. This would solve the issue of password revocation but involves altering a patient's appearance or lifestyle. This again was of concern the some patients who preferred not to wear a medical bracelet due to their appearance. Another subset of individuals said they would rather avoid a reminder of their condition, both to themselves and others around them. There was also slight concern of human readability and possible misplacement when having a password that was printed on the wristband. [2]

6.3.2 Proximity bootstrapping

Proximity bootstrapping would by used be medical personnel and involves the use of the device outside the body. When placed on the body of a patient the device would wirelessly negotiate a temporary key. Patients particularly liked this solution because the user must give implicit consent by allowing the person reading information to place the device against their skin. This solution was also well accepted because medical personnel will be able to read information from the patient if the patient is unresponsive. [2]

7. CONCLUSIONS

BANs and BSNs are becoming an interesting solution in many scenarios where rapid data collection may be crucial. Recently the size and price of BAN and BSN hardware has dramatically decreased which allowed these type of networks to become more feasible.

Antenna design and power management are two of the most interesting issues when it comes to BANs and BSNs, due the close proximity to or implantation of components in the body.

BANs and BSNs also pose unique security challenges both in terms of low level wireless data transfers and user level passwords and security. The challenges related to security can possibly be addressed both by the use of the IEEE 802.15.4 protocol and creative uses of new body modification and hardware like tattoos or proximity devices.

The world of low power networking is always changing and will undoubtably lead to much more common medical, military, and even automotive data collection devices in the not so distant future.

8. REFERENCES

[1] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung. Body area networks: A survey. *Mob. Netw. Appl.*, 16(2):171–193, Apr. 2011.

[2] T. Denning, A. Borning, B. Friedman, B. T. Gill, T. Kohno, and W. H. Maisel. Patients, pacemakers, and implantable defibrillators: Human values and security for wireless implantable medical devices. In *Proceedings of the 28th international conference on Human factors in computing systems*, CHI '10, pages 917–926, New York, NY, USA, 2010. ACM.

[3] Y.-K. Huang and A.-C. Pang. A comprehensive study of low-power operation in IEEE 802.15.4. In *Proceedings of the 10th ACM Symposium on Modeling, analysis, and simulation of wireless and mobile systems*, MSWiM '07, pages 405–408, New York, NY, USA, 2007. ACM.

[4] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester. A survey on wireless body area networks. *Wirel. Netw.*, 17(1):1–18, Jan. 2011.

[5] C. Liolios, C. Doukas, G. Fourlas, and I. Maglogiannis. An overview of body sensor networks in enabling pervasive healthcare and assistive environments. In *Proceedings of the 3rd International Conference on PErvasive Technologies Related to Assistive Environments*, PETRA '10, pages 43:1–43:10, New York, NY, USA, 2010. ACM.

[6] S. M, E. A. Soujeri, R. Rajan, and H. A. I. Design of a Zigbee-based RFID network for industry applications. In *Proceedings of the 2nd international conference on Security of information and networks*, SIN '09, pages 111–116, New York, NY, USA, 2009. ACM.

[7] N. Sastry and D. Wagner. Security considerations for IEEE 802.15.4 networks. In *Proceedings of the 3rd ACM workshop on Wireless security*, WiSe '04, pages 32–42, New York, NY, USA, 2004. ACM.