Security in Low Energy Body Area Networks for Healthcare

Lav Gupta, lavgupta at wustl.edu (A paper written under the guidance of Prof. Raj Jain)

Download 

Abstract: Healthcare expenses are a growing concern in most countries. This has forced medical researchers to look for non-intrusive and ambulatory health monitoring of patient's vital signs. The objective is to reduce patient visits and the use of medical and support staff for frequent examinations. Body Area Networks(BANs) consist of implanted, or worn, tiny health monitoring sensor nodes so that the vital body parameters and movements of the patient can be recorded and communicated to the medical facilities for processing, diagnosis and prescription. BANs are required to have small form and low power consumption. Reducing energy consumption of the sensor and communication equipment is one of the key research areas. It is also important for BANs to be secure, protected and reliable. Failure to obtain authentic and correct medical data may prevent a patient from being treated effectively, or even lead to wrong treatments. As patient identity can be obtained by correlating physiological information, privacy concerns must be addressed for wide acceptance of the technology. While security is paramount, the cost of implementing security techniques in BANs may be prohibitive. It, therefore, becomes necessary to find cryptographic solutions that consume less energy. Research efforts are being made to reduce the cost of cryptography used in BANs. In this paper we discuss the current and future security solutions for low energy BANs.

Keywords: Wireless Sensors, Body Area Network, Energy Efficiency, Security, Health, Implanted Medical Device, Symmetric Encryption, Public Key Cryptography, Elliptic Curve Cryptography

Table of Contents

1. Introduction

Healthcare expenses are a growing concern in most countries. As people age, their dependence on the healthcare system increases. People above the age of 60 years show larger dependence on the health care system because of increased preponderance of age related diseases like cardiac ailments, respiratory problems, arthritis, neurological diseases and dementia. According to World Health Organization (WHO), by the year 2020 people older than 60 years will outnumber children below 5 years. By 2047 people 60 and above will be 2 billion, up from 841 million today. About 80% of this elderly population will be in low and middle-income countries. According to the US Bureau of the Census, in US alone elderly people are expected to double to 70 million by 2025. This would cause a tripling of the healthcare expenditure to about $ 5.4 trillion from the 2004 figure. This represents a staggering 20% of the Gross Domestic Product (GDP)! A

fundamental change is needed in the way in which healthcare is delivered [Ullah12] [Chatterji14]. In this section we look at BAN as an agent that could provide a revolutionary change in the way the medical system works.

A large part of the expense in providing healthcare is attributed to patients' visits, indoor treatment and need for continuous monitoring of the chronically ill patients. This has forced medical researchers to look for methods for non-intrusive and ambulatory health monitoring of patient's vital signs. The idea is to reduce patient visits and consequent use of medical and support staff for conducting frequent tests like Electro Cardio Gram (ECG), blood pressure or blood sugar levels. Besides, it is also desirable to have the capability of monitoring patients, while they go about their daily routines, and updating their data in real time over the Internet. This would help the doctors and other medical staff to take into account updated records for taking timely decisions that are vital for patients' health and well-being. Body Area Networks (BANs) provide the capability of achieving these goals and provide an economical solution to the challenges that healthcare system faces today.

Body Area Networks (BANs) consist of implanted (inside the body) or worn (over the body) tiny health monitoring sensor nodes for recording vital body parameters and movements of the patient and communicating them to the medical facilities for processing, diagnosis and prescription. These networks are known by various names: Body Area Networks (BANs), Body Area Sensor Networks (BASNs) and Wireless Body Area Networks (WBANs). We shall use the term BANs in this paper. These BANs provide long term health monitoring of patients under natural neurological and physiological conditions without constraining their normal activities. BANs have the potential to become part of all the facets of a smart and economical healthcare system viz. diagnostics, prescription, monitoring intake and reaction to medicines, taking care of chronic conditions, supervising recovery from surgeries and handling emergencies. Fig. 1 shows the BAN and associated infrastructure. We shall see in this paper the current status and future directions of research in making the power constrained body area networks secure.

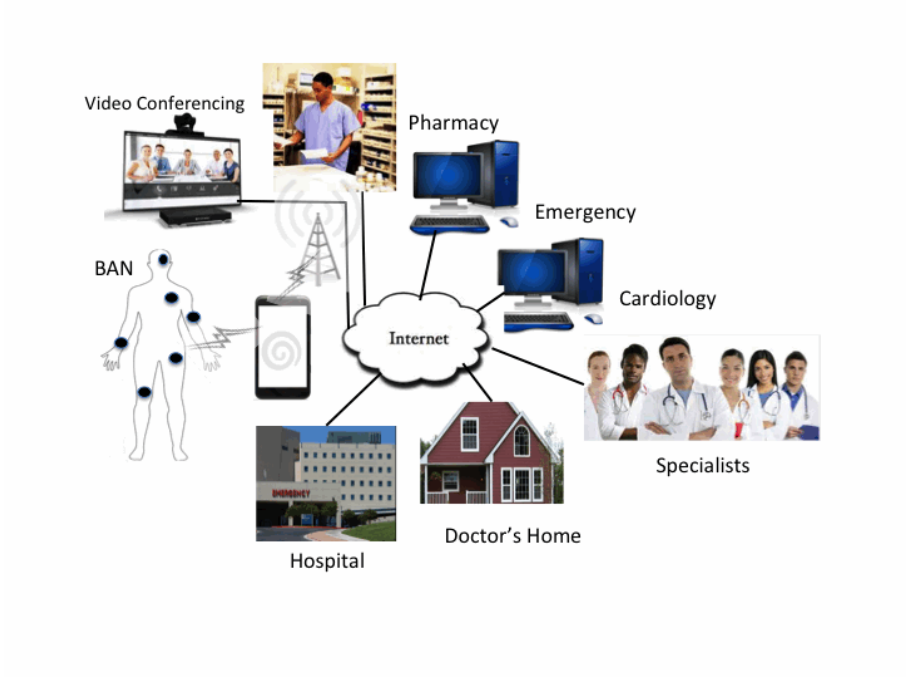

Fig. 1: BAN and Associated Systems

A number of developments have taken place in recent times that have made Body Area BANs possible. These developments include advancements in the field of wearable low power medical sensors that can be integrated with fabric that patients can wear without any kind of discomfort. Along with these sensors, advances in wireless communication and data processing have made wireless Body Area Networks a promising technique that has the potential or revolutionizing the way the healthcare will be sought and delivered. A number of challenges need to be over come to make it widely acceptable by hospitals and patients alike. Section 2 deals with the background material including challenges to implementation of BANs, their application areas and starndards. Section 3 talks about the energy efficiency issues in BANs. How security and privacy is handled is taken up in Section 4 and the steps that have been taken to incorporate low energy cryptography in BANs in Section 5. Section 6 gives the summary and the future research directions in security and energy related issues of BANs.

2. Background

In this section we would discuss the challenges in implementing BANs, their applications and the relevant standards.

2.1 Challenges in implementing BANs

While BANs have immense potential, there are quite a few challenges to its large-scale inclusion in the healthcare regime and mass acceptance. These challenges and what will take to mitigate them is discussed below:

1. Peculiarities of human body: BANs are required to be highly efficient and reliable and at the same time they have to be small, lightweight and low power consuming. While they share common research ground with the general field of wireless sensor networks (WSNs), BANs have their unique challenges. The human body has smaller form, requires different type and frequency of monitoring and most importantly it reacts to any probing and changes in its

environment. The detrimental effect introduced by human skin on low power radio signal also needs to be taken care of. Presence of wires is not desirable in sensors worn over the human body. For example, in the early ECG equipment, the electrodes are wired to a remote receiver. For example the ECG electrodes need to have individual radios that is still a challenge. Sensor nodes can move with regard to each other, for example a sensor node placed on the wrist moves in relation to a sensor node attached to the hip. This requires mobility support [Latre11]

2. Scale, scope and size: As compared to other sensor based applications scale and scope of BANs are different. While in application like agriculture or wild life monitoring the number of sensors would be large and spread out over a large area. Comparatively in BANs the number of sensors would be very small and the area available to deploy the sensor would just be in centimeters or even millimeters. A Sino-atrial node sensor could just be a single tiny sensor that has to be deployed in a couple of millimeters of space. In many other applications accuracy and data availability requirements may not be high or may perhaps be met by a large number of redundant nodes. In BANs this accuracy and reliability is required to be attained with less redundancy, sometimes with just one node! Another challenge is to maintain small battery size and still have a long network life. A heart pacemaker may be required to work for 5 years for more, as replacement is invasive and may be uncomfortable to patients
3. Communication: The communication sub-system is the most energy consuming part of the BAN. Challenge is to optimize signal collection, processing and transmission, management of radio channel for sharing with minimal contention between sensors, power management to maximize battery life [Chen11]. Availability of appropriate spectrum is another challenge faced in large-scale deployment of BANs. The industrial, scientific, and medical (ISM), wireless medical telemetry service (WMTS), ultra-wideband (UWB), or MedRadio wing bands (401â€“402 MHz and 405â€“406 MHz) can be exploited to support on-body communications. However, thee bands are crowded or have other restrictions. Higher power technologies swamp the signal of low-power BAN devices that then suffer severe performance degradation making these bands less appealing for high-fidelity medical applications. Exploiting UWB for wearable applications brings forward the issue of coexistence with high-data-rate multimedia applications. These factors have prompted the FCC to consider opening up 2360â€“2400 MHz spectrum for medical BANs [Patel10].
4. Energy: The new generation sensor devices for BANs need to have improved circuit design, processing and communication features to minimize power consumption and size. Energy limitations of the BAN deployed should be taken into consideration while deciding the level of monitoring. Energy harvesting is important in BANs as in any low energy system. However, in field deployed systems energy can be harvested from sun and wind. In BANs, if alternate sources are indicated, energy would need to be harvested from body movements and vibration. Energy issues of BANs will be discussed in more details in Section 2.
5. Security and privacy: There is a strong case for security and privacy in BANs because of life threatening implications. Patients' data must be securely obtained and transmitted. It should not be accessible to unauthorized persons at any stage. Inter-BAN interference, leading to mix-up of patients' data, needs to be avoided. If the data were compromised then patients' health would be threatened. It is also important to not to reveal patient's personal identification and in many countries required by law. Physiological data like an iris scan may reveal personal identity even if the name is not indicated. Loss of data or low quality of service(QoS) in BANs could lead to incorrect diagnosis and endanger human life. These and other security related issues are discussed in in more details in Section 3.
6. Non-technical factors: Legal, regulatory, and ethical issues are play an important role in adoption of BANs. Their user friendliness, comfort, convenience, and acceptance decide their mass adoption. Support from the key stakeholders including medical electronics industry, patients, physicians, caregivers, policy makers, patient advocacy groups, and insurance companies is vital for BANs to become a pervasive technology [Hanson09].

2.2 Applications of BANs

While healthcare is perhaps its most important application, BANs can actually be used in several applications including sports, interactive gaming, military and security. In this paper we will focus on healthcare. BANs enable a wide range of new applications such as ubiquitous health monitoring (UHM), computer-assisted rehabilitation, emergency medical response system (EMRS), and even promoting healthy living styles. In UHM the BAN frees people from visiting the hospital frequently, and eases the heavy dependence on a specialized workforce in healthcare. Thus, it is a desirable technique to quickly build cost-effective health-care systems, especially for countries that are short of medical infrastructure and well-trained staff. In addition, in an EMRS temporary BANs can be rapidly deployed with minimum human effort at a disaster scene so that the vital signs of injured patients can be monitored and reported to the remote health center in time, which is potentially capable of saving the lives of numerous people. Fig. 2 shows monitoring through BANs.

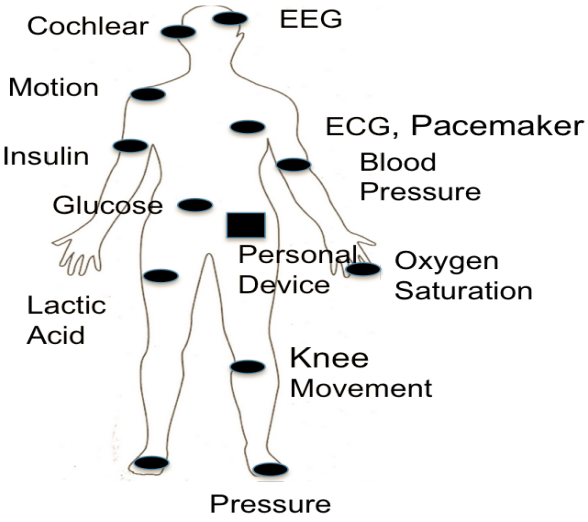

Fig. 2: Patient Monitoring Through BAN

One way to categorize medical applications of BANs is based on the method of monitoring: discrete or continuous. In discrete monitoring the devices are remotely triggered at appropriate times for recording parameters like oxygen saturation of the blood. Continuous monitoring, on the other hand, is required in many cases like cardiac conditions and neurological disorders. Continuous monitoring is valuable when transient abnormalities are otherwise difficult to capture. For instance, many cardiac diseases are associated with episodic rather than continuous abnormalities, such as transient surges in blood pressure, paroxysmal arrhythmias or induced episodes of myocardial ischemia and their time cannot be accurately predicated. Frequent monitoring in diabetics enables proper dosing of medicines and reduces the risk of fainting and in later life blindness, loss of circulation and other complications [Ullah12].

Another method of classifying BANs is based on the location of the sensor: implanted inside the human body or over the body. In-body applications include, monitoring and reconfiguration of pacemakers and implantable cardiac defibrillators, control of bladder function, and retinal implants. On-body medical applications include monitoring blood pressure, electro cardiogram at rest and impost, temperature and respiration. Furthermore, on-body non-medical applications include monitoring forgotten things, establishing a social network, and assessing soldier fatigue and battle readiness.

BANs are human-centric and can facilitate highly personalized and individual care. BANs can offer real-time sensing, processing and control and can be vital in preserving body functions and human life. BAN researchers are already working to improve deep brain stimulation, heart regulation, drug delivery, and prosthetic actuation. BASN technology will also help protect those exposed to potentially life-threatening environments, such as soldiers, first responders, and deep-sea and space explorers [Chen11].

Applications vary in their use of sensor nodes. Due to strong heterogeneity, the data rates vary widely, ranging from a few bps to video streams of several Mbps. Data can also be sent in bursts, which means that it is sent at higher rate during the bursts [Latre11]. Table I shows sensors used for different applications along with their indicative data rates.

Table I BAN Applications, Sensors and Data Rates

Medical condition	Type of sensor	Data rate	Description
Muscular atrophy	Accelerometer/gyroscope	35kbps	Faulty postures and movements
Diabetes	Blood glucoseâ€¨	1600bps	Blood glucose levels post partum and fasting
Cardiac, hypertension	Blood pressure	1000bps	Non invasive systolic, diastolic and venous pressure
Pulmonary, Asthma	CO2 gas sensor	10kbps	Carbon dioxide and oxygen content in the blood
Cardiac arrhythmias and other abnormalities	ECG sensor	12 lead:288kbps, 6lead:71kbps	Electrical activity of the heart
Neurological	EEG sensor	86.4 kbps, deep brain stimulation: 1Mbps	Electrical activity of the brain
Neuromuscular abnormalities	EMG sensor	1.536Mbps	Electrical activity in response to a nerve's stimulation of the muscle
Cyanosis	Pulse Oximetry	16bps	Oxygen delivery to the peripheral tissues
Ophthalmological problems	Retinal sensors	50-700kbps	Chemical, nerve, cell level observation
Ear disorders	Cochlear sensors	200kbps	Ear effusions and perfusions
Gastric abnormalities	Endoscope: 1 Mbps	1 Mbps	Ulcers in the gastric pathway

2.3 Standards for BANs

Interoperability, low cost, and user convenience are key enablers for the mass market. To enable true plug-and-play interoperability, all layers of the protocol stack, application profiles, and data exchange formats have to be standardized. Until relatively recently BAN deployments relied upon general standards for WSNs and other wireless networks. This situation was altered with publication of IEEE 802.15.6 standard in the year 2012. We will discuss here this standard and its precursors IEEE 802.15.4 and Zigbee.

1. IEEE 802.15.4: Many current implementations of BANs use IEEE 802.15.4 [Latre11]. This standard has not been developed specifically for BANs but has been adapted to suit BAN requirements. IEEE 802 standard series is for local and metropolitan area networks. IEEE 802.15.4 was developed in 2006 and updated in 2011 for low rate personal area networks (LR-PANs). LR-PAN Wireless personal area networks (WPANs) are used to convey information over relatively short distances. Unlike wireless local area networks (WLANs), connections effected via WPANs involve little or no infrastructure. This feature allows small, power-efficient, inexpensive solutions to be implemented for a wide range of devices. This standard defines the physical layer (PHY) and medium access control (MAC) sub layer specifications for low-data-rate wireless connectivity with fixed, portable, and moving devices with no battery or very limited battery consumption typically operating in the personal operating space of 10 m. The standard provides for ultra low complexity, ultra low cost, ultra low power consumption, and low data rate wireless connectivity among inexpensive devices. The raw data rate ranges 20 to 250 kb/s and can satisfy a set of applications. The main objectives of an LR-WPAN are ease of installation, reliable data transfer, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol [IEEE11]
2. Zigbee: ZigBee technology offers efficient, low-power connectivity and ability to connect a large number of devices into a single network. It uses the globally available, license-free 2.4GHz frequency band. It enables wireless applications using a standardized set of high level communication protocols sitting atop cost-effective, low-power digital radios based on the IEEE 802.15.4 standard for wireless personal area networks. It defines the network, security and application framework for an IEEE 802.15.4-based system that defines PHY and MAC layers. ZigBee offers low-latency communication between devices without the need for network synchronization delays. It creates robust self-forming, self-healing wireless mesh networks. The ZigBee mesh network connects sensors and controllers without being restricted by distance or range limitations. ZigBee mesh networks let all participating devices communicate with one another, and act as repeaters transferring data between devices. ZigBee Alliance has also developed the ZigBee Health Care public

application for use by assistive devices operating in non-invasive health care. It provides an industry-wide standard for exchanging data between a variety of medical and non-medical devices [Zigbee10].

3. IEEE 802.15.6-2012: IEEE 802.15.6 specifies a short range, low power and reliable wireless communication protocol for use in close proximity to or inside a human body(actually it is not limited to humans). These devices need to communicate with their remote controllers. It uses ISM and other bands as well as frequency bands in compliance with applicable medical and communication regulatory authorities. It allows devices to operate on very low transmit power for safety to minimize the specific absorption rate (SAR) into the body and increase the battery life. It supports quality of service (QoS) to provide for emergency messaging. Since some communications can carry sensitive information, it also provides for strong security [IEEE12].

3. Energy issues in BANs

In this section we will examine in details the energy requirement of BANs, consequences of heat dissipation and energy conservation.

3.1 Requirement from Energy Sources

Energy consumption can be divided into three domains: sensing, communication and data processing. The wireless communication is usually the most power consuming among the three. The size of the battery used to store the needed energy is in most cases the largest contributor to the sensorâ€™s size and weight. As a result batteries are kept small for which energy consumption of the devices needs to be reduced. At the same time, some BANs need to continuously operate for months or years without intervention or battery change. The need for replacement or recharging induces a cost and convenience penalty. This is especially true for implanted devices, as intervention would mean surgical procedures. An implanted pacemaker, for example, would require a lifetime lasting more than 5 years. Lithium batteries work well for handheld electronics, but their capacity is limited in small BAN enclosures. The need to replace or recharge these batteries frequently makes BAN use less desirable. Super-capacitors and carbon-nanotube-based energy stores have great potential to improve battery capacity, but have not yet matured to commercial availability. The search is on for the ideal battery for BANs [Diop13].

3.2 Energy Dissipation and Tissue Safety

During operation, the devices dissipate heat that is absorbed by the body. In case of implantable sensors, the surrounding tissue gets heated up. If the devices become very hot, the tissue may suffer burn damages. In order to limit heat dissipation and increase battery life, the energy consumption needs to be limited to the minimum. Radiation is another concern. The amount of power absorbed by the tissue is expressed by the specific absorption rate (SAR). Since the device may be in close proximity to, or inside, a human body, the localized SAR could be quite large. The localized SAR into the body must be minimized and needs to comply with international and local SAR regulations [Patel10].

3.3 Energy Conservation and Renewal

1. Energy Conservation: In BANs the sensor nodes are low power devices that collect body parameters and communicated them to the central server. In case of long term monitoring it is important that the network has high-energy efficiency and reliability. In BANs, sensor nodeâ€™s transceiver is one of the dominant energy dissipation sources. It is necessary for long battery life that the data acquisition, storage, processing and communication operations are energy efficient. This will also allow the size of the battery to be smaller. Multiple and dynamic power management schemes can be used to prolong lifespan of sensor nodes [Rahim12].

The IEEE 802.15.4 defines some power management mechanisms for edge devices and none for forwarding devices. Thus, most networks built on this standard do not include power management. Some form of duty cycles have been tried such that devices communicate in pre-defined time slots or coordinate communication in some way. Any protocol that is adopted for BAN networks would have to build in energy conservation features at least at the physical and MAC layers. At the physical layer, however, power savings should be attained without compromising fidelity. Ideally there should be a linear relation between the data rate and power consumption so that energy per bit is constant. Seamless connectivity should be maintained when the nodes are mobile. Fast changeovers from transmit to receive and between sleep and wakeup cycles would conserve power.

There is larger scope of energy savings through innovative techniques at the MAC layer. Some MAC layer protocols that have been proposed specifically for BAN that contribute to conservation of energy are given in Table II [Fang09][Timmons09]:

Table II Energy Efficient MAC Protocols for BANs

Protocol	Designation	Principle	Description
CICADA	Cascading Information retrieval by Controlling Access with Distributed Slot Assignment	Multi-hop wireless	All sensors send data, high traffic capability, low delays, no local buffering resulting in small sensors
BAN-MAC	Body Area sensor Network-Media Access Control	Dynamic adjustment of parameters	Ultra Low power, star topology
H-MAC	Heartbeat driven Media Access Control	TDMA based	Uses human heartbeat for synchronization and increases sleep time of radios for energy conservation
BodyMAC	Body Media Access Control	TDMA based	Node remain in sleep mode when there is no data to send
MedMAC	Medical Media Access Control	TDMA based	Variable time slots according to sensorâ€™s requirement

2. Energy Renewal: The lifetime of a node can be enhanced by scavenging energy during the operation of the system. If the scavenged energy is larger than the average consumed energy, such systems could run eternally. However, energy scavenging will only deliver small amounts of energy. A combination of lower

energy consumption and energy scavenging is the optimal solution for achieving autonomous Body Area Networks. For a BAN, energy scavenging from on-body sources such as body heat and body vibration seems very well suited. In the former, a thermo-electric generator (TEG) is used to transform the temperature difference between the environment and the human body into electrical energy. The latter uses, for example, the human gait as energy source. Energy can also be harvested from external sources like sunlight. Recharging batteries with harvested energy could not only extend battery life, but also simplify BAN use. Research challenges are formidable because of node placement variability and uncertainty about the userâ€™s exposure to ambient energy. Finally, the available harvestable power will differ substantially among individuals, which means it will be necessary to carefully match application profiles to activity levels in the target demographic [Ali13].

4. Security in BANs

The patient related data generated, stored and communicated by BANs is critical for medical diagnosis and treatment. Importance of securing this data, therefore, cannot be overemphasized. If the data is corrupted or pilfered, the effect could range from ineffective treatment of patients to mistreatments threatening patients' lives. For widespread acceptance by patients, as an important part of the healthcare system, BANs must also address privacy concerns. Access to patient data must be restricted to authorized uses and according to the law of the country in question. The distributed nature of data in BANs makes implementing security and privacy difficult. It is important to deal with these issues even when the node is compromised or fails. Use of encryption and cryptography is gaining currency for enforcing access control to protect the privacy of patients [Saleem10] [Selimis11].

In WSNs, the security mechanisms (encryption, decryption, signing data, verifying signatures) are the main factors that influence power consumption by sensor nodes. Limited energy prohibits the use of complex security mechanisms for message expansion. BANs are even more energy and storage constrained, therefor, the security protocols designed for WSNs cannot be applied to BANs. Moreover, the key management protocols for WSNs will not work as efficiently as the protocols specifically designed for BANs [Ali13], e.g., currently the public key-based protocols is difficult to implement in BANs. While both symmetric key management strategies for secure trust establishment and public key-based key management schemes have been used in WSNs, it is necessary to well balance security level and the associated energy consumption overhead. Each of these schemes has its own limitations for BANs. In this section the infrastructure for meeting the security requirements and the security mechanisms used in BANs [Lim10].

4.1 Security Requirements

Security and privacy of the patients' physiological and neurological data generated by BANs are two indispensable components BANs. These requirements together ensure that data is securely stored, communicated and accessed by authorized persons. To this end, data confidentiality, integrity and availability are key requirements [Yoon14].

- Confidentiality: The data needs to be kept secure during storage in BAN noes or the central server. Even if the node or server is compromised the attacker should not be able to gain any information.
- Data Integrity refers to ensuring that unauthorized changes to the data cannot be made during storage or transmission. Any malicious changes should be detected before use and the appropriate persons alerted. This can be achieved through data authentication protocols. Data authentication allows a receiver to verify that the claimed sender sent the message. It is essential to verify that the data was sent by the trusted sensor and not by an adversary that tricked the node or the controller into accepting false data. In a BAN, data authentication can be achieved by using symmetric techniques. The node and the controller share a secret key that is used to compute a Message Authentication Code (MAC) of all data. When data arrives with correct MAC, the controller knows that the trusted nodes have sent it.
- Data availability means that correct data is available to the genuine users. Failure to receive correct data may become life threatening. It is also necessary to authenticate any exchange of data with other machines or humans. If adversaries are able to capture critical nodes, patients health would be at stake. Thus in case of criticality, the function may be transferred to another node(s).

Thus, the data stored in a distributive manner in the BAN nodes has to meet, sometimes contradictory, requirements. They should be secure, be securely transferred to the central server when the patient arrives at the hospital or other designated times through the internet, latency should be controlled and updated data should always be available to the physician for timely diagnosis and treatment. Beyond the basic requirements for security and privacy mentioned above some other requirements are as follows[Diop13]:

- Access control: The type and amount of data available to different stakeholders like physicians, support staff, pharmacy and the insurance agencies needs to be clearly controlled. The system should allow different access privileges for various users. If should be possible to implement granular data access policy based on usersâ€™ roles.
- Data Freshness: malicious adversary may replay old data. Along with confidentiality and integrity it is important to ensure that the data is sent in the order it is generated. There are two types of data freshness: weak freshness, which guarantees partial data frames ordering but does not guarantee delay, and strong freshness, which guarantees data frames ordering as well as delay. Some applications like blood pressure monitoring may work well with weak freshness while strong freshness is required during synchronization, e.g., when the controller transmits a beacon.
- Scalability: As the network grows and the number of users becomes larger the system should scale without undue latency. This requires that the computational and storage overheads should be controlled. It should not be resource intensive to implement access policies and management overhead should also be kept under check.
- Flexibility: The patient may change hospitals or doctors and it should be possible to easily transfer central servers and access controls. In case of emergencies physicians who have not seen the patient before need to be immediately authorized. The system should also handle contingencies relating to patient being unconscious or mentally unable to control operation of the BAN. Inability or irresponsiveness in adapting the access rules may threaten a patientâ€™s safety.
- Accountability and non-repudiation: The sender of a message should not be able to falsely deny later that he sent the message, and this fact should be verifiable independently by a third-party without knowing too much about the content of the disputed message(s).
- Secure key distribution: This is necessary to allow encryption and decryption operation for achieving the desired security and privacy. The controller

should be able to perform secure association and dissociation of nodes.

4.2 Security Infrastructure

BANs require a security infrastructure to keep data secure and reliable and protect patients' privacy. However, due to the extreme energy scarcity, bandwidth and storage constraints of the nodes, conventional solutions are not applicable. To design data security and privacy mechanisms for BANs one must overcome a number of challenges, including how to make tough balances between security, efficiency, and practicality. Stringent resource constraints on devices within a BAN, especially the sensor nodes, basically require the security mechanisms to be as lightweight as possible. Practical issues, such as conflicts between security, safety, and usability, also need to be considered carefully. For example, in order to ensure legitimate access to patients' data under time sensitive scenarios such as emergency care, the access control mechanisms should be context-aware and flexible.

Security requirements often vary with application and context, but in general, security for nodes should primarily focus on the protection of the data itself and network connections between the nodes and the server. As discussed confidentiality, integrity and authentication are the most important data security concerns. When considering the network itself, we need have an adapted media access control and often there is need to conceal the physical location of the nodes. Defense has to be set up against malicious attacks on the nodes, denial of service attacks, node capturing, and node injection. Consequence of any of these attacks may be life threatening in body area networks.

Because of the distributed nature of the BANs they tend to be extremely vulnerable to simple node attacks, weaknesses in a subsystem can easily be exploited to mount attacks on the whole network, even beyond the base station or â€œsinkâ€. So itâ€™s crucial to design smart node networks with security considerations as design requirements and not as as an add-on feature of the system. Security will always add some overhead, which will lead to increased power requirements and add on security measures are simply not safe. Tight integration of security techniques in processing and communications simply allows for more efficient use of scarce resources.

Security techniques implemented in BANs would usually have a key management infrastructure. Though necessary, key management is usually considered a primary obstacle to true security for BANs. In other words, the defining characteristics of wireless body area networks conspire to make it difficult for two nodes to share a secret key, a basic requirement of encrypted communications. The best method for key management on the Internetâ€”RSA or Diffie-Hellman based public key cryptographyâ€”even elliptic curveâ€”is untenable on these networks, at least in terms of energy cost of processing, storage and communications. For networks that are infrastructure less, nodes canâ€™t rely on a central security server like, say, a Kerberos server, much less a Public Key Certificate Server. If public key is not an option, a single secret key can be loaded onto all of the nodes but in this case capturing a single node would compromise the entire network. Another approach is to preload that single key, then establish â€œlink keysâ€ unique to every pair of nodes based on the original secret key and then destroy the original secret key. This scheme is not scalable.

Alternatively, the trusted central server can establish link keys with each node, but this is difficult to implement in many networks because it requires time synchronization across nodes, besides which, the trusted central server becomes a single point of failure for the entire network. Random key pre-distribution protocols have also been suggested. If the key is large enough, then every node can establish connections with at least a few others and thereby create a secure network containing all objects. The downsides to this approach include a requirement for a trusted base station, and tamper resistant hardware in each node to conceal the keys that is difficult to achieve.

The BAN nodes have multiple functions. They act as data collectors, processors, and as traffic forwarders for other objects in the network. If public key infrastructure is not established then a common approach is to periodically disseminate fresh keys to nodes. There is risk of interception during dissemination. A malicious user could paralyze these networks by either (1) capturing a single object (node) and extracting the secret keys or (2) modifying the communications code of a captured object. Tamper-resistant hardware could mitigate these concerns (to protect keys and routing functions) but at significant added expense. For these reasons, many security functions on sensors are relegated to software [IPSO10]. In any case whatever hardware, codes and procedures are implemented would need to be individually and â€˜systemâ€™ tested thoroughly before the system is used on humans.

4.3 Security Mechanisms Used in BANs

There are many security schemes proposed for a traditional Wireless Sensor Network (WSN) but few of them can be embedded in a BAN. For example, Security Protocols for Sensor Networks (SPINS) provide data confidentiality, two-party authentication and data freshness, which can be implemented in BAN nodes with low-power computation [Kumar13]. Generally, the application layer is used to explicitly enable the security by adjusting certain control parameters. For example, in IEEE 802.15.4 the application has a choice of security modes that control the different security level [Diop13]. Each security mode has different security properties, protection levels, and frame formats. The IEEE 802.15.4-based security modes can be improved for a BAN according to the application requirements.

The security depends on the size of the MAC frame that can be 32, 64, or 128 bits long. In case of a BAN, the MAC frame size varies from few bytes (implant) to hundreds of bytes (wearable), depending on the application. A longer MAC frame reduces the chances of blind forging. The application layer selects a security mode using an Access Control List (ACL) that controls security and keying information. The destination address of an outgoing packet is matched with address field in the ACL entry. If there is a match, the security mode, key, and nonce1 specified in the ACL entry are used to process the packet. Encryption algorithms are used to prevent unauthorized access. Exchange of keys may be required by devices to be able communicate. The following sections discuss AES-CTR, AES- CBC, and AES-CCM modes for a BAN [Ullah12].

1. AES-CTR: The Counter (CTR) mode can be used in BAN in order to encrypt data. It breaks the cleartext into blocks of 16 bytes each; b1,b2,.....bn and computes ci = bi âŠ• Ek(xi), where ci is the cipher text of jth block, bi is the jth block of data and Ek(xi) is the encryption of the counter xi. The coordinator recovers the plaintext by computing bi = ci⊕Ek(xi).
2. AES-CBC-MAC: In the Cipher-block Chaining Message Authentication Code (CBC- MAC)2 mode, the plaintext is XORed with the previous cipher text until the final encryption is achieved. This mode provides authentication and message integrity by allowing the BAN nodes to compute either 32 bits,

64 bits, or 128 bits Message Authentication Code (MAC). The coordinator computes its own MAC and compares it with the nodeâ€™s MAC. The coor- dinator accepts the packet if both MACs are equal. The mathematical representation of the CBC-MAC is given by: ci = Ek (b i âŠ• ciâ^'1) for generating ciphertexts and b i = Dk (ci) âŠ• ciâ^'1 for generating plaintexts.

3. AES-CCM The Counter with CBC-MAC (CCM) mode combines CTR and CBC modes in order to ensure high-level security that includes both data integrity and encryption. The nodes first apply the integrity protection to the MAC frames using CBC-MAC mode and then encrypts the frames using CTR mode. This mode can be used to send or receive sensitive information such as updating programs in pacemakers and implantable cardiac defibrillators.

Generally, the addition of security protocols to BAN consumes extra energy due to overhead transmission required by the protocols. The best way is to use a stream cipher for en- cryption, where the size of the ciphertext is exactly the same as the plaintext. In this case, the MAC uses 16 bytes of 60 bytes data frame. Moreover, the Cyclic Redundancy Check (CRC) is not required since the MAC itself achieves data integrity. Law et al. concluded that the most energy efficient cipher is Rijndael [Ullah12]. They examined the number of CPU cycles during they key setup and encryption/decryption procedures.

5. Low Energy Cryptographic Solutions for BANs

While security is paramount, the cost of implementing security techniques in BANs may be prohibitive. It, therefore, becomes necessary to find cryptographic solutions that consume less energy. This section deals with the discussion of cryptographic methods in use and those that are proposed and their costs.

5.1 Energy efficient security algorithms

Researchers have proposed a number of methods for making security protocols more energy efficient. One broad category is of techniques that make execution of cryptographic algorithms efficient through a combination of hardware and software techniques. Usually, in these techniques, there is an overhead in the form of an increase in silicon area or more complex software.

Another method of achieving energy efficiency is to use energy-aware protocols. These protocols tune their operation to the environment. This may involve a rule-based tradeoff between the level of security and consumption of energy. Commonly used security protocols, like SSL/TLS, IPSec, etc., have the freedom of realizing the desired security objectives by choosing specific cryptographic algorithms from a predefined set. Additionally, the controller and the BAN nodes can also decide upon parameters that influence the mode of operation of the chosen cryptographic algorithm [Lakshmi13].

Cryptographic algorithms that provide trust that is present in face-to-face meetings are divided into the following categories

1. Symmetric algorithms: These algorithms use the same key for encryption and decryption. They rely on the concepts of â€œconfusion and diffusionâ€ to realize their cryptographic properties and are used mainly for confidentiality purposes [Ma12].
2. Asymmetric algorithms: These algorithms use two keys, public and private, for encryption and decryption. These algorithms are mainly used for authentication and nonrepudiation. Due to the resource constraints of sensors, public-key based cryptographic algorithms like RSA and Diffie-Hellman are too complicated and energy-consuming even for field deployed WSNs. However, the symmetric cryptographic technique has its own qualities that always make it more favorite as compared to public key cryptography for WSNs. Furthermore, to provide security in WSN, encryption keys must be established among sensor nodes. Key distribution refers to the distribution of multiple keys among the sensor nodes. Key management also receives a great deal of attention in data encryption and authentication in WSNs security.
3. Hash algorithms: These algorithms take a message of arbitrary length and output a fixed-length hash of the message. Different messages are expected to produce different hash results. The algorithms can be made parameterizable on a key, in which case, they are referred to as â€œkeyed hash algorithms.â€ They are used for verifying the integrity of the messages exchanged.

We shall discuss is some more detail the secret key and asymmetric algorithms that are being studied for BANs.

5.2 Symmetric or Secret Key Encryption

It is seen that public key encryption (PKE) methods provide better security but they are mathematically hard and cost more in terms of energy consumed. Therefore, most BAN systems today use symmetric key encryption (SKE)(Fig. 3). In SKE, methods like AES and RC4 are used. Most of the WSNs use the symmetric key schemes because these schemes require less computation time than other schemes. Based on the key distribution, key discovery and key establishment there can be different categories of symmetric key schemes. For example, pure probabilistic-based schemes and polynomial-based key pre-distribution schemes are two of them.

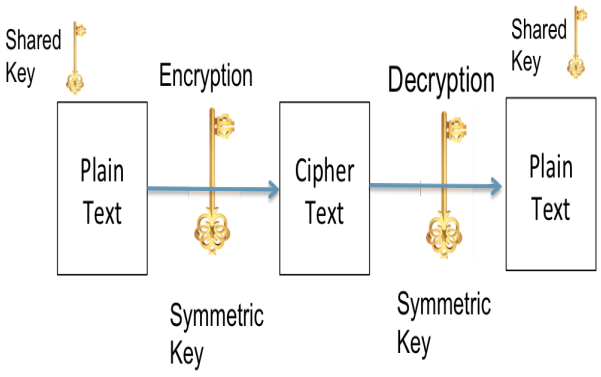

Fig. 3: Symmetric Key Encryption

SKE is today considered to be an efficient choice for distributed access control in BANs. In general, SKE based approaches suffer from three main disadvantages:â€¨Fine-grained access control is hard to realize due to the high key management complexity, they are vulnerable to user collusion, compromising a node will possibly expose the data, since if a node cannot store encrypted copies for all possible users and it must store the data in plaintext. It is desirable that the data remain encrypted even when stored in BAN nodes or servers. In order to achieve both fine-grained access control and efficiency, it is more desirable to encrypt once and for all so that all authorized users can have access.

Symmetric ciphers are of two types, block and stream ciphers. Block ciphers operate on similar-sized blocks of plaintext and ciphertext. Examples of block ciphers include DES and AES. Stream ciphers, such as RC4, convert a plaintext to ciphertext one bit (or byte) at a time. Before a block or stream cipher starts the encryption/decryption operation, the input key (usually 64 bits) is expanded in order to derive a distinct and cryptographically strong key for each round (key setup). Encryption or decryption in symmetric algorithms then proceeds through a repeated sequence (rounds) of mathematical computations. RC4 is supposed to be a fast and efficient stream cipher, which is suitable for encrypting data in high-speed networking applications. However, it has a significant encryption cost compared to other symmetric ciphers. Blowfish exhibits the greatest contrast between the energy costs of key setup and encryption/decryption: The energy cost of key setup is the highest, while that of encryption/decryption is lowest. AES has competitive energy costs, and its cryptanalytic properties have been well studied. The round operations in AES operate on 8-bit data blocks and are amenable to implementation efficiency on 8-bit processors. However, optimizations exist to make AES run extremely fast on 32-bit processors at the cost of some space overhead (up to 4KB). In this case the round operations are transformed into table lookups which can be speeded up using multithreaded processors.

AES offers a good mixture of security and energy efficiency. Its security properties have been well-studied, and it was found to offer high resistance to linear and differential cryptanalysis. In addition, it also has a low energy cost for both key setup and encryption. However, recent studies have pointed out that it might be susceptible to algebraic attacks. In terms of high resistance to cryptanalytic attacks, other algorithms that fare well are 3DES and IDEA. When lower energy consumption is a higher priority, RC5 and Blowfish serve as possible candidates. Blowfish is the ideal choice when large amounts of data are to be transmitted with a low frequency of key refreshes.

5.3 Public Key Cryptography

Encryption in the ultra-low energy domain is an important and growing challenge. Example applications include Implantable Medical Devices (IMDs), Wireless Sensor Networks (WSNs), and Radio Frequency Identification (RFID) tags. In this class of applications, the energy cost of each operation is important for the solutionâ€™s success. For example, in a typical IMD, each extra Joule consumed in computation reduces the life of the device, and each surgical replacement of the device endangers the life of the patient. In the case of IMDs, unauthorized access to an implanted cardiac defibrillator's programming interface poses an unambiguous threat to the patent's health and privacy. Despite the obvious need for security in this domain, relatively few designs have incorporate encryption. The devices that do employ encryption use symmetric (shared-key) techniques, as they are low on computation. Asymmetric key cryptography provides higher security by have higher computational complexity making the energy requirements a difficult proposition or low energy applications like BANs [Darwish11]. Public Key Cryptography (PKC) requires separate keys for encryption and decryption, allowing it to solve a host of security challenges not possible with symmetric cryptography alone. Uses for asymmetric cryptography range from session key establishment for secure communications to digital signatures for message authenticity and non-repudiation. While symmetric cryptography is based on diffusion (data shifts) and confusion (permutations), asymmetric cryptography is built upon a foundation of mathematically hard problems [Targhetta14]. Fig. 4 gives block diagram of PKC.

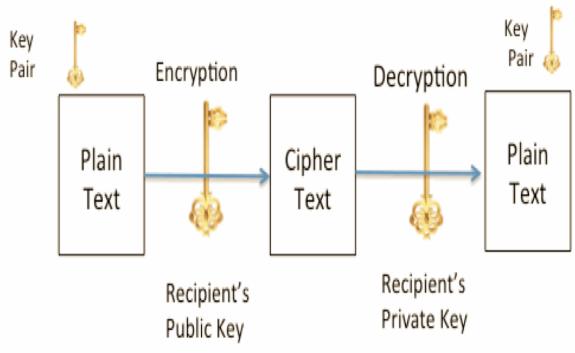

Fig. 4: Public Key Cryptography

The most common methods used in Public Key Cryptography (PKC) are RSA and the elliptic curve cryptography (ECC). However, while the public and private key generation speeds have been increased, encrypting and decrypting large volume of data is slow in RSA and ECC. Researchers have dedicated much effort to achieving significant acceleration using hardware in FPGA and ASIC designs; however, only a few publications seem to investigate the energy consumption aspect of public key cryptography for embedded devices. To see how employing asymmetric cryptographic capabilities on ultraÂlow energy devices can be especially challenging we can take a cue from WSN research. WanÂder et al. found that in WSNs even weak asymmetric cryptography (160-bit ECC, equivalent to 1024-bit RSA) consumes approximately 72% of the energy allotted for communication handshaking. They compared the energy cost of 1024-bit RSA with that of 160-bit ECC to show that 160-bit ECC significantly reduces energy consumption. The results provide a very compelling argument for ECC, showing that, based on an assumed battery life, the device using ECC could execute 4.2 times the number of key exchange operations. Enthused by results in the domain of WSN, researchers are trying to adapt PKC to BAN environments. If energy harvesting is used then the energy budget can be reduced.

6. Summary and Research Directions

To summarize, energy efficient, secure and reliable BANs described in the sections above, can be realized with collaboration among a number of domain experts. For example, for producing trustworthy and acceptable solutions for providing healthcare to the elderly the collaboration is required between technologists, physicians, medical support staff, psychologists and epidemiologists. This would ensure that BANs are not only designed to collect and provide physiological and psychological information but are also acceptable to the elderly. Security in BANs is one of the most important issues. There have been some implementations of symmetric key cryptography. However, public key cryptography provides higher security but at high energy cost. More research is required to make public key cryptography for low energy BAN systems.

Some important research directions are discussed below:

Energy Efficient Devices: Research is being undertaken to improve the design of wearable sensors and make them more patient friendly. The new generation sensors would not require accurate positioning by skilled staff. They would reduce the detrimental effect of the human skin on low-power radio signals. More research is required to find material that would make implantable sensors more compatible with the human tissue. The BAN nodes need to be made smaller, smarter and with long recharge cycles. They need to have smart batteries that last long and recharge themselves by harvesting energy from the patients' body heat or movement. As these devices are very close or inside the human body, concerns regarding electromagnetic energy radiation need to be addressed.

Security, Encryption and Cryptography: Effective authentication schemes based on human facial features and EEG signals are being actively developed in academia and industry. However, these may create privacy issues for the patients. Encryption in the ultra-low energy domain is an important and growing challenge. Research efforts are being made to reduce the energy cost of elliptic curve cryptography. For unconscious patients some method based on biometrics and physiological signals based authentication is necessary.

Communication: Technologyâ€™s success will ultimately lie in its value perceived by the users. BANs must effectively transmit and transform sensed phenomena into valuable information and do so while meeting other system requirements, such as energy efficiency. Research efforts are directed towards designing architectures that would process and deliver the required data securely, timely and accurately in the best interest of the patients' condition. Bluetooth Low Energy is a promising emerging wireless technology that has less communication overhead because it is devised for inter-BAN communication exclusively by supporting a single hop topology, short range coverage, and compatibility with widely used Bluetooth devices. Transmitting signals through bones and taking body movements into account are other areas in which more work is required.

Integration of BANs with other technologies: Efforts are being made to incorporate BAN technology in RFID, WSNs and video surveillance. This would help extend the usefulness of the existing e-healthcare applications. RFID containing patientâ€™s identification can allow fast verification by healthcare providers for providing timely medical care even if the patient is unconscious.

Protocol Layers: Body area propagation environments have been characterized extensively at the link level. There is still a need for accurate models that help researchers pre- dict the impact of realistic channels on network level performance. Taking into account, reliability, latency, mutual interference, energy consumption and mobility factors in such a model will yield a more effective network architecture, so that better routing algorithms for BANs can be devised. Recent years have seen growing interests in using UWB channel models for BANs.

MAC layer: We have discussed above the energy saving protocols already proposed at the MAC layer. Despite these developments a number of issues still remain to be resolved. One is that of network capacity. As the packet size is low, achieving high data rate required for some medical applications would result is high overhead. MAC protocols that reduce overhead are required to be developed. Ultra low power consumption requires effective duty cycle that increase the operations at MAC level. Frame delays may be increased resulting in QoS issues for some applications. The ideal MAC protocol would also take care of a wide variety of sensor nodes and QoS requirements.

Standardization: Interoperability of BANs is important for patient mobility across medical facilities. Intelligent healthcare in ambulatory environment regardless of the patients' location providing them of same kind of privacy and treatment requires more to be done in terms of standardization.

References

1. [Ali13] Aftab Ali, Farrukh Aslam Khan, â€œEnergy-efficient Cluster-based Security Mechanism for Intra-WBAN and Inter-WBAN Communications for Healthcare Applications,â€ Journal on Wireless Communications and Networking, 2013, pp 1-19http://jwcn.eurasipjournals.com/content/2013/1/216
2. [Chatterji14] Somnath Chatterji, Julie Byles, David Cutler, Teresa Seeman, Emese Verdes, â€œHealth, Functioning, And Disability In Older Adultsâ€”Present Status And Future Implications,â€ The Lancet, November 2014http://www.thelancet.com/journals/lancet/article/PIIS0140-6736%2814%2961462-8/abstract
3. [Chen11] Min Chen, Sergio Gonzalez, Athanasios Vasilakos, Huasong Cao, Victor C. M. Leung, â€œBody Area Networks: A Survey,â€ Mobile Networks and Applications archive, Volume 16 Issue 2, 2011, pp 171-193http://dl.acm.org/citation.cfm?id=1968873
4. [Darwish11] Ashraf Darwish, Aboul Ella Hassanien, â€œWearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring,â€ Sensors 2011, pp 5561-5595 http://www.mdpi.com/1424-8220/11/6/5561
5. [Diop13] Abdoulaye Diop, Yue Qi, Qin Wang, Shariq Hussain, â€œAn Advanced Survey on Secure Energy-Efficient Hierarchical Routing Protocols in Wireless Sensor Networks,â€ IJCSI, Volume 10, Issue 1, 2013http://arxiv.org/pdf/1306.4595.pdf
6. [Fang09] G. Fang and E. Dutkiewicz, â€œBodyMAC: Energy efficient TDMA-based MAC protocol for wireless body area networks,â€ 9th International Symposium on Communications and Information Technology, ISCIT, 2009, pp. 1455-1459.http://www.researchgate.net/publication/224084578_BodyMAC_Energy_efficient_TDMA-based_MAC_protocol_for_Wireless_Body_Area_Networks
7. [Hanson09] Mark A. Hanson, Harry C. Powell Jr., Adam T. Barth, Kyle Ringgenberg, Benton H. Calhoun, James H. Aylor, and John Lach, â€œBody Area Sensor networks: Challenges and Opportunities,â€ IEEE Computer Society, 2009, pp 58-69http://people.virginia.edu/~bhc2b/papers/HansonEtalComputer09.pdf
8. [IEEE11] IEEE Standard for Local and metropolitan area networksâ€” Part 15.4: Low-Rate Wireless Personal Area Networks (LR-

WPANs)http://standards.ieee.org/getieee802/download/802.15.4-2011.pdf
9. [IEEE12] IEEE Standard for Local and metropolitan area networksâ€•Part 15.6: Wireless Body Area Networks Sponsor LAN/MAN http://standards.ieee.org/getieee802/download/802.15.6-2012.pdf
10. [IPSO10] Introduction to Security for Smart Object Networks, Internet Protocol for Smart Objects (IPSO) Alliance, Whitepaper, 2010 http://www.ipso-alliance.org/wp-content/media/security_intro.pdf
11. [Kumar13] T Senthil Kumar, T Murugesan, â€œTowards an Approach for Improved Security in Wireless Networks,â€ International Journal of Computer Applications (International Conference on Innovation in Communication, Information and Computing (ICICIC)), 2013, pp 9-13http://www.ijcaonline.org/proceedings/icicic2013/number1/11285-0117
12. [Lakshmi13] Lakshmi P.S., Pasha Sajid, Ramana M.V., â€œSecurity and Energy efficiency in Ad Hoc Networks,â€ Research Journal of Computer and Information Technology Sciences, 2013, pp 14-17http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=6682706&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D6682706
13. [Latre11] BenoË†Ä±t Latre Ì, Bart Braem, Ingrid Moerman, Chris Blondia, Piet Demeester, â€œA survey on wireless body area networks,â€ Wireless Networks, 2011, 1â€“18http://dl.acm.org/citation.cfm?id=1938079
14. [Li10] Ming Li And Wenjing Lou, Worcester Polytechnic Institute Kui Ren, â€œData Security And Privacy In Wireless Body Area Networks,â€ IEEE Wireless Communications, 2010, pp 51-58http://www.cnsr.ictas.vt.edu/publication/WTE_Li_DSAPWBaN.pdf
15. [Lim10] Shinyoung Lim, Tae Hwan Oh, Young B. Choi, â€œSecurity Issues on Wireless Body Area Network for Remote Healthcare Monitoring,â€ IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, 2010, pp 327-332http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5504649&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5504649
16. [Ma12]Tao Ma, Pradhumna Lal Shrestha, Michael Hempel, Dongming Peng, Hamid Sharif, Hsiao-Hwa Chen, â€œAssurance of Energy Efficiency and Data Security for ECG Transmission in BASNs,â€ IEEE Transactions On Biomedical Engineering, Vol. 59, No. 4, 2012, pp 1041-1047http://www.ncbi.nlm.nih.gov/pubmed/22231147
17. [Patel10] Maulin Patel, Jianfeng Wang, â€œApplications, Challenges, and Prospective in Emerging Body Area Networking Technologies,â€ IEEE Wireless Communications, 2010, pp 80-88http://dl.acm.org/citation.cfm?id=1821032
18. [Rahim12] A. Rahim, N. Javaid, M. Aslam, Z. Rahman, U. Qasim, Z. A. Khan, â€œA Comprehensive Survey of MAC Protocols for Wireless Body Area Networks,â€ Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012http://arxiv.org/pdf/1208.2351.pdf
19. [Saleem10] Saleem, S.; Ullah, S.; Kyung Sup Kwak, â€œTowards security issues and solutions in Wireless Body Area Networks,â€ 6th International Conference on Networked Computing (INC), 2010 pp 1-4 http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5484803&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F5481764%2F5484786%2F05484803.pdf%3Farnumber%3D5484803
20. [Selimis11] Georgios Selimis et. al., â€œA Lightweight Security Scheme for Wireless Body Area Networks: Design, Energy Evaluation and Proposed Microprocessor Design,â€ Journal of Medical Systems, 2011 http://www.ncbi.nlm.nih.gov/pubmed/21373804
21. [Targhetta14] Targhetta, A.D.;Owen, D.E.;Gratz, P.V., â€œThe design space of ultra-low energy asymmetric cryptography,â€ IEEE International Symposium on Performance Analysis of Systems and Software (ISPASS), 2014, pp 55-65http://cegroup.ece.tamu.edu/~pgratz/papers/ispass2014_crypto.pdf
22. [Timmons09] N.F. Timmons and W.G. Scanlon, â€œAn adaptive energy efficient MAC protocol for the medical body area networks,â€ 1st International Conference on Wireless communication VITAE, 2009, pp. 587-593.http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5172512&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5172512
23. [Ullah12] Sana Ullah et. al., â€œA Comprehensive Survey of Wireless Body Area Networks,â€ Journal of Med Systems, 2012, 1065â€“1094http://link.springer.com/article/10.1007%2Fs10916-010-9571-3
24. [Yoon14] Min Yoon, Miyoung Jang, Hyeong-Il Kim, and Jae-Woo Chang, â€œA Signature-Based Data Security Technique for Energy-Efficient Data Aggregation in Wireless Sensor Networks,â€ International Journal of Distributed Sensor Networks, 2014, pp 1-10http://www.hindawi.com/journals/ijdsn/2014/272537/
25. [Zigbee10] Zigbee Healthcare Alliance, "Zigbee Healthcare Profile Specification," 2010, https://docs.zigbee.org/zigbee-docs/dcn/10/docs-10-5619-00-0zhc-zigbee-health-care-profile-1-0-public.pdf

List of Acronyms

ACL	Access Control List
AES	Advanced Encryption Standard
BAN	Body Area Network
BASN	Body Area Sensor Networks
ECC	Elliptical Curve Cryptography
ECG	Electro Cardio Gram
EEG	Electroencephalography
EMG	Electromyography
EMRS	Emergency Medical Response System
FCC	Federal Communication Commission
FPGA	Field Programmable Gate Array
GDP	Gross Domestic Product
IEEE	Institute of Electrical and Electronics Engineering
IMD	Implantable Medical Device

ISM	Industrial, Scientific and Medical
LAN	Local Area Network
LOS	Line of Sight
LR-PAN	Low Rate-Personal Area Network
MAC	Media Access Control
MAN	Metropolitan Area Network
NLOS	Non Line of Sight
PHY	Physical Layer
PKC	Public Key Cryptography
QoS	Quality of Service
RFID	Radio Frequency Identification
SAR	Specific Absorption Ratio
SKE	Secret Key Encryption
SPINS	Security Protocol for Sensor Networks
TDMA	Time Division Multiple Access
TEG	Thermo Electrical Generator
UHM	Ubiquitous Health Monitoring
UWB	Ultra Wide Band
WBAN	Wireless Body Area Network
WHO	World Health Organization
WLAN	Wireless Local Area Network
WMTS	Wireless Medical Telemetry System
WPAN	Wireless Personal Area Network
WSN	Wireless Sensor Network

Last Modified: December 1, 2014
This and other papers on current issues in network security are available online at http://www.cse.wustl.edu/~jain/cse571-14/index.html
Back to Raj Jain's Home Page