Wireless Body Area Networks: Attacks and Countermeasures

Pejman Niksaz,
Young Researchers and Elite Club, Mashhad Branch, Islamic Azad University, Mashhad, Iran
pejmanniksaz@outlook.com

Abstract—Wireless Sensor Networks (WSNs) have been identified for their utility in a variety of different fields such as military sensing and tracking, environmental monitoring, patient monitoring and tracking smart environments. Wireless Body Area Network (WBAN) technology is the consequence of the existing WSN technology. These networks are a composition of tiny, inexpensive and low-power biomedical nodes, fundamentally considered for healthcare monitoring applications. The main purpose of these applications is to ensure a monitoring of vital parameters of sick people without any interruption, while giving them the freedom of motion. The more scientists try to develop further cost and energy efficient computing devices and algorithms for WBANs, the more challenging it becomes to fit the security of WBANs into such a limited environment. As a result, being familiar with the security aspects of WBANs is necessary before designing WBAN systems. In this paper, we review the security requirements for WBANs, the different kinds of possible attacks, and also some security mechanisms used to overcome these attacks.

Index Terms— Wireless Body Area Networks, sensor, WBAN, security, attack, WSN, statistical data, challenge.

1 INTRODUCTION

As healthcare costs are rapidly increasing with the world’s population, there has been a need to monitor a patient health status anywhere both in and out of the hospital. This demand and advancement in technology, mobile electronic devices, wireless communication, portable batteries, and sensors caused the development of wireless body area network (WBANS). Wireless body area network is a system that is able to monitor the health conditions of patients and early risk detection constantly by sharing the information with caretakers and physicians. Based on the operating environments this can be classified into two various groups, one is called wearable body area network which is operated on the surface of body and another is implantable body area network which is operated inside the human body.

Generally, two sorts of devices can be differentiated: sensors and actuators. The sensors can be used to measure internal or external certain parameters of the human body. Body temperature, measuring the heartbeat or recording a prolonged electrocardiogram (ECG) are some examples of sensors. On the other hand, the actuators (or actors) take some spectacular actions according to the data they receive from the sensors or through interaction with the user. For instance, an actuator equipped with a built-in reservoir and pump administers the correct dose of insulin to give to diabetics according to the glucose level measurements. Interaction with the user or other person is usually handled by a personal device such as a PDA or a smart phone which acts as a sink for data of the wireless devices.

One of the usages of WBAN is that it can be utilized to offer assistance to the disabled. For example, a paraplegic can be equipped with sensors determining the position of the legs or with sensor attached to the nerves (Huan-Bang, Takizawa, Bin, & Kohno, 2007). Another area of application can be considered in the domain of public safety where the WBAN can be utilized by firefighters, policemen or in a military environment (Hoyt, Reifman, Coster, & Buller, 2002). For example, the WBAN checks the level of toxics in the air and warns the firefighters or soldiers if a life threatening level is detected.

A WBAN is consisted of several to dozens of nodes implanted in or worn on the human body to collect information(Barakah & Ammad-uddin, 2012). The sensor node communicates among them through the wireless channel and transmits the collected biomedical information towards a controller node. Some characteristics of WBANs include:

- It is a small case wireless network for short distance communication within 3 meters (Liu & Kwak, 2010).
- The range of data rate in WBAN is form 10Kbps to 10Mbps.
- The main structure in WBAN is Star topology and BN only communicates with BNC.
- BNs are constrained in their power computation and communication capabilities, specifically for those implanted BNs (Barakah & Ammad-uddin, 2012).
- Security should be energy efficient with minimal overhead and support at least authenticated and encryption operations.
- It closely surrounds the body to consist of its own communication system.

- It is biomedical information that WBAN nodes primarily detect, collect and transmit.

This paper will discuss requirements for secure sensor network protocols, different kinds of attacks in WBANs, and some proposed countermeasures against these attacks.

2 Security Requirements in WBANs

Even though security issues are made a high priority in most networks, little study has been done in this area for WBANs. Additionally, because of strict resource constraints in terms of memory, power, computational capability rate, communication and as well as inherent security vulnerabilities, the security specifications proposed for other networks are not applicable to WBANs. Practically, deployment of WBANs and the integration of convenient security mechanisms need knowledge of the security requirements of WBANs with which are provided as follows (Saleem, Ullah, & Yoo, 2009):

2.1 Data Integrity

When data is transmitted to an insecure WBAN, sometimes, its information can be altered. An adversary will then be able of adapting a patient's information prior to reaching the network coordinator, so endangering the patient's health and maybe even their life. As a result, the received data requires to be assured of not being altered by an adversary through right and correct data integrity by using data authentication protocols.

2.2 Data Confidentiality

Protection of data from disclosure can happens through data confidentiality. The role of WBAN nodes in medical applications is transmitting sensitive information concerning the status of a patient's health. Critical information can be eavesdropped, which may cause a considerable amount of damage towards a patient as the data issued for illegal goals. Data confidentiality can be accessed through encryption of a patient's data via a shared key on a communication channel secured among the WBAN nodes and their coordinator.

2.3 Data Freshness

Data integrity and confidentiality can only be supported if data freshness techniques are used. An adversary has ability to capture data in transmissions and then replay it to create confusion for the WBAN coordinator. Data freshness assures that data is not reused and its frames are in order. There are two different types of data freshness as follows: strong freshness that guarantees delay as well as frame ordering, and weak freshness which provides no guarantee in terms of delay. Strong freshness is essential in synchronization while a beacon is being transmitted to WBAN coordinator, whereas weak freshness is important for WBAN nodes with low duty- cycle.

2.4 Availability

The availability of the patient's information to the physician needs to be ensured at all times. An attack towards availability in WBANs could be capturing and disabling an ECG node leading to loss of life. Therefore, maintenance and capability to switch to another WBAN in case of availability loss is vital.

2.5 Data Authentication

Data authentication is a necessity in both medical and non-medical applications. Both WBAN nodes and the coordinator node need verification that data is being sent from the trust center and not a false adversary. Both of them compute a Message Authentication Code (MAC) for all data by sharing a secret key. When the correct MAC is calculated, the network coordinator will realize that the received message is being sent by a trusted node.

3 Security Management

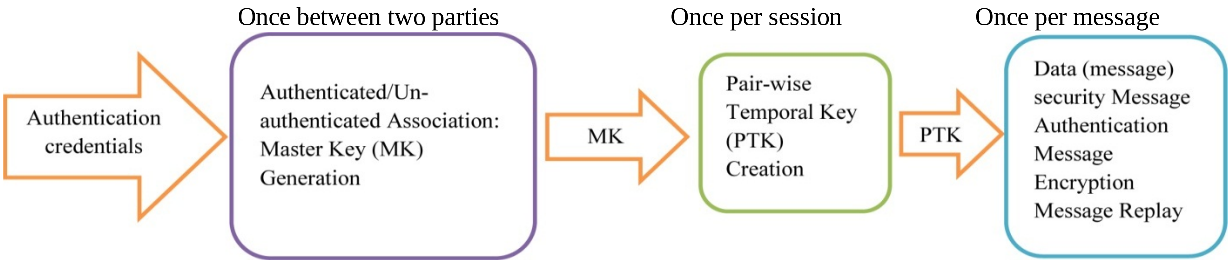
The decryption and encryption operation requires secure management at the coordinator in order to provide key distribution to wireless body area networks. The WBAN coordinator adds and removes WBAN nodes in a secure way during association and disassociation.

The IEEE 802.15.6 standard has proposed a security paradigm for WBANs shown in figure1 that defines three levels of security as follows (Davenport et al., 2009):

a) Level 0- Unsecured Communication- this is the lowest level of security in which data is transmitted in unsecured frames and provides no measure for integrity validation, authenticity and replay defense, privacy protection and confidentiality.

b) Level 1- Authentication but no Encryption- In this level of security, data is transmitted in authenticated but unencrypted frames. It is composed of measures for integrity validation, authenticity and replay defense. However, it provides no privacy protection or confidentiality.
c) Level 2- Authentication and Encryption- This is the highest level of security in which messages are transmitted in authenticated and encrypted frames; therefore, providing measures for integrity validation, authenticity, replay defense, privacy protection and confidentiality. It covers the relevant issues to level 0 and level 1. Selection of the required security level can be done during the association process. In unicast communication, a pre-shared master key (MK) or a new key (generated through unauthenticated association) is activated. In the next step, a Pairwise Temporal Key (PTK) is generated that is used only once per session. In multicast communication a Group Temporal Key (GTK) is generated that is shared with its corresponding group (Kwak, Ullah, & Ullah, 2010).

Fig1. Security Paradigm of IEEE.802.15.6


Once between two parties
Once per session
Once per message
Authentication credentials
Authenticated/Un-authenticated Association: Master Key (MK) Generation
MK
Pair-wise Temporal Key (PTK) Creation
PTK
Data (message) security Message Authentication Message Encryption Message Replay

4 ATTACKS IN WIRELESS BODY AREA NETWORK

In general, attacks on WBAN can be categorized into three different groups (Shi & Perrig, 2004): (a) attacks on service integrity, where the network is forced to accept false information (Wood & Stankovic, 2002), (b) attacks on secrecy and authentication, where an adversary performs eavesdropping, packet replay attacks, or spoofing of pockets, and (c) attacks on network availability (DOS attacks), where the attacker tries to reduce the network's capacity. This section lists and gives a summary discussion about the most important attacks against WBANs.

4.1 Physical Layer

Some of the main responsibilities of physical layer include frequency selection and generation, signal detection, modulation, and encryption (Akyildiz, Su, Sankarasubramaniam, & Cayirci, 2002). Since the medium is radio-based, jamming the network is always possible. The most common attacks in physical layer are jamming and tampering.

4.1.1 Jamming

When the wireless transmission frequency used in a WBAN is known, jamming is a common physical attack that can be simply done by adversaries (X. Wang, Gu, Chellappan, Schosek, & Xuan, 2005), (Zhiping & Hui, 2010). In this kind of attack, an attacker transmits radio signal randomly with a frequency as the sensor nodes are sending signals for communication. The radio signal interferes with the other signal sent by a sensor node and receives within the range of the attacker cannot receive any message. Thus, the nodes in the range of any attacker signals become totally isolated as long as the jamming signal continues and no messages can be given or received among the affected nodes and other sender nodes.

4.1.2 Tampering

Sensor networks usually work outdoors. Because of unattended and distributed nature; the nodes in a WBAN are highly susceptible to physical attacks (Hartung, Balasalle, & Han, 2005). The physical attacks may cause reversible damage to nodes. The adversary can exploit cryptographic keys from the captured node, change the information, modify the program codes or even replace it with a malicious sensor (Wood & Stankovic, 2002). It has been proven that sensor nodes such as MICA2 motes can be compromised in less than one minute time (Xiao, Yu, & Gao, 2007).

4.2 Data Link Layer Attacks

The layer is responsible for multiplexing, frame detection, channel access, and reliability. Attacks on this layer include creating collision, unfairness in allocation, and resource exhaustion.

4.2.1 Collision

An adversary can cause collisions in some special packets such as ACK control messages. One of the results of such collisions is the costly exponential back-off in certain media access control protocols.

4.2.2 Unfairness

Unfairness degrades the network performance by interrupting the Medium Access Control (MAC) priority schemes. Exhaustion of battery resources may occur when a self- sacrificing node always keeps the channel busy.

4.2.3 Resource Exhaustion

Daniel of Service (DoS) attacks happen because of resource exhaustion. For instance, a native link layer implementation may try to transmit the corrupted packets continuously. Unless these hopeless retransmissions are found or prevented, the energy reserved of retransmitting node and those surrounding it will be quickly depleted (Roman, Zhou, & Lopez, 2005).

4.3 Network Layer Attacks

The nodes in WBAN are not required to route the packets to other nodes. Routing is possible when multiple WBANs communicate with each other through their coordinators. Possible attacks include spoofing, selective forwarding, sinkhole, wormhole, Sybil and hello flood.

4.3.1 Spoofed Routing Information

Targeting the routing information in a network can be considered the most direct attack against a routing protocol. An attacker may perform everything in the network such as spoofing, altering, or replay routing information. These disruptions include creation of routing loops, generating fake error messages, extending or shortening source routes, attracting or repelling network traffic from selected nodes, causing network partitioning, and increasing end-to-end delay.

4.3.2 Selective Forwarding

Selective forwarding is a kind of attack where a compromised or malicious node just drops packets it likes and selectively forwards packets to make the suspicion minimum to the neighbor nodes. The damage becomes powerful when these malicious nodes are located closer to the base station (Deng, Sun, Wang, & Cao, 2009). There are two kinds of countermeasures that have been presented against selective forwarding attack. The first involves detection of compromised nodes and routing the data seeking an alternative path and the second involves sending data using multi-path routing (Chen & Lou, 2010).

4.3.3 Sinkhole Attack

In this attack, a malicious node behaves as a black hole to attract all the traffic in the sensor network (Tumrongwittayapak & Varakulsiripunth, 2009). In a flooding-based protocol, at first the attacker listens to requests for routes then replies to the target nodes that contains the high quality or shortest path to the base station.

Once the malicious device has the ability to insert itself among the communicating nodes (for example, a sink and sensor node), it is able to do anything with the packets exchanging between them. As a matter of fact, this attack can affect even the nodes that are significantly farther from the base station (Figure 2).

4.3.4 Wormhole Attack

A wormhole attack (Y.-C. Hu, Perrig, & Johnson, 2002), (L. Hu & Evans, 2004) is a sort of attack in which the attacker keeps the packets (or bits) at one location in the network and tunnels those to another location. Wormhole attacks are serious and dangerous threats to WSNs, because they do not need to compromise a sensor in the network. Rather, they can be applied even at the initial phase when the sensors start to detect the neighboring information (Figure 3).

For example, when node B (which can be the base station or any other sensor in the sys- tem) broadcasts the routing request packet, the attacker receives this packet and sends it again in its neighborhood. All neighboring nodes receiving this replayed packet will consider themselves to be in the range of Node B, and will consider this node as their parent. GPSR (Fenhua & Min, 2010) and GEAR (Yu, Govindan, & Estrin, 2001) are two such geographic-based routing protocols. In one recent article (Madria & Yin, 2009), researchers present a secure routing protocol named SERWA that fights against wormhole attacks. This protocol can discover wormhole attacks without using any specific hardware and can provide a real secure route against them. The simulation of this protocol has shown (Rosello, Portilla, Krasteva, & Riesgo, 2009) that when there are more than two wormholes in the network, more than 50% of the data packets will be attracted to the fake neighbor connections and will be discarded.

Fig 2 Conceptual View of Black Hole Attack

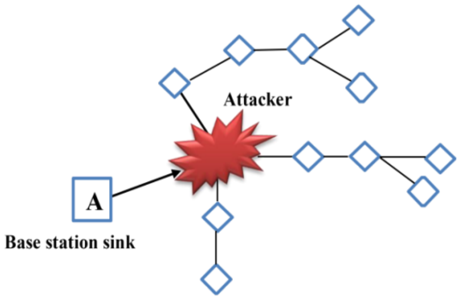
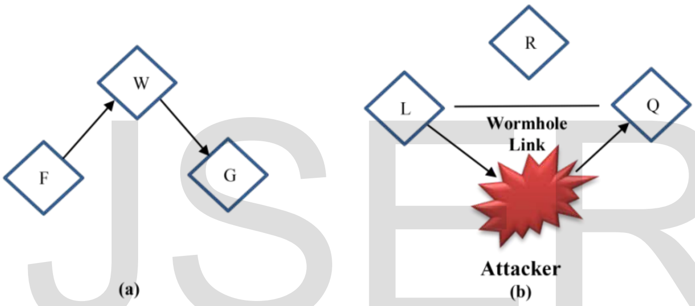


Fig 3 Wormhole Attack



4.3.5 Hello Flood Attack

In a Hello Flood attack, the attacker sends a hello message with a very powerful radio transmission to the network to convince all nodes to choose the attacker for routing their messages (Hamid, Mamun-Or-Rashid, & Hong, 2006). A good countermeasure against Hello Flood attack is authentication. An effective method is to use Authenticated broadcast protocols such as µTESLA. This protocol is based on symmetric key cryptography with minimum packet overheads. The sections below gives further description on µTESLA. One recent paper describes a countermeasure against Hello Flood attack that involves adopting a probabilistic secret sharing protocol and uses bidirectional verification (Hamid et al., 2006), (Douceur, 2002).

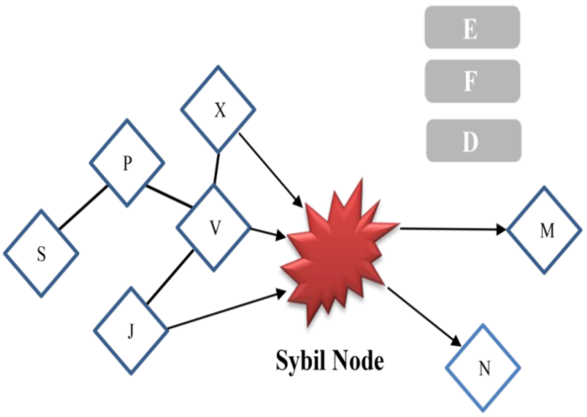
4.3.6 Sybil Attack

In a Sybil attack (Douceur, 2002), (Newsome, Shi, Song, & Perrig, 2004), a single node pre- tends to have multiple identities in the network. Any peer-to-peer network (especially wireless ad hoc) is prone to Sybil attack. This kind of attack has an important effect in geographic routing protocols (Newsome et al., 2004). In the location-based routing protocols, nodes need to exchange location information with their neighbors to route the geographically addressed packets efficiently. A paper by Douceur (Douceur, 2002) suggests that without a logically centralized authority, Sybil attacks are always probable except under severe and unrealistic assumptions of resource parity and coordination between entities (Figure 4).

One of the key requirements for countering Sybil attacks is identity verification. Newsome et al. (2004) (Newsome et al., 2004) have presented a technique using quantitative analysis where random key pre distribution schemes can defend against Sybil attack. For this purpose, they associate a sensor node’s identity with its assigned key using one-way hash function. Based on their mechanism, the network has ability to check part or all of the keys that an identity claims to have and thus counters against Sybil attack.

Moreover, authentication and encryption techniques can prevent an outsider from starting a Sybil attack on the sensor network. Public key cryptography can prevent such an insider attack, but because of the high cost it cannot be used in the resource constrained sensor networks. One solution is to have every node share a unique symmetric key with a trusted base station. Two nodes can then use a Needham-Schroeder-like protocol to verify each other’s identity and set up a shared key. A good example of a protocol that uses such a scheme is LEAP (Tian, Han, Parvin, & Dillon, 2010). In an article by Misra et al. (2010) (Misra & Myneni, 2010), researchers showed that, on average, more than 98% of Sybil nodes are identified by their scheme, while the scheme in another study was found to have 92% accuracy (Demirbas & Song, 2006).

Fig 4 Sybil Attack



4.4 Transport Layer Attacks

The main threats to the transport layer are flooding and desynchronization attacks.

4.4.1 Flooding Attack

Based on another paper (Kim, Lim, Park, & Kang, 2010), adversaries at the transport layer can exploit the protocols that maintain state at either end of the connection. As an example, the adversary may broadcast many connection establishment requests to the victim node to use all the power of its resources, causing a flooding attack. Limiting the number of connections that a node can make is one solution against this kind of attack. But, this can prevent legitimate nodes from connecting to the victim node. Another solution is based on the client puzzles idea presented in (Fallah, 2010).
According to this idea, if a node wants to connect with other nodes, it at first must solve a puzzle. An attacker is unlikely to have the necessary resources, making it impossible to connect fast enough to use a power of a serving node. Although solving puzzles includes processing overhead, it is more suitable than excessive communication.

4.4.2 Desynchronization Attack

In a desynchronization attack, an attacker copies massages many times to one or both endpoints of an active connection using a fake sequence number or control flag (Sadasivam & Moulin, 2009). Thus, attackers desynchronize the endpoints so that sensor nodes transmit the massages again and waste their energy. One solution against this sort of attack is to authenticate all the packets given and received among sensor nodes along with all the control fields in a transport header. The adversary cannot spoof the packets and header and, thus, this attack can be blocked.

5 Security Mechanisms in WBAN

5.1 Cryptography

As wireless medical sensor networks deal with sensitive physiological information, strong cryptographic functions (i.e., authentication, confidentiality, integrity, etc.) are most important requirements for developing any secure healthcare application. These cryptographic functions provide patient privacy and security against many malicious attacks. One of the most important policies in WBAN is selecting appropriate cryptography. Using strong cryptography requires extensive computation and resources that are a challenging task for resource hungry medical sensor nodes that can provide maximum security whilst using the minimum resources. In addition, the selection of cryptography system relies on the computation and communication capability of the sensor nodes. Some researches show that asymmetric cryptography systems are often too expensive for medical sensors and symmetric cryptography systems are not versatile enough (Le, Khalid, Sankar, & Lee, 2011). However, applying the security mechanisms to resource constrained medical sensors should be chosen according to the following considerations. Energy: how much energy is needed to perform the crypto functions. Memory: how much memory (i.e., read only memory and random access memory) is needed for security mechanisms. Execution-time: how much time is required to execute the security mechanisms.

5.2 Key Management

Key management protocols are fundamental requirements to develop a secure application. These protocols are used to set up and distribute various kinds of cryptographic keys to nodes in the network. Generally, there are three types of key management protocols, namely, trusted server, key pre-distribution and self- enforcing (Ng, Sim, & Tan, 2006), (Shaikh, Lee, Khan, & Song, 2006). (i) Trusted server protocols rely on a trusted base station responsible for establishing the key agreement in the network. It is considered that the trusted server protocols are well suited to hierarchical networks in the presence of unlimited resource gateways.

Although, trusted server based schemes provide stronger security to hierarchical networks, in a real- time environment, a trusted- server could become a single point for the entire network failure; hence, they are not suitable for critical applications (e.g., healthcare) (Ng et al., 2006). (ii) Key pre- distribution protocols are based on symmetric key cryptography, where secret keys are stored in the network before the network deployment. The key pre-distribution protocols are easy to implement offer relatively less computational complexity, making them more suitable for resource constrained sensor networks. (iii) Self- enforcing protocols a public key infrastructure provide many advantages, such as, strong security, scalability, and memory efficiency. Earlier public key based solutions were thought to be too computationally expensive (i.e., RSA (Jonsson & Kaliski, 2003) and Diffie- Hellman key exchange) for wireless sensor networks. However, some researches (Kriangsiri Malasri & Wang, 2009), (K. Malasri & Lan, 2006) have shown that elliptic curve cryptographic based schemes are viable on resource constrained networks. In fact, in real- time implementation, the ECC based necessary cryptographic primitives (e.g., signature generation and verification) are still expensive in term of the time complexity.

Aftab et al. have proposed and evaluated an energy- efficient key management scheme for WBAN that takes into account available resources of a node during the whole life cycle of key management. Their proposed scheme is a cluster- based hybrid security framework that supports both intra- WBAN and inter- WBAN communications. By using multiple clusters, energy efficient can be ensured. The cluster formation process itself is secured by using electrocardiogram (EKG)- based key agreement scheme. A highly dynamic and random EKG values of the human body for pairwise key generation and refreshment has been used (Ali & Khan, 2013). Iehab et al. discussed a secure and energy efficient key management scheme for WBAN. In this scheme two techniques i.e. physiological values (PV's) based key management which generate random keys by using the vital signs of human body and pre-loading based scheme, which will be used to strengthen the security of VPs based scheme. The potential limitation of VP's is short key generation, which can easily brute forced and high computational cost whereas in pre-loading the keys are not random and require enough key storage. As a result, they merged PV's and pre- loading techniques by using electrocardiography (EKG/ECG) values of PVs and pre- loading based schemes to strengthen security. The applied technique will enhance the security as well as reduce storage and power consumption (AL-Rassan & Khan, 2011). Sivaprasatham et al. have been proposed a secure key management technique for WBAN. The proposed architecture consists of a set of WBNs connected to the master server via backend server using authentication channel. Initially, backend server and master server use a shared symmetric key. When a node wants to join a network, it forwards a request message protected by the Message Authentication Code (MAC) to the master server via the backend server. The master server verifies the MAC and generates message key with the master key and sends it to the node that initiates the joining process. After all nodes receive key information from the master server, the Base Server (BS) schedules a re- keying period to refresh the master key. Their results show that the proposed technique is more authenticated and confident (Sivaprasatham & Venkateswaran, 2012).

5.3 Secure Routing

In home care or disaster scenarios sensor devices might require sending their data to other devices outside their immediate radio range (Lorincz et al., 2004). Therefore, routing and message forwarding is a crucial service for end to end communication. So far, numerous of routing protocols have been proposed for sensor networks, but none of them have been designed with strong security as a goal (Nasser & Chen, 2007), (Xiangqian, Kia, Kang, & Pissinou, 2009). Karlof-Wagner (Karlof & Wagner, 2003) discussed the fact that routing protocols suffer from many security vulnerabilities, such as an attacker might launch denial of service attacks on the routing protocol. An attacker could also inject malicious routing information into the network, resulting in inconsistencies in the routing. Further, most of current proposals are designed for static wireless sensor networks but mobility has not been taken under consideration, whereas healthcare applications require mobility supported routing protocols. In addition, designing secure routing protocols for mobile networks is a complex task and current WMSNs healthcare security requirements will make it more complex when they become real- time applications.

5.4 Resilience to Node Capture

Resilience against node capture is one of the most challenging problems in sensor networks. In real- time healthcare applications, the medical sensors are placed on a patient's body, whereas the environmental sensors are placed in hospital premises (e.g., word room, operation room etc.) which may be easily accessible to attackers. Thus, an attacker might be able to capture a sensor node, gets its cryptographic information and alter the sensor programming accordingly. Later, he/she can place the compromised node into the network, and that could endanger application success (Kavitha & Sridharan, 2010). The current cryptographic functions (i.e., node authentication and identification) may detect and defend against node compromised attacks to some degree, but these compromised node attacks cannot be detected instantly (Kavitha & Sridharan, 2010), which is a big issue for healthcare application. For example, consider the case of a false alarm. One possible solution to prevent this attack is to use tamper resistant hardware; however, tamper resistant hardware is not a cost effective solution.

5.5 Secure Localization

WMSNs facilitate mobility for patient's comfort, therefore patient location estimations are needed for the success of healthcare applications. Since, medical sensors' sense physiological data of an individual, they also need to report the patient's location to a remote server. As a result, medical sensors have to be aware of patient location, i.e., called localization. In (Boukerche, Oliveira, Nakamura, & Loureiro, 2008) the authors discussed localization systems, which were divided into: distance/ angle estimation, position computation and localization algorithms, and further they discussed attacks on localization systems. In (Xiangqian et al., 2009), (Kavitha & Sridharan, 2010) the authors argue that mobility supported secure localization protocols still need to be explored.

5.6 Trust Management

Trust signifies the mutual association of any two trustworthy nodes (i.e., sensor node and data aggregator node), that are sharing their information. In (Boukerche & Yonglin, 2009) trust as defined as "the degree to which a node should be trustworthy, secure, or reliable during any interaction with the node". Wireless healthcare applications depend on distributed cooperation among the network nodes. The key aspect of healthcare applications is a trust evaluation on the behavior of a node (i.e., data delivery and quality), so trust management systems are useful to detect the degree of trust of a node. Boukerche- Ren (Boukerche & Yonglin, 2009), evaluated the trust for mobile healthcare system. However, trust management must still be implemented in real- time healthcare application using WMSNs, to ensure a clearer picture of trustworthiness of the parties involved (i.e., medical sensors, etc).

5.7 Robustness to Communication Denial of Services

An attacker attempts to disrupt the network's operation by broadcasting high- energy signals. If the broadcasting is powerful enough, then the entire network communication might be jammed. Other attacks are also possible, such as an adversary may delay communication by violating the medium access control protocol. Moreover, an adversary can transmit packets while a neighbor node is also transmitting. The details of DOS attacks and their countermeasures at different layers of WSN routing, is shown in table 3. Since, the WMSN healthcare applications are mobile in nature, as a result, secure DOS attack countermeasures still need further investigation for real- time healthcare application using WMSNs.

5.8 Defense Against DoS Attacks

In this section, defense mechanisms against DoS attacks will be presented.

5.8.1 Defense in the Physical Layer

Jamming attacks may be prevented by employing various spread-spectrum communications such as frequency hopping and code spreading (Li, Chakravarthy, Wang, & Wu, 2011). Frequency-hopping spread spectrum (FHSS) is an approach where signals are transmitted by rapidly switching a carrier between different frequency channels using a pseudo-random sequence known to both the transmitter and the receiver. When a potential attacker is unable to predict the frequency selection sequence, it is impractical for him to jam the frequency being used at a given time. Code spreading is another technique for defending against jamming. However, it needs greater design complexity and energy and is not suitable for use with WSNs. Generally, to maintain low cost and low power requirements, sensor devices are limited to single-frequency use and are therefore highly susceptible to jamming attacks. One approach to tolerating jamming attacks in WSNs is to identify the jammed part of the network and effectively avoid it by routing around. Wood and Stankovic (Wood & Stankovic, 2002) have proposed an approach where the nodes along the perimeter of a jammed region report their status to the neighbors and collectively the affected region is identified and packets are routed around it.

5.8.2 Defense in the Link Layer

A common defense against collision attacks is the use of error correcting codes (Wood & Stankovic, 2002). Most codes work best with low levels of collisions such as those caused by environmental or probabilistic errors. However, these codes also increase extra processing and communication overhead. It is rational to assume that an attacker will always be able to corrupt more than what can be corrected. Although it is possible to detect these cruel collisions, no complete defense mechanism against them is known today.

A possible defense against energy exhaustion attacks is to utilize a rate limiting MAC admission control. This would allow the network to pay no attention to those requests that deliberately exhaust the energy reserves of a node. A second technique is to use time division multiplexing where each node is allocated a time slot in which it can transmit (Wood & Stankovic, 2002). This removes the necessity of arbitration for each frame and can solve the indefinite postponement problem in a back-off algorithm. However, it is still susceptible to collisions.

The effect of an attack launched against a link layer attack can be lessened by use of small frames, since they decrease the amount of time an attacker has to capture the communication channel (Wood & Stankovic, 2002). However, this technique often reduces efficiency and is susceptible to further unfairness as an attacker may attempt to retransmit rapidly instead of waiting for a random time interval.

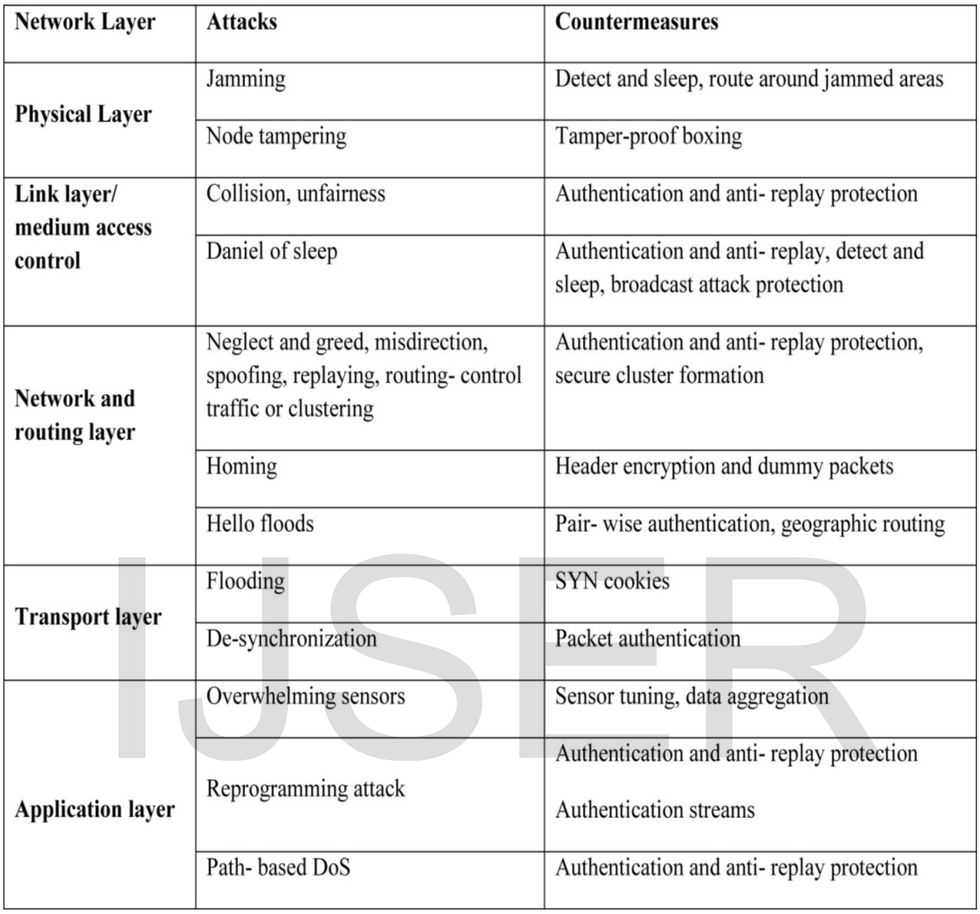
5.8.3 Defense in the Network Layer

A countermeasure against spoofing and alteration is to append a message authentication code (MAC) after the message. By adding a MAC to the message, the receivers can confirm whether the messages has been spoofed or altered. A possible defense against selective forwarding attacks is using digital watermarking technology (Kriangsiri Malasri & Wang, 2009). A second defense is to discover the malicious node or to consider it as failed and seek an alternative route.

5.8.4 Defense in the Transport Layer

To defend against flooding DoS attacks at the transport layer, Aura et al. have proposed a mechanism using client puzzles (Laishun, Minglei, & Yuanbo, 2010). The idea is that each connecting client should express its commitment to the connection by solving a puzzle. As an attacker will not have infinite resources, it will be impossible for him to create new connections fast enough to cause resource starvation on the serving node. A possible defense against de-synchronization attacks on the transport layer is to enforce an obligatory authentication of all packets communicated between nodes (Wood & Stankovic, 2002). If the authentication mechanism is safe, an attacker will not have the ability to send any spoofed messages to any destination node.

TABLE 1
Denial- of- Service Attacks and Countermeasures at Each Network Layer



Network Layer	Attacks	Countermeasures
Physical Layer	Jamming	Detect and sleep, route around jammed areas
	Node tampering	Tamper-proof boxing
Link layer/ medium access control	Collision, unfairness	Authentication and anti- replay protection
	Daniel of sleep	Authentication and anti- replay, detect and sleep, broadcast attack protection
Network and routing layer	Neglect and greed, misdirection, spoofing, replaying, routing- control traffic or clustering	Authentication and anti- replay protection, secure cluster formation
	Homing	Header encryption and dummy packets
	Hello floods	Pair- wise authentication, geographic routing
Transport layer	Flooding	SYN cookies
	De-synchronization	Packet authentication
Application layer	Overwhelming sensors	Sensor tuning, data aggregation
	Reprogramming attack	Authentication and anti- replay protection Authentication streams
	Path- based DoS	Authentication and anti- replay protection

5.9 Defense Against Sybil Attacks

Any defense mechanism against the Sybil attack must ensure that a framework is in place in the network to corroborate that a specific identity is the only identity held by a given physical node (Newsome et al., 2004). Newsome et al. have described three orthogonal dimensions of the Sybil attack taxonomy (Newsome et al., 2004). The three dimensions are: 1) direct vs. indirect communication, 2) fabricated vs. stolen identities, and 3) simultaneity. In direct communication, the Sybil nodes communicate directly with legitimate nodes. In this attack, when a legitimate node sends a radio message to a Sybil node, one of the malicious devices listens to the message. In indirect communication, no legitimate nodes are able to communicate directly with the Sybil nodes. Messages sent to a Sybil node are routed through one or more malicious nodes, which pass the message on to the Sybil node. In case of fabricated identities, the attacker creates arbitrary new Sybil identities. However, if a mechanism is in place to detect false identities, an attacker cannot fabricate new identities. In this case, the attacker needs to assign other legal identities to Sybil nodes. This identity theft may go undetected if the attacker destroys or, for a limited period of time, disables the impersonated nodes. In case of simultaneous attacks, the attacker tries to have all the Sybil identities participate in the network simultaneously. Repeatedly, the attacker may present a large number of identities over a period of time, while deploying a small number of identities at any given point of time.

Newsome et al. primarily describe direct validation techniques, including a radio resource test. In the radio test, a node assigns each of its neighbors a channel and listens to each of them. If the node detects a transmission on the channel, it is assumed that the node transmitting on the channel is a physical node. Likely, if the node does not discover a transmission on the specified channel, it assumes that the identity assigned to the channel is not a physical identity. Another technique to defend against the Sybil attack is to use random key pre-distribution techniques (Newsome et al., 2004). In random key pre-distribution, a random set of keys or key-related information are/is assigned to each sensor node. Thus, in the key set-up phase, each node can detect or compute the usual keys it shares with its neighbors. The common keys are used as shared secret session keys to ensure node-to-node secrecy. Newsome et al. have proposed that the identity of each node is associated with the keys assigned to the node (Jinchao, 2012). With a particular set of captured keys, there is little probability that a randomly created identity will work.

5.10 Defense Against Wormhole Attack

Hu et al. have proposed a new and general mechanism called packet leashes for discovering and defending against wormhole attacks (Y.-C. Hu, Perrig, & Johnson, 2003). In a wormhole attack, a malicious node eavesdrops on a series of packets, then tunnels them through a path in the network and sends them again. This is done to create a false representation of the distance between the two colluding nodes. It is also utilized, mostly, to prevent the routing protocol from continuing by misleading the neighbor discovery process. Guo et al. have presented a strategy based on neighbor node verification (Guo & Lei, 2011). Parasannajit et al. have also used an approach to detect wormholes in a WSN (Laishun et al., 2010).

In the mechanism proposed by the authors, a distance estimation is made between all the sensor nodes in a neighborhood. Using multi-dimensional scaling, a virtual layout of the network is then computed, and a surface smoothing strategy is applied to revise the round-off errors.

Finally, the form of the resulting virtual network is analyzed. If any wormhole exists, the form of the network will bend and curve towards the wormhole. Otherwise, the network will appear flat.

5.11 Related Works

Georgios Selimis et al. have proposed a lightweight security scheme for wireless body area networks. Integrating security functionality to a wireless sensor node increases the size of the stored software program in program memory, the required time that the sensor's microprocessor needs to process the data and the wireless network traffic which is exchanged among sensors. This security overhead has dominant impact on the energy dissipation which is strongly related to the lifetime of the sensor, a critical aspect in Wireless Sensor Network (WSN) technology. Strict definition of the security functionality, complete hardware model (microprocessor and radio), WBAN topology and the structure of the Medium Access Memory (MAC) frame are required for an accurate estimation of the energy that security introduces into the WBAN. In their work, they also estimated extra energy consumption that the security scheme introduces to WBAN based on commercial available off- the- shelf hardware components (microprocessor and radio), the network topology and the MAC frame (Selimis et al., 2011).

In 2011, Honggang Wang et al. proposed an integrated biometric- based security framework for wireless body area networks which takes advantage of biometric features shared by body sensors deployed at different positions of a person's body. The data communication among these sensors is secured via the proposed authentication and selective encryption schemes that require low computational power and less resource (e.g. battery and bandwidth). Specifically, a wavelet- domain Hidden Markov Model (HMM) classification method is utilized for accurate authentication according to the non- Gaussian statistics of ECG (electrocardiogram) signals. Furthermore, the biometric information such as ECG signal is utilized as the biometric key for the encryption in the framework (H. Wang, Fang, Xing, & Chen, 2011).

6 CONCLUSION

WBAN is an emerging and promising technology that will change people's healthcare experiences revolutionary. Security in sensor networks has been an increasingly important issue for academia, industry individuals and group working in this fast growing research area. In this paper, a discussion of the security requirements of WBANs has been proposed. Some well-known attacks and their proposed countermeasures are also discussed in the present report. There are many security solutions or mechanisms that have been proposed for WBANs. However, there is no security mechanism that can provide complete security. Designing a secure WBAN requires proper mapping of security solutions or mechanism with different security parameters.

We provided a comprehensive overview of existing security mechanisms for a WBAN. However, more efforts are required to introduce and implement new security levels that will satisfy the stringent security and privacy requirements of heterogeneous WBAN applications.

References

Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). A survey on sensor networks. *Communications magazine, IEEE, 40*(8), 102-114.

AL-Rassan, I. A., & Khan, N. (2011). Secure & Energy Efficient key Management Scheme for WBAN–A Hybrid Approach. *IJCSNS, 11*(6), 169.

Ali, A., & Khan, F. A. (2013). Energy-efficient cluster-based security mechanism for intra-WBAN and inter-WBAN communications for healthcare applications. *EURASIP Journal on Wireless Communications and Networking, 2013*(1), 1-19.

Barakah, D. M., & Ammad-uddin, M. (2012). *A survey of challenges and applications of wireless body area network (WBAN) and role of a virtual doctor server in existing architecture.* Paper presented at the Intelligent Systems, Modelling and Simulation (ISMS), 2012 Third International Conference on.

Boukerche, A., Oliveira, H. A., Nakamura, E. F., & Loureiro, A. A. F. (2008). Secure localization algorithms for wireless sensor networks. *Communications Magazine, IEEE, 46*(4), 96-101. doi: 10.1109/MCOM.2008.4481347

Boukerche, A., & Yonglin, R. (2009). A secure mobile healthcare system using trust-based multicast scheme. *Selected Areas in Communications, IEEE Journal on, 27*(4), 387-399. doi: 10.1109/JSAC.2009.090504

Chen, H., & Lou, W. (2010). *From nowhere to somewhere: protecting end-to-end location privacy in wireless sensor networks.* Paper presented at the Performance Computing and Communications Conference (IPCCC), 2010 IEEE 29th International.

Davenport, D., Seidl, N., Moss, J., Patel, M., Batra, A., HO, J., . . . Omeni, O. (2009). MedWin MAC and security proposal documentation. *IEEE Document*, 802.815-809.

Demirbas, M., & Song, Y. (2006). *An RSSI-based scheme for sybil attack detection in wireless sensor networks.* Paper presented at the Proceedings of the 2006 International Symposium on on World of Wireless, Mobile and Multimedia Networks.

Deng, H., Sun, X., Wang, B., & Cao, Y. (2009). *Selective forwarding attack detection using watermark in WSNs.* Paper presented at the Computing, Communication, Control, and Management, 2009. CCCM 2009. ISECS International Colloquium on.

Douceur, J. R. (2002). The sybil attack *Peer-to-peer Systems* (pp. 251-260): Springer.

Fallah, M. S. (2010). A puzzle-based defense strategy against flooding attacks using game theory. *Dependable and Secure Computing, IEEE Transactions on, 7*(1), 5-19.

Fenhua, C., & Min, J. (2010). *Improved gpsr routing algorithm and its performance analysis.* Paper presented at the Software Engineering and Service Sciences (ICSESS), 2010 IEEE International Conference on.

Guo, J., & Lei, Z.-y. (2011). *A kind of wormhole attack defense strategy of WSN based on neighbor nodes verification.* Paper presented at the Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference on.

Hamid, M. A., Mamun-Or-Rashid, M., & Hong, C. S. (2006). Routing security in sensor network: Hello flood attack and defense. *IEEE ICNEWS*, 2-4.

Hartung, C., Balasalle, J., & Han, R. (2005). Node compromise in sensor networks: The need for secure systems. *Department of Computer Science University of Colorado at Boulder*.

Hoyt, R. W., Reifman, J., Coster, T. S., & Buller, M. J. (2002). *Combat medical informatics: present and future.* Paper presented at the Proceedings of the AMIA Symposium.

Hu, L., & Evans, D. (2004). *Using Directional Antennas to Prevent Wormhole Attacks.* Paper presented at the NDSS.

Hu, Y.-C., Perrig, A., & Johnson, D. B. (2002). Wormhole detection in wireless ad hoc networks. *Department of Computer Science, Rice University, Tech. Rep. TR01-384*.

Hu, Y.-C., Perrig, A., & Johnson, D. B. (2003). *Packet leashes: a defense against wormhole attacks in wireless networks.* Paper presented at the INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies.

Huan-Bang, L., Takizawa, K. i., Bin, Z., & Kohno, R. (2007, 1-5 July 2007). *Body Area Network and Its Standardization at IEEE 802.15.MBAN.* Paper presented at the Mobile and Wireless Communications Summit, 2007. 16th IST.

Jinchao, Z. (2012). *Research on Key Predistribution Scheme of Wireless Sensor Networks.* Paper presented at the Intelligent Computation Technology and Automation (ICICTA), 2012 Fifth International Conference on.

Jonsson, J., & Kaliski, B. (2003). Public-key cryptography standards (PKCS)# 1: RSA cryptography specifications version 2.1.

Karlof, C., & Wagner, D. (2003). Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks, 1*(2–3), 293-315. doi: http://dx.doi.org/10.1016/S1570-8705(03)00008-8

Kavitha, T., & Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: A survey. *Journal of information Assurance and Security, 5*(1), 31-44.

Kim, N., Lim, H., Park, H. S., & Kang, M. (2010). Detection of multicast video flooding attack using the pattern of bandwidth provisioning efficiency. *Communications Letters, IEEE, 14*(12), 1170-1172.

Kwak, K. S., Ullah, S., & Ullah, N. (2010). *An overview of IEEE 802.15. 6 standard.* Paper presented at the Applied Sciences in Biomedical and Communication Technologies (ISABEL), 2010 3rd International Symposium on.

Laishun, Z., Minglei, Z., & Yuanbo, G. (2010). *A Client Puzzle Based Defense Mechanism to Resist DoS Attacks in WLAN.* Paper presented at the Information Technology and Applications (IFITA), 2010 International Forum on.

Le, X. H., Khalid, M., Sankar, R., & Lee, S. (2011). *An Efficient Mutual Authentication and Access Control Scheme for Wireless Sensor Networks in Healthcare* (Vol. 6).

Li, X., Chakravarthy, V. D., Wang, B., & Wu, Z. (2011). Spreading code design of adaptive non-contiguous SOFDM for dynamic spectrum access. *Selected Topics in Signal Processing, IEEE Journal of, 5*(1), 190-196.

Liu, J., & Kwak, K. S. (2010). *Hybrid security mechanisms for wireless body area networks.* Paper presented at the Ubiquitous and Future Networks (ICUFN), 2010 Second International Conference on.

Lorincz, K., Malan, D. J., Fulford-Jones, T. R. F., Nawoj, A., Clavel, A., Shnayder, V., . . . Moulton, S. (2004). Sensor networks for emergency response: challenges and opportunities. *Pervasive Computing, IEEE, 3*(4), 16-23. doi: 10.1109/MPRV.2004.18

Madria, S., & Yin, J. (2009). SERWA: A secure routing protocol against wormhole attacks in sensor networks. *Ad Hoc Networks, 7*(6), 1051-1063.

Malasri, K., & Lan, W. (2006, 25-28 Sept. 2006). *SNAP: an architecture for secure medical sensor networks.* Paper presented at the Wireless Mesh Networks, 2006. WiMesh 2006. 2nd IEEE Workshop on.

Malasri, K., & Wang, L. (2009). Design and Implementation of a SecureWireless Mote-Based Medical Sensor Network. *Sensors, 9*(8), 6273-6297.

Misra, S., & Myneni, S. (2010). *On identifying power control performing sybil nodes in wireless sensor networks using RSSI.* Paper presented at the Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE.

Nasser, N., & Chen, Y. (2007). SEEM: Secure and energy-efficient multipath routing protocol for wireless sensor networks. *Computer Communications, 30*(11–12), 2401-2412. doi: http://dx.doi.org/10.1016/j.comcom.2007.04.014

Newsome, J., Shi, E., Song, D., & Perrig, A. (2004). *The sybil attack in sensor networks: analysis & defenses.* Paper presented at the Proceedings of the 3rd international symposium on Information processing in sensor networks.

Ng, H. S., Sim, M. L., & Tan, C. M. (2006). Security issues of wireless sensor networks in healthcare applications. *BT Technology Journal, 24*(2), 138-144. doi: 10.1007/s10550-006-0051-8

Roman, R., Zhou, J., & Lopez, J. (2005). On the security of wireless sensor networks *Computational Science and Its Applications–ICCSA 2005* (pp. 681-690): Springer.

Rosello, V., Portilla, J., Krasteva, Y., & Riesgo, T. (2009). *Wireless sensor network modular node modeling and simulation with VisualSense.* Paper presented at the Industrial Electronics, 2009. IECON'09. 35th Annual Conference of IEEE.

Sadasivam, S., & Moulin, P. (2009). On estimation accuracy of desynchronization attack channel parameters. *Information Forensics and Security, IEEE Transactions on, 4*(3), 284-292.

Saleem, S., Ullah, S., & Yoo, H. S. (2009). On the Security Issues in Wireless Body Area Networks. *JDCTA, 3*(3), 178-184.

Selimis, G., Huang, L., Massé, F., Tsekoura, I., Ashouei, M., Catthoor, F., . . . Penders, J. (2011). A lightweight security scheme for wireless body area networks: design, energy evaluation and proposed microprocessor design. *Journal of medical systems, 35*(5), 1289-1298.

Shaikh, R., Lee, S., Khan, M. U., & Song, Y. (2006). LSec: Lightweight Security Protocol for Distributed Wireless Sensor Network. In P. Cuenca & L. Orozco-Barbosa (Eds.), *Personal Wireless Communications* (Vol. 4217, pp. 367-377): Springer Berlin Heidelberg.

Shi, E., & Perrig, A. (2004). Designing secure sensor networks. *Wireless Communications, IEEE, 11*(6), 38-43.

Sivaprasatham, V., & Venkateswaran, J. (2012). A SECURE KEY MANAGEMENT TECHNIQUE FOR WIRELESS BODY AREA NETWORKS. *Journal of Computer Science, 8*(11).

Tian, B., Han, S., Parvin, S., & Dillon, T. S. (2010). *A key management protocol for multiphase hierarchical wireless sensor networks.* Paper presented at the Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on.

Tumrongwittayapak, C., & Varakulsiripunth, R. (2009). *Detecting sinkhole attack and selective forwarding attack in wireless sensor networks.* Paper presented at the Information, Communications and Signal Processing, 2009. ICICS 2009. 7th International Conference on.

Wang, H., Fang, H., Xing, L., & Chen, M. (2011). *An integrated biometric-based security framework using wavelet-domain hmm in wireless body area networks (wban).* Paper presented at the Communications (ICC), 2011 IEEE International Conference on.

Wang, X., Gu, W., Chellappan, S., Schosek, K., & Xuan, D. (2005). *Lifetime optimization of sensor networks under physical attacks.* Paper presented at the Communications, 2005. ICC 2005. 2005 IEEE International Conference on.

Wood, A., & Stankovic, J. A. (2002). Denial of service in sensor networks. *Computer, 35*(10), 54-62.

Xiangqian, C., Kia, M., Kang, Y., & Pissinou, N. (2009). Sensor network security: a survey. *Communications Surveys & Tutorials, IEEE, 11*(2), 52-73. doi: 10.1109/SURV.2009.090205

Xiao, B., Yu, B., & Gao, C. (2007). CHEMAS: Identify suspect nodes in selective forwarding attacks. *Journal of Parallel and Distributed Computing, 67*(11), 1218-1230.

Yu, Y., Govindan, R., & Estrin, D. (2001). Geographical and energy aware routing: A recursive data dissemination protocol for wireless sensor networks: Technical report ucla/csd-tr-01-0023, UCLA Computer Science Department.

Zhiping, L., & Hui, L. (2010). *Mobile jamming attack in clustering wireless sensor network.* Paper presented at the Computer Application and System Modeling (ICCASM), 2010 International Conference on.