A Review of Attacks and Security Protocols for Wireless Sensor Networks

Fangmin Sun [1, 2], Zhan Zhao [1], Zhen Fang, Lidong Du [1], Zhihong Xu [1, 2], and Diliang Chen [1, 2]
1. State Key Laboratory of Transducer Technology Institute of Electronics, Chinese Academy of Sciences, Beijing, China
2. Graduate University of Chinese Academy of Sciences, Beijing, China
Email: sfm0719@163.com, {zhaozhan, zfang, lddu}@mail.ie.ac.cn

***Abstract*—With the development of the wireless communication technology and the improvement of the performance of the MEMS sensor, wireless sensor networks are widely used in various application scenarios such as smart building, intelligent transportation, ubiquitous and unobtrusive health monitoring system, etc. As information communicated among these networks is usually of privacy, so security in wireless sensor networks is of particular importance, and sensitive information must be protected from unauthorized usage for personal advantages and fraudulent acts. While, due to the extremely stringent constraints of energy, memory and computation ability, securing the communication among the sensors has posed various challenges to researchers. And at present, studies toward completely secure sensor networks are still in their infancy stages. In this paper, we explained the basic conceptions and the essential knowledge in the area of wireless senor network; and then we introduced and classified the common security attacks designed to demolish the wireless sensor networks, and the corresponding countermeasures against these issues are followed; examples of security problems in the application of health monitoring field are specially presented in the last section; and finally, we summarized the paper and imagined the possible future development of the security problems of the wireless sensor networks. I hope through this paper, one can learn the recent development of the attack and securing technology in the wireless sensor network and then develop more advanced anti-attack methods.**

***Index Terms*—Wireless Sensor Networks; Constraints; Security Requirements; Attacks; Security Policies; Body Sensor Networks**

I. INTRODUCTION

Wireless sensor networks (WSNs) are based on the random deployment of a large number of tiny, low-cost, and resource-constrained sensor nodes into or very close to the phenomenon to be observed [4]. These sensors sample the required environmental, physiological or other kinds of information and then transmit it to the sink nodes or gateways which further send the information to the central server or database through the internet, the typical architecture of the WSN is shown in Fig1.

WSNs have facilitated many application areas such as tactical surveillance [32], camera and video surveillance [35, 61], body sensor networks for health monitoring [1, 2, 7-11], homeland security monitoring [12], intelligent transportation [5, 6] and smart building [33, 34, 38, 39], etc. Information and data security in many of these applications is very critical, and furthermore, the distributed and randomly deployed nature of these sensor nodes at remote areas makes them vulnerable to numerous security threats. In many cases, the WSN attacks eavesdrop critical information transmitted through the radio, diffuse fake messages or/and make the whole network smashed down; and more seriously, the security breach can result in physical side effects, personal injury, and even death. So in order to make the above mentioned and many more other application scenarios practical, the WSNs must be secured against attacks.

A network attack can be defined as any method, process, or means used to maliciously attempt to compromise network security [30]. Network attacks can be launched in any layer of the ISO network model and can do many kinds of damages to the network. For example, attackers can physically overwrite the memory of the sensor nodes, tamper the data transmitted among the networks, inject bits in the channel, replay previously heard packets, exhaust the energy of the sensor nodes and so on.

Network security services are the collection of all policies, mechanisms, and services that afford a network the required protection from unauthorized access or unintended uses. These services are generally categorized into two broad classes, namely communications security and computer security [16]. Communications security ensures that communication services continue with the required level of quality and that classified data or information cannot be derived or captured from communications by an unauthorized node. It defends against passive or active attacks through communication links or unintentional emanations. Computer security ensures the security of computer hardware and software. It detects when a node or host is compromised, and recovers that specific node or host from the attack.

For is the sensor nodes are usually placed in an opened environment and with extremely limited energy, computation ability and memory resources, Wireless senor networks are not like wired sensor network or other types of wireless networks, and it is more easily for the WSNs to be attacked and more challenging to ensure the

doi:10.4304/jnw.9.5.1103-1113

security of the WSN. Nowadays, the security of wireless sensor networks has been widely studied and many wonderful security policies have been proposed.

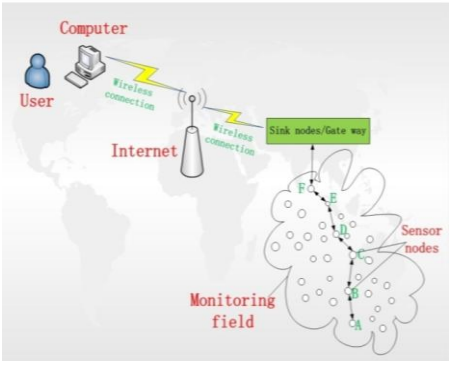

Figure 1. The typical architecture of the wireless sensor networks

Studies on the security of the WSNs are many, for example, the low energy consumption and high security sensor network architecture-MiniSec proposed in [17] provides MAC layer security for the netwoek system. While, authors of paper [13] has put forward a means called UNMASK to mitigate wireless sensor network attacks by detecting, diagnosing, and isolating the malicious nodes. And a practical and effective sinkhole resilient protocol for wireless sensor networks is presented in [36]. and a group-based security scheme for wireless sensor network is devised and tested in [37]; and [40] proposed an authentication scheme for healthcare monitoring system; a novel secure key establishment protocol which is suitable for low resource sensor nodes is presented in [20]. While due to the unique characteristics of the wireless sensor networks, there are still some deficiencies in the existing security protocols. Some security protocols are too power-consuming to apply to the sensor nodes, while others may too complex and memory consuming to adapt to wireless sensor networks.

The main contributions of this paper can be summarized as the following: 1. clearly provided some basic conceptions related to the WSNs and network security; 2. pointed out the unique characteristics and the specific security requirements of the WSNs; 3. offered a brief overview of the general attacks and corresponding security policies; 4. more clearly illustrated the security problems of wireless sensor networks in a specific application instance of medical and health monitoring area.

II. BACKGROUND

Wireless sensor networks is mainly served as an interface to the real world, which provides physical information such as temperature, light, radiation, etc. to a computer system. The major difference between this type of networks and wired networks is their decentralized and specialized nature [44]. Through security and privacy are enormous challenges in all types of wired and wireless networks, while these challenges are of much greater importance in WSNs for the unique features of these networks and the application purposes they serve. For example, sensor nodes are typically very resource-constrained and operate in harsh environment, which facilitates compromises and makes it more difficult to distinguish security breaches from node failures, varying link qualities, and other commonly found challenges in sensor networks. The unique characteristics of the WSNs require security mechanisms customized for WSN applications must to be efficient, low computing complexity and low power consumption.

A well-designed and practical security protocol should be based on the preknowledge of the network's security standards and the existing problems to secure the network. In the following part of this section, we provided a detail description of the security requirements and the existing challenges of securing WSNs.

A. Security Requirements for Wireless Sensor Networks

The security level of the wireless sensor networks is different depending on the specific applications. For example, military applications are extremely security-critical and the breach of the network may lead to very serious results such as the leakage of the key military information of the state or making the battle devices systems disabled, while habitat monitoring are relatively benign ones.

About the security requirements for wireless sensor networks, it seems have no uniform standard at present. Four goals of the security: confidentiality, integrity, authentication, and availability (CIAA) are widely accepted and used in previous studies [14, 15]. Through it seem to be very concise, it may not take everything into consideration. Some More detailed descriptions of this problem have been developed and we synthesized the previous study results and provided the general security requirements for wireless sensor networks in Table1.

And there are many other important security requirements for the security protocols such as low power consumption and low computation complexity, small size of the codes, etc. that need to be considered when design a practical WSN security algorithms. At present, many high performance and efficient schemes for resource constrained WSNs have been studied and proposed.

Paper [19] devised a security protocol which synthesized merits of different cryptographic primitives and realized high security level and low energy consumption; while, paper [45] proposed an secure Energy Efficient Traffic-Aware Key Management (EETKM) scheme, which only establishes shared keys for active sensor nodes that participate in direct communication; in paper [46], the authors proposed an efficient secure group communication scheme (RiSeG) guaranteeing secure group management and secure group key distribution, the scheme is based on a logical ring architecture and not only provides backward and forward secrecy but also addresses the node compromise attack; The authors of [47] introduced a new class of cryptographic schemes, referred to as Hash-Based Sequential Aggregate and Forward Secure Signature (HaSAFSS), which allows a signer to sequentially generate a compact, fixed-size, and publicly verifiable signature efficiently.

TABLE I. SECURITY REQUIREMENTS OF THE WIRELESS SENSOR NETWORKS [14-16]

Confidentiality	To ensure that all sensitive data should be accessible only to the authorized people and should not be leaked across adjacent sensor networks.
End to end message authentication	Sensor nodes in the network should be able to identify if the data packets is really come from another authorized sensor nodes when it received a message. Message authentication is aim at preventing the unauthorized personnel from participating in the network.
Robustness and survivability	Sensor network should be robust enough to resist the various attacks and if an attack succeeds, the impact should be minimized.
Data integrity	The receiver could identify the received messages are not altered or tampered by the middle nodes.
Data freshness	Sensor nodes should be able to identify the new received data packet is the sender's latest generated messages rather than the replay of old messages by unauthorized personnel.
Availability	Ensure that the desired network services are available even in the presence of denial of service attacks.
Self-organization	Nodes should be flexible enough to be autonomous self-organizing and self-healing
Fault tolerance	The network should be able to detect the deficient nodes and correct it. For example, it can modify the routing table to find another route to send data.
Time Synchronization	The security protocols should not be manipulated to produce incorrect data.
Security management	Includes security induction and security maintenance.
Broadcast authentication	A security authentication problem of a single node sending uniform notification to all or a group of nodes.

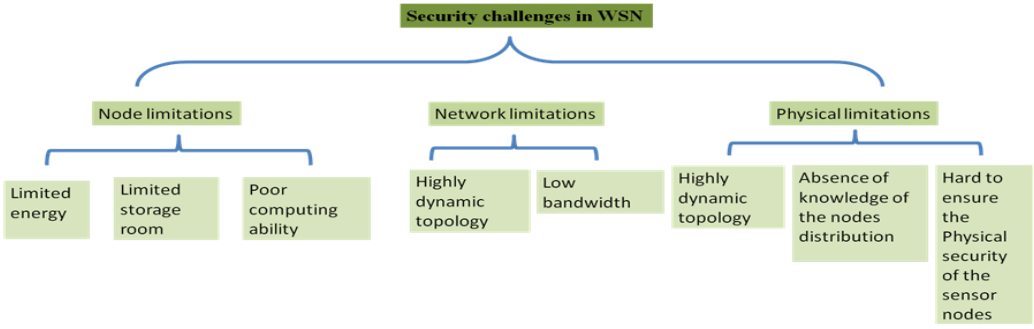

Figure 2. Security challenges in WSN

All these security schemes reduced their resource consumption quite remarkably compared to the conventional security protocols used for the wired or other types of networks, while these schemes may perform less well in large scale networks as it may introduce longer latencies when the number of nodes grows and when neighbor nodes are physically far from each other.

B. Challenges of Security in Wireless Sensor Networks

Wireless sensor network is a special kind of wireless networks but it is different from the common wireless networks in aspects of the number of nodes, computing ability, memory space, energy, band width and communication ability [60]. For the unique characteristics of the WSN, there are many challenges for the security of the WSN. In Fig.2, we generally classified these challenges into three types: node limitations, network limitations and physical limitations. We briefly explained why these are security challenges in WSN in the following section.

1) Limited Energy, Memory and Computing Ability

Wireless sensor nodes are always small in size and powered by batteries, and the energy and memory resources of the sensor nodes are extremely constrained. Thus the WSNs always choose the low data rate and low power consumption wireless communication.

Technologies such as Zigbee, Bluetooth 4.0, etc. traditional security mechanisms that have high overheads are not suitable for resource-constrained WSNs. Waltenegus Dargie, et al introduced this problem in detail in [15].

2) Absence of Knowledge of the Nodes Distribution

The sensor nodes are always randomly distributed in the monitoring target area, it is difficult to ensure that any two nodes in the network have at least one direct or indirect connection. So the commonly used public and private key mechanism are no longer suitable to wireless sensor networks.

3) Hard to Ensure the Physical Security of the Sensor Nodes

In many applications, nodes of the WSNs are operated in the remote, unattended and hard-to-reach locations, and deployed in environments open to public access. It is often the case that the number of the nodes is too large to make it feasible to continuously monitor and protect sensor nodes from attack. These challenges make it difficult to prevent unauthorized physical access and to detect tampering with the sensor devices. Particularly, the low cost of many sensor nodes may not allow advanced or expensive protective measures.

4) Highly Dynamic Topology

Certain popular wireless sensor network applications, including disaster recovery, battlefield communication and athlete monitoring, are characterized by extensive node mobility, intermittent contact between nodes and a highly dynamic network topology. Traditional security schemes are designed for essentially static networks and do not perform well in these cases [18].

5) Low Bandwidth

Wireless sensor networks usually work at the unlicensed 2.4-2.4835GHz frequency range which is shared among major wireless standards such as Wi-Fi and Bluetooth. Most of sensors use the IEEE 802.15.4 protocol [48, 49] to communicate. Zigbee protocol which provides an energy-efficient communication and allows a large number of nodes in a network (60,000 nodes) is one of the most used protocols based on 802.15.4. All in all, in many applications bandwidth is very valuable resource.

Sum up, to secure the wireless sensor networks, one needs to take all the above limitations of the wireless sensor networks into consideration, and try to find practical means and ways to overcome these limitations and protect the information and the network of the WSN.

III. Attacks and Threats on Wireless Sensor Networks

The WSN attacks are similar to that of other types of networks. There are many attacks that have been identified in WSN by the researchers in their literatures.

For example, physical attacks are introduced in detail in [52] and corresponding trusted platform with protected memory that not only protects sensor node's sensitive credentials but also provides a concrete way to trust nodes in the dedicated wireless sensor network was presented; [53] investigated and classified the detection methods of node replication attacks and studied the technical details; while single hop detection method for node clone attacks in mobile wireless sensor networks are described in [56]. In the paper [54], the authors exploit the Hidden Markov Model (HMM) Viterbi algorithm to detect the wormhole attack based on the maximum probabilities computed for a hidden state transition. A model for distributed node exhaustion attacks is proposed in [55]. And different methods to prevent Dos attacks are presented in [58, 59, 62]. And the model of Hello Flood Attack and its countermeasures are presented by Virendra Pal Singh et al in [67], while mobile malicious node attacks and the countermeasures are introduced in [57].

These security attacks can be classified on various criteria, such as the domain of the attacks, or the techniques used in attacks. In this paper, we synthesized the previous studies [22, 23, 31, 51, 70] and roughly classified these network attacks in WSNs by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related. In the following section of this chapter we will introduce these types of attacks in detail.

A. Passive and Active Attacks

According to whether the attacks interrupt the network communication, they can be classified into two major categories: passive attacks and active attacks. A passive attack is said to be the attack obtain data exchanged in the network without interrupting the communication. While an active attack is referred to be the attack implies the disruption of the normal functionality of the network, meaning information interruption, modification, or fabrication. Examples of passive attacks are eavesdropping, traffic analysis, and traffic monitoring etc. Examples of active attacks include jamming [21], impersonating, modification, Denial of Service (DoS), and message replay etc.

B. Internal or External Attacks

According to the domain of the attacks, they can be classified to be internal (insider) and external (outsider) attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows the valuable and secret information. The detail definitions of internal and external attacks are as following:

External attacks: external attacks are launched by external devices. The adversary adopts the means to eaves drop on information, injecting fractional data, and fabricating non-existent records to disturb the normal running of the whole network. It does not control any legitimate sensor nodes thoroughly. Fortunately, such attacks are relatively easier to resist through a combination of cryptography-based and robust communication techniques [51].

Internal attacks: in the internal attacks, the adversary firstly compromises several nodes and accesses all secret information (e.g. cryptography and authentication) stored in the compromised nodes, and then controls the compromised nodes to attack other nodes. It is clearly to see that the invaders of the internal attacks are the sensor Nodes of the WSN itself and these nodes are turned into traitorous nodes.

C. Stealthy and Non-Stealthy Attacks

In a stealthy attack, the goal of the attacker is to make the network accept a false data value. For example, an attacker injects a false data value through that sensor node. In these attacks, keeping the sensor network available for its intended use is essential. And non-stealthy attacks are the other way round.

D. Attacks on Different Layers of the Internet model

The attacks can be further classified according to the five layers of the internet model. Table2 presents a classification of various security attacks and corresponding countermeasures on each layer of the Internet model. It must be noted that network attacks on different layers could be launched at the same time and some attacks can be launched at multiple layers.

Although we discuss the attacks separately in this chapter, it is often the case that the attacks are launched in combination and the combination can be cross-layer in which multiple attacks in different layers are launched in a collaborative way. Examples of multilayer attacks are denial of service (DoS), man-in-the middle, and impersonation attacks.

Take the Denial of Service (DoS) attacks as an example, A DoS attack can be characterized as an attempt of an adversary to stop a network from functioning or to disrupt the services a network provides [15]. DoS attacks could be launched from several layers such as physical

TABLE II. SECURITY ATTACKS AND COUNTERMEASURES ON EACH LAYER OF THE WSNS MODEL

layer	Attacks	countermeasures
Physical layer	Jamming	Hopping, broadband, low duty cycle or mode conversion
	Interceptions or Eavesdropping	Keying method
	Tampering	Node camouflage and hiding
MAC layer	Collision	Using error correction code
	Exhaustion	Setting competitive threshold
	Unfairness	Using short frame strategy or non-priority strategy
Network layer	Neglect and greed	Using redundant paths or detection mechanism
	Homing	Using encryption or hop by hop authentication mechanism
	Misdirection	Egress filtering; authentication, monitoring mechanism
	Blackholes	Authentication, surveillance and redundancy mechanism
Transport layer	Flooding	Client puzzle
	Desynchronization	Authentication
Application layer	Repudiation	Sensor node identity; detection mechanism
	Data corruption	Data retransmission mechanism
Multi-layer attacks	Denial of service(DoS)	Strong authentication and identification of traffic
	Impersonation replay	Adding nonce information or time related counter information to the transmitted data packets
	Man-in-the-middle	Authentication, identity verification and bidirectional link verification

layer, data linker layer, network layer or transport layer, etc. An attacker can employ signal jamming at the physical layer, which disrupts normal communications. At the link layer, malicious nodes can occupy channels through the capture effect taking advantage of the binary exponential scheme in MAC protocols and prevents other nodes from channel access. At the network layer, the routing process can be interrupted through routing control packet modification, selective dropping, table overflow, or poisoning. At the transport and application layers, SYN flooding, session hijacking, and malicious programs can cause DoS attacks. And most often the case, the attack is resulted either by an unintended failure of a node or by unauthorized access of the sensor node. In this case, an intended user is refused of few services. The DoS attack model is presented in [58] by Ju-Hyung Son et al.

IV. SECURITY APPROACHES FOR WIRELESS SENSOR NETWORKS

Security problems are existed in all kinds of networks, and where there are attacks there are corresponding anti-attack mechanisms. Nowadays, network security mechanisms are fairly mature and perfect for the wired networks while it is still in the elementary level in the area of wireless sensor networks. However, fast development and high improvement in WSN security approaches have been achieved in recent years. For the wired and wireless networks, generally, three types of cryptographic primitives are used to provide security services, public key primitives, private key primitives, and hashing functions [50]. Efficient implementations of these primitives for WSNs have been addressed by many researchers in the literature. These implementations can be done either in software or hardware.

Security related issues and challenges in wireless sensor networks are explored in many literatures. It is widely realized that the security methods for existing networks which include mobile ad-hoc network are not well suitable for wireless sensor networks because of the unique characteristics of the WSNs; and the security of WSNs is more difficult and challenging than that of the wired networks or other kinds of wireless networks. Difficult as it is, researchers have overcome numerous challenges and come up with many wonderful security proposals that are suitable for WSNs. In this section, we will summarize the countermeasures to different attacks on different layers of the internet model.

A. Countermeasures in the Physical Layer

The physical layer is concerned with transmitting raw bits of information over wired/wireless medium. It is responsible for signal detection, modulation, encoding, frequency selection and so on, and is hence the basis of network operations [31].

As the sensor nodes are always deployed in the open environment which is out of surveillance of operators, it is often difficult to ensure the physical security of the sensor nodes and the physical layer attacks are challenging to cope with. For example, in the application of forest fire detection, after the sensor nodes are deployed in the open and unattended field, it is very likely that the sensor nodes suffered from physical tamper, and to some extent, it is hard to prevent this from happening. Therefore, although there are some mechanisms that attempt to reduce the occurrences of attacks, more of them focus on protecting information from divulgence.

There are two main approaches that are available to solve this problem: access restriction and encryption. Obviously, through restricting adversaries from physically accessing or getting close to sensors is effective on all the attacks aforementioned, but unfortunately, they are either difficult or infeasible in most cases. Therefore, we usually have to fall back on another type of restrictions: communication media access restriction. By and large, cryptography is the all-purpose solution to achieve security goals in WSNs. It not only can be applied to the data stored on the sensor but also

can be applied to the data in transmission. Cryptography mechanisms are generally classified into two kinds: asymmetric and symmetric. In asymmetric mechanisms the keys used for encryption and decryption are different while in symmetric mechanisms the two nodes share a key to encrypt and decrypt data. So, asymmetric cryptography usually consumes more resources such as computation and memory than symmetric one when compared. Cryptography is indispensable to protect data confidentiality. Once data are encrypted, even if the sensors are captured, it is difficult for the adversaries to obtain useful information. Therefore, the strength of the encryption depends on various factors. As a rule, a more costly encryption can yield higher strength, but it also consumes more valuable resource such as energy, memory, etc. of the network [31].

The key management technique of the encryption method is key establishment and key distribution. A number of key pre-distribution schemes have been developed. A very simple approach is to have a unique pre-loaded key that is shared among the nodes. Then all sensors can encrypt or decrypt data between themselves using this key. Due to its simplicity, this method is very efficient in regards to memory usage and processing overhead, but it suffers from a very serious security problem. If even one of the sensors is captured by an adversary, the security of the entire network will be compromised. Another simple approach, called the basic scheme, is to generate a distinct key between every pair of sensors and store these in the sensors. In this case, if N sensors are deployed in the network, each must store (N-1) keys. Despite ideal resilience, this scheme is not scalable, and is not memory efficient, particularly in large networks. In addition, after node deployment, if a new node wants to join the network, none of the previously deployed sensors will have a common key with the new node [20].

Seen from previous literatures, it is easy to found that the rational and the conventional solution for key management in WSN is to distribute randomly generated keys to each sensor node, this method, to some extent, is energy consuming. Recently, there are many improved schemes have been proposed. An efficient key distribution scheme which is useful to secure data-centric routing protocols in Wireless Sensor Networks is introduced in [63], and this scheme is permit to use local key distribution process to establish Group Key and Pairwise Key. Ali Fanian et al. proposed a novel key establishment protocol which is not only energy efficient but also has low memory requirements and low computational overhead [20]. A secure and Energy-Efficient Traffic Aware key Management (EETKM) is developed for WSN in [45], and this key management scheme can be applied for various routing protocols and is characterized by stronger resilience, low energy consumption and increased delivery ratio. In [64], Shaila K et al. proposed a scheme called Modified Bloom's Scheme (MBS) which makes use of asymmetric matrices in place of symmetric matrices in order to establish secret keys between node pairs. Logical Neighbor Tree (LNT) secure group communication scheme proposed in [78] helps to eliminate the heavy storage cost introduced by the key encryption keys used in the many other schemes and, simultaneously, provides both authentication and robustness against replay attacks of the rekeying messages.

B. Countermeasures in the MAC Layer

Attacks in the MAC layer can be generally classified into two types: traffic manipulation and identity spoofing. To counter attacks in the MAC layer, current researches focus on detection. But it also allows for many kinds of further actions to stop the attacks, such as excluding the attacking nodes from interactions. And for the kind of spoofing attacks, prevention should be a good way [66].

Misbehavior Detection: Because attacks deviate from normal behaviors, it is possible to identify attackers by observing what has happened. Various data can be collected for this purpose, and various actions can be taken after detection.

Identity Protection: Identity can be treated as yet another kind of information whose legitimacy needs to be guaranteed. Therefore, cryptography-based authentication can be used to prevent identity spoofing. Although most authentication schemes are designed for the network layer and the application layer, Readers should keep in mind that the authentication techniques can also be applied to identity protection in the MAC layer.

There are mainly three types of attacks effective on the MAC layer: collision attacks, exhaustion and unfairness. For the collision attacks of the MAC layer, the following two approaches can be taken to deal with: 1. using the error correction code; 2. using the channel monitoring and data retransmission mechanism. One measure to cope with the exhaustion attack is to restrict the transmission speed of the network, the sensor nodes automatically abandon the redundant data requires, while the defect of this method is the falling of the network efficiency. In [55], the authors presented the model of the exhaustion attack and a pattern recognition based way is devised to detect this kind of attack too. Unfairness attack to some extent is a kind of infirm DoS attack, using short packets is one of the mitigating approaches for unfairness attack.

C. Countermeasures in Network Layer

The network layer is responsible for routing of messages from node to node, node to cluster leader, cluster leaders to cluster leaders, cluster leaders to the base station, and vice versa. In the network layer, the key issues include locating destinations and calculating the optimal path to a destination.

By attacking the routing protocols, attackers can absorb network traffic, inject into the path between the source and the destination, and control the network traffic flow. Security of routing protocols depends on the location of nodes and the encryption techniques.

A typical kind of network attack is sinkhole attack, where malicious sensors pretend to be closer to the sinks than all their neighbors. Attracting more traffic, these sensors can either selectively drop the received data (i.e. selective-forwarding attack) or collect sensitive

information. And ways to resist sinkhole attack is proposed in [41, 68].

Clearly, the protocols that construct a routing topology would be significantly affected by these attacks. The attackers can create routing loops, introduce severe network congestion, and channel contention into certain areas. There are malicious routing attacks that target the routing discovery or maintenance phase by not following the specifications of the routing protocols. Since the functionalities of the network layer require the close collaboration of many nodes, all these nodes have to be enclosed for security consideration. It is therefore relatively difficult to mitigate attacks. Nonetheless, some countermeasures are available as follows:

• Routing Access Restriction

There are two ways to restrict the routing access, they are multi-path routing and authentication, and authentication can be end to end or hop by hop. Nowadays many researchers combined the former two methods and formed the multi-path authentication.

• False Routing Information Detection

By attacking the routing protocols, attackers can absorb network traffic, inject themselves into the path between the source and destination, and thus control the network traffic flow. The traffic packets could be forwarded to a non-optimal path, which could introduce significant delay. In addition, the packets could be forwarded to a nonexistent path and get lost. Ways for detecting false routing information are widely studied [24, 74-76].

• Wormhole Detection

An attacker records packets at one location in the network and tunnels them to another location. Routing can be disrupted when routing control messages are tunneled. This tunnel between two colluding attackers is referred as a wormhole [23]. Wormhole detection methods are widely studied by many researchers, and [65, 69] introduced two different wormhole detection methods separately.

Reliability and security of broadcasting is critical in Wireless Sensor Networks. E. Ayday et al built an authentication scheme, on top of a reliable and energy efficient broadcasting protocol called Collaborative Rateless Broadcast (CRBcast) to improve efficiency and reliability. This scheme is tested to be resilient to adversary such as routing and flooding attacks and protocol exploits [77].

D. Countermeasures in the Application Layer

The application layer implements the services seen by users. Two examples of important applications in WSNs are data aggregation and time synchronization, where data aggregation sends the data collected by sensors to base stations, and time synchronization synchronizes sensor clocks for cooperative operations.

The application layer contains user data, and supports many protocols such as HTTP, SMTP, TELNET, and FTP, which provide many vulnerabilities and access points for attackers. The application layers attacks are more attractive as they have direct access to the application data. Attacks in the application layer rely on application data semantics. Therefore, the countermeasures focus on protecting the integrity and confidentiality of data, no matter it is for control or not.

Data Integrity Protection: Data Integrity in its broadest meaning refers to the trustworthiness of information over its entire life cycle [32]. In general, authentication can be used to protect any data integrity.

Data Confidentiality Protection: Encryption is an effective approach to prevent attackers from understanding captured data. Similar to authentication, the principles of encryption do not change for use in different layers.

Anti-attack during data collection is a crucial challenge in WSNs for the sensor nodes are usually deployed at unattended or hostile environments, an adversary an easily compromises several sensor nodes and controls them to launch attacks. Due to the unreliable wireless channels and unsupervised feature of WSNs, the sensor nodes are very easy to be compromised and difficult to be detected. To provide secured sensory data delivery, some security mechanisms have been developed for based on traditional key establishment [79], authentication [43], access control [71], etc. Unfortunately, these security mechanisms cannot provide satisfactory solutions to the internal attack, which can easily acquire the valid cryptographic keys and intercept any packet transmitted through the compromised node.

Several trust models in different application situations have been proposed with various mathematical methodologies. However, presently there is a lack of uniformity for criteria to estimate the performance of those trust mechanisms. Most comparisons of simulation results are limited to the different parameters of the trust model itself, or they fall into the two occasions: with the trust mechanism or without the trust mechanism. Therefore, it is a struggle to build a series of standard evaluation methods for the trust scheme to judge which trust model is much better than the others and why [51].

V. SECURITY OF BODY SENSOR NETWORKS AS AN EXAMPLE

Wireless sensor networks are widely used in various aspects of our life, from simple monitoring of the environment temperature and humidity to complex and significant applications in military surveillance and control. Through there are some slightly differences, the security problems and corresponding countermeasures for different applications are by and large similar. To get a well understanding of the security problems and anti-attack mechanisms of the wireless sensor networks, we took the recently popular and booming application area: medical and health monitoring as an example, and introduced the security problems and approaches in Body Sensor Network (BSN).

As health has become a hot issue among the young and the old, BSN, as a low-cost and convenient method for continuous and long-term health monitoring, has become a burgeoning study field for a few years. Health monitoring involves collection of data about vital body parameters from different parts of the body and making

decisions based on it. This information is of personal nature and is required to be secured [3].

As body sensor network is just a special kind of WSNs, attacks aimed at the WSNs are all effective in the area of BSNs, while for the application of health monitoring the more challenging security problem may be the access authorization, data freshness and data integrity. The patients' physiological signals transmitted through the BSNs are of privacy and they must be restricted that only the authorized person has the right to access them. The leakage of health information may result in the illegal usage. And the BSNs must ensure the freshness, integrity and exactness of the physiological data of the patient so as to the appropriate treatment could be given to the patient on time.

Up to date, security studies for BSNs were many, and different measures are introduced and discussed in [25-29, 33, 43, 71 and 72]. To sum up, for key establishment and authentication, biometrics based methods are widely studied and used, some recent BSNs security mechanisms are introduced here.

Biometrics based BSNs security schemes are proposed in many literatures. The main criterion for a biometric to be suitable for security purpose is whether it is random enough for it to be used to build security system.

For example, BIOSEC [26] examined the utility of various biometric for security purpose. The authors proposed a security mechanism which makes use of biometric derived from the human body to secure the keying material which in turn is used to secure the data communication. The small shortcoming of this biometrical security approach may be the lack of sufficient randomness. In contrast, BSK-WBSN: a biometrics based symmetric cryptographic key establishment approach proposed by Samira Mesmoudi et al. take into account the network topology and the change in the real time, the physiological data have specific properties as changing with time and high level of randomness [29].

While, BLIG (short for: Blinking Led Indicated Grouping) presented in [27] is an approach to deployment of wireless body sensor networks on patients in critical situations, like accidents. It described the requirements for BLIG and explains how the design fulfils these requirements for fast, easy, and secure deployment. But it needs to formalize and prove the security properties and some more extensive scalability analysis and tests may be needed in order to ensure that the technology is capable of handling rather large-scale emergencies with high densities of victims.

In [28], the author introduced IBE-Lite, a lightweight identity-based encryption suitable for sensors, and developed protocols based on IBE-Lite for a BSN. In [25], the authors proposed security solutions to identify attacks on data freshness and preserve message integrity in these networks while [33] introduced an approach to symmetric cryptographic key establishment, based on biometrics physiology.

To sum up, all these approaches toward to solve wireless body sensor network constraints and to meet its security requirements while different measures and structures were taken. Body sensor network as a special kind of wireless sensor network is facing the same security challenges and problems that the WSNs faced, however, BSN could take advantage of the physiological signal it sampled from human body to secure the network, which is other kinds of WSNs could not use. Human physiological signals possess the characteristics of universality, uniqueness, randomness, stability and secrecy. So new information security system based on biometric authentication is green, low power consumption, convenient and transparent to users, and it will be widely used in mobile medical system.

VI. CONCLUSIONS

The future of wireless sensor networks is promising; they are being deployed in many real-world applications, in the context of Ubiquitous Computing, Pervasive Computing, and Ambient Intelligence. In this paper, we concluded the unique characteristics of the wireless sensor networks and presented the requirements and the corresponding challenges of the WSNs security. Commonly seen WSNs attacks are introduced and classified according to different criteria and security approaches and key security techniques are presented in the following. Finally, we summarized the security related issues and technologies in the area of body sensor networks as an illustrative example of the WSNs attacks and security mechanisms. Hopefully by reading this paper, the beginners can have a better view of attacks and countermeasures in wireless sensor networks and the researchers can be motivated to design smarter and more robust security mechanisms and make their networks safer.

REFERENCES

[1] Sana Ullah, Pervez Khan, Niamat Ullah, Shahnaz Saleem, Henry Higgins, Kyung Sup Kwak. A review of wireless body area networks for medical applications. *Network and System Sciences*, 2009.

[2] Guangzhong Yang, Body sensor networks. Springer, 2006.

[3] M. Chen, S. Gonzalez, A. Vasilakos. Body area networks: A survey. *ACM/Springer Mobile Networks and Applications*, vol. 16, no. 2, April, 2011, pp. 171-193.

[4] Erdal Çayırc, Chunming Rong. Security in wireless Ad Hoc and sensor networks. *John Wiley & Sons Ltd*, 2009, pp. 1-7.

[5] Vivek Katiyar, Prashant Kumar, Narottam Chand. An intelligent transportation systems architecture using wireless sensor networks. *International Journal of Computer Applications* (0975 – 8887), pp. 22-26, January 2011.

[6] David Tacconi, Daniele Miorandi, Iacopo Carreras, Francesco Chiti, Romano Fantacci. Using wireless sensor networks to support intelligent transportation systems. pp. 462-473, *Ad Hoc Networks 8*, 2010.

[7] Hans De Clercq, Robert Puers. A neonatal body sensor network for long-term vital signs acquisition. *Sciverse Science Direct, Procedia Engineering 47*, 2012, pp. 981-984.

[8] Yeongjoon Gil, Wanqing Wu, Jungtae Lee. A synchronous multi-body sensor platform in a wireless body sensor

network: design and implementation. *Sensors 2012*, 12, pp. 10381-10394.
[9] Chiung-An Chen, Shih-Lun Chen, Hong-Yi Huang, Ching-Hsing Luo. An asynchronous multi-sensor micro control unit for wireless body sensor networks (WBSNs). *Sensors 2011*, pp. 7022-7036, July 2011.
[10] Shih-Sung Lin, Min-Hsiung Hung, Chang-Lung Tsai, Li-Ping Chou. Development of an ease-of-use remote healthcare system architecture using RFID and networking technologies. *Springer Science+Business Media, J Med Syst, February 2012.*
[11] Lin Liu, Jing Liu. Biomedical sensor technologies on the platform of mobile phones. Front. Mech. Eng. *Springer*, pp. 160-175, January 2011.
[12] Radislav A. Potyrailo, Nandini Nagraj, Cheryl Surman et al, Wireless sensors and sensor networks for homeland security applications. *Trends in Analytical Chemistry*, Vol. 40, pp. 133-145, 2012.
[13] Issa Khalil, Saurabh Bagchi, Cristina N. Rotaru, Ness B. Shroff. UNMASK: Utilizing neighbor monitoring for attack mitigation in multihop wireless sensor networks. *Ad Hoc Networks 8*, pp. 148-164, 2010.
[14] Azzedine Boukerche. Algorithms and protocols for wireless sensor networks. *John Wiley & Sons Ltd*, 2009, pp. 479-502.
[15] Waltenegus Dargie, Christian Poellabauer. Fundamentals of wireless sensor networks: theory and practice. *John Wiley & Sons Ltd*, 2010, pp. 267-284.
[16] Manju. V. C. Study of security issues in wireless sensor network. *International Journal of Engineering Science and Technology (IJEST)*, Vol. 3 October 2011, pp. 7347-7352.
[17] Mark Luk, Ghita Mezzour, Adrian Perrig, Virgil Gligor. MiniSec: A secure sensor network communication architecture. *IPSN'07*, April pp. 25-27, 2007.
[18] Syed Taha Ali, Vijay Sivaraman, Ashay Dhamdhere. A per-hop security scheme for highly dynamic wireless sensor networks. *IEEE 2009*, pp. 1005-1011.
[19] Md. Anisur Rahman, Mitu Kumar Debnath. An energy-efficient data security system for wireless sensor network. *Proceedings of 11th International Conference on Computer and Information Technology, December 2008*, pp. 381-386.
[20] Ali Fanian, Mehdi Berenjkoub, Hossein Saidi, T. Aaron Gulliver. A high performance and intrinsically secure key establishment protocol for wireless sensor networks. *Computer Networks*, 2011, pp. 1849-1863.
[21] Wenyuan Xu, Ke Ma, Yanyong Zhang. Jamming sensor networks: attack and defense strategies. *IEEE Network*, pp. 41-47, June 2006.
[22] David Martins, Herv é Guyennet. Wireless sensor network attacks and security mechanisms: A short survey. *13th International Conference on Network-Based Information Systems*, 2010, pp. 313-320.
[23] Teodor-Grigore lupu. Main types of attacks in wireless sensor networks. *Recent Advances in Signals and Systems*, pp. 180-184.
[24] Karlof C, Wagner D. Secure routing in wireless sensor networks: attacks and countermeasures. *Ad Hoc Networks* 2003, 1(2-3):293–315.
[25] Vidya Bharrgavi Balasubramanyn, Geethapriya Thamilarasu, Ramalingam Sridhar. Security solution for data integrity in wireless bioSensor networks. *27th International Conference on Distributed Computing Systems Workshops*, 2007.
[26] Sriram Cherukuri, Krishna K Venkatasubramanian, Sandeep KS Gupta. BioSec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. *Proceedings of the 2003 International Conference on Parallel Processing Workshops, 2003*.
[27] Jacob Andersen, Jakob E. Bardram. BLIG: A new approach for sensor identification, grouping, and authorisation in body sensor networks.
[28] Chiu C. Tan, Haodong Wang. Body sensor network security: an identity-based cryptography approach. *WiSec'08*, March 31–April 2, 2008.
[29] Samira Mesmoudi, Mohammed Feham. BSK-WBSN: biometric symmetric keys to secure wireless body sensor networks. *International Journal of Network Security & Its Applications (IJNSA)*, Sep 2011, pp. 155-166.
[30] http://www. tech-faq. com/network-attacks. html.
[31] Kai Xing, Shyaam Sundhar Rajamadam Srinivasan, Manny Rivera, Jiang Li, Xiuzhen Cheng. Attacks and countermeasures in sensor networks: a survey. *Network Security, Scott Huang, David MacCallum, Ding Zhu Du* (Eds.), Springer, 2005.
[32] http://Data%20integrity%20-%20Wikipedia, %20the%20free%20encyclopedia. mht.
[33] Carmen C. Y. Poon, Yuan-Ting Zhang, Shu-Di Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and M-Health. *IEEE Communication Magazine*, vol. 44, no. 4, pp. 73-81, 2006.
[34] Krishna Kumar Venkatasubramanian, Ayan Banerjee, Sandeep K. S. Gupta. EKG-based key agreement in body sensor networks. *IEEE*, 2008.
[35] Vaibhaw Dixit， Harsh K. Verma， Akhil K. Singh. Comparison of various security protocols in RFID. *International journal of computer applications* (0795-8887), pp. 17-21, Volume 24, No. 7, June 2011.
[36] Harmandeep Singh, Garima Malik. Approaches to wireless sensor network: security protocols. *World of Computer Science and Information Technology Journal (WCSIT)*, pp. 302-306 Vol. 1, No. 7, 2011.
[37] L. Sang Hyuk, L. Soobin, S. Heecheol et al. . Wireless sensor network design for tactical military applications: Remote large-scale environments. *Military Communications Conference, 2009 (MILCOM 2009). IEEE*, pp. 1-7.
[38] Zhu Wang, Lingfeng Wang, Anastasios I. Dounis, Rui Yang. Multi-agent control system with information fusion based comfort model for smart buildings. *Applied Energy99*, pp. 247-254, 2012.
[39] S. Hussain, S. Schaffner, D. Moseychuck. Applications of wireless sensor networks and RFID in a Smart home environment. *Communication Networks and Services Research Conference, 2009, CNSR '09. Seventh Annual*, 2009, pp. 153-157.
[40] V. Nainwal, P. J. Pramod, S. V. Srikanth. Design and implementation of a remote surveillance and monitoring system using wireless sensor networks. *Electronics Computer Technology (ICECT), 2011 3rd International Conference on*, pp. 186-189.
[41] Fabrice Le Fessant, Antonis Papadimitriou, Aline Carneiro Viana, Cigdem Sengul, Esther Palomar. A sinkhole resilient protocol for wireless sensor networks: Performance and security analysis. *Computer Communications35*, pp. 234-248, 2012.
[42] Md. Abdul Hamid, A. M. Jehad Sarkar. A group-based security scheme for wireless sensor networks. *Ann. Telecommun, Springer*, pp. 455–469, 2012.
[43] Tsung-Chih Hsiao, Yu-Ting Liao, Jen-Yan Huang, Tzer-Shyong Chen, Gwo-Boa Horng. An authentication scheme to healthcare security under wireless sensor

networks. *Springer Science+Business Media,* pp. 3649-3664, 2012.
[44] Javier Lopez, Jianying Zhou. Wireless sensor network security. *IOS Press*, 2008.
[45] C. Gnana Kousalya, G. S. Anandha Mala. Secure and energy-efficient traffic-aware key management scheme for wireless sensor network. *Int J Wireless Inf Networks*, pp. 112–121, 2012.
[46] Omar Cheikhrouhou, Anis Koubaˆa, Gianluca Dini, Mohamed Abid. RiSeG: a ring based secure group communication protocol for resource-constrained wireless sensor networks. *Pers Ubiquit Comput*, pp. 783–797, 2011.
[47] Attila Altay Yavuz, Peng Ning. Self-sustaining, efficient and forward-secure cryptographic constructions for unattended wireless sensor networks. *Ad Hoc Networks 10*, pp. 1204-1220, 2012.
[48] Francesca Cuomo, Emanuele Cipollone, Anna Abbagnale. Performance analysis of IEEE 802. 15. 4 wireless sensor networks: *An insight into the topology formation process. Computer Networks 53*, pp. 3057–3075, 2009.
[49] Lamia CHAARI, Lotfi KAMOUN. Performance analysis of IEEE802. 15. 4/Zigbee standard under real time constraints. *International Journal of Computer Networks & Communications (IJCNC)* Vol. 3, No. 5, pp235-251, Sep 2011.
[50] Abidalrahman Moh'd, Hosein Marzi, Nauman Aslam, William Phillips, William Robertson. A secure platform of wireless sensor networks. *The 2nd International Conference on Ambient Systems, Networks and Technologies. Procedia Computer Science* 5, pp. 115-122, 2011.
[51] Yanli Yu, Keqiu Li, Wanlei Zhou, Ping Li. Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures. *Journal of Network and Computer Applications 35*, pp. 867-880, 2012.
[52] Yusnani Mohd Yussoff, Habibah Hashim, Roszainiza Rosli, Mohd Dani Baba. A review of physical attacks and trusted platforms in wireless sensor networks. *Procedia Engineering 41*, pp. 580-587, 2012.
[53] WenTao Zhu, Jianying Zhou, Robert H. Deng, FengBao. Detecting node replication attacks in wireless sensor networks: A survey. *Journal of Network and Computer Application 35*, pp1022-1034, 2012.
[54] Victor Obado, Karim Djouani, Yskandary Hamam. Hidden markov model for shortest paths testing to detect a Wormhole Attack in a localized wireless sensor network. *Procedia Computer Science 10*, pp. 1010-1017, 2012.
[55] Z. A. Baig. Pattern recognition for detecting distributed node exhaustion attacks in wireless sensor networks. *Computer Communications 34*, pp. 468-484, 2011.
[56] Yanxiang Lou, Yong Zhang, Shengli Liu. Single hop detection of node clone attacks in mobile wireless sensor networks. *Procedia Engineering 29*, pp. 2798-2803, 2012.
[57] Jun-Won Ho, Matthew Wright, Sajal K. Das. Distributed detection of mobile malicious node attacks in wireless sensor networks. *Ad Hoc Networks 10*, pp. 512–523, 2012.
[58] Zhang Yi-ying, Li Xiang-zhen, Liu Yuan-an. The detection and defence of DoS attack for wireless sensor network. *The journal of china universities of posts and telecommunications, October 2012*, 19(Suppl. 2): pp. 52-56.
[59] Ju-Hyung Son, Haiyun Luo, Seung-Woo Seo. Denial of service attack-resistant flooding authentication in wireless sensor networks. *Computer Communications 33*, pp. 1531-1542, 2010.
[60] Asmae Blilat, Anas Bouayad, Nour el houda Chaoui, Mohammed el Ghazi. *Wireless sensor network: Security challenges.*
[61] Kai Lin, Xiaohu Ge, Xiaofei Wang, Chunsheng Zhu, Heung-Gyoon Ryu. Research on secure data collection in wireless multimedia sensor networks. *Computer Communications 35*, pp. 1902-1909, 2012.
[62] Rohan Nanda, P Venkata Krishna. Mitigating denial of service attacks in hierarchical wireless sensor networks. Feature, *Network security*, October 2011.
[63] Abderrahmen Guermazi, Mohamed Abid. An efficient key distribution scheme to secure data-centric routing protocols in hierarchical wireless sensor networks. *Procedia Computer Science 5*, pp. 208-215, 2011.
[64] Shaila K, S H Manjula, Aruna R, Anupama, K R Venugopal, L M Patnaik. Resilience key predistribution scheme using asymmetric matrices for wireless sensor networks. *2009 IEEE International Advance Computing Conference (IACC 2009), Patiala, India, March 2009.*
[65] Dhara Buch, Devesh Jinwala. Prevention of wormhole attack in wireless sensor network. *International Journal of Network Security & Its Applications (IJNSA)*, Vol. 3, No. 5, Sep 2011.
[66] P. Kyasanur, N. H. Vaidya. Detection and handling of mac layer misbehavior in wireless networks. *DSN*, 2003, pp. 173–182.
[67] Virendra Pal Singh, Sweta Jain, Jyoti Singhai. Hello flood attack and its countermeasures in wireless sensor networks. *IJCSI International Journal of Computer Science Issues*, Vol. 7, Issue 3, No 11, May 2010.
[68] Fabrice Le Fessant, Antonis Papadimitriou, Aline Carneiro Viana, Cigdem Sengul, Esther Palomar. A sinkhole resilient protocol for wireless sensor networks: *Performance and security analysis. Computer communications 35*, pp. 234-248, 2012.
[69] Ritesh Maheshwari, Jie Gao, Samir R Das. Detecting wormhole attacks in wireless networks using connectivity information.
[70] Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh. Overview of security issues in wireless sensor networks. *2011 Third International Conference on Computational Intelligence, Modelling & Simulation*, pp. 308-311.
[71] S. S. Mohanavalli, Sheila Anand. Security architecture for at-home medical care using body sensor network. *International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC)* Vol. 2, No. 1, March 2011.
[72] Moshaddique Al Ameen, Jingwei Liu, Kyungsup Kwak. Security and privacy issues in wireless sensor networks for healthcare applications. *J Med Syst*, 12 March 2010.
[73] Tian Bin, Li Qi, Yang Yixian, Li Dong, Xin Yang. A ranging based scheme for detecting the wormhole attack in wireless sensor networks. *The Journal of China Universities of Posts and Telecommunications*, June 2012, 19 (Suppl. 1), pp. 6-10.
[74] Y. Challal , A. Ouadjaout, N. Lasla, M. Bagaa, A. Hadjidj. Secure and efficient disjoint multipath construction for fault tolerant routing in wireless sensor networks. *Journal of Network and Computer Applications 34 (2011)* pp. 1380-1397.
[75] Guoxing Zhan, Weisong Shi, Julia Deng. TARF: A trust-aware routing framework for wireless sensor networks. *EWSN 2010, LNCS 5970*, pp. 65-80, 2010.
[76] Abderrahmen Guermazi, Mohamed Abid. An efficient key distribution scheme to secure data-centric routing protocols in hierarchical wireless sensor networks. *Procedia Computer Science 5* (2011), pp. 208-215.

[77] E. Ayday, F. Fekri. A secure broadcasting scheme to provide availability, reliability and authentication for wireless sensor networks. *Ad Hoc Networks 10*, pp. 1278-1290, 2012.
[78] Omar Cheikhrouhou, Anis Koubaa, Gianluca Dini, Hani Alzaid, Mohamed Abid. LNT: A logical neighbor tree secure group communication scheme for wireless sensor networks. *Ad Hoc Networks 10*, pp. 1419-1444, 2012.
[79] Qi Mi, John A. Stankovic, Radu Stoleru. Practical and secure localization and key distribution for wireless sensor networks. *Ad Hoc Networks 10*, pp. 946-961, 2012.

Fangmin Sun received a B.S. degree in the measurement and control technology and instrument from Xian Electronic Technology University, China, in 2010. She is currently a Ph.D. student in the State Key Laboratory of Transducer Technology Institute of Electronics, Chinese Academy of Sciences. Her current research focuses on nodes design for wireless sensor networks, especially for wireless body sensor networks that used for health monitoring applications.

Zhan Zhao received his B.S. in Physics in 1982 from Shanxi University and his master's and doctoral degrees in Physical Electronics and Devices in 1987 and 2003, respectively. Both the degrees were awarded by the Institute of Electronics, Chinese Academy of Sciences (IECAS). Since 1994, he has been with the State Key Laboratory of Transducer Technology (SKLTT) at IECAS. He was a Visiting Scholar in Rutherford Appleton Laboratory, UK, in 2001. Since 2000, he has been a professor for integrated sensor and microsystem at the SKLTT.

Zhen Fang received his PhD at the Institute of Electronics, Chinese Academy of Sciences. He currently works in the State Key Laboratory of Transducer Technology at the Institute of Electronics, Chinese Academy of Sciences. His major field is wireless sensor networks and microsystems of integrate sensors.