Chapter 7
Security and Privacy Issues in Wireless Sensor and Body Area Networks

Moumita Roy, Chandreyee Chowdhury, and Nauman Aslam

Abstract Advancements in wireless communication and availability of miniaturized, battery powered micro electronics devices have revolutionized the trend of computation and communication activities to the generation of smart computing where spatially distributed autonomous devices with sensors forming wireless sensor network (WSN) are utilized to measure physical or environmental conditions. WSNs have emerged as one of the most interesting areas of research due to its diverse application areas such as healthcare, utilities, remote monitoring, smart cities, and smart home which not only perform effective monitoring but also improve quality of living. Even the sensor nodes can be strategically placed in, on, or around human body to measure vital physiological parameters as well. Such sensor network which is formed over human body is termed as wireless body area network (WBAN) which could be beneficial for numerous applications such as eldercare, detection of chronic diseases, sports, and military. Hence, both network applications deal with sensitive data which requires utmost security and privacy. Thus, the security and privacy issues and challenges related to WSN and WBAN along with the defense measures in place should be studied in detail which not only is beneficial for effective application but also will motivate the researcher to find their own path for exercising better protection/defense. Accordingly, in this chapter a brief overview of both networks is presented along with their inherent characteristics, and the need for security and privacy in either networks is illustrated as well. Besides, study has been made regarding potential threats to security and privacy in both networks and existing measures to handle these issues. Finally the open research challenges are identified to draw the attention of the researcher to investigate further in this field.

Keywords WSN · WBAN · Security · Privacy

M. Roy · C. Chowdhury (✉)
Jadavpur University, Kolkata, India

N. Aslam
Northumbria University, Newcastle upon Tyne, UK
e-mail: nauman.aslam@northumbria.ac.uk

B. B. Gupta et al. (eds.), *Handbook of Computer Networks and Cyber Security*,
https://doi.org/10.1007/978-3-030-22277-2_7

1 Introduction

Developments and technological advancements in wireless communication have initiated the era of smart computing. Rather than super-computing devices, lightweight battery driven consumer electronic devices with sensing and communication capabilities have become affordable today. These devices can be deployed to monitor and control a wide range of phenomena including remote events to daily life activities. These devices are commonly known as sensors that can be deployed spatially over the region where the activities need to be monitored. For example, if the temperature of a power plant needs to be monitored, sensors are to be strategically placed at various locations of the power plant. These distributed autonomous sensors form a wireless sensor network (WSN) [11, 41] where the nodes cooperate among themselves to report their sensed readings to a remote station. Thus, if any sensor node reports a high/low temperature value, users sitting at a remote place may get an alert and may take measures accordingly. In this way, the sensor nodes are utilized to measure physical or environmental conditions such as monitoring forest fire, wild habitats, earthquakes, or even health of bridges.

On the other hand, the advent of small bio-sensors that can either be worn as watches or bracelets or be implanted such as a pacemaker, the concept of wireless body area network (WBAN) [35, 43] is seeded. Such networks can measure body vitals at regular intervals while maintaining the convenience of the user. The users may carry out their daily activities and enjoy the comfort of staying at their homes while these sensors collect their body vitals and report to a medical center. Hence, WBAN can be viewed as a variant of WSN where the network is deployed in/on or around human body. Though sensing and communication are the two key elements for both these networks and hence they share many similarities, there are some significant differences too. Most importantly, in most of these cases, such networks lose their significance if security and privacy issues are not diligently handled. Consequently, this chapter first provides an overview of both WSN and WBAN followed by a brief discussion on the privacy and security issues in Sect. 3 through 5. Existing solutions to these issues and associated deployment hurdles are also presented in the subsequent section (Sect. 6). Potential applications of WSN and WBAN and their security and privacy requirements are also discussed in Sect. 7. This is followed by a discussion of the pertinent research issues. Finally, the chapter concludes in Sect. 9.

2 Overview of Wireless Sensor and Body Area Networks

WSNs have emerged as one of the most interesting areas of research due to its diverse application domains such as healthcare, utilities, remote monitoring, smart cities, and smart home which not only perform effective monitoring but also improve quality of living [35]. WSN is a collection of small sensor nodes

that are deployed over a region where a physical phenomenon is to be detected, monitored, or tracked. The sensors could be deployed over a controlled environment where monitoring or surveillance is critical or in an uncontrolled environment where security for sensor networks is utmost important [61]. Each sensor node consists of four subsystems, namely power supply, sensing, processing, and communication subsystem [6, 35]. Additionally, a sensor node may also have actuators, positioning modules, etc. The sensor nodes are often referred to as "motes" where low power and high frequency transceivers are implemented on chips and digital circuits tend to shrink and be fabricated densely [6]. The nodes sense data and send it to a base station (also called sink) via other nodes.

Vast literature could be found on WSN routing [36, 52], that is, how a sensor node finds suitable path to send a packet to sink. Works can also be found on clustering nodes in WSN [4, 31], energy harvesting [48, 58], and MAC layer communication issues [18, 51]. Few WSN deployments are also reported recently [20, 56].

Now-a-days, smartphones present an interesting combination of sensing, computation, and communication facilities. Additionally, its wide availability and usage make it a viable device for novel application development. These phones can connect through Bluetooth to the bio-sensor nodes to collect body vitals from them and may send the information to a remote server through the Internet. Even the accelerometer sensor of smartphone can itself act as a wearable body sensor to collect data about user's postures to detect activities including fall. Thus, WSN is no longer a way of monitoring remote applications only. The miniaturized, ultra-low power bio-sensor nodes, and wide availability of smartphones paved the way for wireless body area networks (WBAN), a variant of WSN that is increasingly getting importance for smart healthcare. WBAN has immense potential to be used in not only medical internet of things (IoT) applications but also for sports, entertainment, and smart home. Even with availability of the bio-sensor nodes, a patient need not visit a medical facility for checkup when symptoms appear, but can opt for proactive medical supervision. WBAN enables a person to be under constant medical supervision at free-living conditions even residing at home [9]. This is a convenient and important option for effective treatment of chronic diseases and eldercare today.

2.1 Network Architecture

WBAN has evolved as an application area of WSN over human body and thus the basic architecture of both networks is quite similar as well. The sensor networks communication architecture [49] is shown in Fig. 7.1. The sensor nodes are generally scattered over the region where some phenomena are to be reported. Each of these scattered sensor nodes has the capabilities to collect data and route the data to the sink as well as the end users. Data can be routed to the end user by a multi-hop infrastructureless architecture through the sink via Internet or satellite as shown in Fig. 7.1.

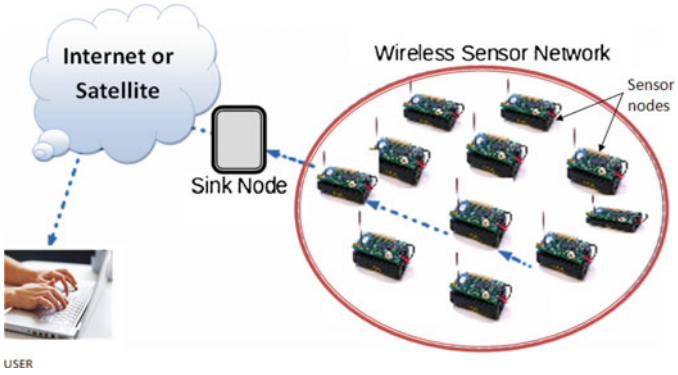

Fig. 7.1 Architecture of WSN

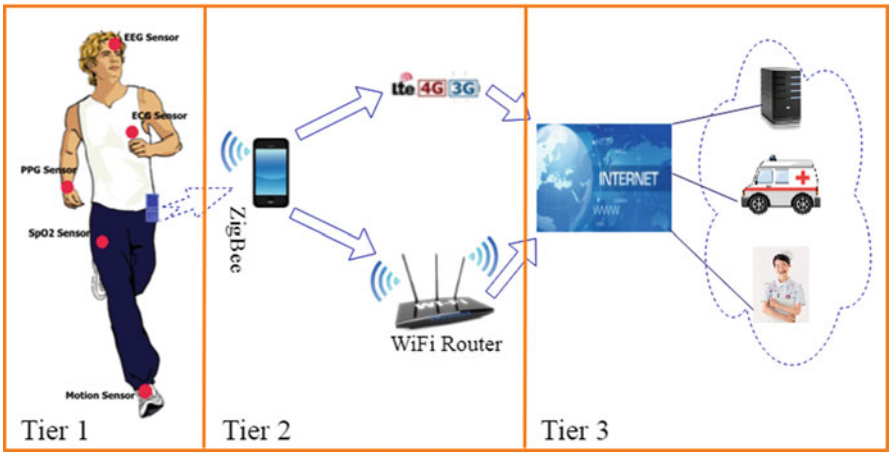

Fig. 7.2 Three tier architecture of WBAN

Similarly, the health monitoring system which can be regarded as an application of WSN is based on three tier architecture [42] as shown in Fig. 7.2. Tier 1 focuses on network formation among bio-sensor nodes together with a network coordinator or the sink (which could be a smart handheld such as smartphone) where the sensor nodes collect health parameters and communicate to the sink; tier 2 includes wireless technologies such as WLAN or GPRS so that the sink of tier 1 could communicate the health data to the remote medical server located at tier 3 to be analyzed by medical professionals.

Both networks comprise of battery-powered devices thus subject to bounded lifetime. Lifetime could be measured in days, months, or even years. For instance, in case of implanted nodes in WBAN such as pacemakers require at least 5 years of lifetime [43]. Besides, the storage capacity of each node in both networks is limited and the nodes having low computational capabilities [3]. Hence, complex

computational approach to address different issues in both networks such as routing [34, 43], reliability analysis [11], and security [39, 44] is usually avoided. However, there are few dissimilarities between these resource constraint networks (i.e., WSN and WBAN) as well. The comparative study [3] between WSN and WBAN is listed in Table 7.1. The sensors exploited in WSN are generally multi-function devices which are designed to be applied in large range network. Besides, the nodes in WSN are subject to movements that result from environmental influences (such as wind or water) or the sensors may be attracted to or carried by mobile entities, or this may be a desired property of the system [41]. The cost sensitive network formation ensures reliability using redundant devices to collect data at the desired location. For example, sensor networks exploited in military application are based on the dense deployment of disposable and low-cost sensor nodes such that destruction of some nodes by hostile actions does not affect the overall throughput [2]. The nodes are deployed following random distribution and point to point communication between nodes take place in WSN. Unlike WSN, the nodes in WBAN are usually single function devices designed to be applied in small range of network (i.e., in, on, or around human body). The nodes in WBAN are placed over human body at specified locations and thus the relative node movements subject to posture change. In addition, the electro-magnetic radiation results due to communication between bio-sensor devices are absorbed by human tissue which is measured in terms of specific absorption rate (SAR) [35]. Several health hazards [35] may take place if regulatory limit of SAR [9] is violated. However, both networks deal with sensitive information depending on their use particularly when it is directly related to human subjects (i.e., in case of WBAN). Hence, both networks require security component to prevent misuse of the technology, although the security aspects could be distinct according to the applicability.

2.2 Performance Metric

System performance of both WSN and WBAN can be measured from different aspects as shown in Fig. 7.3. Applications of both networks have environmental, economic, and social impact on the measurable output [26]. When the focus is on to build a network of resource constraint nodes in order to monitor the environment, the expected outcome is evaluated in terms of energy efficiency and network lifetime such that the resource utilization gets maximized. However, when the feasibility of the system is analyzed in related to economic perspective, the performance of the system is assessed with respect to cost saving operation and maintenance such as overhead cost, reliability, and mean time to failure (MTTF). While considering the social aspect of the applications of WSN as well as WBAN, the goal of these technologies is to improve quality of living. Thus, acceptability of such systems is related to user satisfaction and cost-benefit analysis. However, the performance of each individual perspective when combined with other gives the system a new dimension. For instance, the social impact of the system together with economic

Table 7.1 Comparison between WSN and WBAN

Features	WSN	WBAN
Similarities		
Limited resources	Subject to limited energy (in terms of limited battery power) and storage capacity and low computational capabilities	Subject to limited energy (in terms of limited battery power) and storage capacity and low computational capabilities
Differences		
Sensor/actuator	Multifunction device	Single function device
	Rare or slow movement	Fast relative movement
	Designed to be applied in large range network	Designed to be applied in small range network
	Lifetime is measured in months generally less than 10 years	Lifetime is measured in days; however, in case of implanted sensor it could be less than 10 years
	Cost sensitive	Safety is must (i.e., low SAR) and quality is important
Dependability	Redundancy-based reliability	Reliability is prime requirement
	Expected QoS	Guaranteed QoS
	Security is important	Security is must
Network	Large-scale hierarchical network	Small-scale network usually follows star topology although multi-hop topology is sometimes preferred to restrict energy consumption
	Redundancy in device	Redundancy in device is avoided
	Usually random node distribution	Usually nodes are placed at specified locations in, on, or around human body
Traffic	Burst (dominant) or periodical	Periodical (dominant) or burst
	Uni-directional or bi-directional traffic	Uni-directional traffic from sensor to sink
	M:1 or point to point communication	Generally M:1 communication
Channel	ISM band is utilized	Specific medical channel, ISM band
	Obstacle is unknown	Obstacle is mainly body surface or through body

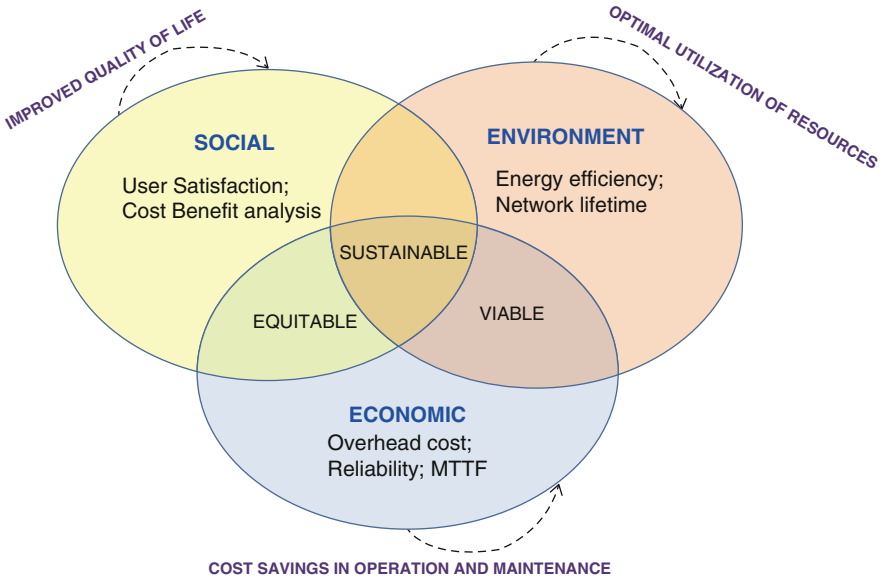

Fig. 7.3 The notion of measuring system performance for both WSN and WBAN

outcome makes the system equitable whereas performance measured in economic and environment point of view makes the system viable. Nevertheless, when all three notions of measuring system performance are integrated sustainable system is obtained.

3 Security Threats in WSN and WBAN

Security is prime concern to any system for effective functioning particularly when it involves wireless technologies. Security is a concept similar to the safety of the system as a whole [3, 32, 45]. Both WSN and WBAN are prone to inherent security challenges that are associated with wireless communications. The basic security requirements [8, 28, 53, 59] related to both networks (illustrated in Fig. 7.4) are as follows.

- **Availability:** This ensures the desired network services are available at right time even in the presence of denial of service attack [59].
- **Data authentication:** This ensures the communication from one node to another is genuine and an adversary cannot masquerade as trusted node.
- **Data confidentiality:** This ensures the given message should only get understood by the intended recipient.

Fig. 7.4 Security requirements in WSN and WBAN

- **Data integrity:** This ensures the message sent by the sender must not get modified on the way before reaching at the receiver.
- **Data freshness:** This ensures that the data is recent and an adversary cannot replay an old message.
- **Secure localization:** Sensor network applications often exploit geographical information of nodes. This security requirement ensures the location information of nodes should not get revealed to the attacker.
- **Flexibility:** This ensures that the network will be used in different scenarios where environmental circumstances, hazards, and mission may change frequently.
- **Robustness:** This ensures that the network should be robust across various security attacks. However, if any attack takes place, its impact should be less.
- **Time synchronization:** Most sensor network applications rely on some form of time synchronization. For instance, a sensor node's radio may often be turned off for some duration to preserve energy resource.

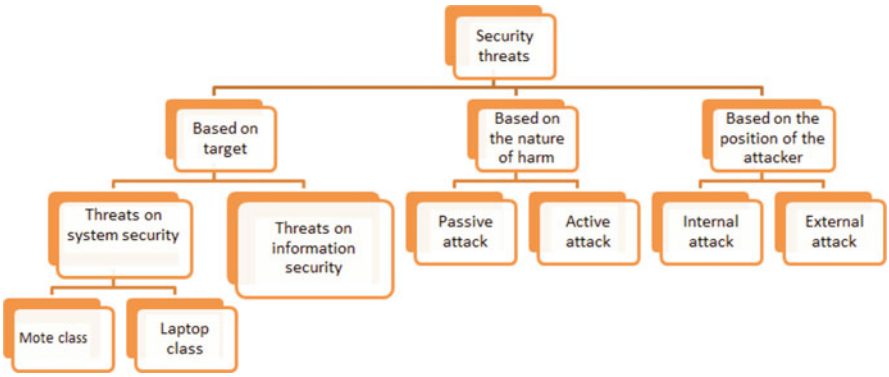

Fig. 7.5 Categorization of security threats in WSN and WBAN

– **Self organization:** WSNs are also ad-hoc networks having flexibility and extensible properties. In WSN, every sensor node is independent and flexible enough to be self-organizing and self-healing according to the situations.

The broadcast nature of wireless communication together with unguided transmission medium brings with it a host of security threats in both networks. The potential threats in both networks are categorized in different ways as shown in Fig. 7.5. First categorization is made based on the target where the adversary attempts to do harm and accordingly imposes threats on system security or information security [3]. Denial of service, impersonations are examples of attacks on system security whereas data modification, eavesdropping, and replaying are examples of attacks on information security. Denial of service (DoS) [28, 47] is a type of attack where the attacker attempts to prevent the legitimate nodes in the network to get service. When an adversary eavesdrops identity information of a trusted node and uses this information to cheat other nodes in the network, the attack is called impersonation [3, 28]. In data modification attack [3, 28] the attacker can delete or replace part or all of eavesdropped information and the modified information is sent back to original receiver to accomplish some illegal purpose. However, in eavesdropping [3] any opponent can intercept radio communications between the wireless nodes freely and easily (due to open nature of wireless medium) to steal data for malicious acts. The attacker can even resend a piece of valid information (obtained through eavesdropping) to original receiver after a while to achieve same purpose in different case. This form of attack is termed as replay attack [3, 28]. However, the threats on system security could be further classified as mote class attack and laptop class attack [59]. In mote class attack [59] an adversary launches attack on WSN exploiting few nodes with similar capabilities to the network nodes whereas in laptop class attack [59] makes use of more powerful devices such as laptop to attack a WSN. Nevertheless, system threats could be further classified based on the intensity of the harm, i.e., passive attack and active attack [3, 59]. Active attacks are more harmful as compared to passive counter

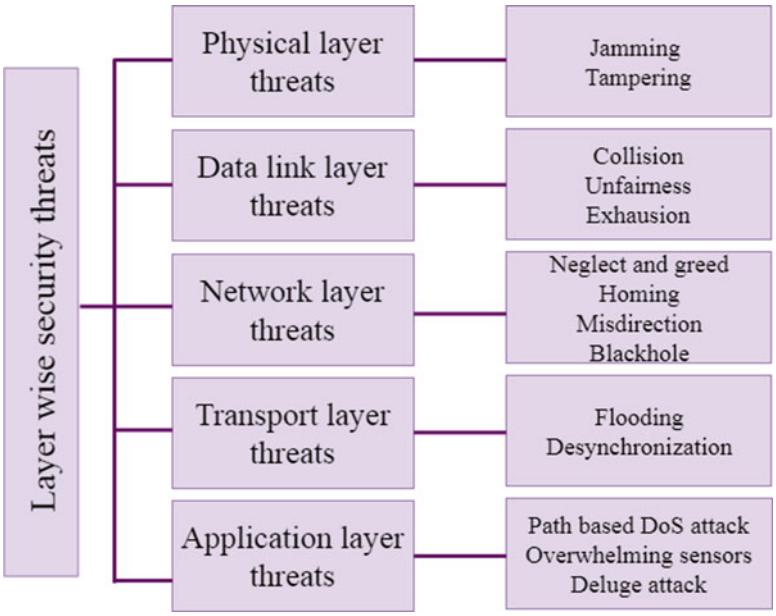

Fig. 7.6 Layer-wise security threats in WBAN

parts. For instance, eavesdropping or monitoring packet exchanges in WSN by a malicious node are examples of passive attack whereas active attacks involve some modifications of data as well as injection of false data. Besides, the system threats could be categorized based on the position of the adversary, i.e., internal attack and external attack [59]. External attack belongs to a node which is not part of the WSN but internal attack takes place when a legitimate node exhibits unintended or unauthorized behavior. Few attacks are occurred at different layers as well thus require to be handled differently at each layer. For instance, DoS attacks in WSN could take place in physical layer in the form of jamming or tampering, at link layer in terms of collision, exhaustion, or unfairness, at network layer it could be neglect and greed, homing, misdirection, black holes and in transport layer this attack could be performed by malicious flooding and desynchronization [37]. Layer-wise security attacks are listed in Fig. 7.6.

Physical Layer Physical layer of WSN as well as WBAN is responsible for frequency selection, carrier frequency generation, signal detection, modulation, and data encryption [59]. Here, vulnerabilities could occur in the following form.

– **Jamming [59]:** This type of attack interferes the radio frequencies used by the nodes in the network. A jamming source could disrupt the entire network or smaller portion of the network.

– **Tampering [59]:** In this type of attack, an attacker can extract sensitive information such as cryptographic keys or other data from the victim node if it get access to that node.

Data Link Layer Data link layer of WSN as well as WBAN is responsible for multiplexing of data streams, data frame detection, medium access, and error control [59]. Here, vulnerabilities could occur in the following form. This layer ensures reliable point to point or point to multi-point connections. Here, potential security threats take place in the following manner.

– **Collision [59]:** Collision occurs when two or more nodes attempt to transmit on the same frequency at the same time.
– **Unfairness [59]:** Unfairness can be regarded as a weak form of DoS attack where the adversary creates unfairness in the network by exploiting collision and exhaustion attacks.
– **Exhaustion [59]:** Repeated collision could be exploited by the attacker to create resource exhaustion.

Network Layer Network layer of WSN as well as WBAN is responsible for routing data from source to destination [8, 59]. Here, vulnerabilities could occur in the following form.

– **Neglect and greed [53]:** This attack occurs when a packet travels in between nodes from sender to destination. The malicious node can force multi-hopping in the network either by splashing some packets or by misdirecting towards wrong a node. Hence, this attack disturbs the network activities of the adjoining nodes.
– **Homing [8]:** In this type of attack search is carried out in the ongoing data traffic to identify the cluster head or key manager that have the capability to terminate the entire network.
– **Misdirection [8]:** In this attack, the attacker misdirects data traffic.
– **Hello flood attack [8]:** In this type of attack, a single malicious node sends a useless message which is then replayed by the attacker to generate high traffic thus the channel gets congested.
– **Selective forwarding [8]:** In this type of attack a compromised node only sends data to the selected few nodes instead of all the nodes. This selected recipients list is made according to the interests of the attacker to achieve his malicious objective.
– **Sybil attack [8]:** Here, the attacker replicates a single node and represents it with multiple identities to the other nodes in the network.
– **Wormhole attack [8]:** This attack causes relocation of data packets through tunneling over a link of low latency.
– **Black hole [53]:** This attack is also referred to as sink holes that launches the attack through building a covenant node seems to be very attractive (i.e., it promotes zero-cost routes to neighboring nodes with respect to the routing algorithm). Accordingly, this causes maximum traffic to flow towards these fake nodes. Thus, nodes adjoining to these malicious nodes collide for immense bandwidth leading to resource contention and message destruction.

– **Acknowledgement flooding [8]:** In this attack, a malicious node spoofs the acknowledgements to provide false information to the destined neighboring nodes.

Transport Layer Transport layer of WSN as well as WBAN is responsible for managing end to end connections [59]. Here, the vulnerabilities could be as follows.

– **Flooding [59]:** In this type of attack, an attacker repeatedly makes new connection requests until the resources required by each connection are exhausted or reach a maximum limit and thus in either case further legitimate requests get ignored.
– **Desynchronization [59]:** Desynchronization causes disruption of an existing connection where an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data. Consequently, the energy is wasted instead by attempting in order to recover from errors which never really existed.

Application Layer Application layer of WSN as well as WBAN carries out the responsibility of traffic management. Besides, this layer also acts as the provider of software for different applications that translates data into a comprehensible form or helps in collection of information by sending queries [8]. Here the following vulnerabilities could take place.

– **Path-based DoS attack [8]:** In this type of attack an attacker creates a huge traffic in the route towards base station.
– **Overwhelming sensors [53]:** In this attack an attacker attempts to overwhelm network nodes with sensor stimuli that causes the network to forward large volumes of traffic to a base station. Hence, network bandwidth is consumed in this attack and node energy is drained. However, it is effective only when particular sensor readings (for example, motion detection or heat signatures) trigger communications instead when sensor readings are sent at fixed intervals.
– **Deluge (reprogramming) attack [53]:** Protocols such as TinyOS's Deluge network-programming system enable remotely reprogram nodes in deployed networks. Most of these systems, including Deluge, are designed to be used in a trustworthy environment. If the reprogramming process isn't secure, an intruder can hijack this process and take control of large portions of a network.

4 Similarities and Differences Between WSN and WBAN with Respect to Security Issues

WSN and WBAN applications deal with sensitive data and thus security is prime requirement in both networks to protect the system from getting misused by the adversary having malicious intention. The network activities take place through wireless medium in both cases. Hence, both WSNs and WBANs are prone to

security threats related to shared broadcast medium [3]. In addition, the lightweight security measures having low computation and communication overhead are desirable to enhance security in the resource constraint networks like WSN and WBAN. However, there are some key differences between these two networks as illustrated earlier (in Sect. 2) and therefore the security techniques designed for WSN may not be applied to build up security in WBAN applications. Since WSN is a large network deployed over large region as compared to WBAN, the sensor nodes in WSN may easily got tampered by the adversary. In addition, clustering could be an overhead for WBAN and thus unlike WSN cluster-based security solutions cannot be applied to WBAN. Moreover, security solutions designed for WBAN must not violate the regulatory limit of SAR. Most importantly, WBAN involves human subjects thus security is utmost important otherwise it could be misused by a person with detrimental objectives and even it could be life threatening as well.

5 Privacy Issues of WSN and WBAN

Privacy is a key issue to be handled in any system that deals with sensitive information. Privacy is concerned about who can access the information [3]. Privacy issues may arise due to many reasons such as personal belief, social and cultural environment, and other general public/private causes citeal2012security. Both WSN and WBAN deal with sensitive information related to physical phenomena or human health, hence privacy is a prime aspect that regulates the acceptability of such system by the people. Health related data are always private in nature and hence sending data out from a patient through wireless media in case of WBAN applications imposes serious threats to privacy of an individual [3]. Even it could be life threatening for an individual if this information is misused by people with harmful intentions. Some of the major aspects to be addressed before deployment of WBAN applications in order to guarantee privacy are where the health data should be stored, who can view the patient's medical record, who will be responsible for maintaining these data in case any emergency arises, and so on. Most importantly, it is to be taken into account that whether the data are obtained with the consent of the person or without it due to the requirement by the system so that the misuse of this private information could be prevented.

The privacy measures [3] must include the following before widespread deployment of the WBAN applications.

- All communications over wireless networks and Internet are required to be encrypted so that these do not give any meaningful information other than the intended recipients.
- It is also essential that individual user should not be identified unless there is a need.
- Another important measure is to create awareness among general public regarding technology along with security and privacy issues and their implications in

order to make balanced judgments concerning the extent to which it may have a negative impact on their own standards of privacy.

6 Existing Security and Privacy Solutions for WSN and WBAN

There are many security mechanisms designed primarily to be applied in generic WSN. However, very few of them could be applied readily to WBAN as well with low power computation [25].

6.1 IEEE 802.11 Security Solutions

The IEEE 802.1X standard defines the standard for port-based network access control to provide compatible authentication and authorization mechanisms for devices interconnected by various 802 LANs [10]. The standard could also be used to distribute security keys for 802.11 wireless LANs (WLANs) [19] that enables public key authentication and encryption between access points (APs) and mobile nodes (MNs). WLAN [19] defines two types of authentication mechanisms which are open system authentication and shared system authentication. In 802.1X, the port denotes the association between MN and AP. The 802.1X authentication system consists of three main components which are supplicant, authenticator, and authentication server (AS) [10]. A supplicant is usually an MN which is requesting WLAN access whereas an authenticator represents the network access server (NAS). In 802.11 AP serves as NAS. A RADIUS server is commonly exploited as the authentication server, although other types of AAA servers such as diameter could also act as the authentication server. The authentication server might be physically integrated into an AP in case of IEEE 802.11 standard.

6.2 IEEE 802.15.6 Security Solutions

The IEEE 802.15.6 is the latest international standard for WBAN which aims to provide an international standard for low-power, short-range, and extremely reliable wireless communication for use in close proximity to, or inside, a human body (but not limited to humans) [57]. A vast range of data rates is supported in IEEE 802.15.6 standard for different applications. This standard targets to cover both medical and non-medical applications with different requirements. The security structure of the IEEE 802.15.6 standard includes several states, procedures, and protocols [57]. A security association in the IEEE 802.15.6 standard is defined as a procedure

to identify a node and a hub to each other, to establish a new master key (MK) shared between them, or to activate an existing MK pre-shared between them. Five protocols are included in the security association in the IEEE 802.15.6 standard which are a non-cryptographic protocol for activating a pre-shared MK, and four key exchange protocols for generating a new MK. The generated/activated MK is then utilized through another protocol for creating of a pairwise temporal key (PTK) which will work as the session key for data security. A protocol is also defined in the standard for the security disassociation procedure as well where after its successful execution, the participants will delete the MK and PTK. The standard includes both authenticated key exchange (AKE) and password-based AKE (PAKE) protocols. A strong cryptographic session key is established between legitimate participants in an authenticated manner using AKE whereas PAKE protocols allow an authenticated key establishment based on a pre-shared human-memorable password.

6.3 IEEE 802.15.4 Security Solutions

The IEEE 802.15.4 standard (for wearable body sensor nodes) has different security modes [25, 46] that can be built on WBANs. The IEEE 802.15.4 defines low-power standard which are designed for low data rate wireless personal area networks (WPANs). This standard specifies the physical and media access control layers, which focus on low-cost and low-speed ubiquitous communication between devices. IEEE 802.15.4 standard is very close to WBANs because it supports low data rate applications having low cost of power consumption. The standard is employed by many designers and researchers in order to develop protocols and mechanisms for WBANs. The IEEE 802.15.4 security suits are categorized into null, encryption only (AES-CTR), authentication only (AES-CBC-MAC), and encryption and authentication (AESCCM) suites. Different security modes and their descriptions are listed in Table 7.2.

6.3.1 AES-CTR

Confidentiality in AES-CTR [25] is protected using advance encryption standard (AES) block cipher with counter mode (CTR) which is also known as integer counter mode. Here, the plaintext (PT) is broken into 16-byte blocks $PT_1, PT_2, ..., PT_n$. The sender j computes the cipher text by $CT_j = PT_j XOR K_{en}(C_j)$, where CT_j denotes the encrypted text or cipher text, PT_j represents the data block, and $K_{en}(C_j)$ gives the encryption key of the counter C_j. The receiver decodes the cipher text using the formula $PT_j = CT_j XOR K_{en}(C_j)$. The encryption and decryption processes are illustrated in Fig. 7.7.

Table 7.2 Different security modes in IEEE 802.15.4 standard

Security modes	Description
Null	No security is provided in this mode
AES-CTR	This security mode provides advance encryption standard (AES) with counter mode (CTR)
AES-CBC-MAC-128	Authentication and message integrity protection are provided here using advance encryption standard (AES) with cipher block chaining (CBC) and 128 bit message authentication code (MAC)
AES-CBC-MAC-64	Authentication and message integrity protection are provided here using advance encryption standard (AES) with cipher block chaining (CBC) and 64 bit message authentication code (MAC)
AES-CBC-MAC-32	Authentication and message integrity protection are provided here using advance encryption standard (AES) with cipher block chaining (CBC) and 32 bit message authentication code (MAC)
AES-CCM-128	This security mode provides high level security by first applying integrity protection using cipher block chaining (CBC) with 128 bit message authentication code (MAC) and then encrypting data payload and MAC by employing AES-CTR mode
AES-CCM-64	This security mode provides high level security by first applying integrity protection using cipher block chaining (CBC) with 64 bit message authentication code (MAC) and then encrypting data payload and MAC by employing AES-CTR mode
AES-CCM-32	This security mode provides high level security by first applying integrity protection using cipher block chaining (CBC) with 32 bit message authentication code (MAC) and then encrypting data payload and MAC by employing AES-CTR mode

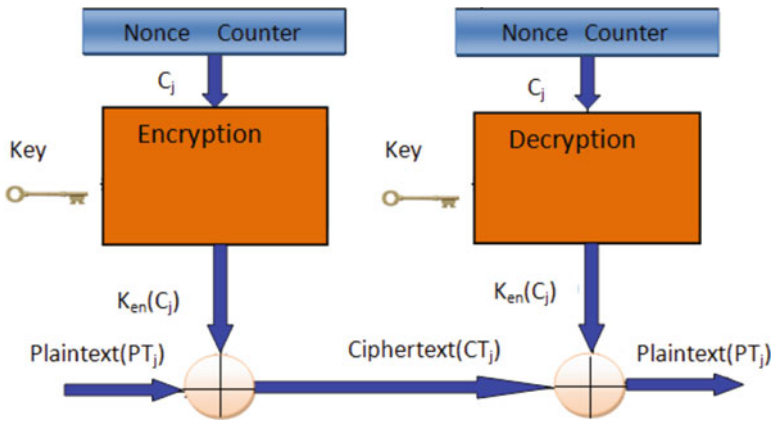

Fig. 7.7 CTR encryption and decryption processes

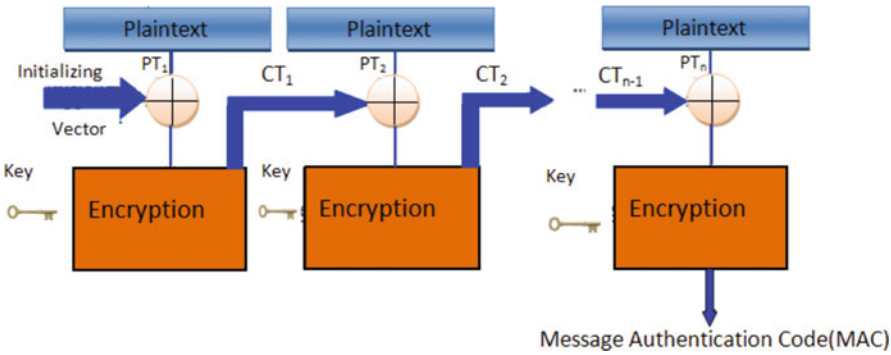

Fig. 7.8 CBC-MAC operation

6.3.2 AES-CBC-MAC

In AES-CBC-MAC [25], authentication and message integrity are provided using a cipher-block chaining message authentication code (CBC-MAC). According to CBC-MAC, an n block message $PT = PT_1, PT_2 \ldots, PT_n$ is authenticated among the parties who share a secret key for the block cipher. The sender can compute either of the 4, 8, or 16 byte message authentication code (MAC). However, the MAC can only be computed by parties having the symmetric key. Here, the plaintext is XORed with the previous cipher text until the final MAC is created where the cipher texts are generated by $CT_j = K_{en}(PT_j XOR CT_{j-1})$ and plaintexts can be generated from the cipher text by $PT_j = K_{de}(CT_j) XOR CT_{j-1}$. The sender appends the plaintext data with the computed MAC. The receiver then verifies the integrity by computing its own MAC and comparing it with the received MAC. The receiver accepts the packet only if both MACs are equal. The block diagram of CBC-MAC operation is illustrated in Fig. 7.8.

6.3.3 AES-CCM

This security suite includes both data integrity and encryption [25] and thus provides high level security. Here, integrity is protected over the header and data payload using CBC-MAC mode and then the data payload is encrypted using AES-CTR mode.

6.4 Existing Research Works

Existing research works that present security solutions for WSN and WBAN are listed according to timeline in Table 7.3. These research works primar-

Table 7.3 Researches on existing security and privacy solutions

Year	Research work	Network	Security mechanism	Threats handled	Performance metric
2008	[29]	WSN	Variation of strong password-based solutions	Threats to user authentication	Computational load, communication cost
2009	[30]	WSN	Secure and energy efficient clustered routing protocol	Usual attacks in WSN	Network lifetime, energy efficiency
2010	[60]	WSN	Key management scheme using hash function	Effect of compromised sensor nodes	Network resilience
2011	[14]	WSN	Symmetric cryptography	Threats to authentication	Energy consumption, scalability
	[46]	WBAN	Null, encryption only (AES-CTR), authentication only (AES-CBC-MAC), and encryption and authentication (AES-CCM)	Threats to eavesdropping, data modification and authentication	Corrupted slots in contention free period, bandwidth utilization, probability of failed guaranteed time slots
2012	[16]	WSN	Lightweight polynomial-based key management protocol	Common attacks to WSN such as node clone, impersonation	Computation and communication overhead
2013	[39]	WBAN	Biometric-based security	Threats to data authentication	Computational complexity, power efficiency
	[4]	WBAN	Cluster-based security mechanism	Spoofed, altered, replayed routing information, selective forwarding, sinkhole, sybil, wormhole attack	Lifetime, energy efficiency
2014	[27]	WSN	Multipath routing	Black hole attacks	Throughput, delay, packet loss
2015	[5]	WSN	Lightweight trust-based routing protocol	Different types of malicious threats	Packet delivery ratio, network lifetime, end to end delay, memory, and energy consumption
2016	[15]	WSN	Energy efficient encryption method	Brute force attack, HELLO flood attack, selective forwarding attack, and compromised cluster head attack	Network lifetime, energy consumption

(continued)

Table 7.3 (continued)

Year	Research work	Network	Security mechanism	Threats handled	Performance metric
2017	[24]	WSN	Payload-based mutual authentication	Network attacks such as replay, resource exhaustion, sybil	Energy consumption, network throughput
	[44]	WBAN	Secure lightweight routing strategy	Blackhole attack	Packet delivery ratio, energy consumption, ratio of false negatives
	[21]	WBAN	Anonymous authentication	Threats to authentication and modification	
2018	[7]	WSN	Certificate-based authentication	Threats to gateway authentication	
	[50]	WBAN	Multilayer authentication protocol and secure session key generation method	Threats to authentication	

ily focus on designing lightweight security techniques [16] to be applied in resource-constrained networks (such as WSN and WBAN) over the years. In [16], lightweight polynomial-based key management (LPKM) scheme has been proposed for distributed WSNs. Different types of keys are established by the sensor nodes to bootstrap trust and secure one-to-one and one-to-many communications in a flexible, reliable, and non-interactive way. The threat model includes most common attacks to WSNs such as node clone attacks, and node impersonation attacks. Besides, LPKM can tolerate dynamic network topology and incurs little computational and communication overhead. In [29], two simple user authentication protocols for WSN are proposed which are variations of a strong password-based solutions. Here, performance is measured in terms of computational load, communication cost, and security of the proposed protocols. Security threats to authentication are mostly handled in this work. A collaborative lightweight trust (CLT) based routing protocol for WSN has been proposed in [5] that incurs minimal overhead in regard to memory and energy consumption. The protocol does not use promiscuous mode of operation to monitor the neighboring nodes for trust assessment, instead it employs a novel trust counselor that monitors and warns the neighboring nodes whose trust falls below a warning threshold. A sensor node is notified with a warning message to rectify the packet forwarding behavior in order to improve its trust relationship with its neighbors. Performance of CLT protocol is measured by theoretical analysis and simulation in terms of packet delivery ratio, network lifetime, end-to-end delay, memory, and energy consumption. Existing literature [14, 60] identifies key distribution in shared broadcast medium is the major concern in employing cryptography-based security solutions. In [60], a novel key management scheme called SKM has been proposed for sequence-based key

management in WSNs. Here, sensor nodes are pre-distributed with the first term and the recursive formula of a numerical sequence. Accordingly, the two tiny pre-distributed information ensure the establishment of pairwise keys between each sensor node with its neighbors after its deployment with a small amount of computation. The efficiency of SKM is obtained through security analysis. Whereas in [14] a lightweight authentication model has been presented for wireless sensor networks. The model is composed of a key management scheme based on the use of simple symmetric cryptographic primitives with very low computational requirements and an authentication protocol. In [24], a lightweight payload-based mutual authentication scheme for a cluster-based hierarchical WSN has been designed. Here, the proposed scheme operates in two steps. First step includes election of an optimal percentage of cluster heads which are then authenticated and allowed to communicate with neighboring nodes. In the next step, each cluster head that acts in a role of server authenticates the nearby nodes for cluster formation. The proposed scheme has been validated using various simulation metrics such as energy consumption, network throughput. Although different security mechanisms have been designed to ensure authentication and protect data integrity, the techniques devised for WSN cannot readily be applied to WBAN as well due to their inherent differences. In [44], an energy efficient lightweight mechanism has been proposed to be applied in WBAN that prevents malicious intruders from dropping data packets or forwarding fake data. The mechanism has been experimented with adhoc on-demand distance vector (AODV) protocol though it can work with any other reactive WBAN routing protocol. Effectiveness of the protocol is evaluated in detecting malicious nodes with low overhead. In [39], the use of biometric characteristics is explored in securing data communication within WBAN and minimizing computational complexity as well as power efficiency. Here, hybrid authentication model is exploited as a conceptual framework for the system. In this work, the framework requires a unique feature of human body regarded as the authentication identity, while the other techniques use hardware and software to achieve the same purpose. In [4], an energy-efficient key management scheme for WBANs has been proposed that takes into account available resources of a node during the whole life cycle of key management. The proposed scheme is a cluster-based hybrid security framework that provides support for both intra-WBAN and inter-WBAN communications. Here, use of multiple clusters gives impact on energy efficiency. Security of the cluster formation process is implemented using electrocardiogram (EKG)-based key agreement scheme. Both preloading of keys and physiological value-based generated keys are exploited in this hybrid key management technique. Highly dynamic and random EKG values of the human body are used here for pairwise key generation and refreshment. The performance of the proposed cluster-based key management scheme is evaluated in terms of energy efficiency and network lifetime. However, for a small network consists of 15 to 20 nodes (standard network size for WBAN [35]) clustering could be an overhead. Exiting security solutions designed for both WSN and WBAN mostly cover threats to authentication and data integrity. Hence, a comprehensive solution is still to be designed to address all other potential threats as well and to obtain a

secure and optimal scheme for either networks. Thus, security and privacy in WSN and WBAN have been part of the active research over the years and will remain in the forthcoming time-frame as well.

7 Potential Applications

WSN applications in diverse domain can be broadly categorized according to their prime objective of deployment as shown in Fig. 7.9. A taxonomy of representative WSN applications is presented in Fig. 7.9. As depicted in the figure, the leading application domains of WSNs include environment, military and surveillance, health (body area networks), industry and agriculture, and urbanization and infrastructure [40]. WSN applications are generally of two types: monitoring and tracking. Remote monitoring is one of the primary concerns of WSN applications where environmental phenomenon or human activities are remotely supervised. In a number of applications, sensor nodes are often deployed in remote areas for monitoring natural phenomena like rain-forest and/or biodiversity monitoring [13], forest fire detection or surveillance [2]. In these applications, nodes are deployed at random (dropped from a vehicle, etc.) or are strategically placed. Such nodes remain more or less static throughout their lifetime though the connectivity varies due to node failure, communication failure, limited hardware resource, and environmental factors which are external to the system. It is mentioned in [13] that sensor networks for such applications are typically deployed in small scale and/or only for a short period of time. One of the major points of concern for this is system reliability [11]. It is not possible to come over and fix the faulty nodes at regular intervals. Security is another major concern for these networks particularly various forms of DoS attacks.

Security is even more important when WSNs are deployed in habitable areas for surveillance and/or infrastructure monitoring. One of the interesting applications in

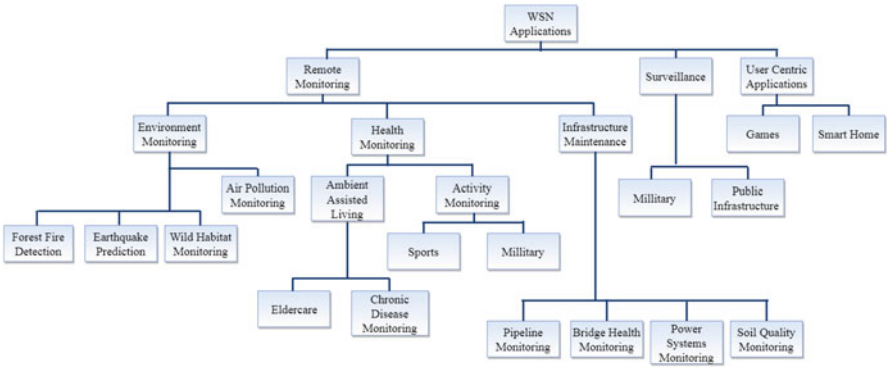

Fig. 7.9 Diverse application areas of WSN

military is military operations involving force protection with unattended ground sensors formed into intelligent networks around forward operating bases [40]. Networked mines called self-healing mine fields that automatically rearrange themselves to ensure optimal coverage are another interesting example. VigilNet (VigilNet. http://www.cs.virginia.edu/wsn/vigilnet/) presents an integrated sensor network system for energy-efficient surveillance missions. Encryption is a widely used mechanism to ensure data privacy and integrity. But even in such cases, tampering a node may divulge the security key information and/or traffic can also be rerouted. However, shared key cryptography [14] may make this kind of attacks difficult to launch. Application layer attacks, as detailed in Sect. 3, can also be launched especially when WSNs are used for surveillance. Ensuring precision and thereby reducing the false positive events is a major challenge in surveillance applications to encourage wide adoption of such prediction measures.

However, WSNs also find applications in sports, entertainment, medical applications, and smart home, where in addition to placing ambient sensors (temperature sensor, proximity sensor, etc.), the sensor nodes are also strategically placed in, on, or around human body to measure vital physiological parameters forming WBAN [35] over human body. WBANs are exploited for developing several applications related to remote healthcare, ambient assisted living even in user centric applications such as gaming and smart home as is summarized in Fig. 7.10. Human activity recognition has garnered a great research interest in recent years [3]. However, the use of WSN in healthcare applications is growing in fast pace where remote medical supervision could be beneficial for eldercare, detection of chronic diseases, etc. With ambient assisted living applications, the aged people can feel more independent in performing everyday activities. For instance, the ironHand project ((2016). D3.3.4 Glove Integrated Prototype (Fourth Iteration). [Online]. Available: http://www.ironhand.eu/) aims to facilitate elders with poor hand grips to continue with their daily work. The idea is to build a robotic glove that can add strengthen the grip for users with impaired hand function. Different accelerometers, muscle sensors (EMG sensor), and infrared sensors (IR sensor) are used in the gloves to capture the tension of muscle, which generates variable length data [33].

WBAN is also applied to monitor the practice of a player as well as his/her fitness in sports like hammer throwing, swimming, water volleyball, cricket, football, etc. [17]. Analyzing sensing data, specialized measures can be taken to improve their performance and maintaining their health. For water sports like swimming and water volleyball, the wearable sensors also change their communication mediums, i.e., from air to water or vice versa due to the movement of body. Hence such applications require not only water resistant case to place the sensors but also smart MAC protocols to tackle change of communication medium on the fly.

It is predicted that WBANs can be used in disaster rescue or emergency response like fire rescue [33] and flood rescue. In disaster rescue, body sensors would broadcast distress signals which can be received by rescue devices, or may get relayed or delivered by neighboring BANs (R. Huang and L. Chu, "Disaster rescue mode for body area networks," U.S. Patent 9 247 375, Jan. 26, 2016. [Online]. Available: https://www.google.ch/patents/US9247375). This adds an important dimension of WBAN applications which not only requires intra-BAN

Fig. 7.10 Diverse application areas of WBAN

but also inter-BAN communication ability in cross-medium. In such applications, different kind of sensors like temperature sensors, multimedia sensors, etc., along with GPS are used. Thus, the data size differs for each type of sensors. In the flood rescue response, sensors may use both water and air as the propagation medium thus requiring smart MAC protocols as well.

In all these applications sensors are either placed in, on, or around human body or they gather data about user behavior. Thus humans are closely related to the system. Hence, these applications call for security issues. For instance, data integrity is a critical requirement for WBAN applications as wrong information about body vitals of an individual could lead to wrong treatment and consequently, fatal consequences. Data privacy is also very important for these applications as sensitive data about user behavior, their daily lifestyles could be divulged and may pose to be a social threat. Even, any information or misinformation about player's fitness may ruin their reputation. Thus, WSN and hence WBAN applications should be made increasingly secure in order to guarantee precision and durability of the monitoring applications for which they are deployed. As more and more parties are getting involved with such applications, stringent privacy norms should also be set.

8 Open Research Issues

Now-a-days, sensors have become the eye of IoT-based applications [1]. Sensing and communications go hand-in-hand to solve a plethora of problems for smart city applications [22]. But rather than placing sensors at a remote location such

as forest fire monitoring, WSNs are increasingly placed in habitable areas, such as city wide air pollution monitoring systems. Presently, sensors are also designed to have some capability of energy harvesting. Thus, with proximity to the sensor deployment and increase of interested parties, maintaining data confidentiality and integrity is becoming harder day-by-day. Intelligent noise removal techniques can also be employed as today's sensors have some computation power. Crowdsourcing is emerging as a new technique for collecting data using the smartphone sensors carried by the citizens [12]. Smart home, smart building [38], and assisted living are important applications where sensing data are used to improve the quality of life of citizens. However, this calls for many important concerns from citizen's point of view, including sharing of personal data such as user location and ambient sound. Sharing of these data can raise significant concerns about security and user privacy [55]. As stated in [23], sensing and sourcing applications potentially collect sensitive sensor data pertaining to individuals that can be used to detect behavioral patterns of individuals. For example, GPS sensor readings can be used to proactively predict traffic congestion levels and/or anomalies in a given community, but at the same time these can be used to infer private information like movement trajectory of an individual, routes they take during their daily commutes, as well as their home and work locations [12]. Thus security and privacy issues of WSNs are even more pertinent for today's sensors that are deployed in habitable areas and are collecting data on urban lifestyle.

Sensors, especially bio-sensors are also worn by citizens and they also pose significant security and privacy challenges that only a few existing solutions could address. Currently, WBANs involve homecare, especially, eldercare and hospital environment scenarios. In homecare and hospital scenarios, body sensors are in direct communication range of the sink, and they do not require to route packets. But only sometimes they require to send data through maximum 2 hops [42]. Thus few literature could be found on routing attacks such as selective forwarding, wormhole and sinkhole attacks in the intra-BAN level of WBANs. However, in the near future, with the deployment of mobile networks, WBANs can play a critical role in treatment of victims in disaster events. In disaster scenarios, body sensors might need to send their data through other devices outside their immediate radio range. Therefore, routing protocols with strong security features will become a crucial service for effective end-to-end communications in the intra-BAN level of WBANs. Intruders may launch denial of service attacks by causing inter-BAN interference and thereby blocking all data traffic from reaching the sink.

The second issue that definitely will become more important in near future is lack of cohesive policy sets to protect the patient's privacy. As WBANs become ubiquitous, more parties such as pharmacies and insurance companies will be involved in the system. Therefore, patient related data will be accessed by more parties, and more attacks on patient privacy are possible that may affect their social lives as well. Thus, privacy attacks may pose to be a major obstacle to growth and development of this technology and may hinder wide adoption of it. If current and future privacy issues are not well formulated, WBAN may remain only as a research prototype. In new set of policies, all possible future parties and privacy threads

associated with them should be considered so that all involved parties find it difficult to abuse from patient data.

The next generation of WSNs and hence WBANs could benefit from the advantage of cloud computing technology. Combining mobile cloud computing with sensors wide applications and business models are beginning to emerge [54]. With the support of mobile cloud computing, the deployment of innovative healthcare monitoring applications with richer multimedia contents is now technically feasible but more reliable quality of service and more types of convergence services are needed. This combination will require new security threads [54]. The growth of sensing technology not only for WBANs but for many other variants of WSNs is rapid and fast thus needing suitable updation of current security and privacy issues. New points of concern will be raised in this area in the near future, in this section we just mentioned a few of them.

9 Conclusions

This chapter presents a thorough study on the security and privacy issues of WSN and WBAN. At the beginning, the networks are studied in detail along with their characteristics, architecture, performance metrics, applications and accordingly a comparative analysis has been made as well. After that the key requirements for security and privacy in both networks are illustrated. A categorization of the potential threats to both networks has also been made to get insight of the attacks such as their origin, nature, and objective. Next, the existing measures are studied accordingly. Finally, the open research challenges are identified to motivate the researchers for further investigation in those areas.

References

1. Adat, V., & Gupta, B. (2018). Security in internet of things: Issues, challenges, taxonomy, and architecture. *Telecommunication Systems, 67*(3), 423–441.
2. Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., & Cayirci, E. (2002). Wireless sensor networks: A survey. *Computer Networks, 38*(4), 393–422.
3. Al Ameen, M., Liu, J., & Kwak, K. (2012). Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of Medical Systems, 36*(1), 93–101.
4. 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), 216.
5. Anita, X., Bhagyaveni, M. A., & Manickam, J. M. L. (2015). Collaborative lightweight trust management scheme for wireless sensor networks. *Wireless Personal Communications, 80*(1), 117–140.
6. Arampatzis, T., Lygeros, J., & Manesis, S. (2005). A survey of applications of wireless sensors and wireless sensor networks. In *Proceedings of the 2005 IEEE International Symposium on Mediterranean Conference on Control and Automation, Intelligent Control* (pp. 719–724). Piscataway: IEEE.

7. Bicket, J., Rowson, J. M., & Phillips, C. (2018). Authentication of a gateway device in a sensor network. US Patent App. 10/085,149.
8. Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of security and privacy issues of internet of things. arXiv preprint arXiv:1501.02211.
9. Cavallari, R., Martelli, F., Rosini, R., Buratti, C., & Verdone, R. (2014). A survey on wireless body area networks: Technologies and design challenges. *IEEE Communications Surveys & Tutorials, 16*(3), 1635–1657.
10. Chen, J. C., Jiang, M. C., & Liu, Y. W. (2005). Wireless lan security and IEEE 802.11 i. *IEEE Wireless Communications, 12*(1), 27–36.
11. Chowdhury, C., Aslam, N., Ahmed, G., Chattapadhyay, S., Neogy, S., & Zhang, L. (2018). Novel algorithms for reliability evaluation of remotely deployed wireless sensor networks. *Wireless Personal Communications, 98*(1), 1331–1360.
12. Chowdhury, C., & Roy, S. (2017). Mobile crowdsensing for smart cities. In *Smart cities: Foundations, principles, and applications* (pp. 125–154). Hoboken: Wiley.
13. Corke, P., Wark, T., Jurdak, R., Hu, W., Valencia, P., & Moore, D. (2010). Environmental wireless sensor networks. *Proceedings of the IEEE, 98*(11), 1903–1917.
14. Delgado-Mohatar, O., Fúster-Sabater, A., & Sierra, J. M. (2011). A light-weight authentication scheme for wireless sensor networks. *Ad Hoc Networks, 9*(5), 727–735.
15. Elhoseny, M., Yuan, X., El-Minir, H., & Riad, A. (2016). An energy efficient encryption method for secure dynamic WSN. *Security and Communication Networks, 9*(13), 2024–2031.
16. Fan, X., & Gong, G. (2012). LPKM: A lightweight polynomial-based key management protocol for distributed wireless sensor networks. In *International Conference on Ad Hoc Networks* (pp. 180–195). Berlin: Springer.
17. Fu, Y., & Liu, J. (2013). Monitoring system for sports activities using body area networks. In *Proceedings of the 8th International Conference on Body Area Networks* (pp. 408–413).
18. Gungor, V. C., & Hancke, G. P. (2009). Industrial wireless sensor networks: Challenges, design principles, and technical approaches. *IEEE Transactions on Industrial Electronics, 56*(10), 4258–4265.
19. Gupta, B. B. (2018). *Computer and cyber security: Principles, algorithm, applications, and perspectives*. Boca Raton: CRC Press.
20. Halder, S., Ghosal, A., & Bit, S. D. (2011). A pre-determined node deployment strategy to prolong network lifetime in wireless sensor network. *Computer Communications, 34*(11), 1294–1306.
21. He, D., Zeadally, S., Kumar, N., & Lee, J. H. (2017). Anonymous authentication for wireless body area networks with provable security. *IEEE Systems Journal, 11*(4), 2590–2601.
22. Hossain, M. S., Muhammad, G., Abdul, W., Song, B., & Gupta, B. (2018). Cloud-assisted secure video transmission and sharing framework for smart cities. *Future Generation Computer Systems, 83*, 596–606.
23. Huang, K. L., Kanhere, S., & Hu, W. (2010). Are you contributing trustworthy data? The case for a reputation system in participatory sensing. In *Proceedings of the 13th ACM International Conference on Modeling, Analysis, and Simulation of Wireless and Mobile Systems (MSWIM'10)* (pp. 14–22). New York: ACM.
24. Jan, M., Nanda, P., Usman, M., & He, X. (2017). PAWN: A payload-based mutual authentication scheme for wireless sensor networks. *Concurrency and Computation: Practice and Experience, 29*(17), e3986.
25. Javadi, S. S., & Razzaque, M. (2013). Security and privacy in wireless body area networks for health care applications. In *Wireless networks and security* (pp. 165–187). Berlin: Springer.
26. Kallio, J., & Koivusaari, J. (2016). WSN related requirement analysis towards sustainable building automation operations and maintenance. In *Ubiquitous computing and ambient intelligence* (pp. 212–217). Berlin: Springer.
27. Khan, K., & Goodridge, W. (2014). Impact of multipath routing on WSN security attacks. *International Journal of Intelligent Systems and Applications, 6*(6), 72.
28. Kompara, M., & Hölbl, M. (2018). Survey on security in intra-body area network communication. *Ad Hoc Networks, 70*, 23–43.

29. Lee, T. H. (2008). Simple dynamic user authentication protocols for wireless sensor networks. In *Second International Conference on Sensor Technologies and Applications, 2008. SENSORCOMM'08* (pp. 657–660). Piscataway: IEEE.
30. Liu, Q., & Wang, P. K. (2009). Secure and energy-efficient clustered routing protocol for wireless sensor networks [j]. *Computer Simulation, 4*, 041.
31. Liu, X., Cao, J., Lai, S., Yang, C., Wu, H., & Xu, Y. L. (2011). Energy efficient clustering for WSN-based structural health monitoring. In *Proceedings IEEE INFOCOM, 2011* (pp. 2768–2776). Piscataway: IEEE.
32. Mainanwal, V., Gupta, M., & Upadhayay, S. K. (2015) A survey on wireless body area network: Security technology and its design methodology issue. In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)* (pp. 1–5). Piscataway: IEEE.
33. Maitra, T., & Roy, S. (2018). Research challenges in ban due to the mixed WSN features: Some perspectives and future directions. *IEEE Sensors Journal, 17*(17), 5759–5766.
34. Movassaghi, S., Abolhasan, M., & Lipman, J. (2013). A review of routing protocols in wireless body area networks. *Journal of Networks, 8*(3), 559–575.
35. Movassaghi, S., Abolhasan, M., Lipman, J., Smith, D., & Jamalipour, A. (2014). Wireless body area networks: A survey. *IEEE Communications Surveys & Tutorials, 16*(3), 1658–1686.
36. Pantazis, N. A., Nikolidakis, S. A., & Vergados, D. D. (2013). Energy-efficient routing protocols in wireless sensor networks: A survey. *IEEE Communications Surveys & Tutorials, 15*(2), 551–591.
37. Pathan, A. S. K., Lee, H. W., & Hong, C. S. (2006). Security in wireless sensor networks: Issues and challenges. In *The 8th International Conference on Advanced Communication Technology, ICACT 2006* (Vol. 2, 6 pp.). Piscataway: IEEE.
38. Plageras, A. P., Psannis, K. E., Stergiou, C., Wang, H., & Gupta, B. B. (2018). Efficient IoT-based sensor big data collection–processing and analysis in smart buildings. *Future Generation Computer Systems, 82*, 349–357.
39. Ramli, S. N., Ahmad, R., Abdollah, M. F., & Dutkiewicz, E. (2013). A biometric-based security for data authentication in wireless body area network (WBAN). In *15th International Conference on Advanced Communication Technology (ICACT)* (pp. 998–1001). Piscataway: IEEE.
40. Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M. (2014). Wireless sensor networks: Recent developments and potential synergies. *The Journal of Supercomputing, 68*(1), 1–48.
41. Romer, K., & Mattern, F. (2004). The design space of wireless sensor networks. *IEEE Wireless Communications, 11*(6), 54–61.
42. Roy, M., Chowdhury, C., & Aslam, N. (2017). Designing 2-hop interference aware energy efficient routing (hier) protocol for wireless body area networks. In *International Conference on Communication Systems and Networks* (pp. 262–283). Berlin: Springer.
43. Roy, M., Chowdhury, C., & Aslam, N. (2017). Designing an energy efficient WBAN routing protocol. In *9th International Conference on Communication Systems and Networks (COMSNETS)* (pp. 298–305). Piscataway: IEEE.
44. Roy, M., Chowdhury, C., Kundu, A., & Aslam, N. (2017). Secure lightweight routing (SLR) strategy for wireless body area networks. In *IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (pp. 1–4). Piscataway: IEEE.
45. Roy, M., Chowdhury, C., & Neogy, S. (2014). Developing secured manet using trust. In *Fourth International Conference on Advances in Computing and Communications (ICACC)* (pp. 183–186). Piscataway: IEEE.
46. Saleem, S., Ullah, S., & Kwak, K. S. (2011). A study of IEEE 802.15. 4 security framework for wireless body area networks. *Sensors, 11*(2), 1383–1395.
47. Saleem, S., Ullah, S., & Yoo, H. S. (2009). On the security issues in wireless body area networks. *International Journal of Digital Content Technology and Its Applications, 3*(3), 178–184.
48. Seah, W. K., Eu, Z. A., & Tan, H. P. (2009). Wireless sensor networks powered by ambient energy harvesting (WSN-heap)-survey and challenges. In *1st International Conference on*

Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology. Wireless VITAE 2009 (pp. 1–5). Piscataway: IEEE.
49. Senouci, M. R., Mellouk, A., Senouci, M. A., & Oukhellou, L. (2014). Belief functions in telecommunications and network technologies: An overview. *Annals of Telecommunications, 69*(3–4), 135–145.
50. Shen, J., Chang, S., Shen, J., Liu, Q., & Sun, X. (2018). A lightweight multi-layer authentication protocol for wireless body area networks. *Future Generation Computer Systems, 78*, 956–963.
51. Sheng, Z., Yang, S., Yu, Y., Vasilakos, A., Mccann, J., & Leung, K. (2013). A survey on the IETF protocol suite for the internet of things: Standards, challenges, and opportunities. *IEEE Wireless Communications, 20*(6), 91–98.
52. Singh, S. K., Singh, M., & Singh, D. K. (2010). Routing protocols in wireless sensor networks–a survey. *International Journal of Computer Science & Engineering Survey, 1*(2), 63–83.
53. Singla, A., & Sachdeva, R. (2013). Review on security issues and attacks in wireless sensor networks. *International Journal of Advanced Research in Computer Science and Software Engineering, 3*(4), 529–534.
54. Stergiou, C., Psannis, K. E., Kim, B. G., & Gupta, B. (2018). Secure integration of IoT and cloud computing. *Future Generation Computer Systems, 78*, 964–975.
55. Tewari, A., & Gupta, B. (2018, in press). Security, privacy and trust of different layers in internet-of-things (IoTs) framework. *Future Generation Computer Systems*. https://doi.org/10.1016/j.future.2018.04.027
56. Tiegang, F., Guifa, T., & Limin, H. (2014). Deployment strategy of wsn based on minimizing cost per unit area. *Computer Communications, 38*, 26–35.
57. Toorani, M. (2016). Security analysis of the IEEE 802.15. 6 standard. *International Journal of Communication Systems, 29*(17), 2471–2489.
58. Vullers, R. J., Van Schaijk, R., Visser, H. J., Penders, J., & Van Hoof, C. (2010). Energy harvesting for autonomous wireless sensor networks. *IEEE Solid-State Circuits Magazine, 2*(2), 29–38.
59. Wang, Y., Attebury, G., & Ramamurthy, B. (2006). A survey of security issues in wireless sensor networks. *IEEE Communications Surveys & Tutorials, 8*, 2–23.
60. Zhang, T., & Qu, H. (2010). A lightweight key management scheme for wireless sensor networks. In *Second International Workshop on Education Technology and Computer Science (ETCS)* (Vol. 1, pp. 272–275). Piscataway: IEEE.
61. Zia, T., & Zomaya, A. (2006). Security issues in wireless sensor networks. In *Proceedings of the International Conference on Systems and Networks Communications (ICSNC 2006)* (p. 40). Piscataway: IEEE.