State of The Art in WBAN Security & Open Research Issues

Ms. Sanchari Saha[1], Dr. Dinesh K Anvekar[2]
[1]*Department of CSE, MVJCE, Bangalore,*
[2]*Dept of CSE, Nitte Meenakshi Institute of Technology, Bangalore*
saha.sanchari85@gmail.com
dinesh.anvekar@gmail.com

Abstract— The increase in average lifespan and health cost in many developed nations are catalysts to innovation in health care. Regular monitoring of vital signs is essential as they are primary indicators of an individual's physical well-being and thus individuals have to make frequent visits to their doctor(s) to get their vital signs checked. These factors along with the advances in miniaturization of electronic devices, sensing, battery and wireless communication technologies have led to the development of Wireless Body Area Networks (WBANs). As the security and privacy of patient-related data are two indispensable components for the system security of the WBAN and since the patient-related data stored in the WBAN plays a critical role in medical diagnosis and treatment, it is essential to ensure the security of these data. The main aim of this paper is to provide a state of the art in the existing WBAN security aspects and also to highlight some key challenges for research in this security concern.

Keywords— *WSN, WBAN, Security, Threat, Research Issues*

*****

I. INTRODUCTION

Recent technological advances in sensors, low-power microelectronics and wireless networking have enabled the design and proliferation of wireless sensor networks capable of autonomously monitoring and controlling environments. One of the most promising applications of sensor networks is human health monitoring. A number of tiny wireless sensors, strategically placed on the human body, create a Wireless Body Area Network (WBAN) that can monitor various vital signs, providing real-time feedback to the user and medical personnel. Generally speaking, three types of devices can be distinguished in WBAN: sensors, actuators and personal device. The sensors are used to measure certain parameters of the human body, either externally or internally. Examples include measuring the heartbeat, body temperature or recording a prolonged electrocardiogram (ECG). The figure 1 represents the placement and purpose of sensor nodes in human body. The actuators (or actors) on the other hand take some specific actions according to the data they receive from the sensors or through interaction with the user, e.g., an actuator equipped with a built-in reservoir and pump administers the correct dose of insulin to give to diabetics based on the glucose level measurements. Interaction with the user or other persons is usually handled by a personal device, e.g. a PDA or a smart phone which acts as a sink for data of the wireless devices. In order to realize communication between these devices, techniques from Wireless Sensor Networks (WSNs) and ad hoc networks could be used [1]. However, because of the typical properties of a WBAN, current protocols designed for these networks are not always well suited to support a WBAN.

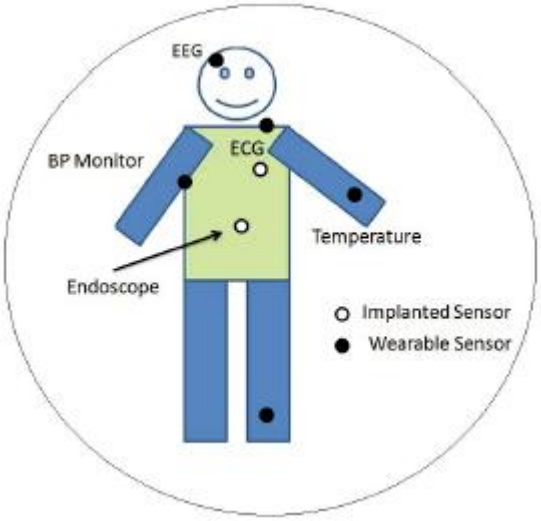

Figure 1: Placement of sensor nodes in human body

In figure 2, a general architecture of the WBAN is represented which consists of tier 1 and tier 2. The figure shows that the collected data is either stored in the WBAN for distributed, local access, or transferred from the WBAN to medical databases in tier 3 for centralized, remote access. The users of the patient-related data of a WBAN may include patients, doctors, nurses, support staff, scientists, and insurance companies. Lack of security in WBANs may hamper the wide public acceptance of this technology, and more importantly can cause life-critical events and even death of patients. Open nature of the wireless medium, makes the patient's data prone to being eavesdropped, modified, lost or injected. Moreover, typical channel characteristics in WBANs such as very low Signal-to-Noise-Ratio (SNR) condition and limitation of body sensors in terms of power budget, memory capacity, communication and computational ability make the possibility

 ISSN: 2321-8169
1958 – 1964

of security attacks and threads in WBANs more likely than traditional Wireless Sensor Networks (WSNs). In addition, in WBANs, both security and system performance are equally important, therefore, the integration of a high-level security mechanism in such resource-constrained networks is difficult. So far, although there are already several prototype implementations of WBANs that deal with QoS and energy efficiency, studies on data security and privacy issues are few, and existing solutions are far from mature.

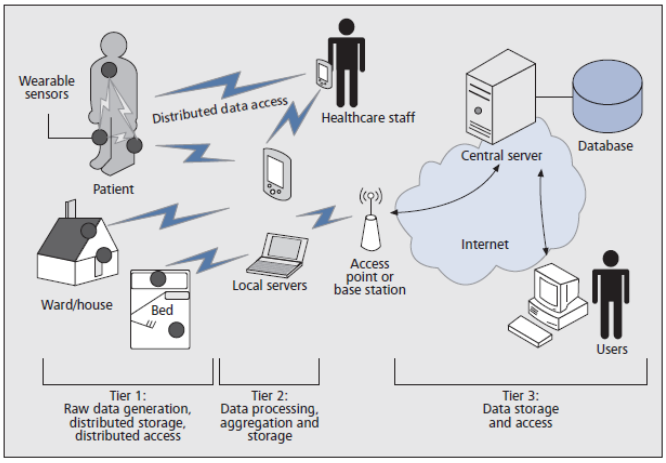

Figure 2: A general architecture of the WBAN

II. Security & Privacy Requirements in WBAN

By data security, we mean data is securely stored and transferred; and data privacy means the data can only be accessed by the people who have authorization to view and use it [2].

Data confidentiality, dependability, and integrity are three most important requirements for distributed data storage in WBAN. In order to prevent patient-related data from leaking during storage periods, the data needs always to be kept confidential at a node or local server. In WBANs the patient-related data is vital, and modified data would lead to disastrous consequences. Thus, data integrity shall be dynamically protected all the time.

Dependability is another critical concern in WBANs, because failure to retrieve correct data may become a life-threatening matter. In order to tackle the threats caused by network dynamics, fault tolerance is required.

A fine-grained data access policy should be enforced to prevent unauthorized access to patient-related data generated by the WBAN. Access control needs to be enforced for patient-related data in WBANs so that private information will not be obtained by unauthorized parties.

In WBANs distributively stored private data may easily be leaked due to physical compromise of a node. Therefore, data encryption and cryptographically enforced access control is needed to protect the privacy of patients.

Authentication is a necessary security service to prevent false data injection and DoS attacks, and is also required to verify a user's identity before data access. Moreover, it is needed to secure data transfer within the WBAN. The sender of the patient-related data must be authenticated, and injection of data from outside the WBAN should be prevented.

Patient-related data must not be modified illegally during storage periods, which shall be checked and detected by a node dynamically.

III. WBAN Attacks

Attacks on secrecy and authentication: Here an adversary performs eavesdropping, packet replay attacks, or spoofing of packets. One example of eavesdrop attacks in WBANs is activity tracking of users [3].

Sinkhole attack: It is similar to selective forwarding except that it is not a passive attack. In this attack, traffic is attracted towards the compromised or false node. This node drops packets in order to stop packet forwarding [4].

Stealthy attacks against service integrity: In this kind of attacks, the attacker attempts to make the network accept a false data value by changing the patient's data before it reaches to the PS. For instance, an attacker can change a high blood pressure value to a normal blood pressure value. This can lead to a disaster event [4].

Attacks on network availability: These attacks are referred to as Denial-of- Service (DoS) attacks. DoS attacks attempt to make network resource unavailable to its users and affect the capacity and the performance of a network [5].

Jamming: It is defined as interference with the radio frequencies of the body sensors. In this attack, the adversary tries to prevent, or interfere with the reception of signals at the nodes in the network. In doing so, the attacker sends a continuous random signal on the same frequency used by the body sensors. Affected nodes will not be able to receive messages from other nodes [5].

Selective forwarding: occurs when an adversary includes a compromised node in a routing path. When a malicious node receives a packet, it will do nothing and drop it. The malicious node can drop packets both selectively (just for a particular destination) and completely (all packets). Selective forwarding attacks are not applicable to the first communications level (intra-BAN level) of WBAN's architecture [5].

Sybil attacks: Here a malicious node, called the Sybil node, illegitimately claims multiple false identities by either fabricating new identities or impersonating existing ones. In WSNs, which involve routing, this attack can cause a routing algorithm to calculate two disjoint paths. In WBANs, at the intra-BAN level of communications, this attack can use feigned identities to send false information to the PS [6].

Spoofing attack: It targets the routing information exchanged between nodes [6], and attempts to spoof, alter, or replay the information with the intention to complicate the network. For example, an attacker could disturb the network by creating routing loops, generating fake error messages and attracting or repelling network traffic from selected nodes [6].

Flooding attack: It is used to exhaust memory resources by sending a large number of connection setup requests. Since body sensors suffer from low memory space, they are vulnerable against flooding attacks [6].

Device level attack: The WBAN often operates in environments with open access by various people (e.g., hospital staff), which also accommodates attackers. The open wireless channel makes the data prone to being eavesdropped, modified, and injected. The sensor nodes in a WBAN are subjected to compromise, as they are usually easy to capture and not tamper-proof. If a whole piece of data is directly encrypted and stored in a node along with its encryption key, the compromise of this node will lead to the disclosure of data.

Network level attack: The WBAN is highly dynamic in nature. Due to accidental failure or malicious activities, nodes may join or leave the network frequently. Nodes may die out due to lack of power. Attackers may easily place faked sensors in order to masquerade authentic ones, and could take away legitimate nodes deliberately.

IV. CHALLENGES IN IMPLEMENTING SECURITY NEEDS IN WBAN:

Wireless Body Area Networks (WBANs) have gained a lot of research attention in recent years since they offer tremendous benefits for remote health monitoring and continuous, real-time patient care. However, as with any wireless communication, data security in WBANs is a challenging design issue.

There are number of challenges in implementing these security needs which one must overcome to design a highly secure and privacy preserving WBAN. A major challenge in implementing security and privacy includes making a balance between security, efficiency, and practicality. Stringent resource constraints on devices within a WBAN, especially the sensor nodes, basically require the security mechanisms to be as lightweight as possible.

Practical challenges, such as conflicts between security, safety, and usability, also need to be considered carefully. For example, in order to ensure legitimate access to patients' data under time sensitive scenarios such as emergency care, the access control mechanisms should be context aware and flexible.

Balancing Security and efficiency

High efficiency is strongly demanded for data security in WBANs, not only because of the resource constraints, but also for the applications. Wearable sensors are often extremely small and have limited power supplies, which render them inferior in computation and storage capabilities. Thus, the cryptographic primitives used by the sensor nodes should be as lightweight as possible, in terms of both fast computation and low storage overhead.

Balancing security and safety

Whether the data can be accessed whenever needed could be a matter of patients' safety. Too strict and inflexible data access control may prevent the medical information being accessed in time by legitimate medical staff, especially in emergency scenarios where the patient may be unconscious and unable to respond. On the other hand, a loose access control scheme opens back doors to malicious attackers. It is hard to ensure strong data security and privacy while allowing flexible access.

Balancing security and usability:

The devices should be easy to use and foolproof, since their operators might be non-expert patients. As the setup and control process of the data security mechanisms are patient-related, they shall involve few and intuitive human interactions.

Device interoperability

Patients may buy sensor nodes from different manufacturers, among which it is difficult to pre-share any cryptographic materials. It is difficult to establish data security mechanisms that require the least common settings and efforts, and work with a wide range of devices.

V. EXISTING SECURITY SOLUTIONS FOR WBAN & DRAWBACKS

Most security protocols and mechanisms need cryptographic primitives in order to integrate the security properties into their operations. These cryptographic primitives are Symmetric Key Cryptography (SKC), Public Key Cryptography (PKC), and Hash functions. There are some authentication schemes based on symmetric key cryptography for WBAN, such as Tinysec [7], MiniSec [8], and μTESLA [9].

TinySec provides authentication, message integrity and confidentiality with low energy consumption and memory usage. However, it depends on the network-wide key distribution mechanism, if a single node is compromised, the entire network will be insecure [10].

MiniSec is publicly available with high security, but the high energy consumption is required when large packets are sent by radio frequency [11].

µTESLA provides source authentication and message integrity by utilizing a one-way hash chain and the delayed key disclosure technique, but it requires time synchronization between all nodes in the network [12] and causes authentication delay. Although these symmetric-key based schemes are efficient in processing time for sensor networks, the complex key management will introduce large memory and communication overhead, hence limit the deployment of practical WBAN.

The Identity-Based Cryptography (IBC) scheme improves the computational efficiency because no public key certificates need to be transmitted. But if a private key generator (PKG) is compromised, all messages protected over the entire lifetime of the public-private key pair used by that server are also compromised. This makes the PKG a high value target to adversaries. To limit the exposure due to a compromised server, the master private-public key pair could be updated with a new independent key pair. However, this introduces a key-management problem where all users must have the most recent public key for the server.

Zero-knowledge proof (ZKP) developed by Goldwasser et al. [13] is an efficient cryptographic protocol with small computational requirement compared to other public key based methods and it can be applied in the authentication and key exchange. An authentication scheme by using interactive ZKP to identify the users is developed in [14] and is applied for identifying wireless sensor nodes in [15]. But the performance of this scheme is low because multiple iterations between sensor nodes and base station are needed to be performed to confirm the identity of the senders.

The IEEE802.11b security specifications include services for link-level authentication and an optional privacy (i.e., confidentiality) service termed Wired Equivalent Privacy (WEP), designed to protect the confidentiality of link layer traffic. The security provisions of the standard present no claims about secure integrity assurance; they simply specify a frame check sequence error control mechanism. Research reports and press accounts have reported serious flaws in the authentication service and the WEP algorithm.

Many problems have been identified with IEEE's 802.11b security mechanisms. Some of them are due to the fact that WEP as a mechanism has problems because it uses a cryptographic algorithm (RC4) that has many weaknesses and is vulnerable to many passive and active attacks. The Initialization Vectors, which are part of the WEP key are short and static. This produces key streams with repeated parts over time, making possible the decryption of the ciphertext. WEP does not have any key management mechanisms. It does not describe how the various keys are shared among users and if and how the keys are to be updated or redefined, when invalidated or discovered by an attacker.

Bluetooth security: The Bluetooth wireless technology has built-in encryption and authentication mechanisms. In order to secure its hosts from attacks, in addition to this, it uses frequency-hopping schemes with 1600 hops/sec with an automatic output power adaptation to reduce the range exactly to the minimum necessary. There are some known drawbacks with Bluetooth security: The E0 stream cipher with 128-bit key length can be broken in proportion to 2^64 steps in some circumstances, using a divide-and-conquer type of attack. Hence, a better, more robust encryption algorithm is necessary to ensure security. The use of Personal Identification Numbers (PIN) codes, in the generation of the link keys and encryption keys, in the security scheme can also cause some problems.
Firstly, the keys are only four digits long so they can be easily guessed. Secondly in a large Bluetooth network with many users, problems will appear with the generation and distribution of all the necessary PINs, because there is no key management protocol. This is certain to cause scalability and flexibility problems that may lead to security problems.

AES-CTR: Confidentiality protection in AES-CTR is provided by using Advance Encryption Standard (AES) block cipher with counter mode (CTR). In this mode, the cipher text is broken into 16-byte blocks b1, b2… b n.

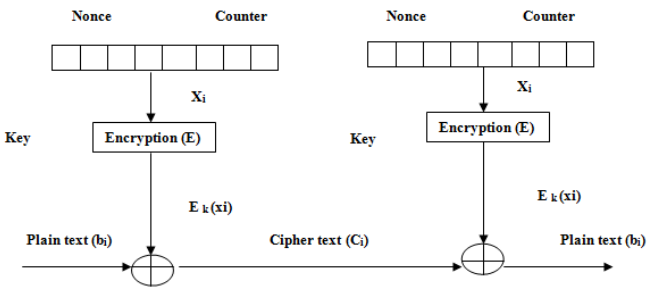

Figure 3: AES-CTR scheme

The sender side, computes the cipher text by ci=bi XOR Ek(xi), where ci is the encrypted text, bi is the data block, and Ek(xi) is the encryption of the counter xi .The receiver decodes the

 ISSN: 2321-8169
1958 – 1964

plaintext by computing bi = ci XOR Ek(xi). The encryption and decryption processes are shown in Figure 3.

AES-CBC-MAC

In AES-CBC-MAC, security including authentication and message integrity protection is provided by using a Cipher-Block Chaining Message Authentication Code (CBC-MAC). CBC- MAC specifies that an n block message B = b1, b2..., b n should be authenticated among parties who share a secret key (K) for the block cipher (E)[16]. The sender can compute either a 4, 8, or 16 byte MAC. The MAC can only be computed by parties with the symmetric key. In this mechanism, the plaintext is XORed with the previous cipher text until the final MAC is created where the cipher texts are generated by ci= Ek(bi XOR ci-1) and plaintexts can be generated by bi= Dk(ci)XOR ci-1.The sender appends the plaintext data with the computed MAC. The receiver verifies the integrity by computing its own MAC and comparing it with the received MAC. The receiver accepts the packet if both MACs are equal. Figure 4 shows the block diagram of a CBC-MAC operation.

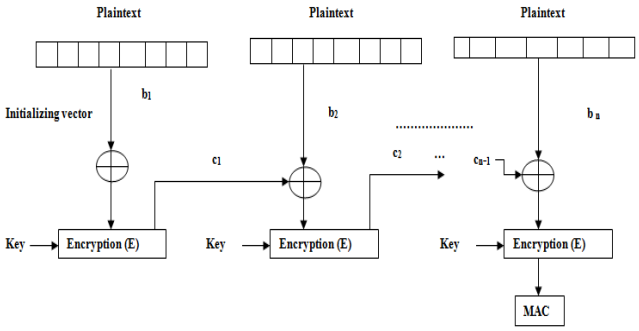

Figure 4: AES-CBC-MAC scheme

Blundo's key predistribution scheme: A security solution proposed by Morchon *et al*. [9], utilizes Blundo's key predistribution scheme. By predistribution polynomial key shares, the patient can easily establish a pair wise key with any authorized entity, and encrypt a copy of his/her data using this key for that entity. Although the patient can exert individual control over of different entities' access rights the patient would need to know the exact set of authorized users when distributing a file, and to encrypt one copy for each user in the set, which is impractical.

Drawbacks: Fine-grained access control is hard to realize due to the high key management complexity. They are vulnerable to user collusion. Compromising a node will possibly expose the data, since if a node cannot store encrypted copies for all possible users, it must store the data in plaintext. It is desirable that the data remain encrypted even when stored in WBAN nodes or servers. In order to achieve both fine-grained access control and efficiency, it is more desirable to encrypt *once and for all* (i.e., encrypt the file once so that all the authorized users can have access).

ABE scheme: Attribute- Based Encryption (ABE), an effective primitive to achieve fine-grained access control [16]. ABE is a one-to-many encryption method, where the cipher text is meant to be readable only by a group of users that satisfy a certain access policy. ABE is collusion-resistant; that is, any set of colluding users will not be able to derive any key belonging to other users. Its expressiveness on the access policy makes it a good candidate for fine-grained data access control in WBANs.

Drawback: patients' privacy information may still be leaked from the access policies, from which patients' or users' identities might be inferred. Therefore, it is desirable to be anonymous

CP-ABE scheme: In Cipher text Policy ABE (CP-ABE) [17] each user is assigned a set of attributes (roles), and a patient can freely choose a set of users/roles that are allowed to gain access to his/her medical data, from which the access policy is derived. Whenever a node in the WBAN generates some data, the access policy is built into the cipher text. The key idea of CP-ABE is to split a secret among secret key components belonging to different attributes owned by a user, which are randomized so as to provide collusion resistance. CP-ABE supports a treelike access policy structure, which is expressive, and it is fairly easy to integrate context related parameters as attributes, such as the time. Recently, Nishide *et al*. proposed two constructions of CP-ABE with a partially hidden access policy [18]. They achieve recipient anonymity by hiding which subset of attributes is specified in the access policy.

Drawback: The complexities of CP-ABE scheme are high, which limits the applicability to WBANs. The CP-ABE scheme requires about 2*m* exponentiations (ECC point multiplications) for encryption, where *m* is the number of attributes included in the AP. For decryption, it uses about 2*l* pairings, where *l* is the number of attributes of the decryptor that match the AP. Implementing CP-ABE on the sensor nodes may not be a good choice, since one point multiplication and pairing operation takes seconds. The PC is ten times far better than sensor nodes, while the PDA is moderately better. Approximately, when the number of attributes is less than 10, it takes several seconds to do ABE encryption and decryption on a PDA. Considering the architecture of a WBAN, it is feasible to encrypt the data at local servers like PDAs or desktop computers. To do so, the sensor nodes can send their data to the local servers for further encryption for access control, and use symmetric encryption to secure the data transfer between sensors and local servers.

VI. OPEN RESEARCH ISSUES

The role of WBANS in healthcare applications is becoming more and more prominent. As this technology becomes

pervasive, it will be exposed to numerous security and privacy threads. It is better to be ready for such situations before the time comes for it.

Currently, WBANs involve homecare and hospital environment scenarios. However, in the near future, with the deployment of mobile and wireless networks, body sensors in WBAN might need to send their data to other devices outside their immediate radio range. Therefore, routing protocols with strong security features will become a crucial service for end-to-end communications in the intra-BAN level of WBANs.

As WBANs become pervasive, 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. Privacy attacks make people pessimistic about WBANs, and will force major obstacles to growth and development of this technology. We feel that without taking care of current and future privacy issues, WBANs will not be accepted by the public. So, strong set of regulations and policies should be formalized and implemented.

The next generation of WBANs could benefit from the advantage of cloud computing technology. Combining mobile cloud computing and WBANs is a very new and interesting topic [19]. But again this combination will involve new security threats that need to be considered.

The growth of WBAN is rapid and fast. Along with current security and privacy issues, new threats may be raised in this area in the near future.

VII. CONCLUSION

A WBAN is expected to be a very useful technology with potential to offer a wide range of benefits to patients, medical personnel and society through continuous monitoring and early detection of possible problems. Security is a fundamental feature for the deployment of wireless body area networks. The deployment of WBANs must satisfy the stringent security and privacy requirements. However, the limitations of body sensors and typical characteristics of WBAN's environment make the design of security procedures complicated. The general security approaches are not applicable for WBANs. A suitable security mechanism in WBANs should be lightweight and inexpensive in term of resource consumption. Data security and privacy in WBANs and WBAN-related e-healthcare systems is an important area, and there still remain a number of considerable challenges to overcome. The research in this area is still in its infancy now, but we believe it will draw an enormous amount of interest in the coming years.

REFERENCES

[1] F.K. Shaikh et al. (Eds.), "Medical Body Area Network, Architectural Design and Challenges: A Survey", WSN4DC 2013, CCIS 366, pp. 60–72, Springer-Verlag Berlin Heidelberg 2013

[2] Ming Li and Wenjing Lou, "Data security and privacy in wireless body area networks", IEEE Wireless Communications • February 2010

[3] Li, M., et al.: Data security and privacy in wireless body area networks. Wireless Commun. 17, 51–58 (2010)

[4] Raazi, S.M.K.-U.-R., et al.: BARI+: A Biometric Based Distributed Key Management Approach for Wireless Body Area Networks. Sensors 10, 3911–3933 (2010)

[5] Raazi, U.R., et al.: A Survey on Key Management Strategies for Different Applications of Wireless Sensor Networks. JCSE 4, 23–51 (2010)

[6] Karlof, C.: Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures. Elsevier's AdHoc Networks Journal, Special Issue on Sensor Network Applications and Protocols, 293–315 (2003)

[7] Karlof, C., Sastry, N.,&Wagner, D. (2004). TinySec: A link layer security architecture for wireless sensor networks. In Proceedings of the 2nd international conference on embedded networked sensor system (pp. 162–175). New York, USA: ACM.

[8] Luk, M.,Mezzour, G., Perrig, A., & Gligor, V. (2007).MiniSec: A secure sensor network communication architecture. In Proceedings of 6th international conference on information processing in sensor networks (pp. 479–488). Cambridge, England: IEEE.

[9] Perrig, A., Canetti, R., Tygar, J.-D., & Song, D. (2002). The TESLA broadcast authentication protocol. UC Berkeley and IBM Research, 5(2), 2–13.

[10] AlMheiri, S. M.,&AlQamzi, H. S. (2013). Data link layer security protocols in wireless sensor networks: A survey. In Proceedings of 10th IEEE international conference on networking, sensing and control (pp. 312–317). Evry, France: IEEE.

[11] Ullah, F., Ahmad, M., Habib, M., & Muhammad, J. (2011). Analysis of security protocols for wireless sensor networks. In Proceedings of 3rd international conference on computer research and development (pp. 383–387). Shanghai, China: IEEE.

[12] Chuchaisri, P., & Newman, R. (2012). Fast response PKC-based broadcast authentication in wireless sensor networks. Mobile Networks & Applications, 17(4), 508–525.

[13] Goldwasser, S., Micali, S.,&Rackoff, C. (1989). The knowledge complexity of interactive proof-systems. SIAM Journal on Computing, 18, 186–208. doi:10.1137/0218012.

[14] Feige, U., Fiat, A., & Shamir, A. (1987). Zero-knowledge proofs of identity. In Proceedings of 19th annual ACM symposium on the theory of computing (pp. 210–217). New York, USA: ACM.

[15] Udgata, S., Mubeen, A.,&Sabat, S. (2011).Wireless sensor network security model using zero knowledge protocol. In Proceedings of 2011 IEEE international conference on communications (ICC) (pp. 1–5). Kyoto, Japan: IEEE

[16] Meingast, M., Roosta, T., Sastry, S.: Security and Privacy Issues with Health Care Information Technology. In: The Proceedings of the 28th IEEE EMBS Annual International Conference (2006)

[17] Saleem, S., et al.: On the Security Issues in Wireless Body Area Networks. International Journal of Digital Content Technology and its Applications 3, 178–184 (2009)

[18] Balasubramanyn, V. B., Thamilarasu, G., & Sridhar, R. (2007). Security solution for data integrity inwireless biosensor networks. In 27th International conference on distributed computing systems workshops. ICDCSW '07, Toronto, Ontario, June 2007, pp. 79–79.

[19] Kurschl, W., Beer, W.: Combining cloud computing and wireless sensor networks. Presented at the Proceedings of the 11th International Conference on Information Integration and Web-based Applications & Services, Kuala Lumpur, Malaysia (2009)

[20] Singele´e, D., Latre´, B., Braem, B., De Soete, M., De Cleyn, P., & Preneel, B. et al. (2008). A secure cross-layer protocol for multi hop wireless body area networks. In 7th International conference on ad-hoc networks & wireless (ADHOCNOW 2008), Vol. LNCS 5198, France, Sep 11–13, 2008, pp. 94–107.

[21] Guennoun, M., Zandi, M., & El-Khatib, K. (2008). On the use of biometrics to secure wireless biosensor networks. In 3rd International conference on information and communication technologies: Fromtheory to applications. ICTTA 2008,Damascus, Apr 2008, pp. 1–5.

[22] Bao, S.-D., Poon, C. C. Y., Zhang, Y.-T., & Shen, L.-F. (2008). Using the timing information of heartbeats as an entity identifier to secure body sensor network. IEEE Transactions on Information Technology in Biomedicine, 12(6), 772–779.