2016 IEEE 41st Conference on Local Computer Networks Workshops

Simulation Framework for a Security Protocol for Wireless Body Sensor Networks

Hussam Al-Hamadi, Amjad Gawanmeh and Mahmoud Al-Qutayri
Department of Electrical and Computer Engineering
Khalifa University, UAE
Email:{hussam.alhamadi, amjad.gawanmeh, mqutayri}@kustar.ac.ae

***Abstract*—The implementation of security protocols within Wireless Body Sensor Network (WBSN) creates chances for more observations in the sake of performance evaluation. The robustness of such protocols can be verified by formalizing its components using different techniques. In addition, simulating the security protocol can provide an insight into several design parameters, such as response to inputs, and help adjusting these design parameters. In this paper, we provide a framework for simulating security protocols within WBSN in order to validate that such protocol meets essential security requirements. Afterwards, we apply it on a security protocol that relies on ElectroCardioGram signal. During the work on this paper, it has been proven that the simulation framework provides the user with the potential to analyze the security aspects of Wireless Body Sensor network applications, such as ElectroCardioGram bio-sensor**

I. Introduction

Wireless Body Sensor Network (WBSN) is a promising technology for our modern lives where communication technology helps us to report our health status to the medical specialists much faster than any time before. However, the reliability and security risks associated with this technology is increasing due to the possibility of capturing sensitive information via WBSN channels and inappropriate design procedures [1]. Securing these channels is a key aspect for trusting the proposed technologies and services. This is crucial as the information processed by such systems impacts people's lives and privacy. For instance, a team of security researchers was successfully able to remotely control a pacemaker by re-instructing, shutting down, or delivering jolts to patient's body [2].

The WBSN applications must meet a lot of mandatory security requirements of healthcare and its legal directives [3], [4]. Ensuring security and privacy in WBSN is the most important requirements. Based on that, the medical sensor data for an ordinary user might be required by some parties for different reason like database or statistical analysis. An adversary may obtain those user data and sells them to who may be interested. For instance, health information of celebrities may be sold or made public in order to hurt him/her. This will invariably affect the concerned person life, career and even the company that he/she works for.

Any proposed security protocol for WBSN should provide proper and effective network access and information transmission, as well as lightweight processes to complete the security protocol steps. The most needed security requirements to solve the security and privacy issues on WBSN are the following:

- Authentication: The assurance to an entity in the WBSN that another entity in the network is who it claims to be.
- Integrity: The assurance to an entity in the WBSN that the received information has not been modified by an unauthorized user or any malicious software.
- Confidentiality: It is very important to protect the transmitted data in the wireless communication channel, where the wireless channel is threatened by an adversary through eavesdropping attacks.

Testing and verifying these security requirements can be handled by several formal techniques, where the predicates and reasoning take place. However, testing the functionality of WBSN based cryptography protocol is not enough. As there are several practical challenging factors may provide other opinions for the adopted security protocol:

- Message size: a good security protocol should takes into account the overload on the message size of the biosensor. Barring in mind, the security protocol requires the biosensor to send some information-related to security within the sequential messages.
- Computational capability: Nowadays, there are high security protocols which require complex mathematical operations and storage. Because of the limited storage and the requirement of low energy consumption of biosensor, WBSN designers prefer lightweight security algorithm to increase the life time of their system.
- Minimum delay: the criteria in WBSN security protocols is to not affect the speed of processing and transmission of vital signs in real-time.

This paper proposes a simulation framework that can demonstrate a security protocol in a WBSN. We are going to adopt the main security requirements by developing a lightweight security protocol and measure the performance of the developed protocol on the WBSN using *Matlab*.

The rest of this paper is structured as follows. In Section II, we present some of the related work on security requirements and which techniques are adopted to verify their security protocol. In Section III, we describe the architecture of WBSN and ElectroCardioGram (ECG) biosensor nodes and our proposed solution in term of security protocol. In Section IV, we provide the proposed simulation framework and experimental

DOI 10.1109/LCNW.2016.33

analysis of the system performance on the proposed protocol. Finally, we make some conclusions in Section V.

II. Related Work

Many authors, such as [5], [6], [7], [8], suggested the deployment of security protocols to provide secure communication between the gateway and server with minimum overhead on the sensors. While, in [9] and [10] the focus is on securing the communication between sensor nodes. Those designs are not practical due to the limited physical resources and processing capability of bio-medical sensors which is a part of the WBSN topology. Besides securing the communications, several researchers proposed techniques to reduce the security overhead on the sensor side. The authors in [11] proposed the use of agent technology as an application inside the gateway to perform security computation on behalf of the sensor node. The computation processes may include authentication (username and password), access control (permission), XML encryption and signature. Whereas, this approach may be applicable to some types of WSNs, it produces some delay which is not suitable for real-time applications, like ECG monitoring.

In security domain, the authors in [12] utilized the formal model to measure the trust metric of U-healthcare systems' entities and their relationship using a model that consists of three layers; trust engine, security manager and security analyzer. In [13], the authors proposed and implemented a secure, adapted triple-key scheme (aTKS) for the WBSN to achieve the privacy and integrity of monitored data with minimal overheads. Their proposed security protocol includes public and private keys, timestamps and hash values which consume bio-sensor resources. Majidi *et al.* [14] highlighted the energy requirement as a central concern in the deployment of cryptographic techniques in WBSNs. They considered the application requirements and the WBSN constraints to identify the most suitable key management technique amongst the available techniques for the purpose of securing data. They built their comparisons based on minimum energy costs. Their experiments prove the high overhead of using RSA and low overhead of the Elliptic Curve Cryptography (ECC) and Advanced Encryption Standard (AES). They prepared the sensing nodes to send packets of encrypted and signed payload. However, specific hardware requirements are necessary to implement the proposed security techniques.

Saleem *et al.* [15], [16] proposed a Machine to Machine (M2M), a Low Cost and Secure (LCS) communication system for the e-Healthcare society. To ensure data privacy, the mechanism involves intelligent authentication based on random distributive key management, electronic certificate distribution, and modified realm Kerberos. Chen *et al.* [17] proposed an event-aided packet forwarding (EPF) protocol, which enables patients to efficiently communicate with each other in privacy-preserving Mobile Healthcare Social Networks (MHSNs). Their EPF protocol adopts predicate encryption to guarantee patient privacy and message confidentiality. Liang *et al.* [18] proposed a privacy-preserving emergency call (PEC) scheme via WBSN. Moreover, their PEC can withstand multiple types of attacks, such as identity theft, forgery, and collusion. However, in their design, they did not consider how to secure the physiological information between the body sensors and the gateway. Similarly, Rongxing *et al.* [19] proposed a secure and privacy-preserving opportunistic computing framework, called SPOC, for a m-Healthcare emergency. Their security analysis shows that the proposed SPOC framework can efficiently achieve user-centric privacy access control in m-Healthcare emergencies. Sasikanth *et al.* [20], who highlighted the necessity for privacy for any personal monitoring technology, developed a conceptual privacy framework for mHealth. They itemized the privacy properties needed in mHealth systems, and discussed the technologies that could support privacy-sensitive mHealth systems. Table I is showing a comparison between previous works with respect to the main security requirements; Authentication, confidentiality and integrity, in addition to privacy and availability.

TABLE I: Security requirements addressed in healthcare systems

Ref	Security Requirements				
	Authentic.	Confid.	Integrity	Privacy	Availability
[15] [16]				√	
[17]		√	√	√	
[14]	√	√	√		
[13]	√	√	√		
[18]	√			√	√
[19]	√	√		√	
[20]	√	√		√	

From previous works, we can notice little considerations on the involvement of the sensors in the security protocols. This is because there is high computation required at the sensor level to accomplish this involvement. Previously the authors of this work [21], [22] presented a method for the verification an ECG biosensor controller within WBSN, as well as formalizing ECG signal components [23], [24]. The authors also presented automatic test case generation for ECG [25] based on formal specification requirements presented in [26]. Therefore, the objective of this work is to extend previous work on ECG biosensor analysis and develop a protocol that ensure the secrecy of the transmitted information within the WBSN entities, and then introduce a simulation framework to demonstrate its efficiency and functionality when used within practical applications such as medical biosensors.

III. Securing WBSN Entities

A WBSN is a network that consists of wearable or implantable wireless biosensors which enables long-term and real-time connection with patient's body through nearby gateway to the server of the healthcare management. As shown in Figure 1 a WBSN is a multiple star topologies including biosensors, gateways and servers where the server is the parent of each star topology and the connection between them expand the area of the WBSN. We assume that each biosensor does not have to communicate with its neighbor nodes, whereas the gateway can handle its group of biosensor and can forward the information to the server. The biosensors collect several vital signs parameters (e.g.; ECG and blood pressure) or activity (e.g.; walking, running, and sleeping), or environmental (e.g., temperature, humidity, and location) from the patient's body and its either processing or forward them to their gateway for advance process. Furthermore, the gateway forwards the processed information to the medical server, which decides the appropriate medical intervention based on the received information and the patient's condition

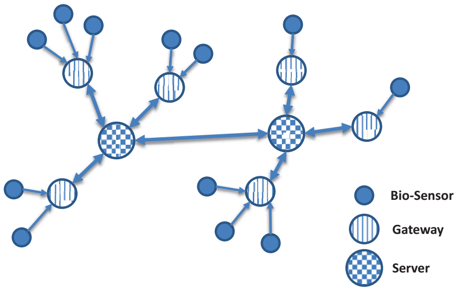


Fig. 1: WBSN Entities and their Topology

In this paper, we describe the Pan-Tompkins [27] which is known to have a higher accuracy for various beat morphologies than other traditional real-time methods. The Pan-Tompkins algorithm includes various types of filters that have been integrated within biosensors to process the ECG signals. The algorithm takes an ECG signals as input and detects *QRS* waves after applying low level signal processing operations, including Band Pass filtering, differentiation, squaring, and windowing. Figure 2 illustrates the steps followed by the algorithm in order to detect *QRS* waves.

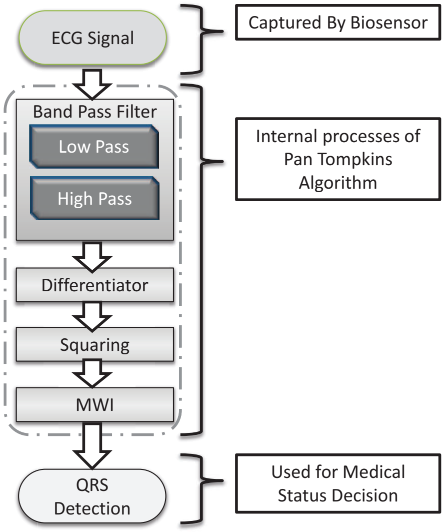


Fig. 2: QRS wave detection using the Pan Tompkins algorithm

The Band Pass Filter consists of low pass and high passes Infinite Impulse Response (IIR) filters. The derivative is the process that follows the band pass filtering and provides information on the slope of the *QRS* wave. Squaring process, amplifies and transfers the output of the derivation into a positive signal point by point, and hence provides better threshold for detecting the *QRS* wave as compared to other waves within the same signal. The Moving Window Integration (MWI) facilitates the analysis process by exposing the *QRS*. This is done by averaging a certain number of samples per window. The MWI is necessary for calculating fundamental ECG signal attributes, such as *R* peak, *RR* interval, *QRS* width, and heart rate ratio. These parameters are used in the sensor analysis algorithms in order to identify any abnormal ECG signals that reflect abnormal hear behavior.

With respect to WBSN security goals, there are two required stages to have a complete protocol implementation. The first stage handles the key exchange process between the WBSN entities. Most proposed protocols at this stage are relied on Trusted Third Party (TTP) to deliver the session keys among the entities evolved on WBSN. In this paper, we suppose the TTP completed its task and exchange the session keys, thus the second stage is on and ready to use the received keys during the security protocol strategic. Developing security protocols require a solid strategic in order to prevent the adversary from breaking it and impersonate specific entity or reach sensitive information. Therefore, we propose a security protocol for the second stage of the WBSN security and evolve all the main components of WBSN to participate in securing the information. Figure 3 shows the content of the messages between the WBSN entities in order to fulfill our proposed security protocol. The notations used throughout this protocol are listed in Table II in the Appendix.

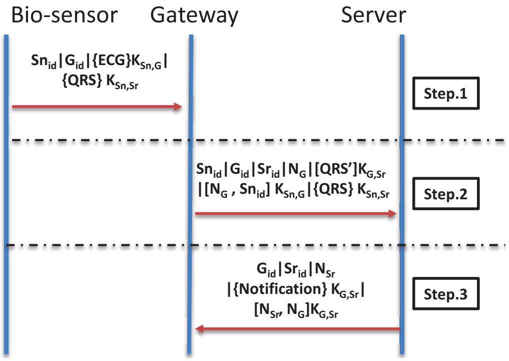

Bio-sensor
Gateway
Server
$Sn_{id}|G_{id}|\{ECG\}K_{Sn,G}|$ $\{QRS\}\ K_{Sn,Sr}$
Step.1
$Sn_{id}|G_{id}|Sr_{id}|N_{G}|[QRS']K_{G,Sr}$ $|[N_{G}, Sn_{id}]\ K_{Sn,G}|\{QRS\}\ K_{Sn,Sr}$
Step.2
$G_{id}|Sr_{id}|N_{Sr}$ $|\{Notification\}\ K_{G,Sr}|$ $[N_{Sr}, N_{G}]K_{G,Sr}$
Step.3

Fig. 3: The Security Protocol Between the WBSN Entities

As we can see, our proposed security protocol allows biosensor nodes to be involved in securing the ECG and its algorithm's output (QRS) even though the distance between the biosensor and gateway is respectively short. Unlike most of the previous security protocols who avoid the over consumption the sensor power by security computations. In our protocol, we substitute several security tools like generating nonce, hashing value generation with ECG signs. We apply this substitution technique on the biosensor side, thus it used what it is already have (ECG and QRS) and does not need to adopt any of the previous security tools. We can describe the process of our protocol by the following steps:

Step.1:This step occurs between biosensor and gateway, where the biosensor captures the ECG signs and processing it using the Pan Tompkins algorithm to detect the QRS on a form of waveform. Then, the biosensor encrypts the ECG with the session key between the biosensor and gateway $K_{Sn,G}$. While the QRS is encrypted by the session key between the biosensor and the server $K_{Sn,Sr}$. Once the gateway receives the message, it can only decrypt its part of the message using the key $K_{Sn,G}$. The gateway processes the received ECG using the Pan Tompkins algorithm to detect the QRS'. Obviously, if everything went right, the QRS' value is equivalent to encrypted QRS value by the $K_{Sn,Sr}$.

Step.2:The gateway encrypts the QRS' by the shared key with the server called $K_{G,Sr}$. It also generates a new nonce (N_G) and hashes it with the biosensor ID using the shared key with the biosensor ($K_{Sn,G}$). Then, the gateway composes the message as seen in Figure 3 and sends it to the server. Once the server received the message, it has the session keys $K_{Sn,Sr}$ and $K_{G,Sr}$ which will be used to decrypt QRS and QRS', respectively. The server then will check the equivalent of QRS and QRS', if they are not similar, the server will drop the message. Otherwise, the server can give more complex analysis on the medical condition.

Step.3:The decision made by the server is considered the notification message for the patient who will use the gateway interface to read it. The notification message will be encrypted using session key $K_{G,Sr}$ in order the specified gateway is the only one responsible to decrypt it. The server also generate its nonce value N_{Sr} and hash it with the gateway's nonce N_G using $K_{G,Sr}$. Once the gateway receives the message, it decrypts the notification and checks its integrity by the challenge the received hash value. If every went right, the gateway display the notification to the patient.

Based on our proposed security protocol, the vital sign of ECG and the output of the Pan Tompkins (QRS) are transmitted securely at all steps. This provides confidentiality of the medical information. In addition, using the session keys which can only been used for each pair at a time, are ensuring the identity of the sender and thus provide the authentication requirements. Nonce and hash value on the other hand provide the freshness and integrity of the messages which is important for real-time systems.

IV. Simulation Framework

In this section, we present our simulation framework that used for modeling the processes of WBSN along with the security protocol steps. In our implementation of the protocol, the ECG biosensor model holds two keys (128 bits) for AES encryption from TTP. The same way is for gateway and server models in order to use them for encryption and decryption processes. We adopt the Cipher Block Chaining (CBC)-mode from the AES-modes list, as it provides more security than ECB and less complication than CFB and OFB modes. The ECG biosensor model has only to generate an Initialization Vector (IV) of 16 bits to complete the CBC-mode procedure. We also equipped the gateway and server sides with the HMAC function and the nonce generation. The Figure 4 shows the adopted simulation framework in *Matlab*, whereas each model is working in series with the others. However, the TTP is not been implemented, instead we run its operation over the biosensor, gateway and server model in order to have the session keys in the work-space.

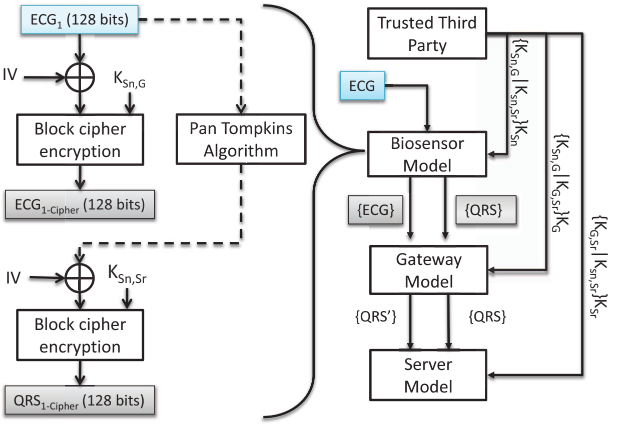
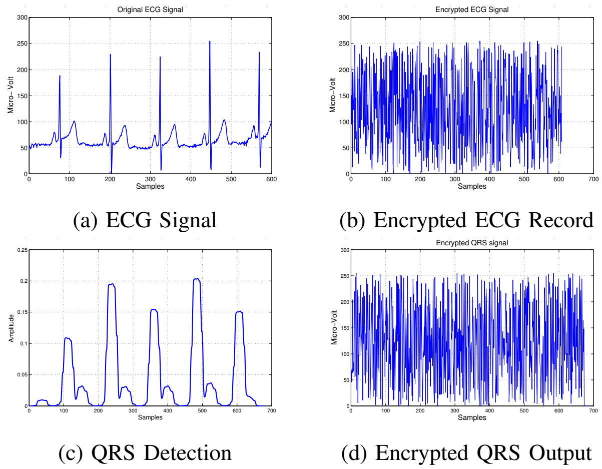


Fig. 4: Simulation Framework for WBSN

In this experiment, we utilize a real ECG record to be our input which has been taken from the well-known open source database of MIT-BIH [28]. We select a 4 seconds ECG record which can be seen in Figure 5a and encrypt it to generate the seen signal in Figure 5b. The protocol waits for the Pan Tompkins to detect the corresponding 16 bytes of QRS wave which shows in Figure 5c, and then encrypts it (Figure 5d).

The encryption results of ECG and QRS are stored in the Maltab work-space, in order to be used for the rest of WBSN models. In the next step, we run the gateway model, which has the ability to decrypt the encrypted ECG only by the stored session key. The gateway then processes the decrypted ECG and detect the QRS' in order to encrypt it. As a result, the server model has two encrypted QRS; one is by biosenosr and another is by the gateway. Running the server model will decrypt those two QRS and using simple *Matlab* function a comparison between the two decrypted QRS would test the authentication of sender and integrity of the information.



(a) ECG Signal

(b) Encrypted ECG Record

(c) QRS Detection

(d) Encrypted QRS Output

Fig. 5: Plot of Encryption Result

Through our implementation, we can measure the payload size of the sensor message. For each 16 bytes from the ECG, the protocol produces 32 bytes divided between 16 bytes encrypted from the ECG and 16 bytes encrypted from the QRS detection. Assuming the sensor and gateway IDs consist of 4 bytes for each, the total payload would be 40 bytes from the maximum payload (127 bytes). We also measured the total consumed time for encrypting the ECG and QRS in addition to generating the QRS at the sensor side for the 4 second ECG. As a result, we found that the absolute time was 0.7s. We did increase the ECG duration by 4 seconds for a number of times and the consumed time by the protocol shows that it can produce the cipher text before the next block is ready to be processed as can been seen in Figure 6.

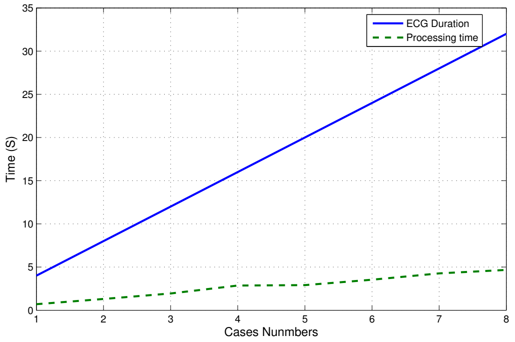


Fig. 6: Consumed time for number of cases on the sensor's side

V. Conclusion

This paper presents a security protocol that provides the main three security requirements; Authentication, Confidentiality and Integrity. In addition, a simulation framework that can be used to validate such requirements is presented. The proposed protocol utilizes the ECG and the output of the Pan Tompkins to replace the nonce and hash on the bio-sensor side of WBSN. The designation of the proposed protocol has been successfully demonstrated using a proposed simulation framework for WBSN entities. This simulation results show the protocol suitability in term of message payload, and efficiency, as it can handle the real-time bio-sensor algorithm (Pan Tompkins) without introducing any delay. As future work, we are going to adopt on of the model checking tools to test the functionality of the proposed security protocol.

References

[1] A. Gawanmeh, H. Al-Hamadi, M. Al-Qutayri, S.-K. Chin, and K. Saleem, "Reliability analysis of healthcare information systems: State of the art and future directions," in *IEEE International Conference on e-Health Networking, Applications and Services*. IEEE, 2015, pp. 68–74.

[2] B. J. Feder, "A heart device is found vulnerable to hacker attacks," *The New York Times*, Mar. 2008.

[3] Health information privacy | HHS.gov. [Online]. Available: http://www.hhs.gov/hipaa/index.html

[4] EUR-lex - 31995l0046 - EN. [Online]. Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[5] H. Lu, J. Li, and M. Guizani, "Secure and efficient data transmission for cluster-based wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 750–761, 2014.

[6] D. He, S. Chan, M. Guizani, H. Yang, and B. Zhou, "Secure and distributed data discovery and dissemination in wireless sensor networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 4, pp. 1129–1139, 2015.

[7] C.-T. Hsueh, C.-Y. Wen, and Y.-C. Ouyang, "A secure scheme against power exhausting attacks in hierarchical wireless sensor networks," *IEEE Sensors Journal*, vol. 15, no. 6, pp. 3590–3602, 2015.

[8] V. Kafle, Y. Fukushima, and H. Harai, "Design and implementation of dynamic mobile sensor network platform," *IEEE Communications Magazine*, vol. 53, no. 3, pp. 48–57, 2015.

[9] D. He, S. Chan, and M. Guizani, "Small data dissemination for wireless sensor networks: The security aspect," *IEEE Wireless Communications*, vol. 21, no. 3, pp. 110–116, 2014.

[10] F. Gandino, B. Montrucchio, and M. Rebaudengo, "Key management for static wireless sensor networks with node adding," *IEEE Transactions on Industrial Informatics*, vol. 10, no. 2, pp. 1133–1143, 2014.

[11] L. Guo, J. Wu, Z. Xia, and J. Li, "Proposed security mechanism for XMPP-based communications of ISO/IEC/IEEE 21451 sensor networks," *IEEE Sensors Journal*, vol. 15, no. 5, pp. 2577–2586, 2015.

[12] C. Subramaniam, A. Ravi, A. Nayak, and S. Thunuguntla, "Actor based domain specific privacy model for U-healthcare system," in *Int. Conf. on Digital Content, Multimedia Technology and its Applications*, 2010, pp. 381–385.

[13] V. Balasubramanian, D. Hoang, and T. Zia, "Addressing the confidentiality and integrity of assistive care loop framework using wireless sensor networks," in *Int. Conf. on Systems Engineering*, 2011, pp. 416–421.

[14] M. Majidi, R. Mobarhan, A. Hardoroudi, A. H-Ismail, and A. Parchinaki, "Energy cost analyses of key management techniques for secure patient monitoring in WSN," in *IEEE Open Systems*, 2011, pp. 111–115.

[15] K. Saleem, A. Derhab, J. Al-Muhtadi, and B. Shahzad, "Human-oriented design of secure machine-to-machine communication system for e-healthcare society," *Computers in Human Behavior*, 2014.

[16] K. Saleem, A. Derhab, and J. Al-Muhtadi, "Low delay and secure m2m communication mechanism for ehealthcare," in *e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on*. IEEE, 2014, pp. 105–110.

[17] L. Chen, Z. Cao, R. Lu, X. Liang, and X. Shen, "EPF: an eventaided packet forwarding protocol for privacy preserving mobile healthcare social networks," in *Global Communications Conference*, 2011, pp. 1–5.

[18] X. Liang, R. Lu, L. Chen, X. Lin, and X. Shen, "PEC: a privacy-preserving emergency call scheme for mobile healthcare social networks," *Journal of Communications and Networks*, vol. 13, no. 2, pp. 102–112, 2011.

[19] R. Lu, X. Lin, and X. Shen, "SPOC: a secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 3, pp. 614–624, 2013.

[20] S. Avancha, A. Baxi, and D. Kotz, "Privacy in mobile technology for personal healthcare," *ACM Computing Surveys*, 2009.

[21] H. Al-Hamadi, A. Gawanmeh, and M. Al-Qutayri, "A verification methodology for a wireless body sensor network functionality," in *IEEE-Biomedical and Health Informatics*. IEEE, June 2014, pp. 635–639.

[22] H. Al-Hamadi, A. Gawanmeh, and M. Al-Qutayri, "Theorem proving verification of privacy in WBSN for healthcare systems," in *Int. Conf. on Electronics, Circuits, and Systems*. IEEE, 2013, pp. 100–101.

[23] H. Al-Hamadi, A. Gawanmeh, and M. Al-Qutayri, "Formal validation of QRS wave within ECG," in *IEEE Int. Conf. on Information and Communication Technology Research*. IEEE, May 2015, pp. 190–193.

[24] H. Al-Hamadi, A. Gawanmeh, and M. Al-Qutayri, "Formalizing electrocardiogram (ECG) signal behavior in Event-B," in *IEEE Int. Conf. on e-Health Networking, Applications and Services*. IEEE, Oct 2014, pp. 55–60.

[25] H. Al-Hamadi, A. Gawanmeh, and M. Al-Qutayri, "An automatic ecg generator for testing and evaluating ecg sensor algorithms," in *International Design & Test Symposium (IDT)*. IEEE, 2015, pp. 78–83.

[26] A. Gawanmeh, "An axiomatic model for formal specification requirements of ubiquitous healthcare systems," in *IEEE Consumer Communications and Networking Conference*. IEEE, 2013, pp. 898–902.

[27] J. Pan and W. J. Tompkins, "A real-time QRS detection algorithm," *IEEE Transactions on Biomedical Engineering*, vol. BME-32, no. 3, pp. 230–236, March 1985.

[28] A. Goldberger, L. Amaral, L. Glass, J. Hausdorff, P. Ivanov, R. Mark, J. Mietus, G. Moody, C.-K. Peng, and H. Stanley. Physiobank, physiotoolkit, and physionet: Components of a new research resource for complex physiologic signals. Circulation 101(23):e215-e220 [Circulation Electronic Pages; http://circ.ahajournals.org/cgi/content/full/101/23/e215], 2000 (June 13).

Appendix

TABLE II: Security Notation

Notation	Description
X_{id}	The entity's id, where X can be the Bio-sensor or the Gateway or the Server.
$M_1 \| M_2$	Denotes the concatenation of messages M_1 and M_2.
$K_{A,B}$	Denotes the secret session key which is shared between A and B.
$\{M\}_{K_{A,B}}$	Is the encryption of message M with the session key K between A and B.
$[M]_{K_{A,B}}$	Is the MAC (Message Authentication Code) for message M with the session key K between A and B.
N_x	Is a nonce generated by entity X (a nonce is an unpredictable number used once used to achieve freshness).
ECG	The captured vital sign by the sensor.
QRS	The detected QRS by the Sensor algorithm.
QRS'	The detected QRS by the Gateway algorithm.