Lightweight Detection of On-body Sensor Impersonator in Body Area Networks

Liping Xie
*School of Computer
Electronic, and Information,
Guangxi University,
Nanning, Guangxi, China
Email: xie5012@mail.gxu.cn*

Weichao Wang
*Dept. of Software and
Information Systems
UNC Charlotte
Charlotte, NC 28223
Email: wwang22@uncc.edu*

Tuanfa Qin
*School of Computer
Electronic, and Information,
Guangxi University,
Nanning, Guangxi, China
Email: tfqin@gxu.edu.cn*

***Abstract*—In the past few years mobile healthcare has attracted a lot of attention from both industry and academia. Medical sensors are usually attached to or implanted inside patient body. Since sensing results of BAN can directly impact the control of medical equipment, the authenticity and integrity of sensing data is essential for safety of patients. Existing research focuses on differentiating on-body sensors from off-the-body impersonators with the help from a control unit.**

In this paper, we propose to exploit wireless channel characteristics to detect on-body impersonators in BAN networks. Depending on whether or not the sensors have line-of-sight connections with the off-the-body control unit, their communication channels demonstrate different properties. For an attacker who demonstrates similar channel characteristics as the victim, a user-configurable challenge-response mechanism is designed to expose the conflicting information submitted by the two nodes. Our simulation results show that with a small increase in communication and computation overhead, we can effectively detect the on-body impersonators.

***Keywords*-body area network; node impersonation attack; communication channel property**

I. Introduction

Among many application scenarios of Cyber-Physical Systems (CPS), intelligent healthcare is a very promising research direction. Deployment of smart sensors and treatment equipment on patient body will allow both healthcare providers and patients to better monitor the body status and respond more promptly to any changes. Such applications evolve into body area networks (BAN) [1]. A BAN is usually a wireless network formed by lightweight, small-size, ultra-low-power, and intelligent wearable devices. These sensors can be strategically placed on the body surface, around body, or implanted inside body. To reduce physical constraint on patients, the sensors transmit collected information to a control unit (CU), which is usually deployed outside of yet close to the patient.

Since intelligent sensors in BAN monitor vital signs of patients and could suggest or even directly perform medical treatment, the authenticity and integrity of collected information is essential for safety of patients [2], [3]. Unfortunately, restricted by the size of and available power to BAN sensors, it is hard to adopt the cryptography based security mechanisms in BAN. Therefore, researchers refer to physical layer mechanisms to enforce security. For example, in [4], the authors design a mechanism to identify an off-the-body attacker who tries to impersonate an on-body sensor. They observe that there exist distinct received signal strength (RSS) variation patterns between on-body sensors and off-the-body nodes. The CU stays relatively static to the on-body sensor since they move together with the patient. On the contrary, the distance between off-the-body impersonator and the CU will change constantly.

In this paper, we investigate a more challenging problem. Specifically, we want to study whether or not physical channel characteristics can be used to detect node impersonation attacks that are conducted by on-body sensors. Below we describe a scenario. Let us assume that a patient has multiple BAN sensors deployed on her body, as shown in Figure 1. Since the information they monitor and collect has different levels of sensitivity, the nodes adopt different security measures for protection. Therefore, the difficulty levels to compromise them are also different. For example, a wireless thermometer measures body temperature of the patient and sends it to control unit. Since human body temperature is not sensitive data, the thermometer does not adopt very strong protection. At the same time, a BAN sensor monitors the glucose level of the patient and transmits collected data to control unit. The control unit will then adjust the speed of an insulin pump based on the information. Since over injection of insulin could directly threaten the life of the patient, the glucose monitor adopts strong protection and is very hard to compromise. Now assume that an attacker compromises the thermometer and uses it to impersonate the glucose sensor. Since both devices are deployed on the patient body, the mechanisms that are designed to detect off-the-body impersonators will not work effectively. A new mechanism must be designed to defend against such attacks.

To solve this problem, we propose a lightweight detection mechanism. The basic idea is as follows. Based on the measurement results in [5], the wireless channel between an on-body sensor in BAN and the off-the-body control unit exhibits different variations depending on whether or not they have line-of-sight (LOS) communication paths. If there exists a LOS path between them, they experience relatively

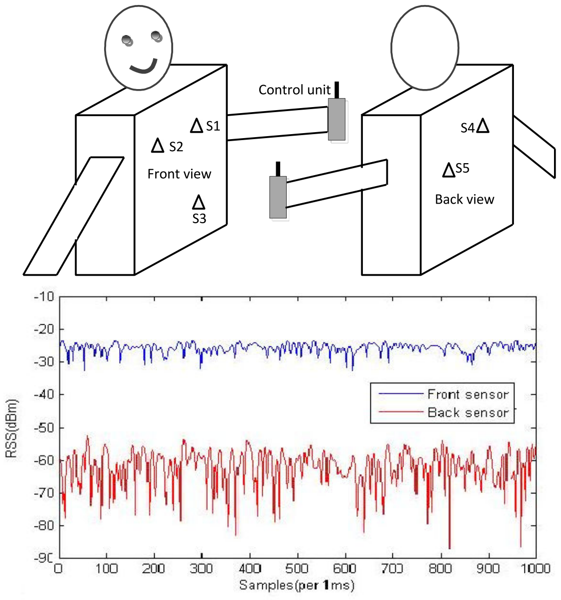

Figure 1. Top: An example BAN setup: CU and 5 sensors. Bottom: Difference between LOS and NLOS channels between BAN sensors and CU.

stable RSS (Received Signal Strength) values with small fluctuations. On the contrary, a non-line-of-sight (NLOS) path will lead to larger variances. Therefore, using the average RSS variations (ARVs), we can classify the channels into two groups: LOS and NLOS. The control unit can measure its channel with a BAN sensor and derive out whether or not there exists a LOS path between them. When a compromised sensor tries to impersonate another node in BAN by sending out false data, the CU will compare the signal pattern of the channel to the expected value. If they do not match, the impersonation attack is detected and the sensed data will be discarded. For two sensors that stay close to each other and demonstrate similar channel patterns to the CU, we propose to adopt a challenge-response procedure for sensing data to cause collisions between the real sensor and the impersonator so that the attack can be detected.

An example is illustrated in Figure 1. The patient carries 5 BAN medical sensors $S1$ to $S5$ on her. Here $S1$, $S2$, and $S3$ are deployed on the front side of her body, while $S4$ and $S5$ are on the back side. We assume that the patient carries a control unit which maintains a relatively stable position to the BAN sensors. In this way, the LOS/NLOS patterns between the CU and the sensors do not change. We use Simulink [6] to simulate the BAN setup described above. Figure 1.Bottom shows the LOS channel between $S1$ and the control unit, and the NLOS channel between $S4$ and CU. If sensor $S4$ tries to impersonate $S1$, the CU can measure the channel ARVs. It can then compare the expected channel pattern to the measured value to detect anomaly.

While the basic idea is straightforward, several issues must be carefully resolved before the approach can be implemented. For example, Figure 1 illustrates only the case when the impersonator has a different channel pattern from that of the victim. What if the victim and the attacker are physically close to each other? For example, sensors $S4$ and $S5$ in Figure 1 are both located in the backside of the patient. As another question, how much overhead will this approach introduce into the system? We will answer these questions in later parts of the paper.

The contributions of the paper are as follows. First, existing channel characteristic based authentication mechanisms for BAN networks focus on differentiating off-the-body impersonators from on-body sensors. Our approach can effectively detect on-body impersonators. Second, this approach does not require the deployment of any additional hardware in the BAN environment. Third, our proposed approach introduces a limited amount of overhead to the BAN sensors. Properties two and three are essential for potential deployment of our approach in resource-constrained BAN networks. Last but not least, we choose a type of abnormal heartbeat, supraventricular ectopic beat (SVEB), as the target of the impersonation attacks. We investigate the detection accuracy and overhead of our approach through simulation.

Related Work:

Since sensor nodes in BAN networks are highly resource constrained, investigators have referred to physical channel properties to achieve security goals. In [7], Ali *et al.* observe that the channel between an on-body sensor and an off-the-body node displays both slow and fast fading components. This property is used to assist key generation between the nodes. In [4], the authors use differences in the average RSS variation between an on-body channel and an off-the-body one to identify BAN sensor and control unit impersonators. The group then push the research one step forward by achieving both device authentication and fast key extraction with the same group of operations in BAN [5].

The remainder of the paper is organized as follows. In Section II we present the details of our approach. Depending on the difference between the average RSS variations (ARVs) of the received signals and expected values, we design two mechanisms to identify the impersonators. In Section III we use fake abnormal heartbeat information to test the detection capability and overhead of our approach. Finally, Section IV concludes the paper.

II. The Proposed Approach

A. System Assumptions

Our BAN network contains n sensors and one control unit (CU). The sensors and the CU use wireless technique to communicate with each other. The sensors are carried on a patient's body so that they can continuously measure her physiological data. When the patient moves, the sensors on her body will also move. Although under some special cases the distances among the sensors may change, we assume that their positions will not change drastically. There is no out-of-band communication channel among the nodes. The sensors are placed at least half wavelength away from each other to avoid correlated wireless channels.

The control unit (CU) is in charge of information collection and aggregation of the BAN. Based on the information processing results, CU could transmit the data to physicians or caregivers. It could also upload the data to some cloud servers so that different persons in need could access it. Similar to [4], we assume that the CU and the sensors stay relatively static during patient movement. We assume that the CU has more resources for protection. Therefore, the CU could not be compromised.

We assume that an attacker will be able to compromise some on-body sensors remotely. Once compromised, the sensor will be under the attacker's control. The attacker will get access to all data/secret keys stored in the sensor. More importantly, the attacker could fully control the wireless communication component of the compromised sensor and send out packets in other nodes' names. This leads to node impersonation attacks. The attacker will not be able to change the physical configuration or position of the node.

B. The Proposed Approach

• Characteristic Difference between LOS and NLOS Channels

In order to reduce extra overhead on the resource constrained nodes in BAN, in this paper we propose to use the characteristics of wireless communication channels to detect impersonators. Previous research shows that although an off-the-body control unit can receive signals from different BAN sensors, depending on whether or not there exists a line-of-sight channel (LOS) between them, the signals could demonstrate different properties. Specifically, experiments in [4], [5] show that for channels between BAN sensors and an off-the-body unit, LOS channels tend to be much more stable than NLOS channels.

This observation can be explained as follows. The propagation procedures of wireless signals are affected by many factors such as direct path loss, multipath, and shadowing. When there exists a LOS path between a sender and a receiver, the direct path becomes the dominant factor. Since the signals received from other paths contribute only a small portion to the overall RSS, the value stays relatively stable. On the contrary, for the NLOS channels, RSS values will experience large fluctuations when we consider the impacts of human tissues and device placement. Figure 1 illustrates the difference between a LOS and an NLOS channel. This figure shows that it is feasible to detect an on-body impersonator through the physical channel properties.

• System Bootstrap

When a BAN network first boots up, the on-body sensors will try to establish connections with the control unit. Since an attacker could not predict at what time the BAN will boot up, we assume that for a short period of time after system bootstrap the sensors are secure. Using this period of time, the control unit could collect the channel properties to the sensors. Please note that similar assumptions can be made when we add some new sensors into a BAN. Through this procedure, the CU can determine whether or not it has a LOS channel to a sensor.

• Detection of Impersonator Who Has Different Channel Signatures from the Victim

If an attacker tries to impersonate another BAN sensor that has different channel properties with the control unit, the CU can easily detect the anomaly. As an example, assuming that sensor $S3$ in Figure 1 has been compromised and tries to impersonate sensor $S4$. Since $S3$ is on the front side of the patient while $S4$ is on her back, their channel properties with the control unit will be quite different. When the CU detects that the RSS variations of the packet do not match to the expected values of the claimed node ID, it will discard the packet and raise the alarm of an impersonation attack.

• Detection of Impersonator Who Has Similar Channel Signatures with the Victim

Under some conditions, the compromised BAN sensor may be physically close to the victim. Therefore, their channel signatures to the control unit are similar. For this type of attack, we need a new detection mechanism.

Before presenting the details of our detection mechanism, let us re-consider the attack scenario. Here the impersonator tries to provide contaminated data to control unit in a stealth way. Therefore, our goal is to detect the existence of such attacks, not necessarily to identify the compromised nodes. If we detect that some impersonator sends out false data in the victim's name, subsequent operations such as remote software based attestation [8] could be adopted to verify system integrity and identify attackers.

With this observation, we propose the following probability based detection mechanism. Our mechanism is built upon the advances in wake-up receivers (WUR) in BAN networks with ultra low power consumption. A low power wake-up receiver (WUR) module monitors a given channel continuously. When the CU wishes to communicate with a BAN sensor, it first sends out a wake-up call. After successful reception of the wake-up call, the WUR unit uses a signal to fire up its primary radio to engage in high-speed communication with the CU. After the transmission, the sensor reactivates its WUR unit and goes back to sleep.

Below we design an impersonator detection mechanism based on this technique. When the control unit receives a data packet from a BAN sensor, it will first examine the channel signature and data content of the packet. If it feels that additional verification is needed, the following steps can be adopted. It will send out a wake-up signal with a random number r_M to the WUR unit associated with the

BAN sensor that we try to verify. There are two possible results of this operation. If the data packet was sent by the real sensor, it should be still awaken. On the contrary, if the packet is actually sent by the impersonator, this signal will wake up the victim. The control unit will then ask the sensor to calculate a keyed hash result $hash(r_M$, msg, $r_M)$ based on the random number r_M and the data packet msg that it just sends out. If the packet is really from the sensor, it can successfully accomplish the task. On the contrary, if the packet is from the impersonator, the sensor will send out a different hash result based on its previous packet, or report an error stating that it has not sent out any packet recently. Either way, this report will trigger the alarm of a node impersonation attack.

Combining the mechanisms described above, we can see that if the attacker and the victim have different channel signatures, the control unit can directly detect the attack. If the two channels are very similar, the control unit can adopt a probability based challenge-response mechanism to detect false data. The relationship between the percentage of packets that are challenged and the attack detection probability will be studied in subsequent sections.

- **Increases in Power Consumption**

The proposed mechanism will incur extra computation and communication overhead on the BAN sensor. Therefore, we must carefully assess the tradeoff between detection capability and increases in overhead. The increased power consumption comes from the following aspects. First, the WUR unit needs to be active almost all the time. Fortunately, based on [9], the WUR has μA operating current versus mA for traditional radios. Therefore, the impacts of this increase can be ignored.

Another increase comes from the reception, computation, and reply of the challenge. Here we compare the proposed approach to two mechanisms. The base line mechanism adopts no security measures. Therefore, an impersonator can supply any data to the control unit. Using the measurement results in [10], [11], we can estimate that the sensor will consume about 82 μJ energy to transmit a 64-byte packet to the CU. This is the base line power consumption.

In the second mechanism to which we plan to compare, we assume that the CU shares a different secret key with each BAN sensor. Under this condition, a Message Authentication Code (MAC) that is calculated based on the data contents and the shared key is attached to every packet. In this way, data integrity is protected and node impersonation attack becomes impossible. However, the cost is a sharp increase in power consumption. If a 16-byte MAC code is attached to every data packet sent by the BAN sensor, the power consumption will increase about 90% (156 μJ).

Using the proposed approach, if a round of challenge-response is triggered for a data packet, the total power consumption will be about 223 μJ, which is about 2.7 times of the base line. Fortunately, several schemes can help to reduce the probability that the extra round of communication is executed. First, if the channel signatures of the victim and the impersonator are different, the attack can be detected without any extra overhead. Second, for the cases in which the channel signature demonstrates no anomaly, end users can define some pre-conditions to activate the challenge-response interactions. Several example scenarios may include: (1) the reported data from the sensor deviates from its normal value range, or the change is large enough to cause new operations at the medical equipment; or (2) the channel signature from the sensor has changed drastically compared to its previous value. In this way, we can effectively reduce the frequency of the execution of challenge-response. Our simulation in Section III will show that our approach will cause a small increase in power consumption in an attack-free environment while maintaining a high detection rate when impersonators show up.

- **Security of the Approach**

Since the proposed approach tries to detect node impersonation attacks on BAN, the safety of it must be carefully studied. An attacker may try several schemes to avoid detection by this mechanism or to abuse it. Below we discuss two cases. First, immediately after a real sensor sends out a packet, the impersonator can send out a false packet. Under this condition, the CU will receive two (possibly conflicting) data packets. However, unless the impersonator rebroadcasts the packet from the sensor, the keyed hash values of the two packets will be different, thus revealing the attack. The second attack that a compromised node can conduct is to abuse the challenge-response verification. It will not send out false data packets. On the contrary, if a packet from the real sensor is challenged by the control unit, the attacker will reply with a wrong hash result. Since the control unit will receive two different hash values, it will assume that an impersonation attack is ongoing and discard the original data packet. In this way, a DoS attack is conducted upon the real sensor. However, this type of abuse cannot be repeatedly used. The false hash result exposes that some sensor has been compromised and stopped to follow the protocol. A detection procedure could then be triggered to identify the compromised node.

III. Simulation and Results

A. Simulation Setup

In the simulation study, we choose the classification of heartbeat of patients as the application. According to the Association for the Advancement of Medical Instrumentation, an arrhythmia is any abnormality in the rate, regularity, site of origin, or activation sequence of the electrical impulses of the heart. In this study, we focus on supra ventricular ectopic beat (SVEB). SVEB originates from the atria or from the atrioventricular node. It could be caused by premature activation of the atrium prior to a normal heartbeat, which may indicate heart failure and atrial fibrillation. Figure 2 shows the ECG of a ventricular ectopic beat.

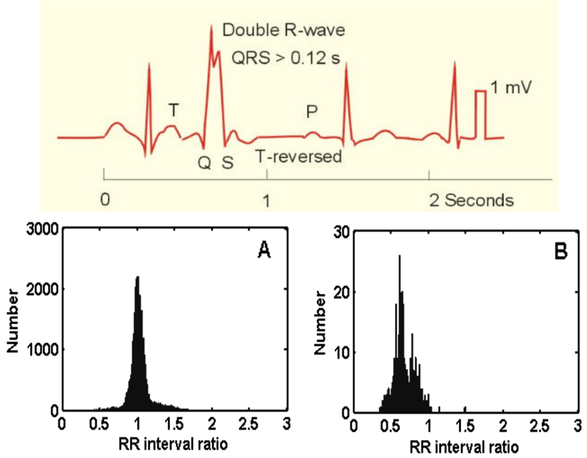

Figure 2. Top: ECG of a ventricular ectopic beat. Bottom: Histograms of normal beats (left) and SVEB RR interval ratios (right). Courtesy of Biomedical Engineering Online Journal and New Human Physiology.

In [12], the authors find out that the ratio of the actual RR interval (the interval between successive R wave fiducial points) to the mean RR interval is a good indicator of SVEB. Please refer to Figure 2.Bottom for the RR interval ratios of a normal heartbeat and a SVEB. In their detection algorithm, if the ratio is smaller than a predetermined threshold (0.8 in their paper), an alarm of SVEB is issued.

Our simulation setup is as follows. A patient has eight BAN sensors attached to her. An electrocardiogram (ECG) is attached to her chest to measure and record the electrical activities of the heart. Other than the ECG, four sensors are attached to her front chest, and three are on her back. An attacker will randomly pick one sensor to compromise so that he can use it to impersonate the ECG. If the compromised sensor is on the back of the patient, our approach will detect the channel anomaly and discard the packet. On the contrary, if the compromised sensor is attached to the front side of the patient, the channel characteristic based scheme will not work. The control unit will examine the data from the sensor. If it detects that a SVEB might be happening now, it will execute the challenge-response based mechanism to double verify the authenticity of the information.

Here we assume that the data reported by the real ECG sensor follows the distribution shown in the left side of bottom of Figure 2. We observe from the figure that with a certain probability, a normal heartbeat may have an RR interval ratio smaller than the threshold value, which will trigger the challenge-response procedure. The attacker's purpose is to inject false SVEB alarms into the system. Therefore, the data it reports follows the distribution shown in the right side of Figure 2.

B. Simulation Results

We are especially interested in two properties of the proposed approach: detection accuracy and increased overhead. Since a real BAN sensor can always pass the challenge-response procedure, the proposed approach will not generate false positives. A false negative may occur when a compromised sensor that is located on the front side of the patient sends out a data entry larger than the pre-determined threshold value. In our simulation, such a data entry will not trigger a SVEB alarm. Therefore, this data entry would be accepted by the control unit.

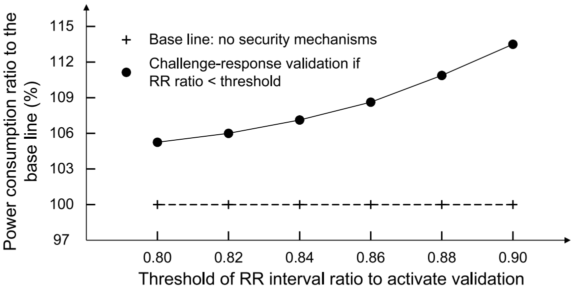

Figure 3. Power consumption at the ECG when there is no attacker in the system.

We conduct two groups of simulation to assess our approach. In the first group of experiment, we setup a base line case. In this experiment, there is no attacker in the system. The CU will monitor the reported RR interval ratios. If the ratio is smaller than the threshold value, it will execute the challenge-response procedure to verify data authenticity. Since in [12] the authors use 0.8 as the threshold value to label a SVEB, in our simulation we experiment with different threshold values ranging from 0.8 to 0.9 to active the verification. We assume that the real ECG sensor sends a data packet with the size of 64 Bytes to the CU. Both the challenge and response during verification have the size of 16 Bytes. The power consumption models of the BAN sensors on data transmission and calculation of the hash function are based on the measurements in [10], [11].

Figure 3 shows the power consumption increase caused by the proposed approach when there is no attacker in the network. The dotted line shows the base line when there is no security mechanism activated. We can see that depending on the selected threshold, the increase in power consumption ranges from 5% to 13%. This is much more efficient than the mechanism to attach a MAC code to every data packet, which will cause an increase of 90%.

In the second group of simulation, we assume that an attacker will randomly choose one BAN sensor attached to the front side of the patient to compromise. He will then use the compromised sensor to impersonate the ECG and send out false data packets. The false data is generated based on the distribution of the SVEB RR interval ratio shown in the right side of bottom of Figure 2. The compromised sensor will keep sending false data with an interval in time until it is detected by the proposed approach. Once detected, the attacker will choose another BAN sensor on the front side of the patient and repeat the malicious activities.

Table I
THE PROBABILITY THAT A FALSE DATA PACKET ACTIVATES THE CHALLENGE-RESPONSE VERIFICATION.

Threshold value	0.80	0.82	0.84	0.86	0.88	0.90
Probability to trigger verification (%)	80	82.7	85.1	87.3	89.6	91.3

Based on the histogram of SVEB RR interval ratios in Figure 2, the probability that a false data entry is smaller than the chosen threshold value is shown in Table I. Figure 4 shows the relationship between the number of false data packets an impersonator can send out and the probability that it is detected. We can see that with the chosen threshold values, almost all impersonators will be caught within three packets.

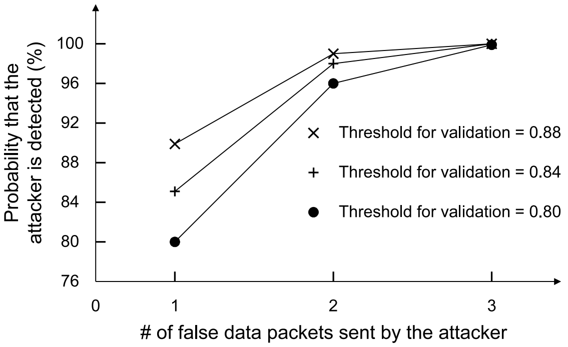

Figure 4. Relationship between the number of false data packets an impersonator sends out and the probability that it is detected.

From the simulation results, we can see that end users can adjust the values of selected parameters to control the tradeoff between detection capability and increases in power consumption. With less than 10% increase in overhead, our approach can capture a fake SVEB message with the probability of 90%. Almost all attackers can be detected within three packets.

IV. CONCLUSION

In this paper we propose an approach that integrates wireless channel characteristics with threshold based challenge-response to detect BAN sensor impersonators that are also attached to the patient body. For an impersonator that demonstrates different channel properties from the victim, its false data will be discarded. For those impersonators that cannot be detected based on this property, a challenge-response verification procedure will force the real sensor and the impersonator to send out conflicting information. The simulation results show that our mechanism can effectively defend against such attacks with a small increase in overhead.

Immediate extensions to our approach consist of the following aspects. First, we plan to implement the proposed approach on real personal medical devices and evaluate its performance in different scenarios. Second, we will continue to investigate the special properties of wireless communication channels in BAN networks and explore other attacks that can be detected based on these properties.

REFERENCES

[1] S. Movassaghi, M. Abolhasan, J. Lipman, D. Smith, and A. Jamalipour, “Wireless body area networks: A survey,” *IEEE Communications Surveys Tutorials*, vol. 16, no. 3, pp. 1658–1686, Third 2014.

[2] D. Halperin and et. al., “Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses,” in *IEEE Sympo. Security and Privacy*, 2008, pp. 129–142.

[3] M. Li, W. Lou, and K. Ren, “Data security and privacy in wireless body area networks,” *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, February 2010.

[4] L. Shi, M. Li, S. Yu, and J. Yuan, “Bana: Body area network authentication exploiting channel characteristics,” *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 9, pp. 1803–1816, September 2013.

[5] L. Shi, J. Yuan, S. Yu, and M. Li, “Mask-ban: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks,” *IEEE Internet of Things Journal*, vol. 2, no. 1, pp. 52–62, Feb 2015.

[6] K. Thotahewa, J. Khan, and M. Yuce, “Power efficient ultra wide band based wireless body area networks with narrowband feedback path,” *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1829–1842, 2014.

[7] S. Ali, V. Sivaraman, and D. Ostry, “Secret key generation rate vs. reconciliation cost using wireless channel characteristics in body area networks,” in *IEEE/IFIP International Conference on Embedded and Ubiquitous Computing (EUC)*, 2010, pp. 644–650.

[8] H. Tan, W. Hu, and S. Jha, “A remote attestation protocol with trusted platform modules (tpms) in wireless sensor networks,” *Security and Communication Networks*, vol. 8, no. 13, pp. 2171–2188, 2015.

[9] M. Prinn, L. Moore, M. Hayes, and B. O’Flynn, “Comparing low power listening techniques with wake up receiver technology,” in *the International Conference on Smart Systems, Devices and Technologies*, 2014, pp. 88–93.

[10] E. Casilari, J. M. Cano-García, and G. Campos-Garrido, “Modeling of current consumption in 802.15.4/zigbee sensor motes,” *Sensors*, vol. 10, no. 6, pp. 5443–5468, 2010.

[11] J. Lee, K. Kapitanova, and S. H. Son, “The price of security in wireless sensor networks,” *Comput. Netw.*, vol. 54, no. 17, pp. 2967–2978, Dec 2010.

[12] H. Huang, J. Liu, Q. Zhu, R. Wang, and G. Hu, “A new hierarchical method for inter-patient heartbeat classification using random projections and rr intervals,” *BioMedical Engineering OnLine*, vol. 13, no. 90, 2014.