# A Sink Node Assisted Lightweight Intrusion Detection Mechanism for WBAN

Xuyang Hou[*‡], Jingjing Wang[*‡], Chunxiao Jiang[†], Sanghai Guan[*‡] and Yong Ren[*]
[*]Department of Electronic Engineering, Tsinghua University, Beijing, 100084, China
[†]Tsinghua Space Center, Tsinghua University, Beijing, 100084, China
[‡]Tsinghua National Laboratory for Information Science and Technology (TNList)
Email: {houxy17, gsh17}@mails.tsinghua.edu.cn, chinaeephd@gmail.com, {jchx, reny}@tsinghua.edu.cn

***Abstract*—Relying on mini wearable or implantable biosensors, the wireless body area network (WBAN) is capable of efficiently collecting as well as of analyzing human physiological information. It has shown great potential in terms of beneficially improving healthcare quality. However, due to stringent resource constraints of biosensors, traditional security schemes, i.e. the encryption and the authentication, may not do well in countering security threats. Moreover, they are not competent in protecting the network from inside attacks and deny of service (DoS) attacks. In this paper, we propose a sink node assisted lightweight intrusion detection mechanism for WBAN, where the sink node can periodically monitor the packet transmission and record the abnormality for further analysis. Our lightweight mechanism results in a very high true positive rate and an ultra-low false positive rate. Extensive analysis and simulations based on Castalia are conducted and verify the validity and efficiency of our proposed mechanism.**

***Index Terms*—WBAN, security threats, intrusion detection.**

## I. Introduction

Recently, the wireless body area network (WBAN) has emerged as a promising technique that may revolutionize the way of healthcare [1]. It is composed of implantable and wearable biosensors, which are responsible for monitoring biologic characteristics, such as temperature, heart rate, blood pressure, electrocardiogram, etc. Fig. 1 shows the typical architecture of a WBAN, where various biosensors are capable of both sensing the human body biologic signs and of forwarding data to the sink nodes. Furthermore, the sink node can analyze data gathered from biosensors, and can transmit pretreatment results to personal servers, such as personal digital assistants (PDAs). Finally, personal servers forward relevant data to the cloud for further feature mining and long-term healthcare monitoring [2].

Since health-related data plays a critical role in medical diagnosis and treatment, inauthentic biologic characteristics may prevent a patient from being treated effectively, or may even lead to a wrong therapeutic approach. Moreover, ethics and legislation also require the confidentiality and security of biologic characteristic data. Hence, security and privacy are the key concerns of WBANs because of the power constraint as well as the defective computation and communication capability of small biosensors, especially of some implantable sensors [3], [4].

In order to address these issues, in the literature, security mechanisms based on symmetric key and public key cryptography have been widely developed [5], [6]. Specifically, Malasri *et al.* in [5] proposed the elliptic-curve cryptography (ECC) algorithm to construct symmetric keys between sensor nodes and the base station. In [6], He *et al.* provided a lightweight system with hash-chain aided key updating mechanism, which was capable of countering powerful mobile attacks and had a high feasibility for real-time application. Given that the human body physiological state was quite random and time-variant, relying on the physiological signals obtained from the patient, Wang *et al.* proposed a biometric encryption technique in order to achieve a mutual authentication, which derived a non-linkable session key between each biosensor and the sink node [7], [8]. Some other mechanisms were also proposed. Specifically, in [9], Thamilarasu *et al.* presented a multi-objective genetic algorithm based intrusion detection system to provide optimal attack detection in WBAN, which modeled the trade-off among detection performance, false positives and resource consumption as a multi-objective genetic algorithm optimization problem. Salem *et al.* in [10] provided an anomaly detection algorithm to detect nodes' abnormal behaviors. However, some of the aforementioned mechanisms are not feasible for resource-constrained nodes in WBANs. Biometric encryptions ignore the fact that these sensor nodes are generally single-function devices which can measure only one physiological parameter for each node, for example. Furthermore, some lightweight cryptography mechanism cannot resist inside attacks and denial of service (DoS) attacks. To prevent a network-wide security breach of WBAN, intrusion detection systems are necessary for exposed malicious nodes.

In this paper, we propose a sink node assisted lightweight intrusion detection mechanism for the WBAN, where the sink node can periodically monitor the packet transmission and record the abnormality for further analysis. Our original contributions are summarized as follows:

- Combining with a range of concrete scenarios in WBAN, we thoroughly analyze the security threats of the WBAN. Moreover, we classify them into two categories based on the counter-measures.
- We propose a sink node aided lightweight intrusion detection mechanism. Our mechanism has a very high true positive rate and an ultra-low false positive rate, which also requires less resource consumption.

978-1-5386-3180-5/18/$31.00 ©2018 IEEE

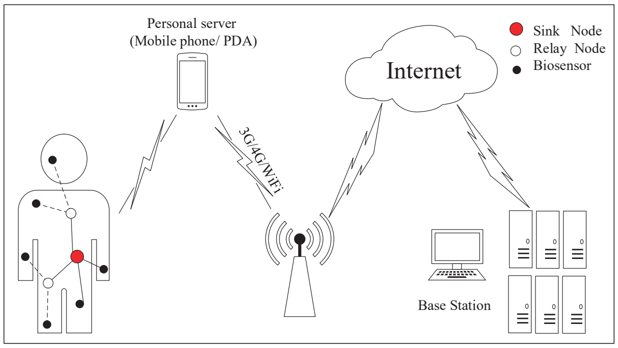


Fig. 1. The architecture of WBAN

- In our simulations, both the path loss and the time-variance characteristic of wireless channel are considered in the context of WBANs, which is more realistic than relying on wireless sensor networks' (WSNs) channel.

The rest of this paper is organized as follows. In Section II, we make a detailed description and classification about the security threats in WBANs. Section III presents our proposed intrusion detection mechanism, followed by simulation results in Section IV. Our conclusions are shown in Section V.

## II. Security Threats in WBAN

Due to the vulnerable nature of the wireless radio, there are various security threats that disturb the reliability as well as the stability of WBAN [11], [12]. The state-of-the-art researches almost transfer the traditional security threats from WSN to WBAN, without considering the difference between them. Specifically, in WSN, the sensor nodes are deployed in public and hostile environment letting them be vulnerable to be captured and physically tampered. By contrast, nodes in WBAN are often implanted in or worn on the human body, which makes it impossible for adversaries to have any physical access. However, malicious nodes are capable of attaching the fake nodes and of masquerading as legitimate nodes to launch attacks.

In this section, first of all, we classify the possible security threats in WBAN into two categories based on their countermeasures. To elaborate a little further, some outside attacks, such as eavesdropping as well as data modification and injection are viewed as the first category, which can be effectively eliminated by *intrusion prevention mechanisms*. The other category includes the replay attack, impersonation attack and the DoS attack, which can be addressed by *intrusion detection mechanisms*. In the following, we provide a brief description of the mentioned-above security threats:

*1) Eavesdropping:* Due to the openness and broadcast nature of wireless mediums, attackers are capable of intercepting the radio channel in order to snoop the data, which can be analyzed then to obtain valuable and private information.

*2) Data Modification and Injection:* Attackers forge medical data by replacing or removing part of or all the eavesdropped information, and then transmit the modified data back to the original receiver.

*3) Replay Attack:* Attackers intercept a piece of valid information, especially some alarm messages, and re-transmit them to the receiver periodically in order to influence the normal operation of WBAN.

*4) Impersonation Attack:* Attackers may masquerade as authenticated nodes to join the network and launch attacks without being detected. Moreover, the dynamic feature of the WBAN makes the impersonation attack more prone to be implemented.

*5) Denial of Service:* DoS attacks can degrade the performance of a network or even break it down in the worst case. However, we still do not have efficient methods to avert this kind of attacks. As for WBAN, several common DoS attacks are listed as follows:

- Jamming: Attackers utilize a small number of jamming nodes to interfere with the wireless communications between nodes.
- Exhaustion: Attackers may send massive unnecessary packets in order to exhaust the resources of the network, such as the 'hello flood attack', for example.
- Selective forwarding: Attackers may impersonate as legitimate nodes and refuse to forward part of or even all the packets.

In this paper, we propose a sink node assisted lightweight intrusion detection mechanism to specifically address the replay, impersonation and DoS attacks, which cannot be countered by the intrusion prevention mechanisms.

## III. A Sink Node Assisted Lightweight Intrusion Detection Mechanism

### A. Assumptions and Configurations

Before introducing our proposed intrusion detection mechanism, we make the following assumptions.

- We consider a two-hop tree based network topology for the WBAN, as shown in Fig. 1, where biosensors are capable of both generating and of transmitting a data packet periodically, while relay nodes are responsible for forwarding it once they receive a data packet.
- The sink node is not restricted by the power supply, the computation capability as well as the storage resource. Moreover, we assume that the security of the wireless communication between the sink node and the base station is guaranteed.

In addition, several configurations are needed to be conducted. Specifically,

- Each biosensor maintains a counter, namely $C_p$, in order to record the number of packets that it has sent so far. When the biosensor reports the sensing information, $C_p$ is inserted into the packet. $C_p$ can be regarded as the sequence number of the packet, based on which the sink node can detect if there is something wrong with the packet during the transmission process.
- Each node in the WBAN is equipped with a unique identity information (ID). When it transmits or forwards a packet, its ID will be attached to the packet. Hence,

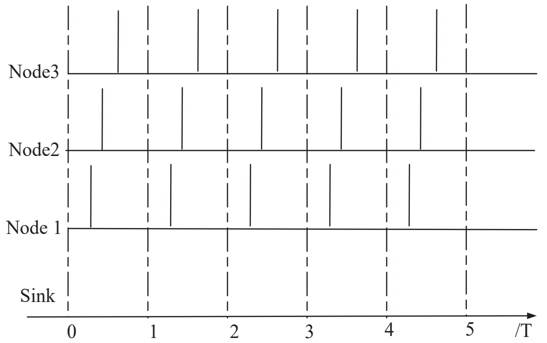


Fig. 2. Synchronization of the sink node.

the sink node can pick out which biosensor reports the sensing information, and which relay node forwards the packet. In this paper, the malicious node can duplicate a legitimate ID but cannot change the original ID of the nodes in the WBAN.

Relying on the state-of-the-art researches [13], [14], our above-mentioned configurations can be easily implemented.

### B. Synchronization of the Sink Node

Since biosensors periodically report their sensing information as shown in Fig. 2, in order to monitor all the packet transmission within one period, the sink node should make a statistical analysis within the same period with respect to these biosensors.

### C. Characteristic Parameters

In order to monitor the packet sent from each biosensor, the sink node maintains a data sheet represented by four characteristic parameters as listed in Table I. Each record in the data sheet corresponds to a biosensor. In our model, the sink node updates the value at certain time and detects the intrusions inside the WBAN based on the value recorded in the data sheet.

### D. Update of Characteristic Parameters

When receiving the data packet, the sink node first verifies the validity of the packet. Then, it updates the corresponding record in the data sheet according to the ID carried by the packet. This process can only be executed at three specific moments. To elaborate a little further,

- After receiving a valid data packet, the sink node firstly retrieves the sequence number $C_p$ and the sensing information $dataRcv$. Then, the sink node examines if the packet is replayed by the malicious node (Data replay detection, as shown in Section III-E). If not, the sink node assigns $C_p$ to $seqNum$ for a backup since $C_p$ is a temporary variable and it may be overwritten, when receiving a new packet. Moreover, the sink node increases the $C_r$ by 1 for one packet successfully received. Finally, the sink node backs up the sensing information $dataRcv$ for further analysis.

TABLE I
CHARACTERISTIC PARAMETERS

| Parameters | A Brief Description |
|---|---|
| $C_l$ | the number of continuously lost packets from a biosensor |
| $C_n$ | the number of lost packets from a biosensor in $NT$ periods, which may not be continuous. |
| $C_r$ | the number of packets that the sink node has received from a biosensor in a single period. |
| $C_p$ | the sequence number of the packet, which denotes the total number of packets that the biosensor has sent so far. |

- At the end of each period, the sink node examines the $C_r$ of each biosensor in the network. If the $C_r$ of a certain biosensor is equal to zero, the sink node makes the decision that the packet transmitted by this biosensor is lost during the transmission process. Hence, it increases both $C_l$ and $C_n$ by $1$, respectively. On the other hand, if $C_r$ is above zero, the sink node considers that there is a successful data transmission in the last period. Then, it assigns the backup of the sequence number $seqNum$ to the last sequence number $C_{pL}$, and resets $C_l$ to $0$. Finally, the sink node resets $C_r$ to $0$.
- At the end of each $NT$ periods, the sink node resets $C_n$ to $0$. In our mechanism, we utilize a *timer callback function* to realize the periodic operations, which can refer to **Algorithm 1**. **Algorithm 2** shows the process of receiving a data packet. Both **Algorithm 1** and **Algorithm 2** include the update operation of the characteristic parameters as listed in Table I as well as the intrusion detection scheme.

### E. Intrusion Detections

Our proposed sink node assisted lightweight intrusion detection mechanism is capable of defending four kinds of intrusions relying on the above-mentioned characteristic parameters of each node. In the following, we will detail the intrusion detection principles.

*1) Data Replay Detection (DRD):* After successfully receiving a data packet, the sink node retrieves the sequence number $C_p$ from the packet, which should be equal to $(C_{pL}+1)$. Hence, we have:

$$C_p = C_{pL} + 1. \tag{1}$$

However, the following two cases may break the rules. One is that malicious nodes replay the packet that they received before, and the other is the reception failure caused by jamming, selective forwarding, or some other reasons.

As described above, the number of continuously lost packets has been recorded by $C_l$. Hence, the rule of data replay

**Algorithm 1** *Timer Callback Function*

```
1: repeat
2:     If $C_l$ is beyond the threshold $N_l$, go to step 14.
3:     If $C_r$ is greater than zero, go to step 5.
4:     Increasing $C_l$ and $C_n$ by 1 respectively and going to step 6.
5:     Assigning $seqNum$ to $C_{pL}$ and resetting $C_l$ to zero.
6:     Resetting $C_r$ to zero.
7: until all biosensors have been examined.
8: Increasing $countNT$ by 1. If it is not equal to $NT$, go to step 15.
9: $countNT = 0$.
10: repeat
11:     If $C_n$ is beyond the threshold $N_n$, go to step 14.
12:     $C_n = 0$.
13: until all biosensors have been examined.
14: Triggering the alarm of data loss attack.
15: End.
```

**Algorithm 2** *The Process of Receiving a Packet*

```
1: Retrieving the sequence number $C_p$ and data item $dataRcv$ from the packet;
2: If $C_p \neq (C_{pL} + C_l + 1)\%N_p$, go to step 6.
3: Assigning the sequence number $C_p$ to $seqNum$, increasing $C_r$ by 1, and backing up the data item $dataRcv$ into the array $data[C_r]$.
4: If $C_r$ is greater than 1, compare all values of the array $data[C_r]$. If not, go to step 8.
5: If values of $data[C_r]$ are different, go to step 7. If not, go to step 8.
6: Triggering the alarm of data replay attack, and then going to step 8.
7: Triggering the alarm of data forging attack.
8: End.
```

detection can be appropriately reformulated as follows:

$$C_p \ = \ (C_{pL} + C_l + 1) \ \% \ N_p. \tag{2}$$

It is noted that $C_p$ is limited to the threshold $N_p$ for saving memory resources. Thus, it should be equal to the remainder of $(C_{pL}+C_l+1)$ against $N_p$ as shown in Eq. (2). Synchronizing the network with attaching a timestamp into the packet is a common approach to counter the replay attack.

In contrast, our mechanism detects the replay attacks by checking whether $C_p$ of the packet satisfies Eq. (2) regardless of the synchronization, which can save a large amount of resources.

*2) Data Loss Detection (DLD):* Each biosensor normally sends one packet within one period. Hence, each $C_r$ should be greater than 0, and if not, the sink node makes the decision that the packet sent by the biosensor is missed during the transmission process. Data loss is possibly caused by the following two reasons. One is that adversaries launch jamming or collision attack, and the other is that adversaries masquerade as legitimate relay nodes and selectively forward the packet that they have received.

As described above, the number of lost packets have already been recorded by $C_l$ and $C_n$. Thus, at the end of each period, the sink node checks $C_l$ to see the number of continuously lost packets, and at the end of every $NT$ periods, the sink node examines $C_n$ to monitor the number of lost packets in $NT$ periods. However, due to the dynamic nature of WBAN, even without any attacks, packet loss may occur. Hence, thresholds $N_l$ and $N_n$ are required. When $C_l$ or $C_n$ is beyond the threshold, the sink node triggers the alarm of data loss attack. It is noted that $C_n$ represents the number of lost packets in $NT$ periods, which can be regarded as packet loss rate. By contrast, $C_l$ denotes the number of continuously lost packets.

*3) Exhaustion Attack Detection (EAD):* The simplest way to implement a DoS attack may be the exhaustion attack. Adversaries can send the sink node or relay nodes massive unnecessary packets to drain their resources, such as the 'hello flood attack'. In our mechanism, the sink node and relay nodes individually maintain a counter to record the number of packets that they have received within one period, and if it is beyond the normal range, the sink node or relay nodes will set off the alarm of exhaustion attacks. Because the detection method has been commonly used, we do not give more description.

*4) Data Forging Detection (DFD):* Lightweight cryptographic protocol may have weaknesses which can be exploited by adversaries. Besides, adversaries generally have great power in computation, since they can easily launch attacks with laptops. Thus attackers may disentangle key materials from the intercepted packet, such as identity information and encryption keys. In this way, all the network is exposed to adversaries, which can arbitrarily launch any attack, such as impersonating as legitimate nodes with the identity information, and forging the packets with the encryption keys. Given that there are few valid measures to counter such attacks, here we propose an efficient method for preventing the risk.

In our mechanism, each node has an exclusive ID, and when a biosensor reports the sensing information, it has to attach its ID to the packet. As a result, when the adversary forges the packet, it has to attach its stolen ID to the forged data. Thus, the sink node receives at least two packets with the same ID, and then the sink node compares the packets. If the sensing information is different, the sink node concludes that some of these packets are forged and data forging alarm will be raised.

As a conclusion, our mechanism addresses the security issues by four ways: DRD against replay attack; DLD against jamming and selective forwarding attack; EAD against exhaustion attack; and DFD against data forging attack. Table II shows the performance analysis of our mechanism compared with other intrusion detection mechanisms. It can be seen that our mechanism is competent to detect all the inside and DoS attacks described in Section II.

TABLE II
PERFORMANCE ANALYSIS OF DIFFERENT INTRUSION DETECTION MECHANISMS

| | Replay Attack | Jamming | Data Forging | Exhaustion DoS | Selective Forwarding |
|---|---|---|---|---|---|
| Salem *et al.* [10] | ✓ | × | × | × | ✓ |
| Salem *et al.* [15] | ✓ | × | × | ✓ | ✓ |
| He *et al.* [16] | ✓ | ✓ | ✓ | ✓ | × |
| Ours | ✓ | ✓ | ✓ | ✓ | ✓ |

## IV. SIMULATION RESULTS

### A. Simulation Environment

Traditional simulation platforms like OPNET, and NS can hardly build a suitable model for WBAN due to its dynamic nature. By contrast, as a specific simulator for WSN and WBAN, Castalia offers a custom path loss map and a time-variant wireless channel environment of WBAN, which is derived from experimental measurements. Thus, it is very appropriate for our experiments.

There are six nodes (one sink node, two legitimate nodes, and three malicious nodes) in our experiments, since Castalia only provides the path loss map of six biosensors. To implement our mechanism, we just modify the application layer of the node. Each biosensor reports the sensing information every $10$ seconds and the packet loss ratio is about $10\%$ without attacks. The sink node monitors $C_l$ every 10 periods, that is, $NT$ is 10. In order to save memory, the threshold for $C_p$ is 16.

### B. Attack Models

We divide the threats that our mechanism addresses into three categories as follows:

$Attack\ I$: Abstraction of replay and data forging attacks. Malicious nodes inject forged packets into the network with random sequence numbers. To verify the validity of our mechanism, malicious nodes randomly launch $400$ attacks and the simulation lasts for $1,000$s.

$Attack\ II$: Abstraction of jamming and selective forwarding attacks. Malicious nodes randomly drop the packets and the packet drop ratio ($PDR$) is $20\%$, $30\%$ and $40\%$, respectively. As described in Section III-E, to monitor the packet loss, the sink node checks $C_l$ every $NT$ periods. The simulation lasts for $400 * NT$ periods, that is $40,000$s.

$Attack\ III$: Abstraction of exhaustion DoS attacks. Malicious nodes send massive packets to the sink node every once in a while, and their delivery rate of packets is about 10 times that of the legitimate nodes. The simulation lasts for $1,000$s.

### C. Result Analysis

We implement the above three attacks and Fig. 3 shows the detection rate of our mechanism. As for intrusion detections, the true positive rate ($TPR$) can be calculated as:

$$TPR = \frac{TP}{TP + FN}, \tag{3}$$

where $TP$ is the number of true positive nodes and $FN$ is the number of false negative nodes in our experiments. The false positive rate ($FPR$) is defined as:

$$FPR = \frac{FP}{TN + FP}, \tag{4}$$

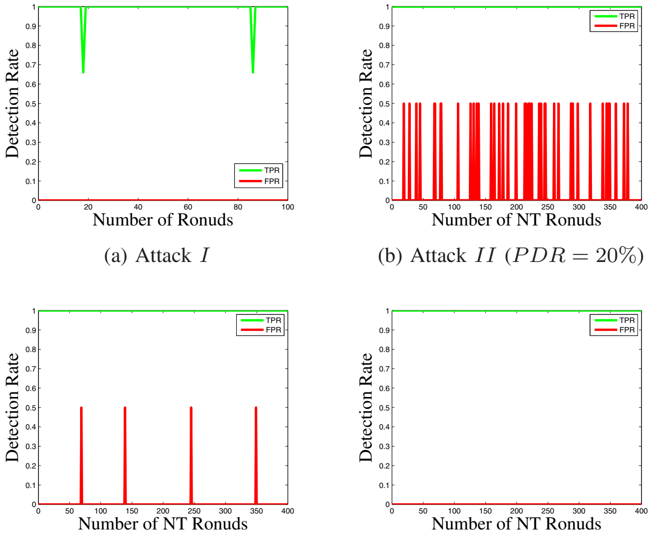
where $FP$ is the number of false positive nodes, and $TN$ is the number of true negative nodes.

As shown in Fig. 3(a), the sink node misses two detections of $Attack\ I$. Thus the $TPR$ is $66.7\%$ ($TP = 2, FN = 1$) at the two moments. As mentioned above, when malicious nodes launch $Attack\ I$, they just randomly forge the sequence number of the packet. Hence, the forged packet may happen to have the same sequence number with a normal one. In this way, data replay detection cannot detect it. However, it will cause the corresponding biosensor's $C_r$ out of the normal range, which can be detected by the data forging detection. However, if the normal packet is lost in transit, and malicious nodes happen to forge a packet with the same sequence number as the lost, then the forged data escapes the detection. In our experiments, malicious nodes totally launch $400$ attacks. Almost all the attacks are successfully detected, and there is no false positive detection.

Fig. 3(b) shows the detection rate in the context, where the $PDR$ of malicious nodes is $20\%$ and the threshold $N_n$ for $C_n$ is also $20\%$. All the attacks have been detected, but there are 30 false positive detections since packet loss occurs even under normal circumstances, and thus the $FPR$ is $50\%$ at those moments ($FP = 1, TN = 1$). Fig. 3(c) shows the detection rate with $PDR$ and $N_n$ equaling to $30\%$. All the attacks have been detected, yet there still are $4$ false positive detections. When $PDR$ and $N_n$ are $40\%$ or above, there is no false positive detection.

As for $Attack\ III$, since malicious nodes need to send massive packets in a short time, thus it can be effectively detected. In our simulations, we set the threshold of $Attack\ III$ to be the number of nodes in the network. All the attacks have been detected and there is no false positive detection. It can be concluded that both $AttackII$ and $Attack\ III$ are DoS attacks. As we all know, DoS attacks are aimed to degrade the performance of the network. Thus adversaries have to deliver massive attacks to realize their illegal purpose. As a result, the mechanism can lead to a very high detection rate with an appropriate threshold.

The detection rate $TPR$ and $FPR$ in Fig. 3 is calculated



(a) Attack $I$

(b) Attack $II$ $(PDR = 20\%)$

(c) Attack $II$ $(PDR = 30\%)$

(d) Attack $II$ $(PDR = 40\%)$

Fig. 3. Detection rate of the attacks

on nodes basis. However there are only several nodes in our experiments subject to the simulation platform. Hence that cannot precisely depict the detection rate of our mechanism. Table III shows the re-calculated detection rate on attacks basis, for example, as for $Attack\ I$, there is total 400 attacks and two of them are missed by the sink node, thus $TPR$ is 99.5% ($TP = 398, FN = 2$). It can be concluded that our mechanism results in a very high true positive rate of 99.5% as well as an ideal false positive rate of 0% when the $PDR$ of $Attack\ II$ is above 40%.

TABLE III
DETECTION RATE PARAMETERIZED IN DIFFERENT ATTACK MODELS

| | $Attack\ I$ | $Attack\ II$ 20% | $Attack\ II$ 40% | $Attack\ III$ |
|---|---|---|---|---|
| $TPR$ | 99.5% | 100% | 100% | 100% |
| $FPR$ | 0% | 3.75% | 0% | 0% |

## V. CONCLUSIONS

In this paper, we first make a detailed description about the security threats of WBAN. Moreover, we propose a sink node aided intrusion detection mechanism to address above-mentioned security issues. In our proposed mechanism, each node has an exclusive ID and each biosensor maintains a counter in order to record the number of packets that it has sent. Biosensors periodically report a packet with the counter and their identity information attached. The sink node monitors the packet transmission and checks the sequence number to detect the intrusions. Extensive analysis and simulations using Castalia have been conducted and verified a very high true positive rate and an ultra-low false positive rate of our proposed mechanism.

## ACKNOWLEDGEMENT

This work was supported by the Shenzhen Science and Technology Program (Grant No. JCYJ20150831192224146), and also funded by Tsinghua National Laboratory for Information Science and Technology (TNList) Cross-discipline Foundation.

## REFERENCES

[1] S. L. Keoh, "Efficient group key management and authentication for body sensor networks," in *IEEE International Conference on Communications (ICC)*, Kyoto, Japan, Jun. 2011, pp. 1–6.

[2] C. Jiang, H. Zhang, Y. Ren, Z. Han, K.-C. Chen, and L. Hanzo, "Machine learning paradigms for next-generation wireless networks," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 98–105, Apr. 2017.

[3] J. Wang, C. Jiang, Z. Han, T. Q. Quek, and Y. Ren, "Private information diffusion control in cyber physical systems: A game theory perspective," in *Computer Communication and Networks (ICCCN), 2017 26th International Conference on*, Vancouver, Canada, Aug. 2017, pp. 1–10.

[4] C. Jiang, L. Kuang, Z. Han, Y. Ren, and L. Hanzo, "Information credibility modeling in cooperative networks: Equilibrium and mechanism design," *IEEE Journal on Selected Areas in Communications*, vol. 35, no. 2, pp. 432–448, Feb. 2017.

[5] K. Malasri and L. Wang, "Design and implementation of a securewireless mote-based medical sensor network," *Sensors*, vol. 9, no. 8, pp. 6273–6297, Aug. 2009.

[6] D. He, S. Chan, and S. Tang, "A novel and lightweight system to secure wireless medical sensor networks," *IEEE journal of biomedical and health informatics*, vol. 18, no. 1, pp. 316–326, Jan. 2014.

[7] H. Wang, H. Fang, L. Xing, and M. Chen, "An integrated biometric-based security framework using wavelet-domain HMM in wireless body area networks (WBAN)," in *IEEE International Conference on Communications (ICC)*, Kyoto, Japan, Jul. 2011, pp. 1–5.

[8] K. Saleem, H. Abbas, J. Al-Muhtadi, M. A. Orgun, R. Shankaran, and G. Zhang, "Empirical studies of ECG multiple fiducial-points based binary sequence generation (MFBSG) algorithm in e-health sensor platform," in *IEEE 41st Conference on Local Computer Networks Workshops*, Dubai, UAE, Nov. 2016, pp. 236–240.

[9] G. Thamilarasu, "Genetic algorithm based intrusion detection system for wireless body area networks," in *IEEE Symposium on Computers and Communication (ISCC)*, Larnaca, Cyprus, Jul. 2015, pp. 160–165.

[10] O. Salem, A. Guerassimov, A. Mehaoua, A. Marcus, and B. Furht, "Sensor fault and patient anomaly detection and classification in medical wireless sensor networks," in *IEEE International Conference onommunications (ICC)*, Budapest, Hungary, Jun. 2013, pp. 4373–4378.

[11] T. Dimitriou and K. Ioannis, "Security issues in biomedical wireless sensor networks," in *First International Symposium on Applied Sciences on Biomedical and Communication Technologies*, Aalborg, Denmark, Oct. 2008, pp. 1–5.

[12] J. Wang, C. Jiang, T. Q. Quek, X. Wang, and Y. Ren, "The value strength aided information diffusion in socially-aware mobile networks," *IEEE Access*, vol. 4, no. 4, pp. 3907–3919, Aug. 2016.

[13] S. Shin, T. Kwon, G.-Y. Jo, Y. Park, and H. Rhy, "An experimental study of hierarchical intrusion detection for wireless industrial sensor networks," *IEEE Transactions on Industrial Informatics*, vol. 6, no. 4, pp. 744–757, Nov. 2010.

[14] C. Wang, T. Feng, J. Kim, G. Wang, and W. Zhang, "Catching packet droppers and modifiers in wireless sensor networks," in *6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks*, Rome, Italy, Jun. 2009, pp. 1–9.

[15] O. Salem, Y. Liu, and A. Mehaoua, "Anomaly detection in medical WSNs using enclosing ellipse and chi-square distance," in *IEEE International Conference on Communications (ICC)*, Sydney, Australia, Jun. 2014, pp. 3658–3663.

[16] D. He, C. Chen, S. Chan, J. Bu, and A. V. Vasilakos, "ReTrust: Attack-resistant and lightweight trust management for medical sensor networks," *IEEE Transactions on Information Technology in Biomedicine*, vol. 16, no. 4, pp. 623–632, Jul. 2012.