2018 IEEE International Conference on Industrial Internet (ICII)

A New Efficient Scheme for Securely Growing WBAN Nodes

Zhouzhou Li, Hua Fang, Honggang Wang, Shaoen Wu, Mahmoud Daneshmand

***Abstract*—Securely growing or de-growing nodes is a mandatory requirement to manage Wireless Body Area Networks (WBANs). This requirement raises significant challenges in node authentication, backward node authentication, initial node configuration, and node de-growth. Unlike the traditional approaches using pre-stored secrets or relying on special authentication hardware, we explore the characteristics of WBAN and wireless signal to develop an efficient scheme for adding/removing WBAN node securely and effectively. The major idea of the proposed scheme is to construct a 'virtual' dual-antennae proximity detection system by fully utilizing the existing legitimate nodes and the behavior of human body. We built a system prototype on wireless devices and verified our scheme through experiments. In addition, a data mining (clustering) algorithm is also applied to successfully detect newly joined legitimate node and identify potential attackers.**

***Index Terms*—Wireless Body Area Network(WBAN), Received Signal Strength Indicator(RSSI), Node Growth, Node De-growth, Node Authentication, Symmetric Key Generation.**

I. Introduction

In recent years, Wireless body area networks (WBANs) WBANs are becoming popular in health care, sports, entertainment, and military applications. However, WBANs has security risk due to its wireless broadcasting nature and carrying sensitive personal health information. Securely growing (including de-growing) WBAN nodes is a mandatory requirement for WBAN management. During node growth, the newly deployed legitimate node shall gain the trust of the WBAN, and vice versa. This is done through authentication and backward-authentication. After that, the WBAN shall initially configure the new node. The initial configuration information shall be imparted to the new node in a secure way. Due to the resource constraint, all these activities has to be done through wireless links, even before secure links are established. Furthermore, the WBAN shall have the capability of preventing itself from attacks.

WBAN node growth (including de-growth) requires the involvement of the end user or technician. The vendors of WBANs provide detail guideline to the end users or technicians, for them to follow. However, due to the characteristics of WBAN, the traditional method is facing critical challenges, including:

1) Knowledge & Expertise Gap: WBAN is a comprehensive technology that combines the advantages of sensing, wireless communication, and Internet techniques. Most of the end users are not familiar with all the techniques; therefore, usually, they are hard to follow the operation steps described in the manual, particularly, when they encounter exceptions.
2) Heterogeneity: WBAN nodes are provided by different vendors. Different vendors may follow different standards, or the same standard but with different versions, to manufacture the nodes. Moreover, the deployed nodes may have different user interfaces. This interface and hardware diversity may be fully covered by user manual.
3) Limited Interfaces: WBAN nodes are resource-constrained. Regularly, each of them has only one MCU, one transceiver, and one antenna; they are battery-powered. All the physical constraints limit their processing capability, receiving signal energy level, working duration. We can only expect a node to provide limited power, capacity, intelligence to support node growth.
4) Node Quantity: The node density of a WBAN is high above an average level compared to other wireless networks. Fully manually adding all the nodes to a WBAN is only possible for a small size WBAN. For a WBAN with hundreds of nodes, its full growth lasts long and may be prone to incur mistakes.
5) Dynamic Security Edge: With nodes joining or exiting a WBAN from time to time, the WBANs security edge dynamically changes. The common configuration of the WBAN should be imparted to the newly joined legitimate node during growth; while the configuration should be obsolete and re-generated timely after a node is leaving the WBAN, or when there is a potential risk threatening the WBAN security. One-time authentication and configuration is simply not adequate for WBAN.

Due to the above critical challenges, we need a nearly automatic, common, efficient, and dynamic scheme to securely adding WBAN nodes. However, the existing schemes did not fully satisfy the requirement. In [1], a lightweight WBAN node authentication scheme, BANA, was proposed, yet it did not rely on prior-trust among nodes and was compatible with commercial off-the-shelf lowend sensors.In [2], the authors proposed a novel mechanism for authenticating a nearby wireless device without requiring pre-shared secrets. In [3], the authors proposed a similar solution as [2]. They introduced a system called Wanda, which could be used to, efficiently, securely, and intently impart data onto wireless devices.We also reviewed [6]–[10]. As a summary, the existing schemes cannot fully satisfy the requirements of secure growth or de-growth of WBAN nodes.

In this paper, we propose a practical and efficient scheme for node growth in WBANs.

The rest of the paper is organized as follows. In Section

978-1-5386-7771-1/18/$31.00 ©2018 IEEE
DOI 10.1109/ICII.2018.00026

II, we construct the system model with legitimate nodes and attackers for further discussion and provide our new scheme. In Section III, we show our prototyping and results. Then, the conclusion and future works will be provided in Section IV.

II. System Model

In this paper, we will discuss the WBAN system model shown in Fig. 1 without losing the generality. The WBAN system includes k legitimate nodes ($N_1 ... N_k$) and a Control Unit (CU). A legitimate node in WBAN is not expected to be a powerful device with plenty resources available, while the CU dominates much more resources than the legitimate nodes. Inside the WBAN, the communication is through secure links due to the openness and insecurity of wireless signals. Without losing the generality, we assume there are secure links (either single hop or multiple hops) established between each legitimate node and the CU.

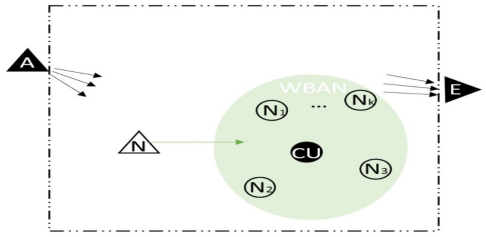

Fig. 1: WBAN System Model

Whenever a new node (N) joins in the WBAN, besides it is physically placed in the WBAN, the representative of WBAN like CU will need to authenticate the new node to ensure it is legitimate. Later, the WBAN will try to initially configure the new node. At this moment, because the node is not fully logically connected to the WBAN, we cannot assume a secure link has been established between them. Therefore, only public insecure link is available, and the initial configuration shall be very careful in case it leaks the secrets of the whole WBAN. Furthermore, whenever a legitimate node leaves the WBAN, still the node keeps the common secrets of the WBAN. This is a security hole; therefore, a routine mechanism is required to detect the nodes leaving and a protection mechanism is activated after the detection.

In this model, we also put attackers (A, E) around the WBAN but they are away with a certain distance. The Line of Sight (LOS) attack is hard to carry out given the time window of node growth is very short and approaching the target is not always possible. Therefore, here, we only consider the Non-LOS attacks. An attacker could be an eavesdropper (E), an active attacker (A), or combinations of them. An eavesdropper only listens, but it is hard to detect. An active attacker sends out signals to hinder the correct decision of legitimate nodes. Among so many active attack types, impersonation attack is prevalent and harder to detect, and it causes serious harm to WBAN node growth. Therefore, in this article we mainly discuss the case of impersonation attack.

To simplify our discussion, we assume each node has a unique ID, that others cannot (double) claim. One example is the public key of an asymmetric key pair every outgoing message will be signed by the private key; that signature can be viewed by the receiver via the public key. Due to the resource constraint, a node may only able to generate a short-term key pair. Before the key pair expire, a new key pair can be generated and form a chain with the old pair (like the block-chain). However, this is not the focus of this article.

A. Methods

1) Node Authentication: A RSSI value can be formulated as $RSSI = SSSI - A(d)$, where SSSI is the 'Sent Signal Strength Indicator,' representing the sending energy; $A(d)$is a function of distance d, representing the energy attenuation during signal propagation. In detail, $A(d)$can be formulated as $A(d) = 10\partial \log_{10}(d)$, where ∂ is the path-loss coefficient, and in free space it is 2 [4]. We can transform the formula to $A(d) = 10 \cdot 2 \cdot \log_{10}(d \cdot c)$, where c is the distance conversion coefficient decided by the media attenuation feature ($c \geq 1$; $c = 1$ when signal is propagated in free space). As a summary, RSSI values are decided by the following factors:

1) The SSSI (sending energy), which is unknown at the receiving side
2) The distance d (signal propagation path)
3) The distance conversion coefficient (media attenuation feature)

The RSSI-based location algorithms usually are utilized to estimate the inter-node distance d from collected RSSI values. However, #1 is an unknown factor at the receiving side. Therefore, directly, we cannot accurately estimate d from RSSI values.

To accurately estimate d, the strategy is to measure multiple RSSI values from a sent message, then calculate differential RSSI value to cancel the SSSI, thus build the relationship between the distance and the RSSI gap.

$$RSSI_1 = SSSI - 10 \cdot 2 \cdot \log_{10}(d_1 \cdot c_1) \quad (1)$$

$$RSSI_2 = SSSI - 10 \cdot 2 \cdot \log_{10}(d_2 \cdot c_2) \quad (2)$$

Subtract (1) from (2), we can get the equation:

$$\Delta RSSI = -20 \cdot \log_{10}(\frac{d_2 \cdot c_2}{d_1 \cdot c_1}) \quad (3)$$

In free space, $c_1 = c_2 = 1$, (3) can be simplified as:

$$\Delta RSSI = -20 \cdot \log_{10}(\frac{d_2}{d_1}) \quad (4)$$

In [2] and [3], the authors exploited two receiving antennae to measure one source signal every time and intently placed the target close to one of the two antennae to cause a large ratio of $\frac{d_2}{d_1}$; therefore, they could obtain a large RSSI gap for a nearby node. A faraway node cannot cause a large ratio of $\frac{d_2}{d_1}$; therefore, it cannot cause a large RSSI gap.

In both [2] and [3], the authors mentioned the rule that the inter-antenna distance should at least be greater than $\frac{\lambda}{2}$, although, they did not explain the reason. In order to reveal the relation between the rule and the equation (4), we set up experiments to verify the Dual Antennae Proximity Detecting and Configuration (DAPDC) system.

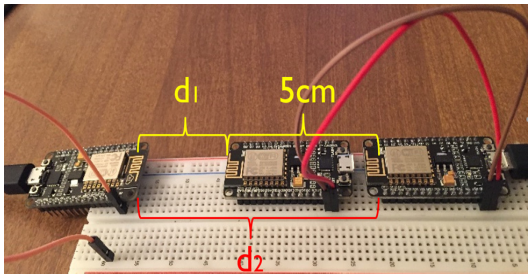

Fig. 2: Experiment with a Nearby Target and Two Receiving Antennae

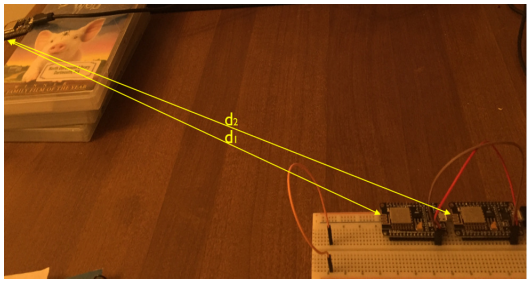

Fig. 3: Experiment with a Faraway Target and Two Receiving Antennae

As shown in Fig. 2, we use three NodeMCU development boards [5], each of which has a MCU, a 2.4GHz Wi-Fi transceiver, and a USB power supply. The left most NodeMCU is the target subject under test. It can send out probe messages (either multi-casted or broadcasted) in every 200ms, which can trigger the other NodeMCUs to measure RSSI values. The middle NodeMCU provides antenna 1 to receive the probe messages; the right most NodeMCU provides antenna 2 to receive the probe messages. As the Wi-Fi signal's wavelength is 13cm, intently, we set $d_1 < 5cm < \frac{\lambda}{2}$ and inter-antenna distance $\Delta d = d_2 - d_1 = 5cm < \frac{\lambda}{2}$. By doing this, we can ensure $d_2 > 2 \cdot d_1$, thus, the RSSI gap between the two antennae should be significant.

In the target subject (the left most NodeMCU), we create an UDP socket and a cyclic 200ms timer. Whenever the timer is fired, a probe message will be broadcasted to the two receiving antennae (the right most two NodeMCUs).

In each of the receiving antenna systems, we create an UDP socket to receive the probe messages. Whenever a probe message is arrived, the system will measure the RSSI value and store it to a log file. Overall, 256 RSSI values per antenna are logged.

Then, as shown in Fig. 3, we keep the receiving antennae (the right most two NodeMCUs in Fig. 2) unchanged, and move the target (the left most NodeMCU) at least 50cm away from the two receiving antennae. The target subject still does the probe things, and the inter-antenna distance is still 5cm at the receiving side except $\frac{d_2}{d_1} < 2$ and $d_1 >> 5cm$. This time, the receiving side also logs the RSSI sequence. Overall, 256 RSSI values per antenna are logged as well.

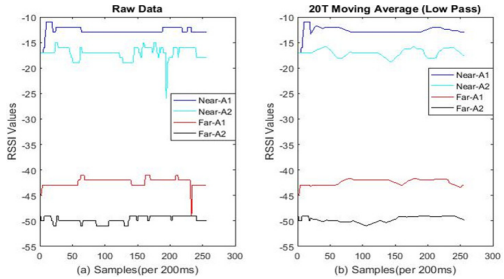

Fig. 4: Raw and Low Pass RSSI Sequences

At last, we analyze the RSSI sequences for both nearby target and faraway target and generate the Fig. 4 by combining the experiment results.

In Fig. 4, the blue line represents the RSSI sequence collected by antenna 1 and triggered by the nearby target. The sky-blue line represents the RSSI sequence collected by antenna 2 and triggered by the nearby target. The red line represents the RSSI sequence collected by antenna 1 and triggered by the faraway target. The black line represents the RSSI sequence collected by antenna 2 and triggered by the faraway target. The RSSI gap between two antennae is used by [2] [3] to determine the proximity of the target. Per [2] [3], the nearby target should have a more significant RSSI gap than that of the faraway target. However, due to the short inter-antenna distance, this rule is broken. Fig. 4(a) gives the raw RSSI sequence. To have a clear and intuitive impression, we also provide Fig. 4(b), which gives the result of low pass filtering. Undoubtedly, this time, the faraway target has a more significant RSSI gap than that of the nearby target. This reveals the wavelength's impact to equation (4) and the limitation of distance-based schemes.

From different attackers' point of views, the closer are the two antennae, the harder is it for attackers to distinguish them from their RSSI values, the harder is it for attackers to break the RSSI-based configuration method [3]. To protect the WBAN during a new node's initial configuration, we need to make the two antennae close. However, the wireless signal's wavelength decides whether the node authentication methods proposed in [2] [3] work or not. Then, we need to make sure that the two antennae are separated at least a half of a wavelength away in free space. This is a dilemma.

To get a hint for solving the dilemma, first, we need to transform equation (3) to:

$$\Delta RSSI = -20 \cdot \log_{10}(\frac{d_1 \cdot c_1 + \Delta d \cdot c}{d_1 \cdot c_1}) \quad (5)$$

Where Δd is the distance between antennae 1 and 2; c is the distance conversion coefficient decided by the media attenuation characteristic and the angle between d_1 and d_2. Almost, the impact of the angle between d_1 and d_2 can be ignored, then, equation (5) can be simplified as:

$$\Delta RSSI \approx -20 \cdot \log_{10}(1 + \frac{\Delta d \cdot c}{d_1}) \quad (6)$$

Where
- Δd is the distance between antennae 1 and 2.
- c is the distance conversion coefficient decided by the media attenuation feature.
- d_1 is the distance between the target and antenna 1.

It is noteworthy that equation (6) is correct only when $\Delta d \cdot c > \frac{\lambda}{2}$. Equation (6) reveals the available equivalent model when the inter-antenna distance is limited. That is utilizing high-attenuation media between the two antennae.

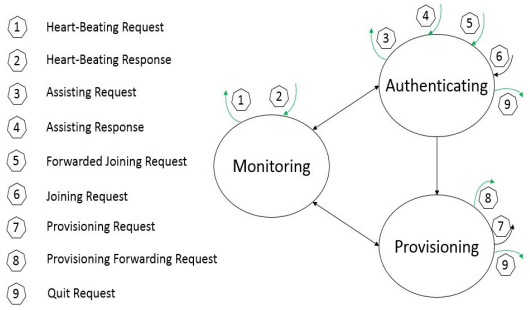

Fig. 5: State Transition Diagram of CU

2) CU: As shown in Fig. 5, the CU is the representative of the WBAN, which oversees the process of node growth and routine sanity check. For a stable WBAN, the CU is in Monitoring state, responsible for detecting the absent condition of legitimate nodes. If absence is detected (no message 2 is received after sending message 1), then the CU will activate a procedure to refresh the common secrets and configuration data of the WBAN. This is to fix the security hole caused by node de-growth. The CU is also responsible for detecting impersonation attacks:

- If the CU is in Monitoring state, then any Joining Request (message 6) is unexpected. Therefore, the CU will warn the user of impersonation attacks.
- If the CU is in Authenticating state, and more than two IDs sending Joining Request at the same period, then the CU will warn the user of impersonation attacks because one time only one Joining Request is expected.
- If the CU is in Provisioning state, then any Provisioning Request (message 7) to the target new node will be collected and analyzed by the CU (of course, the CU will need to change the mode of its wireless interface to capture the messages not destining to it). If other IDs than the CU or the assistant node, unexpected show in the Provisioning Request as senders, then the CU will warn the user of impersonation attacks. This will help the new node during backward authentication, because the new node will not be able to distinguish the legitimate message from an evil one. Also, the CU will check the frequency of Provisioning Request, if more detected than normal frequency, it will also warn the user of impersonation attacks.

Once the CU is put in the Authenticating state (could be manually triggered), it will promote an existing legitimate node to assist the node authentication (to construct a DAPDC). The Assisting Request (message 3) is sent to the existing legitimate node via existing secure link. After that, both the CU and the assistant node can receive Joining Request, while the assistant node will forward his to the CU via Forwarded Joining Request (message 5). Based on the RSSI values that measured by the CU and the assistant node, a data mining (clustering) algorithm will be used to distinguish the new node and impersonation attacker. Later in the 'prototyping' section, we will provide the details about the clustering algorithm.

After successful node authentication, the CU will proceed to Provisioning state. If node authentication failed, the CU will send Quit Request to the assistant node (thus the assistant node will transition back to Autarky state), and transition back to Monitoring state. Since the new node is not expected to handle the backward authentication, we combine the backward authentication and provision tasks in CUs Provisioning state. Once the CU enters the Provisioning state, it can send the Provision Request (message 7) to the new node directly or send the Provisioning Forwarding Request (message 8) to the assistant node for the latter to forward the Provision Request. The selection is fully decided by the content of the configuration data and the assistant nodes RSSI level. In the meantime, the CU will be responsible for detecting evil messages from impersonation attackers. As soon as the first Provision Request is received, the assistant node moves in Provision state.

3) Assistant Node: As shown in Fig. 6, the assistant node is an existing legitimate node. Before it is promoted, it is in the Autarky state only responding the Heart-Beating Request (message 1 and 2). Once it receives the Assisting Request (message 3), it transitions to Authenticating state. In the Authenticating state, the assistant node will collect the Joining Request (message 6) and forward it to the CU (message 5). Once the Provisioning Forwarding Request (message 8) is received, the assistant node transitions to the Provisioning state. In the Provisioning state, the assistant node will translate every Provisioning Forwarding Request to Provisioning Request (message 7) and send the latter to the new node. The assistant node is only responsible for relaying messages. It

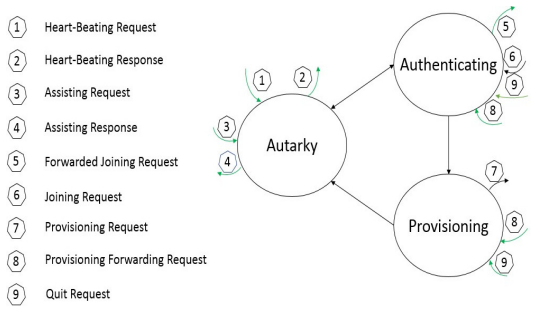

Fig. 6: State Transition Diagram of Assistant Node

relies on the CU to detect the evil message. Once receiving the Quit Request (message 9), the assistant node will transition back to the Autarky state.

4) Newly Joined Node: When the new node is in Growing state, it broadcasts Joining Requests (message 6) at some frequency, until it receives the Provisioning Request (message 7). From Provisioning Requests, the new node figures out the initial configuration data, which is embedded at the physical layer and protected by the physical layer security. The new node relies on the CU to detect impersonation attacks.

5) Attackers: Both passive and active attackers are considered in this article. Passive attacker is hard to detect because it only listens without talking. With the secure links, the sensitive WBAN data can be protected by strong keys during transportation. The passive attacker cannot break the encrypted data without knowing the secret key or having enough time. All the messages with green arrows in Fig. 9 and 10 are transported via secure links, they are eavesdropping-proof. All the messages with black arrows (message 6 and 7) in Fig. 9 and 10 are transported via insecure links, which we shall pay more attention to. To protect these messages, physical-layer security is exploited. Usually, from protocol perspective, the lower layers provide message headers and the higher layers provide message body. In physical-layer security, the logic is reversed: the physical layer contains the data while the upper layers provide headers. Although the upper-layer data is not protected and may be viewed by everyone, the physical layer data (e.g. RSSI) is protected by the mutual and exclusive characteristics of the wireless channel.

Impersonation attackers are typical active attackers. They pretend to be legitimate nodes trying to cheat the legitimate nodes. Compared to other active attacks, impersonation attacks are hard to detect. For simplicity, we use it here as an example of active attacks. To defend impersonation attacks, first the WBAN will need to detect the attacks. In this article, we add the impersonation attack detection mechanism in the CU and the messaging. The CU will keep monitoring unexpected Joining & Provisioning Requests, if detected, alert will be raised. There is a possibility that the impersonation attackers try to disturb the authentication of a new legitimate node by inserting more expected messages. We specify the frequency of Joining and Provisioning Requests to detect these replicated messages.

B. Protocols

Protocols include the local procedure part and the messaging part. The local procedure part was covered by previous sections. Here we only discuss the messages, especially the black-arrow messages because they are subject to incur attacks.

The messaging design for this security scheme will have the upper layer and physical layer parts. The content of the upper layer is public, which could be seen by the attackers. However, the timestamp and the signature can be used to prevent frequently replicated things such as spam emails. The common part of every valid message contains the 'Sender ID', 'Message Type', and a signed 'Sender ID + Message Type + Timestamp'. If the attackers cannot double claim the Sender ID, it cannot fake the correct signature. And the hash of the signature must follow some pre-defined pattern. By doing this, this part of message can provide the solid information about 'who sent this message'. The real data is embedded in the physical layer raw signal, which can be measured by the receiver (RSSI values), yet it is hard to break by the 3rd party per physical layer security.

Message exchange during node growth is complicated, limited by the article size, we ignore this part here.

III. Prototyping and Result

We make a prototyping by implementing the proposed node authentication method in five MICAz Mote Modules. Each of them is equipped with a 2.4 GHz Zigbee transceiver, a ATmega128L low-power MCU, and a modified case to commodate a 3v button battery. Among the five modules, one is acting as the CU. One is acting as the assistant. And one is acting as the newly joined node. The rest two are acting as the attackers. The newly joined node is close to the CU and the assistant. While the two attackers are 50cm away from them. The newly joined node and the two attackers do the same thing, that is broadcasting wireless signals (Joining Requests), the attackers randomly change their positions. All the broadcasted signals are measured by the CU and assistant.

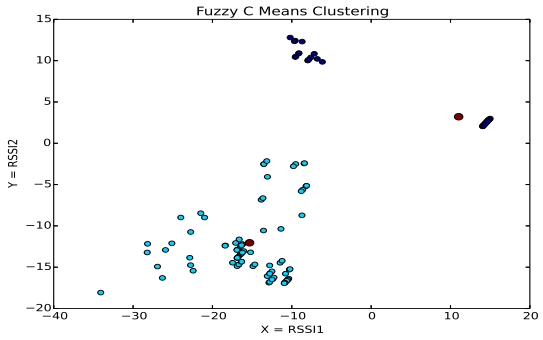

Fig. 7: FCM Clustering on Original RSSI Values

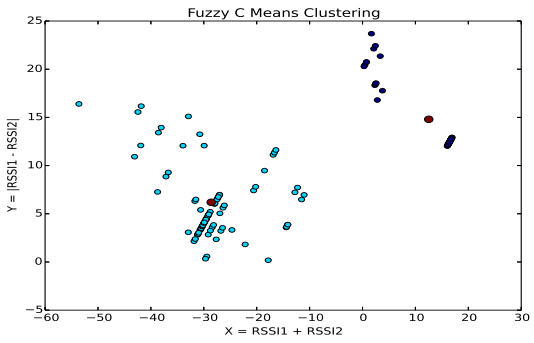

Fig. 8: FCM Clustering on Transformed RSSI Values

We used Fuzzy C Means (FCM) clustering algorithm to category the dual-measurement signals. As shown in Fig. 7 and Fig. 8, each signal caused one measurement at the CU and the assistant node respectively. Therefore, each signal was represented by a two-dimensional point on the figures. Fig. 7 shows the original measurements, the top block and right block are those signals with big gaps (caused by the new legitimate node). The other points are caused by the attackers. FCM was able to distinguish the new legitimate node and the attackers. However, because both $RSSI1 >> RSSI2$ and $RSSI2 >> RSSI1$ conditions are legitimate, the two legitimate blocks are separated. This may cause potential clustering issue, especially FCM does not guarantee the global optimal. We transformed the original data to let $X = RSSI1 + RSSI2$ and $Y = |RSSI1 - RSSI2|$, then we generated Fig. 8. There are two different clusters, one is with bigger variance (attackers) and the other is with smaller variance (new nodes). The FCM clustering algorithm can successfully label the two clusters. We can see from Fig. 8, some attacker points have better RSSI gap than the points in the right block, that is because sometimes the dual-antennae system has a short inter-antennae distance. This prototyping fully prove our inference.

IV. Conclusion and Future Work

In this paper, we propose a practical and efficient scheme for securely growing (including de-growing) WBAN nodes. Our scheme includes the node authentication, backward authentication, initial node configuration, and de-growth issues. Our scheme is a pure software solution, which does not require extra hardware. Therefore, our solution is cost-effective, and interoperable among different standards of devices. There are other advantages of our proposed schemes: (1) It is wavelength-independent, which can support a wide spectrum; (2) It provides a high-speed, stable, and secure configuration link upon insecure wireless channels, which makes it an efficient and secure solution; 3) It takes full advantage of capacity of existing devices and features of WBANs to avoid unnecessary user interactions and technician supports, which is user friendly and easy to deploy.

In addition, our scheme shows the great resistance to impersonation and passive attack. In the future, we plan to explore our solutions in smart health applications based on WBANs.

References

[1] Shi, L., Li, M., Yu, S., & Yuan, J. (2013). *BANA: body area network authentication exploiting channel characteristics.* IEEE Journal on selected Areas in Communications, 31(9), 1803-1816.

[2] Cai, L., Zeng, K., Chen, H., & Mohapatra, P. *Good Neighbor: Ad-Hoc Authentication of Nearby Wireless Devices by Multiple Antenna Diversity,* NDSS Symposium 2011.

[3] Pierson, T. J., Liang, X., Peterson, R., & Kotz, D. (2016, April). *Wanda: securely introducing mobile devices.* In Computer Communications, IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on (pp. 1-9). IEEE.

[4] T. S. Rappaport, "*Wireless communications: principles and practice,*" Prentice-Hall, 2002.

[5] *http://nodemcu.com/index_en.html*

[6] Li, Z., Wang, H., Daneshmand, M., & Fang, H. (2017, May). *Secure and Efficient Key Generation and Agreement Methods for Wireless Body Area Networks.* In Proc. IEEE ICC 2017, 21-25 May 2017, Paris, France.

[7] He, D., Zeadally, S., Kumar, N., & Lee, J. H. (2016). *Anonymous authentication for wireless body area networks with provable security*. IEEE Systems Journal, vol. 11, no. 4, pp. 2590-2601, Dec. 2017.

[8] Javali, C., Revadigar, G., Libman, L., & Jha, S. (2014, July). *SeAK: Secure authentication and key generation protocol based on dual antennas for wireless body area networks*. In International Workshop on Radio Frequency Identification: Security and Privacy Issues (pp. 74-89). Springer International Publishing.

[9] Rushanan, M., Rubin, A. D., Kune, D. F., & Swanson, C. M. (2014, May). *SoK: Security and privacy in implantable medical devices and body area networks*. In Security and Privacy (SP), 2014 IEEE Symposium on (pp. 524-539). IEEE.

[10] Zheng, G., Fang, G., Shankaran, R., Orgun, M., Zhou, J., Qiao, L., & Saleem, K. (2016). *Multiple ECG fiducial points based random binary sequence generation for securing wireless body area networks.* IEEE journal of biomedical and health informatics, vol. 21, no. 3, pp. 655-663, May 2017.