Double Threshold Authentication Using Body Area Radio Channel Characteristics

Nan Zhao, Aifeng Ren, Fangming Hu, Zhiya Zhang, Masood Ur Rehman, Tianqiao Zhu, Xiaodong Yang, and Akram Alomainy

***Abstract*— The demand of portable and body-worn devices for remote health monitoring is ever increasing. One of the major challenges caused by this influx of wireless body area network (WBAN) devices is security of user's extremely vital and personal information. Conventional authentication techniques implemented at upper layers of the Open System Interconnection (OSI) model usually consumes huge amount of power. They also require significant changes at hardware and software levels. It makes them unsuitable for inherently low powered WBAN devices. This letter investigates the usability of a double threshold algorithm as a physical layer security measure in these scenarios. The algorithm is based on the user's behavioral fingerprint extracted from the radio channel characteristics. Effectiveness of this technique is established through experimental measurements considering a variety of common usage scenarios. The results show that this method provides high level of security against false authentication attacks and has great potential in WBANs.**

***Index Terms*— Wireless body area networks, physical layer security, radio channel features, authentication.**

I. Introduction

WIRELESS Body Area Networks (WBANs) have seen a rapid growth in the recent years. Though its applications range from surveillance to entertainment and sports to military, remote health monitoring still serves as the prime focus. Health care devices using IEEE 802.15.6 and IEEE 802.15.4j standards are now part of thousands of households [1]–[7]. Along with numerous benefits, WBAN devices suffer from a number of challenges. Privacy of user and security of a highly personal data based on remote observation of user's vital physical parameters is one of the major issues. Low power requirements due to inherent nature of the body-worn devices and regulatory restrictions further complicate provision of efficient security measures in such devices.

Authentication of user's identity is the first hurdle in development of a secure system before responding to a general security breach and attack [8]. Recent studies show that IEEE 802.15.6 standard still has a long way to go to ensure privacy of the user [9]. In-home health care devices are at a greater risk of potential theft of pre-shared key. Traditional encryption methods have therefore, limited ability of denying admission to an attacker in the network posing as a legitimate node [10]. On top of that, these conventional security methods usually require high power and substantial changes at hardware and software levels. Hence, there is an apparent need to devise new and improved processes for the certification of the WBAN nodes.

Use of Physical Layer Security (PLS) technology based on antenna and propagation channel characteristics can be a well-suited alternative to the conventional security methods for the WBANs. However, benefits of the PLS cannot be exploited to its full extent using traditional protocols by combining 802.15.6 standard for power consumption and emergency transport requirements [11].

Some progress in this direction has been reported in the literature. Ali et al. have proposed a mechanism to secure the data provenance for body-worn devices by exploiting spatio-temporal characteristics of the wireless channel [12]. In [13], wave is used as the noise to assist matching of legal nodes. Shi et al. [14] have used Received Signal Strength Indicator (RSSI) to deal with the issue of authentication of the nodes in the network. This letter presents a new user authentication technique for the WBAN devices based on the combinations of user's behavior fingerprint and channel features, which improves the system security. WBAN sensor nodes equipped with an external antenna has been used to extract the channel characteristics and fingerprint of the user's habitual actions. A number of our daily life scenarios are considered. The experimental results have shown that the proposed authentication method is very proficient in repelling large number of low-level security attacks. Moreover, it does not require a key sharing resulting in a very energy efficient operation.

Following the introduction in this section, the letter is organized in five sections. Section II, describes the methodology and experimental setup. Section III establishes the usability and distinguished ability of the proposed scheme through experimental results and detailed analysis. Conclusions are drawn in Section IV.

II. Methodology and Experimental Setup

The experiments are conducted in a laboratory environment replicating a common home-based health care

Manuscript received June 25, 2016; accepted July 19, 2016. This work was supported in part by the National Natural Science Foundation of China (Grant No. 61301175), Fundamental Research Funds for the Central Universities, Project Funded by China Postdoctoral Science Foundation, Postdoctoral Research Projects Funded in Shaanxi Province. The associate editor coordinating the review of this letter and approving it for publication was S. Yu. *(Corresponding author: Xiaodong Yang.)*

N. Zhao, A. Ren, F. Hu, Z. Zhang, T. Zhu, and X. Yang are with the School of Electronic Engineering, Xidian University, Xi'an 710071, China (e-mail: nan_zhao_@hotmail.com; afren@mail.xidian.edu.cn; fangming95@163.com; zhiyazhang@163.com; tqzhu@mail.xidian.edu.cn; xdyang@xidian.edu.cn).

M. U. Rehman is with the Centre for Wireless Research, University of Bedfordshire, Luton LU1 3JU, U.K. (e-mail: masood.urrehman@beds.ac.uk).

A. Alomainy is with the School of Electronic Engineering and Computer Science, Queen Mary University of London, London E1 4NS, U.K. (e-mail: a.alomainy@qmul.ac.uk).

Digital Object Identifier 10.1109/LCOMM.2016.2597831

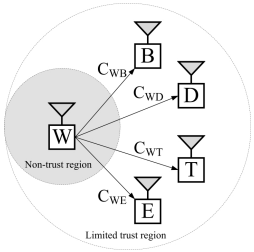

Fig. 1. Illustration of two experimental regions; non-trust region (outer circle) having MSs B, D, T and E monitoring the user brushing teeth, drinking water, taking medicine and eating breakfast; limited-trust region (inner circle) having the WHMD node W.

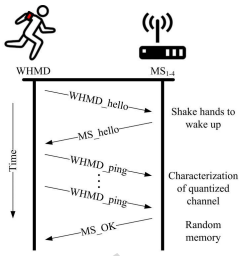

Fig. 2. WHMD and MS1-4 communication timing diagram.

scenario. A battery-powered wearable health-monitoring device (WHMD) has been positioned on the right upper arm of the user. The WHMD communicates continuously with the monitoring station (MS) connected to a computer placed in the same room at a distance of 10m. Four daily life actions of brushing teeth, drinking water, taking medicine, and eating breakfast are considered in this experiment. The WHMD monitors the changes in the radio channel characteristics caused by the user's actions and exchanges the RSSI data with the MS. The MS gathers and stores this data, which provides the behavioral fingerprint of the user. It is then used for the identity authentication.

In a typical indoor environment, radio wave will propagate along multiple paths. Each path will carry different amount of fading and time delay. The complex baseband signal voltage here is defined as:

$$V = \sum_{i=1}^{N} \| V_i \| \, e^{-j\theta_i} \tag{1}$$

where V_i and θ_i are the amplitude and phase of the ith path, N is the total number of paths. The RSSI is defined as:

$$RSSI\,[dBm] = 10log_2\left(\| V \|^2\right) \tag{2}$$

Taking the human body presence in consideration, Equation 2 can be expanded as:

$$MS_{RSSI}\,[dBm] = WHMD_{RSSI} + EIF + User\,[m,s] \tag{3}$$

where EIF is the environmental loss factor and $User[m,s]$ represents the multipath shadow component due to the user motion.

To clearly describe the initial security status of the WBAN nodes, the measurement area is divided into a non-trust and a limited-trust region (Fig. 1). The nodes located in non-trust region are considered to have an initial security status of being suspect and may be compromised. On contrary, the limited-trust region is envisaged to be equipped with basic safety protection measures (for example random storage, etc.). The nodes located in this region are therefore not easy to be compromised and set to have an initial security status of being safe.

Security of the WHMD is relatively easier to be breached as it can get missing or stolen due to user's carelessness. It is therefore. Considered to be in non-trust region. The MS has got fixed installation and less susceptible to stealing. It is therefore placed in the limited-trust region. Complete trust for the MS is however, not realistic as it stores highly sensitive data. Since, this study is intended to prove the idea, considerations in the experimental scenarios are kept simple and advanced hardware or active attacks are not taken into account. They will be however, studied in future expansion of this work.

Four common habits of any user are considered namely brushing teeth, drinking water, taking medicine and eating breakfast. The measurements were taken by making the human subjects to repeat the considered habitual action repeatedly over the course of the measurement. The variations in the channel characteristics in the form of RSSI values are monitored by the WHMD in each scene. It is then transmitted to the MS that keep a record of it.

Fig. 2 shows the communication timing diagram between the WHMD and the MSs. MS_{1-4} represents the four monitoring stations, one in each scenario. When the subjects arrive at the designated measurement scene, the WHMD broadcasts a $WHMD\_hello$ packet. On receiving this $WHMD\_hello$ packet, the MS enters into the active monitoring state and sends an MS_hello packet to the WHMD showing its readiness to receive the WHMD data. The WHMD then starts sending the $WHMD\_ping$ packets until it receives an MS_OK packet from the MS indicating that the MS has gathered sufficient information. During this communication, the MS reads the RSSI value of the $WHMD\_ping$ packets for the characterization of the radio channel to be used for authentication. In addition to the RSSI value, the $WHMD\_ping$ packets also carry other statistics, such as time alignment, battery consumption, etc. This data is however non-sensitive and does not contain any private information. Thus the identification process hardly has any extra packet consumption and no added energy burden to the system. The MS gathers RSSI measurements from each $WHMD\_ping$ packet at 500ms interval. These measurements are randomly stored in the module flash.

Both the WHMD and MS are wireless modules based on Texas Instruments system-on-chip (SOC) for wireless sensor networking solutions, C8051 MCU configuration and control communication unit. The HBE-ubiquitous Sensor Network (USN) module is used as the WHMD. It employs the IEEE 802.15.4 standard and can be programmed to achieve output power levels of -25.2 dBm to 0.6 dBm. The sensitivity of the receiver is -94 dBm. The onboard sensors are equipped with circularly polarized, omnidirectional antennas operating at 2.4 GHz. The module can be used in a variety of WBAN applications as meets the low power consumption and wireless

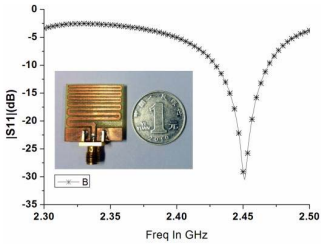

Fig. 3. Prototype and S11 of the meandered line external antenna used with HBE-USN-module.

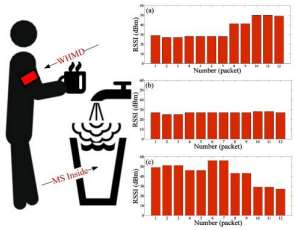

Fig. 4. Measurement scenario for the user in drinking water configuration showing location of the WHMD and the MS with three sets of randomly saved RSSI data recorded by the MS.

management requirements.

The HBE-USN-Sensor tag module is programmed to transmit a power level of -1.5 dBm at 2.425 GHz communication channel to avoid interference with existing Wi-Fi signal available in the experimental area. Communication between the WHMD and the MS is established using an external antenna connected to the HBE-USN-Sensor tag via an SMA port, as shown in Fig. 3. The antenna is of meandered line type operating at 2.4 GHz with good impedance matching and has dimensions of $26mm \times 26mm \times 1mm$. The antenna prototype and measured S_{11} of the antenna is illustrated in Fig. 3.

III. Result and Discussion

The RSSI data has been measured for the four considered user habits. Fig. 4 shows the measurement scenario for the user in drinking water configuration along with three sets of randomly stored RSSI data by the MS. To simplify the idea and ease of understanding, 36 packets are collected and divided into three sets in this work. In practical scenarios, the length of the data could be longer producing better randomness.

The RSSI sequence based on the fingerprint of user's habitual behavior is difficult to replicate or reproduce. In this environment, the WHMD is needed to be certified by the MS who is acting as the certifier. The authentication scheme has two processes namely behavioral fingerprint registration and identity authentication resulting in a double threshold authentication, as shown in Fig. 5.

In order to compare the behavior of the user with the legal template, correlation coefficient (CC) is computed as:

$$CC = \frac{\sum_{i=1}^{n} \left(X_i - \bar{X}\right)\left(Y_i - \bar{Y}\right)}{\sqrt{\sum_{i=1}^{n} \left(X_i - \bar{X}\right)^2} \sqrt{\sum_{i=1}^{n} \left(Y_i - \bar{Y}\right)^2}} \tag{4}$$

where X_i and Y_i are the ith packet of RSSI values, $\overline{X}$ and $\overline{Y}$ are the mean values of RSSI sequence.

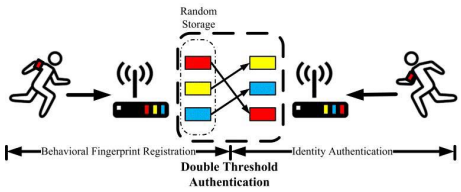

Fig. 5. Double threshold authentication scheme consists of the behavioral fingerprint registration and identity authentication processes.

TABLE I
Correlation Results for the Normal Certification Using Double Threshold Technique

Brushing Teeth CC	WHMD fragment 1	WHMD fragment 2	WHMD fragment 3
MS fragment 1	***0.9957***	0.4001	-0.6617
MS fragment 2	0.7552	0.7053	-0.5910
MS fragment 3	-0.9088	-0.6382	***0.8565***
Drinking Water CC	WHMD fragment 1	WHMD fragment 2	WHMD fragment 3
MS fragment 1	-0.9346	***0.9413***	-0.5838
MS fragment 2	***0.9356***	-0.9828	0.4016
MS fragment 3	0.5409	-0.6077	-0.1661
Taking Medicine CC	WHMD fragment 1	WHMD fragment 2	WHMD fragment 3
MS fragment 1	-0.2093	-0.1427	***0.8565***
MS fragment 2	***0.8103***	-0.2190	-0.4446
MS fragment 3	-0.4626	***0.9836***	-0.3586
Eating Breakfast CC	WHMD fragment 1	WHMD fragment 2	WHMD fragment 3
MS fragment 1	0.1983	***0.8516***	0.2561
MS fragment 2	-0.3945	0.5926	***0.9217***
MS fragment 3	***0.9541***	0.0834	-0.2546

The authentication scheme is implemented in four steps. Step one is the acquisition of the subject's behavior fingerprint by the MS, segmentation of the data and random storage as the template. Step two involves the repetition of the same behavior by the subject wearing the WHMD and collection of the new channel characteristics by the MS. Step three comprises of the MS calculation of the CC of the new channel features with the previously stored information in step one. Finally, step four involves the certification of the WHMD by the MS through double threshold authentication. Certification is granted if correlation value with each template is more than 0.8 and traversal or correlation between two data segments is more than 0.85. It shows that the behavioral fingerprint of the user seeking certification is in good match with the fingerprint of the legal user (template). This employs that the current subject can be perceived as the legal user since it is very difficult to reconstruct the radio channel. If the subject wearing the WHMD passes the authentication stage, its security status (which was in the non-trust region at the beginning) would be elevated to the limited-trust region.

The MS receives the RSSI data from the WHMD for the four considered scenarios. This forms the legal behavior template of the user and is being stored at the MS. To further strengthen the security, this data storage can use certain protection measures, such as fragmented storage or feature extraction. This work uses the fragmented storage approach due to its simplicity and effectiveness by dividing and storing the RSSI data into three segments. The correlation results for the three segments of the WHMD data have been summarized in Table I. The results show that the double threshold algorithm ensures high level of security. It ensures that the user only achieve identity authentication if correlation with the template is greater than 0.8 and traversal correlation or correlation of

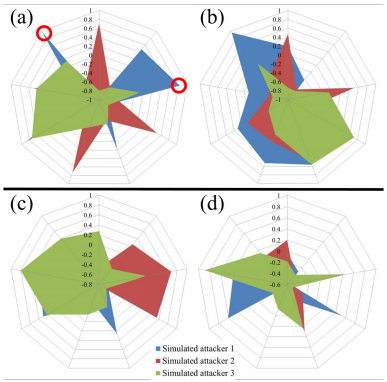

Fig. 6. CC results for the simulated attacks against the double threshold authentication algorithm, (a) Brushing Teeth, (b) Drinking Water, (c) Taking Medicine, (d) Eating Breakfast.

two data segments is more than 0.85 indicating high match to the user behavioral fingerprint.

This double threshold approach is not only a very efficient authentication method but also has strong resistance to the attackers. Three simulated attacks are studied to depict vigor of the proposed technique against the attackers. Worst-case scenario is analyzed assuming that the attackers have compromised the WHMD by reaching the limited-trust region (it is very difficult in realistic conditions due to high isolation and protection provided by traditional measures such as locked doors). These simulated attackers, with similar physique, observe and imitate the action of legal user in every scene. To further test the strength of the proposed approach, these simulations were repeated 10 times.

The results in Fig. 6 show that in even the worst-case scenarios, the attacker cannot succeed in the identity fraud. Only the attacker 1 in brushing the teeth scene has found a rare success, as depicted in Fig. 6(a). Here, two sequence relativity values are greater than 0.85 indicating that the feature is very obvious. This is due to the fact that the Brushing Teeth motion of the simulated attacker is similar to that of the legal user. However, due to the existence of multiple authentication base stations, the fake attacker was unable to complete the attack. Also, this is a rare hit which cannot be repeated multiple times as no other success is observed in the following simulations. Usefulness of the proposed algorithm in the identity authentication and against security attacks is evident from these results.

IV. Conclusion

A new technique for the user identification in WBAN sensor nodes is presented. This physical layer security method is based on the observation of the user's behavioral fingerprint through radio channel characteristics. The body-worn WHMD sends channel information to a static MS. The proposed technique makes use of double threshold identification strategy calculating correlation between first and subsequent RSSI samples received by the MS and traverse correlation between different segments of the sample data itself. Three simulated attacks are also used to study the strength of the proposed technique against the attackers.

Results based on the experimental data collected considering four daily life scenarios of brushing teeth, drinking water, taking medicine and eating breakfast show that the proposed technique can effectively realize the identity recognition and has good resistance to the attackers. The WHMD only sends non-sensitive information packets and the channel characteristics at the time of transmission are unknown to it with minimum privacy at stack. The MS receives the channel characteristics sequences in the form of the RSSI stored randomly in the flash. It also ensures resistance against the attacks in the WBAN home health care scenarios. Furthermore, this method does not demand any hardware upgrades and no additional packet transmissions are required minimizing energy consumption.

These features make this method very suitable for low-power WBAN applications containing highly sensitive private data. Future aspects of this work include enhancement of the robustness of this method with added security of the WBAN applications.

References

[1] P. S. Hall and Y. Hao, *Antennas and Propagation for Body-Centric Wireless Networks*. Norwood, MA, USA: Artech House, 2006.

[2] Q. H. Abbasi, A. Sani, A. Alomainy, and Y. Hao, "On-body radio channel characterization and system-level modeling for multiband OFDM ultra-wideband body-centric wireless network," *IEEE Trans. Microw. Theory Techn.*, vol. 58, no. 12, pp. 3485–3492, Dec. 2010.

[3] M. Kim and J.-I. Takada, "Characterization of wireless on-body channel under specific action scenarios at sub-GHz bands," *IEEE Trans. Antennas Propag.*, vol. 60, no. 11, pp. 5364–5372, Nov. 2012.

[4] M. R. Kamarudin, Y. I. Nechayev, and P. S. Hall, "Onbody diversity and angle-of-arrival measurement using a pattern switching antenna," *IEEE Trans. Antennas Propag.*, vol. 57, no. 4, pp. 964–971, Apr. 2009.

[5] B. Sanz-Izquierdo, J. A. Miller, J. C. Batchelor, and M. I. Sobhy, "Dual-band wearable metallic button antennas and transmission in body area networks," *IET Microw., Antennas Propag.*, vol. 4, no. 2, pp. 182–190, Feb. 2010.

[6] S. Möller, T. Newe, and S. Lochmann, "Prototype of a secure wireless patient monitoring system for the medical community," *Sens. Actuators A, Phys.*, vol. 173, no. 1, pp. 55–65, Jan. 2012.

[7] N. K. Suryadevara, A. Gaddam, R. K. Rayudu, and S. C. Mukhopadhyay, "Wireless sensors network based safe home to care elderly people: Behaviour detection," *Sens. Actuators A, Phys.*, vol. 186, pp. 277–283, Oct. 2012.

[8] Y.-S. Shiu, S. Y. Chang, H.-C. Wu, S. C.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: A tutorial," *IEEE Wireless Commun.*, vol. 18, no. 2, pp. 66–74, Apr. 2011.

[9] *IEEE Standard for Local and Metropolitan Area Networks—Part 15.6: Wireless Body Area Networks*, IEEE Standard 802.15.6-2012, 2012, pp. 1–271.

[10] P. Kumar and H.-J. Lee, "Security issues in healthcare applications using wireless medical sensor networks: A survey," *Sensors*, vol. 12, no. 1, pp. 55–91, 2012.

[11] S. Rezvani and S. A. Ghorashi, "Context aware and channel-based resource allocation for wireless body area networks," *IET Wireless Sensor Syst.*, vol. 3, no. 1, pp. 16–25, Mar. 2013.

[12] S. T. Ali, V. Sivaraman, D. Ostry, G. Tsudik, and S. Jha, "Securing first-hop data provenance for bodyworn devices using wireless link fingerprints," *IEEE Trans. Inf. Forensics Security*, vol. 9, no. 12, pp. 2193–2204, Dec. 2014.

[13] W. Wang, Z. Wang, W. T. Zhu, and L. Wang, "WAVE: Secure wireless pairing exploiting human body movements," in *Proc. IEEE Trustcom/BigDataSE/ISPA*, vol. 1. Helsinki, Finland, Aug. 2015, pp. 1243–1248.

[14] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: Body area network authentication exploiting channel characteristics," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1803–1816, Sep. 2013.