sensors

MDPI

Letter

Patterns-of-Life Aided Authentication

Nan Zhao [1], Aifeng Ren [1], Zhiya Zhang [1], Tianqiao Zhu [1], Masood Ur Rehman [2], Xiaodong Yang [1,*] and Fangming Hu [1]

1 School of Electronic Engineering, Xidian University, Xi'an 710071, China; nan_zhao_@hotmail.com (N.Z.); afren@mail.xidian.edu.cn (A.R.); zhiyazhang@163.com (Z.Z.); tqzhu@mail.xidian.edu.cn (T.Z.); fangming95@163.com (F.H.)

2 Centre for Wireless Research, University of Bedfordshire, Luton LU1 3JU, UK; Masood.UrRehman@beds.ac.uk

* Correspondence: xdyang@xidian.edu.cn; Tel.: +86-29-8820-2830

Academic Editor: Kamiar Aminian

Received: 12 June 2016; Accepted: 20 September 2016; Published: 23 September 2016

Abstract: Wireless Body Area Network (WBAN) applications have grown immensely in the past few years. However, security and privacy of the user are two major obstacles in their development. The complex and very sensitive nature of the body-mounted sensors means the traditional network layer security arrangements are not sufficient to employ their full potential, and novel solutions are necessary. In contrast, security methods based on physical layers tend to be more suitable and have simple requirements. The problem of initial trust needs to be addressed as a prelude to the physical layer security key arrangement. This paper proposes a patterns-of-life aided authentication model to solve this issue. The model employs the wireless channel fingerprint created by the user's behavior characterization. The performance of the proposed model is established through experimental measurements at 2.45 GHz. Experimental results show that high correlation values of 0.852 to 0.959 with the habitual action of the user in different scenarios can be used for auxiliary identity authentication, which is a scalable result for future studies.

Keywords: Wireless Body Area Networks; initial trust; patterns-of-life aided authentication

1. Introduction

Recent years have seen a massive development of wireless sensors. This has enabled Wireless Body Area Networks (WBANs)/Wireless Body Sensor Networks (WBSNs) to become a key technology in real-time health monitoring of patients, providing effective detection and treatment of acute diseases [1–7]. It is envisioned that WBAN/WBSN will have an annual device shipment of 187.2 million units by 2020 [2,3]. The WBANs/WBSNs have successfully proceeded through the adoption phase devising efficient and flexible prototyping and management [8,9]. However, the potential of the WBANs/WBSNs is severely daunted by the challenges of security and privacy of the user's important personal information [10–13]. WBAN nodes need to be simple in hardware and interface due to form-factor, size and energy limitations. This decreases the scope of the traditional non-password authentication mechanisms that mostly require advanced hardware or major modifications to the system software [14]. On the other hand, Physical Layer Security (PLS) schemes are well suited in this scenario. This is due to the fact that the distance between two body-mounted sensor nodes is expected to be much smaller than the distance between a body-mounted sensor and an eavesdropping node in the patient-monitoring WBAN applications. This results in a maximum ambiguity to the eavesdropping party [15]. Although PLS key generation can ensure secrecy, it requires the node authentication as a prelude [16]. Therefore, establishing initial trust (iTrust) between the authentication node (AN) and wearable node (WN) acts as the fundamental step towards a WBAN physical layer security protocol.

Researchers have proposed various techniques in the literature to use the PLS for security and authentication [17–19]. Physical authentication through the actual positioning in wireless local area network is employed in [17]. Indoor space channel detection and ray-tracing tools are used to achieve authentication in [18] while identification and verification of the sender is attained through channel vector in [19]. Key distribution in WBANs has also been dealt in different ways [20,21]. Human body movement-aided authentication is also considered in [22,23] but the focus is on treating the human body motion as the source of jamming.

This study attempts to provide a novel solution to this problem using the patterns-of-life aided authentication model (PLAM) employing the wireless channel features to quantify a user's behavior habits as an authentication parameter. The wireless channel fingerprint formed by the characterization of user's behavior depicts the correlation between the AN and the WN. The WN is worn by the user while performing his daily life actions. The AN, placed at different positions in the vicinity, interacts with the WN automatically and generates a life pattern fingerprint for identification. This eradicates the need of a pre-distributed secure key and danger of lost key and a failed traditional authentication mechanism in the event of a stolen sensor node [14]. To the best of the authors' knowledge, this technique is novel and such a method is not being reported in the open literature.

Following the introduction, this paper is organized in four sections. Section 2 describes the experimental set-up to generate user's patterns-of-life data and presents measured data. Section 3 provides correlation analysis of AN and WN for establishing initial trust and authentication based on the observed patterns-of life. Conclusions and potential future work are provided in Section 4.

2. Experimental Set-up

This work considers the iTrust (initial-Trust) establishment in a WBAN where the user has worn the WN. The user could be stationary or mobile.

The measurements were carried out in a typical laboratory environment with dimensions of H × L × W = 3 m × 7.8 m × 10.8 m inside the new science and technology building at Xidian University. Four ANs installed in the tea table, attendance book, flowerpot and workshop were considered. Figure 1 shows the experimental setup with the ANs being represented by the numbers 1, 2, 3, and 4. The footprints illustrate the daily movement pattern of the user between the four spots. To prove the idea, a common experimental approach is adopted by taking the channel measurements while the user is performing four habitual actions. The daily life actions considered include (1) eating breakfast; (2) sign in to work; (3) watering the flowers and (4) go into operation, as shown in Figures 2 and 3. The users had the liberty to choose their pattern of the four activities initially. This pattern is termed as "template" and was being used for pre-registration. It forms the iTrust value for the ANs. The user is required to repeat the behavioral pattern maintaining the same sequence to ensure the authentication. Hence, if the wireless channel fingerprint of the user's behavior characterization between the AN and WN is found to be in line with the PLAM, the WN obtain an iTrust value is depicted as a check mark in Figure 2. Any drift from the behavioral pattern would result in a failed authentication.

The WBANs are no longer based on stand-alone devices but an integration of various portable electronics operating in the vicinity of the human body. To represent this integrated WBAN environment, the measurements were performed using HBE-Ubi sensor node in half-duplex, two packets per second mode. It sends and receives 36 packages and calculates received signal strength indicator (RSSI) as follows:

$$RSSI = P_{TX}\,(dBm) - PL\,(dBm) \tag{1}$$

$$AN_{RSSI} = WN_{RSSI} + SI + PoL \tag{2}$$

where $P_{TX}\,(dBm)$ is transmit power, $PL\,(dBm)$ represents path loss, SI is surrounding influence and PoL takes into account patterns-of-life radio frequency loss, respectively. The initial behavioral pattern

forms the fingerprint template while the successive actions need to follow this template in order to attain iTrust. The comparison of the template and the pattern of the user's successive movements is presented in Figure 4. The results show meaningful strong correlation between PLAM fingerprint (black line) and the user's movements (red line).

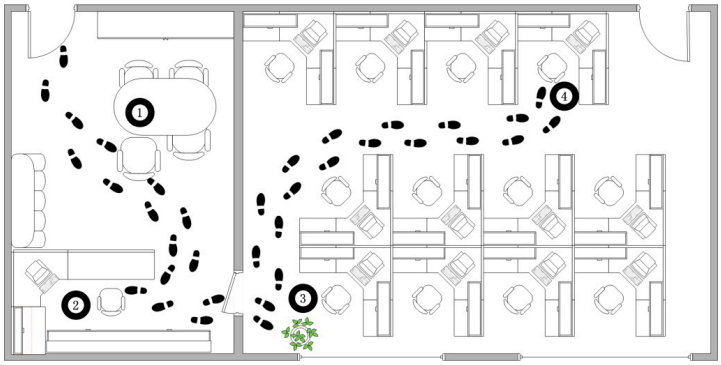

Figure 1. Experiment site map.

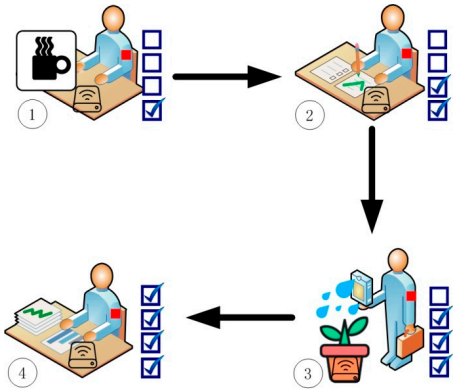

Figure 2. Considered user actions of (**1**) eating breakfast; (**2**) sign in to work; (**3**) watering the flowers and (**4**) go into operation.

Figure 3. Photos for four scenarios explained in Figure 2.

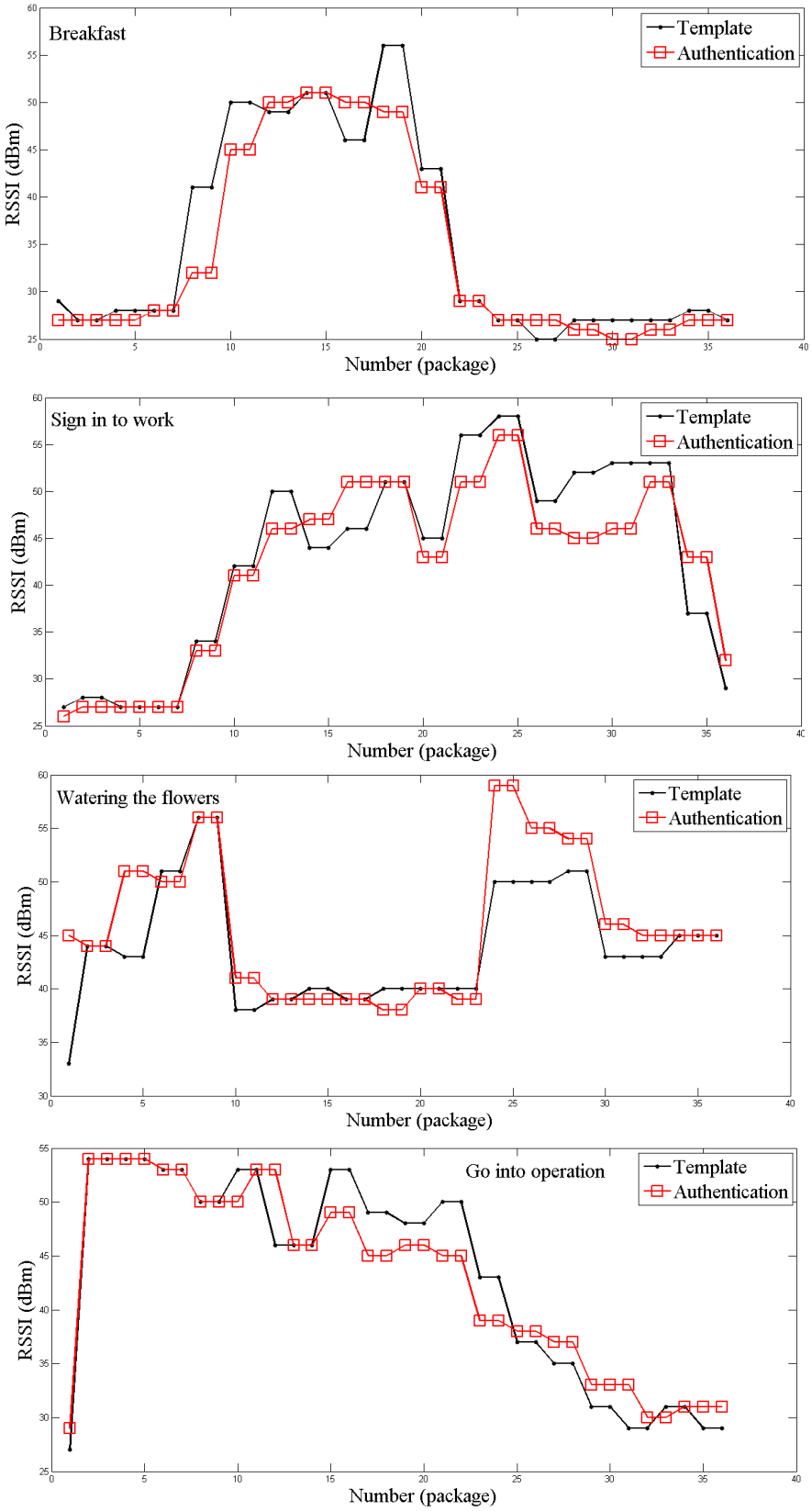

Figure 4. Comparison of measured initial trust (iTrust) and authentication data.

3. Analysis and Discussion

Measured data is used to establish correlation between the PLAM fingerprint and the user's movements in the four considered scenarios. Correlation coefficient values for the four configurations are given in Table 1. These results indicate that the high correlation between the two configurations can well serve the need of iTrust and authentication. As this study adopts a proof-of-concept approach, the measurement data sampling has been limited which can be extended further in practical implementations. It is, however, evident from the analysis of the measured data that even by using simple correlation, enough resolution has been attained to achieve identity authentication.

Table 1. Summary of correlation coefficients for the received signal strength indicator (RSSI) sequences in four measurement scenarios.

Scenario	Correlation Coefficient
Eating breakfast	0.959
Sign in to work	0.943
Watering the flowers	0.852
Go into operation	0.963

Figure 5 highlights the daily routine of the user obtained through the measurements. It is clear that the users were first eating breakfast, and then signing-in to work followed by watering the flowers and going into operation. The results also show that in this PLAM, a correlation coefficient value of $\geq$0.85 between the AN and WN will enable the AN to obtain the iTrust value.

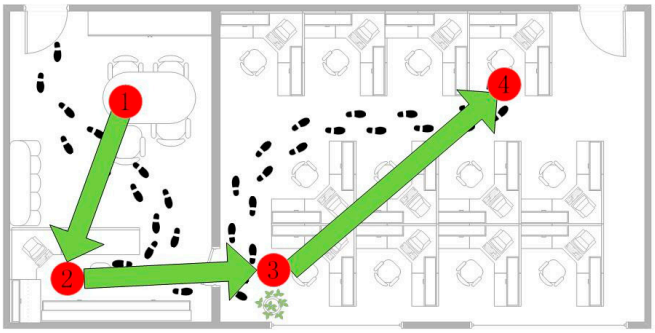

Figure 5. iTrust fingerprint according to user's behavior characterization.

The priori knowledge available to us in the PLS is that the distance between the nodes is greater than half a wavelength. The characteristics of the RSSI sequence make the measurements inaccurate if measured at a distance greater than the half wavelength. Therefore, the channel statistics can be regarded as independent of the distance. It implies that in a practical scenario, the attacker Eve cannot measure the channel between the legitimate users unless she intrudes into the house and successfully imitates the legitimate user's "pattern-of-life" (which is a far-fetched possibility). Hence, PLAM ensures the authentication.

Although, the experiment adopts a simple approach with four representative daily life scenes to establish the usability of the technique, the use of channel characterization of human behavior to achieve identity authentication can be easily expanded to any scene. Moreover, this technique consumes no additional packages. Authentication is extracted from the RSSI sequence of packets required for normal communication between the WBAN nodes such as time alignment, power monitoring, etc. In fact, the proposed technique does not require any communication packet but achieve authentication through the observation of the changes in the channel conditions due to the interaction between the human body and the surrounding environment.

The results of these initial experiments clearly show that the use of the PLAM in the WBAN applications provides a viable authentication solution. The results presented in this paper are in-line with the foundings of other researchers where the human body movement pattern is considered as unique, stable and distinguishable to be used for the node authentication [23–25]. Wang et al. have considered the effects of body motion as a noise into the system [23]. Wu et al. have considered the authentication between the body-mounted nodes, which are not more than 0.2 m apart [24]. In [25], locking/unlocking a smart phone by a specific hand waving pattern is evaluated. However, as the presented technique is a novel approach in the WBANs and no such authentication method has been reported, we cannot provide a performance comparison at this point.

4. Conclusions

Establishing an initial trust between the WBAN nodes is a prelude to the physical layer authentication method. This paper has presented a method of establishing initial trust in the WBAN nodes by characterization of human behavior and its comparison with the PLAM fingerprint. The study has shown that the initial trust with user's patterns-of-life can be achieved that can reduce the consumption of communication packages to minimum which is much valuable for the resource constrained WBAN systems. A preliminary PLAM model has been developed to realize auxiliary status recognition using patterns-of-life through multiple authentication nodes acquiring initial trust value. The working of the model has been evaluated through measurements providing a preliminary implementation of the PLAM multi-node initial trust identification using a HBE-Ubi-Sensor node module. Experimental results show that users can obtain a high correlation value of 0.852 to 0.959 by following a set pattern for their daily activities in different scenarios enabling authentication and effectively removing contingency, which is a scalable result.

Future work will focus on the PLAM fingerprint optimization and iTrust establishment without use of a template. Moreover, proving security against a reasonable adversarial model is also an aspect of future work.

Acknowledgments: The authors would like to thank the reviewers and the editor for their valuable comments. This work was supported in part by the National Natural Science Foundation of China under Grant 61671349, in part by the Fundamental Research Funds for the Central Universities, in part by the China Postdoctoral Science Foundation, and in part by the Postdoctoral Research Projects Funded in Shaanxi Province.

Author Contributions: Nan Zhao, Xiaodong Yang conceived and designed the experiments; Nan Zhao performed the experiments; Nan Zhao analyzed the data; Nan Zhao contributed reagents/materials/analysis tools; Nan Zhao, Aifeng Ren, Zhiya Zhang, Tianqiao Zhu, Masood Ur Rehman, Xiaodong Yang, Fangming Hu wrote the paper.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Hall, P.S.; Hao, Y. *Antennas and Propagation for Body-Centric Wireless Networks*, 2nd ed.; Artech House: Norwood, MA, USA, 2012.
2. Abbasi, Q.H.; Ur Rehman, M.; Qaraqe, K.; Alomainy, A. *Advances in Body-Centric Wireless Communication: Applications and State-of-the-Art*; The IET: London, UK, 2016.
3. Rehman, M.U.; Gao, Y.; Wang, Z.; Zhang, J.; Alfadhl, Y.; Chen, X.; Parini, C.G.; Ying, Z.; Bolin, T. Investigation of on-body bluetooth transmission. *IET Microw. Antennas Propag.* **2010**, *4*, 871–880. [CrossRef]
4. Movassaghi, S.; Abolhasan, M.; Lipman, J.; Smith, D.; Jamalipour, A. Wireless body area networks: A survey. *IEEE Commun. Surv. Tutor.* **2014**, *16*, 1658–1686. [CrossRef]
5. Kartsakli, E.; Lalos, A.S.; Antonopoulos, A.; Tennina, S.; Renzo, M.D.; Alonso, L.; Verikoukis, C. A survey on M2M systems for mHealth: A wireless communications perspective. *Sensors* **2014**, *14*, 18009–18052. [CrossRef] [PubMed]
6. Masse, F.; Gonzenbach, R.; Paraschiv-Ionescu, A.; Luft, A.; Aminian, K. Wearable barometric pressure sensor to improve postural transition recognition of mobility-impaired stroke patients. *IEEE Trans. Neural Syst. Rehabil. Eng.* **2016**. [CrossRef] [PubMed]

7. Pichonnaz, C.; Duc, C.; Gleeson, N.; Ancey, C.; Jaccard, H.; Lécureux, E.; Farron, A.; Jolles, B.M.; Aminian, K. Measurement properties of the smartphone-based B-B score in current shoulder pathologies. *Sensors* **2015**, *15*, 26801–26817. [CrossRef] [PubMed]
8. Fortino, G.; Giannantonio, R.; Gravina, R.; Kuryloski, P.; Jafari, R. Enabling effective programming and flexible management of efficient body sensor network applications. *IEEE Trans. Hum. Mach. Syst.* **2013**, *43*, 115–133. [CrossRef]
9. Galzarano, S.; Giannantonio, R.; Liotta, A.; Fortino, G. A task-oriented framework for networked wearable computing. *IEEE Trans. Autom. Sci. Eng.* **2016**, *13*, 621–638. [CrossRef]
10. Saleem, S.; Ullah, S.; Kwak, K.S. A study of IEEE 802.15.4 security framework for wireless body area networks. *Sensors* **2011**, *11*, 1383–1395. [CrossRef] [PubMed]
11. Kuryloski, P.; Pai, S.; Wicker, S.; Xue, Y. MedSN system for in-home patient monitoring: Architecture, privacy and security. In Proceedings of the 2007 HCMDSS-MDPnP, Joint Workshop on High Confidence Medical Devices, Software, and Systems and Medical Device Plug-and-Play Interoperability, Boston, MA, USA, 25–27 June 2007; pp. 189–191.
12. Mainanwal, V.; Gupta, M.; Upadhayay, S.K. A survey on wireless body area network: Security technology and its design methodology issue. In Proceedings of the 2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS), Coimbatore, India, 19–20 March 2015; pp. 1–5.
13. Kumar, P.; Lee, H.-J. Security issues in healthcare applications using wireless medical sensor networks: A survey. *Sensors* **2012**, *12*, 55–91. [CrossRef] [PubMed]
14. Shi, L.; Li, M.; Yu, S.; Yuan, J. BANA: Body area network authentication exploiting channel characteristics. *IEEE J. Sel. Areas Commun.* **2013**, *31*, 1803–1816. [CrossRef]
15. El Gamal, A.; Koyluoglu, O.O.; Youssef, M.; El Gamal, H. Achievable secrecy rate regions for the two-way wiretap channel. *IEEE Trans. Inf. Theory* **2013**, *59*, 8099–8114. [CrossRef]
16. Ali, S.T.; Sivaraman, V.; Ostry, D. Eliminating reconciliation cost in secret key generation for body-worn health monitoring devices. *IEEE Trans. Mob. Comput.* **2014**, *13*, 2763–2776. [CrossRef]
17. Bhargava, V.; Sichitiu, M.L. Physical authentication through localization in wireless local area networks. In Proceedings of the GLOBECOM '05, IEEE Global Telecommunications Conference, St. Louis, MO, USA, 28 November–2 December 2005.
18. Xiao, L.; Greenstein, L.J.; Mandayam, N.B.; Trappe, W. Using the physical layer for wireless authentication in time-variant channels. *IEEE Trans. Wirel. Commun.* **2008**, *7*, 2571–2579. [CrossRef]
19. Pei, C.; Zhang, N.; Shen, X.S.; Mark, J.W. Channel-based physical layer authentication. In Proceedings of the 2014 IEEE Global Communications Conference, Austin, TX, USA, 8–12 December 2014; pp. 4114–4119.
20. Sampangi, R.V.; Sampalli, S. Butterfly encryption scheme for resource-constrained wireless networks. *Sensors* **2015**, *15*, 23145–23167. [CrossRef] [PubMed]
21. Liu, D.; Ning, P.; Du, W. Group-based key predistribution for wireless sensor networks. *ACM Trans. Sens. Netw.* **2008**, *4*. [CrossRef]
22. Shi, L.; Yuan, J.; Yu, S.; Li, M. MASK-BAN: Movement-aided authenticated secret key extraction utilizing channel characteristics in body area networks. *IEEE Internet Things J.* **2015**, *2*, 52–62. [CrossRef]
23. Wang, W.; Wang, Z.; Zhu, W.T.; Wang, L. WAVE: Secure wireless pairing exploiting human body movements. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; pp. 1243–1248.
24. Wu, Y.; Wang, K.; Sun, Y.; Ji, Y. R2NA: Received Signal Strength (RSS) ratio-based node authentication for body area network. *Sensors* **2013**, *13*, 16512–16532. [CrossRef]
25. Yang, L.; Guo, Y.; Ding, X.; Han, J.; Liu, Y.; Wang, C.; Hu, C. Unlocking smart phone through hand waving biometrics. *IEEE Trans. Mob. Comput.* **2015**, *14*, 1044–1055. [CrossRef]