ISBN 978-981-11-0008-6
Proceedings of 2016 6th International Workshop on Computer Science and Engineering (WCSE 2016)
Tokyo, Japan, 17-19 June, 2016, pp. 618-621
doi: 10.18178/wcse.2016.06.107

Virtual Node Based Location Privacy Protection in Wireless Body Sensor Networks

Lan Yao [1+], Aiyun Yan [2] and Fuxiang Gao[1]

[1] School of Computer Science & Engineering, Northeastern University, China
[2] School of Information Science & Engineering, Northeastern University, China

Abstract. In a wireless body area sensor network (WBAN), biosensor is used to collect the medical data. Data confidentiality is one of the crucial issues for WBAN application, many cryptography techniques are researched to achieve it. However, the adversary can obtain some important information by eavesdropping the pattern of data transmission without detecting the context of data. In addition, the adversary can also infer the location according to the Received Signal Strength Indication (RSSI) values received. In this paper, based on our previous work--PAS, we propose a coordinator for further location privacy protection. This coordinator is a virtual node which has leverage on RSSI values and discombobulates the signals that the adversary receives. The experimental results show that the coordinator protects WBAN users from differential RSS attack and the energy consumption is reasonable.

Keywords: virtual node; location privacy protection; WBAN; differential RSS

1. Introduction

With the development of technology, Wireless Body Area Network (WBAN) has been used widely to monitor the medical data from patients and transmit the data to a data server. The importance of such systems is further underscored by current demographic, social, and economic trends . WBAN can achieve real-time data collection, reduce cost and decrease hospital visiting times.

WBAN is more vulnerable to passive attacks than active attacks, because active attacks can be prevented by carefully designing and deploying data encryption and authentication methods. However, passive attacks can also infer the type of the biosensor by only eavesdropping the transmission pattern although the data are encrypted. Although we can resist passive attacks, the adversary can also locate the patient's position by analyzing spatial variance of the signal strength and applying location techniques, which will leak the location privacy of the patients.

To confront attacks of transmission pattern detection and location detection, we design a strategy -- PAS (Power Adjustment Scheme) by separating all original packets into fixed cell-packets and synchronize all sensors' transmission [1]. In this paper, we install a coordinator in a fixed position near to the patients. Because of the cell-packets, the coordinator can send data in a synchronized way with the biosensors, which will affect the signals uniformly.

The paper is organized as follows. In Section II, we introduce the related works. The VirLoc design is introduced in Section III. Finally, we draw conclusions in Section IV.

2. Related Works

Sometimes a simple eavesdropping attack will reveal the data or the pattern of data collection, which in turn could breach the security and privacy of WBAN applications [1]. Recently, many novel approaches [2]

+ Corresponding author. Tel.: +8613066600872.
E-mail address: yaolan@mail.neu.edu.cn

[4][6][8] have been proposed. [1] presents a regulator so that the transmission pattern between biosensors and the sink is shielded from attackers. Moreover, with the help of RSSI, the adversary may locate them by signal detection. Sangho [3] has proposed an approach of Randomize Transmission Power to adjust the RF levels under the assurance of connection rate, therefore the RSSI values received by the adversary will change although the target patient is actionless.

Transmission power randomization [5] can throw off standard localization systems, but localization algorithms could easily filter out such changes. Hence, Sangho [3] has proposed a novel approach Phantom to allow mobile devices thwart unauthorized adversary's location tracking by creating forged locations. Phantom creates a number of forged locations around the true locations of patients to provide privacy protection.

3. VirLoc Design

3.1. Adversary Localization

Based on the regulator, all sensors send packets in the way of cell-packets.As shown in Fig. 1, A is the patient with biosensors which send cell-packets to the sink. The adversaries use RSS-based fingerprinting[7] technique to locate the patients.

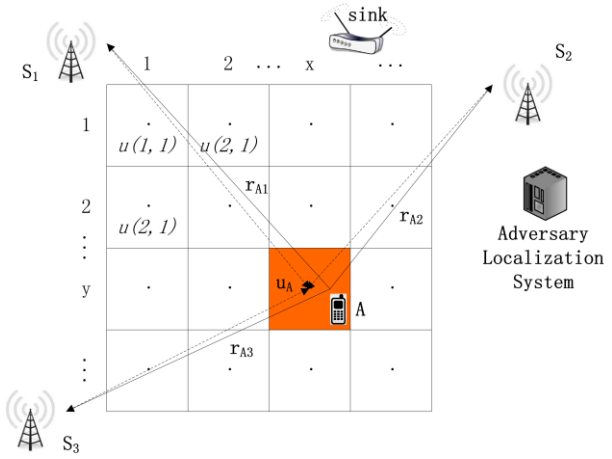

Fig. 1: Adversary's tracking.

The adversary localization system runs three radio signal sensors, S = {S_1, S_2, S_3}, to measure the signal strength from A. We divide the whole area into many small squares whose centres are the reference locations u (x, y), i ∈ C, where C is reference location set. We define RA as the signal strength received by sensors in S, R_A = {r_{A1}, r_{A2}, r_{A3}}. We assume that the adversary localization system has obtained a RSS signature database[3]. In this database, each reference location corresponds to a set of RSS values, R_U = {r_1, r_2, r_3}. The adversary localization system minimizes the mean square error (arg mini$\|R_A-R_U\|^2$, i ∈ C), and regards the location of R_U as the location of A, u_A. A can randomize its transmission power to cause errors in the mean square error estimation, but the adversary could easily find a factor of R_A to filter out the changes[3].

3.2. VirLOC Design

1) Coordinator design

We deploy a sensor B as a coordinator at a fixed position sending packets at the same frequency and length with those from biosensors (in the way of cell-packets). We assume that B does not have limitation on power consumption, so it can work continuously.

Given that all the biosensors send packets at the same frequency and length, therefore the signal received at an adversary sensor is the convolution of A's and B's signals. As shown in Fig.2, the signal strength of A received by S_1 is r_{A1}, received by S_2 is r_{A2}, received by S_3 is r_{A3}. Similarly, the signal strength of B received by S_i are r_{B1}, r_{B2} and r_{B3} respectively. We define r_{AB1} as the final signal received by S_1, which is the convolution of r_{A1} and r_{B1}. The same goes to r_{AB2} and r_{AB3}. Base on R_{AB} = {r_{AB1}, r_{AB2}, r_{AB3}}, the adversary localization system compare R_{AB} and R_U in its RSS signature database and finally obtains the forged location,

G.

2) Security analysis

As shown in Fig. 3, the cooperation of A and B leads a different signal vector R_G from R_A to the adversary and the results of $\|R_A\text{-}R_G\|^2$ is the forged location u_G. Because A (the patient) is mobile, while B is actionless, this approach can create different forged locations, which causes confusion about the number of real transmitters and their locations.

Recall that when there is only A, though A varies its RF level, the adversary localization system can find a factor to filter out the changes, that is it can expand or shrink the received RSSI values simultaneously to find A's location. However, when we deploy a coordinator B in the neighbourhood of A, B places a shift in RSSI at each eavesdropping sensor. The shifts have different influence on each sensor, including direction and magnitude. Thus, the adversary location system must adjust three different factors to determine A's location, which is almost impossible.

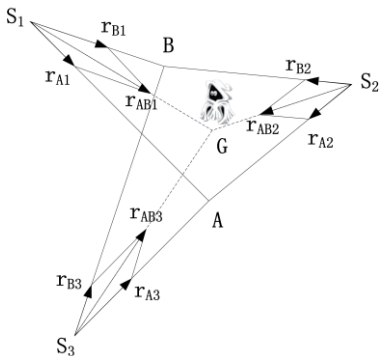

Fig. 2: Adversary's tracking offset, when the coordinator installed.

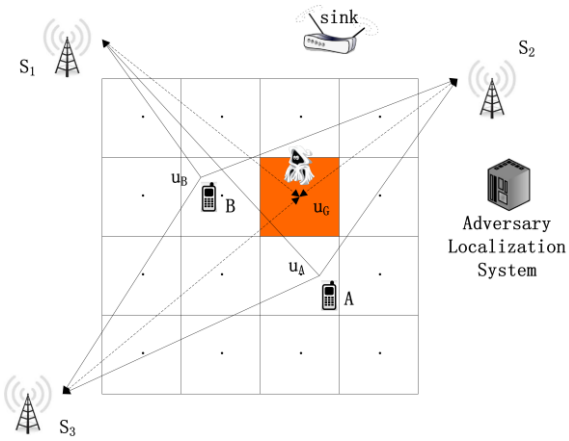

Fig. 3: Forged location that adversary localization system detects.

At present, the propagation models of the wireless signal strength attenuation are mainly Free-space model, Two-ray ground reflection model and Shadowing model. However, the first two models are too idealistic. So in this paper, we choose Shadowing model because it is widely used.

The equation of Shadowing model is [10]:

$$\left[\overline{p_r(d)}\right]_{dBm} = \left[p_r(d_0)\right]_{dBm} - 10*n*\lg(\frac{d}{d_0}) + X_{dBm} \tag{1}$$

where d is the distance between the sender and the receiver, d_0 is the reference distance (m), generally is 1m, $\overline{p_r(d)}$ is the received signal power (d_{Bm}), $\overline{p_r(d_0)}$ is the received signal power (d_{Bm}) at the reference distance d_0, X_{dBm} is the Gaussian random variable whose average value is 0, n is the Path Loss Exponent which depends on the surroundings and the type of a building.

In reality, we use simplified Shadowing model, that is

$$\left[\overline{p_r(d)}\right]_{dBm} = \left[p_r(d_0)\right]_{dBm} - 10*n*\lg(\frac{d}{d_0}) \tag{2}$$

And generally, we choose d_0=1m, so we get the RSSI range formula in a practical application as follows

$$\left[RSSI\right]_{dBm} = \left[\overline{p_r(d)}\right]_{dBm} = A - 10*n*\lg d \tag{3}$$

where A is the received signal power (d_{Bm}) at a distance of 1m.

Reference [9] shows some actual measured values in some references. As the patients are in buildings, we define A as -45 d_{Bm} and n as 2. So the RSSI range formula is

$$f(d) = RSSI = -45 - 20*\lg d \tag{4}$$

As mentioned before in this paper, the signal received at an adversary sensor is the convolution of the two signals. Each received signal strength meets the RSSI range formula, so we use convolution formula as

follows to calculate the signal received at the adversary sensor.

The convolution is

$$y(t)=\int_{-\infty}^{\infty}\left(x(p)*h(t-p)\right)dp \tag{5}$$

The following is the calculating process of the convolution

$$y(d)=\int_{0}^{d}\left((-45-20*\lg\tau)*\left(-45-20*\lg(d-\tau)\right)\right)d\tau \tag{6}$$

The formula after convolution is

$$f(d)=2025*d+1800/\ln 10*d*\ln d-1800/\ln 10*d \tag{7}$$

4. Conclusions

The vulnerability of wireless communication brings challenges for location privacy protection to WBAN. Based on our former work, packets have been synchronized as cells and they are sent synchronously in time, a coordinator which sends same cells as bio-sensors is substantially feasible to be installed near to the bio-sensors to generate interference signals. This paper addresses the design of the coordinator and discusses its effects on RSSI values so as to resist the differential RSS attack. Our experiments show that the coordinator effectively provides location privacy for sensor nodes in a WBAN and the energy overhead is overall acceptable.

5. Acknowledgements

This research is supported by the National Natural Science Foundation of China under Grant No. 61173027 and the Fundamental Research Funds for the Central Universities (N140404006, N130316001).

6. References

[1] Yao L. & Li X. & Yu G. Pattern regulator: protecting temporal usage privacy for wireless body area sensor networks. *IEEE 33rd International Conference on Distributed Computing Systems Workshops (ICDCSW)*, 2013, pp. 327-332.

[2] Ameen M. A. & Liu J.E. & Kwak K. Security and privacy issues in wireless sensor networks for healthcare applications. *Journal of medical systems.* 2012, 36(1): 93-101.

[3] Sangho Oh & Tam Vu & Marco Gruteser & Suman Banerjeey. Phantom: physical layer cooperation for location privacy protection. *The 31st Annual IEEE International Conf. on Computer Communications: Mini-Conference (INFOCOM)*, 2012, pp. 3061-3065.

[4] Jiang T. & Wang H. J. & Hu Y. C. Preserving location privacy in wireless LANs. *Proc of the Conf. on Mobile systems, applications and services*:, 2007, 246-257.

[5] Later B. B. & Braem B. & Moerman I. & Blondia C. & Demeester P. A survey on wireless body area networks. *Wireless Networks*. 2007, 17(1): 1-18.

[6] Ko J. & Lim J. & Chen Y. & Musvaloiu R. & Terzi A. s & Masson G. & Gao T. & Destler W. & Selavo L. & Dutton R. Medisn: medical emergency detection in sensor networks. *ACM Transactions on Embedded Computing Systems (TECS).* 2010, 10(1): 11-25.

[7] Bacak A. & Bolumu B. M. & Enstitusu G. Y. T. & Celebi H. Practical considerations for RSS RF fingerprinting based indoor localization systems. *2014 IEEE 22nd Signal Processing and Communications Applications Conference*, 2014, pp. 497-500.

[8] Sugano M. & Kawazoe T. & OhtY. a & Murata M. Indoor localization system using rssi measurement of wireless sensor network based on zigbee standard. *Target.* 2011, 538: 50.

[9] Fu X. & Peng B. Research on the location of wireless invading host based on Shadowing model. *Micro Electronics and Computer*. 2010, 27(12): 4-9.

[10] Zhang J. & Zhang L. & Ying Y. & Gao F. Research on distance measurement based on RSSI of ZigBee. *Chinese journal of sensors and actuators*. 2009, 22(2): 285-288.