Integrated Node Authentication and Key Distribution Method for Body Area Network

Zhouzhou Li & Hua Fang
University of Massachusetts Dartmouth
Email: zli1@umassd.edu, hfang2@umassd.edu

Honggang Wang
University of Massachusetts Dartmouth
Email: hwang1@umassd.edu

***Abstract*—Node Authentication and Key Distribution are two tightly correlated security tasks for a secure Body Area Networks (BAN) system. Handling them separately may cause many practical issues. Based on the recent advances on node authentication and (shared) key distribution (including key generation), we propose a new integrated method to securely and efficiently conduct the two tasks. We build a system model with the consideration of passive and active attacks and solve some security risks. One of performance metric, key generation rate is significantly improved in our method. We implement and verify the proposed methods on two test beds. The experimental result demonstrates the effectiveness and efficiency of our proposal.**

***Index Terms*—Body Area Network (BAN), Node Authentication, Key Generation, Key Distribution, Received Signal Strength Indicator (RSSI)**

I. Introduction

Body Area Network (BAN), due to its small size, flexible configuration, and convenient deployment, has been widely used in healthcare, sports, military, entertainment fields. Nowadays the main challenge it is facing is its security. Fail to solve the security problem will directly affect its further development, promotion and deployment. Detail security tasks include node authentication, key distribution (including key generation), message encryption and encryption algorithms. Among them, key distribution, especially shared key distribution, is subject to incur attacks because it is lack of strong protection mechanisms. Node authentication is a prerequisite for key distribution, and the relationship between the two tasks is very close.

Most of the existing studies have focused on node authentication or key distribution separately, but rarely studied them comprehensively. This isolated situation led to many practical issues, such as heterogeneous modules, models, and algorithms deal with these two tasks, but they are forced to work together closely, resulting in a lot of incompatible operations, contradictory interaction and inevitable interference, which greatly affects the availability, efficiency and security of the system. On the other hand, users expect use BAN seamlessly over these technology gaps and reduce the human intervention and manual operation, which also puts high demands on BAN design to integrate and simplify the procedures.

Luckily, recent studies on node authentication and shared key distribution for BAN have achieved inspiring progresses respectively. That makes the integration of the two tasks feasible and provides a number of potentially good suggestions in this direction. Proximity-based authentication is promising in node authentication because it greatly simplify the design based on the reasonable assumption that the attackers usually are hard to approach very closely to the target BAN like legitimate nodes. A further progress is exploiting Received Signal Strength Indicator (RSSI), the standard interface of most wireless equipment, to decide the proximity of a node. To increase the accuracy of RSSI-based proximity detection, special tools with more than two RSSI measuring points were invented [1], [2]. On the other hand, studies showed the physical layer security is promising for shared key generation and distribution in BAN because both sides in communication can securely collect similar physical layer signal (reciprocity of their wireless channel) as the source of their shared key and substantially make the task of key generation and distribution a local activity. A further progress is utilizing RSSI as the mutual source of the shared key [3]. To increase the key generation density, node-cooperative methods were proposed [4], [5].

This paper studies a secure, efficient, and user-friendly approach to integrate the tasks of node authentication and key distribution for BAN. Its major contributions are:

- Only uses ordinary Commercial Off-The-Shelf (COTS) devices;
- Minimize user operation via seamlessly integrating node authentication and key distribution for newly introduced node;
- increasing the key generation rate.

The rest of the paper is organized as follows: Section I reviews the literature, especially on the RSSI-based node authentication and shared key distribution methods. Section II presents new integrated node authentication and shared key distribution methods. Section III evaluates the security and efficiency of the new method on different test beds with consideration of passive and impersonation attacks. and Section IV concludes the paper and gives the direction for future work.

II. Related Work

The Out-of-Band (OOB) authentication refers to the usage of other channel to distribute secret key that is used to protect the primary channels communication. No matter what OOB method is used (wired, visual, audible, spectral, etc.,) usually it requires extra hardware and additional software development [6]–[9].

978-1-5386-9223-3/19/$31.00 ©2019 IEEE

The In-Band authentication requires less hardware and software resource, therefore it is more common in BAN environment. Among so many In-Band authentication methods [10], the proximity-based ones are promising to BAN because during node authentication (a small time window), the attacker usually cannot approach to the authenticator(s) timely like the legitimate nodes. This assumption greatly simplified the node authentication process.

Behind the proximity-based authentication, the location techniques form its basis [11], [12]. In comparison with Angle of Arrival (AOA), Time of Arrival (TOA), and Time Difference of Arrival (TDOA), the RSSI-based technique is more attractive because RSSI is a standard interface that can be found in most wireless devices without additional cost, which makes it more suitable in the BAN environment where nodes are mostly resource-limited [13], [14]. One shortage of the RSSI based technique is its accuracy [15]–[17]. To overcome this issue, multiple antennas were used to measure one signal, then compensate the variations [18].

To the best of our knowledge, the first article covering both node authentication and key distribution for BAN is [1]. It exploited a special Control Unit (CU), which has two spatially separated antennae, to derive big RSSI gaps between the two antennae for nearby devices, and derive small RSSI gaps for far-away devices, so that it can distinguish between the nearby and far-away devices. Also, it utilizes the spatial diversity of the two antennae to derive '0' or '1' value from each RSSI measurement, that is one shared bit is derived per RSSI measurement. It reveals the two characteristics of wireless signal: attenuation and reciprocity, which can be used in consistent and simultaneous node authentication and key distribution.

In [2], following a similar idea, the authors presented an IoT authentication tool, Wanda, which is a wand equipped with two spatially separated antennae in a line. The wand can distinguish a nearby device from far-away devices by exploiting the gap caused by signal strength measurements between the two antennae. And the wand is used to impart '0' or '1' to the new node via different antenna (unidirectional, no exchange), that is one shared bit is imparted per wireless signal. Although it was designed for IoT devices, adaption may be needed for BAN devices;

RSSI is a channel level information, which varies with variation of sending energy, propagation path, medium attenuation, noise, and interference [4]. That means it contains plenty information entropy [5]. Deriving only one bit from every RSSI measurement [1], [2] obviously wastes much capacity. In another word, the quantification granularity is over coarse. If a method can derive more bits from a measurement, the key generation rate will tremendously raise and the key distribution time will greatly reduced, which shall benefit both the efficiency and security of key distribution.

We seek a new way fully utilizing the existing legitimate nodes of a target BAN, removing the constraints of the special hardware and inter-antennae distance, and solving some practical issues. Furthermore, we would like to increase the efficiency and security of key generation and distribution by deriving more bits per RSSI measurement. In section 3.2, there are figures for us to explain the difference between [1], [2] and our new method.

III. Proposed Methods

In this article, we propose a new dual antennae based method, which only relies on the existing legitimate nodes to secure the node authentication and key distribution for the newly introduced node.

A. System Model and Assumptions

Fig. 1 shows our simplified system model without loss of generality. In the range of a BAN, there are multiple existing legitimate nodes, and two authenticators. One authenticator is called Authentication Master (AM) and the other is called Authentication Assistant (AA). They cooperate to achieve node authentication and key distribution for a New Node (NN). AM can freely move. And it can promote an existing legitimate node to AA. Control Unit (CU) of the BAN could act as the AM. AA is fixed because it is an existing legitimate node, it just temporarily assists AM for the authentication task. Before authentication, NN should be physically placed in the target body area and fixed there. Therefore, the distance between NN and AA is stable. AA is used to guarantee the stability of this dimension. When AM is moving, it cause some uncertainty to the attackers. AM is used to guarantee the uncertainty of another dimension. When AM moves closely to NN, the signals sent by NN can cause big RSSI measurement gap between the two authenticators, that will be the third dimension to decide the proximity of NN. The attackers need to cheat the authenticators from 3 dimensions at the same time without exposing themselves - this will be much more secure than the basic methods, which only relied on the measurement gap dimension. To include security considerations in our system mode, outside of the BAN, we put passive attackers (e.g., eavesdroppers) and active attackers (e.g., impersonators) around the BAN trying to break its security. The harm of passive attacks is more serious than imagined. First, a passive attacker only receives information and does not send out information, so it is hard to detect. Second, many active attack methods rely on information collected in advance by the passive attack. When we say a system is secured, first it should be able to resist passive attack. That is also the reason we include passive attackers in our model. There are many active attack methods, each of which needs an unique defense mechanism. Due to space limitations, we only analyze the defense against impersonation attacks in this article by putting impersonators in our system model.

Without loss of generality, some reasonable assumptions are taken in this article:

- A legitimate device in a BAN is expected to be resource constraint with limited computing capacity, power duration, and communication facility. We assume a BAN device only has one antenna.

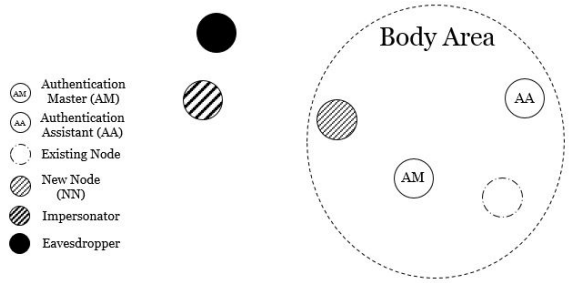

Fig. 1. Simplified System Model

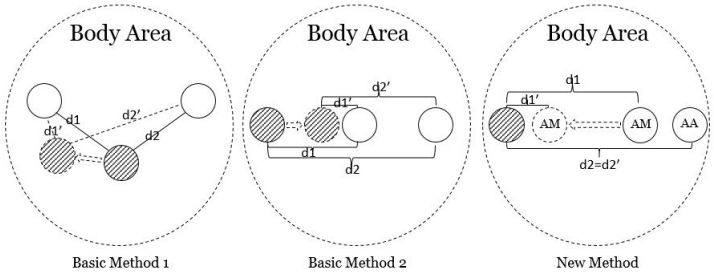

Fig. 2. Three types of models

- An authenticated legitimate nodes in the target BAN can set up and maintain a secured wireless connection/link to the AM for secured communication. AM can promote it to AA.
- Only AM (usually acted by CU) can freely move. Other nodes in the target BAN are fixed.
- To get authenticated, NN should be physically placed in the body area first. Attackers can not approach to the target BAN as closely as the legitimate nodes and NN.
- We say an impersonator fails if it exposed itself to AM or AA (this constrains the impersonators power to a reasonable level)

B. A New Proximity-based Authentication Method

Fig. [**?**] shows the configurations and theory of basic method 1 [1], basic method 2 (the equivalent of the method adopted by [2]), and our new method.

Basic Method 1: NN has distances d_1 and d_2 to the two authenticators. When it moves closely to one of the authenticator, the new distance ratio $d_2'/d_1' >> d_2/d_1$. Far-away node including impersonators cannot cause such big distance ratio.

Basic Method 2: NN is in the line of the two authenticators. It has distances d_1 and d_2 to the two authenticators. When it moves closely to the nearby authenticator, the new distance ratio $d_2'/d_1' >> d_2/d_1$. Far-away node including impersonators cannot cause such big distance ratio.

New Method: NN and AA are fixed in their positions. AM is in the line of NN and AA. AM moves to NN to cause $d_2'/d_1' >> d_2/d_1$. Far-away node including impersonators cannot cause such big distance ratio.

The three methods follow the same theory. The major difference is the two basic methods fix the inter-authenticator distance d and satisfy $d > \frac{\lambda}{2}$, which reflects to the hardware constraint. The new method does not require the two authenticators (AM and AA) keeping their distance, they rely on secure link to cooperate, which in fact removes the hardware constraint.

Compared to the two basic methods, our proposed method has advantages:

- The basic methods require a special authenticator hardware with two spatially separated antennae and $> \frac{\lambda}{2}$ inter-antennae distance.
- When users introduce a NN to a BAN, the NN is expected to stay there without moving. Both basic methods require NN moving.
- Stable d_2 in the new method reflects the real BAN condition - existing legitimate nodes and NN are fixed.
- Stable d_2 in the new method can raise the difficulty for impersonators to cheat AA - if impersonators move intensely (to achieve some fake effect), then it may cause unstable d_2. In another word, stable d_2 limits the impersonators' activity.
- Later for key distribution (including key generation), the uncertain d_1 can cause much higher information entropy, which implies much higher key generation rate.

To implement the theory, RSSI can be used to represent the inter-node distance. Here we can simply treated RSSI as the logarithmic distance. The basic steps of the new method are shown as follows:

1) Physically place the NN to the target body area.
2) AM promotes an existing node to a AA if the existing node is near to the NN and it is not overloaded.
3) NN starts to periodically broadcast authentication frames. Except the frame type and source MAC, no real data is encapsulated in the frames. Both AM and AA will measure the RSSI values of the authentication frames to estimate distances d_1 and d_2.
4) AM shares its RSSI measurements with AA via the secured link. Then AA can calculate the measurement gap (i.e., distance ratio) to decide the proximity of NN.
5) AM moves from AA to NN to cause big RSSI measurement gap. When AA detects this condition, the authentication is passed.

C. An Integrated pproach for Key Distribution

Since AM can freely move, its distance to NN, d_1, varies dynamically. When NN sends out the authentication request frames, AM can measure the frames and share the measurements to AA. The measurement values depend on d_1. On the other hand, NN can also measure the frames carrying the shared measurements from AM although NN cannot interpret the higher layer data. The measurement values also depend on d_1. If AM immediately shares its measurement as it receives a request frame, the interval between NN sending out a request frame and receiving the corresponding sharing frame should be very short. That means d_1 did not get time to change much. So the two measurements should be similar. Fig. 6 shows an example of RSSI values measured by NN (green

curve) and AM (blue curve) when they 'exchange' frames every 200ms and AM responds without delay. By calculating the correlation coefficient between the NN and AM curves, we quantify their similarity, that is 0.9861 in time domain. If we apply Discrete Cosine Transform (DCT) to both curves, their DCT'ed curves have a higher correlation coefficient 0.9950 in frequency domain. As a summary, they are very similar as expected. The bursts in Fig. 3 with RSSI value equal to -128 caused by missing frames (for some unknown reason), which will need special handling. However, we will not cover it here in this paper.

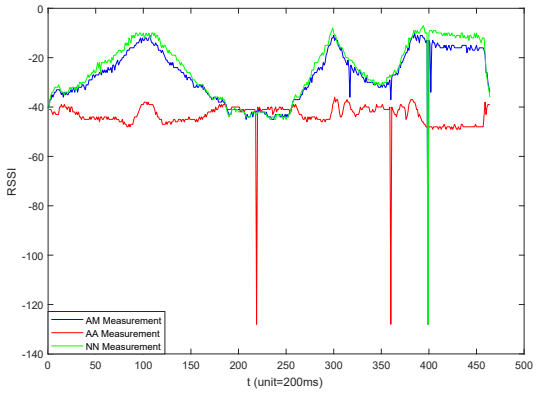

Fig. 3. Similarity between NN and AM Measurements

Using unique() function in Matlab, we can find the AM curve in Fig. 3 has 37 unique values (including -128); NN curve in Fig. 6 has 39 unique values (including -128). Thus to represent a measurement, AM needs $log_2(37-1) \approx 5.17$ bits; NN needs $log_2(39-1) \approx 5.25$ bits. In another word, in Fig. 3, we can derive at least 5 bits from each RSSI measurement, which is five-fold of the key generation rate of **??**.

A threshold substantially separates the measurements into two groups. The group above the threshold can be used to decide the proximity of the new node. The group below the threshold has more fluctuation, which in fact can be used for shared key generation and distribution as shown in our previous work [3]–[5]. By doing this we accomplish node authentication as well as key generation and distribution at the same time. The basic steps of the new method only needs minor update at step 4 to integrate the key distribution (including key generation) sub-task:

4) AM shares its RSSI measurements with AA via the secured link. Then AA can calculate the measurement gap (i.e., distance ratio). **And because of the broadcasting characteristic of wireless signal, the NN can also measure the RSSI of the secured messages (though NN cannot figure out the higher layer content), then both AM and NN will have similar RSSI measurements according to channel reciprocity [3]–[5]). The similar measurements can be a good source of symmetric key generation. Also with similar measurements, the key distribution process is simplified - only a few checksum need to be exchanged to remove minor deviations [3].**

The highlighted part is the new stuff in step 4 supporting key generation and distribution.

IV. Experimental Result

We verify our method according to the configuration shown in Fig. [**?**]. Only two types of frames the nodes exchange for authentication and key distribution. An eavesdropper and an impersonator are placed around the BAN to execute passive and active attacks. The NN periodically (every 200ms) sends out type 1 frames to request authentication. AM and AA will measure the RSSI values of the received type 1 frames. AM then shares its measurements with AA by sending AA type 2 frames. Each type 2 frame only shares one AM measurement. In the meantime, NN measure the received type 2 frames (though it cannot interpret the high layer content.) And save the measurement values as the source of shared key (between NN and AM). The eavesdropper collects all the type 1 and type 2 frames for analysis. The impersonator also periodically sends out type 1 frames trying to act as a NN and cheat the authenticators.

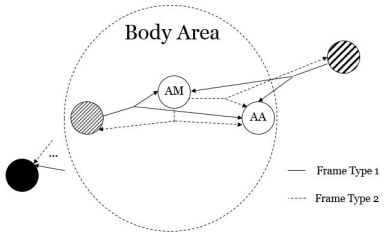

Fig. 4. Experimental Configuration

1,2 - The purpose of type 2 frame is to share the measured RSSI value from AM to AA via their secured link, that is why "Timestamp" and "RSSI" attributes are dot-lined because they are unseen to others. Although others can measure the RSSI of type 2 frame when they receive it (due to the broadcasting character of the wireless signal), the RSSI of the frame is not correlated to the RSSI attribute encapsulated in the higher layer of the frame. The others including eavesdroppers and NN. NN will measure the RSSI values from the type 2 frames and collect them as the source of the shared key.

* - The Measured RSSI attribute is dot-lined because it is measured by the receivers and each receiver has its unique measurement value (due to the diversity of distance and propagation path), which is unseen (secure) to other receivers.

Fig. 5 shows one experiment result:

- The measurement gap caused by the nearby NN (i.e., the green curve in Fig. 5) has continuous big segment (above the threshold); the measurement gap caused by the farther away impersonator (i.e., the purple curve in Fig. 5) does not have.
- The measurements between AM (the blue curve in Fig. 5) and NN are very similar ($\rho > 0.997$) and have enough fluctuation ($entropy > 5$).

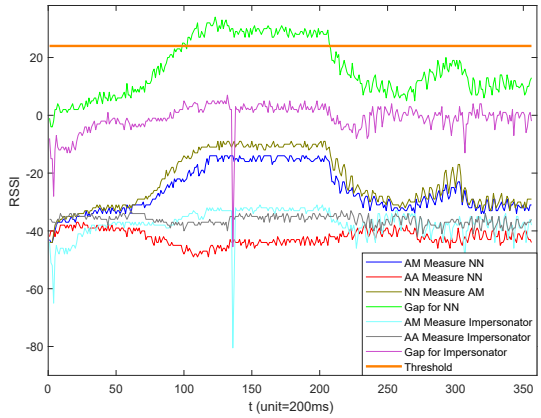

Fig. 5. Experiment Result: One Example

- The AM measurement on impersonator (i.e., the sky blue curve in Fig. 5) does not have enough fluctuation ($entropy < 5$). And it is not similar with the blue curve ($\rho = 0.552$). That means the impersonator cannot figure out the blue curve from the sky blue curve that the impersonator can indirectly and approximately obtain by measuring the frames from AM.

This time more missing frames are observed (19 of 356 frames). We use a simple single imputation (SI) technique to impute the missing values, which is replaced by the mean of its priors and successors.

We verify the experiments on two test beds. One is Crossbow MICAz-based ([19]); the other is ESP8266-based (**??**). The prior is equipped with 2.4G Hz ZigBee wireless transceiver and wired antenna; the later is equipped with 2.4G Hz WiFi wireless transceiver and patch antenna. We do not see much difference between the two test beds.

V. Conclusion

In this paper we proposes a new cooperative method to accomplish node authentication and key distribution tasks at the same time. The new method more fits more in the BAN environment than the existing methods. It efficiently integrates two core security tasks for BAN and solves a practical issue. Also, it increases the shared key generation rate and speed up the whole key distribution process. It reduces the users operations and proves to be user-friendly and attack-resistant.

VI. Acknowledgement

The research is partly supported by NSF awards (1401690 and 1401711).

References

[1] 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 Proc. *International Workshop on Radio Frequency Identification: Security and Privacy Issues* (pp. 74-89). Springer, Cham.

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

[3] Li, Z., & Wang, H. (2016, April). A key agreement method for wireless body area networks. In *Proc. Computer Communications Workshops (INFOCOM WKSHPS), 2016 IEEE Conference on* (pp. 690-695). IEEE.

[4] Li, Z., Wang, H., Daneshmand, M., & Fang, H. (2017, May). Secure and efficient key generation and agreement methods for wireless body area networks. In Communications (ICC), 2017 IEEE International Conference on (pp. 1-6). IEEE.

[5] Li, Z., Wang, H., & Fang, H. (2017). Group-Based Cooperation on Symmetric Key Generation for Wireless Body Area Networks. IEEE Internet of Things Journal, 4(6), 1955-1963.

[6] Stajano, F. (2000, April). The resurrecting ducklingwhat next?. In International Workshop on Security Protocols (pp. 204-214). Springer, Berlin, Heidelberg.

[7] Saxena, N., Ekberg, J. E., Kostiainen, K., & Asokan, N. (2006, May). Secure device pairing based on a visual channel. In Security and Privacy, 2006 IEEE Symposium on (pp. 6-pp). IEEE.

[8] M. T. Goodrich, M. Sirivianos, J. Solis, G. Tsudik, and E. Uzun, Loud and clear: Human-verifiable authentication based on audio, in ICDCS, 2006, pp. 1010.

[9] NFC Forum. [Online]. Available: http://nfc-forum.org

[10] Farid, Z., Nordin, R., & Ismail, M. (2013). Recent advances in wireless indoor localization techniques and system. Journal of Computer Networks and Communications, 2013.

[11] Mao, G., Fidan, B., & Anderson, B. D. (2007). Wireless sensor network localization techniques. Computer networks, 51(10), 2529-2553.

[12] Han, G., Xu, H., Duong, T. Q., Jiang, J., & Hara, T. (2013). Localization algorithms of wireless sensor networks: a survey. Telecommunication Systems, 52(4), 2419-2436.

[13] Pathirana, P. N., Bulusu, N., Savkin, A. V., & Jha, S. (2005). Node localization using mobile robots in delay-tolerant sensor networks. IEEE transactions on Mobile Computing, 4(3), 285-296.

[14] Cheng, L., Wu, C. D., & Zhang, Y. Z. (2011). Indoor robot localization based on wireless sensor networks. IEEE Transactions on Consumer Electronics, 57(3).

[15] Zhang, R. B., Guo, J. G., Chu, F. H., & Zhang, Y. C. (2011). Environmental-adaptive indoor radio path loss model for wireless sensor networks localization. AEU-international Journal of Electronics and Communications, 65(12), 1023-1031.

[16] Luo, X., OBrien, W. J., & Julien, C. L. (2011). Comparative evaluation of Received Signal-Strength Index (RSSI) based indoor localization techniques for construction jobsites. Advanced Engineering Informatics, 25(2), 355-363.

[17] Hamdoun, S., Rachedi, A., & Benslimane, A. (2013, August). Comparative analysis of RSSI-based indoor localization when using multiple antennas in Wireless Sensor Networks. In Selected Topics in Mobile and Wireless Networking (MoWNeT), 2013 International Conference on (pp. 146-151). IEEE.

[18] Jiang, J. R., Lin, C. M., Lin, F. Y., & Huang, S. T. (2013). ALRD: AoA localization with RSSI differences of directional antennas for wireless sensor networks. International Journal of Distributed Sensor Networks, 9(3), 529489.

[19] http://www.openautomation.net/uploadsproductos/micaz_datasheet.pdf

[20] https://www.espressif.com/en/products/hardware/esp8266ex/overview