SeAK: Secure Authentication and Key Generation Protocol Based on Dual Antennas for Wireless Body Area Networks

Chitra Javali[1,2](✉), Girish Revadigar[1,2], Lavy Libman[1,2], and Sanjay Jha[1]

[1] School of Computer Science and Engineering, UNSW, Sydney, Australia
[2] NICTA, Sydney, Australia
{chitraj,girishr,llibman,sanjay}@cse.unsw.edu.au

Abstract. The increasing interest in the usage of wireless body area networks (WBAN) in healthcare and other critical applications underscores the importance of secure communication among the body sensor devices. Associating an unknown device with an existing network without prior knowledge of a secret key poses a major challenge. Existing authentication schemes in WBAN are typically based on received signal strength (RSS). However, RSS techniques using a single antenna are susceptible to environmental factors and are vulnerable to attacks that use variable transmission power. We present SeAK, the first secure light-weight device pairing protocol for WBAN based on RSS obtained by dual-antenna transceivers utilizing spatial diversity. With spatially separated antennas, the RSS values from a nearby device are large and distinct, as opposed to those from a far-away device. SeAK exploits this effect to accomplish authentication and shared secret key generation simultaneously. We have implemented a prototype of SeAK on the Opal sensor platform with a 2.4 GHz compatible RF231 radio. We demonstrate that our protocol is able to achieve a 100 % success acceptance rate, securely authenticate a nearby device and generate a 128-bit secret key in 640 ms, as opposed to 15.9 s in other recent RSS-based schemes (e.g. ASK-BAN).

1 Introduction

In recent years, the medical field has observed a tremendous growth of wireless medical devices ranging from low-power medical radios that harvest body energy [12], to implanted medical devices (IMD) and wearable devices for remote monitoring of patients [25]. The ability of devices such as cardiac defibrillators, pacemakers, pulse-oximeters and glucose monitors to communicate in a wireless medium has opened up new opportunities for more reliable e-healthcare. According to a recent survey, the global market for wearable medical devices was valued at USD 2.0 billion in 2012 and is expected to reach a value of USD 5.8 billion in 2019 [5].

NICTA is funded by the Australian Department of Communications and the Australian Research Council through the ICT Centre of Excellence program.

N. Saxena and A.-R. Sadeghi (Eds.): RFIDSec 2014, LNCS 8651, pp. 74–89, 2014.
DOI: 10.1007/978-3-319-13066-8_5

Though the wireless medium provides numerous advantages, on the flip side there are a number of threats associated with authenticity, confidentiality and integrity of the sensitive health information. As the wireless system is an open access medium, an intruder can pair with the body area network and send false health-related information to the BS which may result in diagnosis errors, tamper the physiological data sensed by other body-worn devices, jam the network by creating interference or inject false commands leading to fatal outcomes.

As per the IEEE 802.15.6 Technical Requirements Document [4], *"Consideration should be given to secure device pairing (or association). Pairing consists of device authentication and key exchange. WBAN devices should successfully complete the secure pairing process before engaging in secure data communication with other WBAN devices"*. The initial trust establishment without any prior stored key from the manufacturer is a challenging aspect of security in WBAN. Employing cryptographic algorithms like Diffie-Hellman to generate shared secret keys is expensive for WBAN devices due to limited memory and computation power. Furthermore, in case of emergency, a third party/hospital authority must be able to communicate with the body-worn device of a patient which holds critical health information with minimal human intervention. The patient might not be able to provide the security information when he/she is unconscious or in critical condition. If the authority is unaware of the cryptographic key or the key is lost, then the problem of gaining access to WBAN becomes more complicated. Additionally, WBAN security must be robust enough to avoid active attacks as well as accidental access/commands from external devices. Access must be provided only to the legitimate external off-body devices such as wireless monitoring devices [2], external device programmers [3] etc. by dynamic authentication.

As the body worn devices have size and power constraints, security mechanisms should not add a high overhead to the devices in terms of hardware or software complexity. Some prior efforts of adapting public key cryptography protocols (e.g., TinyECC) to tiny sensor nodes have been evaluated as complex and memory consuming [27]. In recent years, there has been growing research interest in physical layer security which exploits the unique wireless channel characteristics between two devices. The unique channel characteristics are space and time dependent and decorrelate rapidly after a distance of *1/2* the wavelength (λ) of the wireless transmission channel [22]. These spatio-temporal characteristics have been exploited for authentication [23] and pairwise session key-generation [7,24] in WBAN.

However, the previously proposed device authentication mechanisms are based on received signal strength (RSS) from a single antenna. It has been shown in recent work that RSS is susceptible to environmental factors and is unreliable as it varies over a period of time even for a static transceiver [11]. In addition, as RSS is a function of the transmission power, an attacker can easily vary the transmitting power to induce high received signal strength and get authenticated as a legitimate device. Thus, the existing authentication procedures for WBAN [23,24] may not be able to distinguish between a malicious node and a legitimate device. Furthermore, the existing work in WBAN address authentication and pair-wise secret key generation separately.

In this paper, we propose a physical-layer based efficient, light-weight, close proximity secure device pairing protocol (SeAK) for WBAN, which performs authentication and shared secret key generation *simultaneously*. Our proposed scheme employs dual-antenna devices, utilizing the spatial diversity of antennas and the property that RSS values on the two antennas tend to be substantially different when the other device is nearby, in contrast to similar RSS values on both antennas obtained from far-away devices. This allows legitimate nearby devices to be distinguished effectively from potential attacker far-away devices.

Although RSS from multiple antennas of a receiver has been exploited in Wi-Fi systems with MIMO capability [9,30], multiple antenna architectures have not been used in WBAN. As the WBANs are being increasingly employed in pervasive healthcare applications, a revolution has already started in the research area of designing specialized devices and smart antennas for WBAN, e.g. tiny and flexible strip antennas, micro-strip antennas, textile antennas, and button antennas [6,8,17]. With the advent of smart wearable devices and antennas, the use of multi-antenna architecture in WBAN devices is expected to be widely employed in the near future. To the best of our knowledge, the work presented in this paper is the first to demonstrate the use of dual-antenna based secure pairing in the context of WBAN.

Our contributions can be summarised as follows:

- We propose an efficient secure pairing protocol for resource constrained devices of WBAN, which uses the spatial diversity of dual-antenna transceivers to perform authentication and secret key generation concurrently, and requires minimal human intervention.
- We validate the proposed approach experimentally and show that it completes the authentication and generation of a 128-bit secret key in 640 ms with a 100 % acceptance success rate, which indicates the suitability of our protocol for practical applications.

The rest of the paper is organized as follows. Section 2 discusses the related work. Section 3 explains our system model and assumptions. Sections 4 and 5 present the SeAK protocol and its implementation. Section 6 presents our experiments and results. In Sect. 7, we discuss the security evaluation of our protocol. We conclude the paper in Sect. 8.

2 Related Work

Extensive research has been carried out on secure device pairing based on wireless channel characteristics [16,20,26,29]. Authenticating a device in close proximity was first proposed in Amigo [26]. Ensemble [16] extended Amigo and proposed a cooperative proximity based authentication, in which the nearby trusted devices analyse the RSS variations between pairing devices to determine legitimacy. In [20], two devices located within a distance of $\lambda/2$ authenticate each other based on the analysis of phase and amplitude measurements of radio frequency (RF) signal from a public RF transmitter. The above mechanism requires multi-band transceivers and hence is not suitable for WBAN. Authors in [29] have proposed a hypothesis testing mechanism for physical layer authentication in which the two communicating parties store the channel responses of initial communications between them and subsequently compare those for the current message to validate a legitimate transmitter.

Ideally, for wearable medical devices, security mechanisms must be simple, light-weight, robust, and should not be dependent on specialized hardware or sensors. RSS based authentication has received little attention in the research community [23,24]. In WBAN, BANA [23] has studied the RSS characteristics of single antenna devices and has proposed an authentication protocol for on-body devices of WBAN. BANA takes about 12 s for authentication and requires frequent packet exchanges between the body-worn devices. An extended version ASK-BAN [24] addresses authentication and key generation separately. ASK-BAN uses two different channel states — static channel for authentication and dynamic channel for key generation, i.e., the subject should not perform any body movement during the authentication process, whereas the key generation mechanism requires body motion. In ASK-BAN, the time taken for authentication and key generation is 12 s and 15.9 s respectively.

RSS has been exploited in prior work [9,30] for security in Wi-Fi systems with MIMO capability. In [9], though authentication is based on channel characteristics, the key exchange protocol is based on the computationally complex Diffie-Hellman mechanism. In [30], key generation is performed with the cooperation of multiple mobile Wi-Fi devices equipped with multiple antennas.

Based on our survey of security protocols for wireless networks and body area networks, we believe that our work is the first secured pairing/association protocol based on physical layer characteristics using antenna diversity for low-data rate, small form-factor devices of WBAN.

3 System Model and Assumptions

3.1 RSS on Single v/s Dual Antenna

RSS has been widely used for localization [13,21] and attack detection [11] in wireless networks. The authors in [28,31] have shown that RSS has an irregular pattern even for a fixed transmitter and receiver. In a typical system consisting of a receiver and transmitter, if the sender sends a radio signal with power P_s, then the received power P_r at the receiver can be expressed as

$$P_r = P_s K / d_r^{\alpha} \tag{1}$$

where K is a constant, α is the distance power exponent and d_r is the distance between receiver and sender.

Now, if we consider receiver employing two antennas to capture the radio signals then the received power ratio can be calculated from (1) as

$$\frac{P_{r1}}{P_{r2}} = \frac{P_s K / d_1^{\alpha}}{P_s K / d_2^{\alpha}} \tag{2}$$

where $d_1 \neq d_2$.

From (2), the received power ratio is dependent only on the two distances, namely, the distance between the sender and receiver antennas A1 (d_1) and A2 (d_2) in contrast to (1), which implies that the received power P_r is dependent on transmission power P_s.

The concept discussed in this section forms the basis for our proposed protocol.

3.2 System Overview

In our system model, we assume there is one CU and one or more wearable sensor devices to be authenticated. The CU and wearable devices are within the communicating range of WBAN (≈3 m) [14]. In our system design, the CU is the only device that requires the additional feature of dual-antenna, and has the potential to authenticate other devices communicating with it by its unique property of antenna diversity. The sensor devices may have one or two antennas. We assume there is no prior association or secret key exchanged between the CU and other devices, and none of the devices are compromised. We also assume that the user or any other person authenticating a legitimate device is honest. We assume the availability of suitable secret key renewal procedures for wearable devices after on-body deployment.

As our focus is on secure device pairing, we are mainly concerned in detecting the masquerade attack in which a non-legitimate node poses as a legitimate node and communicates with the CU. We assume the presence of off-body adversaries only, i.e. the attacker is not present on-body or in the close vicinity of the WBAN, and is located at a distance of at least 1–2 m away from the CU. The adversary may use high or varying transmit power, and attempt to pair with the CU. The adversary lacks the capability of jamming the communication.

Figure 1 depicts our proposed system in which the CU and the device B to be authenticated are placed close to each other. The two antennas A1 and A2 of CU are separated by a distance D cm. The RSS values measured by A1 and A2 will yield a large difference for the nearby device B placed at a distance of d_1 and d_2 from A1 and A2 respectively. In contrast, for a far-away device E, the difference in RSS values measured at A1 and A2 of CU will be small.

4 SeAK Protocol

Our main focus in this paper is to achieve initial trust between an already trusted device CU and a new sensor device. The sensor device has to establish a secure link with the already trusted CU before joining the network (WBAN) and begin

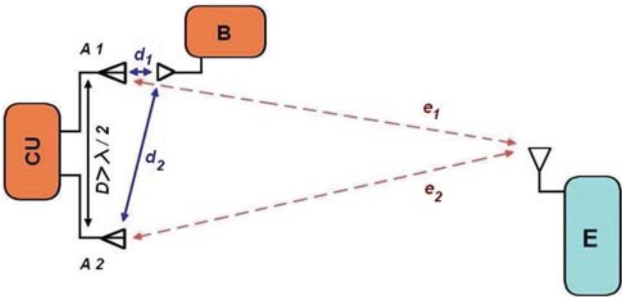


Fig. 1. The CU equipped with two spatially separated antennas A1 and A2 can effectively distinguish between a nearby legitimate device and a far-away attacker based on the RSS indicator difference obtained on its two antennas.

measuring the physiological data. Our proposed SeAK protocol is executed during the device pairing/association to establish a secure channel between the CU and device, by performing authentication and shared secret key generation simultaneously. SeAK protocol is described below.

1. The user holds the device to be authenticated in close proximity at a distance of d cm aligned to any one of the antennas A1 or A2 of CU. The device sends an association request *Assoc Req* to CU. The CU responds with an acknowledgement *ACK* to notify the start of association process.
2. The CU sends a probe packet *Probe[i]* to the device from antenna A1. In response, the sensor device measures the RSSI of the received packet and transmits a probe response *Probe Resp[i]* to CU. The CU in turn measures the RSS indicator (RSSI). The index value $i = \{1,\ 2,\ \ldots\ N\}$ tracks the number of packets N required for the association procedure.
3. The CU transmits a total of N packets at an interval of t ms by randomly switching between the two antennas A1 and A2. Let $X = \{x_1, x_2, \ldots x_N\}$ and $Y = \{y_1, y_2 \ldots y_N\}$ represent the set of RSSI measured by CU and device. Additionally, in order to evaluate the RSSI difference, CU stores the RSSI obtained at the two antennas A1 and A2 in separate data sets $R1 = \{r1_1, r1_2, \ldots r1_p\}$ and $R2 = \{r2_1, r2_2, \ldots r2_q\}$ respectively.
4. The absolute average RSSI difference RD_{avg} is calculated as $((r1 - r2)_j + (r1 - r2)_{j+1} + \ldots + (r1 - r2)_n)/n$. where $j = \{1,\ 2,\ \ldots n\}$ and n represents the minimum of p and q. The notations p and q denote the total number of samples captured by A1 and A2 respectively.
5. CU compares RD_{avg} with the threshold RSSI difference RD_{th} and the device is confirmed as legitimate if RD_{avg} is greater than RD_{th}, else discarded. CU notifies the device about successful authentication by sending an *Assoc Resp[ACCEPT]* message.
6. After successful authentication, both CU and device use the RSSI values stored during probe exchange for generating a shared secret key. The maximum *max* and minimum *min* values of RSSI are determined to obtain a *mid* value as *(max − min)/2*. Each RSSI sample is decoded as either bit 0 or 1 based on whether the sample value is smaller or greater than *mid*. Due to

spatial separation of the two antennas of CU, the RSSI measured by both the devices when CU employs A1 will be substantially distinct compared to RSSI obtained when CU employs A2. The process of bit extraction is repeated for N samples at both the nodes. Thus, both CU and the device derive an initial shared secret key.

Any packet loss during the probe exchange is handled by retransmissions. Once the CU and device have established a secure channel between them, the device is ready to be worn on-body.

5 Implementation

We have implemented the proof of concept in TinyOS environment. The Opal sensor platform [15], used in testbeds like FlockLab [19] and Twonet [18], was used for CU, and Iris motes were used as the sensor devices to be authenticated and as eavesdroppers. Our protocol can be implemented for commercially available off-the-shelf sensor devices which support dual antenna architecture.

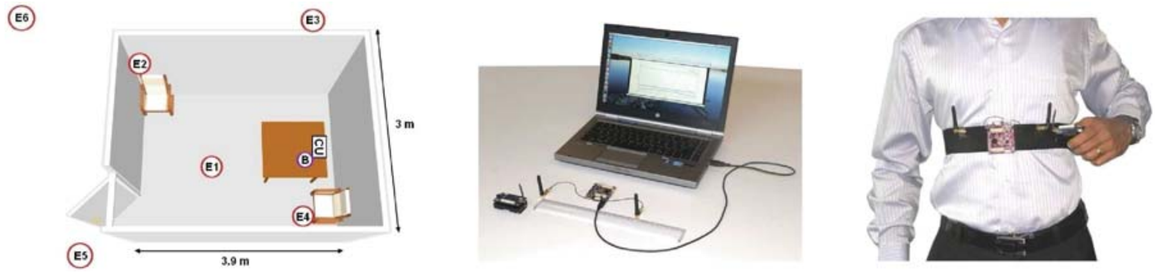
Opal can be configured to work in either single antenna mode or antenna diversity mode. When single antenna mode is enabled, only one default antenna is used for both transmission and reception of packets. In antenna diversity mode, the transceiver radio checks the preamble field of a received frame to select one of the two antennas with the highest radio frequency (RF) signal strength. The scanning of preamble field is repeated for every new frame. The probability that both the antennas experience identical fading and multi-path effects is less when the two antennas are spatially separated to receive independent signals. However, in our system design we require that both the antennas should be able to receive RF signals independently, and also our system must not be dependent on the radio transceiver for the receiver diversity. Hence, we have modified the TinyOS driver and RF231 lower layer stack code to select one of the two antennas from the application layer, for transmission as well as reception of the packets.

For our implementation, the antenna diversity algorithm is disabled for dual-antenna RF230 radio [1] by setting the bit ANT_DIV_EN of ANT_DIV (0x0D) register to 0. The two externally connected 2.4 GHz antennas A1 and A2 are enabled by setting ANT_SEL bit of the same register to 0 and 1 respectively in the TinyOS driver program. At any instant of time only one of the antennas is enabled by the application and the time taken to switch between the two antennas is less than 100 ns [19]. Hence the power consumed by the CU is equivalent to that of a single antenna device.

6 Experiments and Results

6.1 Test Environment

In order to authenticate a legitimate device, there are two main factors to be identified: (i) The optimal displacement between the two antennas of CU to gain a large RSSI difference, (ii) An upper bound distance between CU and device. In order to get uncorrelated signal characteristics, we placed the two receiving antennas of CU 7 cm ($> \lambda/2$) apart and incremented the separation in steps up to 30 cm[1]. We conducted the first set of experiments by placing CU and the device off-body and the second set for on-body. In the following subsections we describe the test set up for off-body and on-body environments.



(a) Off-body set up environment. CU: Control Unit, B: Device, E1-E6: Eavesdroppers

(b) Off-body set up: The device to be authenticated placed close to one of the antennas of CU

(c) CU on-body: Subject wearing CU and holding the device to be paired in close proximity

Fig. 2. Test environment

CU off-body: The experiments were conducted in a room of dimension $3.9 \times 3\,\text{m}^2$ as shown in Fig. 2a. Figure 2b shows the off-body set-up where both CU and the device were placed on a table. These experiments were conducted to study the off-body channel characteristics and the ability of authenticating a device when CU is present off-body. Experiments were conducted by placing the device B at different distances d varying from 1 cm to 30 cm with respect to antenna A1 of CU. Evaluation was done by placing the device at various angles, e.g. 0°, 45° and 90° w.r.t A1, and also repeated for the antenna A2.

The tests were conducted for inter-packet intervals t of 250 ms, 100 ms, 50 ms, 10 ms and 5 ms respectively. For the experiments we set the number of packets exchanged between CU and device to be $N = 250$.

CU on-body: In this set-up, CU was placed on the body of a subject as shown in Fig. 2c and the device B to be authenticated was held in close proximity of the CU. The distance between the two receiving antennas D was varied from 10 cm to 30 cm, and for various D the distance d between CU and device was also changed[2]. A similar set of experiments to that of off-body set-up were conducted.

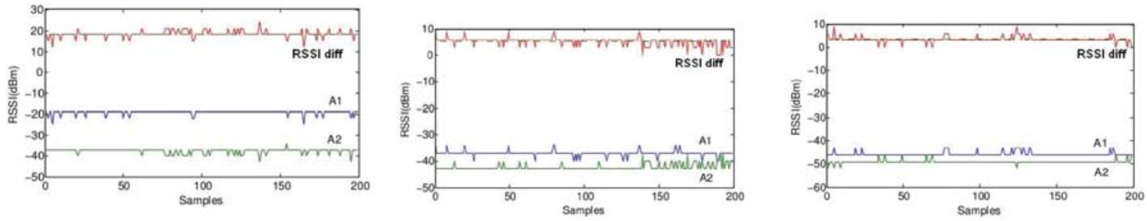
[1] For 2.4 GHz, $\lambda = 12.5\,\text{cm}$

[2] We believe that the use of specialised antennas like micro-strip antennas and button antennas as well as advances in wearable technologies more generally, will allow such levels of spatial diversity in the near future [8,17].

6.2 Results

In this section we evaluate the experimental results obtained for off-body and on-body scenarios. We analyse the set of results obtained when the device was aligned to A1 of CU.

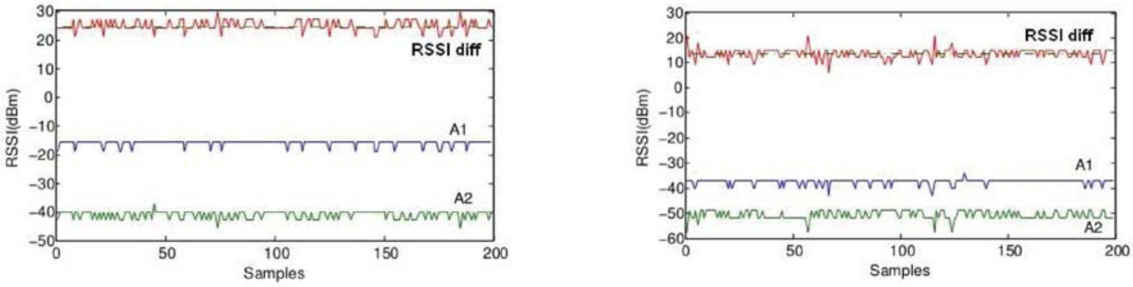
CU off-body: From Fig. 3, one can observe that for $d = 1$ cm, RSSI obtained at A1 is greater than that of A2 and the RSSI obtained at both the antennas decrease as the distance d of the device increases with respect to CU. From Figs. 3a and b it can be observed that the difference in the RSSI obtained at A1 and A2 substantially reduces when d increases from 1 cm to 15 cm. On further increasing d to 30 cm, the RSSI of A1 and A2 almost coincide.



(a) d = 1cm, RD_{avg} = 18.21 (b) d = 15cm, RD_{avg} = 5.51 (c) d = 30cm, RD_{avg} = 3.0

Fig. 3. Results for off-body setup when D = 10 cm

Figure 5a reveals that, as the distance between the 2 antennas D increases, the RSSI difference of A1 and A2 also increases. In contrast, for a fixed D, the RSSI difference decreases as the distance d between the device and CU increases. At $d = 30$ cm for various values of D, the RSSI difference of A1 and A2 is substantially smaller compared to $d = 1$ cm.



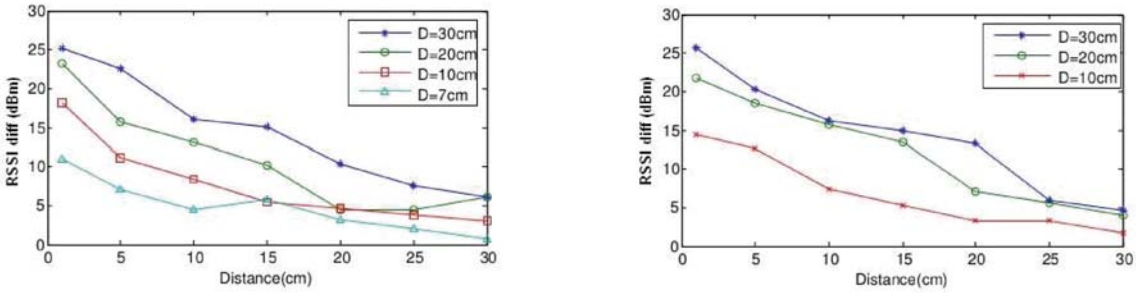
(a) d = 1cm, RD_{avg} = 25.6

(b) d = 20cm, RD_{avg} = 14.9

Fig. 4. Results for on-body setup when D = 30 cm

CU on-body: Fig. 4 depicts the on-body experimental results for $D = 30$ cm. The graphs reveal that the behaviour of on-body characteristics resemble the off-body ones. There is a comparatively large difference in the RSSI difference of A1 and A2 when the device is very near to CU and 20 cm away from CU. Figure 5b shows the variation of RSSI difference with d and D, which resembles the off-body characteristics.

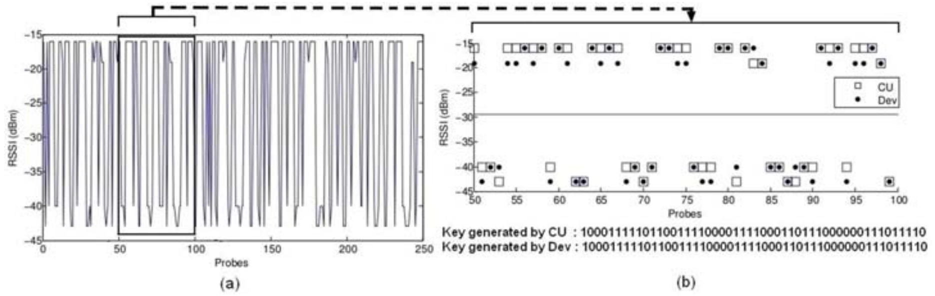
Comparing the RSSI difference varying with distance d for off-body and on-body experiments from Figs. 5a and 5b respectively, it can be observed that both the set-ups indicate similar characteristics. The results for a few additional configurations are presented in Figs. 7 and 8 in the Appendix.



(a) RSSI difference for CU off-body setup

(b) RSSI difference for CU on-body setup

Fig. 5. RSSI difference with respect to distance d for various D



Key generated by CU : 10001111101100111100001111000110111000000111011110
Key generated by Dev : 10001111101100111100001111000110111000000111011110

Fig. 6. Secret key generation (a) RSSI samples obtained at CU (b) Key generation mechanism

Key Generation: In this section, we illustrate the secret key generation mechanism of our proposed protocol which utilises the RSSI samples measured by the CU and the device during probe exchange. We present the results for one of the on-body set-up with $D = 30$ cm and the device aligned to one antenna at a distance of 1 cm from the CU. Figure 6a depicts the RSSI samples from both antennas at CU. Figure 6b shows a subset of data (samples with index 50 to 100) from Fig. 6a overlapped with the corresponding RSSI samples at the device. From the above figure, we observe that there is a high correlation between the channel characteristics of CU and the device. Though both CU and the device are stationary, the spatial separation between the two antennas of CU result in obtaining distinct RSSI values, approximately equal to −15 dBm and −44 dBm on either side. By assigning 1 bit binary coding, i.e., bit 1 and 0 to the upper and lower block respectively, CU and the device extract 100 % matching keys.

6.3 Impact of Parameter Variation

Variation of D: The two antennas of CU have to be spatially separated so that there is no channel correlation and the characteristics of the received signals differ. From Fig. 5, the RSSI differences obtained for $D = 30$ cm are much greater than the values obtained for $D = 7$ cm and 10 cm. Hence we select $D > 10$ cm as an appropriate displacement between A1 and A2 to achieve a large RSSI difference.

Variation of d: Observing Fig. 5 for $d \leq 15$ cm, the RSSI difference ranges from 25.88 to 5.51 where as for $d > 15$ cm, the RSSI difference drops dramatically compared to the maximum value for each of the corresponding D. Thus, we set the threshold values RD_{th} for each D as shown in Table 1.

Table 1. RSSI difference threshold (RD_{th}) for $D = 10$ cm, 20 cm and 30 cm

D (cm)	RSSI difference threshold (RD_{th})
10	5.51
20	10.17
30	15.07

Effectiveness: To differentiate between a legitimate and a non-legitimate device, several experiments were conducted for $D = 20$ cm, 30 cm and d was varied from 1 cm to 40 cm. For each set-up we calculated the average value of RSSI difference from the two antennas A1 and A2 and compared with the RD_{th} from Table 1. We computed the acceptance rate of legitimate device and rejection rate of a non-legitimate device by repeating the off-body experiments for 40 different positions aligned with antenna A1 and A2 separately. We observed from our experimental results that $t = 5$ ms was an appropriate inter-packet interval to determine the legitimacy of a device. Thus, in order to successfully authenticate and generate a shared secret key of 128 bit length our protocol requires 640 ms. The success acceptance rate accomplished is 100 % and the rejection rate of a non-legitimate device for $D = 30$ cm is 100 % which drops to 95 % for $D = 20$ cm. This variation in RSSI difference from RSSI threshold RD_{th} is due to noise and path loss components.

7 Security Evaluation

In this section we evaluate the robustness of our system against active and passive attacks. An attacker may impose as a legitimate device by sending probe packets to CU and try to pair with CU, to further gain access to the WBAN. We have analysed the possibility of such an attack by placing multiple adversaries at different locations as shown in Fig. 2a. The RSSI difference obtained at CU from different adversaries is shown in Table 2. It can be seen that the RSSI difference is significantly less than the RSSI threshold for any of the values of D from Table 1.

Table 2. RSSI difference obtained by Eve (E1 - E6) at distances of E1 = 270 cm, E2 = 360 cm, E3 = 180 cm, E4 = 100 cm, E5 and E6 > 4 m for $D = 10$ cm

Adversary	E1	E2	E3	E4	E5	E6
RSSI Difference	0.05	1.3	1.5	0.1	0.5	2.3

Additionally, an adversary can achieve high RSSI by either of the following two possible mechanisms:

Varying transmission power attack: To evaluate our proposed protocol against varying transmission power attack, we have placed the attacker "Eve" at 360 cm from the CU. For each $D = 10$ cm, 20 cm and 30 cm, the attacker's transmission power was set at different levels. As seen from Table 3, though the attacker transmits with the highest possible power, the RSSI difference at CU is very small. The RSSI difference for Eve is in the range of 0.0 to 2.4 which is significantly smaller than the RSSI difference threshold RD_{th}.

Table 3. RSSI difference for $d = 360$ cm and varying transmitting power

D (cm)	RSSI difference		
	Ps = 3 dBm	Ps = 0 dBm	Ps = −17 dBm
10	0.0	0.9	1.9
20	0.2	0.03	1.5
30	0.15	0.2	2.4

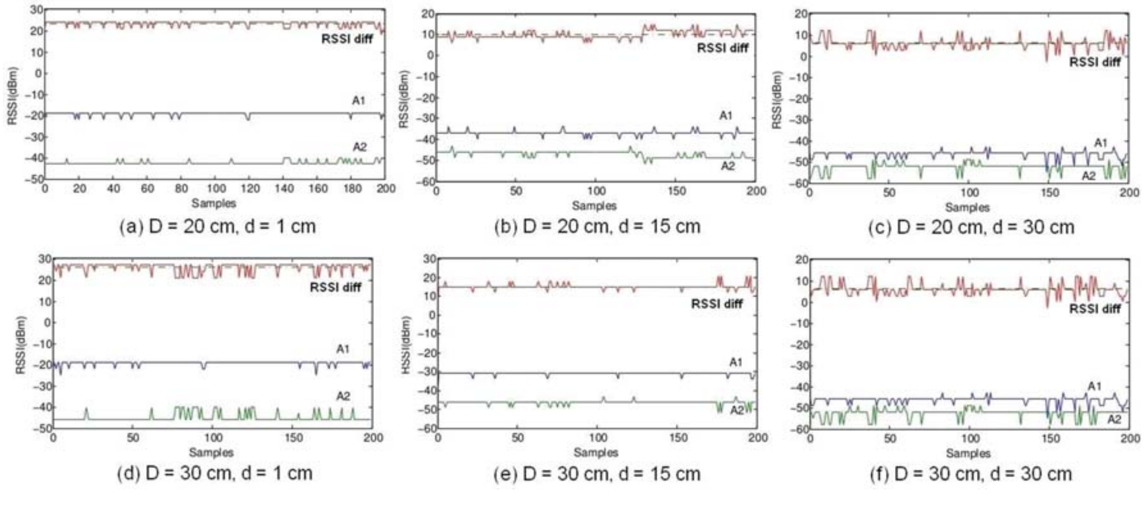
Beam-forming attack: In this type of attack, the adversary forms a focused beam on the CU to induce an acceptable value of RSSI difference. In order to have a focused beam with narrow-width main lobe, the attacker would require a large antenna array [9]. The presence of such a large antenna would be easily noticeable. In addition, in our system model, the distance between the two receiving antennas is $<$ 40 cm, hence a beam-forming attack would be difficult to achieve.

Robustness of key generation: A passive eavesdropper situated at any other location will not be able to derive the same key as CU/B due to unique spatio-temporal characteristic of the wireless channel [22]. The secret keys generated during secure device pairing have been verified for randomness by performing NIST statistical tests and the results reveal that the keys generated have highest entropy = 1. The shared randomness between any two devices is exemplified by the mutual information (MI) [10]. The MI *I(X:Y)* between CU and B is 0.9896 and that of eavesdroppers placed at different locations ranges from 0.322 to 0.00225. Which is far less than that of CU and B, thereby decreasing the probability of Eve obtaining the same secret key as CU/B. Even if Eve has multiple antennas, the MI of Eve will be further reduced due to multi-path effects and other random factors like noise [30].

8 Conclusion

We have presented a light-weight secure device pairing protocol for WBAN which utilizes the spatial diversity of dual-antenna devices to obtain large and distinct values of RSS on the two antennas from a communicating node placed near one of the antennas. In contrast, a device placed far-away cannot induce such large difference in the measured RSSI. Hence, a nearby legitimate device can be easily distinguished from a far-away attacker. At the same time, the considerably different values of RSS obtained from the two spatially separated antennas are used for shared key generation. Our experimental results demonstrate that the success acceptance rate of a legitimate nearby device is 100 %, and authentication combined with secret key generation can be achieved in 640 ms, which is faster by more than an order of magnitude in authentication and key generation as compared to the most recent related work in WBAN.

A Off-Body Set-Up



(a) D = 20 cm, d = 1 cm

(b) D = 20 cm, d = 15 cm

(c) D = 20 cm, d = 30 cm

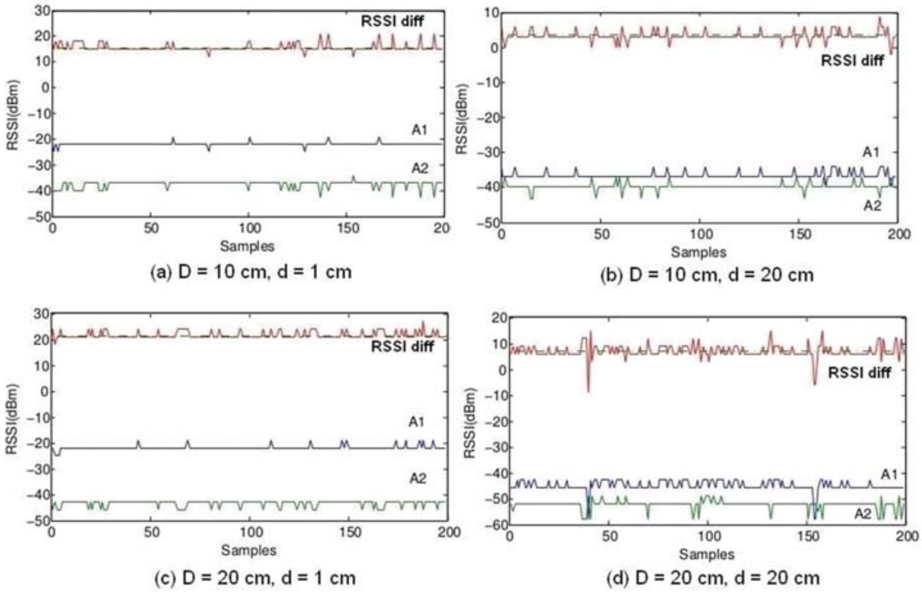
(d) D = 30 cm, d = 1 cm

(e) D = 30 cm, d = 15 cm

(f) D = 30 cm, d = 30 cm

Fig. 7. RSSI variation for various off-body experiments

B On-Body Set-Up



(a) D = 10 cm, d = 1 cm

(b) D = 10 cm, d = 20 cm

(c) D = 20 cm, d = 1 cm

(d) D = 20 cm, d = 20 cm

Fig. 8. RSSI variation for various on-body experiments

References

1. AT86RF231/ZU/ZF datasheet. http://www.atmel.com/images/doc8111.pdf. Accessed 31 Jan 2014
2. Glucose monitor. http://www.medtronic.com.au/your-health/diabetes/device/continuous-glucose-monitor/what-is-it/index.html. Accessed 12 Feb 2014
3. InterStim iCon Patient Programmer. https://professional.medtronic.com. Accessed 18 Feb 2014
4. TG6 technical requirements document (TRD) IEEE P802.15-08-0644-09-0006. https://mentor.ieee.org/802.15. Accessed 24 Feb 2014
5. Wearable medical devices market survey. http://www.prnewswire.com/news-releases/wearable-medical-devices-market-is-expected-to-reach-usd-58-billion-globally-in-2019-transparency-market-research-235220471.html. Accessed 18 Feb 2014
6. Wearble Antennas. http://www.pharad.com/wearable-antennas.html. Accessed 5 Feb 2014
7. Ali, S.T., Sivaraman, V., Ostry, D.: Zero reconciliation secret key generation for body-worn health monitoring devices. In: Proceedings of ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) (2012)
8. Batchelor, J., Swaisaenyakorn, S., Miller, J.: Personal and body area network channels between dual band button antennas. In: Proceedings of Asia-Pacific Microwave Conference (APMC) (2009)
9. Cai, L., Zeng, K., Chen, H., Mohapatra, P.: Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas. In: Proceedings of Network and Distributed System Security Symposium (NDSS) (2011)
10. Cover, T.M., Thomas, J.A.: Elements of Information Theory. Wiley, New York (1991)

11. Demirbas, M., Song, Y.: An RSSI-based scheme for sybil attack detection in wireless sensor networks. In: Proceedings of International Symposium on World of Wireless, Mobile and Multimedia Networks (WoWMoM) (2006)
12. Gollakota, S., Hassanieh, H., Ransford, B., Katabi, D., Fu, K.: They can hear your heartbeats: non-invasive security for implantable medical devices. In: Proceedings of ACM SIGCOMM (2011)
13. Haeberlen, A., Flannery, E., Ladd, A.M., Rudys, A., Wallach, D.S., Kavraki, L.E.: Practical robust localization over large-scale 802.11 wireless networks. In: Proceedings of ACM MobiCom (2004)
14. Hanlen, L.W., Smith, D., Zhang, J.A., Lewis, D.: Key-sharing via channel randomness in narrowband body area networks: is everyday movement sufficient?. In: Proceedings of International Conference on Body Area Networks (BodyNets) (2009)
15. Jurdak, R., Klues, K., Kusy, B., Richter, C., Langendoen, K., Brünig, M.: Opal: a multi-radio platform for high throughput wireless sensor networks. IEEE Embed. Syst. Lett. **3**(4), 121–124 (2011)
16. Kalamandeen, A., Scannell, A., de Lara, E., Sheth, A., LaMarca, A.: Ensemble: cooperative proximity-based authentication. In: Proceedings of ACM MobiSys (2010)
17. Khaleel, H.R., Al-Rizzo, H.M., Rucker, D.G., Elwi, T.A.: Wearable yagi microstrip antenna for telemedicine applications. In: Proceedings of IEEE Radio and Wireless Symposium (RWS) (2010)
18. Li, Q., Han, D., Gnawali, O., Sommer, P., Kusy, B.: Twonet: large-scale wireless sensor network testbed with dual-radio nodes. In: Proceedings of ACM Conference on Embedded Networked Sensor Systems (SenSys) (2013)
19. Lim, R., Ferrari, F., Zimmerling, M., Walser, C., Sommer, P., Beutel, J.: Flocklab: a testbed for distributed, synchronized tracing and profiling of wireless embedded systems. In: Proceedings of International Conference on Information Processing in Sensor Networks (IPSN) (2013)
20. Mathur, S., Miller, R.D., Varshavsky, A., Trappe, W., Mandayam, N.B.: ProxiMate: proximity-based secure pairing using ambient wireless signals. In: Proceedings of MobiSys (2011)
21. Park, J.G., Curtis, D., Teller, S.J., Ledlie, J.: Implications of device diversity for organic localization. In: Proceedings of IEEE INFOCOM (2011)
22. Rappaport, T.S.: Wireless Communications: Principles and Practice. Prentice Hall, Englewood Cliffs (2001)
23. Shi, L., Li, M., Yu, S., Yuan, J.: BANA: body area network authentication exploiting channel characteristics. In: Proceedings of ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) (2012)
24. Shi, L., Yuan, J., Yu, S., Li, M.: ASK-BAN: authenticated secret key extraction utilizing channel characteristics for body area networks. In: Proceedings of ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) (2013)
25. Shnayder, V., Chen, B.R., Lorincz, K., Jones, T.R.F.F., Welsh, M.: Sensor networks for medical care. In: Proceedings of International Conference on Embedded Networked Sensor Systems (SenSys) (2005)
26. Varshavsky, A., Scannell, A., LaMarca, A., de Lara, E.: Amigo: proximity-based authentication of mobile devices. In: Krumm, J., Abowd, G.D., Seneviratne, A., Strang, T. (eds.) UbiComp 2007. LNCS, vol. 4717, pp. 253–270. Springer, Heidelberg (2007)

27. Wilhelm, M., Martinovic, I., Schmitt, J.B.: Secret keys from entangled sensor motes: Implementation and analysis. In: Proceedings of ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec) (2010)
28. Wu, K., Tan, H., Ngan, H., Liu, Y., Ni, L.M.: Chip error pattern analysis in IEEE 802.15.4. IEEE Trans. Mob. Comput. **11**(4), 543–552 (2012)
29. Xiao, L., Greenstein, L.J., Mandayam, N.B., Trappe, W.: Fingerprints in the ether: using the physical layer for wireless authentication. In: Proceedings of IEEE ICC (2007)
30. Zeng, K., Wu, D., Chan, A., Mohapatra, P.: Exploiting multiple-antenna diversity for shared secret key generation in wireless networks. In: Proceedings of IEEE INFOCOM (2010)
31. Zhou, G., He, T., Krishnamurthy, S., Stankovic, J.A.: Impact of radio irregularity on wireless sensor networks. In: Proceedings of ACM MobiSys (2004)