# BANA: Body Area Network Authentication Exploiting Channel Characteristics

Lu Shi
Dept. of CS
U. of Arkansas at Little Rock
Little Rock, AR 72211
lxshi@ualr.edu

Ming Li
Dept. of CS
Utah State University
Logan, UT 84322
ming.li@usu.edu

Shucheng Yu
and Jiawei Yuan
Dept. of CS
U. of Arkansas at Little Rock
Little Rock, AR 72211
{sxyu1,jxyuan}@ualr.edu

## ABSTRACT

Wireless body area network (BAN) is a promising technology for real-time monitoring of physiological signals to support medical applications. In order to ensure the trustworthy and reliable gathering of patient's critical health information, it is essential to provide node authentication service in a BAN, which prevents an attacker from impersonation and false data/command injection. Although quite fundamental, the authentication in BAN still remains a challenging issue. On one hand, traditional authentication solutions depend on prior trust among nodes whose establishment would require either key pre-distribution or non-intuitive participation by inexperienced users, while they are vulnerable to key compromise. On the other hand, most existing non-cryptographic authentication schemes require advanced hardware capabilities or significant modifications to the system software, which are impractical for BANs.

In this paper, for the first time, we propose a lightweight body area network authentication scheme (BANA) that does not depend on prior-trust among the nodes and can be efficiently realized on commercial off-the-shelf low-end sensor devices. This is achieved by exploiting physical layer characteristics unique to a BAN, namely, the distinct received signal strength (RSS) variation behaviors between an on-body communication channel and an off-body channel. Our main finding is that the latter is more unpredictable over time, especially under various body motion scenarios. This unique channel characteristic naturally arises from the multi-path environment surrounding a BAN, and cannot be easily forged by attackers. We then adopt clustering analysis to differentiate the signals from an attacker and a legitimate node. The effectiveness of BANA is validated through extensive real-world experiments under various scenarios. It is shown that BANA can accurately identify multiple attackers with minimal amount of overhead.


*WiSec'12,* April 16–18, 2012, Tucson, Arizona, USA.


## Categories and Subject Descriptors

C.2.0 [**General**]: Security and Protection; C.2.1 [**Network Architecture and Design**]: Wireless Communication

## General Terms

Security, Design

## Keywords

Wireless Body Area Network, Sensor, Authentication, RSS, Physical Layer

## 1. INTRODUCTION

Wireless body area network (BAN) or body sensor network (BSN) has been an area of significant research in recent years [24, 46, 7]. A BAN is a wireless network usually formed by lightweight, small-size, ultra-low-power, interoperable and intelligent wearable sensors [7], which are strategically placed on the body surface, around it or implanted inside the human body. To monitor the wearer's health status or motion pattern, these sensors measure, process, and transmit the body's physiological signs to a control unit (CU) without constraining the activities of the wearer. Physicians and caregivers can then access the collected data for real-time diagnosis and trigger treatment procedures in return. For example, upon detecting high blood sugar level from a glucose monitoring device, an insulin pump will receive a command from the CU to inject a required dose of insulin [32]. The BAN technology enables numerous exciting applications, such as ubiquitous health monitoring [17] and emergency medical response (EMS) [25], etc. It has the potential to revolutionize the healthcare delivery in hospitals, operation theaters, and homes.

As BAN applications deal with sensitive patient medical information, they have significant security, privacy and safety implications which may prevent the wide adoption of this technology. There have been wide privacy concerns in the public towards IMDs [1]; however, the data security in a BAN has not drawn enough attention, although the lack of it would lead to fatal consequences [19, 8]. Especially, node authentication is the fundamental step towards a BAN's initial trust establishment (e.g., key generation) and subsequent secure communications. Since IMDs transmit critical health monitor reports to and receive commands from the CU, if an attacker successfully pretends to be a legitimate sensor node or CU and joins the BAN, it can either report wrong patient

health status information or inject false commands which may put the patient's safety at risk. In current practices, the interoperable medical devices (IMDs) are not designed with enough security in mind. Over the years, there are a number of reported remote hacking incidents of individual IMDs [42, 14] exploiting the unprotected wireless channel. In a BAN, the situation is even worse if attacker can spoof multiple medical devices simultaneously. Thus, an effective node authentication mechanism is the key to BAN's security and patient safety.

Despite past research efforts on authentication in wireless networks, the same issue in BAN still remains a challenge because of its unique features and stringent application-level requirements. Traditionally, authentication has been relying on pre-distributed secret keys among nodes in a network. For example, there is a lot of literature on key distribution in wireless sensor networks (WSNs) [13, 5, 11, 12, 22, 23, 34]. However, if directly applied to a BAN, this method requires the end-users to basically trust the whole distribution chain which may involve numerous less trustworthy users. In addition, BAN's user is usually unexperienced humans which implies high usability is required, where ideally "*plug-and-play*" is desired. Any key distribution/management process should be minimized, automatic, and transparent to users. Thus, node legitimacy in a BAN should be established *without assuming prior security context* among nodes. Furthermore, as the medical sensors become ubiquitous, they could be compromised and pre-shared secret keys can be stolen. These keys allow attackers to imposter any legitimate node, which renders traditional cryptographic authentication mechanisms ineffective. Therefore, node authentication mechanisms in BAN should have *minimal reliance on cryptography*. Finally, the low-end medical sensor nodes are extremely constrained in resources (including hardware, energy and user interfaces), while existing non-cryptographic authentication mechanisms mostly require advanced hardware such as multiple-antennas [51], or significant modifications to the system software. It is very important to note that, we *should not introduce additional hardware assumptions* to the BAN, not only because that adds cost but also it is not easily compatible with legacy systems.

Identifying these challenges, in this paper, we put forward BANA — a practical node authentication scheme for body area networks that does not depend on prior-trust (or pre-shared secrets) among the nodes. We exploit unique physical layer characteristics within a BAN environment, namely, the distinct received signal strength (RSS) variation behaviors between an on-body and an off-body communication channel. That is, when two legitimate devices are placed on the same user's body, the RSS variation of the channel between them is much more stable than the case when one of the devices is off-the-body, especially when the body as a whole is *in motion*. This channel characteristic arises naturally from the multi-path fading environment surrounding a BAN, thus a legitimate on-body channel's RSS variation profile is very hard to be forged by an off-body attacker, unless it can create a perfect channel[1]. We then design BANA based on this characteristic, and propose to use clustering analysis to differentiate the signals from a legitimate node and an attacker. We find that BANA works effectively under a wide range of scenarios with low false-positive and false-negative rates, and can correctly identify multiple attackers even when they collude. BANA can be efficiently realized on commercial off-the-shelf low-end sensor devices.

[1]An attacker equipped with high-gain directional antenna may create a low RSS-variation off-body channel, but this attack involves many difficulties, whose feasibility is discussed in Sec. 6.3.

## Our Contributions

(1) We identify a new type of channel characteristics in BAN that can be used to increase its security. Namely, the dramatic differences in RSS variations between on-body and off-body channels, especially under artificially induced body motions. We theoretically explain its cause, and validate this characteristic through extensive experimental study under different scenarios.

(2) We propose BANA, a novel non-cryptographic node authentication scheme for BAN based on the new channel characteristics. We perform clustering analysis on the average RSS variation (ARV) to differentiate signals of a legitimate node and an attacker. Our scheme is resource-efficient and does not require additional hardware.

(3) We validate effectiveness and efficiency of BANA through extensive experiments on a body sensor network testbed. In particular, it is shown that our scheme can accurately identify multiple colluding attacker nodes even when their number is up to 5 times of legitimate nodes, while incurring minimal amount of overhead. The time required for authentication can be as short as 12 seconds for a group of six body sensors.

The rest of this paper is organized as follows. We review related work in Section 2. The problem definition, including system model and attack model, will be introduced in Section 3. Section 4 presents our findings on the new channel characteristics, while Sec. 5 gives BANA's main design. In Section 6, we evaluate its security and performance, and discuss its limitations. We conclude the paper in Section 7.

# 2. RELATED WORK

Related research on authentication in WSNs, especially in BANs can be mainly divided into two categories – cryptographic and non-cryptographic authentication mechanisms. Traditionally, authentication in WSNs and BANs relied on the existence of prior security context [6, 26, 10, 27, 9, 52]. Those mechanisms generally either involve high computational overhead or complex key management. Tan et. al. [41] proposed lightweight crypto-based authentication schemes. However, they still require prior-trust among the nodes or a trusted authority for key distribution, which lowers the usability of a BAN. It is worthy to note that secure device pairing methods are recent alternatives that do not assume pre-shared secrets, while enjoying higher usability (e.g., GDP [21, 20]). However, they assumed the existence of some additional out-of-band (OOB) secure channel that facilitates human-aided verification, which may not be intuitive to use. Thus, in what follows we only survey non-cryptographic authentication techniques related to BAN.

## 2.1 Biometric-based Authentication

Physiological values are used to assist authentication and key generation by measuring and comparing the physiological signals separately at the sender and the receiver [35, 45, 44, 39, 47, 50, 15], such as electrocardiogram (EEG) and photoplethysmogram (PPG), iris, fingerprint etc. These methods can achieve "plug-and-play" without relying on pre-

shared secrets, but it is hard for every body sensor in different positions to measure the same physiological signal with the same accuracy. Others use common accelerometer data extracted from motion of the body [30, 31]. However, they require specialized sensing hardware for every sensor.

## 2.2 Channel-based Authentication

Zeng et. al. [51] classified non-cryptographic authentication schemes into three different categories: software-based, hardware-based, and channel/location-based. Both software-based and hardware-based solutions are vulnerable to attacks that mimick the characteristics of the signature and impersonation. Channel/location-based solutions leverage the observation that RSS tends to vary over time due to mobility and channel environments.

Recently there have been an increasing interest in RSS-based authentication [43, 18, 4]. Zeng et. al. [51] proposed to use temporal RSS variation lists to deal with identity-based attack, where an intruder T who tries to impersonate another user B that is communicating with A can be detected by A. However, they focused on identification while our work focuses on distinguishing legitimate nodes from false ones (i.e., there is no specific identify to impersonate). The secure device pairing scheme proposed by [4] performed proximity detection based on differential RSS, but requires additional hardware (at least two receiver antennas). Other identification/authentication schemes build a signature for each device's wireless channel, for example, the temporal link signature in [33] uses channel impulse response. However, this method requires a learning phase and also advanced hardware platforms such as GNU radio.

## 2.3 Proximity-based Authentication

Several schemes are based on co-location detection. Amigo in [43] extends the Diffie-Hellman key exchange with verification of device co-location. Each device monitors the radio environment for a short period of time and generates a signature including its RSS, which is used for similarity detection. In Ensemble [18], with the pairing devices transmitting and the trusted body-worn personal devices receiving, the latter determine proximity by monitoring the transmissions. Similarly, Mathur et. al. [28] proposed a co-location based pairing scheme by exploiting environmental signals. The main drawback of these methods is, the devices need to be within half wavelength distance of each other, which is restrictive for medical sensors deployed in a BAN.

Other works exploit secure ranging techniques to determine a device's proximity [38], such as distance bounding [3]. The general concern with RF distance bounding is it requires specialized/advanced hardware, otherwise high accuracy cannot be achieved. In [37], Rasmussen and Capkun proposed the first design of RF distance bounding that can be realized fully using wireless channel, but that involves multi-radio capabilities and additional hardware.

Our work can be classified as both channel-based and proximity-based authentication, since we exploit the fact that an off-body attacker have quite different RSS variation behavior with an on-body sensor. Different from existing works, BANA does not require any additional hardware, only legitimate sensors need to be placed on/near the body.

# 3. PROBLEM DEFINITION

## 3.1 System Model and Assumptions

We consider a wireless body area network composed of $n$ sensors and a CU. The sensors are carried on the body of a patient; they continuously measure and collect physiological data about the patient (e.g., heart rate, blood oxygenation, glucose level, etc.) and send them to the CU. They are limited in energy supply, memory space, and computation capabilities. The CU could be a more powerful hand-held device such as smart phone or PDA; it processes or aggregates the data, and then presents it to physicians/caregivers locally or to remote users. All the devices in a BAN are equipped with a radio interface, which enables them to communicate over wireless channel (e.g., Bluetooth, ZigBee, WiFi, etc.). The devices are also assumed to be within one-hop range of each other. We assume that the CU is not compromised. We do not assume the existence of any additional hardware (e.g., multiple antenna, accelerometer, GPS), or out-of-band communication channel. The CU is placed in close physical proximity of sensors and their distance is normally much smaller than two meters (e.g., holding by the user).

## 3.2 Attack Model

In this paper, we mainly consider impersonation attacks, where the attacker attempts to join the BAN by disguising either as a legitimate sensor devices or as the CU. The attacker(s) may either be a single device or multiple colluding ones, who may possess advanced hardware. They can forge physical addresses like MAC address, eavesdrop the wireless channel, modify, replay or inject false data, and can transmit packets at varying power levels.

In addition, the attacker may have knowledge about the wireless environment around the BAN. For example, it could survey the location where the BAN will be setup by measuring the channel in advance, and can derive corresponding signal propagation models. Besides, the attacker may make use of the history data collected in previous interactions with the BAN, to predict the path loss of the channel between itself and a legitimate node. The attacker is also aware of the deployed security mechanisms, the transmission technology, and the technical specs of the sensors and CU. Also, the attacker may either locate within either line-of-sight (LOS) or non-line-of-sight (NLOS) with respect to the BAN user and the devices. However, we assume that the attacker's device(s) are away from the body, whose distances are larger than those between legitimate sensors and the CU themselves. If the attacker is physically in close proximity of a user, it would be easily spotted.

Note that, in this paper we do not consider jamming or Denial-of-Service (DoS) attacks. During an authentication process, it is possible that attacker falsely claims to have the ID of a valid sensor, so as to confuse the CU about which one is legitimate, or simply prevent a legitimate sensor from being successfully authenticated. However, this can be regarded as one type of DoS attack.

## 3.3 Design Requirements

The primary goal is to achieve node authentication, that is, to distinguish a legitimate body sensor/CU from an attacker. This is a fundamental requirement for the security of a BAN. After authentication, a shared secret key can be established between each sensor node and the CU in order to

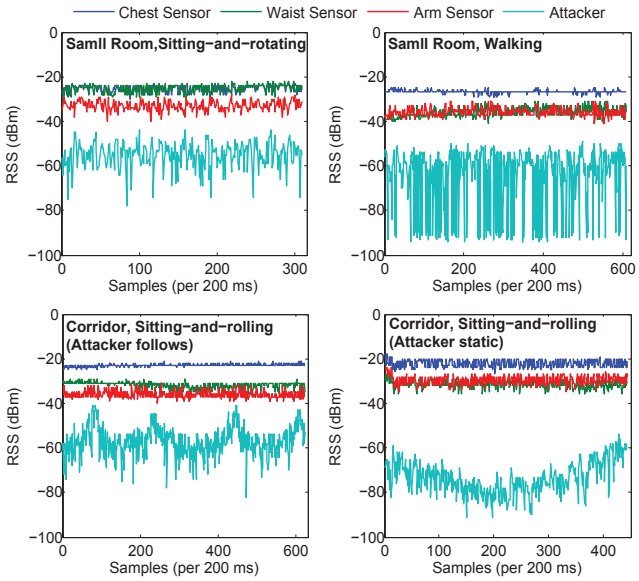


**Figure 1: RSS variations in different body motion scenarios.**

protect the sensitive health monitor data. We do not elaborate on shared key establishment in this paper since there are many existing techniques to do so (e.g., Diffie-Hellman)[2].

Moreover, the authentication mechanism shall have the following properties: (1) Usability, since the users of BAN are anticipated to be non-experts like normal patients. "*Plug-n-play*" is our desired usability goal. (2) Efficiency, resource consumption must be minimized to preserve energy; (3) Speed, since additional latency imposed by security mechanisms may cause a difference between live and death in EMS scenarios; (4) Low-cost: they should rely on *commercial off-the-shelf* (COTS) hardware and should not require big change to existing platforms. (5) Reliability, which means they should work under various types of scenarios.

# 4. UNIQUE CHANNEL CHARACTERISTICS OF A BAN

The channel within a BAN can display substantial differences with respect to other types of channels, such as in WLAN and cellular environments. There are some existing research on BAN's channel measurement [40]. Most of them focus on determining the channel model itself for enhancing communication performance; only a few of them studied the characteristics of BAN channel related to security purposes. Recently, Ali et al. observed that the channel between an on-body sensor (OBS) and off-body base station displays both slow and fast fading components [2]. They use it to facilitate secret key extraction from the channel, but it is not clear how can this be applied to BAN authentication.

In what follows, we use *on-body* channel to refer to the channel where both transceivers are located on the same body or in close vicinity to the body, and use *off-body* channel to refer to the situation that one of the transmitters is on-body (on the surface or in close vicinity to body) while the other is off-body (at a distance away). Note that, the off-body channel characteristics analyzed in this section applies to most types of attacker device, except those using a directional antenna to create a pointed, ideal path between the attacker and CU. However, as we will discuss later, although the directional attack seems possible theoretically, in practice it can be hard to carry out mainly due to the body motion in our scheme.

[2]For example, a possible solution is to split a Diffie-Hellman public key into chunks and carry each of them in an authentication packet in BANA. Then the man-in-the-middle attack will fail, because the middleman's packets' RSS variations cannot pass BANA's check.

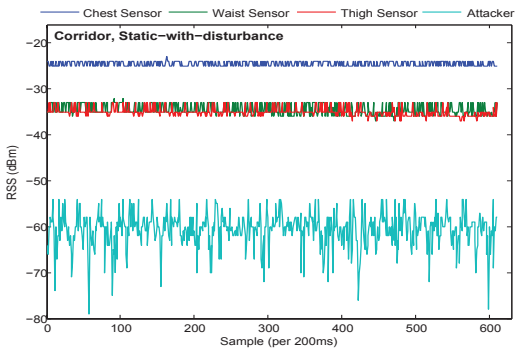


**Figure 2: RSS variations under channel disturbance.**

## 4.1 Distinct RSS Variation Profiles between On-body and Off-Body Channels

In this paper, we observe significant differences between the RSS variation behavior between on-body and off-body channels. That is, the off-body channel displays much severer fading than the on-body channel over time, in terms of both fading amplitude and rate. In particular, we found two classes of scenarios under which this difference is prominent: (1) *Body motion*, especially when the body parts are relatively static to each other. There are many real-world examples for such motions: slow-walking, sitting in a wheel-chair and pulled by others, rotating, lying on a moving operation table, etc. (2) *Channel disturbances*. Alternatively, when the body is static, moving objects/people between an off-body link creates a similar effect. For example, in a crowded hospital or emergency room environment.

**Experimental Evidences**. To testify our claim, we carried out experiments using five Crossbow's TelosB motes (TPR2400). The TelosB platform includes an IEEE 802.15.4 radio with integrated antenna, a low-power MCU with extended memory and an optional sensor suite. We configured three of these devices as body sensors, separately worn on the chest ($S_1$), strapped to the right waist ($S_2$), and tied to the left thigh ($S_3$). For the other two sensors, one works as CU that is tied to a pole carried by the patient (regarded as on-body), and another models an off-body attacker (off-body). The sensor placement and the configuration of small office are shown in Fig. 5. We performed experiments in two scenarios: a small office and a large corridor of a college building. For the small office scenario, the patient either walks randomly, or sits on a chair and spins. The off-body link is non-line-of-sight (NLOS) in this case, and the attacker remains static. For the corridor scenario, the patient sits on a wheelchair and moves back and forth along a straight line with the help of a caregiver; attacker is either static, or follows behind and moves in a similar pattern. In addition, to

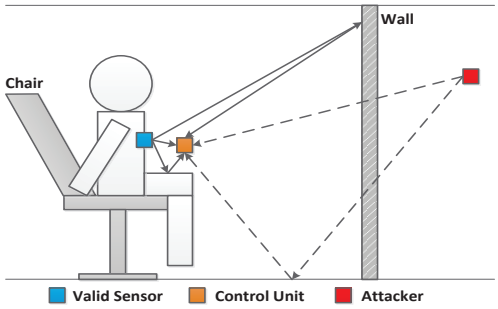


**Figure 3: Illustration of wireless channels from the OBS and the attacker, respectively, to the control unit.**

simulate channel disturbances, we let the patient be static while there are people walking around the corridor.

We measured the RSSI received from each other sensor by the CU, where the sampling step is 200ms. Results for body motion scenarios are shown in Fig. 1, while those for channel disturbance is shown in Fig. 2. Two prominent characteristics can be observed.

- **On-Body Channel is Much More Stable Even Under Body Motion.** For example, in Fig. 1, the RSS from the attacker is apparently experiencing large variations while RSS from all the OBSes are still stable with small fluctuations. The RSSI variations of OBSs are less than $5-10dB$, while for the attacker its RSSI varies much faster with a range of $45dB$. For other scenarios, similar observations can be found.
- **Off-Body Channel is Unpredictable.** The off-body channel's fading is much more random and unpredictable than the on-body channel.

Note that the difference in RSS variation profiles still holds when there is small relative motion between body parts. To validate its universality, we also conducted other sets of experiments in different rooms and on different subjects, and results are consistent. Due to space limitations they are not presented here.

## 4.2 Theoretical Explanation

Next we will analyze the reasons of above observed phenomenons. As we know, radio wave propagation is greatly affected by direct path loss, multipath, shadowing, and other interference, which are both time and environment specific and difficult to predict. Taking movement into account increases the unpredictability of the radio environment dramatically [18]. However, this has much less effect for an on-body channel than an off-body channel.

**On-Body Channel**: Although signal propagation over on-body channel suffers from the effect of the human body with its complex shape and different tissues, it is well-known that at very close range, the *direct path* (DP) is the dominant path among all the multi-path components [36]. As depicted in Fig. 3, since the OBS and CU are very close to each other (usually less than 1 meter), the RSS received from reflection off the walls and floors only contributes a small proportion to the overall RSS. Therefore, during body motions, the effects of signal reflection and absorption will not change dramatically as the OBS and the CU keep their position and distance relatively static. Ideally, the coherence time of the on-body channel goes towards infinity.

**Off-Body Channel**: For an off-body transceiver, the relative motion between it and CU/OBS results in Doppler shift. In addition, the motion also changes the phases and amplitudes of signals arriving from various multi-paths whereas the DP no long dominates. Thus when the off-body transceiver is at a certain distance away, the superposition of multi-path components lead to large-scale and fast variations in fading amplitude. This effect is particularly conspicuous in NLOS situations, as the signal is subjected to losses caused by penetrating walls, floors, doors and windows. Thus, any change in the environment will result in remarkable RSS variations at the receiver side. For a back-of-the-envelop calculation, assume the body is moving straight at $v = 0.6$m/s. The coherence time of the off-body channel is $T_c = \lambda/2v \approx 0.1$s, where $\lambda = 0.125$m if $f = 2.4$GHz. Note that our sample interval is 0.2s.

# 5. MAIN DESIGN OF BANA

This section describes the main design of BANA based on the channel characteristics. We first focus on the one-way authentication, that is the CU authenticates other body sensors. Our scheme can be adapted to handle the opposite case, which will be discussed in Sec. 6.

## 5.1 Overview

Our scheme exploits the fact that the RSS at the CU received from an off-body attacker experiences much larger fluctuations because of the multipath effect and Doppler spread, compared with that of an OBS. We formalize the degree of signal fluctuation as *average RSS variation* (ARV), which indicates the average amplitude of change in path loss between two consecutive time slots of RSS measurement (one time slot is slightly longer than the channel coherence time). In order to prevent the attacker from predicting its channel condition to the CU, we require each sensor to send response messages to the CU, after a time larger than the channel coherence time. After having collected all the RSSes over a short period of time and computed the ARV for each node, the CU uses cluster analysis to classify them into two groups. Due to large differences between the ARVs, the clustering procedure will have high chance of success. Note that, measuring RSS requires no additional hardware and can be fully realized on low-end sensor nodes.

## 5.2 The BANA Protocol

Our secure authentication protocol assumes that legitimate sensor devices have been attached to the patient's body before the execution of our protocol. One or more off-body attacker nodes may present in vicinity. Our protocol distinguishes legitimate on-body sensors from off-body attacker nodes as follows.

(1) The CU broadcasts a hello message $M = (x, t_0, t)$ using a certain transmission power $P_{tx}$ to nearby devices, asking them to respond after $x$ second(s), where $x$ is a system parameter, e.g., $x$ can be 1. The hello message $M$ sent by the CU requires all the responding devices to send back response messages $m$ repeatedly every $t$ milliseconds after $x$ second(s) and continue for $t_0$ seconds. The CU will not respond to any sensor device during the $t_0$ seconds until it finishes the authentication process, providing no oppor-

| Stage | The Control Unit (CU) | | The $i^{th}$ sensor |
|---|---|---|---|
| (1) Discovering | Broadcasts a hello message;<br>where $x$ is a random number chosen by the CU;<br>$t_0$ defines total response time;<br>$t$ defines time interval of each response message; | $\xrightarrow{M=(x,t_0,t)}$ | Responds after $x + \frac{t_r}{1000}$ seconds where $t_r$ is a random number picked by the sensor; |
| (2) Responding | Measures the channel; | $\xleftarrow{m_1,m_2,...,m_{NT}}$ | Sends response messages every $t$ milliseconds for total time of $t_0$ seconds, letting $NT = 1000 \times t_0/t$; |
| (3) Classification | Calculates the average RSS variations $ARV_i$:<br>$Sum_i = \sum \lvert RSS_k - RSS_{k+1} \rvert$, $ARV_i = Sum_i/NT$;<br>Classifies $ARV_1$, $ARV_2$, ... , $ARV_n$<br>into two groups; | | |
| (4) Decision | Accepts if $ARV_i$ belongs to the group with a smaller average RSS variation value; | $\xrightarrow{Acceptance}$ | Ready for data transmission. |
| | Rejects otherwise. | $\xrightarrow{Rejection}$ | Fails in authentication. |

**Figure 4: Description of the authentication process**

tunities to the attacker for measuring the realtime channel between itself and the CU.

(2) Upon receiving the hello message, a sensor device $i$ generates a small random number $t_r$, e.g., we can have $t_r < t$, and sends it back CU. CU collects the $t_r$'s from all responding devices and make sure there is no duplicated ones to avoids future transmission collision. After the CU has agreed on the random numbers, it notifies the responding devices to repeatedly send messages $m$ to the CU after $x$ seconds plus $t_r$ milliseconds. Specifically, the $i^{th}$ sensor keeps sending response messages $m_1, \ldots, m_{NT}$ every $t$ milliseconds and continue for $t_0$ seconds, where $NT = 1000 \times t_0/t$. Both $t_0$ and $t$ are appropriately set system parameters. For $t_0$, it should be large enough for the CU to collect sufficient signal samples and measure the channel accurately. But if $t_0$ is too large, a patient will spend too much time on sensor devices authentication which is not affordable to the patient if the data measured by the sensor devices is urgently needed for emergency treatment. For $t$, generally it must be no less than the coherence time to ensure accurate estimation of channel variation, where the coherence time is defined to be the time duration over which the channel impulse response is considered to be not varying.

(3) After having collected the RSSs for all the responding devices, the CU calculates the average RSS variation for each node $i$ by computing $ARV_i = Sum_i/NT$, where $Sum_i$ is the sum of all the absolute values of RSS variation for every two consecutive time interval $t$. Finding out values of $ARV_1, ARV_2, ..., ARV_n$ for all the received signals, the CU applies a classification algorithm to partition them into two groups, where one group has a smaller mean of $AVR$ while the other group has a larger one.

(4) Based on the classification result, the CU accepts the sensor devices whose $ARV$ values belong to the cluster with a smaller average of $ARV$ while rejecting the devices in the other group.

## 5.3 Discussion

1. Deployment: $n$ sensors are put to their designated places on the patient's body. And the CU is attached to an external equipment, which is placed at a relatively constant position and distance to all the worn sensors. All of the OBSes shall have a clear line of sight to the CU. The distances between each sensor and the CU $d_1$, $d_2$, ..., $d_n$ must be larger than half-wavelength. Therefore, no correlation exists between wireless channels to each sensor and those to the CU. In this case, even if the attacker is able to measure the signals sent by the legitimate sensors, it is not able infer the channel to the CU.

2. Average RSS Variation (ARV): to compare and distinguish remote sensors from on-body sensors, measurements of the signal fluctuations are necessary. According to what we observe from Fig.2, the RSS of a remote sensor was experiencing dramatic fluctuations, which changed very fast in a short period of time, while on-body sensors keep relatively stable RSS with small variations over time. So within a small time interval, the RSS variation of a remote sensor is mostly larger than that of a on-body sensor. Then over a period of time, the average RSS variation of the remote sensor will still be larger than that of the on-body sensor. Based on this observation, we utilize average RSS variation to check the degree of signal fluctuations for both remote sensors and on-body sensors. To calculate the average RSS variation, the CU adds up all the absolute values of RSS differences between every time interval for each signal, and divides the sum by the total number of discrete time points for that signal.

3. Classification method: In addition to the obvious differences of the average RSS variations between remote sensors and on-body sensors, we also noticed that the average RSS variation values are closed to each other for remote sensors, so are the on-body sensors themselves. Intuitively, these ARVs will form two distinct groups. In our protocol enables the CU to achieve this by employing a classification method. The sensors whose average RSS variation value belong to the group with a smaller overall average RSS variation, are trusted as valid sensors. Otherwise, they are treated as illegal sensors. As one of the popular classification algorithm, K-means clustering provides a method of cluster analysis aiming to partition $n$ observations into $k$ clusters, in which each observation belongs to the cluster with the nearest mean, and fit well for our scheme. Note that, K-means clustering requires no prior-knowledge about the data distribution, thus there is no training phase.

| Test Plan | Location | Movement | Patient | Attacker Placement |
|---|---|---|---|---|
| 1 | Small room | sitting-and-rotating | person 1 | Attacker #1,2: inside of the room.<br>Attacker #3,4: next door (separated by a wooden wall)<br>Attacker #5,6: more than 5 meters away |
| 2 | Small room | walking | person 1 | Attacker #1,2: inside of the room.<br>Attacker #3,4: next door (separated by a wooden wall)<br>Attacker #5,6: more than 5 meters away |
| 3 | Medium room | sitting-and-rotating | person 3 | Attacker #1,2: inside of the room.<br>Attacker #3,4: next door (separated by a wooden wall)<br>Attacker #5,6: more than 5 meters away |
| 4 | Corridor | sitting-and-rolling | person 1 | Attacker #1: following the patient.<br>Attacker #2-6: static, at different distances |
| 5 | Corridor | sitting-and-rolling | person 2 | Attacker #1: following the patient.<br>Attacker #2-6: static, at different distances |

**Figure 6: The Testing Plans**

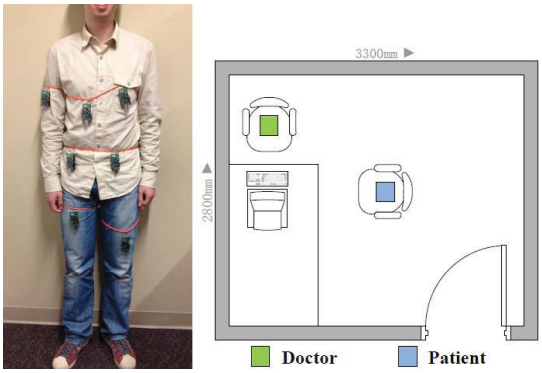


**Figure 5: Sensor Placement on the Human Body and the Small Room Layout.**

## 6. EVALUATION

We conducted experiments under different settings to validate our proposed scheme. Specifically, we took into account the effect of the following factors: position of the body sensor, surrounding environment such as room size, type of patient movement, location of the attacker, and difference between individual patients.

### 6.1 Experimental Setup and Results

In our experiments, we configured seven TelosB motes (numbered from 1 to 7) as OBSes, separately worn on the chest and the arms, strapped to the both sides of waist, and tied to both the left and right thighs. We used a TelosB mote to emulate the controller for simplicity. On receiving the signal from sensors, the controller measures the RSSI and sends it to the computer for analysis. By this we can emulate all the functionalities of a real controller. In each experiment we also put 6 TelosB motes (numbered from 1 to 6) at different locations with different distances to the patient to simulate the attackers. In our experiments, we use these motes mainly to measure the channel properties of body sensors and real attackers. Based on the collected data, we will analyze the probability at which legitimate body sensors are successfully accepted as well as the attackers' strategies and their successful probability of impersonating as authentic body sensors by using the strategies.

To simulate typical real-life scenarios, we choose three locations to conduct the experiments: a small office with a large table and two chairs inside, a medium size room with two large tables and five chairs inside, and the corridor in our university's building. The small room has four walls and its size is 2.8m(width) x 3.3m(length) x 2.7m(height) as shown in Fig. 5. The medium size room has the similar layout but of size 4.5m(width) x 5.5m(length) x 2.7m(height). The size of the corridor is 4.5m(width) x 40m(length) x 3.0m(height).

Our experiments were conducted on three persons to test the difference between individuals - person 1 and person 3 are males with heights of 170cm and 176cm respectively. Person 2 is a female with height of 170cm. During the experiments, we used the following movements which can easily be performed in real life: 1) *sitting-and-rotating*. In this movement, the person acting as the patient sits on a chair (with wheels) with the controller fixed to the front of her/him. Another person helps her/him rotate the chair slowly. This movement is only used in the small room and the medium size room. 2) *sitting-and-rolling*. In this movement, the person acting as the patient sits on a chair (with wheels) with the controller fixed to the front of her/him. Another person pushes the chair from back and walks from one end of the corridor to the other end. 3) *walking*. In this movement, the person acting as the patient stands and walks slowly. This movement will be tested in the small room where there may not be enough space to move the chair. In each movement, we fixed the controller at the distance of about 30cm away from the front side of the "patient".

To validate our proposed scheme we planned several experiment scenarios considering the combinations of the impacting factors. Fig. 6 summarizes out these test plans:

1) *Plan 1, 2:* The experiments were conducted on *Person 1* in the small room. For plan 1, the patient sits on a chair in the middle of the room. The movement used is sitting-and-rotating and the speed of the rotation is about 8 rpm. For plan 2, the person slowly but randomly walks in the room, holding the controller to the front of her/him. In both plans, the 6 "attackers" are strategically placed as follows: #1 and #2 are inside of the room, one on the table and the other hung on the door. Both of them are less than 2 meters away from the patient. #3 and #4 are placed at different places in the room next door, both less than 3 meters away from the patient. The wall between the two rooms is wooden. Both #5 and #6 are placed more than 5 meters away from the patient on the same floor in the building.

| | Plan 1 | Plan 2 | Plan 3 | Plan 4 | Plan 5 |
|---|---|---|---|---|---|
| OBS1 | 1.605 | 0.482 | 2.012 | 1.899 | 1.814 |
| OBS2 | 2.699 | 0.932 | 1.734 | 2.286 | 4.870 |
| OBS3 | 2.463 | 0.991 | 1.626 | 1.923 | 2.890 |
| OBS4 | 3.104 | 1.149 | 2.142 | 2.264 | 2.104 |
| OBS5 | 3.544 | 1.181 | 1.947 | 2.115 | 2.395 |
| OBS6 | 2.133 | 1.010 | 1.844 | 1.910 | 1.677 |
| OBS7 | 1.922 | 0.836 | 1.709 | 2.122 | 2.359 |
| ATK1 | 5.667 | 6.182 | 6.319 | 4.536 | 4.447 |
| ATK2 | 6.346 | 6.342 | 5.301 | 5.971 | 5.860 |
| ATK3 | 5.754 | 7.003 | 6.005 | 5.097 | 4.964 |
| ATK4 | 5.259 | 5.936 | 6.211 | 5.365 | 5.359 |
| ATK5 | 5.835 | 6.670 | 5.255 | 5.173 | 5.778 |
| ATK6 | 5.152 | 4.721 | 5.438 | 5.527 | 5.753 |

**Figure 7: The average RSS variation measurements (in dB) for Test Plan 1-5. On-Body Sensors (OBS) #1-7 are located on middle chest, left waist, right waist, left thug, right thug, left chest, and right arm respectively. Attackers (ATK) are located as described in Fig. 6**

2) *Plan 3:* The setting of plan 3 is similar to that of plan 1 and 2. The main difference is that the distances between the attackers and the patient are a bit larger than those in plan 1 and 2 because of a larger room size. In this plan *Person 3* acts as the patient.

3) *Plan 4, 5:* These two experiments were conducted in the corridor in our university's building. In both plans we used the movement of sitting-and-rolling. Plan #4 is conducted on *Person 1* and #5 is on *Person 2*. The placement of the "attackers" are the same in both plans: attacker #1 follows the patient at a fixed distance of 1 meter; attackers #2 - 6 are randomly distributed along the corridor without moving.

We intend to use these experiments to simulate several typical real life scenarios in which the body sensors are authenticated in places such as the hospital testing room, the home room, the hallway of the hospital, etc.

At the beginning of each experiment, the controller broadcasts a hello message to all the nodes. After 1 second, the controller starts to receive messages and measure their RSSIs every 200ms, i.e., $t = 200$ms[3]. Each experiment lasts for 1-2 minutes. After having collected all the RSSIs, for each node $i$ we calculate the the average RSS variation (ARV) between two consecutive 200ms slots. A larger ARV means that the communication channel between the node and the controller undergoes sharp fluctuation during the experiment. To generate sample data for statistics study, we conducted 15 experiments in total, with some of the cases repeatedly tested. Fig. 7 gives a summary of the measured ARVs under different test plans. For brevity, we just show the results of 5 non-repeated experiments. In the following section we will show the statistic data which includes the complete set of results generated in the 15 experiments.

From this table we can observe the following facts: 1) 34 out of the total 35 on-body sensor ARVs are less than 4dB. All of them are less than 5dB. But those of all the "attackers" are greater than 4dB. This verifies our observation that by introducing appropriate movements the off-body nodes (attackers) tend to undergo larger fluctuation in path loss than the on-body sensors. 2) The variance of the ARVs of on-body sensors in each test plan is relatively small (for example in plan 1 it is 0.4609 as compared to 3.0186, the overall variance of all the ARVs in the plan). Intuitively this indicates that the ARVs of on-body sensors tend to converge to a certain (relatively small) value and form a cluster. Correct identification of such a cluster will lead to successful authentication of on-body sensors. 3) Occasionally, few on-body sensors would experience large path loss fluctuation (resulting in a large ARV, e.g., plan 5 OBS2) due to various reasons such as inappropriate placement of the CU, interruption from improper body movement, etc. This will cause rejection of the on-body sensor(s) (i.e., the false positive error). 4) The ARVs of on-body sensors are empirically bounded. In all our 15 test cases, there is no on-body sensor with measured ARV exceeding 5dB. 5) Deploying off-body nodes ("attackers") in vicinity does not necessary results in a relatively similar ARVs. For example, attacker #2 and #3 in plan 1 and 2 are placed about 1 meter away from each other in the same room. But their ARVs differs remarkably as compared to those of other attackers. This can be explained by factors such as different multipath effects as well as distinct Doppler spread if the two nodes are more than half wave length away from each other.

## 6.2 Evaluation

Based on the experiment results obtained above, we first evaluate the accuracy of our scheme without strategic attackers[4]. In particular, we will study the false positive rate (i.e., rate of failing to accept authentic on-body sensors) and the false negative rate (i.e., rate of failing to reject off-body attackers.). Then, we discuss several possible strategic attacks, their impacts, and our countermeasures. Finally, we evaluate the efficiency of our proposed scheme, including computation/communication costs and authentication time.

### 6.2.1 Effectiveness

To study the statistical property of the scheme we conducted 15 experiments under the five test plans. In addition to the 5 experiments presented in Fig. 7, the other 10 experiments were conducted based on the five plans by slightly but randomly changing some settings such as the speed of movement and the number and/or the position of the on-body sensors. From each experiment, we obtained a set of ARVs on which we ran the classification algorithm to differentiate on-body nodes and off-body nodes (attackers). In particular, we used the *kmeans* function in Matlab with the cluster number set as 2. We study the impacts on the false positive rates and false negative rates by the following factors respectively: the location of the experiment, the type of movements, and the choice of people. For each case, the *false positive rate* is computed as the percentage of total number of rejected on-body sensors out of the total number of on-body sensors, i.e.,

$$\text{false positive rate} = \frac{\sum_{i \in EXP}(\#\text{ of rejected OBSs})}{\sum_{i \in EXP}(\text{total } \#\text{ of OBSs})} \cdot 100\%,$$

where $EXP$ mean the set of all the experiments in the

[3]To make 200 ms greater than the coherence time of the channel between the controller and each individual attacker, in each experiment we assure that the controller moves at a speed greater than 31.25cm per second (Note that the wavelength of IEEE 802.15.4 signal is about 12.5cm).

[4]Attackers who employ some strategies to spoof the CU, rather than following the protocol honestly.

| | False Positive | False Negative |
|---|---|---|
| small | 3.7% | 0 |
| medium | 2.9% | 0 |
| corridor | 3.3% | 0 |
| sitting-and-rotating | 2.2% | 0 |
| sitting-and-rolling | 3.7% | 0 |
| walking | 4.8% | 0 |
| person 1 | 2.0% | 0 |
| person 2 | 4.8% | 0 |
| person 3 | 2.8% | 0 |
| overall | 3.3% | 0 |

**Figure 8: The false positive rates and false negative rates under different settings with non-strategic off-body attackers.**

case. Similarly, the *false negative rate* is computed as the percentage of total number of accepted off-body sensors (attackers) out of the total number of off-body sensors (attackers).

Our analysis results are summarized in Fig. 8. From this table we observe that the false negative rate in our experiments is zero. This is mainly due to the fact that the off-body nodes (attackers) did not launch any strategic attack during the experiment. But such a result does indicate that our scheme is effective against non-strategic attacks (in which an off-body device is deployed in the vicinity of the patient hoping to get authenticated as an on-body sensor). The false negative rates are computed for scenarios with different locations and movements as well as different individuals. As is shown the difference among the three locations is no larger than 0.8%, which indicates the less impact from location as long as the environment surrounding the patient is relatively simple, e.g., not many reflecting angles or objects near the patient. The impact of the movement is slightly higher as compared to that of the location. For example, the false positive rate for *walking* almost doubles that for *sitting-and-rotating* (4.8% vs. 2.2%). This is mainly because it is usually harder for individuals, unless well-trained, to control the smoothness of the movement (i.e., keeping the relative location between the CU and on-body sensors stable) while walking. But it will be relatively easier while sitting on a chair. From the results, we also observe a slight difference among individuals. But such a difference is mainly caused by the difference of individuals' controlling of the movements. The overall false positive rate is 3.3% taking all the 15 experiments into accounts.

### 6.2.2 Security Against Strategic Attackers

A smart attacker may carry out strategic attacks to improve the chance of getting the off-body nodes accepted by the CU. For this purpose the attacker can employ the following two methods: 1) reducing the fluctuation of path loss measured by the CU via varying the transmission power; 2) deviating the clustering method.

*Attack Method 1:* To reduce the fluctuation of path loss measured by the CU, the attacker needs to accurately measure or predict the communication channel to the CU so as to compensate the path loss via adjusting the transmission power. But as the CU does not transmit any signal after having sent out the request message, the attacker is

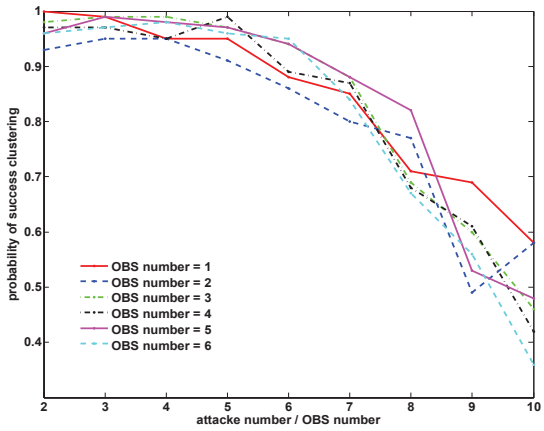


**Figure 9: Impact of the attacker node number on our clustering method.**

not able to measure the realtime channel impulse response. Alternatively, the attacker may resort to measuring the realtime property of the channel to on-body sensors as the estimation of the channel to the CU. However, in our scheme the CU is located at least half wave length away from the on-body sensors, the channel to them are mutually uncorrelated. Another way is to predict the channel based on historical channel measurements. However, the channel coherence time is very short (less than 200ms) due to the movements we introduced.

*Attack Method 2:* In this method, the attacker attempts to deviate our clustering method through introducing an overwhelming number of off-body attacker nodes. This method may work because for clustering algorithm like k-means the centroid of the clusters tends to locate close to the majority. In the extreme case, if there is just a single on-body sensor but a large number of off-body attacker nodes, the clusters will be centered around the attacker nodes (i.e., their ARVs) with very high probability. To verify the effect of such attack, we did a simulation by varying the number of attacker nodes to make it times more than that of the on-body sensors. Each node is randomly assigned a ARV according to the real distribution measured in our experiments. For any given number of attacker nodes and on-body sensors, we run the classification algorithm 1000 times and measure the probability of successful clustering (i.e., no false positive/negative error). We consider four cases with on-body sensor number of 1, 2, 3, 4, 5, and 6 respectively. The simulation result is shown in Fig. 9. From this figure, it is clear that when the ratio of attacker number to on-body sensor number is less than 6, our clustering scheme always succeeds with a probability greater than 90%.

Although it seems difficult to completely thwart this attack, launching such a powerful attack is not only expensive but also easily detectable due to the large number of attacking devices involved. To keep the cost of such attack high, while clustering the CU can always create a small number of replica nodes for the node with the minimum ARV. This is because the attacker needs to deploy times more nodes to achieve a relatively high success probability.

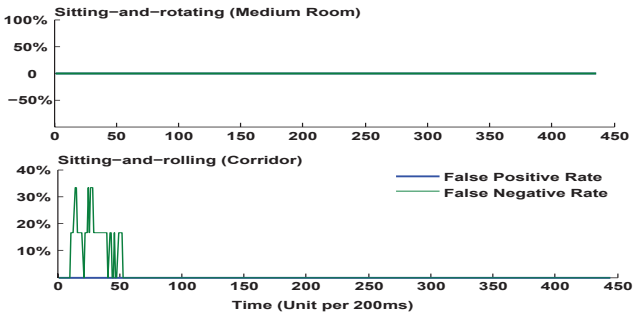


**Figure 10: False positive/negative rate at different time.**

### 6.2.3 *Efficiency*

The efficiency of our proposed scheme can be evaluated by authentication time, computation and communication costs.

*Authentication Time:* In our experiments, authentication time is set as 1-2 minutes, letting the CU receive sufficient number of sample RSSs for analysis. However, the actual time needed for authenticating a sensor node may not necessarily have to be 2 minutes. To measure the actual time required to authenticate a sensor node, for each $i \leq NT$ we plotted a false positive/negative rate calculated from the subset of sample $[1, \cdots, i]$, where $NT$ is the total number of samples obtained from the experiment and the samples were taken per 200ms. As shown in Fig. 10, for some experiments both false positive rate and false negative rate quickly become stable as 0. This means that for these cases, the on-body sensor nodes and off-body attackers can be immediately differentiated by checking only several samples. For some experiments, the two rates are not stable until some number of samples are examined as shown in the bottom picture in Fig. 10. This is particularly true for some special locations such as large empty hallway with less multi-path effect. This is because the channel between the remote LOS attacker and the CU is less sensitive to certain movement, e.g., slowly rolling toward the attacker, since the affect of Doppler spread is dominant. Interestingly, analysis on these experiment results shows that in each experiment the two error rates become stable after the first 60 samples (i.e., 12s). This means that in all our experiments, the CU just need to measure up to 12 second to obtain the same authentication results as we have had. For cases of small room and medium room, the time can be reduced to less than 1 second.

*Computation and Communication Costs:* The computational cost for each sensor node is negligible since no time-consuming task is executed on it. On the controller's side, the most computation-intensive task the execution of the clustering algorithm. As the k-means clustering itself is NP-hard, heuristic algorithms are usually employed. The complexity of the algorithm can be $O(n^{dk+1}logn)$ if $d$ and $k$ are fixed[16], where $n$ is the number of $d-$dimension entities to be clustered, and $k$ is the number of clusters. In our scheme, $d$ and $k$ are fixed to 1 and 2 respectively. So the complexity can be $O(n^3logn)$, where $n$ is corresponding to the number of sensor nodes which is a relatively small number. The communication cost for each body sensor is mainly caused by the messages sent to the CU every 200ms, which only needs to include the node's identity.

## 6.3 Discussion and Future Work

From our experiments, it is clear that our proposed solution is effective, with very high success probability in distinguishing legitimate on-body sensors from off-body nodes, including both non-strategic and strategic attacker nodes. the motions being studied can be easily carried out by any inexperienced patient in typical real life scenarios. They are very effective in creating the difference of RSS variation between on-body and off-body links, which will increase the accuracy of the clustering results.

*Realizing two-way authentication*: In the above we mainly showed how the CU authenticates body sensor nodes. For the other way round, we can let the CU send response messages to all the sensors after sensors' messages. Note that the real CU in the BAN is assumed to be not compromised (continuously presented). Due to the channel reciprocity, the RSS values received by each sensor from the CU are also more stable over time than those from the attackers. Thus if there exists more than one claimed-to-be CUs, each sensor will pick the node with the smallest ARV as CU.

For the sake of two-way authentication, we are assuming isotropic noise conditions, meaning that the ambient RF energy located at Alice, Bob or Eve are roughly equivalent, and consequently radio links will be approximately symmetric due to channel reciprocity. We note that similar assumptions and limitations were identified in [29]. What is important, though to realize in our work, is that the off-body channel will exhibit significantly higher variance than the on-body channel, thereby facilitating our methods.

We note that there has been further investigation into using the actual channel response, as opposed to RSS, for authentication. We refer the reader to [48, 49] for examples of this complementary work.

*Attacks using directional antenna:* A possible limitation of BANA is when dealing with attackers provided with a directional antenna. In BANA, the distinction between on- and off-body channels is mainly introduced by the multi-path environment surrounding a BAN. Such a distinction could be eliminated when the attacker uses a directional antenna to create a focused beam to reduce the multi-path effect. While this attack seems to be effective, we believe that it is difficult to launch in practice. In particular, in BANA the patient carries out random motions that we suggested. Such random motions will make it hard for the attacker's directional antenna to accurately direct toward the patient, which is particularly true for NLOS scenarios such as closed rooms. To improve the accuracy of pointing toward the patient, the attacker may want to use an antenna with a wider beam. However, a large beam angle can easily make the multi-path effect eminent. On the other hand, a highly directional antenna with a narrow beam is usually large in size, which would make the attacking device more easily detected in practice. As an interesting future work, we will further study the practicality of attacks using directional antenna.

# 7. CONCLUSIONS

This paper, for the first time, proposes a lightweight authentication scheme for body area networks – BANA without depending on prior-trust among the nodes. We achieve this by exploiting physical layer characteristics unique to a BAN, namely, the distinct variation behaviors of received signal strength (RSS) between an on-body communication

link and an off-body link. Specifically, the latter is much more unstable over time, especially under various artificially induced whole body motions. Our experiment results have validated such an observation and shown that our clustering method is effective in differentiating on-body sensors from off-body nodes. Analysis shows that our scheme is effective even with the presence of a number of strategic attackers. For future work, we will explore a more effective solution that thwarts strategic attackers with an overwhelming number and study the practicality of attacks using directional antenna. In addition, we will explore other implications of BAN's channel characteristics in enhancing its security from physical layer, for example, secret key extraction. Finally, we note that our study has assumed that the radio link is symmetric between Alice and Bob, and the amount to which this assumption is true in general needs to be extensively explored in future work, which we are conducting.

## Acknowledgements

We thank the anonymous reviewers, and our shepherd, Prof. Wade Trappe for their helpful comments.

# 8. REFERENCES

[1] Experts see data breach risks in medical devices on hospital networks. `http://www.ihealthbeat.org/articles/2011/5/12/`.

[2] S. Ali, V. Sivaraman, and D. Ostry. Secret key generation rate vs. reconciliation cost using wireless channel characteristics in body area networks. In *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on*, pages 644–650. IEEE, 2010.

[3] S. Brands and D. Chaum. Distance-bounding protocols. In *Advances in Cryptology - EUROCRYPT'93*, pages 344–359. Springer, 1994.

[4] L. Cai, K. Zeng, H. Chen, and P. Mohapatra. Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas. In *Network and Distributed System Security Symposium*, 2011.

[5] H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In *IEEE S & P '03*, page 197, 2003.

[6] O. Cheikhrouhou, A. Koubaa, M. Boujelben, and M. Abid. A lightweight user authentication scheme for wireless sensor networks. In *Computer Systems and Applications (AICCSA), 2010 IEEE/ACS International Conference on*, pages 1 –7, may 2010.

[7] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung. Body area networks: A survey. *Mob. Netw. Appl.*, 16:171–193, April 2011.

[8] S. Cherukuri, K. K. Venkatasubramanian, and S. K. S. Gupta. Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. *Parallel Processing Workshops, International Conference on*, 0:432, 2003.

[9] O. Delgado-Mohatar, A. Fuster-Sabater, and J. M. Sierra. A light-weight authentication scheme for wireless sensor networks. *Ad Hoc Networks*, 9(5):727 – 735, 2011.

[10] S. Devi, R. Babu, and B. Rao. A new approach for evolution of end to end security in wireless sensor network. *International Journal on Computer Science and Engineering*, 3:2531–2543, 2011.

[11] R. Di Pietro, L. Mancini, and A. Mei. Random key-assignment for secure wireless sensor networks. In *Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 62–71. ACM, 2003.

[12] W. Du, J. Deng, Y. Han, P. Varshney, J. Katz, and A. Khalili. A pairwise key predistribution scheme for wireless sensor networks. *ACM Transactions on Information and System Security (TISSEC)*, 8(2):228–258, 2005.

[13] L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In *CCS '02*, pages 41–47, 2002.

[14] D. Halperin, T. Heydt-Benjamin, B. Ransford, S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno, and W. Maisel. Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses. In *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pages 129–142. Ieee, 2008.

[15] X. Hei and X. Du. Biometric-based two-level secure access control for implantable medical devices during emergencies. In *The 30th IEEE International Conference on Computer Communications (INFOCOM 2011)*, pages 346 – 350, Shanghai, P.R.China, April 2011.

[16] M. Inaba, N. Katoh, and H. Imai. Applications of weighted voronoi diagrams and randomization to variance-based k-clustering: (extended abstract). In *Proceedings of the tenth annual symposium on Computational geometry*, SCG '94, pages 332–339, New York, NY, USA, 1994. ACM.

[17] E. Jovanov, A. Milenkovic, C. Otto, and P. C. de Groen. A wireless body area network of intelligent motion sensors for computer assisted physical rehabilitation. *J Neuroengineering Rehabil*, 2(1), March 2005.

[18] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca. Ensemble: cooperative proximity-based authentication. In *Proceedings of the 8th international conference on Mobile systems, applications, and services*, MobiSys '10, pages 331–344, New York, NY, USA, 2010. ACM.

[19] M. Li, W. Lou, and K. Ren. Data security and privacy in wireless body area networks. *IEEE Wireless Communications Magazine*, Feb. 2010.

[20] M. Li, S. Yu, J. D. Guttman, W. Lou, and K. Ren. Secure ad-hoc trust initialization and key management in wireless body area networks. *ACM Transactions on Sensor Networks (TOSN)*, (To Appear), 2012.

[21] M. Li, S. Yu, W. Lou, and K. Ren. Group device pairing based secure sensor association and key management for body area networks. In *INFOCOM, 2010 Proceedings IEEE*, pages 1 –9, march 2010.

[22] D. Liu and P. Ning. Establishing pairwise keys in distributed sensor networks. In *CCS '03*, pages 52–61, 2003.

[23] D. Liu, P. Ning, and W. Du. Group-based key predistribution for wireless sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 4(2):1–30, 2008.

[24] K. Lorincz, D. Malan, T. Fulford-Jones, A. Nawoj,

A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton. Sensor networks for emergency response: challenges and opportunities. *IEEE Pervasive Computing*, 3(4):16–23, Oct.-Dec. 2004.

[25] K. Lorincz, D. Malan, T. Fulford-Jones, A. Nawoj, A. Clavel, V. Shnayder, G. Mainland, M. Welsh, and S. Moulton. Sensor networks for emergency response: challenges and opportunities. *IEEE Pervasive Computing*, 3(4):16–23, Oct.-Dec. 2004.

[26] K. Malasri and L. Wang. Addressing security in medical sensor networks. In *HealthNet '07*, pages 7–12, 2007.

[27] M. Mana, M. Feham, and B. A. Bensaber. A light weight protocol to provide location privacy in wireless body area networks. *CoRR*, abs/1103.3308, 2011.

[28] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam. Proximate: proximity-based secure pairing using ambient wireless signals. In *Proceedings of the 9th international conference on Mobile systems, applications, and services*, pages 211–224. ACM, 2011.

[29] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: extracting a secret key from an unauthenticated wireless channel. In *Proceedings of the 14th ACM international conference on Mobile computing and networking*, pages 128–139. ACM, 2008.

[30] R. Mayrhofer and H. Gellersen. Shake well before use: Authentication based on accelerometer data. In A. LaMarca, M. Langheinrich, and K. Truong, editors, *Pervasive Computing*, volume 4480 of *Lecture Notes in Computer Science*, pages 144–161. Springer Berlin / Heidelberg, 2007.

[31] R. Mayrhofer and H. Gellersen. Shake well before use: Intuitive and secure pairing of mobile devices. *IEEE Transactions on Mobile Computing*, 8:792–806, 2009.

[32] M. Patel and J. Wang. Applications, challenges, and prospective in emerging body area networking technologies. *Wireless Communications, IEEE*, 17(1):80 –88, february 2010.

[33] N. Patwari and S. Kasera. Robust location distinction using temporal link signatures. In *Proceedings of the 13th annual ACM international conference on Mobile computing and networking*, pages 111–122. ACM, 2007.

[34] A. Perrig, R. Szewczyk, J. Tygar, V. Wen, and D. Culler. Spins: Security protocols for sensor networks. *Wireless networks*, 8(5):521–534, 2002.

[35] C. Poon, Y.-T. Zhang, and S.-D. Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. *IEEE Communications Magazine*, 44(4):73–81, April 2006.

[36] T. Rappaport and L. Milstein. Effects of radio propagation path loss on ds-cdma cellular frequency reuse efficiency for the reverse channel. *Vehicular Technology, IEEE Transactions on*, 41(3):231 –242, aug 1992.

[37] K. Rasmussen and S. Capkun. Realization of rf distance bounding. In *Proceedings of the USENIX Security Symposium*, 2010.

[38] K. Rasmussen, C. Castelluccia, T. Heydt-Benjamin, and S. Capkun. Proximity-based access control for implantable medical devices. In *Proceedings of the 16th ACM conference on Computer and communications security*, pages 410–419. ACM, 2009.

[39] K. Singh and V. Muthukkumarasamy. Authenticated key establishment protocols for a home health care system. In *ISSNIP '07*, pages 353–358, Dec. 2007.

[40] D. Smith, L. Hanlen, J. Zhang, D. Miniutti, D. Rodda, and B. Gilbert. Characterization of the dynamic narrowband on-body to off-body area channel. In *Communications, 2009. ICC'09. IEEE International Conference on*, pages 1–6. IEEE, 2009.

[41] C. C. Tan, H. Wang, S. Zhong, and Q. Li. Body sensor network security: an identity-based cryptography approach. In *ACM WiSec '08:*, pages 148–153, 2008.

[42] K. Timm. Medical device hacking prompts concern. `http://www.cyberprivacynews.com/2011/08/medical-device-hacking-prompts-concern/`.

[43] A. Varshavsky, A. Scannell, A. LaMarca, and E. De Lara. Amigo: proximity-based authentication of mobile devices. In *Proceedings of the 9th international conference on Ubiquitous computing*, UbiComp '07, pages 253–270, Berlin, Heidelberg, 2007. Springer-Verlag.

[44] K. Venkatasubramanian, A. Banerjee, and S. Gupta. Pska: Usable and secure key agreement scheme for body area networks. *Information Technology in Biomedicine, IEEE Transactions on*, 14(1):60–68, 2010.

[45] K. Venkatasubramanian and S. Gupta. Physiological value-based efficient usable security solutions for body sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, 6(4):1–36, 2010.

[46] K. Venkatasubramanian, S. Gupta, R. Jetley, and P. Jones. Interoperable medical devices: Communication security issues. *Pulse, IEEE*, 1(2):16–27, 2010.

[47] K. K. Venkatasubramanian and S. K. S. Gupta. Physiological value-based efficient usable security solutions for body sensor networks. *ACM Trans. Sen. Netw.*, 6:31:1–31:36, July 2010.

[48] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe. Using the physical layer for wireless authentication in time-variant channels. *Wireless Communications, IEEE Transactions on*, 7(7):2571 –2579, july 2008.

[49] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe. Channel-based detection of sybil attacks in wireless networks. *Trans. Info. For. Sec.*, 4:492–503, September 2009.

[50] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li. Imdguard: Securing implantable medical devices with the external wearable guardian. In *The 30th IEEE International Conference on Computer Communications (INFOCOM 2011)*, pages 1862 – 1870, Shanghai, P.R.China, April 2011.

[51] K. Zeng, K. Govindan, and P. Mohapatra. Non-cryptographic authentication and identification in wireless networks. *Wireless Commun.*, 17:56–62, October 2010.

[52] T. Zia and A. Zomaya. A lightweight security framework for wireless sensor networks. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, 2:53–73, september 2011.