BANA: Body Area Network Authentication Exploiting Channel Characteristics

Lu Shi, *Student Member, IEEE,* Ming Li, *Member, IEEE,* Shucheng Yu, *Member, IEEE,* and Jiawei Yuan, *Student Member, IEEE*

***Abstract*—In wireless body area network (BAN), node authentication is essential for trustworthy and reliable gathering of patient's critical health information. Traditional authentication solutions depend on prior trust among nodes whose establishment would require either key pre-distribution or non-intuitive participation by inexperienced users. Most existing non-cryptographic authentication schemes require advanced hardware 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. Different from previous work, BANA does not depend on prior-trust among nodes and can be efficiently realized on commercial off-the-shelf low-end sensors. We achieve this by exploiting a unique physical layer characteristic naturally arising from the multi-path environment surrounding a BAN, i.e., the distinct received signal strength (RSS) variation behaviors among on-body channels and between on-body and off-body communication channels. Based on distinct RSS variations, BANA adopts clustering analysis to differentiate the signals from an attacker and a legitimate node. We also make use of multi-hop on-body channel characteristics to enhance the robustness of our authentication mechanism. 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.

***Index Terms*—Wireless Body Area Network, Sensor, Authentication, RSS, Physical Layer.**

I. Introduction

WIRELESS body area network (BAN) has been an area of significant research in recent years [1], [2]. A BAN is a wireless network usually formed by lightweight, small-size, ultra-low-power, interoperable and intelligent wearable sensors [2], which are strategically placed on the body surface, around body or implanted inside body. To monitor the wearer's health status or motion pattern, these sensors measure, process, and transmit physiological signals to a control unit (CU) without constraining the wearer's activities. Physicians and caregivers can then access the collected data for real-time diagnosis and trigger treatment procedures in return. The BAN technology enables numerous exciting applications, such as ubiquitous health monitoring [4] and emergency medical response (EMS) [5], 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 great privacy concerns in the public towards interoperable medical devices (IMDs) [6]; however, data security in BANs has not drawn enough attention, although the lack of it would lead to fatal consequences [7], [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, IMDs are not designed with enough security considerations. Over the years, a number of remote hacking incidents of individual IMDs [9], [10] are reported, which exploited unprotected wireless channels. In BANs, the situation is even worse if attackers 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) [11], [12], [13], [14], [15], [16]. However, directly applying this method to a BAN requires end-users to basically trust the whole distribution chain which may involve numerous less trustworthy users. In addition, BAN's user is usually inexperienced 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 medical sensors become ubiquitous, they could be compromised and pre-shared secret keys can be stolen. These keys allow attackers to pretend to be any legitimate node, which renders traditional cryptographic authentication mechanisms ineffective. Therefore, node authentication mechanisms in BAN should

Manuscript received September 15, 2012; revised January 1, 2013 and April 30, 2013.

L. Shi, S. Yu, and J. Yuan are with Department of Computer Science, University of Arkansas at Little Rock, AR 72204 (e-mail: {lxshi, sxyu1, jxyuan}@ualr.edu).

M. Li is with Department of Computer Science, Utah State University, UT 84322 (e-mail: ming.li@usu.edu).

Digital Object Identifier 10.1109/JSAC.2013.130913.

have *minimal reliance on cryptography*. Finally, low-end medical sensors 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 [17], or significant modifications to the system software. It is important to note that we *should not introduce additional hardware assumptions* to the BAN, not only because of extra cost but also due to compatibility issue with legacy systems.

Identifying these challenges, in this paper we put forward BANA, a practical node authentication scheme for BANs that does not depend on prior-trust/pre-shared secrets among nodes. We exploit unique physical layer characteristics within a BAN environment, i.e. 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-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 design BANA based on this characteristic, and utilize clustering analysis to differentiate signals from a legitimate node and an attacker.

Moreover, we observe that authentication is transitive for BAN. In other words, if node A believes node B is on-body and the CU believes node A is on-body, it is safe for CU to believe that B is on the same body as A. Utilizing this transitivity property, BANA can be extended to multi-hop authentication for on-body nodes with relatively unstable single-hop channel to the CU. Complementary sensors can be placed on body or nearby for relaying purpose if necessary, so that each on-body device has at least one relatively stable multi-hop channel to the CU. These extra nodes can be small and simple devices that only sense, send and receive radio signals. This type of sensors is widely available at low cost in the market, and is easily attached to human body without affecting normal movements. By employing stable multi-hop channels for authentication, the performance of BANA is further improved with lower false positive rate.

Experimental and simulation results show 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. Besides, BANA can be efficiently realized on commercial off-the-shelf (COTS) low-end sensor devices.

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 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, our scheme can accurately identify multiple colluding attackers even when their number is up to 5 times of legitimate nodes, with minimal amount of overhead. Authentication time can be as short as 12 seconds for a group of 6 body sensors.

Note that this paper is the extended version of our conference paper [18]. The rest of this paper is organized as follows. We review related work in Section II. Problem definition is introduced in Section III. Section IV presents our new findings on channel characteristics, while Section V gives BANA's main design. We further extend BANA to multi-hop authentication in Section VI. Section VII evaluates BANA's performance compared with multi-hop BANA. Section VIII discusses the security and usability of our scheme, followed by the conclusion in Section IX.

II. Related Work

Related research on authentication in WSNs, especially in BANs can be mainly divided into two categories – cryptographic and non-cryptographic mechanisms. Traditionally, authentication in WSNs and BANs relied on the existence of prior security context [19], [20], [21], [22], [23]. If the device in BANs is physically compromised, the prior security context in the device will be disclosed to attackers. Besides, most of those mechanisms generally either involve high computational overhead or complex key management. Among different cryptographic methods, IBE-based authentication mechanisms [24], [25], [26] do not require prior-trust among nodes but a trusted certificate authority for key generation. It is also 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 [27], [28]). However, they assumed the existence of additional out-of-band (OOB) secure channel that facilitates human-aided verification, which may not be intuitive to use. To avoid above issues, [29] proposed a lightweight authentication scheme for BANs utilizing hash-chain techniques, but only achieves 70% accuracy.

From another perspective, non-cryptographic method provides an alternative way of authentication without key pre-distribution and non-intuitive user participation. And most non-cryptographic schemes have simpler protocols with less complicated computation. Thus, in what follows, we focus on surveying non-cryptographic authentication techniques related to BANs.

A. Biometric-based Authentication

Physiological values are used to assist authentication by measuring and comparing physiological signals separately at

[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. VIII.

the sender and the receiver [30], [31], [32], [33], [34], [35], [36], such as electrocardiogram (EEG), iris, fingerprint etc. Although these methods do not rely on pre-shared secrets, it is hard for body sensors in different positions to measure the same physiological signal with the same accuracy. Common accelerometer data extracted from body motion is also used for authentication in [37], [38], but specialized sensing hardware is required for every sensor.

B. Channel-based Authentication

Recently there has been an increasing interest in RSS-based authentication [39], [40], [41]. Channel-based solutions leverage the observation that RSS tends to vary over time due to mobility and channel environments. Zeng et al. [17] proposed to use temporal RSS variation lists to handle identity-based attack, where an intruder 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 identity to impersonate). The secure device pairing scheme proposed by [41] performed proximity detection based on differential RSS, but requires 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 [42] uses channel impulse response, but this method requires a learning phase and advanced hardware platforms such as GNU radio.

C. Proximity-based Authentication

Several schemes are based on co-location detection. Amigo in [39] 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 [40], 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. [43] 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 [44], such as distance bounding [45]. The general concern with RF distance bounding is it requires specialized/advanced hardware; otherwise high accuracy cannot be achieved. In [46], 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 authentication scheme is both channel-based and proximity-based, since we exploit the fact that an off-body attacker has obviously distinct RSS variation behavior with an on-body sensor. Different from existing works, BANA does not require any additional hardware. Only legitimate sensors are placed on/near the body. Thus our solution not only provides a simple, lightweight alternative to cryptographic authentication mechanisms, but also promises effectiveness, efficiency and applicability in real life scenarios.

III. Problem Definition

A. System Model and Assumptions

Our system includes n sensors and one CU to form a wireless BAN. These sensors are carried on a patient's body for continuously measuring and collecting physiological data (e.g. heart rate, blood oxygenation, glucose level, etc.) and sending them to the CU. We consider these devices as COTS sensors that are limited in energy supply, memory space, and computation capabilities. Worn on the body or carried by the patient, the CU is placed near body with close physical proximity, e.g., with a distance of smaller than 2 meters to each on-body sensor. Possibly being a hand-held device as smartphone or PDA, the CU processes or aggregates the data, and presents it to caregivers, physicians, emergency services and even medical researchers locally and/or remotely. Note that the CU is assumed to be not compromised. Every device in a BAN can communicate over wireless channel (e.g., Bluetooth, ZigBee, WiFi, etc.) via a radio interface. We do not assume the existence of any advanced hardware (e.g., multiple antenna, accelerometer, GPS), or auxiliary out-of-band communication channel. Sensors are placed at least half wavelength (12.5 cm for ZigBee radio) away from one another to guarantee non-correlated wireless channels, and their positions keep static during authentication.

B. Attack Model

There is at least one attacker present in the system. Collusion may exist between multiple attackers with advanced hardware. Attackers are off-body, locating either line-of-sight (LOS) or non-line-of-sight (NLOS) to the BAN user and legitimate devices. The distance between the attacker and the patient can vary in a large range, e.g., from 1 meters to tens of meters. We do not consider on-body attacks in which malicious devices are deployed on the patient's body. Since attackers deployed on-body or near body may be easily found by the patient himself/herself or caregivers, we consider the possibility of on-body attacker scenarios is relatively low, thereby not taking it into account. Although on-body attack is not in the scope of this paper, it can be easily thwarted by combining some cryptographic methods with our scheme.

Among various attack scenarios, we mainly consider impersonation attacks, where the attacker attempts to join the BAN by disguising as either a legitimate on-body sensor or the CU. Aware of the deployed security mechanism, transmission technology, and the technical specs of sensors and the CU, the attacker can forge physical addresses, eavesdrop the wireless channel, modify, replay or inject false data, and transmit packets at varying power levels. And the attacker may have knowledge about the wireless environment around the BAN. It could survey the setup location of the BAN by measuring the channel in advance, and derive corresponding signal propagation models. Besides, the attacker may use history data from previous interactions with the BAN, to predict the path loss of the channel between itself and a legitimate node.

Note that, we do not consider jamming or Denial-of-Service (DoS) attacks. During authentication, it is possible that attacker falsely claims to have the ID of a valid sensor, so as to severely affect CU's judgment on the identities of suspect sensors, or simply prevent a legitimate sensor from being successfully authenticated. However, if it does not make the attacker accepted by the CU, this can be regarded as one type of DoS attack.

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

Moreover, the authentication mechanism shall have the following properties: (1) Usability. BAN users 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. Additional latency imposed by security mechanisms may cause a difference between life and death in urgent scenarios; (4) Low-cost. It should use *COTS* hardware and require little change to existing platforms. (5) Reliability. It should work under various types of scenarios.

IV. Unique Channel Characteristics of a BAN

Channels within a BAN can display substantial differences with respect to other types of channels, such as in WLAN and cellular environments. There is some existing research on BAN's channel measurement [47]. Most of them focus on determining the channel model to enhance 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 [48]. They use it to facilitate secret key extraction from the channel, but it is not clear how this can 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 *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 apply 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 is hard to carry out mainly due to the body motion in our scheme.

A. Distinct RSS Variation Profiles between Communication Channels

1. Distinct RSS Variation Profiles between On-body and Off-Body Channels. We claim that significant differences of RSS variation exist between on-body and off-body channels. That is to say, off-body channel displays much severer fading than on-body channel over time, in terms of fading amplitude and rate. Particularly, we found two types of scenarios under which this difference is prominent: (1) *Body motion*, especially when all parts of the body are relatively static to each other. Examples of such motions include: slow-walking, sitting in a rolling wheel-chair, rotating, etc. (2) *Channel disturbances*. Alternatively, when the body is static, moving objects/people between an on-body sensor and an off-body device creates similar channel differences, for example, in a crowded hospital or emergency room.

2. Distinct RSS Variation Profiles among On-body Channels. Depending on distinct sensor positions, some of the on-body channels may experience more dramatic variations due to the impact of human body. For example, data transmission from the sensor on the front to the sensor on the back is hardly possible without scattering obstacles. In this case, relaying strategy is needed by introducing one or more sensors placed between them as relay nodes.

Experimental Evidences. To testify our claim, we performed on-body channel measurements in time domain using Crossbow's TelosB motes (TPR2400) as the working devices. 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. TelosB motes have the same hardware configuration as many COTS medical sensors [49] such as ECG and EMG sensors.

First, we configured three devices as body sensors, separately worn on the chest, strapped to the right waist, and tied to the left thigh or right arm. The other two sensors respectively work as the CU tied to a wooden pole carried by the patient (regarded as on-body) and an off-body attacker. During the experiment, the CU was taken care to keep relatively stationary to all the on-body sensors, which were fixed at their respective positions. 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 NLOS in this case, and the attacker remains static. For the corridor scenario, the patient sits on a wheelchair and pushed back and forth along a straight line by a caregiver; attacker is either static, or follows behind in a similar moving pattern. Furthermore, to simulate channel disturbances, the patient keeps static while other people walking around the corridor. In both scenarios, each activity lasted for a specified duration (2 min). We measured the RSSI received from each other sensor by the CU, where the sampling step is 200ms. Results for both scenarios are consistent with out claim, as shown in Fig.1. Since channel disturbance is not the focus of our protocol, please refer to [18] for corresponding results.

We also consider the cases in which some on-body links are NLOS as the off-body links are, e.g., an on-body device is placed on the back of the body while others on the front of the body. Additional measurements were carried out to discover RSS fluctuation difference among on-body channels due to distinct sensor placements. As Fig. 5 shown, we configured five devices as on-body sensors placed on chest (S_1), left abdominal area (S_2), right side of the back (S_3, S_4) and upper

[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.

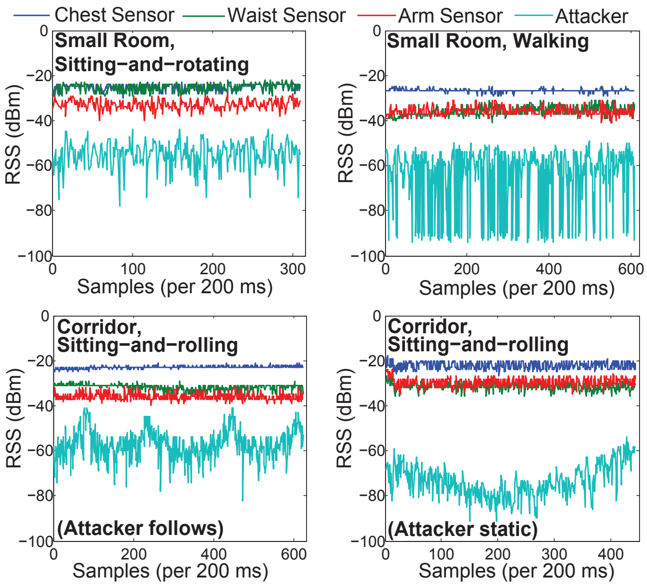


Fig. 1. RSS variations in different body motion scenarios.

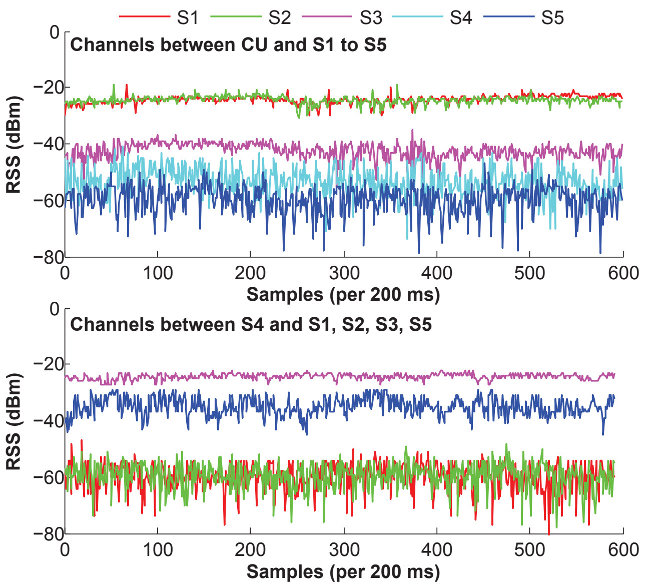


Fig. 2. RSS variations among on-body channels.

back in the center (S_5). The settings of the CU, attacker and test scenarios are the same as in previous measurements. During the measurements, including the CU, all devices broadcast messages in the round-robin way. When one device is broadcasting, others respectively measure the RSS from it. With each round of 200ms, every device obtains 5 RSS measurements for each of others per second. The measured RSSs from one of the above scenarios are displayed in Fig. 2. It is obvious that for channels to the CU, S_4 and S_5 (cf. the bottom two waveforms in the top figure) suffer larger RSS variations compared with others, which were both positioned on the back while the CU was in front of the subject. For channels to S_4, among all the others, only from S_3 and S_5 the RSS variations kept relatively stable (cf. the top two waveforms in the bottom figure), while others experienced relatively large variations.

To sum up, three prominent characteristics of on-body and off-body channels can be observed from the measurements.

(1) On-body channel is much more stable than off-body channel even under body motion. For example, in Fig. 1, RSS from the attacker is apparently experiencing large variations while RSS from all the OBSes are stable with small fluctuations. The RSS variations of OBSs are less than $5-10dB$, while for the attacker's RSS varies much faster with a range of $45dB$. Similar observations can be found in other scenarios. On the other hand, off-body channel's fading is much more random and unpredictable than 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.

(2) On-body channels have obviously different variations. For example, in Fig. 2 S_1, S_2 and S_3 have stable RSS values with small fluctuations for their channels to the CU, while S4 and S5 obviously experiencing larger RSS variations. For channels to S_4, only S_3 and S_5 have stable RSS values; others all exhibit highly variable RSS values. Other experimental settings demonstrated the similar phenomena. As a close approximation to the actual channel property, especially for heterogeneous devices, fluctuation of RSS values reflect channel variations.

(3) On-body channels between LOS locations tend to be much more stable than NLOS locations. This is clearly shown by Fig. 2. For example, S_3 has much more stable RSSs for its channel to S_4 than others. S_5 is somewhat more stable than S_1, S_2, and the CU. Recall that in our placement, S_4 and S_5 are both on the back of the subject in LOS locations. S_3 is deployed very close to S_4 with a clear LOS. S_1, S_2 and CU are all on the front side of the subject.

B. *Theoretical Explanation*

Radio wave propagation is known to be greatly affected by direct path loss, multipath, shadowing, and other interference, which are both time and environment specific and difficult to predict. Movement increases the unpredictability of the radio environment dramatically [40]. However, this has much less effect for an on-body channel than an off-body channel. On-body channels are more complicated due to body effects. According to [50], on-body signal propagation mainly include a creeping wave diffracted from the human tissue and trapped along the body surface. Received signals of on-body sensors are further affected by human movements and motions, device placement, and surrounding environment. As shown in [51], for on-body channels, the distance between transmitter and receiver is weakly correlated to the path loss since shadowing effect is more influential due to different body shapes. Besides, [52] stated that shadowing can be also caused by voluntary and involuntary movements, which affects LOS.

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 [53]. As depicted in

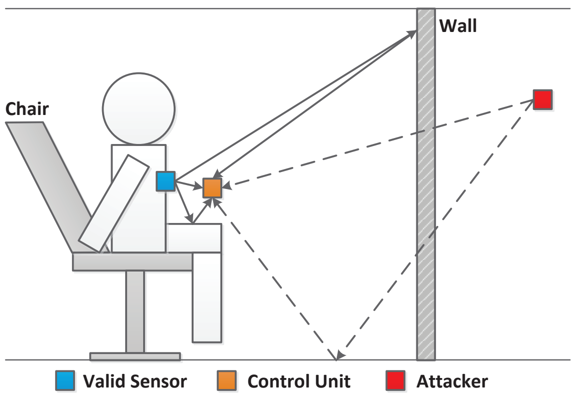


Fig. 3. Illustration of wireless channels from the OBS and the attacker, respectively, to the control unit.

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, thereby remaining relatively stable channel fading in **LOS** scenarios. For **NLOS** scenarios, due to the obstruction by device placement, impact of human tissue and body movements, channel fading becomes more unpredictable and tend to be more fluctuating in terms of both amplitude and rate compared with line-of-sight settings. Notice that 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 longer dominates. When the off-body transceiver is at a certain distance away, the superposition of multi-path components leads 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-envelope 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.

V. Main Design of BANA

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

A. Overview

Our scheme exploits the fact that RSS at the CU received from an off-body attacker experiences much larger fluctuations due to 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). 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 RSS values 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.

B. The BANA protocol

Our secure authentication protocol assumes that legitimate sensor devices have been attached to the patient's body before executing the protocol. One or more off-body attacker nodes may be present in vicinity. As shown in Fig. 4, BANA 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, and waits for response, where x is a system parameter. This hello message M 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 opportunities to the attacker for measuring the real-time channel between itself and the CU.

(2) Upon receiving the hello message, the i^{th} sensor generates a small random number t_r, and sends it back to the CU. The CU collects the t_r values from all responding devices and make sure they are not duplicated 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 continues 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 authentication, which is not affordable to the patient if the measured data 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 as 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. Given values of $ARV_1, ARV_2, ..., ARV_n$ for all the received signals, the CU

Stage	The Control Unit (CU)		The i^{th} sensor
(1) Discovering	Broadcasts a hello message; where x is a random number chosen by the CU; t_0 defines total response time; 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 t_0 seconds, letting $NT = 1000 \times t_0/t$;
(3) Classification	Calculates the average RSS variations ARV_i: $Sum_i = \sum \lvert RSS_k - RSS_{k+1}\rvert$, $ARV_i = Sum_i/NT$; Classifies ARV_1, ARV_2, ... , ARV_n 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.

Fig. 4. Description of the authentication process

applies a classification algorithm to partition them into two groups, where one group has a smaller mean of ARV while the other has a larger one.

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

C. Discussion

1. Deployment: n sensors are put to designated places on the patient's body. The CU is attached to an external device, which keeps a relatively constant position and distance to all the worn sensors. All the OBSes shall have a clear LOS to the CU. Distances between each sensor and the CU d_1, ..., d_n must be larger than half-wavelength, so that no correlation exists between wireless channels to each sensor and those to the CU. In this case, even if the attacker can measure the signals sent by legitimate sensors, it cannot 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. Therefore, within a small time interval, the RSS variation of a remote sensor is mostly larger than that of an 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 ARVs between remote sensors and on-body sensors, we also noticed that the ARV values are closed to each other for remote sensors, so are the on-body sensors themselves. Intuitively, these ARVs form two distinct groups. Our protocol enables the CU to achieve this by employing a classification method. The sensors, whose ARVs belong to the group with a smaller overall average RSS variation, are trusted as valid devices. Otherwise, they are treated as illegal ones. As one of the popular classification algorithm, K-means clustering provides a method of partitioning n observations into k clusters, in which each observation belongs to the cluster with the nearest mean. By taking $k = 2$, K-means clustering fits well for our scheme. Note that, K-means clustering requires no prior-knowledge about the data distribution, thus there is no training phase.

4. Realizing two-way authentication: In the above we have showed how the CU authenticates body sensor nodes. For the other way round, we let the CU send response messages to all the sensors after sensors' messages, which will be easily performed as discussed in Section VI. Note that the real CU in the BAN is assumed to be not compromised.

5. Credentials for future communications: During authentication, secret keys can be extracted between each authenticated on-body device and the CU based on channel measurements as proposed in our work [54]. Especially, unstable channels between on-body devices themselves can be utilized together to maximize the key generation rate and entropy of the final pairwise key. These keys serve as credentials for future communications between legitimate on-body devices and the CU. Since key generation is out of the scope of this paper, we focus on authentication.

VI. Extend BANA to Multi-Hop Authentication

Applying BANA to real-life scenarios, we notice that if the CU and an on-body sensor are on different sides of the human body (i.e. the link between them is NOLS), BANA might not successfully identify that sensor as a legitimate device due to the great impact of the body. In this case, the channel between the two devices will be unstable with larger RSS variations as the off-body channels are. However, with trusted on-body sensors working as relay nodes, this issue can be solved by extending BANA protocol in one-hop range to multi-hop authentication. In other words, we claim that the trust relationship is transitive. For example, if RSS variations between sensor A and sensor B and that between sensor B and sensor C are both stable, i.e. A trusts B and B trusts C, while channel between A and C are experiencing larger RSS fluctuations, A can trust C with a high confidence. This transitivity property of trust relationship is utilized to achieve multi-hop BANA, thereby reducing the false positive rate of BANA in many circumstances.

A. The multi-hop BANA protocol

The authentication process of the multi-hop BANA protocol is briefly described in this section.

(1) Similarly, the CU first broadcasts a hello message $M = (x, t_0, t)$ by a certain transmission power to surrounding sensors and requests responses from them after a short period of time.

(2) Upon receiving the hello message, each responding sensor randomly chooses a small number t_r and broadcasts the response message in the TDD manner as scheduled. This is repeated every t milliseconds and last for t_0 seconds. Note that t must be no less than the channel coherence time. However, different from BANA, during the t_0 seconds, every node, including the CU, measures the RSS values of each received message.

(3) After collecting the RSSs for all the responding sensors, each node calculates the ARVs for all the other nodes. Obtaining all the ARV values, classification is performed to partition these values into two groups, one with a smaller ARV mean and the other with a larger ARV mean. This step is equivalent to classifying the channels by their ARVs. Instead of only letting the CU authenticate the sensors, we let every sensor authenticate all the other ones in the system.

(4) Every device broadcasts the list of its trusted neighbor devices whose ARVs belongs to the group with a smaller ARV mean. If two sensors accept each other, we say that they have a trust relationship, for which we draw a solid line between them representing the trust link; otherwise, no line is drawn between them. Therefore, a trust topology graph can be obtained indicating the relation of whether or not one sensor accepts the other as an authenticated on-body sensor. Notice that a trust relationship between two sensors is established if and only if both of them accept each other. If one sensor accepts the other as a trusted device but the other rejects, no trust relationship is established between them. To help the final decision of the authentication, each sensor records the information of its trust topology graph with corresponding node IDs.

(5) Based on the trust topology information, the CU will check whether or not there exists a trust path, possibly including multiple hops, to reach the suspect sensor. The existence of such a path indicates that the suspect sensor can be accepted safely.

Using this method, we can obtain a graph of trust relationship of the nodes for our experiment in Section IV, as shown in Fig. 5. From Fig. 5, we can see that S_1, S_2, and S_3 are accepted by the CU while S_4 and S_5 are rejected. S_3 and S_5 are accepted by S_4 while all the rest are rejected. If we consider the multi-hop trust relationship, we can easily see the following phenomena in Fig. 5: for every pair of on-body sensors, at least one multi-hop path of trust relationship can be found between them, i.e., the resulting graph is actually a connected graph.

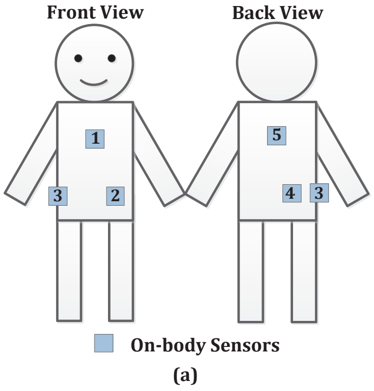


Fig. 5. (a). Another sensor deployment on the body; (b) Corresponding sensor trust relationship topology.

Our measurements in Sec.IV show that such a connected graph can be easily achieved by strategically deploying extra on-body sensors to serve as hubs. For example, if we place a few sensors on protruding body parts (e.g. arms) as hubs, most sensors can be covered – a one-hop trust path exist between each of them and one of hubs; if the CU is placed at LOS locations to the hubs, channels between hubs and the CU tend to be stable and trust paths between them exist. The CU and the hub hence interconnect BAN nodes through these trust paths. In addition, multi-hop BANA relies less on the strictly relative positioning between the CU and each sensor, which relaxes the requirements for patients on motion control as compared to BANA.

B. The correctness of multi-hop BANA

As shown in BANA, with artificially introduced movements, off-body devices have a very low probability, denoted as p, to get falsely accepted by on-body devices. For n-hop authentication, the chance of off-body devices being falsely accepted increases to np from p in BANA. According to BANA, p is very low (close to zero) in most circumstances. Moreover, as we discussed above, a BAN device can find a multi-hop trust path to the CU within few hops through hubs, i.e., n can be very small in practice (e.g., $n \leq 3$ for Fig. 5(b)). Therefore, np can also be very low and multi-hop BANA will not introduce a significant false negative rate for practical applications.

VII. Evaluation

Experiments were conducted 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, placement of the on-body devices, and subject differences.

A. Experimental Setup and Results

Our experiments were conducted on Crossbow TelosB motes (TRP2400) equipped with IEEE 802.15.4 radio. In our

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

Fig. 6. The Testing Plans

experiments, we mainly emphasize on studying the effectiveness differentiating on-body nodes from off-body nodes.

For BANA, we configured seven TelosB motes (numbered from 1 to 7) as OBSes, separately worn on the chest and arms, strapped to both sides of waist, and tied to both the left and right thighs. We used a TelosB mote to emulate the CU for simplicity. On receiving signal from sensors, the CU measures 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 attackers. These motes are mainly used to measure the channel properties of body sensors and real attackers. Based on the collected data, we analyze the probability at which legitimate body sensors are successfully accepted as well as 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). 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).

Three subjects were involved to test the difference between individuals - subject 1 and subject 3 are males with heights of 170cm and 176cm respectively, and subject 2 is a female with height of 170cm. During the experiments, we used the following movements which can be easily performed in real life: 1) *Sitting-and-rotating*. The subject acting as the patient sits on a chair (with wheels) with the controller fixed to the front of her/him. Another subject helps her/him rotate the chair slowly (about 8rpm in the experiments). This movement is only used in the small room and the medium size room. 2) *Sitting-and-rolling*. The subject acting as the patient sits on a chair (with wheels) with the controller fixed to the front of her/him. Another subject pushes the chair from behind and walks from one end of the corridor to the other end. 3) *Walking*. The subject acting as the patient walks slowly by himself/herself. This movement will be tested in the small room where space is limited 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 different factors which are summarized in Fig. 6. 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 = 200ms[3]. Each experiment lasts for 1-2 minutes. After having collected all the RSSIs, for each node i we calculate 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 Fig. 7 we 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 ARVs of all the "attackers" are greater than 4dB. This verifies our observation that with appropriate movements off-body nodes (attackers) tend to undergo larger fluctuation in path loss than on-body sensors. 2) The variance of 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 leads 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

[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).

	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

Fig. 7. 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

various reasons such as inappropriate placement of the CU, interruption from improper movements, etc. This will cause rejection of 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, the ARVs of all body sensors are below 5dB. 5) Deploying off-body nodes ("attackers") in vicinity does not necessarily result 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 differ remarkably from those of other attackers. This can be explained by factors such as different multipath effects as well as distinct Doppler spread if two nodes are more than half wave length away from each other.

In addition, we extend the experiments to the open area scenario, which were done in a 15m (width) x 50m (length) parking lot without walls and ceilings. Two subjects were involved, performing randomly walking during the experiments. Configurations for sensor placement are the same as in previous experiments. Based on the ARVs obtained by running the BANA protocol, we observe that the average ARV of on-body channels is 2.1384dB, while off-body channels has an average ARV of 4.0636dB, which is almost two times larger than the one for on-body channels. For open area scenario, due to the decrease of multipath effects caused by walls and ceilings, the RSS variations mainly depend on body movements themselves and channel disturbance caused by passersby. In this case, the ARVs for both on-body and off-body channels are smaller than in the corresponding values in-door scenarios. But the difference between ARVs of on-body channels and ARVs of off-body channels is still large enough for the classification algorithm to distinguish them.

B. Evaluation of BANA protocol

Based on the above experiment results, we first evaluate the accuracy of our scheme without strategic attackers[4]. In particular, we study the false positive rate (i.e., rate of failing to accept valid 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 with impacts and countermeasures. Finally, we evaluate the efficiency of our scheme, including computation/communication costs and authentication time.

TABLE I
THE FALSE POSITIVE/NEGATIVE RATES UNDER DIFFERENT SETTINGS WITH NON-STRATEGIC OFF-BODY ATTACKERS IN BANA.

	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

1) Effectiveness: To study the statistical property of our scheme we conducted 15 experiments under the five test plans. Besides the 5 experiments presented in Fig. 6, the other 10 experiments were based on the five plans by slightly but randomly changing some settings such as the movement speed and the number and/or the position of 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: location of the experiment, type of movements, and subject difference. For each case, the *false positive rate (FPR)* is computed as the percentage of total number of rejected on-body sensors out of the total number of on-body sensors, i.e.,

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

where EXP is the set of all the experiments in the case. Similarly, the *false negative rate (FNR)* is computed as the percentage of the number of accepted off-body sensors (attackers) out of the total number of off-body sensors (attackers).

Our analysis results are summarized in Table. I. From this table we observe that the false negative rate in our experiments is zero. This is mainly due to the fact that 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 trying 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 less impact from location as long as the environment surrounding the patient is relatively simple, e.g., few reflecting angles or objects near the patient. The impact of movements is slightly higher 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%), since it is usually harder for individuals, unless well-trained, to guarantee the smoothness of the movement (i.e., keeping the relative location between the CU and on-body sensors stable)

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

while walking. But it will be relatively easier while sitting on a chair. From the results, we also observe a slight difference among individuals, which is mainly caused by the difference of individuals' controlling of the movements. The overall false positive rate is 3.3% based on all the 15 experiments.

2) Security against strategic attacks: A smart attacker may carry out strategic attacks to improve the chance of getting off-body nodes accepted by the CU. For this purpose the attacker can employ the following methods: reducing the fluctuation of path loss measured by the CU by varying transmission power, deviating from clustering method, using directional antenna.

Varying transmission power To reduce the fluctuation of path loss measured by the CU, the attacker must accurately measure or predict the communication channel to the CU so as to compensate the path loss by varying transmission power. But as the CU does not transmit any signal after broadcasting the request message, the attacker is not able to measure real-time channel impulse response. Alternatively, the attacker may resort to measuring the real-time property of channels 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 on-body sensors, so the channel to them are mutually uncorrelated. Another way is to predict the channel based on historical channel measurements. But the channel coherence time is very short ($\leq 200ms$) due to introduced movements.

Deviating from clustering method The attacker attempts to deviate our clustering method through introducing an overwhelming number of off-body attacker nodes. This 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 on 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. 8. 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.

Using directional antenna A possible limitation of BANA is when dealing with attackers with a directional antenna, which is known as beam-forming attacks. 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 multi-path effect. While this attack seems to be effective, we believe that it is difficult to launch in practice. Specifically, in BANA the patient carries out suggested random motions. 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 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.

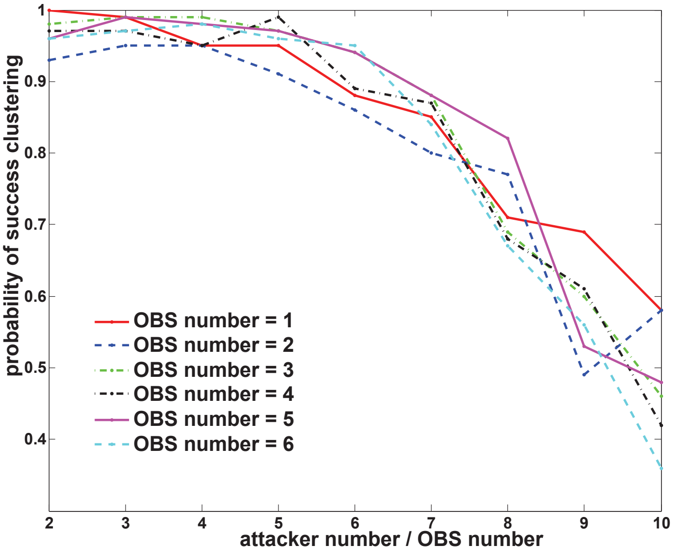


Fig. 8. Impact of the attacker node number on our clustering method.

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 attackers. The involved motions can be easily performed by any inexperienced patient in general real life scenarios. They effectively create difference of RSS variation between on-body and off-body links, which increase accuracy of the clustering results.

3) Efficiency: The efficiency of our proposed scheme is evaluated by authentication time, computation and communication costs.

Authentication Time: In our experiments, authentication time is set as 1-2 minutes for the CU receiving sufficient sample RSS for analysis. However, the actual authentication time for a sensor node may not 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. Results show that, in some scenarios, such as sitting-and-rotating in the medium room, both false positive rate and false negative rate quickly

TABLE II
THE FALSE POSITIVE RATES FOR MULTI-HOP BANA COMPARED WITH BANA.

	BANA	Multi-hop BANA
small	39.85%	8.33%
medium	30.00%	0
corridor	50%	0
sitting-and-rotating	27.50%	5%
sitting-and-rolling	50%	0
walking	41.67%	4.17%
person 1	45.31%	4.69%
person 2	43.75%	2.08%
person 3	20.83%	0
overall	40.44%	2.94%

become stable as 0, indicating that 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 a certain number of samples are examined as shown in Fig. 9. 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 effect 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 only 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 is negligible since no time-consuming task is executed on it. On the controller's side, the most computation-intensive task is the execution of the clustering algorithm. As the k-means clustering itself is NP-hard, heuristic algorithms are usually employed. The algorithm complexity can be $O(n^{dk+1} logn)$ if d and k are fixed[55], 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. Thus the complexity can be $O(n^3 logn)$, where n is corresponding to the number of sensors, which is a relatively small number. The communication cost for each sensor is mainly caused by messages sent to the CU every 200ms, which only include the node's identity.

C. Experimental comparison between BANA and multi-hop BANA

To compare the enhancement of multi-hop BANA with one-hop BANA in terms of false positive rate, 17 additional experiments were conducted with random combinations of location, movement, sensor placement and subject. In these experiments, we used 10 TelosB motes: 8 as on-body sensors, one as the CU and one as the off-body attacker. We also varied the ratio of number of on-body sensors to that of off-body attackers from 8:1 to 1:1. These experiments kept the same configurations of location, and followed the plans of experiment scenarios in Fig. 6 with RSS sample rate of 200ms. But different from previous experiments, movement requirements were relatively relaxed. For example, for the walking movement, subjects can walk freely instead of walking slowly. The CU is either put in the front the body or attached to the body. On-body sensors were placed freely on the back and front of the body by roughly following our suggestion in Section VI-B, e.g. on chest, abdominal area, back, etc. Note that previous experiments only tested the cases wherein sensors are placed on the same side of the body and the CU.

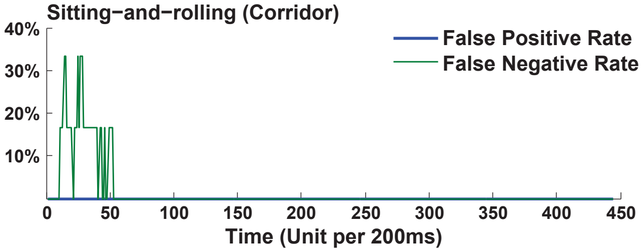


Fig. 9. False positive/negative rate at different time.

Experiment results are shown in Table. II. We notice that compared with Table. I, the overall false positive rate is increased from 3.3% to 40.44%. The reason is that while previous experiments strictly required careful movements and placed all the on-body sensors on the same side of the body, the latter ones have relaxed movement requirements and different sensor placements. From Table.I II, we can see that the overall false positive rate for multi-hop BANA is almost 14 times less than that of BANA, reducing from 40.44% to 2.94%. Such a dramatic difference can mainly be explained by the help of the trust relay sensors forming trust paths from the CU to suspect sensors, especially those not on the same side of the body and the CU. Regarding handling sensors on the other side of the body and the CU, it is clear that multi-hop BANA shows the advantage over BANA.

Interestingly, for multi-hop BANA, all the false positives happened in the small room scenario. This can be partially explained by the fact that small rooms tend to have more severe multipath effect due to close distances to walls. In addition, in these 17 experiments, the false negative rate under different on-body to off-body node ratios remains 0, which is the same as in BANA.

VIII. Conclusion

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, i.e. 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 to enhance its security from physical layer, such as secret key extraction. Finally, we note that our study has assumed a symmetric radio link between Alice and Bob, and the amount to which this assumption is true in general needs to be extensively explored.

REFERENCES

[1] 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*, vol. 3, no. 4, pp. 16–23, oct.-dec. 2004.

[2] M. Chen, S. Gonzalez, A. Vasilakos, H. Cao, and V. C. Leung, "Body area networks: A survey," *Mob. Netw. Appl.*, vol. 16, no. 2, pp. 171–193, Apr. 2011.

[3] M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 80–88, february 2010.

[4] 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*, vol. 2, no. 1, p. 6, march 2005.

[5] 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*, vol. 3, no. 4, pp. 16–23, oct.-dec. 2004.

[6] "Experts see data breach risks in medical devices on hospital networks," may 2011. [Online]. Available: http://www.ihealthbeat.org/articles/2011/5/12/experts-see-data-breach-risks-in-medical-devices-on-hospital-networks.aspx

[7] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks," *IEEE Wireless Commun.*, vol. 17, no. 1, pp. 51–58, february 2010.

[8] S. Cherukuri, K. Venkatasubramanian, and S. Gupta, "Biosec: a biometric based approach for securing communication in wireless networks of biosensors implanted in the human body," in *Parallel Processing Workshops, 2003. Proceedings. 2003 International Conference on*, oct. 2003, pp. 432–439.

[9] K. Timm, "Medical device hacking prompts concern," august 2011. [Online]. Available: http://www.cyberprivacynews.com/2011/08/medical-device-hacking-prompts-concern/

[10] 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*, may 2008, pp. 129–142.

[11] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in *Proc. 9th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2002, pp. 41–47.

[12] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Security and Privacy, 2003. Proceedings. 2003 Symposium on*, may 2003, pp. 197–213.

[13] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," *ACM Trans. Inf. Syst. Secur.*, vol. 8, no. 2, pp. 228–258, May 2005.

[14] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proc. 10th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2003, pp. 52–61.

[15] D. Liu, P. Ning, and W. Du, "Group-based key predistribution for wireless sensor networks," *ACM Trans. Sen. Netw.*, vol. 4, no. 2, pp. 11:1–11:30, Apr. 2008.

[16] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "Spins: security protocols for sensor networks," *Wirel. Netw.*, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[17] K. Zeng, K. Govindan, and P. Mohapatra, "Non-cryptographic authentication and identification in wireless networks [security and privacy in emerging wireless networks]," *IEEE Wireless Commun.*, vol. 17, pp. 56–62, october 2010.

[18] L. Shi, M. Li, S. Yu, and J. Yuan, "Bana: body area network authentication exploiting channel characteristics," in *Proc. fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*. New York, NY, USA: ACM, 2012, pp. 27–38.

[19] K. Malasri and L. Wang, "Addressing security in medical sensor networks," in *Proc. 1st ACM SIGMOBILE international workshop on Systems and networking support for healthcare and assisted living environments*. New York, NY, USA: ACM, 2007, pp. 7–12.

[20] S. A. Devi, R. V. Babu, and B. S. Rao, "A new approach for evolution of end to end in wireless sensor network," *International J. Computer Science and Engineering*, vol. 3, no. 6, pp. 2531–2543, june 2011.

[21] M. Mana, M. Feham, and B. A. Bensaber, "A light weight protocol to provide location privacy in wireless bodyarea networks," *International J. Network Security & Its Applications*, vol. 3, no. 2, pp. 1–11, march 2011.

[22] O. Delgado-Mohatar, A. Fuster-Sabater, and J. M. Sierra, "A light-weight authentication scheme for wireless sensor networks," *Ad Hoc Networks*, vol. 9, no. 5, pp. 727–735, 2011.

[23] T. Zia and A. Zomaya, "A lightweight security framework for wireless sensor networks," *J. Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, vol. 2, pp. 53–73, september 2011.

[24] C. C. Tan, H. Wang, S. Zhong, and Q. Li, "Body sensor network security: an identity-based cryptography approach," in *Proc. first ACM conference on Wireless network security*. New York, NY, USA: ACM, 2008, pp. 148–153.

[25] C. Tan, H. Wang, S. Zhong, and Q. Li, "Ibe-lite: A lightweight identity-based cryptography for body sensor networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 13, no. 6, pp. 926–932, Nov. 2009.

[26] W. Drira, E. Renault, and D. Zeghlache, "A hybrid authentication and key establishment scheme for wban," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, June 2012, pp. 78–83.

[27] 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*, march 2010, pp. 1–9.

[28] 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 Trans. Sensor Networks (TOSN)*, 2012.

[29] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang, "Exploiting prediction to enable secure and reliable routing in wireless body area networks," in *INFOCOM, 2012 Proc. IEEE*, March 2012, pp. 388–396.

[30] 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 Commun. Mag.*, vol. 44, no. 4, pp. 73–81, april 2006.

[31] K. K. Venkatasubramanian and S. K. S. Gupta, "Physiological value-based efficient usable security solutions for body sensor networks," *ACM Trans. Sen. Netw.*, vol. 6, no. 4, pp. 31:1–31:36, Jul. 2010.

[32] K. Venkatasubramanian, A. Banerjee, and S. Gupta, "Pska: Usable and secure key agreement scheme for body area networks," *IEEE Trans. Inf. Technol. Biomed.*, vol. 14, no. 1, pp. 60–68, jan. 2010.

[33] K. Singh and V. Muthukkumarasamy, "Authenticated key establishment protocols for a home health care system," in *Intelligent Sensors, Sensor Networks and Information, 2007. ISSNIP 2007. 3rd International Conference on*, dec. 2007, pp. 353–358.

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

[35] 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)*, Shanghai, P.R.China, April 2011, pp. 1862–1870.

[36] 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)*, Shanghai, P.R.China, April 2011, pp. 346–350.

[37] R. Mayrhofer and H. Gellersen, "Shake well before use: Authentication based on accelerometer data," in *Pervasive Computing*, ser. Lecture Notes in Computer Science, A. LaMarca, M. Langheinrich, and K. Truong, Eds. Springer Berlin / Heidelberg, 2007, vol. 4480, pp. 144–161.

[38] ——, "Shake well before use: Intuitive and secure pairing of mobile devices," *IEEE Trans. Mobile Computing*, vol. 8, pp. 792–806, 2009.

[39] A. Varshavsky, A. Scannell, A. LaMarca, and E. De Lara, "Amigo: proximity-based authentication of mobile devices," in *Proc. 9th international conference on Ubiquitous computing*. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 253–270.

[40] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: cooperative proximity-based authentication," in *Proc. 8th international conference on Mobile systems, applications, and services*. New York, NY, USA: ACM, 2010, pp. 331–344.

[41] 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.

[42] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in *Proc. 13th annual ACM international conference on*

Mobile computing and networking. New York, NY, USA: ACM, 2007, pp. 111–122.

[43] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: proximity-based secure pairing using ambient wireless signals," in *Proc. 9th international conference on Mobile systems, applications, and services*. New York, NY, USA: ACM, 2011, pp. 211–224.

[44] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin, and S. Capkun, "Proximity-based access control for implantable medical devices," in *Proc. 16th ACM conference on Computer and communications security*. New York, NY, USA: ACM, 2009, pp. 410–419.

[45] S. Brands and D. Chaum, "Distance-bounding protocols," in *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 1994, pp. 344–359.

[46] K. B. Rasmussen and S. Čapkun, "Realization of rf distance bounding," in *Proc. 19th USENIX conference on Security*. Berkeley, CA, USA: USENIX Association, 2010, pp. 25–25.

[47] 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*, june 2009, pp. 1–6.

[48] 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*. IEEE, 2010, pp. 644–650.

[49] "Shimmer sensor units and modules." [Online]. Available: http://www.shimmer-research.com/products-2

[50] J. Ryckaert, P. De Doncker, R. Meys, A. de Le Hoye, and S. Donnay, "Channel model for wireless communication around human body," *Electronics Letters*, vol. 40, no. 9, pp. 543–544, april 2004.

[51] F. Di Franco, C. Tachtatzis, B. Graham, D. Tracey, N. Timmons, and J. Morrison, "On-body to on-body channel characterization," in *Sensors, 2011 IEEE*, oct. 2011, pp. 908–911.

[52] F. Di Franco, C. Tachtatzis, B. Graham, M. Bykowski, D. Tracey, N. Timmons, and J. Morrison, "The effect of body shape and gender on wireless body area network on-body channels," in *Antennas and Propagation (MECAP), 2010 IEEE Middle East Conference on*, oct. 2010, pp. 1–3.

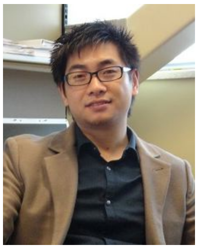
[53] T. Rappaport and L. Milstein, "Effects of radio propagation path loss on ds-cdma cellular frequency reuse efficiency for the reverse channel," *IEEE Trans. Veh. Technol.*, vol. 41, no. 3, pp. 231–242, aug 1992.

[54] L. Shi, J. Yuan, S. Yu, and M. Li, "Authenticated secret key extraction utilizing channel characteristics for body area networks," in *Proc. 6th ACM conference on Security and Privacy in Wireless and Mobile Networks*, 2013, p. to appear.

[55] M. Inaba, N. Katoh, and H. Imai, "Applications of weighted voronoi diagrams and randomization to variance-based k-clustering: (extended abstract)," in *Proc. tenth annual symposium on Computational geometry*. New York, NY, USA: ACM, 1994, pp. 332–339.

Lu Shi (S'11) received her B.E. in Electrical Engineering at Xidian University, China, in 2009, and M.S. in Electrical Engineering at University of Southern California in 2010. She is currently a Ph.D candidate in Computer Science department at University of Arkansas at Little Rock. Her main research interests include Information Security, with recent focus on Wireless Network Security, Cyber-physical System Security. She is a student member of IEEE.

Ming Li (S'08-M'11) received his Ph.D. in Electrical and Computer Engineering from Worcester Polytechnic Institute, M.E and B.E in Electronic and Information Engineering from Beihang University in China. He joined the Computer Science Department at Utah State University as an assistant professor in 2011. His research interests are in the general areas of cyber security and privacy, with current emphases on data security and privacy in cloud computing, security in wireless networks and cyber-physical systems. He is a member of IEEE and ACM.



Shucheng Yu (S'07-M'10) received his Ph.D in Electrical and Computer Engineering from Worcester Polytechnic Institute, a M.S. in Computer Science from Tsinghua University and a B.S. in Computer Science from Nanjing University of Post & Telecommunication in China. He joined the Computer Science department at the University of Arkansas at Little Rock as an assistant professor in 2010. His research interests are in the general areas of Network Security and Applied Cryptography. His current research interests include Secure Data Services in Cloud Computing, Attribute-Based Cryptography, and Security and Privacy Protection in Cyber Physical Systems. He is a member of IEEE.

Jiawei Yuan (S'12) is a Ph.D student at University of Arkansas at Little Rock. He received his B.S. from University of Electronic Science and Technology of China in 2011. He worked as an intern at Research Programs of Information Technology at UAMS since Aug. 2011. His research interests are in the areas of cloud computing and network security, with current focus on securing the data and computation outsourced into the cloud. He is a student member of IEEE.