ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area Networks

Lu Shi, Jiawei Yuan, Shucheng Yu
Department of Computer Science
University of Arkansas at Little Rock
Little Rock, AR 72204
{lxshi, jxyuan, sxyu1}@ualr.edu

Ming Li
Department of Computer Science
Utah State University
Logan, UT 84322
ming.li@usu.edu

ABSTRACT

Recently there has been an increasing interest on bootstrapping security for wireless networks merely using physical layer characteristics. In particular, the focus has been on two fundamental security issues - device authentication and secret key extraction. While most existing works emphasize on tackling the two issues separately, it remains an open problem to simultaneously achieve device authentication and fast secret key extraction merely using wireless physical layer characteristics, without the help of advanced hardware or out-of-band channel.

In this paper, for the first time, we answer this open problem in the setting of Wireless Body Area Networks (BANs). We propose ASK-BAN, a lightweight fast authenticated secret key extraction scheme for intra-BAN communication. Our scheme neither introduces any advanced hardware nor relies on out-of-band channels. To perform device authentication and fast secret key extraction at the same time, we exploit the heterogeneous channel characteristics among the collection of on-body channels during body motion. Specifically, with simple body movements, channel variations between line-of-sight on-body devices are relatively stable while those for non-line-of-sight devices are unstable. ASK-BAN utilizes the relatively static channels for device authentication and the dynamic ones for secret key generation. On one hand, ASK-BAN achieves authentication through multi-hop stable channels, which greatly reduces the false positive rate as compared to existing work. On the other hand, based on dynamic channels, the key extraction process between two on-body devices with multi-hop relay nodes is modeled as a max-flow problem, and a novel collaborative secret key generation algorithm is introduced to maximize the key generation rate. Extensive real-world experiments on low-end COTS sensor devices validate that ASK-BAN has a high secret key generation rate while being able to authenticate body devices effectively.

WiSec'13, April 17-19, 2013, Budapest, Hungary.

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; Authenticated Key Generation; RSS; Physical Layer

1. INTRODUCTION

Secure wireless communications have been more imperative than ever with increasing prevalence of wireless devices. Among the others, two most fundamental issues for secure wireless communications are device authentication and secret key extraction. Over years research in this area has shifted its attention to bootstrapping security for wireless communications merely based on physical layer characteristics. Such a fact is mainly caused by increasing concerns on drawbacks of applying conventional public and symmetric-key techniques in wireless networks: pre-loading secret keys on heterogeneous wireless devices is less practical; wireless devices are more likely subject to physical compromise attacks; cryptographic primitives for authentication and key distribution are expensive for many wireless applications; most cryptographic primitives assume computation boundary of attackers; so on and so forth. Bootstrapping security from physical layer characteristics can eliminate the complex process of key distribution and the computational assumptions, and thus is believed to offer better efficiency and security for wireless networks.

Existing literature in this direction mainly utilizes three types of physical layer characteristics for bootstrapping security: *advanced hardware* [1, 5, 3, 20, 21], *out-of-band communication channels* [17], and *wireless channel measurements* [28, 14, 25]. The first two approaches both assume the availability of additional resources. Information measured or extracted from the advanced hardware (e.g., multiple antenna) and auxiliary out-of-band (OOB) channels (e.g., ambient radio channels) is used for device authentication [5, 3, 22, 11] or secret key generation [1], or both of them together [27]. However, in ubiquitous environments, wireless devices, especially commercial-off-the-shelf (COTS) ones, are usually constrained in hardware configuration. System stack requires extra modifications to meet the configuration. And OOB communication channels are not always available. The third approach, wireless channel measurements, bootstraps security by only measuring wireless communication channels (e.g., RSS). With minimal requirements on the wireless system, wireless channel measurement based approach is promising in bootstrapping security for wireless devices in ubiquitous environments. Particularly, practical systems often require device authentication and secret key generation to be fulfilled simultaneously. To our best knowledge, there is no such work that is able to simultaneously provide effective device authentication and fast secret key extraction simply by wireless channel measurements.

In this paper, we answer this open problem in the setting of wireless Body Area Networks (BANs) and propose a lightweight, body movement-aided authenticated secret key extraction scheme for intra-BAN communication, namely ASK-BAN. ASK-BAN does not assume the existence of any advanced hardware or out-of-band communication channel with nodes in BAN, ensuring that it can be widely applied to COTS devices. In ASK-BAN, device authentication and secret key extraction are simultaneously achieved only based on measurements of the communication channels between the BAN nodes. Device authentication guarantees that all the sensor devices to communicate with the CU are on the same body of one person, which utilizes *relatively stable channels* between on-body devices and distinguishes them from off-body devices that have *remarkably unstable channels* to the CU due to simple body movements that the patient artificially performed during the process. Concurrently, secret keys are extracted between every authenticated on-body device and the CU, utilizing their *relatively unstable channels*. ASK-BAN is designed based on our two important observations of channel characteristics when the patient is conducting some simple body movements: 1) channels between CU and on-body sensors (OBSs) deployed in line-of-sight (LOS) vicinity tend to be much more stable than OBSs deployed in non-line-of-slight (NLOS) locations. However, channels between off-body devices and CU experience much severer fluctuations than on-body channels, whether the OBSs are LOS or NLOS to CU. 2) Authentication is transitive in BANs. That is, 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 node B is on-body.

Specifically, between every on-body sensor and CU, ASK-BAN attempts to find two types of channels – multi-hop stable channels and multi-hop unstable channels – for authentication and key extraction respectively. Using the transitivity property, an on-body sensor is accepted if it has at least one relatively stable multi-hop channel to the CU. Along the multi-hop unstable channels between one sensor and the CU, a secret key is generated with the help of relay nodes. That is, pairwise keys between relay nodes are utilized to maximize the key generation rate and entropy of the final secret key between that sensor and the CU, in terms of number of bits.

Our experiments on real sensor devices show that both stable and unstable multi-hop on-body channels are very easy to be created in practice. Our scheme is shown to be able to simultaneously provide node authentication and secret key extraction with a high key rate.

Our Contribution The contribution of this paper can be summarized as follows.

- To our best knowledge, ASK-BAN is the first scheme that provides authenticated secret key extraction using only wireless channel measurements.
- In most scenarios, combined with body movements, ASK-BAN greatly reduces false positive rate through the multi-hop authentication scheme.
- ASK-BAN introduces a novel collaborative secret key extraction scheme with multi-hop relay nodes based on the max-flow algorithm, which can find application in other wireless systems.

The rest of the paper is organized as follows. Section 2 gives an overview of related work. Section 3 defines the problem as well as the system model. We illustrate our observations of unique BAN channel characteristics in Section 4, which is followed by the detailed description of ASK-BAN in Section 5. Section 6 evaluates and discusses our experimental and simulation results of implementing ASK-BAN on real sensors. We conclude this paper in Section 7.

2. RELATED WORK

In this section, we review existing research on non-crypto key generation and authentication schemes based on physical layer characteristics.

First, we note that using a *non-wireless* channel and under some constrained scenarios, it is easy to simultaneously achieve secret key generation and device authentication. Existing works in this direction are mainly *biometric-based* and *motion-based*. Using physiological signals, many schemes have been proposed to measure and compare physiological information collected by the sensors, such as electrocardiogram (ECG), photoplethysmogram (PPG), iris and fingerprint, to assist authentication and key establishment without a priori distribution of keying material. For authentication, [22] introduced a security mechanism using biometric traits as the authentication identity. And [11] presented a light-weight secure access control scheme for implanted medical devices (IMDs) during emergencies, utilizing basic biometric information or iris data to prevent unauthorized access. For key generation combined with authentication, schemes in [27, 32, 29, 30] established physiological data-based keys between devices for verification. However, the major drawback of biometric-based techniques is that the biometrics derived from physiological features are usually accompanied with high degrees of noise and variability inherently present in the signals. Also it is difficult to guarantee consistent physiological signals measurements with same accuracy for every sensors located in different positions. Moreover, not all the physiological parameters have the same level of entropy for key generation. According to [4], for example, heart rate is not a good choice because its level of entropy is not satisfactory. Given the above issues, their applications are limited.

For motion-based key generation, [1] established a secure connection between two devices by shaking them together and generating a key from the measured acceleration data by appropriate signal. For authentication, [5] used information extracted from companion accelerometers and coherence measurements to determine whether the devices are on the same body. For authentication with key extraction, schemes in [20, 21] exploited the same movement patterns when shaking devices together for authentication, and generated shared secret keys based on the the measured acceleration data in the shaking process. But similar to biometric-based ones, these schemes require specialized sensing hardware and human participation, which is demanding for COTS devices.

On the other hand, using *wireless channel* for authentication and/or key generation has been of great interest recently. For device authentication, wireless channel has been used to determine *device proximity*. Cai et al. in [3] utilized multiple antenna to perform ad hoc pairing of nearby wireless devices, in which the proximity of the sender can be implied by the difference between the received signal strengths (RSS) measured by distinct antennas on the receiver. Similar schemes also include Amigo [28] and Ensemble [14] which perform proximity-based authentication of physically co-located/closely placed devices, using channel measurement-based signatures or variations in RSS. Recently, Shi et al.[25] proposed BANA, basing the lightweight authentication scheme on RSS measurements only. By artificially introducing body motions or channel disturbance, BANA authenticates on-body devices due to relatively stable channels to CU compared to those from off-body attackers to on-body BAN nodes. However, BANA only considers authentication for LOS on-body devices, which is limited in some sensor deployments. For key generation, several seminal works were proposed, including Mathur et. al. [18] and Jana et. al. [13]. Along this direction, one of the key research topics is to improve the key generation rate. Lai et. al. [15] exploited random channels associated with relay nodes in the wireless network as additional random sources for key generation. Note that [15] was only concerned about key generation between two nodes with one-hop relay nodes.

Nevertheless, it has been demanding to realize authentication and key generation at the same time using wireless channel alone, primarily due to a dilemma: authentication usually requires proximity, while fast key generation requires channel fading that proximity cannot provide. Take BANA in [25] for example, since its authentication process does not result in a credential and hence is "memoryless", it is difficult to derive an authenticated secret key extraction scheme by straightforward combination of BANA with existing key extraction techniques. Alternatively, directly utilizing channels between BAN sensors and the CU would result in a very low key generation rate, because these channels are too stable to carry high entropy for key extraction. For only RSS-based solutions, fast key extraction and device authentication seem to be two conflicting objectives due to the gap between their distinct requirements on channel stability.

In this paper, we address the challenge and take a step forward for achieving effective authentication and fast key generation concurrently only based on wireless channels in BAN. Unlike previous work, our scheme, ASK-BAN, does not require advance hardware for physical layer characteristic measurement, nor does it rely on any auxiliary OOB channel. Since wireless channel characteristics can be measured by most COTS devices, ASK-BAN can be easily applied in a wide range of applications.

3. PROBLEM DEFINITION

3.1 System Model and Assumptions

In our system, the wireless BAN is composed of n sensors and one control unit (CU). Worn on the body surface of a patient, these sensors measure physiological signals (e.g., heart rate, blood pressure, etc.) of the patient and transmit the collected data to the CU. As COTS sensors, they are resource-constrained with limited energy supply, memory space and computation capabilities. CU is worn on body or placed near the body with close physical proximity, i.e. with a distance of smaller than 1 meters to each of the on-body sensors, responsible for aggregating and/or processing the received data, and relaying the data to caregivers, physicians, emergency services and even medical researchers locally or remotely. CU could be a hand-held device such as smart phone or PDA.

All the devices in the BAN are able to communicate over wireless channels (e.g., Bluetooth, ZigBee, WiFi, etc.) directly to each other through their radio interfaces. Neither advanced hardware (e.g., multiple antenna, accelerometer, GPS) nor out-of-band channel is considered to exist with the sensors. We assume that the relative positions between the BAN nodes are static during the security bootstrapping process with body movements. Extensive existing research work has shown that, coherent signal observations located greater than half wavelength away from two communicating wireless devices are typically not correlated. In this paper, we place every node at least half wavelength (for Zigbee radios it is approximately 12.5cm) away from each other to ensure uncorrelated wireless channels.

Note that body movements are involved during the running of our proposed protocol. Considering some patients have limited moving capability, we introduce several easily-done body movement options in our experiments:(1) slowly walking at random; (2) slowly rotating by sitting on a spinning chair; and (3) sitting on a rolling wheelchair, which is moved back-and-forth along a straight line with the help of caregiver.

3.2 Attack Model

In this paper, at least one attacker node is present in the system. Multiple attacker nodes may exist and collude with each other with advanced hardware. Attacker locations could be either line-of-sight (LOS) or non-line-of-sight (NLOS) to the BAN user and the legitimate devices including sensors and the CU. Following existing proximity-based authentication schemes [3, 28, 14], our primary goal for authentication is to differentiate on-body BAN devices, whether LOS or NLOS to the CU, from those off the body. Thus we assume attacker devices are deployed off-body. In other words, we do not consider attacks wherein malicious devices are placed on the patient's body. But the distance between the attacker and the patient could vary largely in a wide range, e.g., from 1 or 2 meters to tens of meters.

Among different attack scenarios, we are mainly concerned about impersonation attack, in which attacker devices attempt to pretend to be a legitimate on-body sensor or the CU in order to join the BAN, thereby constructing a shared secret key with CU or sensors for the purpose of launching further attacks during communication. Attackers are aware of the deployed security mechanisms, transmission technology, and the technical specs of the sensors and the CU. They are able to fabricate physical addresses (e.g. MAC address), eavesdrop the wireless channel, replay or inject false data, and transmit packets with varying power. Beyond the above capabilities, attackers may be knowledgeable about the wireless channel environment surrounding the BAN. For instance, an attacker may have investigated the location in advance and measured the signal propagation models in that location using his own devices. Also, historical data collected in previous BAN activities might be used by the attacker for prediction of the path loss of the channel between himself and a legitimate node.

Note that we do not consider jamming and Denial-of-Service (DoS) attacks in this paper. Furthermore, CU is assumed to be not compromised. As the CU could be a hand-held device such as a smartphone, advances in existing techniques for mobile security can applied to safeguard the CU, which are out of the scope of this paper.

3.3 Design Requirements

The main goal of our design is to achieve authenticated key generation, i.e., efficiently establishing a shared secret key between each legitimate on-body sensor and CU while the system effectively differentiating valid sensors/CU from off-body attacker nodes, thereby securing future communication. Our scheme is designed for application scenarios such as setting up on-body devices at home, in hospital, or even during moving.

In addition, the authenticated key generation scheme is expected to have following properties: (1) Lightweight: our scheme shall not involve expensive operations on on-body devices that are resource-constrained ; (2) Usability: common users, such as patients, do not have to get involved in complicated setup and use of the BAN. Instead, *Plug-n-play* is a preferred usability goal; (3) Fast authentication and key extraction: applying our scheme would not put the patient's life at risk in emergency scenarios; this requires that our scheme shall be able to authenticate the nodes and extract keys of satisfying length in a fairly short time period; (4) Compatibility: our scheme shall be compatible with *commercial-off-the-shelf* (COTS) sensors and does not require additional hardware or changing the existing system stack; (5) Reliability: our scheme shall work under various types of scenarios with desirable accuracy.

4. CHANNEL CHARACTERISTICS WITH BODY MOTIONS IN BAN

To bridge the gap between fast secret key extraction and device authentication, in this paper we made some significant observations of special channel characteristics along with body motions in BAN. These new findings lead to a solution to the dilemma mentioned above and build the basis of our authenticated key extraction scheme. For brevity, in the following part we use *on-body channel* to denote the communication channel wherein both transceivers located on the same human body or one of them is in close vicinity of the body (i.e. the CU). And *off-body channel* is referred to as the channel wherein one transceiver on/close to body and the other off-body at a distance away.

4.1 Distinct RSS Variations among On-Body Channels with Body Motions

Previous work [7, 6, 16, 25] has shown that in a BAN, there exists significant differences of RSS variation profiles between on-body and off-body channels when body motions are involved. In this paper, we claim that, with body motions, the channel variations among distinct on-body channels may differ notably even if the on-body sensors remain in relatively static positions to each other, but the variation for all these on-body channels are still relatively stable compared to those for off-body channels. That is, depending on different positions of the on-body devices including sensors and the CU, some on-body channels, especially those NLOS to each other, may experience more dramatic variations than other on-body ones over time in terms of both amplitude and changing rate. But considering both the on-body channels and off-body channel together, off-body channels prominently display much larger RSS fluctuations than those of all the on-body channels.

Experimental Evidence. To validate our claim, on-body channel measurements were carried out in time domain, with the test setup consisting of six Crossbow TelosB motes (TRP 2400). TelosB motes have the same hardware configuration as many COTS medical sensors [26] such as ECG and EMG devices. TelosB platform includes an IEEE 802.15.4 radio with an integrated antenna, a low-power MCU with extended memory and an optional sensor suite. As shown in Fig. 1(a), five of these devices are configured as on-body sensors, placed on: chest (S_1), left abdominal side (S_2), right side of the back (S_3, S_4), and high centered back (S_5). The remaining one (S_6) works as the CU and is located closed to other sensors. The CU is fixed to a wooden pole carried by the subject in front of him. During the experiment care was taken to ensure that CU was keeping relatively stationary to all the on-body sensors during the experiment. All the on-body sensors were all fixed at their respective locations in the whole process.

The subject performed easily-done body movements we suggested in Section III, including walking randomly, slowly rotating on a chair, and moving back-and-forth on a rolling wheelchair. Note that substantial body motions should be avoided to keep on-body sensors and the CU relatively stationary to each other. Each activity lasted for one minute. We measured the first two types of movements in a small office and a medium office. The third one was performed in a large corridor inside a college building.

During the experiment, all the devices, including the CU, broadcast messages in the round-robin fashion. When one device is broadcasting, others measure the RSS received from that device, respectively. Each round takes 200ms, i.e., each node obtains 5 RSS measurements for every other node per second. Fig. 2 shows the RSS measurements in one of these settings. From the figure, we can clearly see that for channels to the CU, S_4 and S_5 (cf. the bottom two waveforms in the top figure) obviously exhibit larger RSS variations than others. Note that during the experiment S_4 and S_5 were put on the back of the subject while the CU faces the front of subject's body. For channels to S_4, only S_3 and S_5 are relatively stable (cf. the top two waveforms in the bottom figure) and all the other channels undergo relatively high variations.

We classified these channels by their average RSS variations (ARVs) into two groups by existing classification algorithm. Here, ARVs are calculated by averaging the RSS variations between consecutive measurements. Then letting all the sensors authenticate one another in the system directly, sensors with ARV in the group of smaller ARV mean value are accepted; otherwise rejected. Based on the authentication result, we can draw a graph indicating the relation of whether or not one sensor accepts the other one as an authenticated on-body sensor. If two sensors accept each

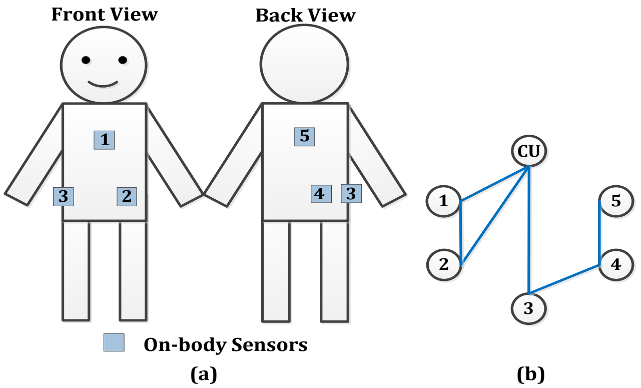

Figure 1: (a) Sensor deployment on the body; (b) Sensor Trust Relationship Topology.

other, we say that they have a *trust relationship*, or they *trust* each other, for which we draw a solid line between them. In this way, we obtain a trust relationship graph of all the tested sensors in our experiment, as shown in Fig. 1(b). Note 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 but conversely the other rejects, no trust relationship is established between them.

From Fig. 1(b), we can see that S_1, S_2 and S_3 are accepted by the CU while S_4 and S_5 are rejected. And S_3 and S_5 are accepted by S_4 while remaining ones are rejected. Considering trust relationship transitivity, i.e. multi-hop trust relationship, we noticed the following phenomenon illustrated in Fig. 1(b): for any pair of on-body sensors, at least one multi-hop path of trust relationship can be found between them, producing actually a connected graph. Our experiment shows that such a connected graph can be easily achieved by strategically deploying a few extra on-body sensors to serve as "hubs". For example, if we attach one sensors to the arm as the "hub", most of the on-body sensors around it would be connected through this "hub" – a one-hop trust path exists between each of them and the nearby "hub". If the CU is placed at LOS locations to these "hubs", channels between the "hubs" and the CU tend to be stable and trust paths between them can be easily found, thereby interconnecting the CU and BAN nodes by trust paths through "hubs". With a few "hub" sensor nodes, the authentication range is able to cover the whole body.

To sum up, our observation includes two prominent characteristics of on-body channels while body motions are involved:

(1) On-Body channels exhibit 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 channels from S_4 and S_5 to CU obviously experiencing larger RSS variations. For channels to S_4, only S_3 and S_5 have stable RSS values; all the other nodes display highly variable RSS values. For other experimental settings the similar phenomenon is observed again. As a close approximation to the actual channel property, especially for heterogeneous devices, fluctuation of RSS values reflects the variations of the channel.

(2) Channels between LOS on-body devices tend to be much more stable than those in NLOS locations. This is clearly shown in Fig. 2. For example, S_3 has much stabler RSSs for its channel to S_4 than other nodes.

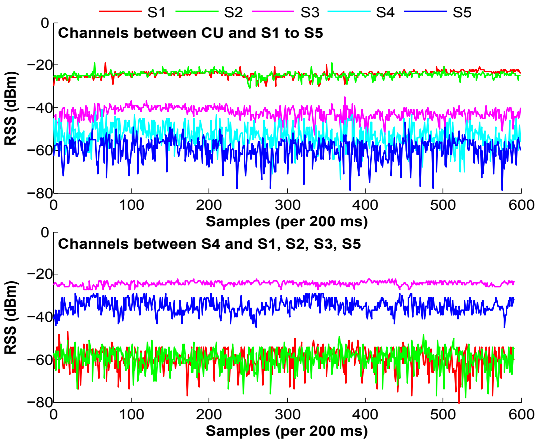

Figure 2: RSS variations among on-body channels.

S_5 is somewhat stabler than S_1, S_2, and the CU. Recall that in this sensor placement, S_4 and S_5 are both on the back of the subject and in clear LOS locations to each other. S_3 is deployed very close to S_4 with clear LOS. S_1, S_2 and the CU are all on the front side of the subject.

4.2 Theoretical Explanation

As we know, direct path loss, multi-path, shadowing and other interference all play important roles in radio wave propagation. The instantaneous received signal strength is a sum of many components coming from different directions due to severe reflection of the transmitted signal reaching the receiver. And the time-variant on-body propagation channels are more complicated because of the effects of the human body. According to [23], on-body signal propagation is mainly composed of a creeping wave diffracted from the human tissue and trapped along the body surface. For different positions on the body, the received signals are further affected by human movements, device placement and surrounding environment. [9] has shown that for on-body channels, the distance between transmitter and receiver has weak correlation to the path loss since shadowing effect has more influence due to different body shapes. Besides, [8] points out that both voluntary and involuntary movements also cause shadowing affecting the line-of-sight.

Line-of-sight channels. Although radio propagation over on-body channels are affected by many factors, it is well understood that the direct path (DP) plays a dominant role among all the factors if the devices are at very close range. Unsurprisingly, the fading of these channels remains relatively stable as long as the devices are kept static at their positions.

Non-line-of-sight channels. As the line-of-sight was obstructed due to the device placement, or body movements break the line-of-sight, fading of NLOS channels is more unpredictable. For BANs, the channel fading is also affected by creeping wave diffracted from the human tissue and trapped along the body surface. Therefore, NLOS channels tend to be more fluctuating in terms of both aptitude and rate.

5. MAIN DESIGN OF ASK-BAN

In this section, we present the main design of our authenticated key extraction scheme ASK-BAN, which is based on the channel characteristics along with body motions. ASK-BAN focuses on fast shared secret key generation between each valid on-body sensor and the CU during the authentication process.

5.1 Overview

Based on wireless channel measurements, we find that there exists a paradox of achieving effective authentication and efficient key extraction simultaneously. That is, while requiring stable channels in terms of RSS variations for authentication, the system needs unstable channels to provide more randomness and higher entropy for fast key generation. To resolves this situation, according to our channel characteristic observations in Section 4, ASK-BAN introduces a "double-win" strategy by involving easily-performed body movements and utilizing different RSS variations not only between on-body and off-body channels but also among on-body channels themselves.

To be specific, ASK-BAN provides multi-hop authentication between the CU and on-body sensors with the help of trusted sensors as relay nodes. We claim that *the trust relationship is transitive*. For example, while channel between sensor A and sensor C experiencing larger RSS fluctuations, 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, then A can trust C with high confidence, and A-B-C is a *trust path* between A and C. Therefore, ASK-BAN asks the verifying nodes (being on-body sensors or the CU) to check whether or not there exists a trust path, possibly including multiple hops, to reach the suspect node. The existence of such a path indicates that the suspect node can be accepted safely. False positive rate in ASK-BAN is expected to be remarkably reduced in many circumstances even with sparsely distributed sensor placement.

For secret key extraction, the main challenge is to achieve a high key generation rate during the authentication process. To this end, between each on-body sensor and the CU, ASK-BAN exploits possible multi-hop paths that exhibit relatively large RSS variations. Different from the collaborative key generation in [15], ASK-BAN utilizes multi-hop relay nodes between the sensor and the CU. It is easy to verify that multi-hop relay solution is secure as long as the on-body devices are deployed half wavelength away from each other for channel independence.

5.2 The ASK-BAN Protocol

The details of our authenticated secret key generation scheme can be described as the following steps:

(1) *Pairwise Key Generation:* A shared secret key will be generated for each pair of sensors in the system, denoted as k_{ij} between sensor S_i and sensor S_j ($k_{ij} = k_{ji}$). In our experiments, we choose Adaptive Secret Bit Generation (ASBG) [13] to build the shared secret key from RSS measurements, which utilizes a modified version of Mathur's quantizer [19] in conjunction with Cascade's information reconciliation [2] and privacy amplification based on leftover hash lemma [12]. Different from ASBG, ASK-BAN generates $(n+1)^2$ pairwise keys among $n+1$ nodes including the CU. Naive application of ASBG will result in $(n+1)^2$ rounds of key generation, which is unacceptably inefficient. To tackle this issue, ASK-BAN proposes a time division duplex (TDD) method to aggregate the communication. That is, nodes in ASK-BAN broadcast messages in the round robin fashion. In this way, we generate $(n+1)^2$ pairwise secret keys with an increase of the time complexity by the order of n than in ASBG, assuming that each broadcast is efficient.

Algorithm 1: Initial Authentication

```
for $i = 1$ to $n + 1$ do
    $S_i$ broadcasts a hello message $M = (x; t_0; t)$;
    for $j = 1$ to $n + 1$ And $j \neq i$ do
        $S_j$ responses after $x + t_{rj}/1000$ seconds, keeps
        repeating every $t$ ms for $t_0$ seconds; $S_i$ measures
        RSS and calculates $S_j$'s $ARV_j$;
    end
    $S_i$ performs classification on all the $ARV$s;
    for $j = 1$ to $n + 1$ And $j \neq i$ do
        if $S_j$ is valid then $S_i$ records $(S_j, T)$;
        else $S_i$ records $(S_j, F)$;
    end
    $S_i$ constructs a trust table based on all the records;
end
```

(2) *Initial Authentication:* As shown in Algorithm 1, CU first broadcasts a hello message $M = (x, t_0, t)$ using a certain transmission power P_{tx} to the sensors around it, requesting responses after x seconds, where x is a random number picked by CU. Upon receiving the hello message, each responding sensor randomly chooses a small number t_r and broadcasts it, indicating the starting time for sending response message. CU collects and checks all the t_r values, ensuring no duplicated ones exist to avoid further transmission collision. And then all the responding sensors broadcast response messages m in the TDD manner as scheduled, repeatedly every t milliseconds and last for t_0 seconds. During the t_0 seconds, each node, including the CU, measures the RSS value of each received message. It is important to note that t is required to be no less than the channel coherence time. Alternatively, this kind of RSS measurements can also be done in parallel with the pairwise key generation stage (step 1) to save time. In that case, the response messages m become whatever messages transmitted in step 1. To avoid confusion, we define this process here as a separate step.

After having collected the RSSs from all the responding sensors, each node calculates the average RSS variation (ARV) for all the other nodes. Applying classification algorithm to these ARV values, they will be partitioned into two groups, where one group has a smaller mean of ARVs and the other group has a larger one. According to the classification result, the CU accepts the sensors whose ARVs belong to the group with smaller ARV mean and rejects the remaining ones in the other group. In this way, each BAN node authenticates all the other nodes. To help further communication, each node records its accept/rejection decision with corresponding node IDs into a table, showing its trust relationship with other sensors in the system by T (accept) or F (rejection).

(3) Authenticated Secret Capacity Broadcast: To construct a key between itself and the CU, each sensor broadcasts the secret capacities of channels between itself and others, and obtains the weighted capacity topology of the whole system. For the convenience of presentation, in this paper we define "secret capacity" as the number of bits with each pairwise secret key generated in step 1. In the rest of the paper we alternatively call it "secret capacity" or just "capacity" for brevity. ASK-BAN performs authentication along with broadcasting capacity information since previous authentication is memoryless.

Algorithm 2: Authenticated Secret Capacity Broadcast

```
for $i = 1$ to $n + 1$ do
    for $j = 1$ to $n + 1$ And $j \neq i$ do
        $S_i$ broadcasts a secret capacity message
        $M_{ij} = (ID_i, ID_j, T/F, C_{ij})$;
        each sensor than $S_i$ stores $M_{ij}$, measures RSS;
    end
end
for each node $S_i$ do
    set trusted group $TG \leftarrow \emptyset$;
    compute $ARV$ for all the other sensors;;
    perform classification on all the $ARV$s;
    for $j = 1$ to $n + 1$ And $j \neq i$ do
        if $S_j$ is valid then $TG \leftarrow TG \cup \{S_j\}$;
    end
    set $VG \leftarrow TG$;
    while $VG \neq \emptyset$ do
        for each $S_j \in VG$ do
            for $k = 1$ to $n + 1$ And $S_k \notin TG$ do
                if $M_{jk}$ indicates $T$ then $TG \leftarrow TG \cup \{S_k\}$,
                $VG \leftarrow VG \cup \{S_k\}$;
            end
        end
        $VG \leftarrow VG \backslash \{S_j\}$;
    end
    save $TG$ as the trust table;
    construct a security capacity topology based on all the
    capacity messages of nodes in $TG$;
end
```

To be specific, a sensor node S_k broadcasts a capacity message $(ID_k, ID_l, T/F, C_{kl})$ which contains the ID of the endpoints of the channel with each of its neighbors, say S_l, the trust relationship learned from previous steps, and the channel secret capacity C. Sensors that receive capacity messages store the messages in the buffer temporarily. Meanwhile, each of S_k's neighbors measures the channel, collects RSS values and calculate S_k's ARV for later authentication. This means that broadcasting the capacity messages shall last for t_0 seconds similar to step 2, in the TDD manner with possibly repeated broadcasting of the messages.

For a single node, it assumes there is a null trusted group at the beginning. After all sensors broadcasting own capacity messages and getting capacity messages from others, each one performs classification on the collected ARVs, producing two groups with different ARV mean values, and then adds the sensors whose ARV values are in the group with smaller ARV mean into the trusted group. The nodes in the trusted groups are believed to be authenticated or trusted. The capacity messages of trusted neighbors will be processed to find the nodes that are trusted by these neighbors, i.e., those with a T in the neighbors' capacity message. These newly found node are added into the trusted group if they were not there. This process is recursively executed until all the nodes with a trust path to the node are added to the trusted group. At the end of this phase, each node will has the knowledge of all the channel secret capacity information as well as the set of trusted neighbors. An undirected weighted graph, depicting the capacity topology, can be derived based on the capacity messages, with the weight of each edge representing the secret capacity on the channel. Algorithm 2 summarizes the above process.

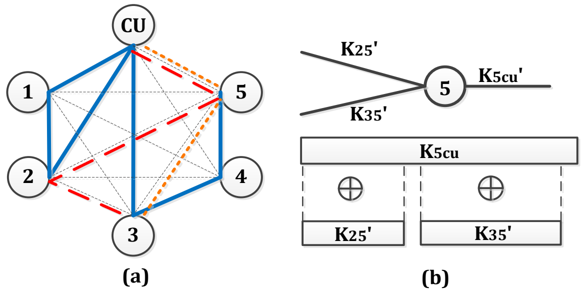

Figure 3: (a) Max-flow path from Sensor 3 to CU; (b) Max-flow multi-path merging scenario.

Algorithm 3: Key Aggregation Broadcast

```
each node runs the max-flow algorithm for source and CU
with the secrecy capacity graph;
for each node $S_j$ other than source and CU do
    for each max-flow path $P_x$ that $S_j$ belongs to do
        determine the keys $k'_{ij}$ and $k'_{jk}$ from $k_{ij}$ and $k_{jk}$ for
        neighbor $S_i$ and $S_k$ respectively;
        broadcast $M_{xj} = (j, p_{ij}, p_{jk}, k'_{ij} \oplus k'_{jk})$;
        // $p_{ij}/p_{jk}$ are positions of $k'_{ij}/k'_{jk}$ in $k_{ij}/k_{jk}$.
        source and CU store $M_{xj}$ if $j$ is trusted;
    end
end
for each max-flow path $P_x$ do
    source and CU derive a shared key $k_x$ using $M_{xj}$'s;
end
source and CU derive the final shared key as the
concatenation of $k_x$'s;
```

(4) Deciding Maximum Entropy: Based on the capacity topology, we would like to know the maximum size of secret key, in terms of bit number, that can be delivered from each sensor to CU based on the channels with different secret capacities. In the above authentication process, CU might directly accept some on-body sensors, whose channels to CU are stable with a low-entropy key between each of them and CU. Even if the sensor is authenticated by multi-hop authentication, it cannot guarantee that the direct unstable channel between itself and CU has the highest entropy. The task is thus to find out the maximum secret key that can be obtained between a sensor and CU according to the capacity topology. We realize that this actually becomes a generalization of single-source single-sink maximum-flow problem[24]. Therefore, each sensor node runs the maximum-flow algorithm on the topology to find the path(s) through which the entropy of the key information transmitted from itself to CU can be maximized.

(5) Key Aggregation Broadcast: After finding the max-flow path(s) between a source sensor node and the destination node CU, the sensor node securely exchanges its derived secret key along the path(s) to help itself and CU extract a shared maximum secret key. For this purpose, each of the remaining sensors on the path(s), except the source sensor and the destination node CU, broadcasts the XORed value of the keys shared with its previous-hop and next-hop sensors in turn. For example, in Fig.3, if there is a max-flow path 3-2-5-CU between node 3 and the CU, the intermediate nodes 2 and 5 shall broadcast $k_{23} \oplus k_{25}$ and $k_{25} \oplus k_{5CU}$ respectively. Note that if these two keys are not of the same length, the longer one will be truncated for the XOR operation. Only having the knowledge of its shared key k_{23} with node 2, node 3 derives the shared key k_{25} from the broadcast message $k_{23} \oplus k_{25}$ thereby obtaining k_{5CU} from $k_{25} \oplus k_{5CU}$. In the similar way, CU can derive the shared key k_{23} and k_{25}

based on the broadcast messages. On this max-flow path, the shared secret key between node 3 and CU will be either k_{23} or k_{5CU}, which is truncated to the length of the shorter one of k_{23} and k_{5CU}. If there exists other max-flow paths between node 3 and CU, a key will be obtained on each of these paths following the above process, and all these keys are concatenated to form the ultimate shared secret key between node 3 and CU.

It is noteworthy that this kind of multi-hop relay does not result in losing the entropy of the ultimate shared key, which can be easily proven using the method in [15]. During the broadcast process, when the source sensor and the CU receive such a key aggregation message, they will refer to the trust table stored in the memory to decide whether or not to accept the content of the message. The broadcast message is accepted if and only if its sender is in the trust table. Based on the information obtained from every accepted broadcast messages, with the key possessed by itself, this sensor gets all the shared keys along the path(s) by XOR operations if all the nodes on the path(s) are trusted. The final secret key shared with the CU is the concatenation of the shared keys from individual max-flow paths.

Here, special attention shall be paid to the case of *merging* or *splitting* of the paths on the nodes, i.e., there might be two or more flows merging into one flow on a node or one flow splitting into two or multiple flows. As the topology graph is undirected, *merging* and *splitting* are essentially the same. Take Fig.3 for example, there are two max-flow paths 3-2-5-CU and 3-5-CU, which join at node 5. As the secret key bits extracted from different paths are required to be independent to each other, we shall guarantee no overlapped bits used by the XORed value sent from node 5 for the two paths. Specifically, in the two messages $k'_{25} \oplus k'_{5CU}$ and $k'_{35} \oplus k''_{5CU}$ for the two paths respectively, k'_{5CU} and k''_{5CU} shall be non-overlapped segments of k_{5CU}, where k'_{25} and k'_{35} are bits drawn from k_{25} and k_{35} separately. Therefore, besides the XORed value of neighboring keys, the broadcast message also needs to include the bit segment starting position of each key used by the XOR operation. That is, k'_{5CU} may start from bit position P_1 in k_{5CU} with length L_1 and k''_{5CU} with position P_2 length L_2, where $P_1 + L_1 \leq P_2$. Note that the lengths L_1 and L_2 are not necessary to be included in the broadcast message, because the receiving nodes are able to derive this information for each path after running the same max-flow algorithm. But the broadcast message shall point out which max-flow path the message is for, i.e. the message $k'_{25} \oplus k'_{5CU}$ is for path 3-2-5-CU. In implementation, such information can be represented using bit maps to save space. The above processing method is also applicable for n-to-1 merge where $n > 2$. More generally, it can be easily applied to n-to-m cases wherein both merging and splitting happen on the same node. Algorithm 3 describes the process combining both step (4) and (5).

5.3 Security Analysis

Node Authentication: With artificially introduced simple body movements, we assume that for one-hop authentication, i.e. direct authentication between two devices without any relay node, off-body devices have a very low probability, denoted as p, to falsely get accepted by on-body devices. In ASK-BAN, for authentication with the help of k-hop relay nodes, the chance of off-body devices being accepted mistakenly increases from p to kp. However, $p \leq 1$ and p is generally very low. Moreover, a BAN device can find at least one multi-hop trust path to the CU with the help of "hubs". In practice a patient will not wear too many BAN devices on-body, implying that the value of k shall be small in real-world applications (e.g., $k \leq 3$ for Fig. 1(b)). Thus, with small kp, off-body devices actually do not get more chances to be authenticated. From another perspective, due to extra nodes for relaying purpose in ASK-BAN, every legitimate on-body sensor has more opportunities to be accepted. Therefore, multi-hop authentication would not result in a significant false positive rate in reality.

Secrecy of the Extracted Key: As attackers are off-body and their channels to on-body devices are uncorrelated to on-body channels, they are not able to derive the secret key bits generated by on-body nodes. It is remarkable that, in step 5 we did not impose any requirement for RSS-based authentication, while step 1 does not have this problem since step 2 can actually be integrated with step 1 without affecting the system performance. We claim that this does not compromise our security goals. The reason is that what the attacker is able to achieve at best is to broadcast messages in the name of an legitimate node. However, broadcasting XORed value of his own keys or other random strings does not give the attacker more chances of obtaining the secret keys shared between on-body sensors, nor does it reduce the entropy of the final shared key derived by on-body sensors. In fact, this kind of behavior can only cause denial-of-service attack, which is out of the scope of our security goals.

Also we point out that broadcasting XORed values of each node dose not cause losing entropy of the shared key on each max-flow path between this node and the CU as discussed in [15], nor does it result in losing entropy of another on-body node's shared secret key as long as the on-body channels are not correlated with off-body channels. Moreover, the secret keys shared by different on-body sensors and the CU are not required to be independent since they trust each other.

Man-In-The-Middle Attacks: As stated in [10], signal-based key generation schemes are vulnerable to Man-in-the-Middle (MITM) attacks only by using off-the-shelf hardware. Although Eve is positioned at least half a wavelength away from Alice and Bob and Eve only has uncorrelated estimates between Alice and Bob, MITM attack can be launched by impersonating both Alice and Both and injecting Eve's own information during the channel response estimation (the quantization phase, specifically), which is used by Alice and Bob as part of their secret key.In this way, the secret key generated by Alice and Bob might be revealed partially. Although it seems practical, this kind of attack does not work well on our ASK-BAN system. Since ASK-BAN performs authentication and key generation at the same time, attackers has few chances to pass authentication and get involved in the key extraction phase. In addition, in ASK-BAN, the secret key between Alice and Bob is generated not only based on the physical properties between themselves, but also based on the channel measurements of relaying devices between them. In this case, it is difficult for attackers to guess all bits of the final secret key.

Beam-forming Attacks: Theoretically, a powerful faraway attacker might form a special beam using advanced devices, such as directional antenna, attempting to produce relatively stable channels to on-body devices and finally get accepted by the system mistakenly. As analyzed in [3], we believe this type of attack is hard to implement in practice, if not completely impossible. In particular, the width of the main lobe beam is inversely proportional to the antenna array size. To successfully launch this attack, a large antenna is required since the distance between every two on-body devices is no more than 1 to 2 meters. In most of the real-life scenarios, larger antenna array will probably raise suspicion. For NLOS antenna arrays, it is more difficult to perform such an attack since attackers cannot accurately direct the antennas toward the patient who is conducting random body movements during the whole process. Furthermore, multipath effects caused by walls and indoor objects will also distort the intended beam.

5.4 Discussion

Node deployment: In ASK-BAN, BAN nodes are required to be strategically deployed such that there exists both stable (trust) path(s) and unstable path(s) between every sensor to the CU. In practice, this is easy to achieve. For example, we can either place several in front of the body and others on the back/side of the body, or attach a few extra COTS sensors to arms/legs to serve as "hubs", keeping their relatively close to each other to guarantee the existence of LOS and NLOS channels. Our experiments show that this kind of placement is effective and easy-to-use for ordinary users.

It is important to note that not all of these device are medical sensors in some circumstances, i.e., a few of them might be the extra nodes specially introduced to help with authentication and/or secret key extraction. It is not necessary for extra nodes to have the capability of measuring physiological features; they could be general devices with the basic communication and forwarding ability. Therefore, using extra nodes would not increase the costs greatly.

In addition, as ASK-BAN relies less on the strict relative positioning between the CU and each BAN sensor, it relaxes the requirements for patient on controlling body movements.

Scalability: Number of nodes may impact the performance of our scheme since ASK-BAN utilizes TDD for message broadcasting in most steps. A large number of nodes would result in a long duration for each round of TDD, thereby probably causing some pairs of nodes to measure RSSs in different coherence time periods for their shared channel. Key generation rate will also be affected due to the high error rate for RSS measurements between the pairs. To eliminate these potential effects, we can either limit the number of sensor nodes to a reasonable range, or force the nodes to cluster into groups of fixed size. For example, while node 1 just measuring nodes $\{1, 2, \cdots, k\}$, node 2 measures nodes $\{2, \cdots, k, k+1\}$, $\cdots$, and node n measures nodes $\{n, 1, 2, \cdots, k-1\}$. The corresponding algorithm will be the same except that each node needs to set the secret capacity of nodes outside its set as 0.

6. EVALUATION

To evaluate our scheme ASK-BAN, experiments are conducted under different settings. The evaluation mainly focuses on two aspects - effectiveness of node authentication and efficiency of secret key extraction. During the experiments we considered various factors that may affect the performance of the scheme, including room size, type of patient's body motion, placement of the on-body nodes as well as differences between subjects.

6.1 Experimental Setup

Experiments were conducted on Crossbow TelosB motes (TRP2400) which are all equipped with IEEE 802.15.4 radio. We used ten TelosB motes in experiments: eight motes as on-body sensors, one as the CU and one as the off-body attacker. During the experiments, the realtime RSSs measured by the motes are sent to the computer for analysis and simulation. We also varied the ratio of number of on-body sensors to that of off-body attackers. For device authentication, we emphasize on the effectiveness of differentiating on-body motes from off-body nodes with our multi-hop authentication scheme. For secret key extraction, our major concern is the key generation rate between sensors and the CU.

To show the advantage of ASK-BAN, we compare its authentication performance with BANA. Experiments were conducted in three locations - a small room, a medium-sized room and a relatively large corridor in a college building. Three subjects, two males and one female, are involved in the experiments. The following body movements are studied: walking randomly; sitting-and-rotating, i.e. subject who acts as a patient sits on a chair and the chair is rotated; sitting-and-rolling, i.e. subject who acts as a patient sits on a chair with wheels and is moved around by another subject. These movements are easy to self-perform or accomplished with help for patients even with limited moving capability. On each subject, according to the usual positions of COTS on-body sensors in real applications, the mote placement location includes chest, arms, back, waist, thighs. It is important to note that we do not have stringent requirements on the movements. For example, for walking randomly, subjects are allowed to walk normally rather than walking specially slowly. Also, the CU is not required to be placed at a strictly fixed location. The CU can either be put away from the body or be hang on the body. In addition, on-body sensors can be placed on both the back and the front of the body without affecting the performance of ASK-BAN. Note that BANA only tested the cases wherein sensors are all placed in front of the body and facing CU.

6.2 Results and Evaluation

6.2.1 Node Authentication

For node authentication alone, we conducted 18 experiments with the random combination of the following factors - experiment location, type of body movement, mote placement and subject. In the experiments we sample the collected RSSs every 200ms. For some of the scenarios, we varied the ratio of on-body sensors to off-body attackers from 7:1 to 5:3. Note that in the settings of large corridor, the attacker is either static or following behind the rolling wheelchair, while in the settings of small room and medium room the attacker is static inside/outside the room. The results are shown in Table 1 with comparison to BANA.

From the table, we can see that the overall false positive rate for the 18 experiments in ASK-BAN is almost 16 times less than that of BANA, reducing from 37.72% to 1.75%. Such a dramatic difference can mainly be explained by the flexible sensor placement in the experiments. With sensors in the front, on the back, on the side or other positions of the body, some of them do not have LOS channels to the CU directly. As BANA was designed for direct LOS on-body device authentication, it is not surprising that its false

	ASK-BAN	BANA
Small	2.38%	38.10%
Medium	2.70%	37.84%
Corridor	0%	37.14%
Sitting-and-rotating	0%	34.29%
Sitting-and-rolling	0%	37.14%
Walking	4.55%	40.91%
Subject 1	3.13%	31.25%
Subject 2	2.27%	40.91%
Subject 3	0%	39.47%
overall	1.75%	37.72%

Table 1: The false positive rates for ASK-BAN and BANA.

positive rate obviously increases to an extent that is not affordable since on-body sensor with NLOS channels to the CU would probably be rejected.

Interestingly, the false positives in ASK-BAN mainly happened in the small room and medium room scenarios, as well as the walking scenarios. This can be partially explained by the fact that small rooms and medium rooms tend to have more severe multipath effect due to the close distance from the patient to the walls while the patient is randomly walking. In these experiments, the false negative rate of ASK-BAN under different on-body to off-body node ratios remains 0, which is the same as in BANA.

6.2.2 *Authenticated Secret Key Extraction*

Our experiments also validate the efficiency of ASK-BAN in terms of secret key extraction rate. In our experiments, to obtain the precise key generation rate, we lasted the key extraction process for 30 seconds during the authentication. Based on the 30-second measurements, we calculate the final key generation rate (bps) as the total number of generated secret key bits during this process divided by 30. In these tests, we tried to maximize the number of RSSs measured per second, thereby expecting the maximal value of the secret key extraction rate. Using TelosB motes (TRP2400) we found that during each round of TDD broadcast, a transmission time (t) of $6ms$ for each mote results in a near-perfect packet delivery ratio (PDR). When the time t is reduced to $4ms$, the PDR dramatically decreases by up to 30%. If t is long, the measured channels might be more independent due to short coherence time, from which the key entropy benefits, while the key generation rate is reduced. If t is short, the key generation rate is increased but with lower entropy. To balance the tradeoff and find a propriate value of t, we tried both $5ms$ and $6ms$ in the experiments.

As mentioned Section 5.2, ASK-BAN adopts the ASBG scheme for pairwise key generation, which uses a modified version of Mathur's quantization. For Mathur's quantization, two thresholds $q-$ and $q+$ are used such that RSS values within $[q-, q+]$ are dropped, where $q- = mean - \alpha * std\_deviation$ and $q- = mean + \alpha * std\_deviation$, $0 < \alpha < 1$. The $Range$ of remained RSS values is divided into M intervals and then for each RSS value $\lfloor \frac{Range}{M} \rfloor$ bits can be extracted. During this process, appropriate choice of quantization parameters is critical to the final secret key rate. In particular, the quantization thresholds and intervals play important roles. Lower quantization thresholds and less intervals would produce more bits, but possibly with higher bit error rate as well as lower entropy.

In our experiments, we varied the parameters and attempted to find the best ones for future reference. For this purpose, we picked RSS serials for the measured channels, including relatively stable channels and unstable ones. And then we tried to extract secret keys based on single channel, using the ASBG scheme with varying α and M respectively. Experimental results show that $\alpha = 0.7$ and $M = 4$ result in best key generation rate in general as shown in Fig.4. Therefore, in the rest of our experiments, we stick to these values for α and M.

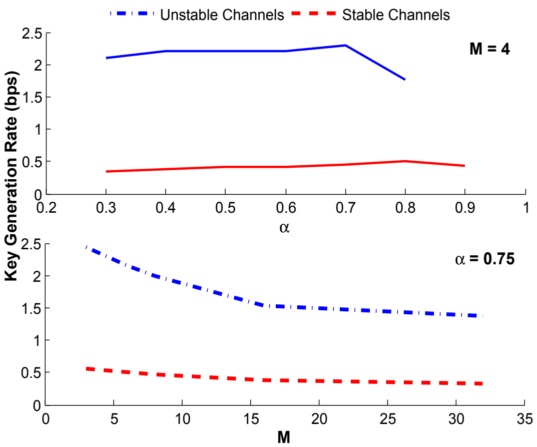

Figure 4: Secret key rate versus quantization thresholds and intervals, based on single channel.

Key Generation Rate of ASK-BAN: Based on our experiments with eight on-body devices, Fig. 5 presents results of small room scenario and corridor scenario. Specifically, in small room scenario sitting-and-rotating was performed by the three subjects respectively, while in corridor scenario sitting-and-rolling was performed, with similar configuration of sensor placements. We found that ASK-BAN is able to achieve an average secret key rate of $7.29bps$ in the corridor if $t = 6ms$ for each node. For the small room scenarios, while the corresponding rate is about $8.03bps$ with $t = 5ms$, for $t = 6ms$ setting it is also about $8.03bps$. Therefore, to generate a 128-bit key, ASK-BAN only needs $15.9s$ in small room scenarios and $17.5s$ in corridor scenarios, which outperforms other candidate solutions we considered for BANs. On the other hand, if we utilize the direct channel to the CU for each node to extract the secret key, the average bit rates are about $1.04bps$, $0.90bps$, and $0.94bps$ for the settings of corridor-$6ms$, small room-$5ms$, and small room-$5ms$, respectively. This means that ASK-BAN boosts the secret bit rate for about 8 times than that if using direct channels to the CU. Note that for $t = 5ms$ and $t = 6ms$, the final key rate is comparable.

We also applied the collaborative secret key generation method suggested by Lai et al.[15] for comparison. To collaboratively generate the shared secret key between one sensor and the CU, all the available sensor nodes are selected as one-hop relay nodes. That is, multiple paths, each with one relay node chosen from other nodes are built between that sensor and the CU. The comparative results are shown in Fig. 5. From this figure, it is easy to see that ASK-BAN is about 2 to 4 times faster than one-hop relay method. Meanwhile, we noticed that the secret key bit rates in small rooms are slightly larger than those in the corridor on average.

In summary, along with node authentication, ASK-BAN is able to achieve up to 9bps for a single node. To update keys over time, instead of regenerating authenticated key from

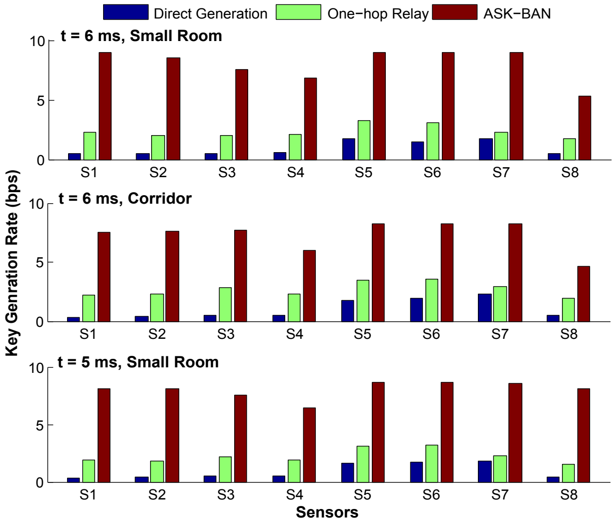

Figure 5: Comparison of secret key rate of ASK-BAN utilizing max-flow algorithm, one-hop relay method, and direct generation.

scratch, a complementary mechanism [31] can be combined with our scheme, which utilizes dynamic secrets extracted from real-time communication to update the system secret by XOR operation.

Secrecy of On-body Channel: To measure the secrecy of the on-body channels, we evaluated the mutual information between on-body channels and off-body channels. Assume A and B are two on-body nodes and C is the off-body attacker. When A is broadcasting, the RSSs measured by B are denoted as RSS_{AB} and those by the attacker are RSS_{AC}. And RSS_{BA} and RSS_{BC} represent the corresponding values by A and C respectively when B is broadcasting. We use mutual information $I(RSS_{AB}; RSS_{AC})$ and $I(RSS_{BA}; RSS_{BC})$ to estimate the channel dependencies for AB-AC and BA-BC separately. $I(RSS_{AB}; RSS_{BA})$ is also used to estimate the dependency between channels AB and BA. We selected channels on the max-flow paths and examined the above channel dependency values. Results show that mutual information between on-body channels and off-body channels is less than 0.5 on average for 6 to 7 bits RSS measurements, indicating good independence between on-body channels and off-body channels. And the mutual information for RSSs measured by the two endpoints for each channel is around 1 on average. Endpoints that measure the channel in consecutive time slots exhibit higher dependency than those measured in more distributed time slots.

7. CONCLUSIONS

In this paper, for the first time we propose ASK-BAN, a lightweight authenticated secret key extraction protocol for BAN only based on wireless channel measurements. We observed that the heterogeneous channel qualities among the collection of on-body channels - those between line-of-sight (LOS) on-body devices are relatively stable while those for non-line-of-sight (NLOS) devices are more dynamic. By utilizing this channel property, we solved the self-contradictory paradox of achieving effective node authentication and fast secret key extraction simultaneously. Our multi-hop authentication scheme in ASK-BAN can significantly reduce the false positive rate compared to previous work. To maximize the secret key generation rate, we combine the multi-hop authentication scheme with a novel collaborative secret key extraction solution based on the max-flow algorithm. Experimental and simulation results show that ASK-BAN is able to provide accurate node authentication while achieving fast secret key extraction.

For future work, we would like to further improve the secret key extraction rate. Moreover, it is interesting to provide protection against strong attacks such as attackers with directional antenna.

8. REFERENCES

[1] D. Bichler, G. Stromberg, M. Huemer, and M. Löw. Key generation based on acceleration data of shaking processes. In *Proceedings of the 9th international conference on Ubiquitous computing*, UbiComp'07, Berlin, Heidelberg, 2007. Springer-Verlag.

[2] G. Brassard and L. Salvail. Secret-key reconciliation by public discussion. In T. Helleseth, editor, *Advances in Cryptology ął EUROCRYPT ąŕ93*, volume 765 of *Lecture Notes in Computer Science*, pages 410–423. Springer Berlin / Heidelberg, 1994.

[3] L. Cai, K. Zeng, H. Chen, and P. Mohapatra. Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas. In *Proceedings of the Network and Distributed System Security Symposium, NDSS 2011, San Diego, California, USA, 6th February - 9th February 2011*. The Internet Society, 2011.

[4] 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*, pages 432 – 439, oct. 2003.

[5] C. Cornelius and D. Kotz. Recognizing whether sensors are on the same body. In *Proceedings of the 9th international conference on Pervasive computing*, Pervasive'11, Berlin, Heidelberg, 2011. Springer-Verlag.

[6] S. Cotton, A. McKernan, A. Ali, and W. Scanlon. An experimental study on the impact of human body shadowing in off-body communications channels at 2.45 ghz. In *Antennas and Propagation (EUCAP), Proceedings of the 5th European Conference on*, pages 3133 –3137, april 2011.

[7] S. Cotton, A. McKernan, and W. Scanlon. Received signal characteristics of outdoor body-to-body communications channels at 2.45 ghz. In *Antennas and Propagation Conference (LAPC), 2011 Loughborough*, pages 1 –4, nov. 2011.

[8] 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*, pages 1 –3, oct. 2010.

[9] 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*, pages 908 –911, oct. 2011.

[10] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinovic. A practical man-in-the-middle attack on signal-based key generation protocols. In *Computer Security - ESORICS 2012*, volume 7459 of *Lecture Notes in Computer Science*, pages 235–252. Springer Berlin Heidelberg, 2012.

[11] X. Hei and X. Du. Biometric-based two-level secure access control for implantable medical devices during

emergencies. In *INFOCOM, 2011 Proceedings IEEE*, pages 346 –350, april 2011.

[12] R. Impagliazzo, L. A. Levin, and M. Luby. Pseudo-random generation from one-way functions. In *Proceedings of the twenty-first annual ACM symposium on Theory of computing*, STOC '89, pages 12–24, New York, NY, USA, 1989. ACM.

[13] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy. On the effectiveness of secret key extraction from wireless signal strength in real environments. In *Proceedings of the 15th annual international conference on Mobile computing and networking*, MobiCom '09, pages 321–332, New York, NY, USA, 2009. ACM.

[14] 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.

[15] L. Lai, Y. Liang, and W. Du. Phy-based cooperative key generation in wireless networks. In *Communication, Control, and Computing (Allerton), 2011 49th Annual Allerton Conference on*, pages 662 –669, sept. 2011.

[16] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester. A survey on wireless body area networks. *Wirel. Netw.*, 17(1):1–18, Jan. 2011.

[17] 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*, MobiSys '11, pages 211–224, New York, NY, USA, 2011. ACM.

[18] 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.

[19] 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*, MobiCom '08, pages 128–139, New York, NY, USA, 2008. ACM.

[20] R. Mayrohofer and H. Gellersen. Shake well before use: authentication based on accelerometer data. In *Proceedings of the 5th international conference on Pervasive computing*, Pervasive'07, Berlin, Heidelberg, 2007. Springer-Verlag.

[21] R. Mayrohofer and H. Gellersen. Shake well before use: Intuitive and secure pairing of mobile devices. *Mobile Computing, IEEE Transactions on*, 8(6), june 2009.

[22] 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. *Communications Magazine, IEEE*, 44(4):73 – 81, april 2006.

[23] J. Ryckaert, P. De Doncker, R. Meys, A. de Le Hoye, and S. Donnay. Channel model for wireless communication around human body. *Electronics Letters*, 40(9):543 – 544, april 2004.

[24] F. Shahrokhi and D. W. Matula. The maximum concurrent flow problem. *J. ACM*, 37(2):318–334, Apr. 1990.

[25] L. Shi, M. Li, S. Yu, and J. Yuan. Bana: body area network authentication exploiting channel characteristics. In *Proceedings of the fifth ACM conference on Security and Privacy in Wireless and Mobile Networks*, WISEC '12, pages 27–38, New York, NY, USA, 2012. ACM.

[26] Shimmer. http://www.shimmer-research.com/p/sensor-and-modules.

[27] 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*, pages 353 –358, dec. 2007.

[28] 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.

[29] 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, jan. 2010.

[30] K. K. Venkatasubramanian and S. K. S. Gupta. Physiological value-based efficient usable security solutions for body sensor networks. *ACM Trans. Sen. Netw.*, 6(4):31:1–31:36, July 2010.

[31] S. Xiao, W. Gong, and D. Towsley. Secure wireless communication with dynamic secrets. In *INFOCOM, 2010 Proceedings IEEE*, pages 1–9, march 2010.

[32] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li. Imdguard: Securing implantable medical devices with the external wearable guardian. In *INFOCOM, 2011 Proceedings IEEE*, pages 1862 –1870, april 2011.