MASK-BAN: Movement-Aided Authenticated Secret Key Extraction Utilizing Channel Characteristics in Body Area Networks

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

***Abstract*—Recently, most wireless network security schemes merely based on physical layer characteristics tackle the two fundamental issues—device authentication and secret key extraction 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, we answer this open problem in the setting of wireless body area networks (BANs). We propose MASK-BAN, a lightweight fast authenticated secret key extraction scheme for intra-BAN communication. Our scheme neither introduces 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. On one hand, MASK-BAN achieves authentication through multihop stable channels, which greatly reduces the false positive rate as compared to existing work. On the other hand, based on dynamic channels, key extraction between two on-body devices with multihop 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 commercial-off-the-shelf sensor devices validate MASK-BAN's great authentication capability and high-secret key generation rate.**

***Index Terms*—Authenticated key generation, physical layer, received signal strength (RSS), sensor, wireless body area network (WBAN).**

I. Introduction

With increasing prevalence of wireless devices, secure wireless communications have been more imperative than ever focusing on two most fundamental issues, device authentication, and secret key extraction. Recent research has shifted attention to bootstrapping security for wireless communications merely based on physical layer characteristics. Such a trend is mostly due to rising concerns on drawbacks of applying conventional public and symmetric-key techniques in wireless networks: preloading secret keys on heterogeneous wireless devices is less practical; wireless devices are more likely to be subject to physical compromise; expensive cryptographic primitives for authentication and key distribution; and assumptions of attacker computation boundary. Bootstrapping security from physical layer characteristics can eliminate the complex process of key distribution and the computational assumptions, and thereby achieving better efficiency and security for wireless networks.

Existing literature in this area mainly utilizes three types of physical layer characteristics for bootstrapping security: 1) *advanced hardware* [1]–[5]; 2) *out-of-band (OOB) communication channels* [6]; and 3) *wireless channel measurements* [7]–[9]. Approaches based on the first two types assume the availability of additional resources to measure or extract information for device authentication [2], [3], [10], [11] or secret key generation [1], or both [12]. However, in ubiquitous environments, wireless devices, especially commercial-off-the-shelf (COTS) ones, are usually constrained in hardware configuration that requires extra modifications of system stack. OOB communication channels are not always available. Wireless channel measurements-based approach is promising in bootstrapping security for wireless devices in ubiquitous environments, since the requirements on the wireless system are minimal—only measuring wireless communication channels [e.g., received signal strengths (RSSs)]. Practical systems often require device authentication and secret key generation to be fulfilled concurrently. To our best knowledge, there is no such work simultaneously providing effective device authentication and fast secret key extraction simply by wireless channel measurements.

In this paper, we answer this open problem in wireless body area networks (BANs) and propose MASK-BAN, a lightweight, body movement-aided authenticated secret key extraction scheme for intra-BAN communication. Without advanced hardware and OOB communication channel, MASK-BAN achieves device authentication and secret key extraction simultaneously only by wireless channel measurements between BAN nodes. MASK-BAN is inspired by our important observations of channel characteristics when body movements are involved: channels between the control unit (CU) and on-body sensors (OBSs) in line-of-sight (LOS) vicinity tend to be more stable than OBSs in nonline-of-sight (NLOS) locations. However, channels between off-body devices and CU experience much severer fluctuations than on-body channels, whether

Manuscript received July 01, 2014; revised October 26, 2014; accepted December 29, 2014. Date of publication January 12, 2015; date of current version February 10, 2015. This work was supported by the National Science Foundation (NSF) under Grant CNS 1347552.

L. Shi, J. Yuan, and S. Yu are with the Department of Computer Science, University of Arkansas at Little Rock, Little Rock, AR 72211 USA (e-mail: lxshi@ualr.edu; jxyuan@ualr.edu; sxyu1@ualr.edu).

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

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JIOT.2015.2391113

OBSs are LOS or NLOS to CU. Utilizing *relatively stable channels* between OBSs, device authentication guarantees that all the sensor devices to communicate with CU are on the same body. Concurrently, secret keys are extracted between every authenticated OBS and CU, utilizing their *relatively unstable channels*. Specifically, to seek multihop stable channels and multihop unstable channels between every OBS and CU, MASK-BAN introduces authentication transitivity, i.e., trust relationship is established between nodes A and B if node A authenticates a relay node, which authenticates node B. In this way, an OBS is validated if at least one relatively stable multihop channel to the CU exists. Along multihop unstable channels between one sensor and CU, a final secret key is derived from pairwise keys between relay nodes in between with maximized key generation rate and entropy in terms of number of bits. Our experiments on real-sensor devices prove the existence of both stable and unstable multihop on-body channels. MASK-BAN is shown to provide concurrent node authentication and secret key extraction with a high rate.

We summarize our major contributions as follows. 1) MASK-BAN is the first work that provides authenticated secret key extraction using only wireless channel measurements. 2) Generally, MASK-BAN greatly reduces false positive rate through our multihop authentication scheme. 3) MASK-BAN introduces a novel collaborative secret key extraction scheme with multihop relay nodes based on the max-flow algorithm, which can find application in other wireless systems.

Note that this paper is the extended version of [13]. This paper is organized as follows. Section II gives an overview of related work. Section III defines the problem and the system model. We illustrate our observations of unique BAN channel characteristics in Section IV, followed by the detailed description of MASK-BAN in Section V. Section VI evaluates and discusses our experimental and simulation results of implementing MASK-BAN on real sensors. We conclude this paper in Section VII.

II. Related Work

In this section, we review existing noncrypto key generation and authentication schemes based on physical layer characteristics.

By using *nonwireless channels* in some constrained scenarios, it is possible to simultaneously achieve secret key generation and device authentication. Such works are mainly *biometric-based* and *motion-based*. By physiological signals, physiological information collected from sensors is compared, such as electrocardiogram (ECG), iris ,and fingerprint, to assist authentication and key establishment without a prior distribution of keying material [10]–[12], [14]–[16]. However, biometrics derived from physiological features usually suffer from high degrees of noise and variability inherently present in the signals. Also, it cannot guarantee consistent physiological signal measurements with the same accuracy for sensors in different positions. Moreover, not all the physiological parameters have the same level of entropy for key generation [17]. Similarly, motion-based authentication and key generation [1], [2], [4], [5] require specialized sensing hardware and human participation, which is demanding for COTS devices.

In recent years, *wireless channels* become widely used for authentication and/or key generation. For device authentication, wireless channels have been used to determine *device proximity* by the difference between the RSS [3], [7], [8]. Taking advantage of wireless channel characteristics with body motions, Shi *et al.* [9] proposed body area network authentication (BANA), a lightweight authentication scheme based on RSS measurements only. However, BANA only considers authentication for LOS on-body devices. For key generation, several seminal schemes were proposed [18], [19]. Along this direction, one of the key research topics is to improve the key generation rate. Lai *et al.* [20] exploited random channels associated with relay nodes in the wireless network as additional random sources for key generation, but only between two nodes with one-hop relay nodes.

Nevertheless, using wireless channel alone, it has been demanding to realize authentication and key generation at the same time in such a dilemma: authentication usually requires proximity, while fast key generation requires channel fading that proximity cannot provide. Take BANA [9] for example, since its authentication does not generate a credential and hence is “memoryless,” it is difficult to derive an authenticated secret key by directly applying existing key extraction techniques to BANA. Alternatively, simply utilizing channels between BAN sensors and CU would result in a low-key generation rate with low entropy carried by these stable channels. 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. Addressing this challenge, we take a step forward for achieving effective authentication and fast key generation concurrently only based on wireless channels in BAN. Unlike previous work, our MASK-BAN does not require advance hardware for physical layer characteristic measurement, nor does it rely on auxiliary OOB channels. Since wireless channel characteristics can be measured by most COTS devices, MASK-BAN can easily be adopted in a wide range of applications. To the best of our knowledge, our work is the first in the literature to achieve authenticated secret key generation using channel characteristics.

III. Problem Definition

A. System Model and Assumptions

Our wireless BAN is composed of n COTS sensors and one CU. Worn on the body, sensors measure physiological signals and transmit the collected data to CU, but are resource-constrained with limited energy supply, memory space, and computation capabilities. As a hand-held device such as a smart phone or PDA, CU is worn on body or placed near the body with close physical proximity, i.e., less than 1 m to all OBSs, for aggregating and/or processing the received data, and relaying the data to local or remote trusted third-parties such as caregivers, physicians, and emergency services.

All the BAN devices have wireless communication capability, but neither advanced hardware (e.g., multiple antenna, accelerometer, and GPS) is equipped nor OOB channel is available. We assume static relative positions between the BAN nodes during the security bootstrapping process with body movements. Extensive existing work has shown that the coherent signal observations located greater than half wavelength away from two communicating wireless devices are typically not correlated. In this paper, nodes are placed at least half wavelength (approximately 12.5 cm for Zigbee radios) away from each other to ensure uncorrelated wireless channels. For some users may have limited mobility, easily-done body movement options are available in our experiments: 1) slowly random walking; 2) slowly rotating by sitting on a spinning chair; and 3) moving back-and-forth in a straight line by sitting on a wheelchair trundled by a caregiver.

B. Attack Model

Multiple attackers with advanced hardware may exist with potential collusion. Following existing proximity-based authentication schemes [3], [7], [8], our authentication aims at differentiating on-body BAN devices from off-body ones. Thus, we assume attacker devices, either LOS or NLOS to legitimate OBSs and CU are deployed off-body in random locations. Distance between attacker and user could vary greatly from 1 m to tens of meters. Attacks with malicious devices placed on the user's body are not considered.

Our primary concern is impersonation attack, in which attacker devices attempt to pretend to be a legitimate OBS or CU to join the BAN, thereby launching further attacks. Attackers are aware of the deployed security mechanisms, transmission technology, and the technical specs of the sensors and CU. They are able to fabricate physical addresses, eavesdrop wireless channels, replay or inject false data, and vary transmission power. They may be knowledgeable about the surrounding wireless channel environment. Also, historical data might be used for path loss prediction of the channel between the attacker and a legitimate node. Note that we do not consider jamming and denial-of-service (DoS) attacks in this paper. CU is assumed to be not compromised. Advances in existing techniques for mobile security can be applied to safeguard CU, which are out of the scope of this paper.

C. Design Requirements

Our main design goal is to efficiently establish a shared secret key between each legitimate OBS and CU, whereas effectively differentiating valid OBSs/CU from off-body attacker nodes. Our scheme applies to scenarios such as setting up OBSs at home, in hospital, or even during moving. In addition, the proposed scheme is expected to have following properties: 1) *lightweight*: expensive operations are not involved on OBSs; 2) *usability*: the device is *plug-n-play* by common users without complicated setup and use of the BAN; 3) *fast authenticated key extraction*: applying our scheme would not put user's life at risk in emergency scenarios, i.e., authenticated keys shall be extracted with a sufficient length in a fairly short-time period; 4) *compatibility*: our scheme shall be compatible with *COTS* sensors and does not require additional hardware or changing existing system stack; and 5) *reliability*: our scheme shall work under various scenarios with desirable accuracy.

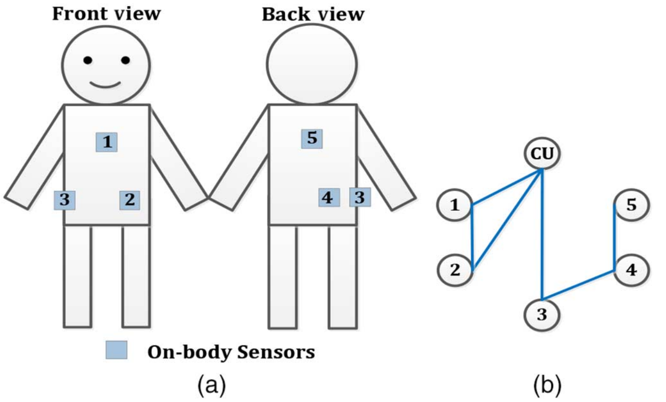

Fig. 1. (a) Sensor deployment on the body. (b) Sensor trust relationship topology.

IV. Channel Characteristics With Body Motions in BAN

To bridge the gap between fast secret key extraction and device authentication, we made some significant observations of special channel characteristics with body motions in BAN. These new findings solve the dilemma above and build the basis of our authenticated key extraction scheme. For brevity, *on-body channel* denotes the communication channel wherein both transceivers are on the same body or one of them is in close vicinity of the body (i.e., CU). *Off-body channel* denotes the channel wherein one transceiver on/near body and the other off-body at a distance away.

A. Distinct RSS Variations Among on-Body Channels With Body Motions

Shi *et al.* [9], Cotton *et al.* [21], [22], and Latré *et al.* [23] have shown that in a BAN, significant differences of RSS variation profiles exist between on-body and off-body channels with body motions. In this paper, we claim that, with body motions, channel variations among on-body channels may differ notably even if OBSs remain relatively static to each other, but the variation for all on-body channels are still more stable compared to those for off-body channels. That is, depending on different positions of OBSs and 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 amplitude and changing rate. But overall, off-body channels prominently display much larger RSS fluctuations than those of on-body channels.

1) Experimental Evidence: To validate our claim, we took on-body channel measurements in time domain with six Crossbow TelosB motes (TRP2400), which have the same hardware configuration as many COTS medical sensors. As shown in Fig. 1(a), five motes are configured as OBSs, placed on: chest (S_1), left abdominal area (S_2), right side of the waist (S_3, S_4), and upper back (S_5); one mote is carried in front by the subject as CU and close to other sensors. All the motes were fixed

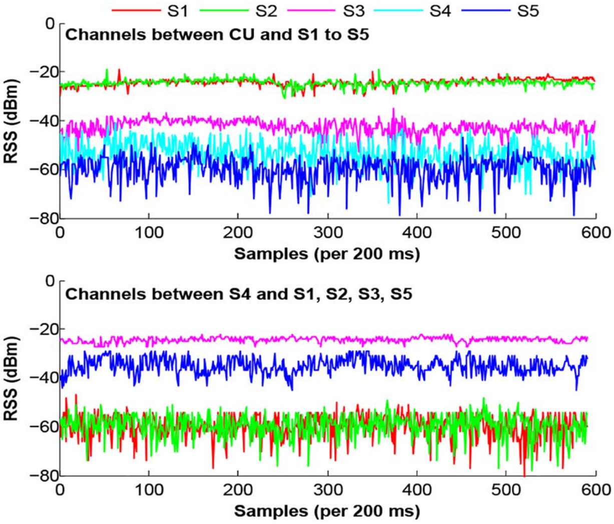

Fig. 2. RSS variations among on-body channels.

and kept relatively stationary to each other. The subject performed 1-min simple body movements suggested in Section III for each test. Different types of movement were performed in a small office, a medium office, and a large indoor corridor. RSS measurements are collected by all the devices during their round-robin message broadcasting of 200 ms, i.e., each node obtains 5 RSS measurements for every other node per second. From the RSS measurements, we observed two prominent characteristics of on-body channels while body motions are involved, as shown in Fig. 2 for one of our settings.

a) 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 CU, whereas S_4-CU and S_5-CU channels experiencing much larger RSS variations. For channels to S_4, all the nodes display highly variable RSS values except S_3 and S_5. Similar phenomenon is observed in other settings. As a close approximation to actual channel property, especially for heterogeneous devices, fluctuation of RSS values reflects channel variations.

b) Channels between LOS on-body devices tend to be much more stable than NLOS ones: For example, in Fig. 2, for channels to S_4, S_3 has much steadier RSSs than others. S_5 is somewhat more stable than S_1 and S_2. This is due to the sensor placement. S_5 is LOS to S_4, both on the back of the subject. S_3 is very close to S_4 with clear LOS. Other sensors are all on the front side of the subject.

Every sensor applies two-group classification to all the channels between it and others by their average RSS variations between consecutive measurements (ARVs). Sensors with ARV in the group of smaller ARV mean value are trusted, i.e., believed to be on the same body. In this way, a graph can be derived indicating the direct trust relationship between sensors denoted by a solid connecting line, as shown in Fig. 1(b). Note that a trust relationship between two sensors is established if and only if they trust each other. The trust relationship graph in Fig. 1(b) is based on the measurements of the same test in Fig. 2. We can see that only S_1, S_2, and S_3 are directly trusted by CU, and only S_3 and S_5 are trusted by S_4. With authentication transitivity, between any pair of OBSs, at least one multihop path of trust relationship can be found. This can be easily obtained by strategically deploying extra OBSs as "hubs" that link all OBSs and CU together. By this means, authentication range is extended to cover the whole body.

B. Theoretical Explanation

Direct path (DP) loss, multipath, shadowing, and other factors are known to contribute to radio wave propagation. The time-variant on-body propagation channels are more complicated due to effects of the human body. On different body parts, whether LOS or NLOS, received signals are further affected by body shape, human movements, device placement, and surrounding environment [24], [25]. For *LOS channels*, among different factors affecting radio propagation over on-body LOS channels, it is well understood that the DP plays a dominant role if devices are at very close range. Unsurprisingly, corresponding channel fading remains relatively stable as long as devices are kept static at their positions. For *NLOS channels*, obstructed by the device placement or body movements, fading of NLOS channels is more unpredictable. In BANs, channel fading is also affected by creeping wave diffracted from human tissue and trapped along the body surface [26]. Therefore, NLOS channels tend to be more fluctuating in terms of amplitude and rate.

V. Main Design of MASK-BAN

To reconcile the paradox of achieving effective authentication and efficient key extraction simultaneously only with wireless channel measurements, our authenticated key extraction scheme, MASK-BAN, introduces a "win–win" strategy based on the channel characteristics with body motions shown in Section IV. With the help of trusted relay sensors, multihop authentication is proposed to remarkably reduce false positive rate, especially when OBSs are sparsely distributed. Contrarily, multihop paths with larger RSS variations are exploited for fast secret key extraction between each valid OBS and CU during the authentication.

A. MASK-BAN Protocol

1) Initial Authenticated Pairwise Key Generation: For each pair of sensors, an authenticated shared secret key k_{ij} is generated between sensors S_i and S_j ($k_{ij} = k_{ji}$). Our pairwise key generation solution is derived from the adaptive secret bit generation (ASBG) technique [19], which builds secret keys from RSS measurements, and provides high key bit rate by utilizing a modified version of Mathur's quantizer [18] in conjunction with Cascade's information reconciliation [27] and privacy amplification [28]. While ASBG only uses the measured RSSs for extracting secret key bits, MASK-BAN also uses them for device authentication at the same time by evaluating ARVs for the devices as in BANA [9], i.e., based on the RSSs, each node calculates ARVs for all the other sensors and applies the two-group classification; only those in the group with a smaller ARV mean are accepted and others are rejected.

The combination of secret key extraction and device authentication is nontrivial. In particular, different from ASBG which only considers pairwise key establishment between two nodes, MASK-BAN needs to efficiently generate $n(n+1)/2$ pairwise keys among $n+1$ nodes including CU. Naive application of ASBG would result in $n(n+1)/2$ rounds of key generation, which could be unacceptably inefficient. To solve this problem, a time division duplex (TDD) method is applied in MASK-BAN in order to aggregate the communication. Specifically, within time t (where t shall be no larger than the channel coherence time) each node broadcasts in turn for an equal amount of time t_{tx}, such that within t: 1) every node has a chance to transmit and 2) each pair of nodes is measuring the same channel (i.e., their respectively measured RSSs of the channel in between shall be approximately the same) in order to extract the same key bits. This process lasts for t_0 seconds until adequate number of bits are extracted. Parameters t, t_0 and t_{tx} are chosen and broadcast by CU at the beginning of the process based on empirical results and the number of devices participating in the process. Note that every node shall report its unique identification number ID immediately after receiving the initialization message from CU.

Algorithm 1. 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 $ARV$s 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
```

However, this TDD-based approach opens the door for the attacker to impersonate as an OBS: within transmission rounds of time t each, if a device A always transmits before the attacker (who claims to be OBS and joins the authenticated key generation process), the latter is able to measure the channel between A and itself; with the knowledge of the channel and the received RSS from A, the attacker can adjust its transmission power during broadcasting to manipulate the received RSSs on A to be relatively less fluctuating (thus a small ARV) in order to pass the authentication.[1] To mitigate such attack, MASK-BAN requires devices reverse their order of broadcasting for any two consecutive time slots (each of t), i.e., if in time slot x the devices broadcast in order $\mathrm{ID}_1, \mathrm{ID}_2, \ldots, \mathrm{ID}_{n+1}$, the order will be $\mathrm{ID}_{n+1}, \mathrm{ID}_n, \ldots, \mathrm{ID}_1$ in slot $x+1$. In this way, for any device, the attacker only has the chance to measure the channel in half of the time slots. Consequently, our ARV-based authentication solution is modified such that for each device two ARVs are calculated by others, one for odd time slots $1, 3, 5, \ldots$, and the other for even time slots $2, 4, 6, \ldots$. If any one of the two ARVs fails the classification process, the corresponding device is denied.

At the end of this process, in addition to the pairwise secret keys, each node records its authentication decision to all the others for each of which it stores an entry, i.e., a tuple of $\langle \mathrm{ID}_i$, T (trust)/F (rejection)$\rangle$, in a trust relationship table.

2) Authenticated Secret Capacity Broadcast: Secret capacity (or capacity for brevity) denotes the number of bits with each pairwise secret key generated in Step (1). Each sensor S_k broadcasts a capacity message $(\mathrm{ID}_k, \mathrm{ID}_l, T/F, C_{kl})$ containing ID of the endpoints of the channel with each of its neighbors, say S_l, trust relationship learned from previous steps, and channel secret capacity C. Sensors that receive capacity messages store the messages in the buffer temporarily. Meanwhile, each of S_k's neighbors measures RSSs of the channel and calculates S_k's ARVs for later authentication. In this step, capacity broadcast shall also last for t_0 seconds, in the TDD manner with possibly repeated broadcasting, and the same technique of reversing broadcasting order as in step 1) is applied.

Every node assumes a null trusted group in the beginning. After all sensors broadcasting their own capacities and getting capacity from others, each performs two-group classification on the collected ARVs, and adds the sensors whose ARV values (for both odd and even time slots) are in the group with smaller ARV means into the trusted group. The capacity messages of trusted neighbors will be processed to add the nodes that are trusted by these neighbors into the trusted group, i.e., those with a T in the neighbors' capacity message. This process is repeated until all the other nodes with trust paths to this node are added to the trusted group. At the end of this phase, each node has the knowledge of all the channel capacity information as well as the set of trusted neighbors. An undirected weighted graph of capacity topology can be derived based on the capacity messages, with the weight of each edge representing the capacity on the channel. Algorithm 1 summarizes the process above. Since previous authentication is memoryless, MASK-BAN performs authentication along with broadcasting capacity information.

3) Deciding Maximum Entropy: In the authentication above, CU might directly accept some OBSs, but whose

[1] Note that this problem does not exist with BANA in which the transmission of each device is one-way.

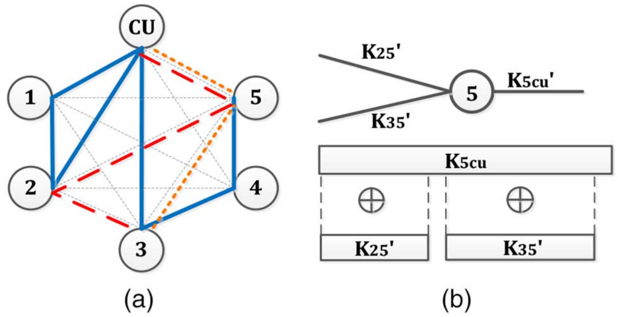

Fig. 3. (a) Max-flow path from Sensor 3 to CU. (b) Max-flow multipath merging scenario.

channels to CU are stable with low-entropy keys between. Even if the sensor is authenticated by multihop authentication, it cannot guarantee that the direct unstable channel between itself and CU has the highest entropy. Therefore, MASK-BAN finds out the maximum size of secret key, in terms of bit number, between each sensor and CU based on the channels of different capacities. As a generalization of single-source single-sink maximum-flow problem [29], each sensor runs the maximum-flow algorithm on the capacity topology to seek the path(s) through which the entropy of the key information transmitted from itself to CU can be maximized.

4) Key Aggregation Broadcast: After finding the max-flow path(s) in between, the sensor node securely exchanges its secret key(s) obtained along the path(s) to construct the final shared secret key of maximum size between itself and CU. For this purpose, each intermediate sensor on the path(s) broadcasts the XORed value of the keys shared with its previous-hop and next-hop sensors in turn. The broadcast message is accepted if and only if its sender is in the trust table. With the accepted broadcast messages and keys possessed by itself, the sensor node gets the key(s) along the path(s) by XOR operations. For example, in Fig. 3, if there is a max-flow path 3-2-5-CU between node 3 and CU, intermediate nodes 2 and 5 broadcast $k_{23} \oplus k_{25}$ and $k_{25} \oplus k_{5\mathrm{CU}}$, respectively. Note that if two keys are not of the same length, the longer one will be truncated in the XOR operation. Only knowing k_{23} with node 2, node 3 derives k_{25} from the $k_{23} \oplus k_{25}$ broadcast thereby obtaining $k_{5\mathrm{CU}}$ from $k_{25} \oplus k_{5\mathrm{CU}}$. Likewise, CU derives k_{23} and k_{25} from the broadcast messages. On this max-flow path, the key between node 3 and CU will be either k_{23} or $k_{5\mathrm{CU}}$, truncated to the same length as the shorter one of k_{23} and $k_{5\mathrm{CU}}$. If multiple max-flow paths exist between a node and CU, their final shared secret key is the concatenation of the keys from individual max-flow paths obtained as above.

Algorithm 2. 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;
```

Of particular note is the case of paths *merging* or *splitting* on the nodes. As the topology graph is undirected, *merging* and *splitting* can be treated in the same way. Assume two max-flow paths 3-2-5-CU and 3-5-CU in Fig. 3, e.g., which join at node 5. As the secret key extracted from different paths are required to be independent, overlapped bits shall not be used by the XORed value sent from node 5 for the two paths. Specifically, in $k'_{25} \oplus k'_{5\mathrm{CU}}$ and $k'_{35} \oplus k''_{5\mathrm{CU}}$ for respective paths, $k'_{5\mathrm{CU}}$ and $k''_{5\mathrm{CU}}$ shall be nonoverlapped segments of $k_{5\mathrm{CU}}$, 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 shall include the bit segment starting position of each key used by the XOR operation. That is, $k'_{5\mathrm{CU}}$ may start from bit position P_1 in $k_{5\mathrm{CU}}$ with length L_1 and k''_{5CU} with position P_2 length L_2, where $P_1 + L_1 \leq P_2$. Note that lengths are not necessary to be broadcast, because the receiving node can infer 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, e.g., $k'_{25} \oplus k'_{5\mathrm{CU}}$ is for path 3-2-5-CU. In implementation, such information can be represented by bit maps to save space. The processing method above is also applicable to 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 2 combines Steps 3) and 4).

B. Security Analysis

1) Node Authentication: Hampered by artificially simple body movements, we claim 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 OBSs. With 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 small. In practice, a user will not wear too many OBSs, implying a small value of k in real-world applications. With small kp, off-body devices actually do not get more chances to be authenticated. From another perspective, due to extra relay nodes in MASK-BAN, legitimate OBSs has more opportunities to be accepted. Therefore, multihop authentication would not result in a significant false positive rate in reality.

2) Secrecy of the Extracted Key: As attackers are off-body and their channels to OBSs are uncorrelated to on-body channels, they are not able to derive the secret key bits generated by OBSs. It is remarkable that Step 4) does not impose any requirement for RSS-based authentication. In particular, broadcasting

XORed value of its own keys or other random strings does not help the attacker obtain the keys between OBSs, nor does it reduce the entropy of the final key shared with CU. In fact, this kind of behavior only causes DoS attack, which is out of the scope of this paper. Also, we point out that broadcasting XORed values of each node dose not cause losing entropy of the key on each max-flow path between the node and CU as discussed in [20], nor does it result in losing entropy of another OBS's secret key as long as on-body channels are not correlated with off-body channels. Moreover, the secret keys between different OBSs and CU are not required to be independent since they trust each other.

3) Man-in-the-Middle (MITM) Attacks: During key generation between two devices A and B, an MITM attacker's goal is to impersonate both of the devices to each other, and establish keys shared between itself and both A and B, respectively, through actively disrupting/injecting messages. There are two possible types of MITM adversaries against our scheme, categorized by whether the attacker extracts all key bits or only parts of the key.

The first type of MITM adversary proceeds as follows. Upon receiving every ith probing message from A to B, the attacker (*M*) measures the received signal strength indicator (RSSI) from A to itself $(r_M^{\mathrm{A}}(i))$, reactively jams the packet at the same time so that B will not receive it,[2] and then sends a probing reply packet to A. *M* first sets a target RSSI value as r_t. *M* then calculates the difference $r_d = r_M^{\mathrm{A}}(i) - r_t$, and transmits the reply with power $r_0 - r_d + r_\delta(i)$, where r_0 is the default transmission power used by A and B, and $r_\delta(i), 1 \le i \le N$ is a sequence of RSSIs to induce excursions (1 or 0 bits, either above q^+ or lower than q^-, the decision thresholds which are set by *M*). The excursion RSSI sequence can be pregenerated by *M* such that the ARV of it is small, so as to pass the authentication at node A. This attack relies on channel reciprocity and manipulation of transmission power.

However, the above attack would require *M* to possess either a full-duplex transceiver or a directional antenna (which are costly), in order to measure the RSSI from A while simultaneously jam B. Moreover, our scheme can easily defend against it. First, the above attack exploits that A always send probes before B such that *M* always gets a measurement of the channel before itself sends probes to A. We can require the order of probing to change (in the case of two devices A and B, A and B can take turns to send probes first), such that half of the time *M* cannot predict the channel between A and itself. Second, in our design each device sends probes immediately after each other, so there is no time gap between them. Any attempt to jam a probing packet will be detected as that incurs a time gap that a node treats as noise.

The second type of MITM attack only extracts parts of the key bits between A/B and *M* using off-the-shelf hardware, introduced by [31]. This attack is launched by impersonating both A and B and injecting *M*'s own packets during the quantization phase, which is used by A and B as parts of their secret key. The idea is to exploit occasional opportunities, which happen when the RSSIs from both A and B to *M* are similar, upon which *M* jams packets between A and B and then inserts his reply packets to both A and B, so similar RSSIs can be expected such that a bit known by *M* will be agreed between A and B. One might think that *M* can also manipulate its transmission power of reply packets to create more stable RSSI sequences at both A and B. However, this attack requires a setup phase to correctly estimate the quantization thresholds q^+ and q^- used by A and B, during which *M* sends out probes without any prior knowledge of these thresholds. Using our scheme, the attacker's existence can be detected at this phase, because *M* has no way to correctly manipulate his transmission power without knowing the thresholds. In other words, either *M* will be detected by our ARV-based authentication scheme, or *M* will not correctly estimate the thresholds during setup if he tries to manipulate its transmission power. Moreover, the timing-based jamming detection method mentioned in the above paragraph also applies to this case.

4) Beam-Forming Attacks: Theoretically, a powerful faraway attacker might form a special beam by advanced devices (e.g., directional antenna), attempting to create relatively stable channels to OBSs to spoof the authentication algorithm. However, in BANs, we believe that it is extremely hard to implement this type of attack in practice.

First, due to many factors such as communication angle, node orientation, and link asymmetry, deploying nodes with directional antennas are different from with omnidirectional antennas. Nodes with omnidirectional antennas enjoy symmetricity in 360° without considering the factors above. But in the case of directional antennas, the antenna beam is required to continuously and precisely steer in the direction of the targeted BAN device in motion, which is very challenging. On one hand, the angle-of-arrival (AoA) of the targeted device needs to be tracked and the beam-forming algorithm be updated based on it in real time. But the attacker needs to obtain the signals sent by the targeted device to be able to compute the AoA [32]. While in our scheme, it is not always the case that the targeted device sends packets before the attacker (in fact the order of transmission among all devices should rotate periodically), such that AoA measurement is not always feasible. On the other hand, 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 OBSs is no more than 1–2 m. In most real-life scenarios, large antenna array will probably raise suspicion. For NLOS antenna arrays, such an attack becomes even more difficult since attackers can hardly direct the antennas accurately toward the patient who is randomly moving during the whole process. Furthermore, shadowing effects caused by walls and indoor obstacles will also attenuate the directed beam in a random way.

A possible countermeasure to the beam-forming attack is to equip the CU with multiantennas (now many smartphones have MIMO capability), and take the AoA measurements from all the devices into consideration as additional information in our authentication protocol. The intuition is that, since the OBSs are close to and relatively static w.r.t. CU, their AoAs should remain stable over time no matter how the body moves. However, it is difficult for an off-body attacker to maintain

[2] Previous work showed that reactive jamming is quite realistic with high-success rates [30].

the same AoA to an OBS, because not only the physical AoA changes but also the CU's antenna orientation changes, which affect the antenna gain. Implementing and evaluating this defense will be part of our future work.

C. *Discussion*

1) Node Deployment: In MASK-BAN, extra sensor nodes might be strategically deployed as "hubs," such that there are both stable (trust) path(s) and unstable path(s) between every sensor to CU. Our experiments show that this kind of placement is effective and easy-to-use. Extra nodes are not required to measure 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 MASK-BAN relies less on the strict relative positioning between CU and each BAN sensor, it relaxes the requirements on controlling body movements.

2) Scalability: The number of nodes may impact the performance since MASK-BAN utilizes TDD for message broadcast. A large number of nodes would cause a long duration for each round of TDD, thereby probably resulting in RSS measurements in difference coherence time periods for some channels. Key generation rate will also be affected due to the high error rate for inaccurate RSS measurements. 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 $\{1, 2, \ldots, k\}$, node 2 measures nodes $\{2, \ldots, k, k+1\}, \ldots,$ and node n measures nodes $\{n, 1, 2, \ldots, k-1\}$. The corresponding algorithm will not vary except that each node needs to set the capacity of nodes outside its set as 0.

3) Authentication Transitivity: Based on the observations of channel characteristics in Section IV, it is safe to apply authentication transitivity in our scheme since the probability of an attacker having stable channels to OBSs is small. During the process, OBSs and CU are moving but keeping relative static to each other to produce less channel variations. Even if the attacker follows the same movement in the same room as the user, a channel to the same extent of stability is difficult to be achieved in practice. Therefore, the assumption of authentication transitivity is valid in our scheme.

VI. Evaluation

To evaluate MASK-BAN, experiments are conducted under different settings. Various factors that may affect the performance of the scheme are considered, including room size, type of body motion, OBSs placement, and differences between subjects. The evaluation mainly focuses on effectiveness of node authentication and efficiency of secret key extraction.

A. *Experimental Setup*

Experiments were conducted on ten Crossbow TelosB motes (TRP2400): eight motes as OBSs, one as CU and one as the off-body attacker. Real-time RSSs are measured and sent by motes to the computer for analysis and simulation. We also varied the ratio of OBS number to off-body attacker number. To show the advantage of MASK-BAN, its authentication performance is compared with BANA. Three locations—a small room, a medium-sized room, and a large indoor corridor—are used in the tests. Involved subjects include two males and one female. Three body movement options suggested in Section III-A are studied: 1) walking randomly; 2) sitting-and-rotating; and 3) sitting-and-rolling, which can be easily self-performed or helped even with limited mobility. According to the usual positions of COTS OBSs in real applications, motes are placed on chest, arms, back, waist, and thighs. Note that we do not have stringent requirements on the movements. For example, subjects are allowed to walk normally rather than very slowly. Also, CU is not required to be strictly fixed. CU can either be put away from the body or be hang on the body. In addition, OBSs can be placed on both the back and the front of the body without affecting the performance of MASK-BAN, while BANA only tested the cases wherein sensors are all placed in front of the body and facing CU.

TABLE I
False Positive Rates for MMASK-BAN and BANA

	MASK-BAN (%)	BANA (%)
Small	5.36	38.98
Medium	1.35	33.92
Corridor	0	43.57
Sitting-and-rotating	2.5	30.90
Sitting-and-rolling	0	43.57
Walking	4.36	41.29
Subject 1	3.91	38.28
Subject 2	2.18	42.33
Subject 3	0	30.15
Overall	2.35	39.08

B. *Results and Evaluation*

1) Node Authentication: 33 experiments were conducted with the random combination of location, type of body movement, mote placement, and subject. RSSs are sampled every 200 ms. For some scenarios, we varied the ratio of OBSs to off-body attackers from 8:1 to 1:1. Note that in the settings of large corridor, the attacker is either static or following behind the rolling wheelchair, whereas in the settings of small room and medium room, the attacker is static inside/outside the room.

Results in Table I show that the overall false positive rate in MASK-BAN is almost 16 times less than that of BANA, reducing from 39.08% to 2.35%. Such a dramatic difference can mainly be explained by the flexible sensor placement in the experiments, in which some sensors do not have LOS channels to CU. As BANA was designed for direct LOS OBS authentication, it is not surprising that its false positive rate greatly increases due to rejection of OBSs with NLOS channels to CU. Aided by the trust relay sensors, MASK-BAN shows the advantage of authenticating sensors with NLOS channels to CU over BANA.

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

2) Authenticated Secret Key Extraction: Efficiency of MASK-BAN was validated 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 s during authentication. Based on the 30-s measurements, the final key generation rate (b/s) is calculated as the total number of generated secret key bits during this process divided by 30. In our experiments, the human movement speed is around 2 m/s, which indicates an approximate channel coherence time of 62.5 ms or so. With a total of eight OBS nodes plus the CU, we estimated that each node can transmit for no longer than 7 ms. In our experiments, we found that during each round of TDD broadcast, a transmission time (t_{tx}) of 6 ms for each mote results in a near-perfect packet delivery ratio (PDR) for up to 3 byte data payload. When t_{tx} is reduced to 4 ms, PDR dramatically decreases by up to 30% for only one byte data payload. In order to maximize the number of RSSs measured with the hope of maximizing secret key bits, we tried both 5 and 6 ms in the experiments. Note that the channel coherence time cannot be accurately calculated due to the unstable human movement speed. A shorter t_{tx} (and hence smaller t) does not necessarily result in more secret key bits though a larger number of RSSs is measured. This is because RSSs measurements for consecutive time slots could be less independent and thus, bear less entropy if t is smaller than the channel coherence time.

As mentioned in Section V-A, ASBG, adopted for pairwise key generation, is based on Mathur's quantization. For Mathur's quantization, two thresholds $q-$ and $q+$ are used such that RSS values within $[q-, q+]$ are dropped, where $q- = \text{mean} - \alpha * \text{std\_deviation}$ and $q- = \text{mean} + \alpha * \text{std\_deviation}$, $0 < \alpha < 1$. The $range$ of remained RSS values is divided into M intervals and then for each RSS value $\lfloor \frac{\text{range}}{M} \rfloor$ 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 the 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 and unstable ones, and tried to extract keys based on single channel using ASBG with varying α and M, respectively. Results show that $\alpha = 0.7$ and $M = 4$ derive best key generation rate in general as shown in Fig. 4, and we stick to these values for α and M in the rest of the experiments.

Key Generation Rate of MASK-BAN: With eight OBSs, Fig. 5 presents results of small room and corridor settings. We found that MASK-BAN is able to achieve an average secret key rate of 7.29 b/s in the corridor if $t = 6$ ms for each node. For the small room scenarios, while the corresponding rate is about 8.03 b/s with $t = 5$ ms, for $t = 6$ ms setting it is also about 8.03 b/s. To generate a 128-bit key, MASK-BAN only needs 15.9 s in small room scenarios and 17.5 s in corridor scenarios, which outperforms other BAN candidate solutions. On the other hand, if the key extraction utilizes the direct channel to CU for each node, the average bit rates are about 1.04, 0.90, and 0.94 b/s for the settings of corridor-6 ms, small room-5 ms, and small room-5 ms, respectively. This means that MASK-BAN boosts the secret bit rate about eight times than that if using direct channels to CU. Note that for $t = 5$ ms and $t = 6$ ms, the final key rate is comparable.

For comparison, we also applied the collaborative secret key generation method suggested in [20], in which all the available sensors are selected as one-hop relay nodes. That is, multiple paths, each with one relay node chosen from other nodes, are built between every sensor and CU. From the comparative results are shown in Fig. 5, it is easy to see that MASK-BAN is

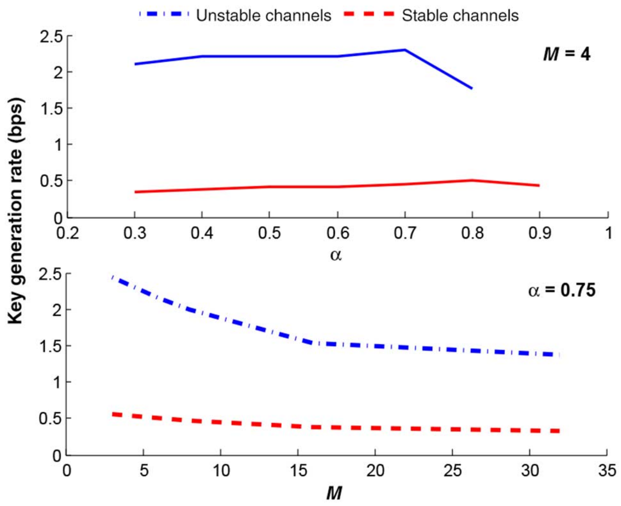

Fig. 4. Secret key rate versus quantization thresholds and intervals, based on single channel.

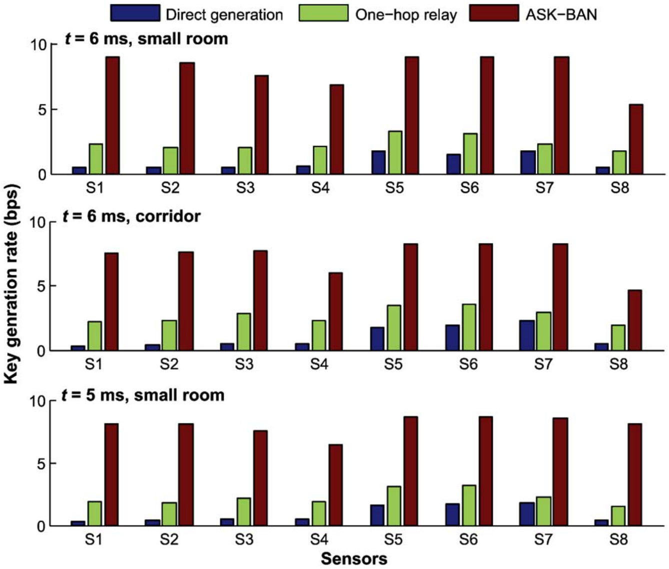

Fig. 5. Comparison of secret key rate of MASK-BAN utilizing max-flow algorithm, one-hop relay method, and direct generation.

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, MASK-BAN can achieve up to 9 b/s for a single node. To update keys over time, instead of regenerating from scratch, a complementary mechanism [33] 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 on-body channels, we evaluated the mutual information (MI) between on-body and off-body channels. Assume A and B are OBSs and C is the off-body attacker. When A is broadcasting, RSSs measured by B and C are denoted as $\mathrm{RSS}_{\mathrm{AB}}$ and $\mathrm{RSS}_{\mathrm{AC}}$, respectively. $\mathrm{RSS}_{\mathrm{BA}}$ and $\mathrm{RSS}_{\mathrm{BC}}$ represent the corresponding values by A and C, respectively, when B is broadcasting. We use MI $I(\mathrm{RSS}_{\mathrm{AB}}; \mathrm{RSS}_{\mathrm{AC}})$ and $I(\mathrm{RSS}_{\mathrm{BA}}; \mathrm{RSS}_{\mathrm{BC}})$ to estimate the channel dependencies for AB–AC and BA–BC, separately. $I(\mathrm{RSS}_{\mathrm{AB}}; \mathrm{RSS}_{\mathrm{BA}})$ is also used to estimate the dependency between channels AB and BA. We selected channels on the max-flow paths and examined their dependency values. Results show that MI 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. MI 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 in more distributed time slots.

3) Power Consumption: TelosB mote (TPR2400) integrates TI MSP430 microcontroller and a RF radio transceiver module CC2420, powered by two AA batteries. Energy consumption of the device mainly consists of that caused by code execution and that by data transmission. In MASK-BAN, data transmission happens in three stages—step 1), 2), and 4), which consume most of time spending on authenticated secret key generation. Throughout these three steps, all the nodes transmit in TDD manner with one node sending while all the rest receiving the message. Therefore, for coarse-grain estimation of the energy consumption of each node, we can amortize the total authenticated key generation time T as $\frac{T}{n+1}$ for transmission and $\frac{nT}{n+1}$ for receiving data frames. According to [34], CC2420 uses the voltages of 2.92 and 2.88 V to transmit and receive the data frames, respectively. The corresponding current consumptions are 17.4 mA (TX) and 19.7 mA (RX) [35]. To generate a 128-bit secret key, MASK-BAN needs approximately 15.9 s in small rooms and 17.5 s in corridor. Therefore, the estimated energy consumption on communication for each node are about 891.6 and 981.4 mJ in the two settings, respectively. The energy consumption on computation is approximately 85.9 and 94 mJ, respectively according to TelosB mote specification (the current draw is 1.8 mA in active mode) [36]. Therefore, the total energy consumption for small room is about 977.5 mJ and that for corridor is 1075.4 mJ or so. The capacity of an Alkaline AA battery ranges from 1700 to 3000 mAh, indicating a total energy of 18 360 000–32 400 000 mJ for a pair of AA batteries, each with voltage of 1.5 V. Therefore, we believe that the energy consumption of MASK-BAN is expected not to significantly reduce the lifetime of battery if the frequency of authenticated secret key generation is approximately configured, e.g., once per day.

VII. Conclusion

In this paper, we have proposed MASK-BAN, a lightweight authenticated secret key extraction scheme for BAN only based on wireless channel measurements. We observe that the heterogeneous channel qualities among the collection of on-body channels—those between LOS on-body devices are relatively stable, whereas those for NLOS devices are more dynamic. Utilizing this channel property, we solve the self-contradictory paradox of achieving effective node authentication and fast secret key extraction simultaneously. Our multihop authentication method greatly reduces the false positive rate compared to previous work. To maximize the secret key generation rate, a novel collaborative secret key extraction solution is given based on the max-flow algorithm. Experimental and simulation results show both authentication effectiveness and secret key extraction efficiency in MASK-BAN.

References

[1] D. Bichler, G. Stromberg, M. Huemer, and M. Löw, "Key generation based on acceleration data of shaking processes," in *Proc. 9th Int. Conf. Ubiquit. Comput.* (UbiComp'07), 2007, pp. 304–317.

[2] C. Cornelius and D. Kotz, "Recognizing whether sensors are on the same body," in *Proc. 9th Int. Conf. Pervasive Comput. (Pervasive'11)*, 2011, pp. 332–349.

[3] L. Cai, K. Zeng, H. Chen, and P. Mohapatra, "Good neighbor: Ad hoc pairing of nearby wireless devices by multiple antennas," in *Proc. Netw. Distrib. Syst. Security Symp. (NDSS'11)*, Feb. 6–9, 2011.

[4] R. Mayrohofer and H. Gellersen, "Shake well before use: Authentication based on accelerometer data," in *Proc. 5th Int. Conf. Pervasive Comput. (Pervasive'07)*, 2007, pp. 144–161.

[5] R. Mayrohofer and H. Gellersen, "Shake well before use: Intuitive and secure pairing of mobile devices," *IEEE Trans. Mobile Comput.*, vol. 8, no. 6, pp. 792–806, Jun. 2009.

[6] S. Mathur, R. Miller, A. Varshavsky, W. Trappe, and N. Mandayam, "Proximate: Proximity-based secure pairing using ambient wireless signals," in *Proc. 9th Int. Conf. Mobile Syst. Appl. Serv. (MobiSys'11)*, 2011, pp. 211–224.

[7] A. Varshavsky, A. Scannell, A. LaMarca, and E. De Lara, "Amigo: proximity-based authentication of mobile devices," in *Proc. 9th Int. Conf. Ubiquitous Comput. (UbiComp'07)*, 2007, pp. 253–270.

[8] A. Kalamandeen, A. Scannell, E. de Lara, A. Sheth, and A. LaMarca, "Ensemble: Cooperative proximity-based authentication," in *Proc. 8th Int. Conf. Mobile Syst. Appl. Serv. (MobiSys'10)*, 2010, pp. 331–344.

[9] L. Shi, M. Li, S. Yu, and J. Yuan, "BANA: Body area network authentication exploiting channel characteristics," in *Proc. 5th ACM Conf. Security Privacy Wireless Mobile Netw. (WISEC'12)*, 2012, pp. 27–38.

[10] 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, Apr. 2006.

[11] X. Hei and X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 346–350.

[12] K. Singh and V. Muthukkumarasamy, "Authenticated key establishment protocols for a home health care system," in *Proc. 3rd Int. Conf. Intell. Sens. Netw. Inf. (ISSNIP'07)*, Dec. 2007, pp. 353–358.

[13] L. Shi, J. Yuan, S. Yu, and M. Li, "Ask-ban: Authenticated secret key extraction utilizing channel characteristics for body area networks," in *Proc. 6th ACM Conf. Security Privacy Wireless Mobile Netw. (WiSec'13)*, 2013, pp. 155–166.

[14] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, "Imdguard: Securing implantable medical devices with the external wearable guardian," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1862–1870.

[15] 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.

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

[17] 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 *Proc. Int. Conf. Parallel Process. Workshops*, Oct. 2003, pp. 432–439.

[18] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, 2008, pp. 128–139.

[19] S. Jana *et al.*, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom'09)*, 2009, pp. 321–332.

[20] L. Lai, Y. Liang, and W. Du, "Phy-based cooperative key generation in wireless networks," in *Proc. 49th Annu. Allerton Conf. Commun. Control Comput. (Allerton'11)*, Sep. 2011, pp. 662–669.

[21] S. Cotton, A. McKernan, and W. Scanlon, "Received signal characteristics of outdoor body-to-body communications channels at 2.45 GHz," in *Proc. Loughborough Antennas Propag. Conf. (LAPC'11)*, Nov. 2011, pp. 1–4.

[22] 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 *Proc. 5th Eur. Conf. Antennas Propag. (EUCAP'11)*, Apr. 2011, pp. 3133–3137.

[23] B. Latré, B. Braem, I. Moerman, C. Blondia, and P. Demeester, "A survey on wireless body area networks," *Wirel. Netw.*, vol. 17, no. 1, Jan. 2011, pp. 1–18.

[24] F. Di Franco *et al.*, "On-body to on-body channel characterization," in *Proc. IEEE Sensors*, Oct. 2011, pp. 908–911.

[25] F. Di Franco *et al.*, "The effect of body shape and gender on wireless body area network on-body channels," in *Proc. IEEE Middle East Conf. Antennas Propag. (MECAP'10)*, Oct. 2010, pp. 1–3.

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

[27] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," in *Advances in Cryptology: EUROCRYPT'93*, T. Helleseth, Ed. New York, NY, USA: Springer, 1994, vol. 765.

[28] R. Impagliazzo, L. A. Levin, and M. Luby, "Pseudo-random generation from one-way functions," in *Proc. 21st Annu. ACM Symp. Theory Comput. (STOC'89)*, 1989, pp. 12–24.

[29] F. Shahrokhi and D. W. Matula, "The maximum concurrent flow problem," *J. ACM*, vol. 37, no. 2, pp. 318–334, Apr. 1990.

[30] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Short paper: Reactive jamming in wireless networks: How realistic is the threat?" in *Proc. 4th ACM Conf. Wireless Netw. Security (WiSec'11)*, 2011, pp. 47–52 [Online]. Available: http://doi.acm.org/10.1145/1998412.1998422

[31] 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'12*. New York, NY, USA: Springer, 2012, vol. 7459.

[32] J. Xiong and K. Jamieson, "Securearray: Improving wifi security with fine-grained physical-layer information," in *Proc. 19th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom'13)*, 2013, pp. 441–452 [Online]. Available: http://doi.acm.org/10.1145/2500423.2500444

[33] S. Xiao, W. Gong, and D. Towsley, "Secure wireless communication with dynamic secrets," in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[34] M. Amiri, "Measurements of energy consumption and execution time of different operations on tmote sky sensor motes," M.S. thesis, Info. Technol., Masaryk Univ., Brno, Czech Republic, 2010.

[35] Texas Instruments Incorporated. "Chipcon AS SmartRF CC2420 preliminary datasheet (rev. C)," 2013 [Online]. Available: http://www.ti.com/lit/ds/symlink/cc2420.pdf

[36] Crossbow Technol. Inc. "TelosB datasheet" [Online]. Available: http://www.willow.co.uk/TelosB_Datasheet.pdf

Lu Shi (S'11) received the B.E. degree in electrical engineering from Xidian University, Xi'an, China, in 2009, the M.S. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 2010, and is currently working toward the Ph.D. degree in computer science at the University of Arkansas at Little Rock, Little Rock, AR, USA.

Her research interests include information security, wireless network security, and cyber-physical system security.

Jiawei Yuan (S'12) received the B.S. degree from the University of Electronic Science and Technology of China, Chengdu, China, in 2011, and is currently working toward the Ph.D. degree at the University of Arkansas at Little Rock, Little Rock, AR, USA.

His research interests include cloud computing and network security, securing the data, and computation outsourced into the cloud.

Shucheng Yu (S'07–M'10) received the B.S. degree in computer science from the Nanjing University of Post and Telecommunication, Nanjing, China, the M.S. degree in computer science from Tsinghua University, Haidian, China, and the Ph.D. degree in electrical and computer engineering from the Worcester Polytechnic Institute, Worcester, MA, USA.

In 2010, he joined the Department of Computer Science, University of Arkansas at Little Rock, Little Rock, AR, USA, as an Assistant Professor. His research interests include network security and applied cryptography, secure data services in cloud computing, cross-layer security in wireless networks and embedded systems, attribute-based cryptography, and security and privacy in cyber physical systems.

Dr. Yu is a member of the ACM.

Ming Li (S'08–M'11) received the Ph.D. degree in electrical and computer engineering from the Worcester Polytechnic Institute, Worcester, MA, USA.

In 2011, he joined the Computer Science Department, Utah State University, Logan, UT, USA, as an Assistant Professor. His research interests include cyber security and wireless networks, security and privacy in cloud computing and big data, wireless security, and cyber-physical system security.

Dr. Li is a member of the ACM. He was the recipient of a National Science Foundation (NSF) CAREER Award in 2014.