Cooperative Physical Layer Secret Key Generation by Virtual Link Estimation

Chitra Javali, *Member, IEEE,* Girish Revadigar, *Member, IEEE,*
Ming Ding, *Senior Member, IEEE,* Zihuai Lin, *Senior Member, IEEE,* and Sanjay Jha, *Senior Member, IEEE*

***Abstract*—In recent years, researchers have explored using unique radio propagation characteristics between two devices for extracting symmetric keys. However, the state-of-the-art has following limitations: (i) paying more attention to only when the devices are in communication range, and (ii) considering only the devices that are mobile. Secret key generation for devices which are not in communication range and for stationary nodes is quite a challenging task. In this work, we study the feasibility of generating secret keys between two devices which do not possess any direct link with the help of a trusted relay. We propose a novel key generation protocol for unreachable nodes, and a multi-level quantization mechanism. We implement our solution using off-the-shelf commercially available resource constrained devices suitable for IoT and wireless body area networks. We conduct an extensive set of experiments in indoor environments for various scenarios involving stationary and mobile nodes. Our results reveal that an eavesdropper cannot obtain sufficient useful information about the shared keys when at least any one of the three legitimate devices is mobile. The entropy of shared keys obtained between the legitimate devices ranges from ≈0.97 to 0.98 bit, which is very close to the highest entropy of binary key.**

***Index Terms*—Secret key generation, Physical layer security, IoT, Wireless body area network.**

I. Introduction

THE ability of connecting machines to machines and machines to infrastructure has gradually evolved over the past few years and recently was given a prominent name known as pervasive networking. All the devices involved in this ecosystem sense, gather enormous amount of data, and process them into constructive actions. Furthermore, connecting all the smart devices brings people, data, and objects together. Cisco has predicted that there will be 50 billion connected devices by 2050 [1]. Pervasive networking also extends to smart wearable devices, which measure vital physiological data of a person, and forward it to the cloud based services for remote patient monitoring.

C. Javali is with The Institute for Infocomm Research (I2R), A*STAR, Singapore. E-mail: chitra_javali@i2r.a-star.edu.sg.

G. Revadigar is with Huawei International Pte. Ltd. Singapore. E-mail: girish.revadigar@huawei.com.

M. Ding is with Data61, CSIRO, Sydney, Australia E-mail: Ming.Ding@.data61.csiro.au

Z. Lin is with The School of Electrical & Information Engineering, The University of Sydney, Australia E-mail: zihuai.lin@sydney.edu.au.

S. Jha is with The School of Computer Science and Engineering, UNSW Sydney, Australia. E-mail: sanjay.jha@unsw.edu.au.

The initial version of the paper was published in Proceedings of the International Conference on Body Area Networks (BodyNets) 2015.

For future smart health-care applications, it is envisaged that the body-worn devices will be capable to seamlessly communicate with smart wireless devices embedded in the infrastructure (body-to-infrastructure), and body worn device of another person (body-to-body) for efficient acquisition of health related data. Body-to-body communication can also be exploited to save the bandwidth of the base stations in mobile networks. Secure data communication is paramount in such scenarios because (i) the medium of such communication is a wireless one, which is prone to eavesdropping, and (ii) the protocols in body-worn devices cannot be designed as sophisticated as those in base stations due to their limited capabilities. The most naive method for secure communication is to employ secret keys pre-stored in the devices by the manufacturer. However, a node is easy to be compromised in pervasive networks and this may result in key extraction by an attacker. As the devices e.g., body-worn sensors are resource constrained, it is not feasible to deploy traditional computationally complex cryptographic security mechanisms. In particular, the devices are required to exchange information securely and efficiently without security mechanisms incurring an overhead or requiring additional features. To improve security, the secret keys used by the devices must be generated and renewed dynamically.

Finding alternatives to heavy weight cryptographic algorithms for key generation has been an active research area [2], [3]. One of the approach is to extract secret keys by exploiting the unique wireless channel characteristics between two devices possessing a direct communication link [4], [5]. Secret key generation for reachable nodes in body area networks has been extensively studied in [5]–[9]. However, it is not very practical to assume that two devices always possess a direct link. For instance, if two devices, Alice and Bob intend to communicate but are not within their transmission range, then it is not feasible to extract secret keys between these two devices using existing the mechanisms, which only focus on single hop direct links. In addition, recent work [4], [10] has paid more attention to secrete key generation only when the devices are in motion. However, extracting keys when the devices are stationary is still an open problem. In order to address the above challenges, we propose a scheme to extract secret keys from spatial-temporal characteristics of wireless channel between two legitimate unreachable and/or stationary devices, with the help of an intermediate trusted node acting as a relay.

In this work, we study how accurately a source node, say Alice, can estimate the virtual/unseen channel link between an

intermediate node Relay and a destination node Bob, in order to extract secret keys from wireless channel characteristics. To be precise, Alice predicts the virtual channel link between Relay-Bob and estimates the end-to-end link characteristics between itself and Bob. Our proposed scheme has the following benefits compared to prior research: (i) secret keys can be generated even though the source and destination are not within communicating range, (ii) despite the fact that one/two transceiver(s) may be stationary, they can still generate secret keys between them with good entropy indicating sufficient randomness, and (iii) compared to the traditional scheme where a relay just acts as an information passing node, our scheme employs a smart relaying protocol, which reduces the number of time slots required and helps to achieve throughput improvement.

Our contributions in this work are as follows:

i. We propose a secret key generation scheme for the IoT devices that are not in communication range by exploiting wireless channel characteristics i.e., received signal strength (RSS).
ii. We implement our solution using off-the-shelf IoT devices and conduct extensive experiments in indoor environments to evaluate the performance of our protocol.
iii. We propose a multi-level (ML) quantization scheme to improve the key generation rate and bit agreement of the devices.
iv. We extend our proposed protocol to wireless body area networks (WBAN) and verify its feasibility for practical applications.

The rest of the chapter is organised as follows: Section II presents the related work. In Section III and IV, we provide an overview of the assumptions of our system model and preliminaries. In Section V and VI, we present our proposed secret key generation protocol, and single and multi-level bit extraction methods. The evaluation metrics, experimental set-up, performance and security analysis are presented in Section VII. The experimental set-up for wireless body area network and evaluation are explained in Section VIII, followed by concluding remarks in Section IX.

II. Related Work

In this section, we present the literature survey of secret key generation schemes and cooperative secret key generation methods for wireless devices and WBAN.

Secret key generation between two nodes: Secret key generation exploiting wireless channel characteristics [11] between two legitimate nodes has been extensively studied and was initially investigated by researchers of [12], [13]. Since then, there has been an increasing interest in the domain to study the theoretical aspects and implement in practice [4], [10], [14], [15] the above theory. The authors in [4] have proposed and constructed a system to extract channel response of 802.11 packets for key generation between two communicating parties and have also studied the performance of their proposed scheme measuring the RSS of packets exchanged between the legitimate devices. The authors in [10] have analysed deep fades of wireless channels to extract correlated secret bits between two transceivers. In [14], the researchers have proposed a key generation method exploiting channel state information in OFDM systems. Key generation has also been investigated for ultra-wide band systems [16] and narrow band spectrum such as FM signals [17]. All these work assumed that either of the legitimate devices is mobile as it is an essential factor for key generation to produce randomness in the channel.

Recently, the researchers in [5]–[7] have employed dual antennas to overcome the dependency of mobility for key generation in WBAN. SeAK [6] presents a scheme for secure pairing i.e., authentication and secret key generation simultaneously between a wearable device and a control unit in WBAN by exploiting spatial diversity of the dual antennas. The authors in iARC [7] have presented a scheme to generate keys in static channels by employing dual antenna having different characteristics such as radiation pattern and range. Artificial randomness is added to the channel by introducing a frequency hopping mechanism to increase the bit rate between the base station and the sensor device, both of which are worn on-body. Key generation performance between two devices is dependent on the mobility of device(s) and the sampling rate of the channel. In slow fading channels, if the sampling rate is increased, the bit rate will increase, however the entropy of the key will decrease. To overcome this problem, the researchers in [5], have proposed a scheme to dynamically identify the suitable samples between a base station and a body-worn device to increase the bit rate and also achieve higher key agreement.

Cooperative secret key generation: Few researchers have proposed cooperative key generation using a relay [18]–[27] to improve the key generation rate. The authors in [18] have considered secret key generation based on radio propagation characteristics, where two legitimate parties communicate through a trusted relay. This work employs physical layer methods such as amplify and forward (AF) and amplify and forward with artificial noise (AF with AN) to perform key generation through simulation. However, these schemes have the following drawbacks: (i) in the conventional AF method, an adversary is able to obtain information about the secret key from the signal transmitted by the relay, and (ii) the maximum secret key capacity achieved by simulation is 1.3 bits/time slot which is very low. The researchers in [19], [20] have investigated the usage of relays to improve the secret key generation rate for slow changing channels between the legitimate nodes. The relays act as sources of additional randomness in the channel between the legitimate nodes and the authors show through simulations that the multiplexing gain is increased by the presence of relay nodes. The authors in [21] have proposed cooperative key generation using a relay extracting phase randomness in narrow band fading channels. The paper presents theoretical upper bounds for the maximum secret key rate. In another research work [23], the authors have utilised multi-antenna for legitimate nodes and the relay to achieve higher secret key rate. The relay applies AF scheme to transmit the signals received from both the legitimate nodes. Simulation results reveal that as the number of antennas and the relays increases, the secret key rate also increases.

The authors in [28] have proposed to utilise two different channel conditions for authentication and secret key generation in WBAN. The on-body devices are authenticated when the channel is relatively static, and dynamic channels are used for secret key generation. The authors employ the max-flow algorithm presented in [29] for wireless devices that use relays, to increase the key generation rate between two on-body legitimate devices. However, in this work each of the on-body nodes need to maintain a trust table and all the nodes have to perform key processing when requested by the source and destination nodes.

Different from the above work, in this work, we propose to use a relay to generate the secret key when two nodes are not in communicating range, study the feasibility of extracting the secret keys independent of mobility and evaluate the performance using commercially available off-the-shelf devices. We believe that this work is the first to investigate the feasibility of key extraction exploiting RSS characteristics in real time environment where two nodes are communicating via a relay. We evaluate the performance of our proposed scheme with respect to two major domains i.e., IoT and WBAN. The initial version of our proposed scheme and results was presented in [30]. In this work, we extend our protocol to WBAN and also propose a multi-level quantization to improve the key generation performance in both IoT and WBAN and evaluate by conducting extensive experiments.

III. Assumptions

We assume that the two legitimate transceivers - Alice and Bob are not within communicating range. In other words, they do not possess any direct link. A trusted node acts as a Relay between the two legitimate devices[1]. All the nodes communicate in the same frequency spectrum and the multi-path fading channel is modelled as Rayleigh fading. The channel sampling time T for all the legitimate nodes for a single probe exchange is less than the channel coherence time T_{ch}. T_{ch} is defined as the time during which the channel coefficients do not change. The reciprocity of the channel holds true, i.e., the channel characteristics between Alice-Relay is identical to that of Relay-Alice and the same is valid for the channel between Bob and Relay when sampled within T_{ch}. Similar to the existing schemes in physical layer security, we assume passive eavesdropper (Eve), who cannot jam, interfere or modify the signals transmitted between the legitimate nodes. The position of Eve is more than half a wavelength (λ) of the carrier frequency being used from any of the legitimate nodes. Eve can overhear all the transmissions of the legitimate nodes and is aware of the secret key extraction algorithm. We also assume that the noise at Alice, Bob, Relay and adversaries are independent and identically distributed (i.i.d) complex Gaussian random variables with zero mean and a variance of σ^2.

[1]If we do not assume Relay as a trusted node, active attacks such as man-in-the-middle (MITM) and Byzantine attack are possible. Security against active adversaries is a separate research problem which we do not address in this work.

IV. Preliminaries

Secret key generation exploiting wireless channel characteristics consists of two phases, i.e., (a) channel sampling phase, and (b) key extraction phase. In the first phase, the legitimate parties exchange multiple probes and estimate the channel between them. Phase (b) converts the channel estimates into secret bits which will be presented in the next section.

In this section, we first provide an overview of secret bit extraction between two legitimate parties within their direct transmission, then review a traditional scheme for extracting keys with the help of a Relay when the two authenticated devices are not be able to communicate directly. In the subsequent section, we propose a scheme of extracting the secret keys with the help of Relay that has potential advantages compared to the traditional scheme.

A. Secret Key Generation Between Two Legitimate Nodes

Let us first review the basic algorithm of key generation between two devices: Alice and Bob. Alice transmits a signal x_{AB} to Bob. The received signal at Bob at time instant i is:

$$y_B(i) = h_{AB}(i)x_{AB}(i) + n_B(i). \tag{1}$$

Similarly, Bob immediately transmits a signal x_{BA} to Alice and the received signal at Alice at time instant j is:

$$y_A(j) = h_{BA}(j)x_{BA}(j) + n_A(j). \tag{2}$$

Eve overhears all the transmissions between Alice and Bob, and her received signals can be written as:

$$y_{AE}(i) = h_{AE}(i)x_{AB}(i) + n_E(i) \tag{3}$$

$$y_{BE}(j) = h_{BE}(j)x_{BA}(j) + n_E(j) \tag{4}$$

where $h_{AB}(i)$ and $h_{BA}(j)$ are the complex channel fading coefficients associated with the channels Alice-Bob and Bob-Alice respectively, whereas $h_{AE}(i)$ and $h_{BE}(j)$ are the fading coefficients between Alice-Eve and Bob-Eve. $n_B(i)$, $n_A(j)$, $n_E(i)$ and $n_E(j)$ are the complex Gaussian noise random variables. If $(j - i) < T_{ch}$, then due to channel reciprocity between Alice and Bob, $h_{BA} \approx h_{AB}$. Let $\mathbf{Y}_A = \{y_A(1), y_A(2), \ldots, y_A(m)\}$ and $\mathbf{Y}_B = \{y_B(1), y_B(2), \ldots, y_B(m)\}$ be the respectively received signals at Alice and Bob at different time instants $i = \{1, 2, \ldots m\}$. After sufficient number of samples are exchanged between the two nodes, secret bits are generated by performing the level-crossing or quantization algorithm [4].

If Eve is located at a sufficient greater distance than $\lambda/2$ from Alice and Bob, then the signals received by Eve will be uncorrelated with those of the two legitimate parties. This is due to the fact that in a Rayleigh fading model representing a rich-scattered indoor environment, the correlation between wireless channel fading coefficients decreases rapidly with distance d and follows the zeroth-order Bessel function of the first kind J_0, given by $J_0(2\pi d/\lambda)$ [31].

B. Traditional Scheme

In this scheme, for key generation between unreachable nodes Alice and Bob, the Relay acts as a packet forwarder. The time slot for the three devices is as shown in Figure 1 and

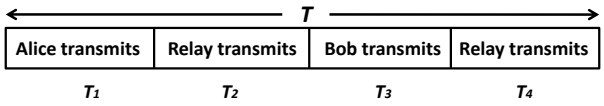


Fig. 1: Traditional scheme for secret key generation requires 4 time slots.

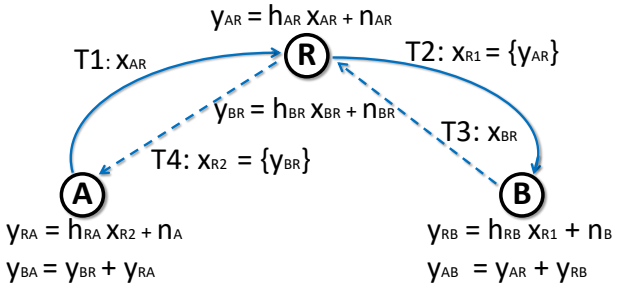


Fig. 2: Traditional scheme for secret key generation protocol.

the protocol is depicted in Figure 2. All the channel estimates are measured within T_{ch}. The received signal by Relay, when Alice transmits a known probe x_{AR} is:

$$y_{AR} = h_{AR}x_{AR} + n_{AR}. \tag{5}$$

The relay then forwards the estimated response y_{AR} in the probe x_{R1} to Bob in time slot T_2. Bob receives the signal:

$$y_{RB} = h_{RB}x_{R1} + n_B. \tag{6}$$

Bob extracts y_{AR} and computes the total channel link estimation as:

$$y_{AB} = y_{AR} + y_{RB}. \tag{7}$$

In the next time slot T_3, Bob transmits a known probe x_{BR} to Relay, so as Relay is aware of the link between itself and Bob:

$$y_{BR} = h_{BR}x_{BR} + n_{BR}. \tag{8}$$

Relay again appends y_{BR} to the probe x_{R2} being sent to Alice. In the last time slot, Alice performs the same operation as Bob in order to obtain the total link between itself and Bob:

$$y_{BA} = y_{BR} + y_{RA}. \tag{9}$$

As Eve is at a distance $> \lambda/2$, she will receive uncorrelated signals with respect to the legitimate devices, as explained in previous subsection. However, irrespective of Eve obtaining the uncorrelated signals, she can easily overhear the probes transmitted by the Relay to Alice and Bob that have the measured estimates appended in the probe. As a result, Eve can easily obtain the end-to-end link between Alice and Bob and hence also the secret key generated between the legitimate nodes. In the following section we propose our protocol which has three advantages when compared to the traditional scheme: (i) conceal the wireless channel characteristic information from the eavesdropper, (ii) increase the throughput, and (iii) extend the applicable range of the key generation scheme.

V. The Proposed Scheme

In this section, we propose our algorithm and illustrate with an example.

A. Algorithm

Alice, Bob and Relay communicate within T_{ch}. The total time T is divided into 3 time slots T_1, T_2 and T_3 during which Alice, Bob and the Relay transmit known probes respectively as shown in Figure 3. The proposed protocol is shown in Figure 4, which reduces the number of time slots from 4 (as in traditional scheme) to 3 so as to improve the throughput considerably. This increase in throughput has been well studied by researchers in [32]. Alice transmits x_{AR} to the Relay in the time slot T_1. The received signal at the Relay is:

$$y_{AR} = h_{AR}x_{AR} + n_{AR}. \tag{10}$$

In the second time slot T_2, Bob transmits x_{BR} to the Relay and the received signal at the Relay is:

$$y_{BR} = h_{BR}x_{BR} + n_{BR}. \tag{11}$$

Relay computes the value:

$$\Delta = y_{AR} - y_{BR} \tag{12}$$

and broadcasts a signal $x_R = \{\Delta\}$ i.e., value Δ appended in the probe. By obtaining Δ value, Alice and Bob estimate the end-to-end link in the following manner:
Alice receives the signal

$$y_{RA} = h_{RA}x_R + n_A \tag{13}$$

and extracts Δ value from x_R and obtains the link between Relay and Bob by:

$$y_{BR} = y_{RA} - \Delta. \tag{14}$$

Alice estimates the end-to-end channel link i.e., Alice-Bob by:

$$y_{BA} = y_{RA} + y_{BR}. \tag{15}$$

Similarly, Bob also estimates the end-to-end link by computing the following:

$$y_{RB} = h_{RB}x_R + n_B \tag{16}$$

$$y_{AR} = y_{RB} + \Delta \tag{17}$$

$$y_{AB} = y_{AR} + y_{RB}. \tag{18}$$

The received signals, $y_{BA} \approx y_{AB}$ as these are measured within T_{ch}. Alice and Bob exchange multiple samples through the Relay to estimate the virtual link between them for extracting secret bits.

The eavesdropper receives the signals transmitted by Alice and Bob respectively as:

$$y_{AE} = h_{AE}x_{AR} + n_{AE} \tag{19}$$

$$y_{BE} = h_{BE}x_{BR} + n_{BE}. \tag{20}$$

Eve is more interested in the Δ value computed by the Relay which is required to estimate the end-to-end link. The received signal by Eve when Relay transmits the packet is:

$$y_{RE} = h_{RE}x_R + n_{RE}. \tag{21}$$

Let us analyse two eavesdroppers, Eve1 and Eve2 who follow Alice and Bob's operations respectively. Both the adversaries extract the value Δ from the estimated measurement y_{RE}. Considering the scenario for Eve1, similar to Eq. (14), she

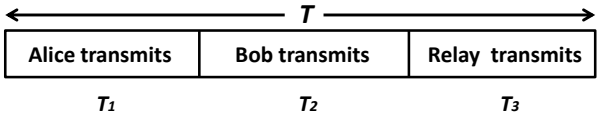


Fig. 3: Time slots allocated to three legitimate nodes in our proposed scheme.

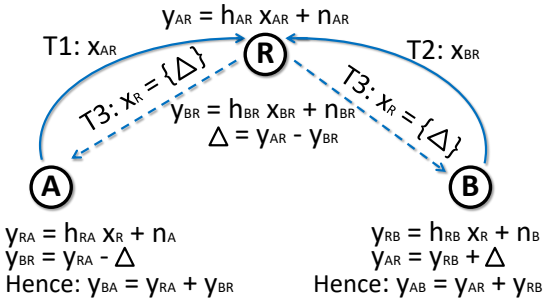


Fig. 4: Proposed protocol for secret key generation leveraging NC scheme.

subtracts Δ value from the channel estimate y_{AE} (Recall that y_{AE} is Eve1's estimated channel measurement when Alice had transmitted to Relay in time slot T_1) which yields:

$$\hat{y}_{BR} = y_{AE} - \Delta \tag{22}$$

which Eve1 assumes to be the identical channel measurement (that Alice has obtained) between Bob and Relay. It should be noted that $y_{AE} \neq y_{RA}$ as Eve1 is present at a different location than that of Alice. As explained in Section IV-A, the fading coefficients received by two receivers with respect to a transmitter are entirely independent, as the fading process decorrelates rapidly for distance $>\lambda/2$. As y_{AE} and y_{RA} are entirely different estimates, it follows that $\hat{y}_{BR} \neq y_{BR}$. In the next step Eve1 adds y_{AE} and $\hat{y}_{BR}$ (similar to Eq. (15)) which gives her a different value than that of Alice/Bob:

$$\hat{y}_{BA} = y_{AE} + \hat{y}_{BR}. \tag{23}$$

Even if we consider the case of Eve2 who follows same operations as those of Bob, Eve2 will not be able to obtain similar estimated values as Alice/Bob. The above explanation of Eve1 also holds for Eve2 as well.

B. Example

In this section, we provide a numerical example of our protocol that is illustrated in Figure 5. In the first step, Alice transmits a known probe to the Relay x_{AR}. Let the measured RSS at the Relay be $y_{AR} = 5$. In the second step, Bob transmits x_{BR} to Relay and the measured RSS of this probe by the Relay is $x_{BR} = 7$. Now, as the Relay has both the channel estimates from Alice and Bob, it evaluates Δ i.e., $y_{AR} - y_{BR} = 5 - 7 = -2$. Relay transmits the Δ value in a packet x_R to Alice and Bob, that measure the channels estimates y_{RA} and y_{RB} at their respective ends. As observed in the last step, Alice computes the virtual link between Relay and Bob as $y_{BR} = y_{RA} - \Delta = 5 - (-2) = 7$ and obtains the total

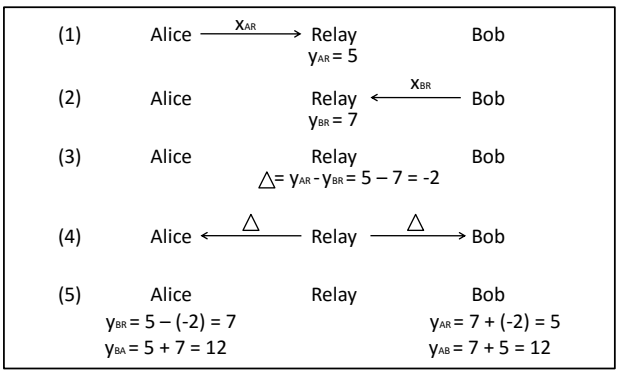


Fig. 5: Example of our proposed scheme.

link by adding Alice-Relay and Relay-Bob channel estimate. Hence Alice now achieves $y_{BA} = y_{RA} + y_{BR} = 5 + 7 = 12$. Similarly Bob also evaluates the virtual link between Relay and Alice as $y_{AR} = y_{RB} + \Delta = 7 + (-2) = 5$ to get the total link $y_{AB} = y_{AR} + y_{RB} = 5 + 7 = 12$. Thus Alice and Bob obtain a similar estimation of the link between them with the help of the Relay.

Let us analyse the channel estimates of an eavesdropper who is overhearing all the communication between the three legitimate nodes. When Alice and Bob transmit a probe x_{AR} and x_{BR} to Relay, Eve measures its channel estimate as $y_{AE} = 8$ and $y_{BE} = 4$. As explained in previous section, we know that Eve is more curious to know about the Δ value transmitted by Relay, as it is easily obtainable from the packet transmitted by the Relay. Eve measures $y_{RE} = 6$ and extracts $\Delta = -2$ from the packet x_R. Consider Eve1 who follows similar operations as Alice. Eve1 evaluates $y_{\hat{BR}} = y_{AE} - \Delta = 8 - (-2) = 10$ and obtains the total link estimate between Alice and Bob as $y_{\hat{BA}} = y_{AE} + y_{\hat{BR}} = 8 + 10 = 18$ which is an entirely different value than the one calculated by Alice. Similarly Eve2 who follows Bob's operation will not be able to get matching values as of Bob.

In real time environments, Alice and Bob will not obtain the same RSS values and there will be slight variation due to noise and multi-path fading. However, the signals measured by the two devices will be highly correlated when the packets are exchanged in the coherence time, which is a fundamental property of wireless channel. Hence, Alice and Bob can generate keys with higher agreement after quantizing the RSS values.

VI. Bit Extraction

The transmission of packets between Alice-Relay; Bob-Relay and broadcast of the packet from Relay is one channel estimation, and hence considered as one sequence. As mentioned in Section V, in the first phase of secret key generation, all the three legitimate devices (Alice, Bob and Relay) exchange a total of N number of packet sequences. Next, in the second phase, the samples collected by the legitimate devices (Alice and Bob) are passed through a moving average filter i.e., similar to a low-pass filter which results only in small scale fading variations. The samples are further converted to

bits by either single or multi-level quantization explained in the following section.

A. Single Bit Quantization

The resultant channel samples are mapped to binary bits by employing level crossing algorithm. The samples are encoded based on the following:

$$Q(x) = \begin{cases} 1 & \text{if } x > q_+^u \\ 0 & \text{if } x < q_-^u \end{cases}$$

where $q_+^u = (mean(U^m) + \alpha \times std\_dev)$ is the upper threshold, and $q_-^u = (mean(U^m)$ - $\alpha \times std\_dev)$ is lower threshold. $U^m \in \mathbf{Y}_A$ and $U^m \in \mathbf{Y}_B$ for Alice's and Bob's samples respectively. *std_dev* is the standard deviation and α is selected to control the quantizer thresholds [4]. For our experiments, we set $\alpha = 0.5$ similar to previous work [30]. The samples that occur within the thresholds are discarded and do not contribute to secret bits.

B. Multi-level (ML) Quantization

The secret key generation rate depends on the number of bits extracted per sample during quantization. A higher bit rate is desirable to reduce the time needed to generate a secret key. In the above section, a single-bit quantization method has been explained where each RSS sample contributes only one secret bit. In order to increase the bit rate (a.k.a., key rate), we propose a new multi-level (ML) quantization method. Our ML-quantization is an improved method of the bit generation scheme proposed in [33] and is equivalent to non-linear quantization that encodes the RSS samples in each non-overlapping window W of fixed size.

Following are the steps of the multi-level quantization process:

i. Consider a non-overlapping moving window of W consecutive RSS samples. For each window, calculate the range of RSS as $RSS\_Range = (Max\_RSS - Min\_RSS)$, where the terms Max_RSS and Min_RSS denote the maximum and minimum RSS values respectively.
ii. The number of bits with which each RSS sample in the window can be encoded is computed as $N = log_2(RSS\_Range)$. The range of RSS samples is then divided into $M = 2^N$ levels.
iii. We insert a 'guard space', an interval between two consecutive quantization levels to reduce the bit mismatch during key generation. Let us consider δ as the percentage of the range of RSS present in the guard space. Hence, the total guard space size, $gbsize = RSS\_Range * \delta$ where $0 \leqslant \delta \leqslant 1$.
iv. The number of guard spaces present in an M level quantization is *(M-1)*. The size of each guard space can be calculated as:

$$S_{gb} = (gbsize)/(M-1). \tag{24}$$

v. The size of each quantization level is then calculated as:

$$S_l = (RSS\_range - gbsize)/M. \tag{25}$$

vi. Each quantization level is assigned with an N-bit binary value. To convert the RSS samples to binary, each RSS sample is encoded according to the level in which it lies. For instance, for a 4-level quantization, the RSS samples in each level are encoded as per 2-bit binary coding. The samples in guard space are discarded.

C. Key Reconciliation

In the following, we state the advantages of our proposed ML-quantization over the schemes presented in [4], [33], and present a lightweight key reconciliation method. As we extract multiple bits from each sample, the bit rate improves significantly compared to the scheme in [4]. The method in [33] divides the range of RSS into multiple consecutive levels of equal size. In practical scenarios, when the two devices measure RSS values during channel sampling, the individual RSS values recorded by both the devices for the same packet index may be slightly different, which leads to the samples that are at the border of quantization levels being quantized at different levels by two devices. This results in bit disagreement and it is difficult to identify which of the bits in the string generated by the two parties are not matching. Hence, the process in [33] reduces the bit agreement between the two parties, making key reconciliation an un-avoidable step, which is an expensive step for resource constrained IoT devices [5].

On the other hand, in our method, a guard space is introduced between two consecutive quantization levels. Since the samples varying in their quantization levels will be in the guard space, they are discarded. This decreases the bit disagreement between the legitimate devices. After quantization, the samples discarded by both the parties may be same or different. For example, let the indexes of the samples discarded by Alice are {1, 5, 7, 8, 10, 12, 16, 19}, and those by Bob are {1, 2, 7, 8, 12, 13, 16, 20}. Now we can notice the indexes where the bit-mismatch occurs in the keys of Alice and Bob are: Alice = {2, 13, 20}, and Bob = {5, 10, 19}. In order to reduce the bit-disagreement, Alice and Bob exchange their list of indexes discarded during quantization and agree to use only the common indexes not discarded by both the parties for key generation. For the above example, Alice and Bob decide to discard the indexes = {1, 2, 5, 7, 8, 10, 12, 13, 16, 19, 20}. This improves the bit agreement at both sides with just one pair of packet exchange, and avoids costly reconciliation techniques [34]. It is also worth noting that, the eavesdropper capturing this information cannot obtain any useful information about the key generated by Alice and Bob. This is because, even if the eavesdropper discards the same sample indexes and generates the key by following the same method using their own RSS samples, the bits generated will be different as her RSS signal will be uncorrelated with that of the legitimate devices.

D. Key Verification

Once Alice and Bob have extracted bits from the signals either by single-bit or ML-quantization techniques, both the devices need to verify whether the keys obtained by them

matches with each other. Hence, Alice creates a message *msg* concatenating with the generated secret key k and calculates the hash i.e., $h(msg + k)$. For hash algorithm, we employ SHA-256. Alice then appends the *msg* to $h(msg + k)$ and sends $(msg, h(msg + k))$ to Bob. Bob extracts the *msg* and calculates the hash of the message with his own key k' and checks whether the evaluated hash message is equal to the one sent by Alice. If both the hash messages are same then Bob concludes that the $k' = k$. Bob sends a response message $(resp\_msg, h(resp\_msg, k'))$ so that Alice can confirm Bob's derived key. Later, Alice and Bob can perform privacy amplification [35] by using methods like universal hash functions or XOR operations.

VII. Evaluation

A. Evaluation Metrics

Once we have the binary strings of the secret bits, we quantify the bits extracted by the legitimate devices by the following four metrics:

(i) *Entropy* - The randomness of the generated secret bits is evaluated by entropy, and is measured in bits. The higher the randomness, more is the entropy of the key. The keys need to possess sufficient entropy to prevent it from being predicated by an attacker. The entropy value ranges from 0 to 1 for binary strings.

(ii) *Bit agreement* - It is defined as the ratio of number of matching bits of the keys at the two parties to the key length. This metric should be high with regard to the device pair of Alice and Bob.

(iii) *Secret bit rate* - It is the number of shared secret bits generated per unit time and is measured in bps.

(iv) *Mutual Information (MI)* - MI(Alice:Bob) quantifies how much information does Bob's secret bits reveal about Alice's secret bits. MI is measured in bits and its value is 0 when two extracted secret bit strings are statistically independent. More the MI between Alice and Bob, there is less uncertainty in Alice knowing about Bob's secret bits or Bob knowing about Alice's secret bits.

B. Experimental Set-up

In our experimental set-up, all the devices communicate in the same channel and frequency space of 2.4 GHz. We implemented the proposed protocol on Iris motes having RF230 radio in TinyOS environment. The floor plan of an indoor environment and experimental set-up are as shown in Figure 6. It was conducted in a lab where there were people sitting at their cubicles and moving around. The two eavesdroppers, Eve1 and Eve2 were placed at a distance of 0.1 m each, on either side of the Relay. The adversaries are very curious to obtain RSS values from the legitimate devices, hence we have placed Eve1 and Eve2 close to Relay, as it is the only legitimate device that receives the RSS signals from Alice and Bob. In addition, in our experimental set-up rather than the eves following only one part of evaluation either Alice or Bob, for additional security analysis we have two eves following the protocol evaluation by both Alice and Bob separately, i.e., Eve1 follows Alice's operation whereas

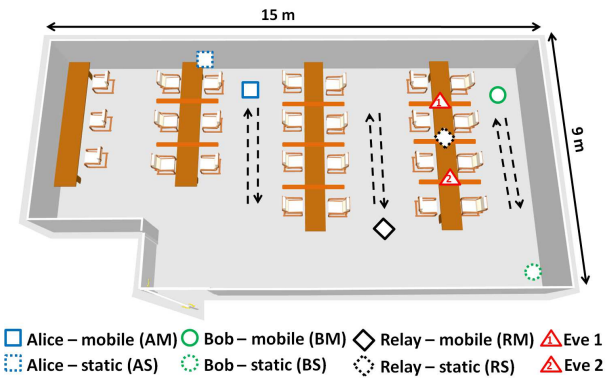


Fig. 6: Floor plan of experimental set-up in an indoor environment.

TABLE I: Various experimental scenarios with nodes as mobile and stationary

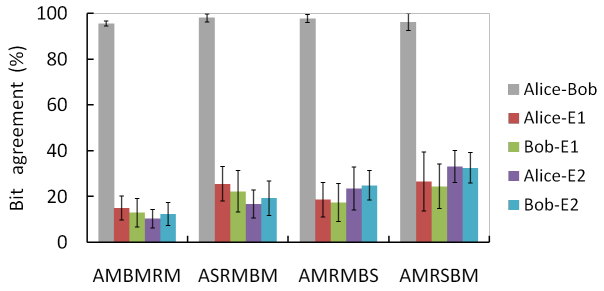
Expt	Stationary			Mobile		
	Alice	Relay	Bob	Alice	Relay	Bob
AMRMBM	·	·	·	✓	✓	✓
ASRMBM	✓	·	·	·	✓	✓
AMRMBS	·	·	✓	✓	✓	·
AMRSBM	·	✓	·	✓	·	✓
ASRSBM	✓	✓	·	·	·	✓
AMRSBS	·	✓	✓	✓	·	·
ASRMBS	✓	·	✓	·	✓	·
ASRSBS	✓	✓	✓	·	·	·

Eve2 follows Bob's evaluation to obtain the secret keys. We validated our protocol for several scenarios i.e., when all the legitimate nodes are stationary, or either one/two of them is/are stationary, and also when all are mobile as shown in Table I. Each mobile and stationary scenario were repeated 15 times and each experiment was conducted for 5-10 minutes.

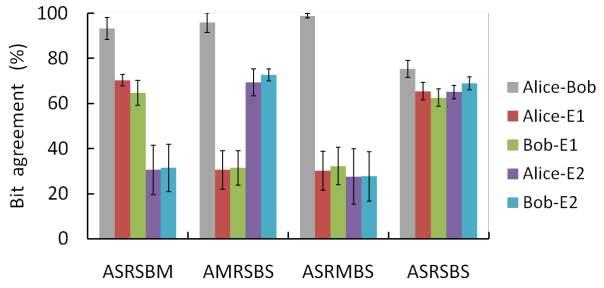
In each of the mobility based scenarios, the subject(s) holding the devices was/were moving at a speed of 0.5 m/s back and forth. The rate at which the channel varies can be represented by the maximum Doppler frequency (f_d). In an indoor environment, for the carrier frequency 2.4 GHz; $f_d = v/\lambda = (0.5 \times 2.4 \times 10^9)/(3 \times 10^8) = 4$ Hz, which gives $T_{ch} = 250$ ms. The transmission of packets for one round of channel estimation i.e., Alice-Relay; Bob-Relay and broadcast of the packet from Relay to Alice and Bob, was performed within T_{ch}.

Another important part in our protocol is synchronisation of the legitimate devices. As Relay being the node which is in communication range with Alice and Bob, it initially sends a *START* packet to both the devices indicating the time slots during which each of the devices need to transmit their packets. Time slot available for each of the legitimate devices spans to a maximum of 20 ms.

First let us analyse the performance of our scheme between the two legitimate devices Alice and Bob in all experimental scenarios.



(a) Bit agreeement when two/three nodes are mobile.



(b) Bit agreeement when two/three nodes are stationary.

Fig. 8: Bit agreement of all the devices for various scenarios.

C. Performance Analysis of Alice-Bob Key Generation

In this section, we analyse the performance of our protocol considering single-bit quantization.

1) All nodes are mobile - AMRMBM: In this scenario, we have all the three nodes Alice (A), Bob (B) and Relay (R) moving back and forth as shown in Figure 6. Here the two channels A-R and R-B vary randomly. As observed from Figure 7a, the RSSI values estimated by Alice and Bob for the end-to-end link have high amount of variation, i.e., about 20 dBm. Due to the reciprocity property of wireless channels, the two end devices indicate high correlation in the estimated links. Mobility of the nodes also adds more randomness to the samples measured, which helps to achieve keys with a high entropy. From Figure 8a, we observe that the bit agreement is about 95%-97% between Alice and Bob.

2) One node is stationary - ASRMBM, AMRMBS, AMRSBM: For the case of ASRMBM, which features Alice as stationary and Relay and Bob mobile, the channel R-B varies randomly (due to the mobility of Relay and Bob). The channel A-R also has varying RSSI values due to the movement of the Relay. The same explanation also applies to the other two scenarios AMRMBS and AMRSBM of having two mobile channel links. Though this scenario has one of the nodes as stationary, we observed that the entropy of the keys is as good as the scenario when all nodes are mobile. The bit agreement between Alice and Bob is about 96%–99% for all the 3 scenarios in this case as observed from Figure 8a.

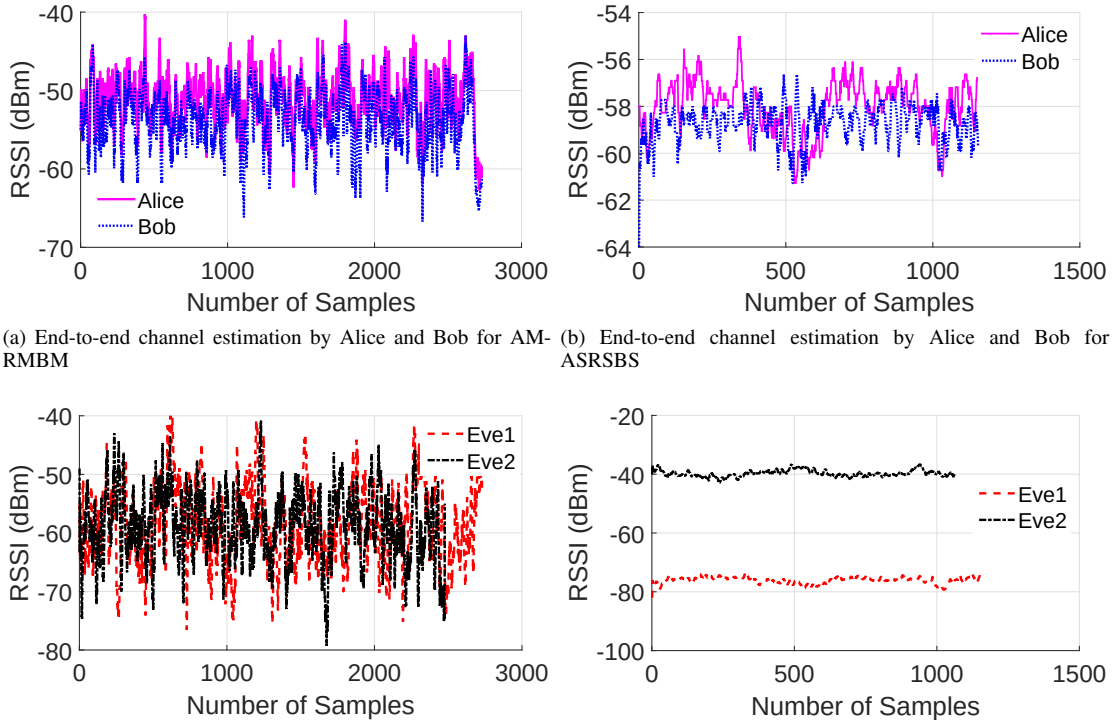
3) Two nodes are stationary - ASRSBM, AMRSBS, ASRMBS: Let us consider the case of ASRSBM. Here, as Alice and Relay are stationary, the channel between them has a minimal amount of variation, whereas since Bob is mobile, the channel link between R-B has higher fluctuation. Figure 9a shows Alice's observations of the channel A-R. As Alice and Relay are static, we observe that RSSI variation is only about 1-2 dBm from the mean value. In contrast, from Figure 9b we can observe that due to the movement of Bob, the estimated channel by Alice between R-B varies from -78 dBm to -64 dBm. Alice and Bob evaluate the end-to-end link between them, the net result is the corresponding sum of the RSS measurements of A-R and R-B. Figure 9c shows that the end-to-end variation is from -135 dBm to -148 dBm for Alice, which shows the channel changes fast enough to extract secret keys. The same explanation holds good for AMRSBS. In case of ASRMBS, two nodes Alice and Bob are stationary and Relay is mobile, it has two varying channel links because of the movement of the Relay in between the two nodes. This makes guessing the secret key difficult for the adversaries. Bit agreement is about 93%, 95% and 98% for ASRSBM, AMRSBS and ASRMBS respectively as can be seen in Figure 8b.

TABLE II: Mutual information (in bits) for various experimental scenarios.

Expt.	MI(A:B)	MI(A:E1)	MI(B:E1)	MI(A:E2)	MI(B:E2)
AMRMBM	0.8798	0.0233	0.0211	0.0143	0.0333
ASRMBM	0.7831	0.0625	0.0522	0.0416	0.0619
AMRMBS	0.8331	0.0818	0.0717	0.0523	0.0624
AMRSBM	0.8659	0.0851	0.0866	0.0569	0.0430
ASRSBM	0.7665	0.5601	0.5265	0.2318	0.2076
AMRSBS	0.7516	0.2518	0.2952	0.5931	0.6052
ASRMBS	0.7239	0.1012	0.0918	0.1100	0.0822
ASRSBS	0.6899	0.5999	0.5554	0.5988	0.6031

4) All nodes are static - ASRSBS: From Figure 7b, we notice that the channel estimations between Alice and Bob are not highly correlated and the RSSI values vary with very minimal deviation which is about 2-3 dBm. This minimum degree of variation produces secret key bits with a low entropy [36]. In this case, the bit agreement on an average is only 76% as observed from Figure 8b due to the fact that in static scenarios, uncorrelated noise component at the two ends and multi-path effects will have strong influence on the signal variation [31]. Most of the bits are discarded as they do not contribute to the randomness of the channel which reduces the bit rate.

We have evaluated the randomness of the bits generated in all experiments by calculating entropy of the keys. Our results reveal that, when all the nodes are stationary the entropy is 0.45 bits, whereas for all other scenarios with at-least one node as mobile, the entropy ranges from 0.8965 to 0.9810 bits (The highest entropy for binary key is 1 bits). Additionally, we also perform the NIST [37] entropy test that verifies the randomness of a given bit string. The test result outputs a p-value which can be used to verify the outcome. The p-value >0.01 indicates that the corresponding test was passed, while p-value <0.01 indicates that the test was failed. The keys generated by our scheme in all cases pass NIST entropy test. Note that the net RSSI measured at either end of the devices may not be valid RSS values, as different radios have specific range of RSSI. For example, RSSI ranges from -91 dBm to -10 dBm for RF230 radio and for CC2420 it varies from



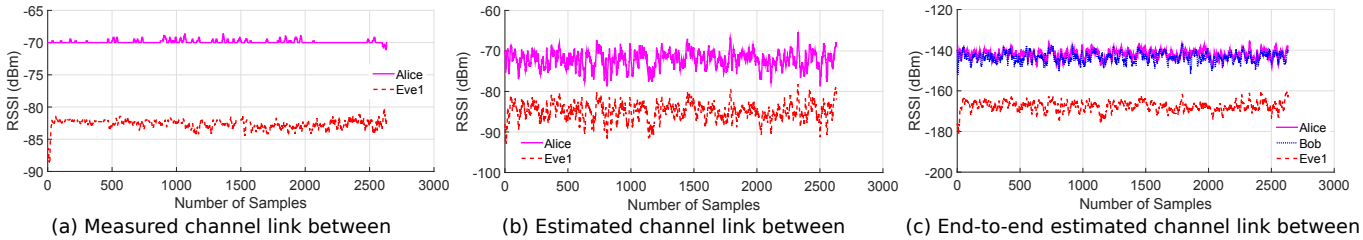
(a) End-to-end channel estimation by Alice and Bob for AMRMBM

(b) End-to-end channel estimation by Alice and Bob for ASRSBS

(c) End-to-end channel estimation by E1 and E2 for AMRMBM

(d) End-to-end channel estimation by E1 and E2 for ASRSBS

Fig. 7: The channel estimations of Alice and Bob have high correlation. The eavesdropper's (E1 and E2) channel estimations vary from those of legitimate nodes.



(a) Measured channel link between Alice - Relay

(b) Estimated channel link between Relay - Bob

(c) End-to-end estimated channel link between Alice - Bob

Fig. 9: Channel estimation by Alice and Eve1 when two of the legitimate nodes i.e., Alice and Relay are stationary: ASRSBM.

-100 dBm to 0 dBm. In our scheme the main goal is that the two devices which do not communicate directly must come to a common key agreement with the help of a relay by estimating the virtual channel link at the other side. Table II shows the MI between all the devices in various experimental scenarios. We can see that the MI between Alice and Bob is from 0.8798 to 0.689 bits. The MI is lowest when all legitimate nodes are stationary i.e., for the case ASRSBS and it is nearly same as that of eavesdropper. The channel variations of Alice and Bob vary over a very minimal range (2 - 3 dBm) due to non-movement of the nodes. An example of RSS variation of this scenario can be observed in Figure 7b. The eavesdropper measuring the RSS samples from the legitimate devices also had minimum variation of RSS values, due to which the MI of the adversary with the legitimate devices is similar to that of the MI of Alice and Bob. For better security, we recommend generating the keys when at least one of the devices are in motion This can be achieved by detecting sufficient variation in RSS using a threshold based method employed in [5]. We evaluated the bit rate and observed that, on an average it varies from 24.32 bps to 18.8 bps for the cases which have at least one channel link as mobile. The bit rate reduces by 60%–70% for all static channels (ASRSBS).

We have analysed the energy consumption of our proposed protocol. Figure 10 shows the set-up for energy consumption analysis. The sensor board was supplied with an external source of battery V_{bat} = 3 V. A resistor R = 10 Ω was connected in series with the board. The current drawn by the sensor mote when idle was 8.7 mA and increased to 12.32 mA when performing the key generation operation. The total energy consumed was 0.727 mJ.

D. Performance Analysis for ML-quantization

In this section, we present the secret bit rate and bit agreement analysis considering our ML-quantization for key generation. Recall that the first step in ML-quantization is to determine the number of bits to be assigned per sample, that

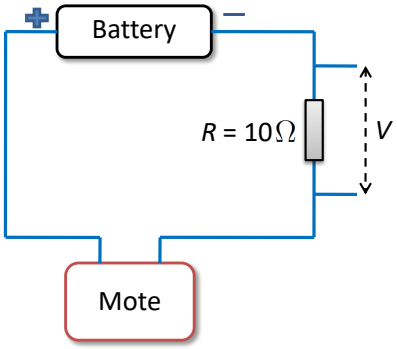


Fig. 10: Energy consumption analysis set-up.

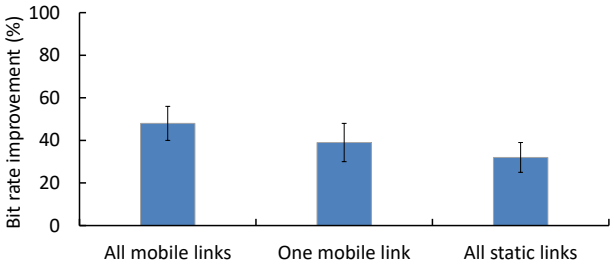
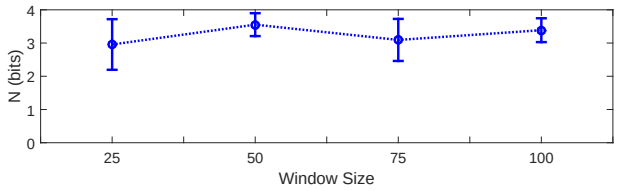


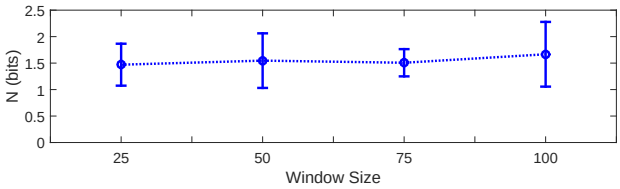
Fig. 11: Bit rate improvement of ML-quantization over single bit quantization.

is calculated by the method explained in Section VI-B. We estimate N for different cases, viz., (i) when all the nodes are mobile, (ii) two nodes are mobile, (iii) one node is mobile, and (iv) all nodes are static, for various sizes of window W. Figure 12a and 12b show N estimated for all mobile and all static nodes scenarios respectively, considering W as 25, 50, 75 and 100 samples. It can be noticed that, for the case of all mobile nodes, the links between Alice to Relay and Relay to Bob vary sufficiently, and hence, the observed RSS fluctuation results in $N > 3$ for all values of W. Similarly, for static nodes, the N estimated for different W is $\approx$ 1–2 bits.

Based on our experimental results, we fix the number of bits in the quantization N as follows; $N = 3$ for all mobile nodes, $N = 2$ for two nodes mobile, and one node mobile scenarios, and $N = 1$ for all static nodes. Based on the number of bits fixed as above and considering $W = 50$ samples and $\delta = 0.2$, we calculate the maximum bit rate for different cases. Our results show that, the bit rate when all channel links are mobile is 30–36 bps, where as for one mobile link scenarios, the bit rate is 22–26 bps. For the case of all static channel link, the bit rate observed is $\approx$ 10–12 bps. Figure 11 shows the bit rate improvement of ML-quantization over single- bit quantization. As observed from the figure, the bit rate improvement is the highest for the case of all mobile channel links as the RSS has more randomness when compared to the static channels. The bit agreement obtained between the legitimate devices for the scenario of mobile nodes was 92%-93%. The agreement when two or only one node as mobile was 88%-90%. The bit agreement for stationary case remains the same as only single bit quantization was employed for bit extraction from the analysis as explained in the previous paragraph. We observe



(a) When all the nodes are mobile



(b) When all the nodes are static

Fig. 12: Estimation of maximum number of bits N during quantization for different W.

that the agreement for the ML-quantization is lower than the single bit quantization for the cases when at least one node is mobile, due to the fact that if the quantization of single sample varies then there is a difference of two or three bits which results in higher bit disagreement. Hence, if the number of bits are increased for quantization the bit disagreement between the legitimate devices increases.

E. Security Analysis

The two eavesdroppers Eve1 and Eve2 capture packets from all the 3 nodes, and are very curious about the packets transmitted by the Relay, as Relay is the device which receives packets from both Alice and Bob, subtracts the two received RSSI and then appends the value Δ in the probe to broadcast.

1) All nodes are mobile - AMRMBM: As all the nodes are mobile, due to the inherent property of unique spatio-temporal characteristics, both eavesdroppers receive uncorrelated samples with respect to the legitimate devices. The RSSI samples of Eve1 and Eve2 vary in a different pattern than those of Alice and Bob as observed from Figure 7a and 7c. The bit agreement of Eve1 and Eve2 ranges from 10% to 20% w.r.t Alice/Bob as seen from Figure 8a. From Table II, the MI observed for Eve1 and Eve2 is too low compared to Alice and Bob, which indicates that not much useful secret key bit information can be obtained when all nodes are mobile.

2) One node is stationary - ASRMBM, AMRMBS, AMRSBM: As this scenario has two varying channel links, it is not feasible for either Eve1 or Eve2 to obtain similar set of RSSI as those of legitimate devices. All the cases in this scenarios see eavesdropper's bit agreement of only 12%-39% with Alice/Bob as shown in Fig. 8a. The MI is < 0.1 bits for Eve1 and Eve2 with Alice and Bob as observed from Table II. This scenario is as good as having all the nodes as mobile.

3) Two nodes are stationary - ASRSBM, AMRSBS, ASRMBS: We shall divide this case into two different scenarios: (i) ASRSBM, AMRSBS and (ii) ASRMBS. Let us consider (i) ASRSBM, we know that as it has only one node as mobile, it leads to only one mobile link and one stationary

link. The channel estimation by Eve1 for the link A-R and R-B is as shown in the Figure 9a and 9b respectively. As the channel A-R does not have large random changes, Eve1 can easily predict the channel link from A-B. We observe from Figure 8b, that the bit agreement of Eve1 with Alice/Bob when the channel A-R varies minimally is about 58%-70%, whereas Eve2 following Bob's operation cannot exactly predict the secret bits. Hence the bit agreement of Eve2 with that of Alice/Bob drops to about 30%. Similarly for AMRSBS scenario, Bob is stationary which is an advantage for Eve2 and she can predict the extracted keys by about 65% to 70%. From Table II the MI is also high for Eve1 with Alice/Bob for ASRSBM scenario and Eve2 for AMRSBS. In (ii) ASRMBS experimental scenario there are two mobile channel links, thus both the eavesdroppers have low key agreement and MI with the legitimate devices.

4) All nodes are static - ASRSBS: Comparing Figure 7b and 7d, we observe that the correlation of eavesdroppers is less than that of Alice and Bob. Though Alice and Bob are stationary, adversaries RSSI values differ as they are located at a distance greater than $\lambda/2$ [4]. Bit agreement of Eve1 and Eve2 with Alice and Bob ranges between 58%-68%. By observing Table II, it can be noticed that Eve1 and Eve2 though individually might have MI less than Alice/Bob, their combined MI can reveal more information about the keys between Alice-Bob compared to other scenarios. In such cases, privacy amplification mechanisms [35] can be employed to strengthen the keys between Alice-Bob.

VIII. Virtual Link Estimation for WBAN

In this section, we present the virtual link estimation algorithm for wireless body area network (WBAN). A WBAN consists of a number of on-body sensors that sense the physiological data and communicate to a co-ordinator or control unit for data aggregation and processing. This control unit may be further connected to cloud services for remote health-care patient monitoring. In WBAN, the communication mode between the non-line-of-sight (NLOS) nodes is multi-hop communication rather than single hop. The researchers in [38] have studied that the path loss in WBAN is much higher than free space communication due to absorption of RF waves by the human body. Additionally, if strong RF waves are employed for NLOS, then it may damage the human tissue. The authors have analysed the performance of multi-hop communications in WBAN and reveal that it is the most reliable form of communications. In the following sections, we explain the experimental set-up for WBAN and the results.

A. Experimental Set-up

The Iris motes acting as Alice, Bob and Relay were placed on-body of a subject. To validate the feasibility of our protocol the experiments were conducted by placing the sensor nodes at different positions on the subject. Figure 13 shows the experimental set-up of the sensor motes on body for different cases: Case (i) Alice was placed on arm, Relay on waist and Bob on the knee, Case (ii) Alice was placed at the back whereas positions of Relay and Bob remained the same and Case (iii) Alice was placed at the back of chest, Relay was held in hand and Bob at the ankle and Case (iv) Alice was placed at the back, and Relay on the chest, and Bob on the waist. We have considered all practical situations that include a combination of LOS and NLOS which correspond to the different set-ups of IoT experiments explained in VII-B. The main goal here is to study the feasibility of our proposed protocol for multi-hop secret key generation in WBAN. Figure 14 shows the floor plan used for WBAN experiments. Similar to the previous research papers [19], [28] we consider the presence of off-body eavesdroppers. The subject was walking at a speed of 1 m/sec. Both the eavesdroppers were overhearing the communication between the legitimate devices. The algorithm was followed as explained in Section V.

B. Results

In this section, we analyse the performance of key generation by considering the single bit quantization.

1) Entropy: We evaluated the randomness of the generated bits by the legitimate devices. The approximate entropy for all the four cases of on-body experiments is explained in the following:

(i) In the first case, during walking, both the arm and the knee of a person have sufficient movement, hence both the links Alice–Relay and Bob–Relay show randomness. Thus the keys generated have a high entropy ≈0.97–0.98 bits.
(ii) In the second case, the link between Alice–Relay has less randomness compared to the other links during walking, as the device placed on the chest does not experience much movement. This case is equivalent to the one explained in Section VII-C3 where two nodes are stationary. Hence the entropy obtained in this case is lower than that of first case, i.e., 0.72-0.80 bits.
(iii) The third case has two mobile links, thus the entropy obtained also ranges from 0.962 to 0.986 bits.
(iv) In the fourth case, all the three nodes do not have sufficient movement during walking and the entropy obtained is ≈0.52 bits.

2) Bit agreement: Figure 15 shows the bit agreement for all the cases. The bit agreement for the on-body set-up was similar for the cases of (i) and (iii), as both these scenarios have two mobile links when a person is walking. The achievable bit agreement was 93% to 98%. In case of set-up (ii), the bit agreement ranges from 93% to 95%. For the scenario (iv), the bit agreement ranges from 78% to 80% though all the devices were nearby and placed on the chest. This result is similar to the scenario when all nodes are stationary in Section VII-C4.

3) Secret bit rate: We observed that, for the first case, the two links i.e., Alice to Relay and Relay to Bob showed sufficient variation and hence, the bit rate measured was 22.6–25.8 bps. For the cases (ii) and (iii), as there was only one link varying, the bit rate was about 16–18.24 bps. For the fourth case, as none of the links had enough variation, the only change in the link strength was due to the effects of multi-path propagation in indoor environments when the

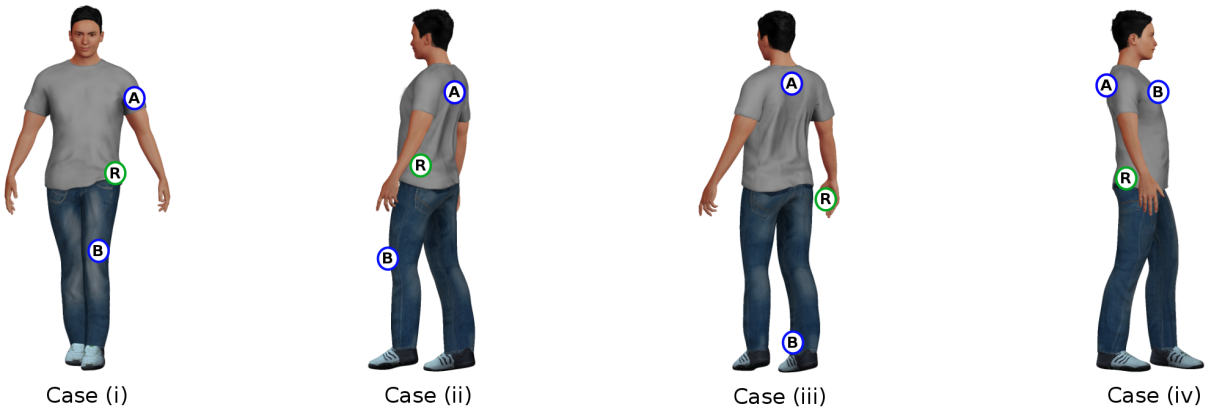


Fig. 13: The legitimate nodes worn on-body by a subject for all the four different cases. A-Alice, R-Relay and B-Bob.

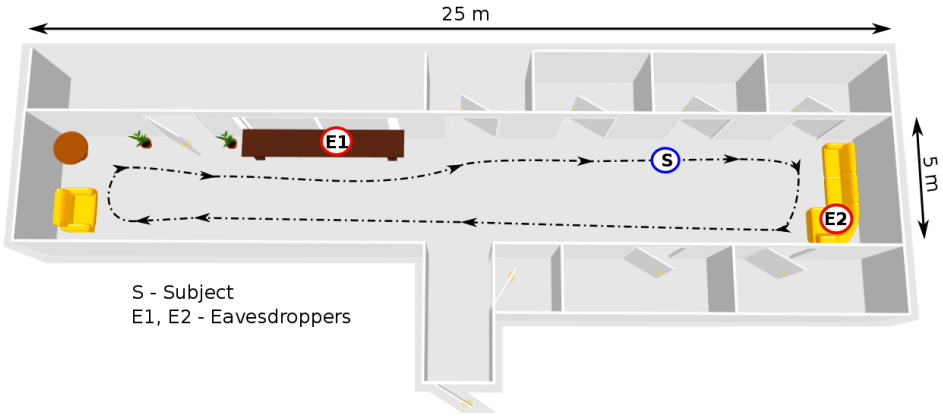


Fig. 14: Floor plan of experimental set-up in an indoor environment for WBAN.

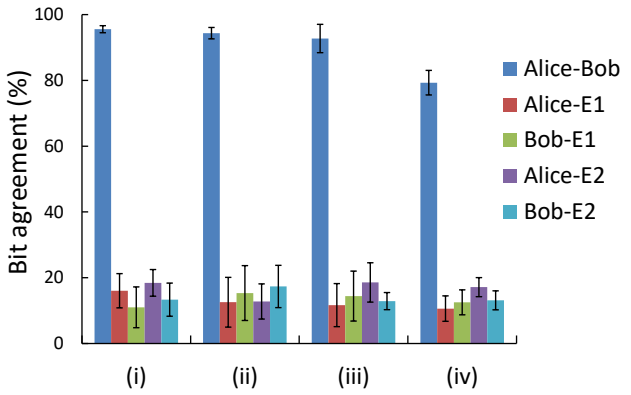


Fig. 15: Bit agreement of all the devices in WBAN for various scenarios shown in Figure 13.

subject was walking, the bit rate observed was about 9.7-11.5 bps, which is low compared to all other cases.

4) Mutual information (MI): Table III shows the MI obtained between the legitimate devices and the eavesdroppers. The MI between Alice and Bob in cases (i)–(iii) is greater than 0.8 bits as they either have one link or both the links are mobile. Case (iv) has MI comparatively lower than the rest as for nodes which do not have much movement, the noise component is more dominant. We can notice that the eavesdropper's MI is very less compared to MI of Alice and Bob. Hence, neither E1 nor E2 can obtain useful information about the keys generated by the legitimate devices.

C. Performance Analysis Using ML-quantization

In this section, we analyse the performance of proposed scheme for WBAN by employing our ML-quantization for key generation. We set the quantization parameters as $W = 50$ and $\delta = 0.2$. We conducted a similar analysis as explained in Section VII-D to find the upper bound on the number of bits N assigned during quantization. Our results revealed that the values of N estimated for off-body IoT and WBAN experiments with different W values were in the same range for similar type of experimental set-up. Specifically, for the experiment case (i) in WBAN, the estimated N value was in the range 2 to 3.5. Thus we set $N = 3$ for this case. Similarly using the experimental results, we set N for other scenarios as well, i.e., $N = 2$ for the case (ii) and (iii), and $N = 1$ for case (iv). Considering these upper limits, the bit rate achieved in WBAN cases (i) to (iv) is 33–42 bps, 24–30 bps, and 11–14 bps respectively. The bit agreement achieved were similar to the results obtained for IoT scenarios i.e., we observed that the bit agreement decreased when we employed ML-quantization scheme.

TABLE III: MI (in bits) between legitimate devices and eavesdroppers

Different cases	MI(A:B)	MI(A,B:E1,E2)
Case (i)	0.898	0.23
Case (ii)	0.823	0.20
Case (iii)	0.8869	0.301
Case (iv)	0.789	0.28

IX. Conclusion

We have proposed and implemented a physical layer based secret key generation protocol for wireless nodes which are not in their direct transmission. Our protocol employs a trusted relay between two unreachable legitimate devices and can generate secret keys with good entropy even when one or two of the three devices are stationary. We have implemented the proposed protocol on devices with small form factor applicable for health-care applications and conducted an extensive set of experiments to evaluate the performance. The experimental evaluation results for both the investigated IoT and WABN scenarios are similar. Our results reveal that we can achieve a bit agreement of about 95%-99% when at-least one of the three nodes is mobile. The MI of the legitimate devices ranges from 0.8798 to 0.689 bits, which is comparatively higher than the MI measured by the adversaries. For both IoT and WBAN applications, the ML-quantization mechanism gives a higher secret bit rate compared to the single bit quantization method.

Acknowledgment

This work is partially supported by Australian Research Council Discovery grant DP150100564.

References

[1] "Cisco: The Internet of Things," Whitepaper April 2011.

[2] C. Javali and G. Revadigar, "Birds of a Feather Flock Together: Fuzzy Extractor and Gait-Based Robust Group Secret Key Generation for Smart Wearables," in *Proc. EAI International Conference on Security and Privacy in Communication Networks (SecureComm)*, 2018.

[3] G. Revadigar, C. Javali, W. Xu, A. V. Vasilakos, W. Hu, and S. Jha, "Accelerometer and Fuzzy Vault-Based Secure Group Key Generation and Sharing Protocol for Smart Wearables," *IEEE Transactions on Information Forensics and Security (TIFS)*, vol. 12, no. 10, pp. 2467–2482, 2017.

[4] 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 ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2008.

[5] G. Revadigar, C. Javali, W. Hu, and S. Jha, "DLINK: Dual Link Based Radio Frequency Fingerprinting for Wearable Devices," in *Proceedings of the IEEE International Conference on Local Computer Networks (LCN)*, 2015.

[6] C. Javali, G. Revadigar, L. Libman, and S. Jha, "SeAK: Secure Authentication and Key Generation Protocol based on Dual Antennas for Wireless Body Area Networks," in *Proceedings of the Workshop on RFID Security (RFIDsec)*, 2014.

[7] G. Revadigar, C. Javali, H. Asghar, K. Rasmussen, and S. Jha, "Mobility Independent Secret Key Generation for Wearable Health-care Devices," in *Proceedings of the EAI International Conference on Body Area Networks (BodyNets)*, 2015.

[8] G. Revadigar, C. Javali, W. Xu, W. Hu, and S. Jha, "Secure Key Generation and Distribution Protocol for Wearable Devices," in *Proc. IEEE International Conference on Pervasive Computing and Communications (PerCom) Work In Progress*, 2016.

[9] G. Revadigar, C. Javali, H. Asghar, K. Rasmussen, and S. Jha, "Secret Key Generation for Body-worn Devices by Inducing Artificial Randomness in the Channel," *Technical Report UNSW-CSE-TR-201506, UNSW Australia*, 2015.

[10] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *Proceedings of the ACM Conference on Computer and Communications Security (CCS)*, 2007.

[11] K. Zeng, "Physical Layer Key Generation in Wireless Networks: Challenges and Opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, June 2015.

[12] R. Ahlswede and I. Csiszar, "Common Randomness in Information Theory and Cryptography. I. Secret Sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[13] U. M. Maurer, "Secret Key Agreement by Public Discussion from Common Information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[14] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and Practical Secret Key Extraction by Exploiting Channel Response," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, April 2013.

[15] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret Key Extraction from Wireless Signal Strength in Real Environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, May 2013.

[16] R. Wilson, D. Tse, and R. A. Scholtz, "Channel Identification: Secret Sharing Using Reciprocity in Ultrawideband Channels," *Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, September 2007.

[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 International Conference on Mobile Systems, Applications, and Services (MobiSys)*, 2011.

[18] T. Shimizu, H. Iwai, and H. Sasaoka, "Physical-Layer Secret Key Agreement in Two-Way Wireless Relaying Systems," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 650–660, 2011.

[19] L. Lai, Y. Liang, and W. Du, "Cooperative Key Generation in Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 8, pp. 1578–1588, 2012.

[20] ——, "PHY-based Cooperative Key Generation in Wireless Networks," in *Proceedings of the Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, September 2011, pp. 662–669.

[21] Q. Wang, K. Xu, and K. Ren, "Cooperative Secret Key Generation from Phase Estimation in Narrowband Fading Channels," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 9, pp. 1666–1674, 2012.

[22] H. Zhou, L. M. Huie, and L. Lai, "Secret Key Generation in the Two-Way Relay Channel With Active Attackers," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 3, pp. 476–488, March 2014.

[23] C. D. T. Thai, J. Lee, and T. Q. S. Quek, "Physical-Layer Secret Key Generation With Colluding Untrusted Relays," *IEEE Transactions on Wireless Communications*, vol. 15, no. 2, pp. 1517–1530, February 2016.

[24] N. Wang, N. Zhang, and T. A. Gulliver, "Cooperative Key Agreement for Wireless Networking: Key Rates and Practical Protocol Design," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 2, pp. 272–284, February 2014.

[25] T. X. Vu, P. Duhamel, and M. D. Renzo, "On the diversity of network-coded cooperation with decode-and-forward relay selection," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4369–4378, August 2015.

[26] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," *IEEE Transactions on Wireless Communications*, vol. 12, no. 12, pp. 6076–6085, December 2013.

[27] C. D. T. Thai, P. Popovski, E. de Carvalho, and F. Sun, "Diversity-multiplexing trade-off for coordinated direct and relay schemes," *IEEE Transactions on Wireless Communications*, vol. 12, no. 7, pp. 3289–3299, July 2013.

[28] L. Shi, J. Yuan, S. Yu, and M. Li, "ASK-BAN: Authenticated Secret Key Extraction Utilizing Channel Characteristics for Body Area Networks," in *Proceedings of the ACM Confernce on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2013.

[29] L. Lai and S. W. Ho, "Key Generation Algorithms for Pairwise Independent Networks Based on Graphical Models," *IEEE Transactions on Information Theory*, vol. 61, no. 9, pp. 4828–4837, September 2015.

[30] C. Javali, G. Revadigar, M. Ding, and S. Jha, "Secret Key Generation by Virtual Link Estimation," in *Proceedings of the EAI International Conference on Body Area Networks (BodyNets)*, September 2015.
[31] W. C. Jakes, *Microwave Mobile Communications*. Hoboken, NJ: Wiley, 1972.
[32] S. Zhang, S. C. Liew, and P. P. Lam, "Physical-Layer Network Coding," in *Proceedings of the ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2006.
[33] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret Key Extraction from Wireless Signal Strength in Real Environments," *IEEE Transactions on Mobile Computing*, vol. 12, no. 5, pp. 917–930, 2013.
[34] G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," ser. EUROCRYPT. Springer-Verlag New York, Inc., 1994, pp. 410–423.
[35] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer, "Generalized Privacy Amplification," *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915–1923, 1995.
[36] 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 ACM International Conference on Mobile Computing and Networking (MobiCom)*, 2009.
[37] NIST, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," 2010.
[38] X. Liang, X. Li, Q. Shen, R. Lu, X. Lin, X. Shen, and W. Zhuang, "Exploiting Prediction to Enable Secure and Reliable Routing in Wireless Body Area Networks," in *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM)*, 2012.