Secret Key Generation by Virtual Link Estimation

Chitra Javali[*†], Girish Revadigar[*†], Ming Ding[†], and Sanjay Jha[*]
{chitraj,girishr,sanjay}@cse.unsw.edu.au; ming.ding@nicta.com.au

[*]School of Computer Science & Engineering, UNSW Australia, Sydney, AUSTRALIA
[†]National ICT Australia (NICTA), Australian Technology Park, Sydney, AUSTRALIA

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 the following limitations: (i) paying more attention to only when the two devices are in communication range, and (ii) generating keys only when the devices are in motion. Secret key generation for devices which are not in communication range and for stationary nodes is quite a challenging task. In this paper, 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 and implement our protocol using off-the-shelf commercially available resource constrained devices suitable for health-care applications which are a vital part of pervasive networks. We conduct an extensive set of experiments in an indoor environment for various scenarios involving stationary and mobile nodes. Our results show that the key generation rate increases by 20 times compared to the existing mechanisms using the same sampling frequency. We analyse the mutual information shared between the legitimate devices and eavesdroppers and our results reveal that, when at least any two of the three legitimate devices are mobile, an eavesdropper cannot obtain sufficient useful information to guess the shared keys.

Categories and Subject Descriptors

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

General Terms

Security, Algorithms, Design, Experimentation

Keywords

Body-to-body communication, Physical layer security, Secret key generation,

.

BODYNETS 2015, September 28-30, Sydney, Australia

DOI 10.4108/eai.28-9-2015.2261448

1. INTRODUCTION

The ability of connecting machines to machines, 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 the vital physiological data of a person, and forward it to the hospital for remote patient monitoring.

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 reduce the bandwidth of the base stations in mobile networks. Secure data communication is paramount in such scenarios. 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 constraint, 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 being 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. One of the approach is to extract secret keys by exploiting the unique wireless channel characteristics between two devices within communication range [8, 13]. Secret key generation for reachable nodes in body area networks has been extensively studied in [6, 10–13]. However, it is not 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 range, then it is not feasible to extract secret keys between these two devices using existing mechanisms, which only focus on single hop direct links [8]. In addition, recent work 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 devise a scheme to extract secret keys from spatio-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.

Note that authors in [14] have also 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 is very low i.e., 1.3 bits/time slot from simulation results. Researchers in [7] have studied by simulation that usage of relay increases the key rate. The scheme employs traditional packet forwarding at the relay which involves considerable number of packet exchanges not feasible for resource constrained devices.

In this paper, we study how accurately a source node, say Alice, can estimate the virtual/unseen channel link between the intermediate node Relay and destination node Bob, in order to extract secret keys from wireless channel characteristics. To be precise, Alice predicts the unseen 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, and (iii) compared to the traditional scheme where a relay just acts as an information passing node, our scheme employs a smart relaying protocol leveraging Network Coding (NC) concept, which reduces the number of time slots required and helps to achieve 33% throughput improvement.

We believe that this work is the first to investigate the feasibility of key extraction exploiting received signal strength (RSS) characteristics and NC concept in real time environment when two nodes are communicating via a relay. The rest of the paper is organised as follows: Section 2 provides an overview of the assumptions of our system model. In Section 3 we first present secret key generation between two legitimate devices within communication range, and then we explain the traditional scheme of extracting keys with the help of relay. In the third part we propose our algorithm. Section 4 presents experimental results and security analysis, followed by concluding remarks in Section 5.

2. 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 multipath 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 fraction of time during which the channel parameters do not vary. 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 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 independently identically distributed (i.i.d) complex Gaussian random variables with zero mean and a variance of σ^2.

3. ALGORITHM

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) comprises of converting the channel estimates into secret bits which we present in the next section.

In this section, we first provide an overview of secret bit extraction between two legitimate parties within communication range, and then a traditional scheme to extract keys with the help of a Relay when the two authenticated devices are not within communication range. In the third part, we propose our scheme of extracting the secret keys with the help of Relay that has potential advantages compared to the traditional scheme.

3.1 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:

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

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

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

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

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

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

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 set of consecutive signals measured at Alice and Bob for $i = \{1, 2, \ldots m\}$ at different time instants. After sufficient number of samples are exchanged between the two

[1] Note that 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 intend to study in our future work.

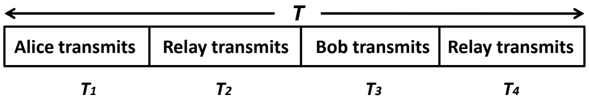


Figure 1: Traditional scheme for secret key generation requires 4 time slots.

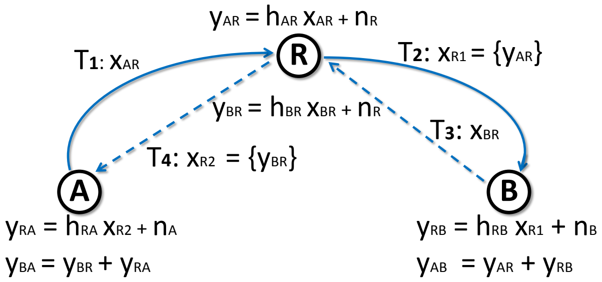


Figure 2: Traditional scheme for secret key generation protocol.

nodes, secret bits are generated by performing level-crossing or quantisation algorithm [8].

If Eve is located at a sufficient distance $> \lambda/2$ 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 $J_0(2\pi d/\lambda)$ [4].

3.2 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 Fig. 1 and the protocol is depicted in Fig. 2. All the channel estimates are measured within T_{ch}. The received signal by Relay, when Alice transmits a known probe x_{AR} is:

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

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:

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

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 subsection 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.

3.3 Proposed scheme

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 Fig. 3. The proposed protocol is as shown in Fig. 4. Reducing the number of time slots from 4 (as in traditional scheme) to 3 improves the throughput by 33%. This achievement in throughput has been well studied by researchers in [15]. Alice transmits x_{AR} to the Relay in the time slot T_1. The received signal at the Relay is:

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

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

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

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 channel estimates, $y_{BA} \approx y_{AB}$ 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:

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

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

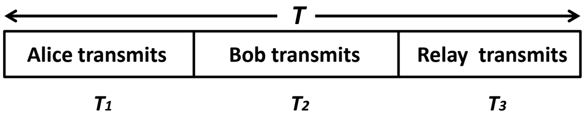
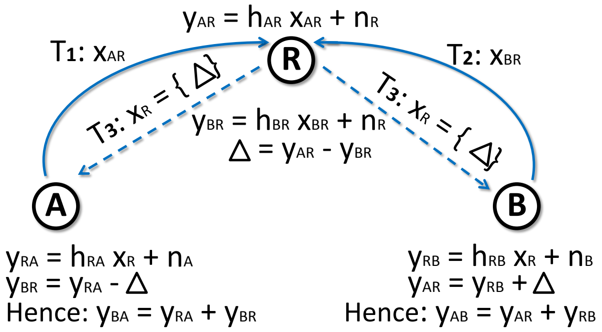


Figure 3: Time slots allocated to three legitimate nodes in our proposed scheme.



$y_{AR} = h_{AR}\, x_{AR} + n_R$
T_1: x_{AR}
T_2: x_{BR}
R
T_3: $x_R = \{\Delta\}$
$y_{BR} = h_{BR}\, x_{BR} + n_R$
$\Delta = y_{AR} - y_{BR}$
T_3: $x_R = \{\Delta\}$
A
B
$y_{RA} = h_{RA}\, x_R + n_A$
$y_{BR} = y_{RA} - \Delta$
Hence: $y_{BA} = y_{RA} + y_{BR}$
$y_{RB} = h_{RB}\, x_R + n_B$
$y_{AR} = y_{RB} + \Delta$
Hence: $y_{AB} = y_{AR} + y_{RB}$

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

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:

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

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 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) giving:

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

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 3.1, 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.

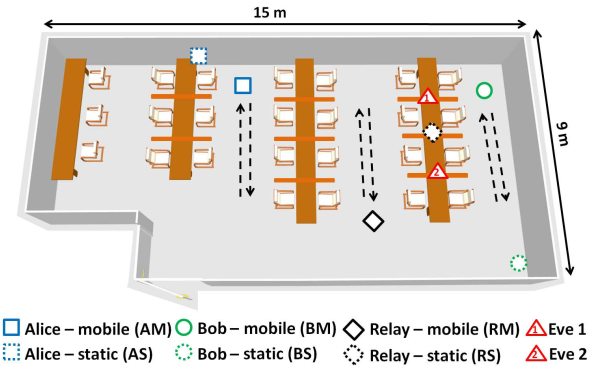


Figure 5: Floor plan of experimental set-up in an indoor environment.

Table 1: 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	✓	✓	✓	·	·	·

4. EXPERIMENTAL EVALUATION

In our experimental set-up, all the devices communicate in the same channel and frequency band of 2.4 GHz. We implemented the proposed protocol on Iris motes having RF230 radio in TinyOS environment. Alice, Bob and the Relay execute the protocol described in Section 3.3. The floor plan of an indoor environment and experimental setup are as shown in Fig. 5. The two eavesdroppers, Eve1 and Eve2 were placed at a distance of 0.1 m each, on either side of the Relay. Eve1 performs operations similar as Alice and Eve2 as that of Bob. Both the eavesdroppers measure the received signal strength indicator (RSSI) from Alice and Bob and also the corresponding Δ value from the Relay. 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 1. For experiments involving mobile nodes, the devices Alice, Bob and Relay were worn on the right arm of 3 different subjects and for stationary scenarios, the nodes were placed on a table. Each scenario was repeated 15 times and each experiment was conducted for 5-10 minutes.

In each of the mobility based scenarios, the subject(s) 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.

4.1 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 3, 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 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 [8].

For our experiments, we set $\alpha = 0.5$. The samples that occur within the thresholds are discarded and do not contribute to secret bits. After bit extraction, there may be bit discrepancies in the extracted keys generated at the two nodes. This is due to the multi-path effects in an indoor environment [4]. In such a case, Alice and Bob exchange error-correcting messages to achieve 100% identical strings [3]. Later, Alice and Bob perform privacy amplification by using methods like universal hash functions to overcome the information leaked in error-correcting phase [2].

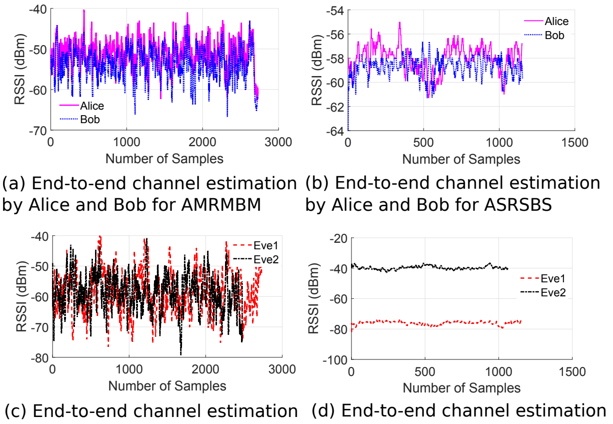
Once we have the binary strings of the secret bits, we quantify the bits extracted by the legitimate devices by the following four metrics:
(i) *Entropy* - The randomness of the generated secret bits is evaluated by entropy. Higher the randomness, more is the entropy of the key. Keys need to possess 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 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.

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

4.2 Performance Analysis of Alice-Bob

4.2.1 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 Fig. 5. Here the two channels A-R and R-B vary randomly and as observed from Fig. 6a, 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 value to the randomness of the samples measured, which helps to achieve keys with good entropy. From Fig. 7a, we observe that the bit agreement is about 95%-97% between Alice and Bob.



(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

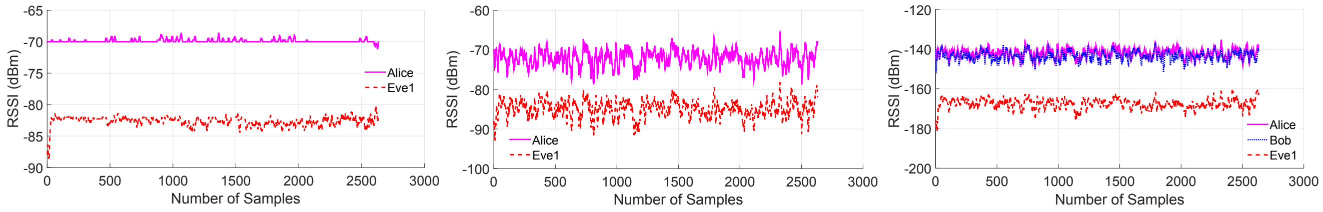
Figure 6: The channel estimations of Alice and Bob have high correlation. The eavesdropper's channel estimations vary from those of legitimate nodes.

4.2.2 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 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 Fig. 7a.

4.2.3 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. Fig. 8a 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 Fig. 8b 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. Fig. 8c 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

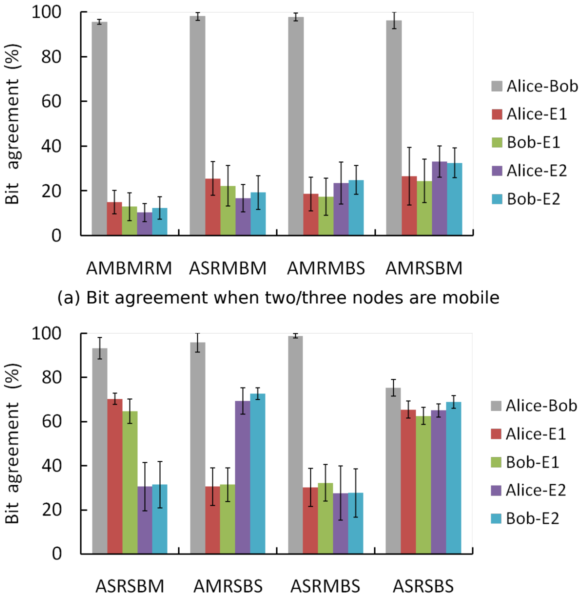


(a) Measured channel link between Alice - Relay

(b) Estimated channel link between Relay - Bob

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

Figure 8: Channel estimation by Alice and Eve1 when two of the legitimate nodes i.e., Alice and Relay are stationary: ASRSBM.



(a) Bit agreement when two/three nodes are mobile

(b) Bit agreement when two/three nodes are stationary

Figure 7: Bit agreement of all the devices for various scenarios.

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 seen in Fig. 7b.

4.2.4 All nodes are static - ASRSBS

From Fig. 6b, 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 [5]. In this case, the bit agreement on an average is only 76% as observed from Fig. 7b 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 [4]. 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 using NIST entropy test [9]. Our results reveal that, when all the nodes are stationary the entropy is ≈ 0.45, whereas for all other scenarios with at-least one node as mobile, the entropy ranges from 0.8965 to 0.9810. 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 -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 2 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. The MI is lowest when all legitimate nodes are stationary. 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).

Table 2: 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

4.3 Security Analysis

The two eavesdroppers Eve1 and Eve2 capture packets from all the 3 nodes, and moreover 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.

4.3.1 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 Fig. 6a and 6c. The bit agreement of Eve1 and Eve2 ranges from 10% to 20% w.r.t Alice/Bob as seen from Fig. 7a. From Table 2, 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.

4.3.2 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 have eavesdropper's bit agreement of only 12%-39% with Alice/Bob as shown in Fig. 7a. The MI is < 0.1 for Eve1 and Eve2 with Alice and Bob as observed from Table 2. This scenario is as good as having all the nodes as mobile.

4.3.3 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 Fig. 8a and 8b 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 Fig. 7b, 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 2 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.

4.3.4 All nodes are static - ASRSBS

Comparing Fig. 6b and 6d, 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 $\lambda/2$ [8]. Bit agreement of Eve1 and Eve2 with Alice and Bob ranges between 58%-68%. By observing Table 2, 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 [2] can be employed to strength keys between Alice-Bob.

5. CONCLUSION AND FUTURE WORK

We have proposed and implemented physical layer based secret key generation protocol for wireless nodes which are not in communication range. Our protocol employs a trusted relay between two unreachable legitimate devices and can generate secret keys with good entropy even when one/two of the three devices are stationary and achieves a throughput improvement by 33% compared to the traditional scheme. We have implemented our protocol on devices with small form factor applicable for health-care applications and conducted an extensive set of experiments to evaluate the performance. Our results reveal that we can achieve a bit agreement of about 95%-99% when all/one/two of the three nodes are mobile. The MI of the legitimate devices ranges from 0.8798 to 0.689, which is comparatively higher than the MI measured by the adversaries. In our future work, we intend to consider an untrusted relay in place of the trusted one, which can also collude with an eavesdropper in order to extract or manipulate the information exchanged between legitimate devices. The proposed protocol can also be extended for multi-hop scenario which is a challenging and interesting topic.

6. ACKNOWLEDGEMENT

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

7. REFERENCES

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

[2] C. H. Bennett, G. Brassard, C. Crepeau, and U. M. Maurer. Generalized Privacy Amplification. *IEEE Transaction on Information Theory*, 41(6):1915–1923, 1995.

[3] G. Brassard and L. Salvail. Secret-Key Reconciliation by Public Discussion. EUROCRYPT, pages 410–423. Springer-Verlag New York, Inc., 1994.

[4] W. C. Jakes. *Microwave Mobile Communications.* Wiley, Hoboken, NJ, 1972.

[5] 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 *Proc. ACM MobiCom*, 2009.

[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 *Proc. RFIDsec*, 2014.

[7] L. Lai, Y. Liang, and W. Du. Cooperative Key Generation in Wireless Networks. *IEEE Journal on Selected Areas in Communications*, 30(8):1578–1588, 2012.

[8] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik. Radio-telepathy: Extracting a Secret Key from an Unauthenticated Wireless Channel. In *Proc. ACM MobiCom*, 2008.

[9] NIST. A statistical test suite for random and pseudorandom number generators for cryptographic applications. 2010.

[10] G. Revadigar, C. Javali, H. Asghar, K. Rasmussen, and S. Jha. iARC: Secret Key Generation for Resource Constrained Devices by Inducing Artificial Randomness in the Channel. In *Proc. ASIACCS*, 2014.

[11] G. Revadigar, C. Javali, H. Asghar, K. Rasmussen, and S. Jha. Mobility Independent Secret Key Generation for Wearable Health-care Devices. In *Proc. BodyNets*, 2015.

[12] 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.

[13] G. Revadigar, C. Javali, W. Hu, and S. Jha. DLINK: Dual Link Based Radio Frequency Fingerprinting for Wearable Devices. In *Proc. IEEE LCN*, 2015.

[14] T. Shimizu, H. Iwai, and H. Sasaoka. Physical-Layer Secret Key Agreement in Two-Way Wireless Relaying Systems. *IEEE Trans. Information Forensics and Security*, 6(3):650–660, 2011.

[15] S. Zhang, S. C. Liew, and P. P. Lam. Physical-Layer Network Coding. In *Proc. ACM MobiCom*, 2006.