Collaborative Secret Key Extraction Leveraging Received Signal Strength in Mobile Wireless Networks

Hongbo Liu, Jie Yang, Yan Wang, Yingying Chen
Department of Electrical and Computer Engineering, Stevens Institute of Technology
Castle Point on Hudson, Hoboken, NJ 07030
{hliu3, jyang, ywang48, yingying.chen}@stevens.edu

***Abstract*—Securing communication in mobile wireless networks is challenging because the traditional cryptographic-based methods are not always applicable in dynamic mobile wireless environments. Using physical layer information of radio channel to generate keys secretly among wireless devices has been proposed as an alternative in wireless mobile networks. And the Received Signal Strength (RSS) based secret key extraction gains much attention due to the RSS readings are readily available in wireless infrastructure. However, the problem of using RSS to generate keys among multiple devices to ensure secure group communication remains open. In this work, we propose a framework for collaborative key generation among a group of wireless devices leveraging RSS. The proposed framework consists of a secret key extraction scheme exploiting the trend exhibited in RSS resulted from shadow fading, which is robust to outsider adversary performing stalking attacks. To deal with mobile devices not within each other's communication range, we employ relay nodes to achieve reliable key extraction. To enable secure group communication, two protocols, namely *star-based* and *chain-based*, are developed in our framework by exploiting RSS from multiple devices to perform group key generation collaboratively. Our experiments in both outdoor and indoor environments confirm the feasibility of using RSS for group key generation among multiple wireless devices under various mobile scenarios. The results also demonstrate that our collaborative key extraction scheme can achieve a lower bit mismatch rate compared to existing works when maintaining the comparable bit generation rate.**

I. Introduction

The usage of wireless devices (e.g., PDAs, smartphones, and laptops) has become an inseparable part of our daily lives, which actively involves in information sharing and various data transactions in ways that previously were not possible. However, to ensure the successful deployment and adoption of these emerging applications, secure communication is crutial to support data transmission confidentiality, data integrity, and device authentication among multiple wireless devices. For example, police officers covering different street blocks need to share with each other the monitoring information along their daily patrol routes and the recording of the crime information by areas. Another example is a group of travelers want to limit the sharing of travel plans, journals, pictures and video clips among themselves through the peer-to-peer association.

Although there have been active research in applying traditional cryptographic-based methods such as public key infrastructure (PKI) to wireless networks, these methods may not be always applicable because of the limited resources on wireless devices (e.g., limited battery and computation power), and lacking of a fixed key management infrastructure due to highly dynamic mobile wireless environments (e.g., peer-to-peer association, neighborhood devices changing frequently). In addition, the openness of the wireless transmission medium makes the key establishment itself vulnerable to eavesdropping—adversaries within communication range of legitimate devices can monitor any information exchanges of key generation and renewal. In this study, we examine secure group communication among multiple wireless devices by exploiting physical layer information of radio channel instead of using the traditional cryptographic-based methods.

The main advantage of the secret key generation utilizing physical layer information of radio channel is that it allows any two wireless devices within transmission range of each other to extract a shared symmetric cryptographic key while does not require a fixed infrastructure or a secure communication channel [1]–[3]. Based on the *principle of channel reciprocity*, two wireless devices can extract identical secret bits independently by using the sampled sequence collected from the radio channel between them within the coherence time of the channel. Unlike existing key generation algorithms, such as Diffie-Hellman, which rely upon computational hardness of problems, secrete key generation using channel randomness provided by the temporal and spatial variation of the radio channel can achieve information-theoretical secrecy [4].

Comparing to various physical layer information of radio channel (such as channel phase [5], [6]), sampling Received Signal Strength (RSS) is an attractive approach to generate secret keys as the RSS readings are readily available in the existing wireless infrastructure and thus presents tremendous cost savings. However, previous works on RSS based secret key generation mainly focused on improving the secret bit generation rate between a pair of wireless devices (by exploiting temporal and spatial variations of radio channel [7], [8], multiple antenna diversity [9], and multiple frequencies [10]). The problem of using RSS to perform key generation among multiple wireless devices to ensure secure group communication remains as a challenge.

In this work, we propose collaborative secret key extraction for a group of wireless devices using readily available RSS measurements from these devices, rather than relying on a key distribution infrastructure. The building block of our proposed framework is a secret key extraction scheme, which exploits the trend exhibited in RSS to encode secret bit to achieve a lower bit mismatch rate comparing to previous works under hight bit generation rate. We show that our scheme is robust to the attacker who stalks the mobile devices for key regeneration. To address the issue of generating secret keys between a pair of wireless devices not within each other's communication range, we further define a metric using difference of RSS and employ relay nodes to assist in key generation.

978-1-4673-0775-8/12/$31.00 ©2012 IEEE

To enable secure group communication, two protocols, namely *star-based* and *chain-based*, are developed in our framework by exploiting RSS from multiple devices to perform group key generation collaboratively. In particular, the star-based collaborative key extraction is designed for scenarios when multiple wireless devices are within each other's communication range (e.g., people traveling together), whereas the chain-based approach deals with scenarios when not all wireless devices under consideration are within each other's communication range, but they are interconnected (e.g., patrolling police officers).

We conducted experiments in both outdoor (e.g., park and street) and indoor (e.g., office building) environments using MICAz motes to evaluate the effectiveness of our proposed collaborative key generation framework. Our experimental results confirm the feasibility of using RSS for group key generation among multiple wireless devices under various mobile scenarios. The results also demonstrate that our fading-trend assisted key extraction scheme can achieve a lower bit mismatch rate compared to existing works when maintaining the comparable secret bit generation rate.

The rest of the paper is organized as follows. We place our work in the context of related research in secret key extraction in Section II. We provide our system model and experimental methodology in Section III. We present the proposed RSS trend based secret key extraction scheme in Section IV. In Section V, we describe our collaborative key extraction when two wireless devices, who intent to establish keys, cannot directly communicate with each other. Next, we present the group key extraction methods for different network scenarios in Section VI. Finally, we conclude our work in Section VII.

II. Related Work

There has been active research in secret key generation and several radio channel features have been proposed for key extraction in wireless networks. Phase difference is first proposed in [11], in which differential phase of two-tone signal was measured and quantized to generate secret keys. Phase difference was further exploited in [5], [6]. In [5], random phase is used for secret key extraction in an OFDM system, whereas [6] proposed an scheme for efficient key establishment. The impulse response of a wireless channel was used to generate a shared secret [4], [12], [13]. Ultra-wideband radios were used in [12] to measure the impulse response, while [13] and [4] estimated impulse response from cellular signals and WiFi signals, respectively. Statistics of the Angle-of-Arrival (AOA) was used in [2] as a signature for key generation, however, it requires an access point to have a programmable phased array antenna.

Received signal strength or channel gain is the most commonly used radio channel feature for secret key extraction due to it is readily available in existing wireless infrastructure, and thus it is easy to measure with little effort. For RSS based methods, previous works mainly focused on exploiting temporal and spatial variations of radio channel [1], [3], [4], [7], [8], [14], [15], multiple antenna diversity [9], and multiple frequencies [10] for secret bit extraction between a pair of wireless devices. In [14], the authors proposed to encode the change in signal envelop during a transmission to encode and decode transmitted messages. [15] used the universal software radio peripheral (USRP) and GNU software radio to generate 24-bit signature based on the measured channel gain. In [1], the deep fades of channel gain that periodically occur in mobile channels was proposed to extract secret bits. [4] generated secret bit using the RSS extracted from 802.11a packets with mobile devices. [7], [8] focused on improving the secret bit generation rate in mobile wireless networks, while [10] proposed to use multiple frequencies to generate secret keys in static wireless sensor networks. Multiple-antenna diversity was exploited in [9] for improving the secret bit generation rate. However, none of these RSS based methods considered key generation for multiple wireless devices leveraging RSS.

Different from the above works, we address the problem of secret key generation for a group of wireless devices using readily available RSS measurements. Further, we evaluated our proposed framework in both outdoor and indoor environments.

III. System Overview and Experimental Methodology

A. System Overview

Generating group secret key is essential to ensure secure communication among multiple wireless devices. Previous RSS-based key extraction schemes only work with pairwise devices within communication range of each other. In this framework, we focus on secret key extraction for a group of wireless devices by exploiting the RSS measurements from these devices collaboratively. There are a number of challenges arising from utilizing RSS measurements for group key generation. First, the RSS values obtained between a pair of devices cannot be securely passed to other devices, making it hard to reach key agreement among multiple devices without the availability of a fixed infrastructure. Second, due to the dynamics of mobile devices, the devices within the group that needs to establish a secret key may not be within each other's communication range, making the existing RSS-based methods not applicable.

To address these challenges, we define a metric called *DOSS* which represents the difference of signal strength measured at one wireless devices via different radio channels. In our framework, instead of passing the RSS measurements directly, the DOSS values will be passed to other devices to facilitate key extraction. By utilizing this simple metric, an eavesdropping attacker, monitoring the communication among a group of wireless devices, cannot obtain the exact RSS measurements between a pair of devices, and consequently it cannot regenerate the secret group key as the attacker is usually located at greater than a half-wavelength away from the legitimate devices.

Our framework consists of two protocols, *star-based* and *chain-based*, to facilitate reliable secret key generation among multiple wireless devices. The star-based collaborative key extraction protocol is designed for the scenarios when the group of wireless devices under consideration are within the communication range of each other. For example, a group of travlers are visiting the same scenic spot. A device in the group will be randomly picked to serve as the *virtual central node* by passing the DOSS values to other devices to perform key extraction collaboratively. Whereas under the scenarios when the group of wireless devices are not within the communication range of each other, our chain-based collaborative key extraction protocol constructs a virtual topology where the devices in the group under consideration are connected with

one another like a chain. Each device in the chain involves to pass the corresponding DOSS values to its neighbor device in the next step of the chain. The chain-based approach may incur accumulated RSS noise across multiple devices. We examine the effectiveness of the chain-based approach in real world scenarios and our results presented in Section VI can serve as a guideline for designing group key generation in mobile environments leveraging RSS.

To establish secret keys for secure group communication, we develop two building blocks for our framework, *fading trend based secret key extraction* and *relay node assisted collaborative key extraction*.

- **Fading trend based secret key extraction:** Existing pairwise key generation methods merely use thresholding on RSS measurements alone to extract secret bits. We take a different view point by combining the trend exhibited in RSS measurements with RSS thresholding to generate multi-bit secret keys. Since there should be exact or similar fading trend presented in the RSS measurements between a pair of wireless devices according to the channel reciprocity. The fading trend based approach helps to better capture the similarity presented by channel reciprocity as opposed to using the RSS values directly.
- **Relay node assisted collaborative key extraction:** We employ a relay node for key extraction when two wireless devices cannot communicate directly. The relay node communicates with this pair of wireless devices and sends the DOSS values to them. These two devices utilize the received DOSS values and the measured RSS readings between the relay node to themselves to generate key secretly. When two wireless devices are farther away, multiple relay nodes may be employed to assist in the key extraction process.

B. Experimental Methodology

Experimental Setup: We conducted experiments using MICAz wireless motes, which compose a micro-controller, a built-in antenna and a CC2420 radio chip operating at 2.4 GHz. We set up a mobile wireless network with 6 MICAz motes and one additional mote connected to a laptop acts as the network sink. We use the probe packet to fulfill our needs to collect RSS measurements. Each node broadcasts probe packets at the rate of 20 pkt/sec. The probe packet includes the sending node ID and the packet sequence number. When a node receives a probe packet, it measures the RSS and extracts the sending node ID and packet sequence number, and inserts this information into the probe packet it will send next. After the sink node receives the probe packet sent or forwared from other nodes, it extracts these information and stores it in the database. Therefore, the sink can obtain all the RSS measurements on the channel between any pair of nodes. To evaluate our framework, we categorize our experimental setup as following:

- To test fading trend based key extraction, we use a pair of MICAz motes sending probe messages to each other;
- To test relay node assisted key extraction, we choose 1, 2, 3 or 4 MICAz motes as relay nodes respectively to forward the measured information to sink node and make the rest of the 2 MICAz motes as the pair of wireless devices who want to set up the secret key.
- To test group key extraction, we use all 6 MICAz motes. In particular, 6 MICAz motes are chosen to construct a virtual chain topology to run the chain-based key extraction protocol, while 1 MICAz mote is chosen as the virtual central node when running the star-based protocol.

Experimental Scenarios: We conducted experiments by running our mobile wireless network to collect RSS measurements in both outdoor and indoor environments. Our outdoor environments include *park* and *street*. The park is covered with tall trees, multiple small roads and fountains. Our street environment is from the Hoboken train station to Stevens spanning over 10 street blocks. During our experiments, we measured RSS under two different conditions: one is having pedestrians passing through our mobile wireless network, and the other is not having pedestrians passing through. Thus, for outdoor environments we have four experimental scenarios numbered as below: *A (park, with pedestrian)*, *B (park, without pedestrian)*, *C (street, with pedestrian)*, and *D (street, without pedestrian)*. In our indoor environment, the RSS measurements are collected in classrooms, stairs and hallways, indicated as *E (building)*. The outdoor experiments are performed under the presence of dynamic environmental movements (including people walking, kids running, and cars driving around) and all the motes involved in secret key generation are constantly moving. There are total 25 data sets, each lasts for about 5 minutes.

Metrics: To evaluate the performance of our framework, we use the following metrics:

Bit mismatch rate: For key extraction between a pair of wireless devices, the bit mismatch rate is defined as the number of bits that do not match between two devices divided by the number of bits extracted from RSS quantization. For group key extraction, it is defined as the averaged bit mismatch rate from all pairs of devices in the group.

Bit generation rate: The bit generation rate represents as the number of secret bits extracted per RSS measurement.

Randomness: The standard NIST test suite is employed to measure the randomness of the generated secret bit string.

IV. Fading Trend based Secret Key Extraction

In this section, we present our fading trend based secret key extraction scheme, which is the building block to support collaborative key extraction for a group of mobile devices. A security analysis is provided for the scheme. We also evaluate the performance of the scheme using real data collected under different environments.

A. Scheme Description

1) Algorithm: Given the RSS measurements from the same radio channel, the RSS readings measured by a pair of wireless devices, e.g., Alice and Bob, within the coherence time should be identical based on the principle of wireless channel reciprocity. In practice, there will be mismatch due to the half-duplex operating mode of standard transceivers (e.g., one device cannot send and receive packets at the same time) and the measurement errors. However, we found that the fading exhibited in RSS measurements over time for a pair of mobile devices follows similar increasing or decreasing trend despite of the mismatch of absolute values, as shown in figure 1. This observation inspires us to utilize the fading trend to reduce the

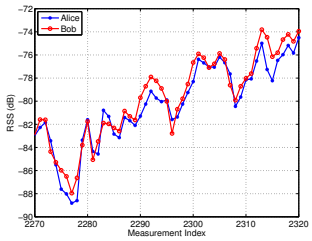


Fig. 1. Segments of RSS measurements from a pair of mobile devices in park.

secret bit mismatch rate when extracting secret bits from RSS measurements.

The proposed fading trend based secret key extraction algorithm includes three components: *interpolation*, *fading trend estimation* and *thresholding*. Two variants are proposed in the thresholding step: basic RSS fading trend and median thresholding (**RTM**) and extended RSS fading trend and quantization (**RTQ**). The algorithm flow is displayed in Algorithm 1.

We use the following standard notations: (a) "$\wedge$" is the AND operation; (b) "$\vee$" stands for OR operation; (c) $\hat{r}(k)$ denotes RSS measurement extracted from the probe packet at time k.

Interpolation: Due to the half-duplex operating mode of standard transceivers, the probe packet transmitted by Alice and Bob has a short delay, which results in the channel measurements asymmetry. And this becomes one of the sources causing RSS reading mismatch. To address this issue, we use the cubic Farrow filter based interpolation technique on top of the measurement RSS readings so that Alex and Bob are able to estimate the RSS measurements at common time instants [16].

Fading trend estimation: The objective of this step is to extract one secret bit at RSS each measurement that exhibits *fading trend*. To determine the fading trend on one particular RSS measurement $\hat{r}(k)$, we examine its previous sample $\hat{r}(k-1)$ and the second following sample $\hat{r}(k+2)$. Here we define $\Phi^1 = \hat{r}(k) - \hat{r}(k-1)$ and $\Phi^2 = \hat{r}(k+2) - \hat{r}(k)$. If the set of RSS measurements $\{\hat{r}(k-1), \hat{r}(k), \hat{r}(k+2)\}$ consist of a monotone sequence, i.e., Φ^1 and Φ^2 has the same positive or negative relationship, a fading trend is determined. Using this approach, for the fading trend estimation at each measurement, there is only one overlapped RSS sample. Thus, the possible correlation caused by fading trend estimation is minimized. The secret bit, $b_k(1)$, encoded at $\hat{r}(k)$ is determined as 1 or 0 which corresponds to increasing or decreasing fading trend, as computed in equation 2 displayed in Algorithm 1.

Thresholding: Two variants of secret bits extraction are proposed at this step.

RTM: This basic version of our proposed scheme uses the median value of all RSS measurements, θ, as the single threshold to extract another secret bit for each RSS measurement. The bit, $b_k(2)$ is encoded as 1 or 0 depending on whether $\hat{r}(k)$ is larger than θ or not, as described in equation 3 of Algorithm 1.

RTQ: The extended version of our key generation scheme extracts multiple bits per RSS measurement in addition to the trend based quantization at the previous step. Instead of using single threshold, we are inspired by the idea of quantization in signal processing to extract secret bits via multiple thresholds. In order to extract $m-1$ bits per measurement, the RSS measurements $\hat{r}(k)$ is quantized into $2^{(m-1)}$ equally-likely

Algorithm 1 Algorithm flow for fading trend based secret bit extraction per RSS measurement.

Require: INPUT:
$\hat{r}(k-1), \hat{r}(k), \hat{r}(k+2)$: the RSS readings measured from the probe packet with time index $k-1, k, k+2$;
OUTPUT:
$[b_k(1), b_k(2), \cdots, b_k(m)]$: m-bit secret bit sequence extracted from RSS measurement $\hat{r}(k)$;
PROCEDURES:

1: **Interpolation:**
Using cubic Farrow filter based interpolation technique.

2: **Fading trend estimation:**
For a set of RSS measurements $\{\hat{r}(k-1), \hat{r}(k), \hat{r}(k+2)\}$,

$$b_k(1) = \begin{cases} 0 & \Phi^1 < 0 \wedge \Phi^2 < 0 \\ 1 & \Phi^1 > 0 \wedge \Phi^2 > 0 \end{cases} \quad (2)$$

3: **Thresholding:**
RTM:

$$b_k(2) = \begin{cases} 0 & \hat{r}(k) < \theta \\ 1 & \hat{r}(k) \geq \theta \end{cases} \quad (3)$$

RTQ:
$b_k(i), i = 2, \cdots, m$: Using quantization via multiple thresholds.

levels. Let $F(\hat{r}(k))$ be the cumulative distribution function of $\hat{r}(k)$. The thresholds used for extracting secret bits are determined by the inverse of $F(\hat{r}(k))$,

$$\rho_j = F^{-1}(\frac{j}{2^w}), k = 1, \cdots, 2^{m-1} - 1 \quad (1)$$

In addition, $\rho_0 = min(\hat{r}(k))$ and $\rho_{2^{m-1}} = max(\hat{r}(k))$. When $\hat{r}(k)$ falls between any neighboring thresholds, gray coding techniques [17] are employed for extracting $m-1$ bits, $b_k(i), i = 2, \cdots, m$, from $\hat{r}(k)$.

By examining through the measurements, all the RSS readings exhibiting the fading trend can be found. Alice and Bob will exchange their own set of index that includes all the measurements have the fading trend. The measurements at the common indexes are then encoded to secret bits by using our proposed fading trend estimation and thresholding. The remaining set of measurements without the fading trend will be quantized to secret bits by using existing multi-level quantization method [3]. One of the encouraging observations from our various experimental scenarios is that we found over 75% of RSS measurements exhibit a fading trend.

2) Bit Mismatch Probability Analysis: We next provide a theoretic analysis of the probability of bit disagreement when using the fading trend for secret bit encoding. $\hat{r}_A(\kappa)$ and $\hat{r}_B(\kappa)$ are measured RSS readings at Alice and Bob respectively,

$$\begin{aligned} \hat{r}_A(\kappa) &= r_A(\kappa) + n_A(\kappa) \\ \hat{r}_B(\kappa) &= r_B(\kappa) + n_B(\kappa). \end{aligned} \quad (4)$$

where $\kappa = k-1, k, k+2$. The RSS measurements are determined by the radio channel and noise $n(\kappa)$ at different time instants. $n(\kappa)$ is assumed as i.i.d Gaussian noise, following $N(0, \sigma^2)$. According to the reciprocity principle, for each time instant κ, $r_A(\kappa)$ should be equal to $r_B(\kappa)$. Assuming each RSS measurement is independent, both Φ_A^i and $\Phi_B^i, i = 1, 2$, also follow Gaussian distribution with variance $2\sigma^2$, where Φ_A^i and $\Phi_B^i, i = 1, 2$, has the same definition as Φ_i for Alice and Bob respectively. The following conditions need to be fulfilled if there is a bit disagreement:

$$\begin{aligned} &\{\Phi_A^1 > 0 \wedge \Phi_B^1 < 0 \wedge \Phi_A^2 > 0 \wedge \Phi_B^2 < 0\} \\ \vee \quad &\{\Phi_A^1 < 0 \wedge \Phi_B^1 > 0 \wedge \Phi_A^2 < 0 \wedge \Phi_B^2 > 0\} \end{aligned} \quad (5)$$

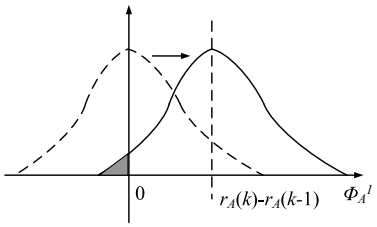


Fig. 2. Illustration of the bit disagreement probability analysis.

Then the probability for bit disagreement can be derived as:

$$\begin{aligned} Pr(err) =& Pr(\Phi_A^1 > 0 \wedge \Phi_B^1 < 0 \wedge \Phi_A^2 > 0 \wedge \Phi_B^2 < 0) \\ &+ Pr(\Phi_A^1 < 0 \wedge \Phi_B^1 > 0 \wedge \Phi_A^2 < 0 \wedge \Phi_B^2 > 0) \\ =& (1 - F(\Phi_A^1 = 0))(1 - F(\Phi_A^2 = 0))F(\Phi_B^1 = 0)F(\Phi_B^2 = 0) \\ &+ F(\Phi_A^1 = 0)F(\Phi_A^2 = 0)(1 - F(\Phi_B^1 = 0))(1 - F(\Phi_B^2 = 0)). \end{aligned} \quad (6)$$

where $F()$ is the cumulative distribution function for Gaussian distribution.

To illustrate, Figure 2 depicts the probability density function of Φ_A^1. If the mean value of $(r_A(k) - r_A(k-1))$ of Φ_A^1 has a large deviation from 0, which means the signal strength changes sharply from $r_A(k-1)$ to $r_A(k)$ due to the fading effects, the probability that $\Phi_A^1 < 0$ shown as the shaded area will be extremely small. Due to the reciprocity principle, $r_A(k) - r_A(k-1)$ equals to $r_B(k) - r_B(k-1)$, which implies that Φ_A^i and $\Phi_B^i, i = 1, 2$, have the same mean value, and it results in the probability of $\Phi_B^1 < 0$ to be also small. Therefore, the first term of equation (6) should be a small value, which indicates a small bit disagreement probability. Similar analysis can be applied for the second term in equation (6) as well.

B. Security Analysis

1) Attack model: We consider a passive adversary called *Stalker*, who follows the trajectory of either Alice or Bob and eavesdrops all the wireless communication between Alice and Bob during key generation. The Stalker is able to measure the radio channels between itself to both Alice and Bob when Alice and Bob exchanging probe packets. In addition, Stalker can obtain the secret key extraction algorithm and corresponding parameters for key generation. However, Stalker can not be very close to either Alice or Bob (at least half of wavelength away), otherwise it increases the exposure of itself to be detected. The property of spatial decorrelation makes it impossible for any adversary devices who locate at $\lambda/2$ away to measure the same wireless channel as legitimate devices [18]. Therefore, even though Stalker follows the trajectory of a legitimate device, the obtained RSS measurement will not present the same fading trend and thus cannot extract the same secret key successfully.

2) Experimental Results: Figure 3 presents our experimental results of a pair of MICAz nodes with the presence of Stalker (using an additional MICAz mote placed at 30 cm away). We found that the bit mismatch rate incurred by Stalker is much higher than that of between the pair of legitimate devices under different scenarios identified as A, B, C, D, and E in Section III-B. This observation validates the high security of using channel measurements for secret key extraction.

C. Performance Evaluation

We compare our fading trend based key extraction scheme with the representative previous work [7], which uses multi-level quantization.

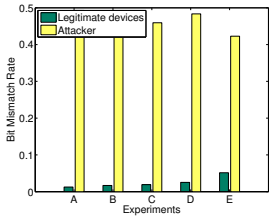


Fig. 3. Bit mismatch rate for legitimate devices and attacker under different scenarios.

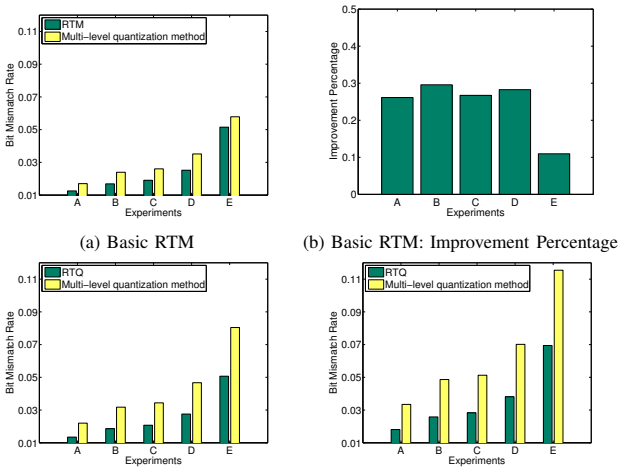
1) Performance of Bit Mismatch Rate: **Basic RTM scheme:** Figure 4(a) shows the bit mismatch rate versus different experimental scenarios from A to E for both our method and the multi-level quantization method when maintaining the same secret bit generation rate at 2 bits per measurement. We observed that our fading trend based method outperforms the multi-level quantization approach by more than 26% for outdoor environments, particularly, 26%, 30%, 27%, 28% for scenarios A∼D respectively, and around 11% for indoor environment as in shown in figure 4(b). In addition, the scenarios with pedestrians passing between our mobile devices achieve lower bit mismatch rate, indicating the presence of larger fading, which benefits our proposed method.

Extended RTQ scheme: Figure 4(c) and (d) presents the bit mismatch rate for RTQ scheme and the multi-level quantization method when generating 3 bits and 4 bits from one RSS measurement. By comparing Figure 4(c) and figure 4(d), we observed that as the the number of secret bits extracted per RSS measurement increases, the bit mismatch rate also increases for both methods. However, our proposed method outperforms the multi-level quantization method for more than 40% under each scenario, and the performance improvement becomes more significant as the number of encoded bits increases. The increased bit mismatch rate for both methods is caused by the increasing number of thresholds for quantizing RSS measurements. However, due to the fading trend employed, the bit mismatch rate of our method does not increase as much as the multi-level quantization method when the number of encoded bits increases.

2) Performance of Randomness: To ensure that the secret key generated is substantially random, the standard randomness test suite from NIST [19] is employed to verify the effectiveness of the secret bits extracted after secret key reconciliation and privacy amplification [6]. Since the bit length generated from our experiments should meet the recommended size of the NIST tests, we run 8 NIST tests and calculate their p-values. The results of these tests for 5 different experimental scenarios are listed in Table I. All the cases pass the test, and have the p-value much larger than 0.01, which is the threshold to pass the test.

V. Relay Node Assisted Collaborative Key Extraction

In this section, we address the issue when a pair of wireless devices are not within each other's communication range by designing a collaborative key extraction scheme under the assistance of relay nodes. The secret bit encoding in this scheme utilizes the fading trend based scheme discussed in Section IV.



(a) Basic RTM (b) Basic RTM: Improvement Percentage

(c) Extended RTQ: 3-bit (d) Extended RTQ: 4-bit

Fig. 4. Bit mismatch rate under various experimental scenarios.

A. Overview

Since there is no common radio channel that two devices (e.g., Alice and Bob) can measure directly when they are not within each other's communication range, we propose to use the collaborative efforts from one or more relay nodes, who connect between these two devices, to assist in secret key generation between them. However, due to the open nature of wireless medium, any information forwarded by relay nodes will be eavesdropped, which makes it infeasible to pass RSS measurements directly to either Alice or Bob for secret key generation. To solve this problem, we define a metric called *DOSS* which represents the *difference of signal strength* measured at each relay node from two different radio channels that the relay nodes connected to other devices. Instead of passing the RSS readings, the DOSS values will be passed to other devices to facilitate key extraction. Without obtaining the exact RSS measurements, an adversary cannot regenerate the same secret key between Alice and Bob.

B. Protocol

1) Description: We use the following notation to illustrate each device: Alice and Bob are denoted as P_0 and P_J, and we assume there are $J-1$ relay nodes, $P_j, j = 1, \cdots, J-1$, on the routing path between Alice and Bob.

Step 1: Alice and Bob communicate via one or more relay nodes, $P_j, j = 1, \cdots, J-1$, using existing routing protocols [20].

Step 2: Any two neighboring devices exchange the probe packets for extracting channel measurement. The RSS measured at relay node P_j from its neighboring devices P_{j-1} and P_{j+1} are $\hat{r}_{P_{j-1},P_j}(k)$ and $\hat{r}_{P_{j+1},P_j}(k)$, respectively. Alice and

TABLE I
NIST STATISTICAL TEST SUITE RESULTS

Test	A	B	C	D	E
Freq.	0.55	0.42	0.23	0.55	0.55
Block Freq.	0.86	0.87	0.81	0.87	0.96
Cum. sums (Fwd)	0.72	0.54	0.22	0.72	0.96
Cum. sums (Rev)	0.81	0.81	0.39	0.81	0.96
Runs	0.84	0.50	0.51	0.84	0.69
Longest run of 1s	0.76	0.42	0.51	0.84	0.83
FFT	0.65	0.65	0.65	0.65	0.17
Approx. Entropy	0.92	0.65	0.39	0.92	0.92
Serial	0.50 0.50	0.50 0.50	0.50 0.50	0.50 0.50	0.50 0.97

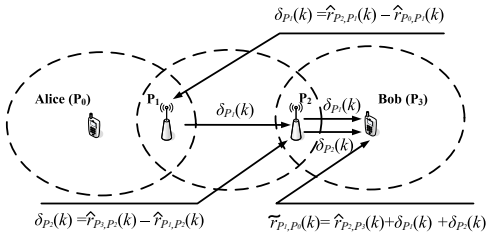


Fig. 5. Illustration of relay node assisted collaborative key extraction.

Bob obtain the RSS measurements $\hat{r}_{P_1,P_0}(k)$ and $\hat{r}_{P_J,P_{J-1}}(k)$ from relay node P_1 and P_{J-1}, respectively.

Step 3: Each relay node P_j calculates the DOSS values based on the radio channels it uses to communicate with devices P_{j-1} and P_{j+1}:

$$\delta_{P_j}(k) = \hat{r}_{P_{j+1},P_j}(k) - \hat{r}_{P_{j-1},P_j}(k), \tag{7}$$

and then forward it to the relay node in the next hop P_{j+1}. Eventually, $\delta_{P_j}(k)$ is forwarded to Bob.

Step 4: Once the DOSS values from each relay node arrives at Bob, Bob is able to estimate the radio channel between Alice and the relay node P_1:

$$\tilde{r}_{P_1,P_0}(k) = \hat{r}_{P_{J-1},P_J}(k) + \sum_{j=1}^{J-1} \delta_{P_j}(k). \tag{8}$$

Since Alice can directly measure the radio channel between the relay node P_1 and Alice: $\hat{r}_{P_1,P_0}(k)$, both Alice and Bob have obtained the common channel information of radio channel between Alice and relay node P_1. Thus, secret keys can be generated secretly between Alice and Bob by using the key extraction algorithm.

One alternative is to utilize all the channel information along the path between Alice and Bob by letting the relay nodes send the DOSS values to both Alice and Bob. However, we found that the generated key presents the same secrecy as this simple approach, which only uses the channel information between Alice and the first relay node. Figure 5 illustrates our proposed protocol by employing two relay nodes P_1 and P_2. We note that this protocol is generic to any key extraction algorithms using RSS. In this work, we use the fading-trend based scheme.

2) Performance Analysis: Under an ideal situation, based on the reciprocity principle of wireless channel, our relay node assisted key extraction protocol could make Alice and Bob obtain identical RSS measurements. The estimated value of $\hat{r}_{P_1,P_0}(k)$ by Bob is:

$$\begin{aligned}\tilde{r}_{P_1,P_0}(k) =& r_{P_{J-1},P_J}(k) - \delta_{P_{J-1}}(k) - \delta_{P_{J-2}}(k) - \cdots - \delta_{P_1}(k)\\ =& r_{P_J,P_{J-1}}(k) - (r_{P_J,P_{J-1}}(k) - r_{P_{J-2},P_{J-1}}(k))\\ & - (r_{P_{J-1},P_{J-2}}(k) - r_{P_{J-3},P_{J-2}}(k)) - \cdots\\ & - (r_{P_2,P_1}(k) - r_{P_0,P_1}(k))\\ =& r_{P_0,P_1}(k) = r_{P_1,P_0}(k)\end{aligned} \tag{9}$$

However, in real world scenarios, the estimated RSS measurements is affected by measurement noise, and is different from that measured by Alice. We have $\hat{r}_{P_j,P_{j-1}}(k) = r_{P_j,P_{j-1}}(k) + n_{P_j,P_{j-1}}(k)$, where $n_{P_j,P_{j-1}}(k) \sim N(0,\sigma^2)$ is assumed to follow a Gaussian distribution. Thus,

$$\begin{aligned}\tilde{r}_{P_1,P_0}(k) =& \hat{r}_{P_{J-1},P_J}(k) - \delta_{P_{J-1}}(k) - \delta_{P_{J-2}}(k) - \cdots - \delta_{P_1}(k)\\ =& r_{P_1,P_0}(k) + \sum_{j=1}^{J} n_{P_{j-1},P_j}(k) - \sum_{j=1}^{J-1} n_{P_{j+1},P_j}(k)\end{aligned} \tag{10}$$

The estimated value $\tilde{r}_{P_1,P_0}(k)$ also follow the Gaussian distribution with $N(r_{P_1,P_0}(k),(2J-3)\sigma^2)$. The variance of noise increases linearly as the number of relay nodes between Alice and Bob increases. We will study the impact of the accumulated noise in our relay node assisted key extraction scheme.

C. Security Analysis

1) Attack Model: In this work, we assume wireless devices involved in key generation (e.g., Alice and Bob) are authenticated using existing methods. However, relay nodes may not be authenticated. Untrusted relay nodes may corrupt the measured channel information, consequently, the key establishment between Alice and Bob cannot be successful. Further, the untrusted relay nodes may collect the channel information and regenerate the secret key between Alice and Bob in order to decode the data transmission between Alice and Bob and conduct more harmful attacks. We assume not all the relay nodes are malicious.

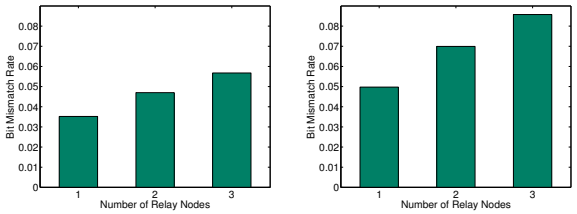
2) Security Strategy: If an untrusted relay node corrupts the forwarded DOSS values, Alice and Bob can not extract the secret key successfully, and neither does the relay node. Thus, it is more likely that an untrusted relay node wants to regenerate the secret key since it knows the DOSS values. Our proposed protocol can cope with this kind of relay node by employing relay nodes from more than one route to complete its key generation process. In this way, the relay nodes on each route can only obtain partial information and cannot generate a complete secret key. To illustrate, Alice and Bob can get a certain number of RSS measurements, say K measurements, using the routing path $\{P_1, P_2, \cdots, P_{J-1}\}$. Alice and Bob then switch to utilize a different routing path, e.g., $\{P'_1, P'_2, \cdots, P'_{J-1}\}$, which has no overlapping relay nodes with the first routing path, for another collection of K' RSS measurements. Alice and Bob then generate secret keys by combining K and K' measurements. Thus, any untrusted relay node can only obtain partial RSS measurements and cannot derive the secret keys.

D. Performance Evaluation

Figure 6 presents the bit mismatch rate of our relay node assisted key extraction scheme under two different experimental scenarios *A (park, with pedestrian)* and *B (park, without pedestrian)*. In general, the low bit mismatch rate is achieved for both cases. As the number of relay nodes increases from 1 to 3, the bit mismatch rate goes up. When there are pedestrians moving across our mobile network (i.e., case A), our relay node assisted protocol performs much better when using fading trend based key extraction. To reconcile the mismatch on the secret bits between Alice and Bob, existing error correction code can be employed. Here we assume $[n, m, 2t+1]_2 = [23, 12, 7]_2$-Golay code [21] is exploited in our proposed scheme with error tolerance $\frac{t}{n} = 13\%$. According to figure 6, when the number of relay nodes is 3, the bit mismatch rate is still within the error tolerance of Golay code, which indicates the feasibility of our rely node assisted key extraction scheme.

VI. Secret Key Extraction for Multiple Wireless Devices

In this section, we develop two protocols, namely *star-based* and *chain-based*, on group secret key extraction and evaluate their performance.



(a) A (park, with pedestrian) (b) B (park, without pedestrian)

Fig. 6. Performance of relay node assisted key extraction.

A. Overview

We examine two typical scenarios in mobile wireless networks when performing group key extraction for multiple devices. The first one is when all wireless devices within the group under consideration are within each other's communication range, which means any two devices are directly connected. For example, a group of travelers are visiting different places and would like to establish secure communication among themselves. For this scenario, we choose one device as the virtual central node and the rest of the devices in the group forms a star topology. The virtual central node facilitates the group key extraction by passing the DOSS values to other nodes and perform key extraction collaboratively.

When not all wireless devices within the group under consideration are within each other's communication range, they are interconnected with either group or non-group members. We form the devices within the group to a virtual chain-based network, where nodes are sequentially connected. We develop a chain-based collaborative key extraction protocol, where each device in the chain involves to pass the corresponding DOSS values to its neighbor device in the next step of the chain. The chain-based approach deals with a more dynamic mobile environment than that of star-based approach. We note that the virtual chain-based topology is a special case of the tree-based topology and represents the worst case scenario in terms of accumulated noise during group key extraction using RSS. Both star-based protocol and chain-based protocl are generic and can be used with any key extraction scheme. In this work, we integrate these two protocols into our fading trend based key extraction scheme.

B. Star-based Group Key Extraction Protocol

1) Protocol Description: There are four steps in star-based protocol. We assume there are J nodes in the group. Each group member is represented as P_j, where $j = 1, 2, ...J$.

Step 1: First, the group will randomly select a group member, say P_1, serving as the virtual central node. The secret key will be extracted based on the radio channel between P_1 and another randomly selected device P_2. Each member device needs to estimate the channel measurement of radio channel between P_1 and P_2.

Step 2: Each group member $P_j, j = 2, \cdots, J$ extracts the channel measurement $\hat{r}_{1,j}(k)$ by exchanging probe packets with P_1. In the meanwhile, P_1 also obtains the RSS measurements, $\hat{r}_{P_j,P_1}(k)$ from all P_js.

Step 3: Next, P_1 calculates the DOSS value between the channel it communicates with P_2 and the one it communicates with $P_j, j = 3, \cdots, J$:

$$\delta_{P_j}(k) = \hat{r}_{P_j,P_1}(k) - \hat{r}_{P_2,P_1}(k) \tag{11}$$

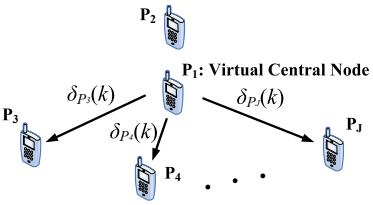


Fig. 7. Illustration of star-based group key extraction protocol

Then $\delta_{P_j}(k)$ is forwarded to P_j so that P_j could estimate the radio channel between P_1 and P_2:

$$\tilde{r}_{P_2,P_1}(k) = \hat{r}_{P_1,P_j}(k) - \delta_{P_j}(k). \tag{12}$$

Step 4: Finally, the group of devices estimate on the channel measurements between P_1 and P_2. The fading-trending based key extraction scheme is then adopted for secret bit extraction.

Figure 7 shows an example of star-based group key extraction protocol with 5 wireless devices in the group.

2) Performance Analysis: According to Equation 12, the estimated channel measurement $\tilde{r}_{P_2,P_1}(k)$ by $P_j, j = 3, \cdots, J$, can be expanded as:

$$\begin{aligned}\tilde{r}_{P_2,P_1}(k) =& \hat{r}_{P_1,P_j}(k) - (\hat{r}_{P_j,P_1}(k) - \hat{r}_{P_2,P_1}(k)) \\ =& n_{P_1,P_j}(k) + n_{P_2,P_1}(k) - n_{P_j,P_1}(k) + r_{P_1,P_2}(k)\end{aligned} \tag{13}$$

Assume the noise in the RSS measurements follows an i.i.d zero-mean Gaussian distribution, $N(0, \sigma^2)$. Then, $\tilde{r}_{P_2,P_1}(k)$ also follows a Gaussian distribution with $N(\hat{r}_{P_2,P_1}(k), 3\sigma^2)$. And the estimated RSS measurements $\tilde{r}_{P_2,P_1}(k)$ by each group member $P_j, j \geq 3$ are all following the same distribution. Thus, the bit mismatch rate between any associated pair of wireless devices in the group, i.e., P_1 and $P_j, j \geq 3$, should maintain at the same level regardless of the device group size.

C. Chain-based Group Key Extraction Protocol

In this protocol, the wireless devices form a virtual chain topology as depicted in Figure 8. We also assume there are J wireless devices in the group. Each group member is represented as P_j, where $j = 1, 2, ..J$.

1) Protocol Description: There are four steps in chain-based group key extraction protocol.

Step 1: A chain-based topology is formed with P_1 and P_J as the head and tail node respectively, and the radio channel between P_1 and P_2 is chosen as the channel for secret bit extraction for all the members. In other words, all the group members need to estimate RSS measurements on the radio channel between P_1 and P_2.

Step 2: Each node extracts the RSS from the probe packet sent by its neighboring nodes. Except that P_1 and P_J has only one RSS measurement $\hat{r}_{P_2,P_1}(k)$ and $\hat{r}_{P_{J-1},P_J}(k)$ respectively, other group member P_j, with $(j \neq 1, J)$, collects two RSS measurements $\hat{r}_{P_{j-1},P_j}$ and $\hat{r}_{P_{j+1},P_j}$.

Step 3: The DOSS value between the two RSS readings measured by $P_j, j = 2, \cdots, J-1$ is given as:

$$\delta_{P_j}(k) = \hat{r}_{P_{j+1},P_j}(k) - \hat{r}_{P_{j-1},P_j}(k) \tag{14}$$

Then $\delta_{P_j}(k)$ is forwarded by traversing P_j's subsequent nodes on the chain until it reaches P_J. In the meanwhile, P_j also estimates $\hat{r}_{P_2,P_1}(k)$ based on the DOSS values forwarded from all its previous nodes as:

$$\tilde{r}_{P_2,P_1}(k) = \hat{r}_{P_{j-1},P_j}(k) - \sum_{t=2}^{j-1} \delta_{P_t}(k). \tag{15}$$

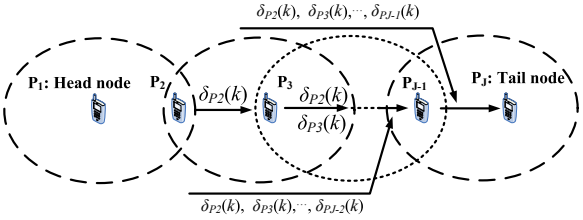


Fig. 8. Illustration of chain-based group key extraction protocol

Step 4: Each group member performs key extraction on the estimated RSS measurements of the wireless channel between P_1 and P_2.

Figure 8 illustrates our proposed protocol with 5 wireless devices in the group. Another possible solution is to utilize all the channel information on the chain by letting each device multicast the DOSS values to both its ancestors and descendants. However, we found that the generated key presents the same secrecy as this simple approach, which only uses the channel information between P_1 and P_2.

2) Performance Analysis: From Equation 15, the estimated value of channel measurement $\hat{r}_{P_2,P_1}(k)$ by P_j can be further derived as:

$$\tilde{r}_{P_2,P_1}(k) = r_{P_2,P_1}(k) + \sum_{t=2}^{j} n_{P_{t-1},P_t}(k) - \sum_{t=2}^{j-1} n_{P_{t+1},P_t}(k) \tag{16}$$

Since we assume the noise on each channel is i.i.d, the distribution of estimated value $\tilde{r}_{P_2,P_1}(k)$ follows $N(r_{P_2,P_1}(k), (2j-3)\sigma^2)$. It shows that the variance of $\tilde{r}_{P_2,P_1}(k)$ grows linearly as j increases. Therefore, the bit mismatch rate will also become higher with larger group size.

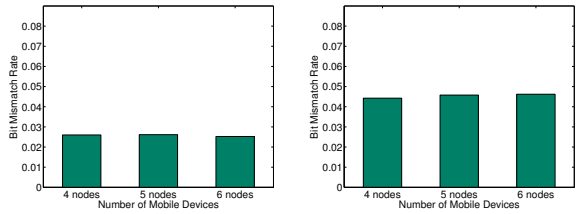
D. Extended Chain-based Group Key Extraction Protocol

When a portion of the group members are isolated from the rest of the group. In this case, non-group device members could be employed to connect the sub-groups. The basic idea is that intra-group communication follows the chain-based group key extraction protocol and inter-group communication uses the relay node assisted collaborative key extraction.

Each sub-group constructs a chain-based topology within itself. The head node and tail node of the intra-group are responsible for communicating with other sub-groups via relay nodes who are non-group members. Thus, an extended chain-based topology consists of both group and non-group members. The devices from the same sub-group follow the chain-based group key extraction protocol, while the non-group member nodes take care of relaying the DOSS values from one sub-group to another.

E. Performance Evaluation

1) Performance of Star-based Group Key Extraction Protocol: In Figure 9, we studied how the number of devices in the group affects the bit mismatch rate during group key extraction. We observed that the bit mismatch rate is stable as the group size increases for both scenarios A and B while maintaining the bit generation rate at 2 bits per measurement. These results are consistent with our theoretical analysis. The slight difference on the bit mismatch rate under each scenario among different group sizes is because the noise on each pairwise channel does not strictly follow identical Gaussian distribution. Furthermore, we found that the performance of our protocol is better under scenario A with pedestrians, again



(a) A (park, with pedestrian) (b) B (park, without pedestrian)

Fig. 9. Performance of star-based group key extraction.

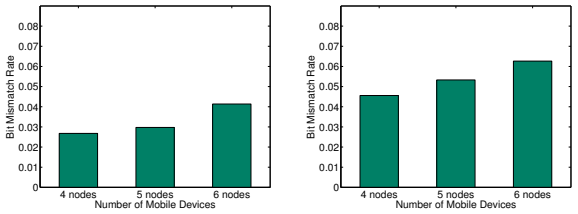
confirming the effectiveness of our fading trend based key extraction scheme.

2) Performance of Chain-based Group Key Extraction Protocol: Figure 10 presents the bit mismatch rate for chain-based group key extraction protocol. We observed that as the group size increases, the bit mismatch rate under both scenarios A and B increases while maintaining the bit generation rate at 2 bits per measurement. For scenario A, the bit mismatch rate increases from 0.034 to 0.058 when the number of group members changes from 4 to 6, whereas scenario B has the bit mismatch rate increasing from 0.056 to 0.073. This is due to the increasing noise variance when DOSS values are accumulated along the chain-based topology. According to the analysis in Section V, these bit mismatch rates are still within the error tolerance range of Golay code.

Due to the space limitation, the performance of extended chain-based group key extraction scheme is not presented.

VII. Conclusions

In this paper, we addressed the problem of performing secret key extraction for a group of wireless devices by exploiting the readily available Received Signal Strength (RSS) in radio channels, without relying on a fixed infrastructure. There are two building blocks in our framework: a secret key extraction scheme that utilizes the trend exhibited in RSS measurements resulted from shadow fading to encode secret bits; and a relay node assisted mechanism that solves the issue when mobile devices are not within each other's communication range. Our fading trend based key extraction scheme can achieve lower bit mismatch rate comparing to existing studies while maintaining a similar key generation rate. Whereas the relay node assisted mechanism uses difference of signal strength to ensure the security of the key extraction and is resilient to the presence of untrusted relay nodes. To enable secure group communication, two protocols, namely *star-based* and *chain-based*, are developed in our framework by exploiting RSS from multiple devices to perform group key generation collaboratively. The star-based collaborative key extraction protocol is designed for the scenarios when the group of wireless devices under consideration is within the communication range of each other, while the chain-based protocol involves handling the scenarios when the group of wireless devices are not within the communication range of each other. Our real experiments in both outdoor (e.g., park and street) and indoor (e.g., office building) environments using a mobile wireless network with multiple MICAz motes confirm the feasibility of leveraging RSS for group key generation among multiple wireless devices. The effectiveness of star-based and chain-based protocols built on top of fading-trend based key extraction and relay node assisted mechanism is demonstrated through our experimental study.



(a) A (park, with pedestrian) (b) B (park, without pedestrian)

Fig. 10. Performance of chain-based group key extraction.

References

[1] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *ACM CCS*, 2007, pp. 401–410.

[2] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776–3784, 2005.

[3] S. Jana, S. Premnath, M. Clark, S. Kasera, N. Patwari, and S. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *ACM MobiCom*, 2009, pp. 321–332.

[4] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *ACM MobiCom*, 2008, pp. 128–139.

[5] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *IEEE ICASSP*, 2008, pp. 3013–3016.

[6] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *IEEE INFOCOM*, 2011.

[7] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, pp. 17–30, 2009.

[8] J. Croft, N. Patwari, and S. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," in *ACM/IEEE ICNP*, 2010, pp. 70–81.

[9] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting multiple-antenna diversity for shared secret key generation in wireless networks," in *IEEE INFOCOM*, 2010, pp. 1–9.

[10] M. Wilhelm, I. Martinovic, and J. Schmitt, "Secret keys from entangled sensor motes: implementation and analysis," in *ACM Wisec*, 2010, pp. 139–144.

[11] J. Hershey, A. Hassan, and R. Yarlagadda, "Unconventional cryptographic keying variable management," *IEEE Transactions on Communications*, vol. 43, no. 1, pp. 3–6, 1995.

[12] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, "On the secrecy capabilities of itu channels," in *IEEE VTC-2007 Fall*, 2007.

[13] R. Wilson, D. Tse, and R. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, 2007.

[14] M. Tope and J. McEachen, "Unconditionally secure communications over fading channels," in *IEEE MILCOM*, 2001.

[15] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in *Proceedings of the 5th ACM workshop on Wireless security*, 2006, pp. 33–42.

[16] C. W. Farrow, "A continuously variable digital delay element," in *IEEE International Symposium on Circuits and Systems*, 1988.

[17] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *IEEE ISIT*, 2006, pp. 2593–2597.

[18] A. Goldsmith, *Wireless Communications*. New York, NY, USA: Cambridge University Press, 2005.

[19] A. R. et al.", "A statistical test suite for random and pseudorandom number generators for cryptographic applications," 2001.

[20] D. Luiz, A. Dasilva, T. Lin, T. Lin, D. Scott, and F. Midkiff, "Mobile ad-hoc network routing protocols: Methodologies and applications," ECE Department, Virginia Tech, Tech. Rep., 2004.

[21] J. H. V. Lint, *Introduction to Coding Theory*, 3rd ed. Secaucus, NJ, USA: Springer-Verlag New York, Inc., 1998.