Collaborative Group Key Extraction Leveraging Received Signal Strength in Real Mobile Environments

Hongbo Liu*, Jie Yang*, Yan Wang*, Yingying Chen*, Can Emre Koksal†

*Department of ECE, Stevens Institute of Technology, Hoboken, NJ 07030

{hliu3, jyang, ywang48, yingying.chen}@stevens.edu

†Department of ECE, Ohio State University, Columbus, OH 43210

koksal@osu.edu

Abstract

Secret key generation among wireless devices using physical layer information of radio channel has been an attractive alternative for ensuring security in mobile environments. Received Signal Strength (RSS) based secret key extraction gains much attention due to its readily availability in wireless infrastructure. However, the problem of using RSS to generate keys among multiple devices to ensure secure group communication in practice remains open. In this work, we propose a framework for collaborative key generation among multiple wireless devices leveraging RSS. 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 are developed to perform collaborative group key generation via star and chain topologies respectively. We further provide the theoretic analysis on the achievable secrecy rate for both star and chain topologies in the presence of an eavesdropper. Our prototype development using MICAz motes and extensive experiments using fading trend based key extraction demonstrate the feasibility of using RSS for group key generation in both indoor and outdoor environments, and concurrently achieving a lower bit mismatch rate compared to existing works.

Index Terms: collaborative secret key extraction, received signal strength, group key extraction, mobile wireless network.

1 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. To ensure the successful deployment and adoption of these emerging applications, secure communication is crucial 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; soldiers carrying out a particular task need to share task plans and real-time monitoring results among themselves, but not to unauthorized parties. Another example is a group of travelers want to limit the sharing of travel plans, journals, pictures and video clips within the group through the peer-to-peer association.

There have been active research in applying traditional cryptographic-based methods such as public key infrastructure (PKI) to wireless networks, these methods, however, 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 de-

vices can extract identical secret bits independently by using the sampled sequence 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, secret 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 focus 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, rather than relying on a key distribution infrastructure. Our initial work on this topic is reported in the conference paper [11] appeared in International Conference on Computer Communications 2012. This journal submission represents a significantly lengthened and enhanced version of the conference paper. The group of wireless devices involved in key generation may not be within each other's communication range. We address this issue by employing a relay node assisted approach and define a metric using difference of RSS to maintain secrecy among devices. To enable secure group communication, two protocols are developed in our framework via *star* and *chain* topologies respectively by exploiting RSS from multiple devices to perform group key generation collaboratively. In particular, the collaborative key extraction via the star topology is designed for scenarios when multiple wireless devices are within each other's communication range (e.g., people traveling together), whereas the approach via the chain topology 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 and soldiers carrying out military tasks).

We analyze the reliability and scalability of the proposed collaborative secret key extraction framework by deriving the maximum achievable group key rate for our scheme under both star and chain topologies. Our analysis provides insights into the amount of drop in key rate as the size of the group grows and enables us to find the best topology the group can form in order to achieve a high key rate. Additionally, to deal with various noises in real-world scenarios, we propose a secret key generation scheme exploiting the trend exhibited in RSS resulted from shadow fading to encode secret bit to work with our group key extraction framework. Our fading trend based key extraction aims to achieve a lower bit mismatch rate comparing to existing works when maintaining the comparable bit generation rate.

We build a system prototype using MICAz motes and conduct extensive experiments in both outdoor (e.g., park and street) and indoor (e.g., office building) environments 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 2. We provide our framework overview and attack model in Section 3. We then describe the building block in our framework, relay node assisted collaborative key extraction, in Section 4. We next present our group key extraction protocols via the star topology in Section 5 and chain topology in Section 6 together with the corresponding theoretic analysis. We discuss the group key extraction under the hybrid topology in Section 7. To deal with various noises in practice, we show how to perform secret key extraction using RSS fading trend in Section 8. We present the prototype implementation and performance evaluation

results in Section 9. Finally, we conclude our work in Section 10.

2 Related Work

There have been active theoretic studies on characterizing secrecy capacity using physical layer information. Wallace et al. [12, 13] presented the mutual information secret bit rate bounds from theoretical channel models. An information theoretic bound for secrecy rate between two nodes in the presence of an eavesdropper node is proposed in [14]. And the theoretic basis for the feasibility of using channel state information in OFDM system for key generation is also explored in [15].

Various radio channel features have been proposed for secret key extraction in literature. Phase difference is first proposed in [16], 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, 17, 18]. Ultra-wideband radios were used in [17] to measure the impulse response, while [4] and [18] 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, 19, 20], multiple antenna diversity [9], and multiple frequencies [10] for secret bit extraction between a pair of wireless devices. In [19], the authors proposed to encode the change in signal envelop during a transmission to encode and decode transmitted messages. [20] used the universal software radio peripheral (USRP) and GNU 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] to improve the bit generation rate. However, none of these RSS based methods considered key generation for multiple wireless devices.

Different from the above works, our group key generation method utilizing readily available RSS measurements is lightweight, and thus is a practical solution for different types of wireless networks. To show the practicality of our proposed method, we analyze the basic information theoretic limits of the achievable key rate (for the analysis of group secret key rates for the general source models, see [21] and [22]) and build a prototype using MICAs motes to evaluate it in both outdoor and indoor environments.

3 System Model

3.1 Framework 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 a particular wireless device from different radio channels. In our framework, instead of using RSS measurements directly, the DOSS values will be utilized to facilitate key extraction.

Our framework consists of two protocols using *star* and *chain* topologies to facilitate reliable secret key generation among multiple wireless devices. The collaborative key extraction protocol for the star topology 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 travelers are visiting the same scenic spot. In this case, 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 not all the wireless devices in the group are within the communication range of each other, our collaborative key extraction protocol using the chain topology 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 approach for chain topology may incur accumulated RSS noise across multiple devices. Our theoretic analysis discusses this issue in Section 6. We also propose a fading trend based secret key extraction method to achieve a lower bit mismatch rate while maintaining the comparable bit generation rate when comparing to existing works.

3.2 Attack Model

We consider a passive adversary, an *Eavesdropper*, who follows the legitimate mobile devices involving in group key extraction. The eavesdropper's channel gain observation is independent of the channel gain observations of every other legitimate mobile device. It overhears all the public discussion during key generation and can obtain the secret key extraction algorithm and corresponding parameters for key generation. The property of spatial decorrelation makes it impossible for the eavesdropper who locates at at least $\lambda/2$ away to measure the same wireless channel as legitimate devices [23]. However, by accumulating the channel information broadcasted during public discussion phase from multiple wireless devices, the eavesdropper may be able to derive part or all of the group secret key as the number of users increase. To counter that, a subsequent privacy amplification phase should be used by the legitimate users.

4 Relay Node Assisted Collaborative Key Extraction

To achieve group key extraction, one fundamental issue needs to be addressed is when a pair of wireless devices are not within each other's communication range. We employ an approach using relay nodes for key extraction when two wireless devices cannot communicate directly. In particular, we design a collaborative key extraction scheme under the assistance of relay nodes. 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.

We note that the secret bit encoding in this scheme can utilize existing secret key extraction methods [4, 7]. Existing secret key generation methods, however, merely use thresholding on RSS measurements alone to extract secret bits, which may encounter various noises in real-world scenarios and consequently suffer from a higher bit mismatch rate during key extraction. To address this issue, we propose a new key extraction method utilizing fading trend to achieve a lower bit mismatch rate. The details of this method is presented in Section 8.

4.1 Basic Protocol

We use three mobile devices, including Alice, Bob and Ryan, to illustrate the basic idea of the relay node assisted secret key extraction scheme.

Step 1: Alice, Bob and Ryan consist of a one-hop network, where Alice and Bob communicate

via the relay node, Ryan.

Step 2: Any two neighboring devices among Alice, Bob and Ryan exchange the probe packets for extracting channel measurement. The RSS measured at Ryan from its neighboring devices Alice and Bob are $\hat{Y}_{A,R}(t)$ and $\hat{Y}_{B,R}(t)$, respectively. Alice and Bob obtain the RSS measurements $\hat{Y}_{R,A}(t)$ and $\hat{Y}_{R,B}(t)$ from Ryan, respectively.

Step 3: Ryan calculates the DOSS values based on the radio channels it uses to communicate with Alice and Bob, $\delta_R(t) = \hat{Y}_{B,R}(t) - \hat{Y}_{A,R}(t)$, and then forwards it to Bob.

Step 4: Once the DOSS values from Ryan arrives at Bob, Bob is able to estimate the radio channel between Alice and Ryan: $Y_{R,A}(t) = \hat{Y}_{R,B}(t) + \delta_R(t)$. Since Alice can directly measure the radio channel between Ryan and Alice: $\hat{Y}_{R,A}(t)$, both Alice and Bob have obtained the common channel information of radio channel between Alice and Ryan. 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 node, Ryan, send the DOSS values to both Alice and Bob. However, we find that the generated key presents the same secrecy as this simple approach, which only uses the channel information between Alice and Ryan. Figure 1 illustrates our proposed protocol by employing 1 relay node, Ryan. The protocol can be easily extended to the case with multiple relay nodes, which is further discussed in Section 6. We note that this protocol is generic to any key extraction algorithms using RSS. In this work, we apply the fading trend based scheme introduced in Section 8 to our group key extraction framework and compare its performance with exiting method using RSS.

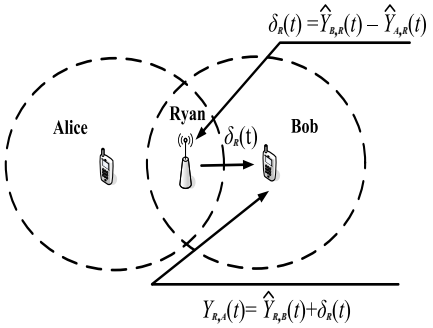


Figure 1: Illustration of relay node assisted collaborative key extraction.

4.2 Security Analysis

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.

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.

5 Group Key Extraction via the Star Topology

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 inside 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. In this scenario, we randomly 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 topology, where nodes are sequentially connected. In this section, we focus our attention on presenting the group key extraction protocol via the star topology and defer the discussion on the group key extraction protocol via the chain topology in Section 6.

5.1 Protocol Design

There are four steps in the protocol via the star topology. We assume there are n nodes in the group. Each group member is represented as j, where $j = c, 1, 2, ..., n-1$.

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

Step 2: Each group member $j, j = 1, \cdots, n-1$ extracts the channel measurement $\hat{Y}_{c,j}(t)$ by exchanging probe packets with 1. In the meanwhile, c also obtains the RSS measurements, $\hat{Y}_{j,c}(t)$ from all j's.

Step 3: Next, c calculates the DOSS value between the channel it communicates with 1 and the one it communicates with $j, j = 2, \cdots, n-1$, $\delta_j(t) = \hat{Y}_{j,c}(t) - \hat{Y}_{1,c}(t)$. Then $\delta_j(t)$ is forwarded to j so that j could estimate the radio channel between c and 1, $Y_{1,c}(t) = \hat{Y}_{c,j}(t) - \delta_j(t)$.

Step 4: Finally, the group of devices estimate on the channel measurements between 1 and c, and perform secret bit extraction.

Figure 2 shows an example of the group key extraction protocol via the star topology with 5 wireless devices in the group.

5.2 Achievable Group Secret Key Rate with the Star Topology

We next analyze the achievable key rate of our scheme under the network via the star topology when an eavesdropper presents. An eavesdropper may accumulate the exchanged information on the public wireless channel and derive the knowledge for key extraction statistically. We denote the virtual central node with c, the eavesdropper node with e and the other nodes with a number in $\{1, \ldots, n-1\}$. We start our analyses with merely the ergodicity assumption for the channel gains,

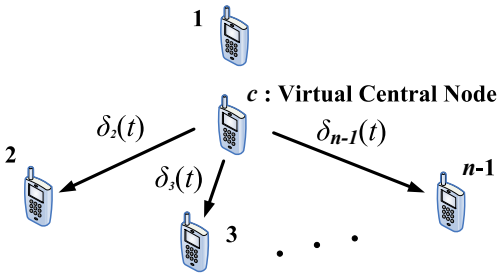


Figure 2: Illustration of the group key extraction protocol via the star topology.

$Y_{i,j}(t)$, but for the sake of simplicity, our evaluations will be for the i.i.d.[1] scenario for all channels $i, j \in \{c, e, 1, \ldots, n-1\}$. The nodes make noisy observations of the gains of particular channels in each time slot $t \in \{1, \ldots, T\}$. We denote the observation of node $j \in \{c, 1, \ldots, n-1\}$ of channel (j, i) in slot. We consider a favorable scenario for the eavesdropper, in particular, the eavesdropper has noiseless observation of $Y_{i,e}(t)$ for all i's and t. In vector notation, we denote any random sequence $Z(t)$ with boldface $\mathbf{Z} \triangleq [Z(1)\ Z(2)\ \cdots\ Z(T)]$. Also, let the entire sequence of observations of e be matrix $\mathscr{Y}^e \triangleq [\mathbf{Y}_{1,e}\ \mathbf{Y}_{2,e}\ \cdots\ \mathbf{Y}_{(n-1),e}]$. At the end of each slot, there occurs a public discussion phase, in which certain nodes broadcast specific information related to the observations. We assume that the eavesdropper overhears all such broadcasts without an error. Let us denote the sequence of public signals broadcast at the end of slot t with $\mathbf{S}_{\text{pub}}(t)$ and the entire set of sequence of publicly shared signals with matrix $\mathscr{S}_{\text{pub}}$. After the public discussion phase, the common key is generated via privacy amplification. Next, we derive the maximum achievable group key rate between the nodes as $T \to \infty$ for the star and the chain topologies.

With the star topology, in each time slot, each node observes the gain of its channel to the virtual central node and the virtual central node observes its gain to each node. The virtual central node c chooses one of the users, such as 1, and uses the observed channel gain to generate the group key. To provide information on $Y_{c,1}(t)$ to other users, in the public discussion phase, node c broadcasts the sequence [2] $\mathbf{S}_{\text{pub}}(t) = [\delta_2(t), \delta_3(t), \cdots, \delta_{n-1}(t)] = [(\hat{Y}_{1,c}(t) - \hat{Y}_{2,c}(t))\ (\hat{Y}_{1,c}(t) - \hat{Y}_{3,c}(t))\ \cdots\ (\hat{Y}_{1,c}(t) - \hat{Y}_{(n-1),c}(t))]$, overheard by all nodes. We start the analysis by stating the amount of common information between node j and node c before privacy amplification. Here we use notation $\mathscr{S}_{\text{pub}} = [\mathbf{S}_{\text{pub}}(1)\ \cdots\ \mathbf{S}_{\text{pub}}(T)]$. The asymptotic common information rate [24], [25] and [26] as $T \to \infty$ can be written as:

$$R_j = \liminf_{T\to\infty} \frac{1}{T} I([\hat{\mathbf{Y}}_{1,c}, \ldots, \hat{\mathbf{Y}}_{n-1,c}]; [\mathscr{S}_{\text{pub}}, \hat{\mathbf{Y}}_{c,j}]) \tag{1}$$

The "collaborative" group information rate before privacy amplification is limited by the worst

[1] Note that the analysis can be easily generalized to the case with asymmetric channels.

[2] Note that this is a sequence of vectors the associated set of observations can be transmitted in time sequentially, as the observations are made, rather than all at once.

node, i.e.,

$$R_{\text{star}} = \min_{1 \le j \le n-1} R_j. \tag{2}$$

Note that the above rate is the amount of common information shared among the legitimate nodes and it does not consider secrecy from the eavesdropper. *After* privacy amplification, the achievable joint *secret* key rate [24], [25] and [26] is:

$$R_{\text{star}}^{\text{sec}} = R_{\text{star}} - \limsup_{T \to \infty} \frac{1}{T} I([\hat{\mathbf{Y}}_{1,c}, \ldots, \hat{\mathbf{Y}}_{n-1,c}]; [\mathscr{S}_{\text{pub}}, \mathscr{Y}^e]) \tag{3}$$

Note that Eq. 3 is general for any ergodic (possibly asymmetric) random process for the channel gain and the observation noise process. With the i.i.d. assumption on the channel gain and the observation noise processes, in the following evaluation of the joint secret key rate, we obtain the group key rate by analyzing an arbitrary user, say user 2, other than user 1. Indeed, since node c uses $Y_{1,c}$ to generate the key, $R_j = R_i \le R_1$ for all users $i, j \ne 1$. Also, due to the i.i.d. assumption, it is sufficient to focus on a single time instant. The secret key rate as given in Eq. (3) can be simply written after dropping the time indices as:

$$\begin{aligned}
R_{\text{star}}^{\text{sec}} &= I([\hat{Y}_{1,c}, \ldots, \hat{Y}_{(n-1),c}]; [\mathbf{S}_{\text{pub}}, \hat{Y}_{c,2}^2]) - I([\hat{Y}_{1,c}, \ldots, \hat{Y}_{(n-1),c}]; [\mathbf{S}_{\text{pub}}, Y_{c,e}, Y_{1,e}, \ldots, Y_{(n-1),e}]) && (4)\\
&= I([\hat{Y}_{1,c}, \ldots, \hat{Y}_{(n-1),c}]; \hat{Y}_{c,2} \mid \mathbf{S}_{\text{pub}}) + I([\hat{Y}_{1,c}, \ldots, \hat{Y}_{(n-1),c}]; \mathbf{S}_{\text{pub}}) \\
&\qquad - I([\hat{Y}_{1,c}, \ldots, \hat{Y}_{(n-1),c}]; Y_{c,e}, Y_{1,e}, \ldots, Y_{(n-1),e} \mid \mathbf{S}_{\text{pub}}) - I([\hat{Y}_{1,c}, \ldots, \hat{Y}_{(n-1),c}]; \mathbf{S}_{\text{pub}}) && (5)\\
&= I([\hat{Y}_{1,c}, \ldots, \hat{Y}_{(n-1),c}]; \hat{Y}_{c,2} \mid \mathbf{S}_{\text{pub}}) && (6)\\
&= I(\hat{Y}_{1,c}; \hat{Y}_{c,2} \mid \mathbf{S}_{\text{pub}}) + I([\hat{Y}_{2,c}, \ldots, \hat{Y}_{(n-1),c}]; \hat{Y}_{c,2} \mid \hat{Y}_{1,c}, \mathbf{S}_{\text{pub}}) && (7)\\
&= I(\hat{Y}_{1,c}; \hat{Y}_{c,2} \mid \mathbf{S}_{\text{pub}}) && (8)\\
&= h(\hat{Y}_{1,c} \mid \mathbf{S}_{\text{pub}}) - h(\hat{Y}_{1,c} \mid \mathbf{S}_{\text{pub}}, \hat{Y}_{c,2}) \\
&= h(\mathbf{S}_{\text{pub}} \mid \hat{Y}_{1,c}) + h(\hat{Y}_{1,c}) - h(\mathbf{S}_{\text{pub}}) - \left[h(\mathbf{S}_{\text{pub}}, \hat{Y}_{c,2} \mid \hat{Y}_{1,c}) + h(\hat{Y}_{1,c}) - h(\mathbf{S}_{\text{pub}}, \hat{Y}_{c,2})\right] && (9)\\
&= h(\hat{Y}_{1,c} - \hat{Y}_{2,c}, \ldots, \hat{Y}_{1,c} - \hat{Y}_{(n-1),c} \mid \hat{Y}_{1,c}) - h(\hat{Y}_{1,c} - \hat{Y}_{2,c}, \ldots, \hat{Y}_{1,c} - \hat{Y}_{(n-1),c}) \\
&\qquad - h(\hat{Y}_{1,c} - \hat{Y}_{2,c}, \ldots, \hat{Y}_{1,c} - \hat{Y}_{(n-1),c}, \hat{Y}_{c,2} \mid \hat{Y}_{1,c}) + h(\hat{Y}_{1,c} - \hat{Y}_{2,c}, \ldots, \hat{Y}_{1,c} - \hat{Y}_{(n-1),c}, \hat{Y}_{c,2}) \\
&= h(-\hat{Y}_{2,c}, \ldots, -\hat{Y}_{(n-1),c}) - h(\hat{Y}_{1,c} - \hat{Y}_{2,c}, \ldots, \hat{Y}_{1,c} - \hat{Y}_{(n-1),c}) \\
&\qquad - h(-\hat{Y}_{2,c}, \ldots, -\hat{Y}_{(n-1),c}, \hat{Y}_{c,2}) + h(\hat{Y}_{1,c} - \hat{Y}_{2,c}, \ldots, \hat{Y}_{1,c} - \hat{Y}_{(n-1),c}, \hat{Y}_{c,2}) && (10)\\
&= h(-\hat{Y}_{2,c}, \ldots, -\hat{Y}_{(n-1),c}) - h(\hat{Y}_{1,c} - \hat{Y}_{2,c}, \ldots, \hat{Y}_{1,c} - \hat{Y}_{(n-1),c}) - h(-\hat{Y}_{3,c}, \ldots, -\hat{Y}_{(n-1),c}) \\
&\qquad - h(-\hat{Y}_{2,c}, \hat{Y}_{2,c}) + h(\hat{Y}_{1,c} - \hat{Y}_{2,c}, \ldots, \hat{Y}_{1,c} - \hat{Y}_{(n-1),c}, \hat{Y}_{c,2}), && (11)
\end{aligned}$$

where (5) follows by the application of chain rule on both terms of the right side of (4), (6) follows since $\hat{Y}_{j,c}$ is independent of $(Y_{c,e}, Y_{1,e}, \ldots, Y_{(n-1),e})$ for all j's, (7) follows by chain rule, and (8) follows since, given $\hat{Y}_{1,c}$ and $\mathbf{S}_{\text{pub}}$, one can determine $\hat{Y}_{j,c}$ for all j's with probability 1, (9) follows from the chain rule for entropies, (10) follows since, given $\hat{Y}_{1,c}$, all the uncertainty in $\hat{Y}_{1,c} - \hat{Y}_{j,c}$ is in $\hat{Y}_{j,c}$ and that $\hat{Y}_{1,c}$ and $\hat{Y}_{2,c}$ are independent, and (11) is by the chain rule.

Now, we evaluate the key rate for the scenario in which the channels are i.i.d. Rayleigh fading. Thus, $Y_{j,i}(t)$ is 0-mean circularly symmetric complex Gaussian with an identical variance σ_Y^2 per dimension for all channels $i, j \in \{c, e, 1, \ldots, n-1\}$. Also, in our evaluations, we assume $W_{i,j}(t)$ to be i.i.d., 0-mean circularly symmetric complex Gaussian with a variance σ_W^2 per dimension for all $i, j \in \{c, 1, \ldots, n-1\}$. Finally, let $\gamma_m \triangleq \frac{\sigma_Y^2}{\sigma_W^2}$ be the measurement SNR. With these assumptions, all five differential entropies in Eq. (11) are those of Gaussian random vectors. In particular, let $\mathbf{1}_{n\times n}$ and $\mathbf{I}_{n\times n}$ denote respectively, the matrix of all 1's and the identity matrix of size $n \times n$. Then, we can write the following for these vectors:

1. $\left[-\hat{Y}_{2,c}, \ldots, -\hat{Y}_{(n-1),c}\right] \sim \mathcal{N}\left(\mathbf{0}, \sigma_Y^2\left(1+\gamma_m^{-1}\right)\mathbf{I}_{(n-2)\times(n-2)}\right)$
2. $\left[\hat{Y}_{1,c} - \hat{Y}_{2,c}, \ldots, \hat{Y}_{1,c} - \hat{Y}_{(n-1),c}\right] \sim \mathcal{N}\left(\mathbf{0}, \sigma_Y^2\left(1+\gamma_m^{-1}\right)\left(\mathbf{I}_{(n-2)\times(n-2)} + \mathbf{1}_{(n-2)\times(n-2)}\right)\right)$
3. $\left[-\hat{Y}_{3,c}, \ldots, -\hat{Y}_{(n-1),c}\right] \sim \mathcal{N}\left(\mathbf{0}, \sigma_Y^2\left(1+\gamma_m^{-1}\right)\mathbf{I}_{(n-3)\times(n-3)}\right)$
4. $\left[-\hat{Y}_{2,c}, \hat{Y}_{c,2}\right] \sim \mathcal{N}\left(\mathbf{0}, \sigma_Y^2 \begin{bmatrix} 1+\gamma_m^{-1} & -1 \\ -1 & 1+\gamma_m^{-1} \end{bmatrix}\right)$
5. $\left[\hat{Y}_{1,c} - \hat{Y}_{2,c}, \ldots, \hat{Y}_{1,c} - \hat{Y}_{(n-1),c}, \hat{Y}_{c,2}\right] \sim \mathcal{N}\left(\mathbf{0}, K_{\mathbf{Z}}\right)$, where the entries of covariance matrix $K_{\mathbf{Z}}$ in the top left portion with coordinates $[1, n-2] \times [1, n-2]$ are identical to $\sigma_Y^2\left(1+\gamma_m^{-1}\right)\left(\mathbf{I}_{(n-2)\times(n-2)} + \mathbf{1}_{(n-2}\right.$ the entries in the $(n-1)$st column and the $(n-1)$st row are all 0, except for $K_{\mathbf{Z}}(2, n-1) = K_{\mathbf{Z}}(n-1, 2) = -\sigma_Y^2$ and $K_{\mathbf{Z}}(n-1, n-1) = \sigma_Y^2\left(1+\gamma_m^{-1}\right)$

Noting that $\det\left(\mathbf{1}_{n\times n} + \mathbf{I}_{n\times n}\right) = n+1$ and[3] $\det\left(K_{\mathbf{Z}}\right) = \sigma_Y^{2(n-1)}\left[n - 1 - \frac{n-2}{\left(1+\gamma_m^{-1}\right)^2}\right]$, we can write

[3] $\det(K_{\mathbf{Z}})$ can be found by 1) multiplying the last row and the last column by -1, 2) shifting the rows by 1 so that the jth row becomes $(j+1)$st row and $(n-1)$st row becomes the first row and likewise for the columns, 3) a cofactor expansion.

$$R_{\text{star}}^{\text{sec}} = \log\left[\left(2\pi e\sigma_Y^2\left(1+\gamma_m^{-1}\right)\right)^{n-2}\right] - \log\left[\left(2\pi e\sigma_Y^2\left(1+\gamma_m^{-1}\right)\right)^{n-2}\cdot(n-1)\right] - \log\left[\left(2\pi e\sigma_Y^2\left(1+\gamma_m^{-1}\right)\right)^{n-3}\right] - \log\left[\left(2\pi e\sigma_Y^2\right)^2\left[\left(1+\gamma_m^{-1}\right)^2-1\right]\right]$$
$$+\log\left[\left(2\pi e\sigma_Y^2\left(1+\gamma_m^{-1}\right)\right)^n\left(n-1-\frac{n-2}{\left(1+\gamma_m^{-1}\right)^2}\right)\right] = \log\left(1+\frac{1/(n-1)}{\left(1+\gamma_m^{-1}\right)^2-1}\right).$$

The achievable secret key rate is illustrated in Fig. 4. As one can see from the figures, for a given measurement SNR, the key rates drop significantly from the initial value (for a few users) as the number of users increase to 10. However, as the measurement SNR is increased (e.g., using more powerful beacon signals to measure the channels), this loss can be compensated to some extent.

From the equation above, we observe that the achievable group key rate $R_{\text{star}}^{\text{sec}}$ in star topology only depends on the group size n and SNR γ_m on wireless channel. As the group size increases, the achievable group key rate decreases, indicating that a larger group is more vulnerable to the eavesdropper attacks. This is because more channel statistical information, embedded in the DOSS information, is exposed to the attacker during public discussion phase among the group members. Furthermore, if SNR on radio channel increases, the achievable group key rate becomes higher. Higher SNR would result in less ambiguity on group key extraction, which benefits the key agreement among group members and is independent from the potential key extraction of the attacker.

6 Group Key Extraction via the Chain Topology

Under the scenarios when not all the wireless devices in the group are within the communication range of each other, our collaborative key extraction protocol via the chain topology constructs a virtual topology where the devices in the group under consideration are connected with one another like a chain as depicted in Figure 3. Each device in the chain involves to pass the corresponding DOSS values to its neighbor device in the next step of the chain. We note that the virtual chain topology is a special case of the tree topology, i.e., hybrid of star and chain topologies, and represents the worst case scenario in terms of accumulated noise during group key extraction using RSS.

6.1 Protocol Design

We assume there are n wireless devices in the group. Each group member is represented as j, where $j = c, 1, 2, ..., n-1$. There are four steps in group key extraction protocol via the chain topology.

Step 1: A chain topology is formed with c and $n-1$ as the head and tail node respectively, and the radio channel between c and 1 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 c and 1.

Step 2: Each node extracts the RSS from the probe packet sent by its neighboring nodes. Except that c and $n-1$ has only one RSS measurement $\hat{Y}_{1,c}(t)$ and $\hat{Y}_{n-2,n-1}(t)$ respectively, each of other group member j, with $(j \neq 1, n-1)$, collects two RSS measurements $\hat{Y}_{j-1,j}$ and $\hat{Y}_{j+1,j}$.

Step 3: The DOSS value between the two RSS readings measured by $j, j = 1, \cdots, n-2$ is given as: $\delta_j(t) = \hat{Y}_{j+1,j}(t) - \hat{Y}_{j-1,j}(t)$. Then $\delta_j(t)$ is forwarded by traversing j's subsequent nodes on the chain until it reaches n. In the meanwhile, j also estimates $\hat{Y}_{1,c}(t)$ based on the DOSS values forwarded from all its previous nodes as: $Y_{1,c}(t) = \hat{Y}_{j-1,j}(t) - \sum_{k=1}^{j-1} \delta_k(t)$.

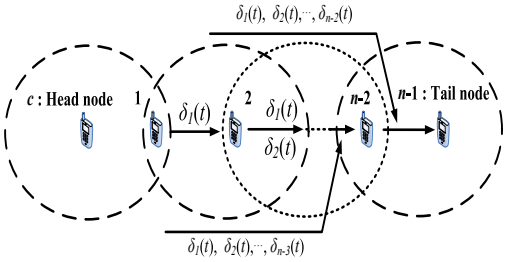


Figure 3: Illustration of group key extraction protocol via the chain topology.

Step 4: Each group member performs key extraction on the estimated RSS measurements of the wireless channel between c and 1.

Figure 3 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 find that the generated key presents the same secrecy as this simple approach, which only uses the channel information between c and 1.

6.2 Achievable Group Secret Key Rate with the Chain Topology

For the chain topology, in addition to the presence of the eavesdropper, noise accumulation embedded in DOSS propagation will also impact the group key generation rate. Under such a topology, we denote the beginning node in the chain topology as c, the eavesdropper node as e and the other nodes as $\{1,\ldots,n-1\}$ With the chain topology, all nodes are ordered from the node c to $n-1$ toward the tail of the chain. In each time slot, each node observes the gain of its channel to its immediate neighbors. For instance, head node c observes $\hat{Y}_{1,c}(t)$ in time slot t, whereas each node j observes both $\hat{Y}_{(j-1),j}(t)$ and $\hat{Y}_{(j+1),j}(t)$. Similar to the star topology, $Y_{c,1}(t)$ is used to generate the group key and the eavesdropper has noiseless observation of $Y_{j,e}(t)$ for all j's and t in the chain topology as well. Node 1 initiates the public discussion phase at the end of slot t and broadcasts $\delta_1(t) = \hat{Y}_{2,1}(t) - \hat{Y}_{c,1}(t)$. Then node 2 relays this information as well as $\delta_2(t) = \hat{Y}_{3,2}(t) - \hat{Y}_{1,2}(t)$ to node 3. Each node along the chain broadcasts all the information as well as the difference between its observations. The public discussion for time t ends when node $n-1$ receives $\mathbf{S}_{\text{pub}}(t) = [\delta_1(t), \delta_2(t), \ldots, \delta_{n-2}(t)] = [\hat{Y}_{2,1}(t) - \hat{Y}_{c,1}(t),\ \hat{Y}_{3,2}(t) - \hat{Y}_{1,2}(t), \ldots\ , \hat{Y}_{(n-1),(n-2)}(t) - \hat{Y}_{(n-3),(n-2)}(t)]$. Note that for $n = 3$, $\mathbf{S}_{\text{pub}} = \hat{Y}_{2,1}(t) - \hat{Y}_{c,1}(t)$ is a scalar and for $n = 2$ (only node c and 1 are existent), there occurs no public discussion. Similar to the star topology, we use notation $\mathscr{S}_{\text{pub}} = [\mathbf{S}_{\text{pub}}(1)\ \cdots\ \mathbf{S}_{\text{pub}}(T)]$.

We start the analysis by stating the amount of common information between nodes j and c before privacy amplification. The asymptotic common information rate [24], [25] and [26] as $T \to \infty$ can be written as:

$$R_j = \liminf_{T\to\infty} \frac{1}{T} I(\hat{\mathbf{Y}}_{1,c}; \mathscr{S}_{\text{pub}}, \hat{\mathbf{Y}}_{(j-1),j}, \hat{\mathbf{Y}}_{(j+1),j}) \tag{12}$$

for all $j \neq n-1$ and

$$R_j = \liminf_{T\to\infty} \frac{1}{T} I(\hat{\mathbf{Y}}_{1,c}; \mathscr{S}_{\text{pub}}, \hat{\mathbf{Y}}_{(n-2),(n-1)}) \tag{13}$$

for node $n-1$. The group information rate is limited by the worst node, thus,

$$R_{\text{chain}} = \min_{1 \le j \le n-1} R_j = R_{n-1} \tag{14}$$

since $n-1$ is at the farthest edge of the network from node c. After privacy amplification, the achievable joint *secret* key rate [24], [25] and [26] is:

$$R_{\text{chain}}^{\text{sec}} = R_{\text{chain}} - \limsup_{T \to \infty} \frac{1}{T} I(\hat{\mathbf{Y}}_{1,c}; \mathscr{S}_{\text{pub}}, Y_{c,e}, Y_{1,e}, \ldots, Y_{(n-1),e}) \tag{15}$$

Similar to the analysis of the star topology, with the i.i.d. assumption on the channel gain and the observation noise process, the secret key rate as given in Eq. (15) can be simply written after dropping the time indices as:

$$\begin{aligned}
R_{\text{chain}}^{\text{sec}} &= I(\hat{Y}_{1,c}; \mathbf{S}_{\text{pub}}, \hat{Y}_{(n-2),(n-1)}) - I(\hat{Y}_{1,c}; \mathbf{S}_{\text{pub}}, Y_{c,e}, Y_{1,e}, \ldots, Y_{(n-1),e}) && (16)\\
&= I(\hat{Y}_{1,c}; \hat{Y}_{(n-2),(n-1)}) \mid \mathbf{S}_{\text{pub}}) + I(\hat{Y}_{1,c}; \mathbf{S}_{\text{pub}}) \\
&\qquad - I(\hat{Y}_{1,c}; Y_{c,e}, Y_{1,e}, \ldots, Y_{(n-1),e} \mid \mathbf{S}_{\text{pub}}) - I(\hat{Y}_{1,c}; \mathbf{S}_{\text{pub}}) && (17)\\
&= I(\hat{Y}_{1,c}; \hat{Y}_{(n-2),(n-1)}) \mid \mathbf{S}_{\text{pub}}) && (18)\\
&= h(\hat{Y}_{1,c} \mid \mathbf{S}_{\text{pub}}) - h(\hat{Y}_{1,c} \mid \mathbf{S}_{\text{pub}}, \hat{Y}_{(n-2),(n-1)}) \\
&= -h(\mathbf{S}_{\text{pub}}) + h(\hat{Y}_{1,c}, \mathbf{S}_{\text{pub}}) + h(\mathbf{S}_{\text{pub}}, \hat{Y}_{(n-2),(n-1)}) - h(\hat{Y}_{1,c}, \mathbf{S}_{\text{pub}}, \hat{Y}_{(n-2),(n-1)}), && (19)
\end{aligned}$$

where (17) follows by the application of chain rule on both terms of the right side of (16), (18) follows since $\hat{Y}_{1,c}$ is independent of $[Y_{c,e}, Y_{1,e}, \ldots, Y_{(n-1),e}]$, and (19) follows from the chain rule for entropies. Identical to the star topology, now, we evaluate the key rate for the scenario in which the channels are i.i.d. Rayleigh fading with the same parameters given in Section 5.2.

Hence, all four differential entropies in Eq. (19) are those of Gaussian random vectors as characterized in what follows:

1. $\mathbf{S}_{\text{pub}} = \left[\hat{Y}_{2,1} - \hat{Y}_{c,1},\ \hat{Y}_{3,2} - \hat{Y}_{1,2}, \ldots, \hat{Y}_{(n-1),(n-2)} - \hat{Y}_{(n-3),(n-2)}\right] \sim \mathscr{N}\left(\mathbf{0}, K_{\mathbf{S}_{\text{pub}}}\right)$, where $K_{\mathbf{S}_{\text{pub}}}$ is an $(n-2) \times (n-2)$ covariance matrix with diagonal entries, $K_{\mathbf{S}_{\text{pub}}}(j,j) = 2\sigma_Y^2(1+\gamma^{-1})$ and $K_{\mathbf{S}_{\text{pub}}}(j,j+1) = K_{\mathbf{S}_{\text{pub}}}(j+1,j) = -\sigma_Y^2$ for all $j \in \{1, \ldots, n-3\}$. All other enties of $K_{\mathbf{S}_{\text{pub}}}$ are identical to 0.

2. $\left[\hat{Y}_{1,c}, \mathbf{S}_{\text{pub}}\right] \sim \mathscr{N}\left(\mathbf{0}, K_{\hat{Y}_{1,c}, \mathbf{S}_{\text{pub}}}\right)$, where $K_{\hat{Y}_{1,c}, \mathbf{S}_{\text{pub}}}$ is an $(n-1) \times (n-1)$ covariance matrix, where the bottom right portion with entries $[2, n-1] \times [2, n-1]$ is identical to $K_{\mathbf{S}_{\text{pub}}}$, and the first row and the first column are as follows: $K_{\hat{Y}_{1,c}, \mathbf{S}_{\text{pub}}}(1,1) = \sigma_Y^2(1+\gamma^{-1})$, $K_{\hat{Y}_{1,c}, \mathbf{S}_{\text{pub}}}(2,1) = K_{\hat{Y}_{1,c}, \mathbf{S}_{\text{pub}}}(1,2) = -\sigma_Y^2$, and the rest of the first column and the first row are all 0's.

3. $\left[\mathbf{S}_{\text{pub}}, \hat{Y}_{(n-2),(n-1)}\right] \sim \mathcal{N}\left(\mathbf{0}, K_{\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}\right)$, where $K_{\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}$ is an $(n-1)\times(n-1)$ covariance matrix, where the top left portion with entries $[1,n-2]\times[1,n-2]$ is identical to $K_{\mathbf{S}_{\text{pub}}}$, and the last row and the last column are as follows: $K_{\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}(n-1,n-1) = \sigma_Y^2(1+\gamma^{-1})$, $K_{\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}(n-2,n-1) = K_{\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}(n-1,n-2) = \sigma_Y^2$, and the rest of the last column and the last row are all 0's.

4. $\left[\hat{Y}_{1,c}, \mathbf{S}_{\text{pub}}, \hat{Y}_{(n-2),(n-1)}\right] \sim \mathcal{N}\left(\mathbf{0}, K_{\hat{Y}_{1,c},\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}\right)$, where $K_{\hat{Y}_{1,c},\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}$ is an $n\times n$ covariance matrix, where the top left portion with entries $[(1,n-1]\times[1,n-1]$ is identical to $K_{\hat{Y}_{1,c},\mathbf{S}_{\text{pub}}}$, and the last row and the last column are as follows: $K_{\hat{Y}_{1,c},\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}(n,n) = \sigma_Y^2(1+\gamma^{-1})$, $K_{\hat{Y}_{1,c},\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}(n-1,n) = K_{\hat{Y}_{1,c},\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}(n,n-1) = \sigma_Y^2$, and the rest of the last column and the last row are all 0's.

The determinants of the above covariance matrices can be calculated recursively as follows. Firstly, let us define $d_n^{(1)} \triangleq \det\left(\frac{1}{\sigma_Y^2}K_{\mathbf{S}_{\text{pub}}}\right)$ for the n-user system. One can observe from the cofactor expansion of $\frac{1}{\sigma_Y^2}K_{\mathbf{S}_{\text{pub}}}$ that, $d_n^{(1)} = 2(1+\gamma_m^{-1})d_{n-1}^{(1)} - d_{n-2}^{(1)}$. With the initial conditions $d_2^{(1)} = 4(1+\gamma_m^{-1})^2 - 1$ and $d_1^{(1)} = 2(1+\gamma_m^{-1})$, we can evaluate $\det\left(K_{\mathbf{S}_{\text{pub}}}\right) = \sigma_Y^{2(n-2)}d_n^{(1)}$ for any given $n>2$, recursively. Similarly, let us define $d_n^{(2)} \triangleq \det\left(\frac{1}{\sigma_Y^2}K_{\hat{Y}_{1,c},\mathbf{S}_{\text{pub}}}\right)$ (see Item 2) and expand $\frac{1}{\sigma_Y^2}K_{\hat{Y}_{1,c},\mathbf{S}_{\text{pub}}}$ via a cofactor expansion, we can find the recursive relation $d_n^{(2)} = (1+\gamma_m^{-1})d_n^{(1)} - d_{n-1}^{(1)}$. It is not difficult to see for $d_n^{(3)} \triangleq \det\left(\frac{1}{\sigma_Y^2}K_{\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}\right)$ that $d_n^{(3)} = d_n^{(2)}$ (by multiplying the final row and column of $d_n^{(3)}$ by -1, we can obtain a symmetric version of $d_n^{(2)}$). Lastly, using a similar cofactor expansion and utilizing the above observations, one can also deduce that, for $d_n^{(4)} \triangleq \det\left(\frac{1}{\sigma_Y^2}K_{\hat{Y}_{1,c},\mathbf{S}_{\text{pub}},\hat{Y}_{(n-2),(n-1)}}\right)$, the following recursive relationship holds: $d_n^{(4)} = (1+\gamma_m^{-1})d_n^{(2)} - d_{n-1}^{(2)}$. Thus, all the determinants can be calculated recursively. Combining all of the above, we have:

$$\begin{aligned} R_{\text{chain}}^{\text{sec}} &= 2\log\left[\left(2\pi e\sigma_Y^2\right)^{n-1}\left((1+\gamma_m^{-1})d_n^{(1)} - d_{n-1}^{(1)}\right)\right] - \log\left[\left(2\pi e\sigma_Y^2\right)^{n-2}d_n^{(1)}\right] - \log\left[\left(2\pi e\sigma_Y^2\right)^{n}\left((1+\gamma_m^{-1})d_n^{(2)} - d_{n-1}^{(2)}\right)\right] \\ &= \log\left(\frac{\left[(1+\gamma_m^{-1})d_n^{(1)} - d_{n-1}^{(1)}\right]^2}{d_n^{(1)}\left[(1+\gamma_m^{-1})d_n^{(2)} - d_{n-1}^{(2)}\right]}\right), \end{aligned} \tag{20}$$

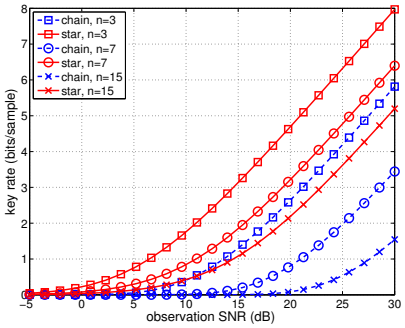
For $R_{\text{chain}}^{\text{sec}}$, similar trend on the achievable group key rate via the chain topology can be observed as in the star topology when varying the group size n and the SNR γ_m. In addition, when the DOSS

value propagates along the chain topology, the noisy measurements will be accumulated. Thus, the observation of SNR keeps decreasing as the group size increases. Group key extraction via the star topology does not involve much noise accumulation, since it has the maximum hop equal to one. Therefore, the decreasing SNR makes the achievable group key rate in the chain topology decrease much faster than that in the star topology.

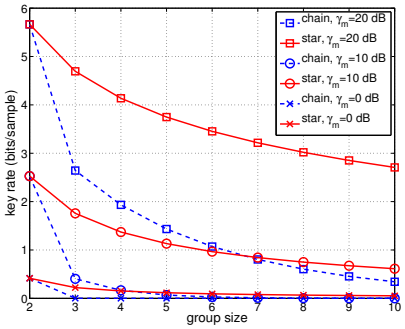
7 Discussion on Group Key Extraction via the Hybrid Topology

In Fig. 4, we illustrate the achievable group key rates, $R^{\text{sec}}_{\text{star}}$ and $R^{\text{sec}}_{\text{chain}}$ as a function of the observation SNR, γ_r, and the group size, n.

As expected, the group key rate decreases with the group size and increases with the observation SNR[4]. The important observation is that, the key rate decreases much faster with the chain topology as shown in Figure 4. This is due to the fact that the observation SNR keeps decreasing as the chain size increases, since the noise accumulates each time the channel gain difference is passed on over the relay. Indeed, the use of chain topology leads to a power penalty between $7-12$ dB, compared to using the star topology, as the number of users vary between $3-15$. This implies that, given a network, users should form as large a star topology as possible. However, as the network size grows, chains are become necessary to connect far-away users, since the observation SNR decreases significantly with the increased distances, due to path losses.



(a) Group key rate vs. observation SNR



(b) Group key rate vs. group size

Figure 4: Illustration of achievable group rate vs. observation SNR and the group size.

[4]Note that, observation SNR can be increased by using a higher-powered pilot signals to measure the channel gains.

With the decreased observation SNR, the pure star topology starts to perform badly as illustrated in Fig. 4. Thus, in an extended network, one should use a hybrid topology in which nodes in a close vicinity connect to form star topologies and such clusters are connected to each other via chains. Using our results, one can find the correct balance between the size of the stars and beyond what distances to start forming chains. When a portion of the group members are isolated from the rest of the group, non-group device members could be employed to connect the sub-groups. Intra-group communication should form a hybrid topology following the guidance as we discussed and inter-group communication uses the relay node assisted collaborative key extraction. We leave this analysis as a future study.

8 Fading Trend based Secret Key Extraction

Based on the above analysis, using RSS measurements directly suffers various noises in real mobile environments and may lead to a higher bit mismatch rate as shown in previous works [4, 7]. We take the view point that there should be similar fading trend presented in the RSS measurements between a pair of wireless devices according to the channel reciprocity. We thus propose a fading trend based secret key extraction algorithm that helps to better capture the similarity presented by channel reciprocity as opposed to using the RSS measurements directly.

8.1 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 find 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 5.

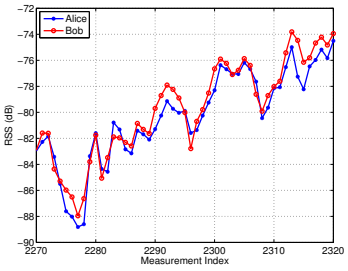


Figure 5: Segments of RSS measurements from a pair of mobile devices in park.

This observation inspires us to utilize the fading trend to reduce the 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) $\hat{Y}(t)$ denotes RSS measurement extracted from the probe packet at time t.

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 Alice and Bob are able to estimate the RSS measurements at common time instants [27].

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 $\hat{Y}(t)$, we examine its previous sample $\hat{Y}(t-1)$ and the second following sample $\hat{Y}(t+2)$. Here we define $\Phi^1 = \hat{Y}(t) - \hat{Y}(t-1)$ and $\Phi^2 = \hat{Y}(t+2) - \hat{Y}(t)$. If the set of RSS measurements $\{\hat{Y}(t-1), \hat{Y}(t), \hat{Y}(t+2)\}$ 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, $b_t(1)$, encoded at $\hat{Y}(t)$ is determined as 1 or 0 which corresponds to increasing or decreasing fading trend, as computed in equation 22 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 measure-

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

Require: INPUT:

$\hat{Y}(t-1), \hat{Y}(t), \hat{Y}(t+2)$: the RSS readings measured from the probe packet with time index $t-1, t, t+2$;

OUTPUT:

$[b_t(1), b_t(2), \cdots, b_t(m)]$: m-bit secret bit sequence extracted from RSS measurement $\hat{Y}(t)$;

PROCEDURES:

1: **Interpolation:**

Using cubic Farrow filter based interpolation technique.

2: **Fading trend estimation:**

For a set of RSS measurements $\{\hat{Y}(t-1), \hat{Y}(t), \hat{Y}(t+2)\}$,

$$b_t(1) = \begin{cases} 0 & \Phi^1 < 0 \wedge \Phi^2 < 0 \\ 1 & \Phi^1 > 0 \wedge \Phi^2 > 0 \end{cases} \tag{22}$$

3: **Thresholding:**

RTM:

$$b_t(2) = \begin{cases} 0 & \hat{Y}(t) < \theta \\ 1 & \hat{Y}(t) \geq \theta \end{cases} \tag{23}$$

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

ments, θ, as the single threshold to extract another secret bit for each RSS measurement. The bit, $b_t(2)$ is encoded as 1 or 0 depending on whether $\hat{Y}(t)$ is larger than θ or not, as described in equation 23 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 $\hat{Y}(t)$ is quantized into $2^{(m-1)}$ equally-likely levels. Let $F(\hat{Y}(t))$ be the cumulative distribution function of $\hat{Y}(t)$. The thresholds used for extracting secret bits are determined by the inverse of $F(\hat{Y}(t))$,

$$\rho_k = F^{-1}(\frac{k}{2^w}), k = 1, \cdots, 2^{m-1} - 1 \tag{21}$$

In addition, $\rho_0 = min(\hat{Y}(t))$ and $\rho_{2^{m-1}} = max(\hat{Y}(t))$. When $\hat{Y}(t)$ falls between any neighboring thresholds, Gray coding [28] are employed for extracting $m-1$ bits, $b_t(i), i = 2, \cdots, m$, from $\hat{Y}(t)$.

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.

8.2 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. $\hat{Y}_{B,A}(t)$ and $\hat{Y}_{A,B}(t)$ are measured RSS readings at Alice and Bob respectively,

$$\hat{Y}_{B,A}(t) = Y_{B,A}(t) + W_{B,A}(t)$$

$$\hat{Y}_{A,B}(t) = Y_{A,B}(t) + W_{A,B}(t),$$

where $t = \tau - 1, \tau, \tau + 2$. The RSS measurements are determined by the radio channel and noise $W(t)$ at different time instants. $W(t)$ is assumed as i.i.d Gaussian noise, following $N(0, \sigma^2)$. According to the reciprocity principle, for each time instant t, $Y_{B,A}(t)$ should be equal to $Y_{A,B}(t)$. 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: $\{\Phi_A^1 > 0 \wedge \Phi_B^1 < 0 \wedge \Phi_A^2 > 0 \wedge \Phi_B^2 < 0\} \vee \{\Phi_A^1 < 0 \wedge \Phi_B^1 > 0 \wedge \Phi_A^2 < 0 \wedge \Phi_B^2 > 0\}$

Then the probability for bit disagreement can be derived as:

$$\begin{aligned} Pr(err) =& Pr(\Phi_A^1 > 0 \wedge \Phi_B^1 < 0 \wedge \Phi_A^2 > 0 \wedge \Phi_B^2 < 0) + Pr(\Phi_A^1 < 0 \wedge \Phi_B^1 > 0 \wedge \Phi_A^2 < 0 \wedge \Phi_B^2 > 0) \\ =& (1 - F(\Phi_A^1 = 0))(1 - F(\Phi_A^2 = 0))F(\Phi_B^1 = 0)F(\Phi_B^2 = 0) + F(\Phi_A^1 = 0)F(\Phi_A^2 = 0)(1 - F(\Phi_B^1 = 0))(1 - F(\Phi_B^2 = 0)), \end{aligned} \tag{24}$$

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

To illustrate, Figure 6 depicts the probability density function of Φ_A^1. If the mean value of Φ_A^1 has a large deviation from 0, which means the signal strength changes sharply from $Y_{B,A}(\tau - 1)$ to $Y_{B,A}(\tau)$ 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, $Y_{B,A}(\tau) - Y_{B,A}(\tau - 1)$ equals to $Y_{A,B}(\tau) - Y_{A,B}(\tau - 1)$, 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 (24) should be a small

value, which indicates a small bit disagreement probability. Similar analysis can be applied for the second term in equation (24) as well.

In this work, we utilize the fading trend based key extraction method as the basis for our two group key extraction protocols via both star and chain topologies in our framework. We compare the performance of our method with existing ones in next section.

9 System Prototype and Experimental Evaluation

9.1 Prototype Implementation

We build a group key extraction system prototype, in which one *initial node* and several *participant nodes* generate a group key collaboratively. The initial node is used to start the procedure of extracting the group key via both star and chain topologies. It is responsible for 1) actively sending probe packets to other participating nodes to collect RSS measurements; 2) being the central node in the star topology and calculating the DOSS value for participating nodes. To ensure the reciprocity of wireless channels, each participating node sends out probe packets once receiving probe packets from any other node. To cooperate the secret key extraction via the chain topology, the participating node is designed to calculate the DOSS value, and inserts it to the probe packet that will be essentially relayed to the end of the chain.

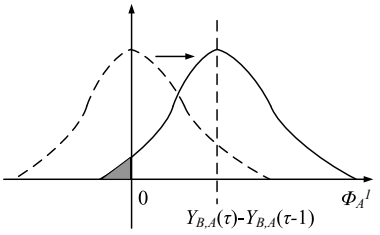
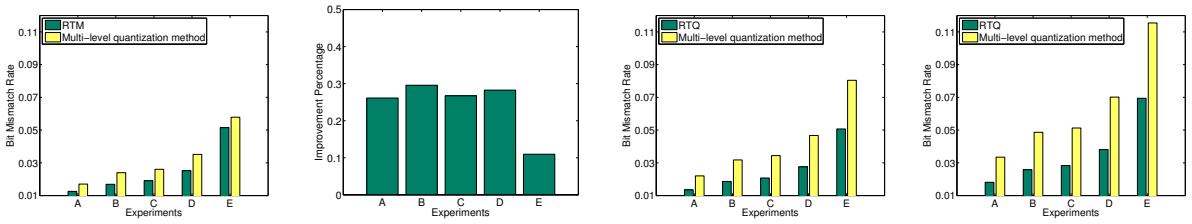


Figure 6: Illustration of the bit disagreement probability analysis.

Our prototype uses Crossbow MICAz motes, which support 2.4GHz IEEE 802.15.4 communication at a high speed of 250kbps. We implement a mobile wireless network using 6 MICAz motes: one acts as the initial node and the other five are participating nodes. One additional mote is connected to a laptop acting as sink. Probe packets are broadcasted at the rate of 20pkt/sec. The probe packet includes the sending node ID and the packet sequence number so that the sink node can distinguish different probe packets. When a node receives a probe packet, it extracts the sending node ID and packet sequence number, and inserts this information into the probe packet it will send out. After the sink node receives the probe packet from other nodes, it extracts this



(a) Basic RTM (b) Basic RTM: Impr. Percentage (c) Extended RTQ: 3-bit (d) Extended RTQ: 4-bit

Figure 7: Bit mismatch rate under various experimental scenarios.

information and stores it in the database. Finally, the sink can obtain all the RSS measurements on the channel between any pair of nodes, and feed them as the input of the fading trend based key extraction algorithm for generating secret bits.

Experimental Setup and Scenarios: We conduct 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 Hoboken train station to Stevens Institute of Technology spanning over 10 street blocks. During our experiments, we measure 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: *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 (BMR): 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 total number of secret bits extracted. For group key extraction, it is defined as the averaged bit mismatch rate from all pairs of devices in the group.

Bit generation rate (BGR): 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.

9.2 Evaluation of Fading Trend based Key Extraction Algorithm

9.2.1 Bit Mismatch Rate (BMR)

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

Basic RTM scheme: Figure 7(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 observe that our method outperforms the multi-level quantization approach by over 26% for outdoor environments, particularly, 26%, 30%, 27%, 28% for scenarios A$\sim$D respectively, and around 11% for indoor environment as shown in figure 7(b). In addition, the scenarios with pedestrians passing between mobile devices achieve lower bit mismatch rate, indicating the presence of larger fading, which benefits our proposed method.

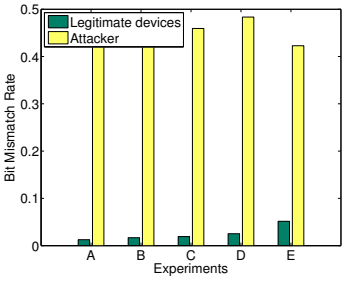


Figure 8: Bit mismatch rate for legitimate devices and attacker under different scenarios.

Extended RTQ scheme: Figure 7(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 7(c) and figure 7(d), we observe that as 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

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

Table 1: NIST statistical test suite results

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.

Comparison of BMR between legitimate user and eavesdropper: Figure 8 presents our experimental results of a pair of MICAz nodes with the presence of eavesdropper (using an additional MICAz mote placed at 30 cm away) for 2 bits per measurement. We find that the bit mismatch rate incurred by eavesdropper 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 9.1. This observation validates the high security of using channel measurements for secret key extraction.

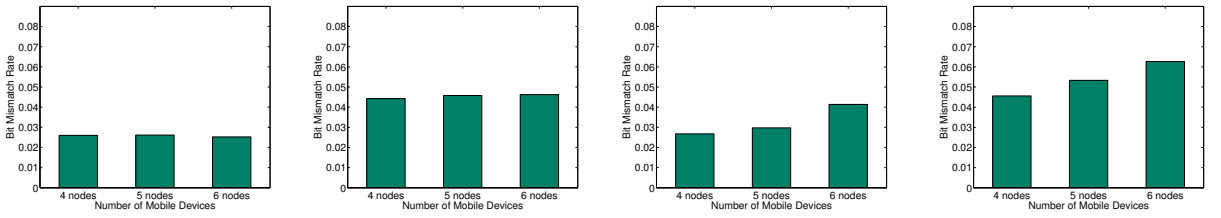
9.2.2 Randomness

To ensure that the secret key generated is substantially random, the standard randomness test suite from NIST [29] 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 test results for 5 different experimental scenarios are listed in Table 1. All the cases pass the test with the p-value much larger than 0.01, which is the threshold to pass the test.

9.3 Group Key Extraction via the Star Topology

We next study how the number of nodes in the group affects the BMR for group key extraction via the star topology in Figure 9 (a) and (b). We observe that the bit mismatch rate is stable when the group size increases under both scenarios A and B when maintaining the bit generation rate at 2 bits per measurement.

The results are consistent with our theoretical analysis in Section 5.2. A slight difference



(a) Star: park, with pedestrian (b) Star: park, without pedestrian (c) Chain: park, with pedestrian (d) Chain: park, without pedestrian

Figure 9: Performance of group key extraction.

exists on the bit mismatch rate under each scenario among different group sizes due to the noise does not strictly follow identical Gaussian distribution in practice. Furthermore, we found that the performance of our protocol is better under scenario A with pedestrians, thus confirms the effectiveness of our fading trend based key extraction scheme.

9.4 Group Key Extraction via the Chain Topology

Figure 9(c) and (d) present the BMR for group key extraction via the chain topology. We observe that as the group size increases, the bit mismatch rate under both scenarios A and B increases when 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. According to the analysis in Section 4, the bit mismatch rates are still within the error tolerance range of Golay code.

10 Conclusions

In this paper, we address the problem of group key extraction by exploiting physical layer information of radio channel. In particular, the group key is extracted when multiple wireless devices work collaboratively with the readily available Received Signal Strength (RSS) in radio channels, without relying on a fixed infrastructure. We propose a relay node assisted mechanism that solves the issue when mobile devices are not within each other's communication range. Our relay node assisted mechanism uses difference of signal strength to ensure the security of the key extraction, and achieves a lower bit mismatch rate comparing to existing studies while maintaining a similar key generation rate when employing key extraction based on fading trend. To enable secure group

communication, two protocols via star and chain topologies are developed in our framework by exploiting RSS from multiple devices to perform group key generation collaboratively. The collaborative key extraction protocol via the star topology is designed for scenarios when the group of wireless devices under consideration is within the communication range of each other, while the protocol via the chain topology involves handling the scenarios when not all wireless devices inside the group are within the communication range of each other. We derive the maximum achievable group key rate by our approach. Our analysis provides important insights on the amount of drop in key rate as the group size grows and enables us to find the best network topology the group can form in order to achieve a high key rate. Our prototype using a mobile wireless network with multiple MICAz motes confirms the feasibility of leveraging RSS for group key generation among multiple wireless devices. The effectiveness of group key extraction via star and chain topologies built on top of fading-trend based key extraction and relay node assisted mechanism is demonstrated through extensive experimental study in both outdoor (e.g., park and street) and indoor (e.g., office building) environments.

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] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *IEEE INFOCOM*, 2012, pp. 927–935.

[12] J. Wallace, "Secure physical layer key generation schemes: Performance and information theoretic limits," in *IEEE ICC'09.*, pp. 1–5.

[13] J. Wallace, C. Chen, and M. Jensen, "Key generation exploiting mimo channel evolution: Algorithms and theoretical limits," in *EuCAP 2009.*, pp. 1499–1503.

[14] U. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Transactions on Information Theory*, vol. 45, no. 2, pp. 499–514, 1999.

[15] S. Draper, A. Sayeed, and T. Chou, "Minimum energy per bit for secret key acquisition over multipath wireless channels," in *IEEE ISIT*, 2009, pp. 2296–2300.

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

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

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

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

[20] 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.

[21] I. Csiszar and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transaction on Information Theory*, vol. 46, pp. 344–366, 2000.

[22] I. Csiszar and R. Ahlswede, "Secrecy capacities for multiple terminals," *IEEE Transaction on Information Theory*, vol. 50, pp. 3046–3061, 2004.

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

[24] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography, part i: Secret sharing," *IEEE Transaction on Information Theory*, vol. 39, pp. 1121–1132.

[25] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transaction on Information Theory*, vol. 39, pp. 733–742, 1993.

[26] U. Maurer and S. Wolf, "Secret key agreement over a non-authenticated channel parts i-iii," *IEEE Transaction on Information Theory*, vol. 49, pp. 822–851, 2003.

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

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

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