Fast and Scalable Secret Key Generation Exploiting Channel Phase Randomness in Wireless Networks

Qian Wang†, Hai Su†, Kui Ren†, and Kwangjo Kim‡
†Department of ECE, Illinois Institute of Technology, Chicago, IL 60616. Email: {qian,hai,kren}@ece.iit.edu
‡Department of CS, KAIST, Daejeon, 305-732, Republic of Korea. Email: kkj@kaist.ac.kr

***Abstract*—Recently, there has been great interest in physical layer security techniques that exploit the randomness of wireless channels for securely extracting cryptographic keys. Several interesting approaches have been developed and demonstrated for their feasibility. The state-of-the-art, however, still has much room for improving their practicality. This is because i) the key bit generation rate supported by most existing approaches is very low which significantly limits their practical usage given the intermittent connectivity in mobile environments; ii) existing approaches suffer from the scalability and flexibility issues, *i.e.*, they cannot be directly extended to support efficient group key generation and do not suit for static environments. With these observations in mind, we present a new secret key generation approach that utilizes the uniformly distributed phase information of channel responses to extract shared cryptographic keys under narrowband multipath fading models. The proposed approach enjoys a high key bit generation rate due to its efficient introduction of multiple randomized phase information within a single coherence time interval as the keying sources. The proposed approach also provides scalability and flexibility because it relies only on the transmission of periodical extensions of unmodulated sinusoidal beacons, which allows effective accumulation of channel phases across multiple nodes. The proposed scheme is thoroughly evaluated through both analytical and simulation studies. Compared to existing work that focus on pairwise key generation, our approach is highly scalable and can improve the analytical key bit generation rate by a couple of orders of magnitude.**

I. Introduction

Securing communications requires the generation of cryptographic keys, which is highly challenging in wireless networks, given that: 1) an online key management center is not available due to the dynamic mobile environment; and 2) the network is vulnerable to eavesdropping due to the broadcast nature of wireless medium. Obviously, not only the usual network communications but also the secret key generation communication itself, which should be conducted when two nodes first meet and begin to set up a secure communication link, is subject to eavesdropping. Existing security research along this direction usually avoids the problem by assuming that there may exist a short safe network bootstrapping phase which is believed to be attack-free. This, however, does not sufficiently address the problem and not apply to the case of dynamic encountering of multiple nodes.

Recently, there has been great interest in physical layer (PHY) security techniques that exploit the inherent randomness in wireless channels for extracting cryptographic keys. Compared with classical key generation algorithms such as Diffie-Hellman key agreement protocol [1], which rely upon computational hardness of problems, secret generation using channel randomness does not assume a computationally-bounded adversary and can achieve information-theoretical secrecy [2]. Using multipath channels as the source of common randomness, these work focus on estimating or measuring a popular statistic of wireless channel, *i.e.*, received signal strength (RSS), for extracting shared secret bits between node pairs [3], [4], [2], [5]. It has been demonstrated that these RSS-based methods are feasible in existing platforms. However, the key bit generation rate supported by these approaches is very low that it significantly limits their practical application given the intermittent connectivity in mobile environments. Another drawback of these RSS-based approaches is that they cannot be directly extended to support efficient group key generation. This is mainly due to the fact that the RSS values obtained between a pair of nodes cannot be efficiently and securely "passed" to other nodes, or in other words, it is hard to safely "accumulate" RSS information across multiple nodes for group key generation. We also note that the RSS-based key generation schemes rely on channel variations or node mobility to extract high entropy bits. That means they are not suitable for establishing secure keys in static environments.

To address these problems, we propose a new set of key generation protocols that inherently support both efficient pairwise and group key generations. Our proposed scheme utilizes the phase reciprocity of wireless communication: the underlying channel response between two transceivers is unique and location-specific, and the transmitted signals from each other will experience almost the same fading in the phase [6]. The proposed pairwise key generation scheme uses time division duplexing for the transmission of the beacons between nodes (The benefit of using a single frequency for all beacons is that channel reciprocity is maintained in multipath propagation scenarios). Each node can estimate the channel phase information which are further converted into bit vectors according to a pre-defined quantization method. The resulting pairwise keys are theoretically be the same as they are generated from the same phase information. The security strength of the scheme is guaranteed based on the fact that it is infeasible for an adversary which is located at a different place with the transceivers to obtain the identical phase information for key generation [3], [6], [4], [2], [5]. In wireless networks, securing group communication is also very important. The naive solution for group key generation is to apply pairwise key generation protocol multiple times between a head node and the other group nodes, based on which a group key selected by the head node can be derived

to the other group nodes using pairwise encryption. However, the number of interactions between the nodes increase linearly with the group size. To satisfy the critical need for efficient protocols, we further propose a time-slotted round-trip scheme for group key generation where one node chosen as an initiator starts the key generation process and transmits the beacons from both the clockwise and anticlockwise direction. Because the sum of phase estimates obtained from the clockwise and counterclockwise transmissions are nearly identical at each node, a common key can be effectively generated. To enhance the robustness of the proposed scheme, we use cryptographic information reconciliation and privacy amplification tools [7], [8] to reconcile bit discrepancies and improve the randomness of the generated keys.

Our Contribution The main contributions of this paper are:

- We propose a new secret key generation approach that utilizes the uniformly distributed phase information of channel responses to extract shared cryptographic keys under narrowband multipath fading models. Compared to existing approaches which only support pairwise key generation, our scheme is highly scalable and can support efficient group key generation. The generated bit stream is very close to a truly random sequence, *i.e.*, our randomness tests show that the average entropy of the bit sequence is close to 1.
- We show that our proposed scheme is more flexible and can be applied in both static and mobile environments. Our scheme introduces phase randomness to bit generation and removes the reliance on node mobility to obtain high entropy bits in contrast to RSS-based approaches.
- We evaluate the proposed schemes through both analytical and simulation studies. The results show that i) our scheme can improve the analytical key bit generation rate by a couple of orders of magnitude and ii) the parameters of the scheme can be selected such that a desired level of key generation accuracy and reliability is achieved with high efficiency.

Organization The rest of the paper is organized as follows: Section II introduces the system model, attack model and some necessary background. Section III provides the detailed description of our proposed schemes including pairwise key generation, group key generation, secret key reconciliation and privacy amplification. Section IV presents the performance analysis. Finally, Section V concludes the paper.

II. Problem Formulation

A. System Model

We consider an infrastructureless wireless network, where nodes dynamically form communication groups. The channel from node i to node j is modeled as a narrowband multipath fading model with channel impulse $h_{i,j}(t)$ and stays roughly constant for several timeslots. We assume channel reciprocity in the forward and reverse directions during the time period of *coherence time* such that $h_{i,j}(t) = h_{j,i}(t)$ and the underlying noise in each channel is additive white Gaussian noise (AWGN). In wireless communications, *coherence time* is a statistical measure of the time duration over which the channel impulse response is essentially invariant, and quantifies the similarity of the channel response at different times. Based on communication theory [6], an entity which is at least $\lambda/2$ (λ is the wavelength) away from the network nodes experiences fading channels to the nodes are statistically independent of the channels between the communicating nodes. All network nodes are assumed to be half-duplex in the sense that they cannot transmit and receive signals at the same frequency simultaneously. Each node possesses a single isotropic antenna and employs a maximum likelihood (ML) estimator for frequency and phase estimation [9]. We also assume that the network nodes possess a common time reference, which can be easily obtained by using GPS.

B. Threat Model

Following the same assumptions in most PHY-based key generation schemes in wireless networks [3], [4], we assume a passive adversary in this paper, who can eavesdrop all the communications between legitimate nodes. Specifically, the whole key generation protocol is known to the adversary, and during key generation process, the adversary can also perform phase estimation based on the received signals. The adversary aims to derive the secret key generated between the legitimate nodes, and it is not interested in disrupting the key establishment protocol by jamming the communication channels. In addition, during the key reconciliation process, the adversary who observes the error-correcting information will try to break the secret key. We assume the participating nodes are all trusted, and node compromise and man-in-the-middle attacks are not considered here as in the existing approaches [3], [2], [4].

C. Preliminaries

Narrowband Fading Models. Following [6], we denote the transmitted signal from node i to j as $s(t) = \Re\{u(t)\, e^{j(2\pi f_c t+\phi_0)}\}$, where $u(t)$ is the complex envelope of $s(t)$ with bandwidth B, f_c is its carrier frequency and ϕ_0 is the phase offset. Under most delay spread characterizations, $\nu_{i,j} \ll 1/B$ implies that the delay associated with the kth multipath component $\tau_k \leq \nu_{i,j}\ \forall k$, so $u(t-\tau_k) \approx u(t)$. So the received signal at node j is $r(t) = \Re\{\big[\sum_n \alpha_n(t)e^{-j\phi_n(t)}\big]e^{j2\pi f_c t}\}$, where $\alpha_n(t)$ is a function of path loss and shadowing while $\phi_n(t)$ depends on delay, Doppler, and carrier offset. Typically, it is assumed that these two random processes $\alpha_n(t)$ and $\phi_n(t)$ are independent.

If $s(t)$ is assumed to be an unmodulated carrier $s(t) = \Re\{e^{j2\pi f_c t}\} = cos 2\pi f_c t$, it is narrowband for any $\nu_{i,j}$. The received signal becomes

$$\begin{aligned} r(t) &= \Re\{e^{j2\pi f_c t}\sum_{n=0}^{N(t)} \alpha_n(t)e^{-j\phi_n(t)}\} \\ &= r_I(t)\cos 2\pi f_c t + r_Q(t)\sin 2\pi f_c t, \end{aligned}$$

where the in-phase and quadrature components are given by $r_I(t) = \sum_{n=1}^{N(t)} \alpha_n(t)\cos\phi_n(t)$ and $r_Q(t) = \sum_{n=1}^{N(t)} \alpha_n(t)\sin\phi_n(t)$, respectively. If the number of resolvable multipath components $N(t)$ is large we can invoke the Central Limit Theorem and the fact that $\alpha_n(t)$ and $\phi_n(t)$ are stationary and ergodic to approximate $r_I(t)$ and $r_Q(t)$ as jointly Gaussian

Parameters: The desired key size ($|K|$) and the number of quantization levels (q). Let t_1 and t_2 denote the start time of two beacon transmissions, respectively. Let $|K|/\log_2(q)$ denote the number of rounds to be repeated.

S_1		S_2
1. Generate $x_1(t)$ with w_c and $\phi_1 \in \mathcal{U}[0, 2\pi]$	$\xrightarrow{x_1(t)=e^{j(w_c(t-t_1)+\phi_1)}}$	
		2.Receive $y_{12}(t) = a_{12}e^{j(w_c t+\phi_1+\theta_{12})} + \eta_{12}(t)$ Estimate w_c as $\hat{w}_{12}$ and $\phi_1 + \theta_{12}$ as $\hat{\phi}_{12}$
	$\xleftarrow{x_2(t)=e^{j(w_c(t-t_2)+\phi_2)}}$	Generate $x_2(t)$ with w_c and $\phi_2 \in \mathcal{U}[0, 2\pi]$ Quantize $(\hat{\phi}_{12} + \phi_2)$ `mod` 2π
3. Receive $y_{21}(t) = a_{21}e^{j(w_c t+\phi_2+\theta_{21})} + \eta_{21}(t)$ Estimate w_c as $\hat{w}_{21}$ and $\phi_2 + \theta_{21}$ as $\hat{\phi}_{21}$ Quantize $(\hat{\phi}_{21} + \phi_1)$ `mod` 2π		

(Repeat steps 1-3 $|K|/\log_2(q)$ times)

Fig. 1: Our protocol for pairwise key generation

random processes. The complex lowpass equivalent signal for $r(t)$ is given by $r_I(t) + jr_Q(t)$ which has phase $\theta = \arctan(r_Q(t)/r_I(t))$, where θ is uniformly distributed, *i.e.*, $\theta \in \mathcal{U}[0, 2\pi]$.

III. Time-slotted Roundtrip Secret Key Generation Protocol

In this section, we first present the protocol for pairwise key generation (*i.e.*, $M = 2$). Then a time-slotted round-trip protocol for group key generation ($M > 2$) is proposed. We also discuss enhancing techniques for key reconciliation and privacy amplification. The basic idea behind our key generation scheme is to exploit the inherent channel randomness associated with distinct pairwise links, *i.e.*, the carriers transmitted back and forth between two nodes will experience the same phase variation over the *coherence time* period [10].

A. Pairwise Key Generation

The protocol for pairwise key generation is shown in Fig. 1. There are two timeslots for each key generation round. The pairwise key generation protocol begins in TS_1 with transmission of a unit-amplitude sinusoidal primary beacon of duration T_1 from S_1 to S_2:

$$x_1(t) = e^{j(w_c(t-t_1)+\phi_1)},$$

where $t \in [t_1, t_1 + T_1)$, and ϕ_1 is the initial phase chosen uniformly at random from $[0, 2\pi]$ by S_1. To simplify the exposition, we assume $t_1 = 0$ in the following discussion, *i.e.*, the protocol starts at time zero point. S_2 observes the initial transient response of the multipath channel $h_{1,2}(t)$ to the beacon $x_1(t)$ over the interval $t \in [\tau_{12}, \tau_{12} + \nu_{12})$, where τ_{12} denotes the delay of the shortest path and ν_{12} denotes the finite delay spread of the channel $h_{1,2}(t)$. In order to achieve a steady-state response at S_2, it is required that $T_1 > \nu_{12}$. The steady-state portion of the beacon received at S_2 can be written as

$$y_{12}(t) = \alpha_{12}e^{j(w_c t+\phi_1+\theta_{12})} + \eta_{12}(t),$$

where $t \in [\tau_{12}+\nu_{12}, \tau_{12}+T_1)$, and $\eta_{12}(t)$ denotes the additive white Gaussian noise (AWGN) in the $1 \rightarrow 2$ channel. α_{12} and θ_{12} are the steady-state gain and the phase response of channel $h_{1,2}(t)$, respectively. At the end of primary beacon, a final transient response of the multipath channel is also received by S_2 over the interval $t \in [\tau_{12}+T_1, \tau_{12}+\nu_{12}+T_1)$. S_2 uses only the steady-state portion of the noisy observation to compute ML estimates of the received frequency and phase, which are denoted by $\hat{w}_{12}$ and $\hat{\phi}_{12}$, respectively. Note $\hat{\phi}_{12}$ is the estimate of the phase $\phi_1 + \theta_{12}$.

Upon the conclusion of the primary beacon $y_{12}(t)$, S_2 begins the transmission of a sinusoidal secondary beacon at $t_2 = \tau_{12} + \nu_{12} + T_1$. The secondary beacon transmitted by S_2 at t_2 can be written as

$$x_2(t) = e^{j(w_c(t-t_2)+\phi_2)},$$

where $t \in [t_2, t_2 + T_2)$, and ϕ_2 is the initial phase chosen uniformly at random from $[0, 2\pi]$ by S_2. S_1 observes the initial transient response of the multipath channel $h_{2,1}(t)$ to beacon $x_2(t)$ over the interval $t \in [\tau_{12} + \nu_{12} + T_1 + \tau_{21}, \tau_{12} + \nu_{12} + T_1 + \tau_{21} + \nu_{21})$, where $\nu_{21} = \nu_{12}$ due to channel reciprocity. In order to achieve a steady-state response at S_1, $T_2 > \nu_{21}$ is required. The steady-state portion of the beacon received at S_1 can be written as

$$y_{21}(t) = \alpha_{21}e^{j(w_c t+\phi_2+\theta_{21})} + \eta_{21}(t),$$

where $t \in [\tau_{12}+\nu_{12}+T_1+\tau_{21}+\nu_{21}, \tau_{12}+\nu_{12}+T_1+\tau_{21}+T_2)$, and $\eta_{21}(t)$ denotes the additive white Gaussian noise (AWGN) in the $2 \rightarrow 1$ channel. α_{21} and θ_{21} are the steady-state gain and the phase response of channel $h_{2,1}(t)$, respectively. At the end of this beacon, a final transient response of the multipath channel is received by S_1 over the interval $t \in [t_2 + \tau_{21} + T_2, t_2 + \tau_{21} + T_2 + \nu_{21})$. Similar to S_2 in TS_1, S_1 uses only the steady-state portion of the noisy observation to compute ML estimates of the received frequency and phase, which are denoted by $\hat{w}_{21}$ and $\hat{\phi}_{21}$, respectively. Note $\hat{\phi}_{21}$ is the estimate of the phase $\phi_2 + \theta_{21}$.

Now S_1 and S_2 can compute the final phase components used for key generation in the first round

$$\begin{aligned} S_1 : \Phi_1^1 &= \hat{\phi}_{21} + \phi_1 \ \textbf{mod}\ 2\pi \\ S_2 : \Phi_2^1 &= \hat{\phi}_{12} + \phi_2 \ \textbf{mod}\ 2\pi. \end{aligned}$$

We uniformly map Φ_1^1 and Φ_2^1 into the quantization interval/index using the following formula:

$$Q(x) \quad = \quad k \quad \text{if } x \in [\frac{2\pi(k-1)}{q}, \frac{2\pi k}{q})$$

for $k = 1, 2, \ldots, q$. Thus, in the first round, the quantization of each phase value generates $\log_2(q)$ secret bits, which are shared between S_1 and S_2.

For round $k = 2, 3, \ldots, |K|/\log_2(q)$, S_1 and S_2 repeat the operations as in TS_1 and TS_2 to generate Φ_1^k and Φ_2^k, which are converted into bit vectors through q-level quantization. After $|K|/\log_2(q)$ rounds, a key of size $|K|$ is generated and shared between S_1 and S_2.

B. Group Key Generation

When nodes form dynamic groups, it requires a common group key to be shared among the communicating nodes for securing group communication. In this subsection, we present an efficient time-slotted roundtrip protocol for group key generation (*i.e.*, $M > 2$) with minimum interactions among the nodes. With M nodes being formed a dynamic group, the protocol has a total of $2M|K|/\log_2(q)$ timeslots for establishing a group key of size $|K|$. The protocol for group key generation is shown in Fig. 2. To simplify the exposition, we assume the nodes in the group are numbered from 1 to M. The activities in each timeslot of round 1 are as follows (for ease of exposition, we ignore the explicit value of t_i for $i = 1, 2, \ldots, 2M$):

(1) In TS_1, S_1 transmits $x_1(t) = e^{j(w_c(t-t_1)+\phi_1)}$ to S_2, where ϕ_1 is chosen uniformly at random over $[0, 2\pi]$. S_2 uses the steady portion of its local noisy observation to compute ML estimates $\hat{\phi}_{12}$ and $\hat{w}_{12}$. Here, $\hat{\phi}_{12}$ is the estimate of $\phi_1 + \theta_{12}$.

(2) In TS_i for $i = 2, 3, \ldots, M$, S_i transmits beacon $x_i(t) = e^{j(w_c(t-t_i)+\hat{\phi}_{(i-1)i})}$ to S_{i+1}, where $x_i(t)$ is a **periodic extension** of the beacon received in TS_{i-1}. Upon receiving the signal, S_{i+1} uses the steady portion of its local noisy observation to compute ML estimates $\hat{\phi}_{i(i+1)}$ and $\hat{w}_{i(i+1)}$. Here, $\hat{\phi}_{i(i+1)}$ is the estimate of $\hat{\phi}_{(i-1)i} + \theta_{i(i+1)}$. Note that in TS_M, S_M transmits $x_M(t)$ to S_1, and S_1 generates $\hat{\phi}_{M1}$ which is the estimate of $\hat{\phi}_{(M-1)M} + \theta_{M1}$.

(3) In TS_{M+1}, S_1 transmits beacon $x'_1(t) = e^{j(w_c(t-t_{M+1})+\phi'_1)}$ to S_M, where ϕ'_1 is chosen uniformly at random over $[0, 2\pi]$. S_M uses the steady portion of its local noisy observation to compute ML estimates $\hat{\phi}_{1M}$ and $\hat{w}_{1M}$. Here, $\hat{\phi}_{1M}$ is the estimate of $\phi'_1 + \theta_{1M}$.

(4) In TS_{M+2}, S_M transmits a sinusoidal beacon $x'_M(t) = e^{j(w_c(t-t_{M+2})+\hat{\phi}_{1M})}$ to S_{M-1}. $x'_M(t)$ is a **periodic extension** of the beacon received in TS_{M+1}. Upon receiving the signal, S_{M-1} uses the steady portion of its local noisy observation to compute ML estimates $\hat{\phi}_{M(M-1)}$ and $\hat{w}_{M(M-1)}$. Here, $\hat{\phi}_{M(M-1)}$ is the estimate of $\hat{\phi}_{1M} + \theta_{M(M-1)}$.

(5) In TS_i for $i = M+3, \ldots, 2M-1$, S_{2M+2-i} transmits $x'_{2M+2-i}(t) = e^{j(w_c(t-t_i)+\hat{\phi}_{(2M+3-i)(2M+2-i)})}$ to S_{2M+1-i}. $x'_{2M+2-i}(t)$ is a **periodic extension** of the beacon received in TS_{i-1}. Upon receiving the signal, S_{2M+1-i} uses the steady portion of its local noisy observation to compute ML estimates $\hat{\phi}_{(2M+2-i)(2M+1-i)}$ and $\hat{w}_{(2M+2-i)(2M+1-i)}$. Here, $\hat{\phi}_{(2M+2-i)(2M+1-i)}$ is the estimate of $\hat{\phi}_{(2M+3-i)(2M+2-i)} + \theta_{(2M+2-i)(2M+1-i)}$.

Parameters: Desired key size ($|K|$), the number of quantization levels (q), and the number of nodes (M).

For round $k = 1, \ldots, |K|/\log_2(q)$

1. In TS_1, S_1 generates $x_1(t)$ with $\phi_1 \in \mathcal{U}[0, 2\pi]$. $S_1 \xrightarrow{x_1(t)} S_2$. S_2 computes $\hat{\phi}_{12}$ and $\hat{w}_{12}$.
2. In TS_i ($i = 2, 3, \ldots, M-1$), S_i generates $x_i(t)$ with $\hat{\phi}_{(i-1)i}$. $S_i \xrightarrow{x_i(t)} S_{i+1}$. S_{i+1} computes $\hat{\phi}_{i(i+1)}$ and $\hat{w}_{i(i+1)}$.
3. In TS_M, S_M generates $x_M(t)$ with $\hat{\phi}_{(M-1)M}$. $S_M \xrightarrow{x_M(t)} S_1$. S_1 computes $\hat{\phi}_{M1}$ and $\hat{w}_{M1}$.
4. In TS_{M+1}, S_1 generates $x'_1(t)$ with $\phi'_1 \in \mathcal{U}[0, 2\pi]$. $S_1 \xrightarrow{x'_1(t)} S_M$. S_M computes $\hat{\phi}_{1M}$ and $\hat{w}_{1M}$.
5. In TS_i ($i = M+2, \ldots, 2M$), S_{2M+2-i} generates $x'_{2M+2-i}(t)$ with estimates obtained in TS_{i-1}. $S_M \xrightarrow{x'_M(t)} S_{M-1} \xrightarrow{x'_{M-1}(t)} \cdots \xrightarrow{x'_3(t)} S_2 \xrightarrow{x'_2(t)} S_1$.
6. $S_1, S_2, \ldots, S_M$ compute $(\phi_1 + \phi'_1 + \theta_{12} + \theta_{23} + \ldots + \theta_{(M-1)M} + \theta_{M1})$ mod 2π and quantize it using $Q(x) = \log_2(k)$ if $x \in [\frac{2\pi(k-1)}{q}, \frac{2\pi k}{q})$.

End

(Repeat steps 1-6 $|K|/\log_2(q)$ times)

Fig. 2: Our protocol for group key generation

Now we show how a common group key can be established among $S_1, S_2, \ldots, S_M$ (For ease of exposition, we ignore the estimation errors here and discuss its effect in Section IV). After round 1, node S_i ($i \in \{2, 3, \ldots, M\}$) obtains estimate $(\phi_1 + \theta_{1,2} + \ldots + \theta_{(i-1)i})$ in TS_{i-1} from the clockwise transmission direction and another estimate $(\phi'_1 + \theta_{1,M} + \ldots + \theta_{(i+1)i})$ in TS_{2M+1-i} from counterclockwise direction. S_i calculates the sum of the two phase estimates as

$$\begin{aligned} \Phi_i \quad &= \quad (\phi_1 + \theta_{1,2} + \theta_{2,3} \ldots + \theta_{(i-1)i}) + (\phi'_1 + \theta_{1,M} + \\ &\quad\quad \theta_{M,M-1} + \ldots + \theta_{(i+1)i}), \quad \text{for } 1 < i < M \\ \Phi_M \quad &= \quad (\phi_1 + \theta_{1,2} + \ldots + \theta_{(M-1)M}) + (\phi'_1 + \theta_{1,M}), \end{aligned}$$

each of which consists of **three** parts: random initial phase ϕ_1, random initial phase ϕ'_1 and the phase responses θ_{ij} (θ_{ji}) of wireless channels $h_{i,j}(t)$ ($h_{j,i}(t)$) along the circles. Different from the other nodes, S_1 can directly use the phase estimates of the beacons received in the clockwise transmission to obtain:

$$\Phi_1 \quad = \quad \phi_1 + \phi'_1 + (\theta_{12} + \theta_{23} + \ldots + \theta_{(M-1)M} + \theta_{M1})$$

S_i ($i = 1, 2, \ldots, M$) can convert Φ_i into $\log_2(q)$ bits through q-level quantization. In subsequent round $k = 2, 3, \ldots, |K|/\log_2(q)$, $S_1, S_2, \ldots, S_M$ repeat the operations from (1) to (5) and perform quantization. After $|K|/\log_2(q)$ rounds, each node can generate a group key of size $|K|$.

C. Discussion

Obviously, the naive method for constructing group key is to run the pairwise key generation protocol multiple times

between a master node and the other slave nodes. However, such "centralized" protocol suffers from low efficiency when the size of the group grows. Assume $N_r = \frac{|K|}{\log_2 q}$. In the centralized group key generation protocol (CGKGP), it requires to run pairwise key generation protocol (PKGP) between the master node and each slave node for generating pairwise keys. The number of timeslots of the CGKGP is $2N_r(M-1)+M+M$, where $2N_r(M-1)$ timeslots are used for pairwise key establishment, M timeslots for key reconciliation and M timeslots for group key distribution to each slave node. In contrast, the proposed GKGP requires $(2M-1)N_r+1$ timeslots, where $(2M-1)N_r$ timeslots are used for group key generation and 1 timeslot for key reconciliation. Thus, when $M > \frac{N_r+1}{2}$ the proposed GKGP outperforms the CGKGP. As an example, if $N_r = 16$, the proposed GKGP is more efficient when $M > 8.5$. When M increases, the advantages become more compelling.

In our proposed GKGP, each node computes the estimated phase of the sinusoidal beacon observed in the previous timeslot and generates a **periodic extension** of the received beacon for transmitting in the next timeslot. Since all nodes share a common time reference, their absolute estimates of the phase of received beacons do not have any phase offset relative to their own local time reference. Thus, the periodic extension of the beacons could accumulate all the channel phases $\theta_{i,j}$ along the transmission circuit. Due to channel reciprocity, the sum of phase estimates obtained from the clockwise and counterclockwise transmission are nearly identical at each node. Note that although we use the absolute starting and ending times of timeslots in our protocol description, they are not critical to the performance of the protocol. This is because each node generate a **periodical extension** of beacons received in the previous timeslot, small deviations or gaps between timeslots only delay the window in which the periodic extension is transmitted and do not change the phase of the beacons.

Since the coherence time of a channel is inversely proportional to the Doppler frequency shift, extracting bits from different "coherence time periods" can increase the average entropy of the bit sequence [4], [2]. This is demonstrated in [4], where a certain level of node mobility helps generate key bits with high entropy. However, in our proposed protocol, we do not have this constraint: for a given coherence time, multiple rounds can be run to generate more random bits with high average entropy as the random initial phases ϕ_1 and ϕ_1' chosen in each round can cause good randomness in the process of bit generation, *i.e.*, the proposed scheme is not constrained by the coherence time, and it can work well even in the static case.

D. Secret Key Reconciliation and Privacy Amplification

According to the reciprocity principle, the generated key bits should theoretically be the same. However, there may exist a small number of discrepancies due to half-duplex beacon transmission and estimation errors caused by noise, interference and hardware variations.

To reconcile the discrepancies between bit streams, we propose to use a cryptographic primitive called *secure sketch* [7]. Generally, a *secure sketch* produces public information s about its input K that does not reveal K, and yet allows exact recovery of K given K' that is close to K. Assume two nodes A and B hold K and K' ($\mathsf{dis}(K,K') \le t$), respectively. Here, $\mathsf{dis}(x,y)$ denotes the number of positions in which x and y differ. Following Code-offset construction in [7], we use a $[n,k,2t+1]_2$ error-correcting code C to correct errors in K' even though K' may not be in C. When performing key reconciliation, node A randomly selects a random codeword c from C and computes *secure sketch* $\mathsf{SS}(K) = s = K \oplus c$. Then s is sent to node B. Upon receiving s, node B subtracts the shift s from K' and gets $\mathsf{Rec}(K', s) = c' = K' \oplus s$. Then node B decodes c' to get c, and computes K by shifting back to get $K = c \oplus s$. As an example, consider $|K| = 128$bit and $\mathsf{dis}(K,K') = 10$. In this case, nodes A and B can employ a $[127, 64, 21]_2$-BCH codes to correct the bit errors. Node A uses the first 127 bit of K to construct the *secure sketch* and sends s and the hash value $h(K)$ to node B. Node B corrects errors in the first 127 bit of K' and uses $h(K)$ as a reference to determine the K. Note that since the error-correcting information s is public to both the communicating nodes and the adversary, it can be used by the adversary to guess portions of the generated key [4]. To cope with this problem, the technique of privacy amplification can be used as a common practice. In particular, we use interactive robust fuzzy extractors, which is very efficient and has been shown to require only a few seconds on consumer-grade computers [8].

E. Security Analysis

The security of the proposed protocols is guaranteed based on the spatial decorrelation assumption that it is almost impossible for an adversary who is located at a *different* place with the transceivers to obtain the identical channel response for key generation. This is a common assumption made in most key generation protocols exploiting channel randomness for bit extraction and has been validated through real experiments, including [3], [4], [2]. Consider the group key generation, only when the adversary located at almost the exact same positions as all group nodes can he obtain the same channel responses from distinct pairwise links. Based on wireless communication theory [6], an entity which is at least $\lambda/2$ away from the network nodes experiences fading channels to the nodes are statistically independent of the channels between the communicating nodes. As an example, consider a wireless system with 900MHz carrier frequency, average node distance 100m, and moving speed 10m/sec. If the adversary is more than 16cm away from the communicating nodes, it experiences independent channel variations such that no useful information is revealed to it.

IV. PERFORMANCE ANALYSIS AND COMPARISON

A. Probability of Successful Key Generation

In the pairwise key generation protocol, each node generates a random initial phase and computes a phase estimate from the sinusoidal beacon observation in each round. We define phase estimation errors $\tilde{\phi}_{12}$ and $\tilde{\phi}_{21}$, where $\tilde{\phi}_{12} = \hat{\phi}_{12} - \phi_{12}$ and $\tilde{\phi}_{21} = \hat{\phi}_{21} - \phi_{21}$.

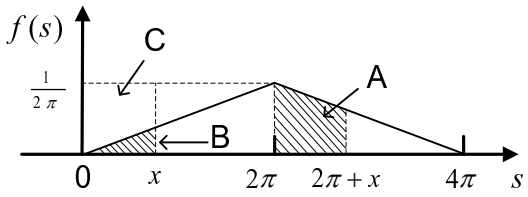


Fig. 3: PDF of s

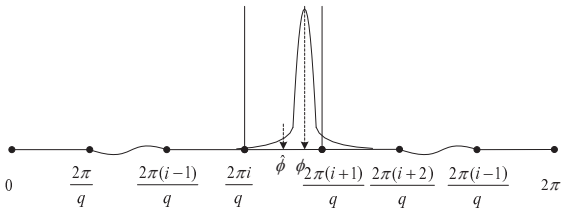


Fig. 4: Estimation error distribution

To facilitate analysis, we assume the duration of the transmitted beacons is equal (*i.e.*, the observation time $T_i = T_o$ for all beacons) and the phase estimates at all sources are unbiased. Note that all observations in different timeslots or at different nodes are affected by independent noise realizations. When the number of samples in the observation increases, the estimation errors converge to zero-mean Gaussian random variables with variances σ_ϕ^2, which can be lower-bouned by the Cramer-Rao bounds (CRB) [9]. When estimating the unknown phase of a sampled sinusoid of amplitude a in white noise with Power Spectral Density (PSD) $\frac{N_0}{2}$, the CRBs for the variance of the phase estimate is given as (refer to [9] for details of single-tone parameter estimation):

$$\sigma_\phi^2 \quad \geq \quad \frac{2f_s N_0(2N-1)}{a^2 N(N+1)} \approx \frac{4N_0}{a^2 T_o}, \tag{1}$$

where f_s is the sampling rate, N is the number of samples in the observation, and T_o is the the observation time (*i.e.*, beacon duration) in second. The approximations can be obtained by assuming that N is large and the fact that $N/f_s = T_o$.

Let P_{QIA} denote the probability that both nodes generate the same quantization index in one round, *i.e.*, the probability of achieving quantization index agreement (QIA). In round k, Φ_1^k and Φ_2^k are quantized into q levels resulting $\log_2(q)$ bits. Thus, with a desired key of size $|K|$, the probability that both nodes generate the same key is given by $p_{key} = P_{QIA}^{|K|/\log_2(q)}$.

In Section III-A, we use Φ_1^k and Φ_2^k to denote the phase components for bit generation in round k. To facilitate analysis, let $\phi = \phi_{12} + \phi_2 = \phi_{21} + \phi_1$ denote the "true" value without estimation errors. To characterize the distribution of ϕ, we have the following Lemma:

Lemma 1: Let $m, n \in [0, 2\pi]$ be two independent random variables that uniformly distributed over $[0, 2\pi]$, then $s_M = m + n \bmod 2\pi$ is also uniformly distributed over $[0, 2\pi]$.

Proof: According to probability theory, the probability density function (PDF) of sum of two independent random variables is the convolution of their PDFs. As shown in Fig. 3, the PDF of s has following form

$$f(s) = \begin{cases} \frac{1}{4\pi^2} s & 0 \leq s < 2\pi \\ \frac{1}{4\pi^2} s + \frac{1}{\pi} & 2\pi \leq s < 4\pi. \end{cases}$$

Thus, given $s \in [0, 4\pi]$, the cumulative distribution function (CDF) of $s_M = s \bmod 2\pi$ can be computed as

$$\begin{aligned} \mathbf{P}\{s_M \leq x\} &= \mathbf{P}\{s \bmod 2\pi \leq x\} \\ &= \int_0^x f(s)ds + \int_{2\pi}^{2\pi+x} f(s)ds, \end{aligned}$$

where $x \in [0, 2\pi]$. $P\{s_M \leq x\}$ is equivalent to sum of area of regions A and B. Due to the symmetry of $f(s)$, the area of region A equals to that of region C. Thus, $\mathbf{P}\{s_M \leq x\} = \int_0^x \frac{1}{2\pi} du (u \in [0, 2\pi])$, where $f_U(u) = \frac{1}{2\pi}$. According to the definition of CDF, the PDF of s_M is equivalent to $\frac{1}{2\pi}$, which implies the s_M is uniformly distributed over $[0, 2\pi]$. ■

The following proposition quantifies the probability P_{QIA}.

Proposition 1: Assume a sampled sinusoid with unknown phase has amplitude a in white noise with PSD $\frac{N_0}{2}$, P_{QIA} at S_1 and S_2 can be approximated as

$$\int_{\frac{2\pi i}{q}}^{\frac{2\pi(i+1)}{q}} P_i^2(\phi) \frac{q}{2\pi} d\phi,$$

where $P_i(\phi) = \int_{\frac{2\pi i}{q}}^{\frac{2\pi(i+1)}{q}} \frac{1}{\sqrt{2\pi}\sigma_\phi} e^{-\frac{(x-\phi)^2}{2\sigma_\phi^2}} dx$.

Proof: In our protocol, ϕ_1 and ϕ_2 are chosen uniformly at random over $[0, 2\pi]$ and channel phase $\theta_{12}(\theta_{21})$ is also uniformly distributed over $[0, 2\pi]$ [6]. Based on Lemma 1, the true phase $\phi = \phi_{12}(\phi_{21}) + \phi_2(\phi_1) \bmod 2\pi = \phi_1 + \theta_{12}(\theta_{21}) + \phi_2 \bmod 2\pi$ is uniformly distributed over $[0, 2\pi]$.

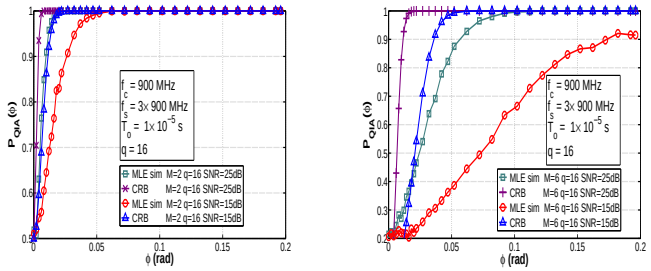
Without loss of generality, assume that ϕ falls into the i-th sector $[\frac{2\pi i}{q}, \frac{2\pi(i+1)}{q})$ $(i \in \{0, 1, \cdots, q-1\})$. As phase estimation errors are independent and Gaussian distributed according to the CRB in Eq.(1), the probability that $\hat{\phi} = \phi + \tilde{\phi}_{12}(\tilde{\phi}_{21}) \in [\frac{2\pi i'}{q}, \frac{2\pi(i'+1)}{q})$ is (see Fig. 4)

$$P_{i'}(\phi) = \int_{\frac{2\pi i'}{q}}^{\frac{2\pi(i'+1)}{q}} \frac{1}{\sqrt{2\pi}\sigma_\phi} e^{-\frac{(x-\phi)^2}{2\sigma_\phi^2}} dx,$$

where $i' \in \{0, 1, \cdots, q-1\}$. Thus, P_{QIA} can be computed as $P_{QIA}(\phi) = \sum_{i'=0}^{q-1} P_{i'}(\phi)^2$. Note that $P_{QIA}(\phi)$ is a function of ϕ. The value of $P_{QIA}(\phi)$ goes up when the "true" ϕ approximates the center of a sector and down when ϕ is close to the boundaries of a sector. In fact, given $\phi \in [0, 2\pi]$, $P_{QIA}(\phi)$ is symmetric to the center of a sector and is changing periodically with period $2\pi/q$. Our simulation results indicate that the variance of phase estimate is much smaller than one. Thus, given $\phi \in [\frac{2\pi i}{q}, \frac{2\pi(i+1)}{q})$, $P_{QIA}(\phi)$ is mainly determined by $P_i(\phi)$ $(i' = i)$. Based on the above analysis, we can compute the average probability of quantization index agreement P_{QIA} as

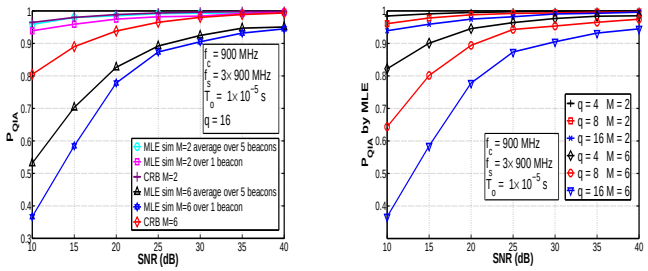
$$P_{QIA} = \int_{\frac{2\pi i}{q}}^{\frac{2\pi(i+1)}{q}} P_{QIA}(\phi) \frac{q}{2\pi} d\phi \approx \int_{\frac{2\pi i}{q}}^{\frac{2\pi(i+1)}{q}} P_i^2(\phi) \frac{q}{2\pi} d\phi.$$

■



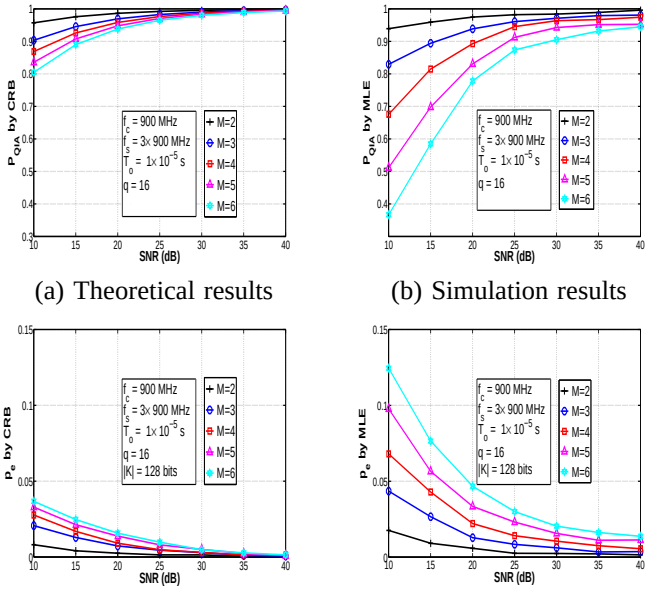
(a) (b)

Fig. 5: P_{QIA} vs. ϕ



(a) (b)

Fig. 7: (a) P_{QIA} vs. SNR. (b) P_{QIA} vs. SNR under different q, M.



(a) Theoretical results (b) Simulation results

(c) Theoretical results (d) Simulation results

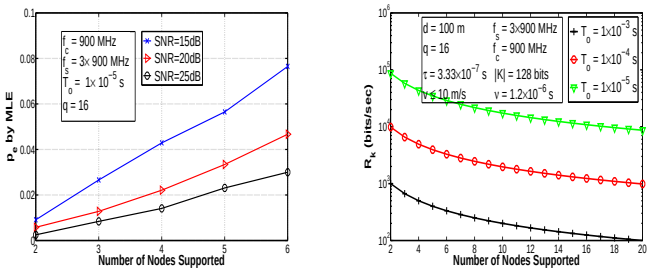
Fig. 6: P_{QIA} and p_e vs. SNR

Now we consider P_{QIA} for group key generation (*i.e.*, $M > 2$). As described in Section III-B, estimations in different timeslots or at different nodes are independent. Thus, the variance of the accumulated estimation errors across M nodes is $\sigma_M^2 = M\sigma_\phi^2$. We can write P_{QIA} as $P_{QIA} \approx \int_{\frac{2\pi i}{q}}^{\frac{2\pi(i+1)}{q}} P_i^M(\phi)\frac{q}{2\pi}d\phi$, where $P_i(\phi) = \int_{\frac{2\pi i}{q}}^{\frac{2\pi(i+1)}{q}} \frac{1}{\sqrt{2\pi}\sigma_M} e^{-\frac{(x-\phi)^2}{2\sigma_M^2}} dx$. The above analysis completes the characterization of P_{QIA} and provides analytical performance predictions based on CRB.

Simulations. Next we present the simulation results of our key generation protocols under multipath channels. We assume that the primary beacon frequency is $\omega_c = 2\pi \cdot 900 \cdot 10^6$ radian/sec and the oscillator phase noise variance parameter is assumed to be 20 rad$^2\cdot$ Hz (the other parameters will be illustrated in specific simulation settings below). Two different methods are used here to estimate the variance of the phase estimation error: (i) full ML estimation and (ii) approximate analytical predictions using CRB for σ_ϕ^2. We use Gray codes (one bit of error is introduced between adjacent sectors) to encode the quantization indices to reduce the bit discrepancies.

We first show how the probability of quantization index agreement is affected by the locations of the true phase ϕ. Fig. 5 plots $P_{QIA}(\phi)$ vs. ϕ from 0 to $\frac{\pi}{q}$ when $T_o = 10\mu s$ and $q = 16$. As we have discussed before, $P_{QIA}(\phi)$ is symmetric to the center of a sector and is changing periodically with period $2\pi/q$. Thus, only ϕ that ranges from 0 to $\frac{\pi}{q} = \frac{\pi}{16} = 0.1963$ is plotted for illustration. We also evaluate the effect of SNR and the number of nodes on the value of $P_{QIA}(\phi)$. The results in Fig. 5 (a) shows that at a low SNR of $10\log_{10}(a^2/2\sigma^2) = 15$dB ($\sigma^2$ is the variance of Gaussian white noise), $P_{QIA}(\phi)$ approaches to 1 quickly when ϕ increases to 0.05 and $P_{QIA}(\phi)$ is low when ϕ gets close to the boundary of the sector. This is because in the boundary region, the probability that $\hat{\phi}$ falls into the neighboring sector becomes larger. As shown in Fig. 5 (b), when the number of nodes M increases, it requires a larger ϕ for $P_{QIA}(\phi)$ to reach 1. As expected, when SNR increases to 25dB, the performance becomes much better especially in the case of $M = 6$. These results suggest that when the number of nodes in a group increases, SNR should also be increased correspondingly to compensate for the larger variance of estimation errors. In addition to the Monte Carlo simulations, Fig. 5 also plots the CRB bound for $P_{QIA}(\phi)$. The close match of the simulation and analytical results shows that the CRB can be used to efficiently predict the performance of pairwise key generation ($M = 2$). Note that when M is large, the CRB becomes less accurately to approximate MLE. This is because the accumulated phase estimation error goes up when M increases, which leads to larger variance of phase estimate (Similar results can be found in Fig. 6).

We next consider the effect of SNR, the number of group nodes M and the number of quantization levels q on P_{QIA} (after averaging over ϕ) and the probability of bit error p_e. Given parameters $T_o = 10\mu s$ and $q = 16$, Fig. 6 (a) and (b) plot the theoretical and simulation results of P_{QIA} vs. SNR under different M, respectively. Similar to Fig. 5, the results show that the higher the SNR, the better matches between the simulation results and CRB results. This is due to the fact that the CRB results become increasingly inaccurate for low SNRs [11]. The deviations between simulation and the CRB results also increases as the number of nodes increases, this is due to the accumulation estimation errors across multiple nodes. Fig. 6 (c) and (d) plot the bit error rate (BER) of generating a key of size $|K| = 128$bit. We define BER as the ratio of bit



(a) (b)

Fig. 8: (a) P_e vs. R_k. (b) R_k vs. number of nodes supported.

discrepancies to $|K|$. The results show that a very low BER can be achieved even in low SNR regimes (*e.g.*, below 20dB). This is due to the use of Gray codes where a quantization index disagreement between two adjacent sectors only introduces one bit error. For such a low BER, $[n, k, 2t+1]_2$-BCH codes with appropriate error correcting capabilities can be used to reconcile these bit discrepancies. Fig. 7 (b) plots the simulation results for P_{QIA} as a function of SNR for different values of q. As expected, a higher SNR is needed to achieve a desired P_{QIA} for large q. In fact, there is a tradeoff since the use of lower values of q leads to low bit generation rate.

In the above settings, the quantization is based on phase estimates generated from a single beacon, a potential improvement on P_{QIA} is to perform quantization based on estimates generated from multiple beacons which have the same initial random phase. We quantize the average of multiple estimates into bit vectors. Let L denote the number of times a beacon with the same initial phase is transmitted. Fig. 7 (a) plots the P_{QIA} vs. SNR under $L = 5$. The results show that with multiple-beacon based estimation, P_{QIA} can be further reduced and the CRB approximation is quite accurate especially for $M = 2$. However, a larger L also undermines the bit generation rate.

B. Scalability and Secret Bit Generation Rate

In our key generation protocol, the number of nodes that can be supported (scalability) and the secret bit generation rate are correlated to each other. Due to the accumulation of estimation errors in group key generation $(M > 2)$, the size of the node group is constrained by the required BER. Fig. 8 (a) plots BER p_e vs. the number of nodes supported under different SNRs. The results show that given a fixed SNR, p_e increases almost linearly as the number of nodes increase. Assume $[127, 85, 13]_2$-BCH code is utilized in the system with error tolerance $\frac{t}{n} \approx 4.72\%$. According to Fig. 8 (a), given SNR=20dB the group size cannot exceed 6; otherwise the system cannot correct the bit errors. Although more powerful BCH codes with high error tolerance can be used to increase the scalability, it leads to more privacy leakage in the key reconciliation step [7].

We next consider the effect of mobility on the scalability. In a mobile scenario, assume $|k| = 128$bit, $q = 16$, $f_c = 900$MHz, $v = 10$m/s and the maximum distance between nodes is $d = 100$m. We choose $T_o = 100\mu$s to ensure high estimation accuracy and it is much larger than the delay spread ν. Thus, the Doppler frequency shift is $f_d = \frac{v}{\lambda} = 30$Hz, which results a coherence time $T_c = \frac{0.423}{f_d} = 14$ms. To guarantee link reciprocity during key generation, T_c is required to include at least one round time:

$$2M(T_o + \tau + \nu) \quad < \quad T_c,$$

where $\tau = \frac{d}{c} = 3.33 \times 10^{-7}$s and ν is the delay spread with a typical value 1.2×10^{-6}s. Then, we can bound the number of nodes supported as $M < 68$.

Based on the above discussion, we can determine the secret bit generation rate as follows: given SNR, acceptable BER based on the error correcting capability, we can first determine the maximum group size the system can support. Then, the approximate secret-bit rate can be computed as $R_k \approx \frac{|K|}{(2M)(T_o+\tau+\nu)} \frac{\log_2(q)}{|K|}$. Here, we assume $|K|/\log_2(q)$ rounds can be run either in the same coherence time period or across multiple coherence time periods. Fig. 8 (b) plots the secret-bit generation rate vs. the number of nodes supported under different observation times. As an example, given SNR=20dB, $T_o = 10\mu$s and $[127, 85, 6]_2$-BCH code, the maximum number of nodes supported is $M = 6$. Thus, the analytical secret-bit rate can be 10^4bit/s approximately.

TABLE I: NIST statistical test. To pass this test, the p-value must be greater than 0.01.

TEST	p − value
DFT	0.9086
Lempel Ziv Compression	1.0
Monobit Frequency	0.8597
Runs	0.8682
Approximate Entropy	0.9286
Cumulative Sums (Forward)	0.9493
Cumulative Sums (Reverse)	0.8188
Block Frequency	0.8666
Serial	0.8825, 1.0000

C. Randomness of Secret Bits

A cryptographic key should be substantially random, otherwise the adversary can crack the key with low time-complexity. We employ a widely used randomness test suit NIST to verify the randomness of the secret-bit generated from our simulation [12]. In the test, we randomly select 10 bit sequences generated from our simulation in both static and mobile cases, and compute their p-values for 8 tests. All the p-values are marginally greater than 0.01, which indicates the sequence is random. The results in Table 1 shows that the average entropy of our generated bit sequences is very close to a truly random sequence.

D. Comparisons with Related Work

This section presents a comparison between our key generation schemes and the existing RSS-based key generation methods. Due to space limitation, we only focus on the closely related work. Most of the previous work on RSS-based key generation are based on the quantization of RSS measurements for bit extraction [3], [4], [2]. In [3], the authors proposed a key generation scheme which quantizes the matching deep fades of RSS measurements based on a pre-defined threshold

γ, *i.e.*, generate 1 if $RSS_d > \gamma$ or generate 0 if $RSS_d < \gamma$. In [2], the authors proposed a scheme that uses level-crossings and quantization to extract bits from RSS measurements or estimated channel impulse response (CIR). The two nodes alternately send known probe signals to each other and estimate the channel response at successive time instants. Secret bits are generated from *excursions* of channel estimates above γ (output 1) or below $-\gamma$ (output 0) that are of a duration equal to m samples. The authors in [4] evaluate the effectiveness of RSS-based key extraction in real environments and show that due to lack of channel variations static environments are not suitable for establishing secure keys.

Excellent efficiency: Compared to the RSS-based methods, our scheme has a much higher secret bit generation rate. There are two major reasons: First, these RSS-based methods either use only the deep fades [3] or RSS measurement above or below the threshold [4], [2], the other samples are all discarded. In particular, if all bits are generated from *excursions*, this will cause a large loss of bits as only one secret bit can be generated from m successive RSS measurements. Different from them, our scheme quantizes phase estimate into multiple bits by using a multi-bit quantization scheme. Second, to maintain a high level of average entropy of key, the bit extraction rate of the RSS-based methods can not exceed Doppler frequency shift f_d too much [2]. However, for a given *coherence time* our scheme can run multiple rounds to generate more bits due to the introduction of phase randomness.

Scalability: Compared to the RSS-based methods that only applicable for pairwise key generation [3], [4], [2], our scheme can support both pairwise key and group key generation. For group key generation, common information should be shared among the group nodes. However, the RSS measurements obtained between a pair of nodes are only shared between themselves. The secure transmission of RSS values to other nodes requires the establishment of secure channels. Establishing group key for secure communication is therefore the same problem as the one we intend to solve. Our scheme relies only on the transmission of periodical extensions of unmodulated sinusoidal beacons, which allows effective accumulation of channel phases across multiple nodes for secret bit generation.

Flexibility: Compared to the RSS-based methods, our scheme can be applied in both static and mobile cases for key generation. The channel impulse response is essentially invariant over the *coherence time*, which is inversely proportional to the Doppler frequency shift f_d. Due to the lack of channel variations in static environments, the RSS-based scheme has to rely on node mobility to reduce the coherence time (or increase f_d) [4], [2]. However, our scheme does not have this constraint. Even in a static case, the introduction of random initial phases (*i.e.*, ϕ_1 and ϕ_1') in each round can effectively cause variations used for bit extraction.

Sound randomness: Compared to the RSS-based methods, our scheme can generate secret bit sequences with higher average entropy. This is because RSS measurements are not uniformly distributed, the key generation scheme highly depends on variation of the channel to ensure the key randomness [3], [4], [2]. Our scheme employs the inherent uniform randomness of channel phases in multipath channels. As analyzed in Section IV-A, the sum of initial phases and channel phases along the transmission circuit is uniformly distributed over $[0, 2\pi]$. Thus, when quantized into bit vectors, the randomness of the generated key is guaranteed.

V. Concluding Remarks

In this paper, we proposed a new secret key generation approach that utilizes the uniformly distributed phase information of channel responses to extract shared cryptographic keys under narrowband multipath fading models. The proposed approach enjoys a high key bit generation rate and achieved scalability and flexibility, and was thoroughly evaluated through both analytical and simulation studies. Compared to existing work that focus on pairwise key generation, our approach is highly scalable and can improve the analytical key bit generation rate by a couple of orders of magnitude. In the above discussion, we assume that nodes in the network share a common time reference. However, when there exists no common time reference among the nodes, they have to keep time using their own independent local oscillator. In this case, each node estimates the phase of received beacons relative to its own time reference, and absolute estimates have an unknown "phase offset" that depend on the phase of the local time reference at each node itself. In our future work, we propose to extend our key generation protocol to an asynchronous setting without relying on a common time reference.

Acknowledgment

This work is partially supported by the US National Science Foundation under grant CNS-0831963.

References

[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. IT-22, pp. 644–654, 1976.

[2] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: extracting a secret key from an unauthenticated wireless channel," in *MobiCom'08*.

[3] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *CCS'07*.

[4] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *MOBICOM'09*.

[5] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *IEEE Transactions on Mobile Computing*, vol. 9, pp. 17–30, 2010.

[6] A. Goldsmith, *Wireless Communications*. Cambridge University Press, 2005.

[7] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, "Fuzzy extractors: How to generate strong keys from biometrics and other noisy data," *SIAM J. Comput.*, vol. 38, no. 1, pp. 97–139, 2008.

[8] B. Kanukurthi and L. Reyzin, "Key agreement from close secrets over unsecured channels," in *EUROCRYPT'09*.

[9] D. Rife and R. Boorstyn, "Single-tone parameter estimation from discrete-time observations," *IEEE Transactions on Information Theory*, vol. 20, no. 5, pp. 591–598, 1974.

[10] D. R. B. III and H. V. Poor, "Time-slotted round-trip carrier synchronization for distributed beamforming," *IEEE Transactions on Signal Processing*, vol. 56, no. 11, pp. 5630–5643, 2008.

[11] F. Athley, "Threshold region performance of maximum likelihood direction of arrival estimators," *IEEE Transactions on Signal Processing*, vol. 53, no. 4, pp. 1359–1373, 2005.

[12] NIST, *A Statistical Test Suite For Random and Pseudorandom Number Generators For Cryptographic Applications*, 800th ed., National Institute of Standards and Technology, 2001.