Secret Key Generation From Mobility

Onur Gungor, Fangzhou Chen, C. Emre Koksal
Department of Electrical and Computer Engineering
The Ohio State University, Columbus, 43210

***Abstract*—We consider secret key generation from relative localization information of a pair of nodes in a mobile wireless network in the presence of a mobile eavesdropper. Our scheme consists of two phases: in the first phase, legitimate node pair exchanges beacon signals to establish localization information based on noisy observations of these beacons; in the second phase, nodes generate secret key bits via a public discussion. Our problem can be categorized under the source models of information theoretic secrecy, where the distance between the legitimate nodes acts as the observed common randomness. We characterize the achievable secret key bit rate in terms of the observation noise variance at the legitimate nodes and the eavesdropper. This work provides a framework that combines information theoretic secrecy and wireless localization, and proves that the localization information provides a significant additional resource for secret key generation in mobile wireless networks.**

I. Introduction

We consider the generation of a common key in a pair of nodes, which move in $\mathbb{R}^2$ (continuous space) according to a discrete time stochastic mobility model. An eavesdropper is also mobile with a mobility pattern, independently of those of the legitimate nodes. We exploit the reciprocity of the distance between a given pair of locations, view the distance between the legitimate nodes as a common randomness shared by these nodes and utilize it to generate secret key bits using the ideas from source models of secrecy.

We propose a system, in which the legitimate nodes use a two stage key generation process: (1) In the first stage, they repeatedly exchange wireless beacons to obtain information regarding the sequence of distances between them over many time slots as they move in the area. The beacon signal may contain explicit information such as a time stamp, or the receiving node can extract other means of localization information by analyzing the angle of arrival, the received signal strength (RSS), etc. We assume that the eavesdropper overhears the beacons and tries to deduce the distance information based on these observations. (2) In the second stage, the nodes communicate over the public channel to agree on a "reliable" secure key based on the observed sequence of relative distances. Using a source model of secrecy, we characterize the achievable secret key bits in terms of the observation noise variance at the legitimate nodes and the eavesdropper. We show that localization information provides a significant additional resource for secret key generation.

Next, we consider the case where legitimate nodes are capable of improving the observation quality by exchanging multiple beacons at a given location. Note however that the improvement comes at the expense of the eavesdropper also improving its observations. We study the tradeoffs involved and show that, while in some cases it may be possible to increase the beacon rate unboundedly with the number of beacons, if the eavesdropper possesses certain capabilities such as measuring the angle of arrival, increasing the number of beacons do not necessarily increase the achievable key rate beyond a certain limit. We also study the loss of key rate due to imperfections such as quantization noise and clock mismatch.

II. Related Work

Source model of secrecy studies generation of secret key bits from common randomness observed by legitimate nodes. In his seminal paper, Maurer showed that, if two nodes observe correlated randomness, then they can agree on a secret key through public discussion [1]. He provided upper and lower bounds on the achievable secret key rates, considering that the nodes have unlimited access to a public channel, accessible by the eavesdropper. Although the upper and lower bounds have been improved over time [2], [3], the secret key capacity of the source model in general is still an open problem. Despite this fact, the source model has been extended to several different settings [4].

There is a vast amount of literature on localization in wireless networks (see, e.g., [5]–[7], and the references therein). There has been some focus on secure localization and position-based cryptography [8]–[11], however, these works either consider key generation in terms of other forms of secrecy (i.e., computational secrecy), or fall short of covering a complete information theoretic analysis. Also a similar line of work in wireless network secrecy considers channel identification [12] for secret key generation. Based on the channel reciprocity assumption, nodes at both ends experience the same channel, corrupted by independent noise. Therefore, nodes can use their channel magnitude and phase response observations to generate secret key bits from public discussion. Another notable work [13] considers secret key generation from common phase information. Considering a narrow-band fading model, the authors describe a hierarchical structure to generate keys, with applications to multi-node key generation. However, the security of the model depends on the fact that eavesdropper's phase observation is independent of the legitimate nodes' phase observation, which does not hold if the eavesdropper observes or estimates the positions and velocities of legitimate nodes using the received signals.

Note that, our approach of using the distances robust with respect to channel issues. There may be numerous scenarios in which channel reciprocity does not hold (e.g., presence

of ground reflections), which leads to the failure of the approaches based on that assumption. However, the distance (or the propagation delay) between two points is identical in both directions, regardless of the medium.

III. System Model

Consider a simple network consisting of two mobile legitimate nodes, called user 1 and 2, and a possibly mobile eavesdropper e. We divide time into discrete slots $\{1, \cdots, n\}$, where slot i covers the time interval $[iT,\ (i+1)T)$. We assume T to be large enough for many beacon-signal[1] exchanges to be possible, but too short for a significant location change to occur. Hence, we assume the location to be constant within a slot. Let $x_j[i] \in \mathbb{R}^2$ be the random variable that denotes the location of node $j \in \{1, 2, e\}$ at slot i in cartesian coordinates. The distance between nodes 1 and 2 in slot i is $d_{12}[i] = |x_1[i] - x_2[i]|$. We use the notation $\mathbf{d}_{12} = \{d_{12}[i]\}_{i=1}^n$. Similarly $\mathbf{d}_{1e}$, $\mathbf{d}_{2e}$ denotes the sequence of distances between nodes $(1, e)$ and nodes $(2, e)$ respectively. Hence, the distance vectors form n triangles, one of which is shown in Figure 1. Furthermore, let $\phi_e[i]$ denote the angle of the triangle at node e at slot i, and $\boldsymbol{\phi}_e = \{\phi_e[i]\}_{i=1}^n$. For the n-tuples $(\hat{\mathbf{d}}_1, \hat{\mathbf{d}}_2)$,

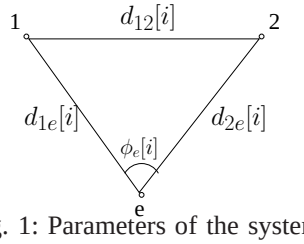


Fig. 1: Parameters of the system

we denote the joint probability density function as $f(\hat{\mathbf{d}}_1, \hat{\mathbf{d}}_2)$, and define [14]

- The mutual information as

$$\mathcal{I}(\hat{\mathbf{d}}_1; \hat{\mathbf{d}}_2) = \log\left(\frac{f(\hat{\mathbf{d}}_1, \hat{\mathbf{d}}_2)}{f(\hat{\mathbf{d}}_1) f(\hat{\mathbf{d}}_2)}\right)$$

- The *average* mutual information as

$$I(\hat{\mathbf{d}}_1; \hat{\mathbf{d}}_2) = \mathbb{E}[\mathcal{I}(\hat{\mathbf{d}}_1; \hat{\mathbf{d}}_2)]$$

- The *spectral-inf* mutual information rate as

$$\text{p-}\liminf_{n\to\infty} \frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_1, \hat{\mathbf{d}}_2) = \sup\left\{\beta : \lim_{n\to\infty} \mathbb{P}\left(\frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_1; \hat{\mathbf{d}}_2) < \beta\right) = 0\right\}$$

- The *spectral-sup* mutual information rate as

$$\text{p-}\limsup_{n\to\infty} \frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_1, \hat{\mathbf{d}}_2) = \inf\left\{\alpha : \lim_{n\to\infty} \mathbb{P}\left(\frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_1; \hat{\mathbf{d}}_2) > \alpha\right) = 0\right\}$$

Similarly, define the entropy, and the average entropy of $\hat{\mathbf{d}}_1$ as $\mathcal{H}(\hat{\mathbf{d}}_1) = \log\left(\frac{1}{f(\hat{\mathbf{d}}_1)}\right)$, and $H(\hat{\mathbf{d}}_1) = \mathbb{E}[\mathcal{H}(\hat{\mathbf{d}}_1)]$, respectively.

[1]We keep the definition of the beacon signal general as a short signal bearing localization information on the initiating node.

The legitimate nodes generate secret key bits from their mobility patterns in two phases: *localization* and *key generation*. In the first (localization) phase, nodes observe the sequence of distances using the beacon signals (e.g., by using the propagation delay (time of arrival) of electromagnetic signals [5]). In the second (secure key generation) phase, the nodes generate secret key bits from the common localization information via public discussion. Now, we explain these phases in more detail:

Phase I - localization: At the beginning of each slot i, node 1 broadcasts a beacon. Considering perfect clock synchronization of the nodes[2], nodes 2 and e obtain a noisy observation of $d_{12}[i]$ and $d_{1e}[i]$ respectively. Let these observation be $\hat{d}_2[i]$ and $\hat{d}_{1e}[i]$. Similarly, node 2 follows up with a beacon and nodes 1 and e observe $\hat{d}_1[i]$ and $\hat{d}_{2e}[i]$, respectively. With the observations of both the beacons, the eavesdropper also obtains a noisy observation, $\hat{\phi}_e[i]$, of the angle between the legitimate nodes. The first phase ends after n slots.

Phase II - key generation: In the second phase, nodes 1 and 2 agree on a secret key based on the observation sequence $\hat{\mathbf{d}}_1 = \{\hat{d}_1[i]\}_{i=1}^n$ and $\hat{\mathbf{d}}_2 = \{\hat{d}_2[i]\}_{i=1}^n$ by communicating over an error-free public channel. This phase is commonly referred to in the source model literature as the public discussion phase [1]. A public discussion algorithm $C_1, \cdots, C_t$ is a t step message exchange protocol, where node 1 send messages $C_1, C_3, \cdots$, at odd steps, and node 2 sends messages $C_2, C_4, \cdots$ at even steps, according to a deterministic function such that

$$H(C_i|\hat{\mathbf{d}}_1, C_{i-1}, \cdots, C_1) = 0,\ \text{odd } i \tag{1}$$

$$H(C_i|\hat{\mathbf{d}}_2, C_{i-1}, \cdots, C_1) = 0,\ \text{even } i \tag{2}$$

At the end of the t step protocol, node 1 obtains S_1, and node 2 obtains S_2 as the secret key, where

$$H(S_j|\hat{\mathbf{d}}_j, C^t) = 0,\ j \in \{1, 2\} \tag{3}$$

Independent of the localization phase, let the eavesdropper obtain its global position observation $\hat{\mathbf{x}}_e$. Then, $\hat{\mathbf{e}} = \{\hat{\mathbf{d}}_{1e}, \hat{\mathbf{d}}_{2e}, \hat{\boldsymbol{\phi}}_e, \hat{\mathbf{x}}_e\}$ denotes the set of eavesdropper's complete observations of the system. We say that secret key bits are reliably generated at rate R if $\forall \epsilon > 0$, $\exists n, t$ such that (1), (2) and (3) are satisfied, and

$$H(S_j)/n = R,\ j \in \{1, 2\}$$
$$\mathbb{P}(S_1 \neq S_2) \leq \epsilon$$
$$I(S_j; \hat{\mathbf{e}}, C^t)/n \leq \epsilon,\ j \in \{1, 2\}$$

The problem of finding a public discussion algorithm $C_1, \cdots, C_t$ that maximizes R is out of the scope of this paper. Our purpose is to understand the effect of localization parameters on achievable key rate R.

[2]We consider the possibility of clock mismatch in Section VI-B and argue that clock asynchrony can be corrected asymptotically as the number of slots $n \to \infty$.

IV. Upper/Lower Bounds

The following corollaries establish the upper and lower bounds on the key bits achievable through public discussion.

Corollary 1: The following key rate is achievable through one way public discussion.

$$R_L = \max\left\{ \left[\text{p-}\liminf_{n\to\infty} \frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_1;\hat{\mathbf{d}}_2) - \text{p-}\limsup_{n\to\infty} \frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_1;\hat{\mathbf{e}}) \right]^+, \left[\text{p-}\liminf_{n\to\infty} \mathcal{I}(\hat{\mathbf{d}}_2;\hat{\mathbf{d}}_1) - \text{p-}\limsup_{n\to\infty} \frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_2;\hat{\mathbf{e}}) \right]^+ \right\} \quad (4)$$

Corollary 2: An upper bound for the key rate achievable through any public discussion is

$$R_U = \min\left\{ \text{p-}\liminf_{n\to\infty} \frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_1;\hat{\mathbf{d}}_2), \text{p-}\liminf_{n\to\infty} \frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_1;\hat{\mathbf{d}}_2|\hat{\mathbf{e}}) \right\} \quad (5)$$

Both corollaries follow directly from Theorem 4 in [14], which generalizes Maurer's results on secret key generation through public discussion [1], to non-i.i.d. settings.

Remarks: **(1)** In this work, we only consider secret key generation from the observations of distance information $\mathbf{d}_{12}$ of the legitimate nodes. One can achieve higher key rates by also considering the the angle and global position information. **(2)** There are better upper and lower bounds available in the literature. By using two-way public discussion, and using randomization at the encoders, one can achieve better lower bound, which is tight for one way public discussion case [2]. Furthermore, a better upper bound is given in [3]. We chose the above bounds for the simplicity of evaluation.
(3) Note that $\hat{\mathbf{e}}$ depends on the capabilities of the eavesdropper. If the eavesdropper cannot estimate the angle-of-arrival, i.e., if the eavesdropper is only equipped with single omnidirectional antenna, then $\hat{\boldsymbol{\phi}}_e = \emptyset$. Similarly, if the eavesdropper cannot observe its global position in the field, then $\hat{\mathbf{x}}_e = \emptyset$. In this work, we only consider the availability of angle information in the eavesdropper, and leave the possibility of the global position observation as a future work.

Equations (4) and (5) are valid for the general stochastic mobility models. In the sequel, we analyze R_L and R_U for the special case where node locations are i.i.d. and observation of the nodes are corrupted by independent additive Gaussian noise. Note that, due to the i.i.d. mobility structure, the conditioning on the past and future observations in R_L and R_U disappear. Hence, we omit the index i and use $f(d_{12}, d_{1e}, d_{2e}, \phi_e)$ to denote the joint probability density function of the node distances and angle at node e, which are the variables that characterize the triangle given in Figure 1. For this case, the upper and lower bound expressions become

$$R_L = \max\left(\left[I(\hat{d}_1;\hat{d}_2) - I(\hat{d}_1;\hat{d}_{1e},\hat{d}_{2e},\hat{\phi}_e) \right]^+, \left[I(\hat{d}_2;\hat{d}_1) - I(\hat{d}_2;\hat{d}_{1e},\hat{d}_{2e},\hat{\phi}_e) \right]^+ \right) \quad (6)$$

$$R_U = \min\left(I(\hat{d}_1;\hat{d}_2), I(\hat{d}_1;\hat{d}_2|\hat{d}_{1e},\hat{d}_{2e},\hat{\phi}_e) \right) \quad (7)$$

where the distance observations and eavesdropper angle observations can be expressed as (omitting the slot index for simplicity)

$$\hat{d}_j = d_{12} + N_j, \quad j \in \{1,2\} \quad (8)$$

$$\hat{d}_{je} = d_{je} + N_{je}, \quad j \in \{1,2\} \quad (9)$$

$$\hat{\phi}_e = \phi_e + N_\phi \quad (10)$$

and N_j, N_{je}, and N_ϕ are zero mean Gaussian noise with variances σ_j^2, σ_{je}^2, and σ_ϕ^2 respectively[3]. Note that the noise in distance observations is due to the limited clock precision, corruption of beacons due to channel noise at the receiver antenna and fading. The case in which there is no angle estimation by the eavesdropper can be represented by choosing the phase estimation error uniform in $(0, 2\pi)$: $N_\phi \sim \mathcal{U}[0, 2\pi]$.

V. Multiple Beacons

Next, we consider the case where legitimate nodes exchange multiple beacons at each time slot. This reduces the observation noise for both the legitimate nodes and the eavesdropper and in this section we study the tradeoffs involved.

Suppose, in each slot, the legitimate nodes exchange K beacons instead of 1. Then, the set of observations for all nodes form a 2-dimensional discrete sequence, e.g., node 1 observes $\{\hat{d}_1[i,1], \cdots, \hat{d}_1[i,K]\}$ in the ith time slot. The observation of each beacon (i,k) has the form given in (8)-(10), where we assume that the noise sequences $N_j[i,k]$, $N_{je}[i,k]$, and $N_\phi[i,k]$ are i.i.d. for every observation point. Note that, a sufficient statistic (Section 2.9 in [15]) for $d_{12}[i]$ at node 1 is $\frac{1}{K}\sum_{k=1}^{K} \hat{d}_1[i,k]$. Consequently, the sequence of K observations of each node in slot i can be summarized by a single observation for that slot:

$$\hat{d}_j[i] = d_{12}[i] + \tilde{N}_j[i], \quad j \in \{1,2\} \quad (11)$$

$$\hat{d}_{je}[i] = d_{je}[i] + \tilde{N}_{je}[i], \quad j \in \{1,2\} \quad (12)$$

$$\hat{\phi}_e[i] = \phi_e[i] + \tilde{N}_\phi[i], \quad (13)$$

where $\tilde{N}_j \sim \mathcal{N}(0, \sigma_j^2/K)$, $\tilde{N}_{je} \sim \mathcal{N}(0, \sigma_{je}^2/K)$, and $\tilde{N}_\phi \sim \mathcal{N}(0, \sigma_\phi^2/K)$ if the eavesdropper estimates the angle and $\tilde{N}_\phi \sim \mathcal{U}[0, 2\pi]$ otherwise. We analyze these two cases separately.

With Angle Observation: The eavesdropper has noisy observations for d_{1e}, d_{2e}, and ϕ_e (illustrated in Fig. 1). It can combine these observations to estimate d_{12}. We assume that the eavesdropper uses the cosine law to obtain its estimate $\hat{d}_e$:

$$\hat{d}_e = \sqrt{\hat{d}_{1e}^2 + \hat{d}_{2e}^2 - 2\hat{d}_{1e}\hat{d}_{2e}\cos(\hat{\phi}_e)}. \quad (14)$$

For $K \gg 1$, $\sigma_1^2/K, \sigma_2^2/K \ll d_{12}$, $\sigma_{1e}^2/K \ll d_{1e}$, $\sigma_{2e}^2/K \ll d_{2e}$ and $N_\phi/K \approx 0$ with high probability. Consequently[4], (14) can be approximated with

$$\hat{d}_e \approx d_{12} + \mathcal{N}\Big(0, A + B\Big), \quad (15)$$

[3]Note that the distance observation noise cannot be perfectly Gaussian. However, under the assumptions $\sigma_1, \sigma_2 \ll d_{12}$, $\sigma_{1e} \ll d_{1e}$, $\sigma_{2e} \ll d_{2e}$, the Gaussian assumption is reasonable.

[4]We omit the derivation due to space constraints. The following follows from a sequence of linear approximations in (14)

where $A = \frac{(d_{1e}-d_{2e}\cos(\phi_e))^2\sigma_{1e}^2+(d_{2e}-d_{1e}cos(\phi_e))^2\sigma_{2e}^2}{Kd_{12}^2}$ is the uncertainty that comes from the distance observation errors, and $B = \frac{(d_{1e}d_{2e}\sin(\phi_e)^2)\sigma_\phi^2}{Kd_{12}^2}$ is the uncertainty that comes from the angle estimate error.

No Angle Observation: As $K \to \infty$, $\sigma_j^2/K, \sigma_{je}^2/K \to 0$ for $j \in \{1,2\}$, and due to the lack of an angle estimate at the eavesdropper, $N_\phi \in \mathcal{U}[0, 2\pi]$. Then,

$$\begin{aligned} R_L &= I(\hat{d}_1;\hat{d}_2) - I(\hat{d}_1;\hat{e}) \\ &= h(\hat{d}_1|\hat{d}_e) - h(\hat{d}_1|\hat{d}_2). \end{aligned}$$

We have

$$\begin{aligned} \lim_{K\to\infty} h(\hat{d}_1|\hat{d}_e) &= h(d_{12}|d_{1e},d_{2e}) \\ &\overset{(a)}{=} h(\sqrt{d_{1e}^2+d_{2e}^2-2d_{1e}d_{2e}\cos(\phi_e)}|d_{1e},d_{2e}) \\ &\overset{(b)}{>} -\infty \end{aligned}$$

where (a) follows from the cosine law. For $u, v \neq 0$, $h(\sqrt{d_{1e}^2+d_{2e}^2-2d_{1e}d_{2e}\cos(\phi_e)}|d_{1e}=u, d_{2e}=v) > -\infty$ since ϕ_e is uniform in $[0, 2\pi]$. Further note that $\mathbb{P}(d_{1e}=0) = 0$, and $\mathbb{P}(d_{2e}=0) = 0$ since nodes cannot be on the exact same location at the same time, hence (b) holds. Similarly,

$$\begin{aligned} \lim_{K\to\infty} h(\hat{d}_1|\hat{d}_2) &= \lim_{K\to\infty} h(d_{12}+\tilde{N}_1|d_{12}+\tilde{N}_2) \\ &= \lim_{K\to\infty} h(\tilde{N}_1-\tilde{N}_2|d_{12}+\tilde{N}_2) \\ &= -\infty, \end{aligned}$$

due to the fact that $(\tilde{N}_1+\tilde{N}_2) \sim \mathcal{N}(0, (\sigma_1^2+\sigma_2^2)/K)$. Hence, $\lim_{K\to\infty} R_L = \infty$. Thus, we conclude that, without the angle estimate at the eavesdropper, any positive key rate can be achieved with the sufficiently large choice of the number of beacons K. On the other hand, when eavesdropper can estimate the angle, the key rate converges to a value that depends on the mobility model.

VI. Practical Issues

A. Quantization

Even though the observations $\hat{\mathbf{d}}_1, \hat{\mathbf{d}}_2, \hat{\mathbf{e}}$ of the nodes are from a continuous space, in practice nodes quantize their observations to store them and the quantized values are used in the public discussion. Let $\psi(\cdot)$ be a predetermined quantization function. Then the legitimate nodes $j \in \{1,2\}$ can obtain quantized versions of the distance observation $\hat{\mathbf{d}}_i^\Delta = \psi(\hat{\mathbf{d}}_i, \Delta)$, where $|\Delta| = \max_x |x - \psi(x)|$ is the resolution of quantization. The eavesdropper is also subject to similar quantization constraints and let $\hat{\mathbf{e}}^{\Delta'} = \psi(\hat{\mathbf{e}}, \Delta')$ be its quantization function with another resolution Δ'. Define

$$\begin{aligned} &R_L^{\mathcal{Q}} = \\ &\max\left\{ \left[\text{p-}\liminf_{n\to\infty} \frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_1^\Delta;\hat{\mathbf{d}}_2^\Delta) - \text{p-}\limsup_{n\to\infty} \frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_1^\Delta;\hat{\mathbf{e}}^{\Delta'})\right]^+ \right. \\ &\left., \left[\text{p-}\liminf_{n\to\infty} \mathcal{I}(\hat{\mathbf{d}}_2^\Delta;\hat{\mathbf{d}}_1^\Delta) - \text{p-}\limsup_{n\to\infty} \frac{1}{n}\mathcal{I}(\hat{\mathbf{d}}_2^\Delta;\hat{\mathbf{e}}^{\Delta'})\right]^+ \right\} \end{aligned}$$

Note that, if $\Delta = \Delta'$, then, by the relationship of continuous and discrete mutual information [15], we have $\lim_{|\Delta|\to 0} R_L^{\mathcal{Q}} = R_L$.

B. Clock mismatch

Assume that there is a clock mismatch between nodes 1, and 2. Consequently, all the observations of $\mathbf{d}_{12}$ of nodes 1 and 2 in localization phase are shifted by a random value γ_1 and γ_2 respectively:

$$\hat{d}_j[i] = d_{12}[i] + N_j[i] + \gamma_j \tag{16}$$

for $j \in \{1,2\}$. Note that we assume the amount of mismatch is random, but it remains constant. Considering the case where N_1 and N_2 are zero mean random variables,

$$\mathbb{E}[\hat{d}_j|\gamma_1,\gamma_2] = \mathbb{E}[d_{12}] + \gamma_j. \tag{17}$$

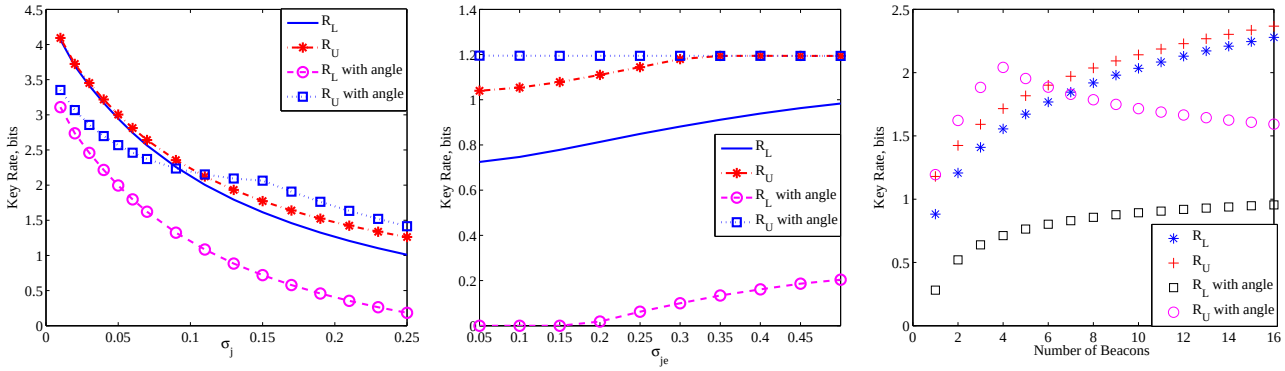
Hence, with the knowledge of the statistics of the mobility, each node $j \in \{1,2\}$ can obtain a perfect estimate of the amount of clock mismatch γ_j as $n \to \infty$, and broadcast it in the public discussion phase. Therefore, clock mismatch does not affect the theoretical bounds of secret key generation rates.

VII. Numerical Results

In this section, we numerically evaluate (6) and (7) for the case where the node locations $\mathbf{x}_1[i]$, $\mathbf{x}_2[i]$ and $\mathbf{x}_e[i]$ for each slot are characterized by i.i.d. circularly symmetric zero mean, unit variance Gaussian random variables. Throughout this section, we assume that the nodes have identical observation noise statistics, i.e., $\sigma_1 = \sigma_2$, and the observation noise for each user is also statistically symmetric at the eavesdropper, i.e., $\sigma_{1e} = \sigma_{2e}$. We assume uniform quantization with precision $|\Delta| = 0.1$ for all nodes, including the eavesdropper. Since $|\Delta| \ll 1$, the calculated rates will be very close to the achievable rates as discussed in Section VI-A. In what follows, we analyze the behavior of R_L and R_U as a function of nodes' observation noise.

In the first example, we fix the eavesdropper observation noise $\sigma_{je} = 0.2,\ j \in \{1,2\}$ and $\sigma_\phi = 0.2$, and observe the key rates as a function of $\sigma_j,\ j \in \{1,2\}$ with and without an angle observation. As shown in Fig. 2a, without angle observation, even the lower bound grows unboundedly as σ_1 and σ_2 decreases. This implies that, theoretically, infinite key rate can be achieved in the case where nodes 1 and 2 have perfect observation of $\mathbf{d}_{12}$. Furthermore, it can be clearly seen that observation of angle by the eavesdropper significantly decreases the secret key rate.

Next, we fix $\sigma_j = 0.3,\ j \in \{1,2\}$ and $\sigma_\phi = 0.2$, and in Figure 2b, we plot R_L and R_U with and without an angle observation, as a function of the eavesdropper observation noise $\sigma_{je},\ j \in \{1,2\}$. Clearly, the secrecy rate increases as the eavesdropper distance observation noise gets stronger. However, the impact of the eavesdropper distance observation noise is much less significant compared to the impact of the observation noise of the legitimate nodes. Indeed, even when the eavesdropper has perfect distance observations, a non-zero key rate is achievable. This, however, is not true when the



(a) (b) (c)

Fig. 2: Key rate vs (a) σ_j, (b) σ_{je}, (c) number of beacons, with and without angle observation

eavesdropper has perfect angle estimates that accompany the perfect distance estimates. In that case, the achievable key rate is 0, since the eavesdropper has perfect knowledge of d_{12}.

Finally, we analyze the impact of multiple beacons. With $\sigma_j = \sigma_{je} = 0.3$ $j \in \{1, 2\}$ and $\sigma_\phi = 0.3$, in Figure 2c, we plot R_L and R_U without and with an angle observation, as a function of the number of beacons. We can see that, using multiple beacons may be beneficial, depending on whether eavesdropper has the angle observation or not. With no angle observation, the key rate grows unboundedly with the number of beacons, as shown in Section V, i.e., the legitimate nodes' benefit by transmitting as many beacons as possible. With an angle observation, the accuracy of the angle estimate as well as the distance estimates at the eavesdropper increase with the number of beacons, and the eavesdropper will be able to locate the nodes highly accurately via the cosine law as n increases. Hence, the key rate remains bounded.

VIII. Conclusion

In this paper, we studied the information theoretic limits of secure key generation using the distance between legitimate nodes in mobile wireless networks. We considered a two stage process to generate keys. In the first stage, legitimate nodes generate relative localization information by exchanging beacons, whereas in the second stage, the nodes generate secret key bits by public discussion. We characterized lower and upper bounds of key rates utilizing results from the source model of secrecy. We showed that when eavesdropper cannot have angle of arrival observation for the transmitted beacons, nodes can highly improve the key rate by exchanging multiple beacons, whereas with an angle observation this is not true. Our current investigations are mainly focused on 1) common secret key generation among multiple nodes in a wireless network, 2) application to wideband localization, and 3) the general non-i.i.d. mobility cases.

References

[1] U.M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Information Theory*, vol.39, no.3, pp.733-742, May 1993

[2] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Information Theory* , vol.39, no.4, pp.1121-1132, Jul 1993

[3] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Information Theory* , vol.45, no.2, pp.499-514, Mar 1999

[4] I. Csiszar and P. Narayan, "Secrecy Capacities for multiterminal channel models," *IEEE Trans. Information Theory*, vol.54, no.6, pp.2437-2452, June 2008

[5] S. Gezici, Z. Tian, G. B. Giannakis, H. Kobayashi, A.F. Molisch, H.V. Poor, and Z. Sahinoglu, "Localization via ultra-wideband radios: a look at positioning aspects for future sensor networks," *IEEE Signal Processing Magazine*, vol.22, no.4, pp. 70- 84, July 2005

[6] Y. Shen and M.Z. Win,"Fundamental limits of wideband localization Part I: A general framework," *IEEE Trans. Information Theory*, vol.56, no.10, pp.4956-4980, Oct. 2010

[7] Y. Shen, H. Wymeersch and M.Z. Win, "Fundamental limits of wideband localization Part II: Cooperative networks," *IEEE Trans. Information Theory*, vol.56, no.10, pp.4981-5000, Oct. 2010

[8] H. Buhrman, N. Chandran, V. Goyal, R. Ostrovsky and C. Schaffner, "Position-based quantum cryptography: Impossibility and constructions,", 2010

[9] A. Srivinasan and J. Vu, "A survey on secure localization in wireless sensor networks", *Encyclopedia of Wireless and Mobile Communications*, 2007.

[10] R. Poovendran, C. Wang, S. Roy, "Secure localization and time synchronization for wireless sensor and ad-hoc networks", Springer Verlag, 2007

[11] N. Chandran, V. Goyal, R. Moriarty and R. Ostrovsky, "Position based cryptography," *Cryptology ePrint Archive*, 2009, http://eprint.iacr.org/2009/

[12] Wilson, R.; Tse, D.; Scholtz, R.A.; , "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE International Conf. Ultra-Wideband, ICUWB 2007*, pp.270-275, 24-26 Sept. 2007

[13] Q. Wang, H. Su, K. Ren and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," *Proc. IEEE INFOCOM 2011*, pp.1422-1430, 10-15 April 2011

[14] M. R. Bloch and J. N. Laneman, "Secrecy from resolvability," *arXiv:1105.5419v1 [cs.IT]*, May 2011

[15] T.M. Cover and J.A. Thomas, "Elements of information theory," Wiley, New-York, 2nd edition, 2006.