On Secret Key Generation through Multipath for Wireless Networks

Dimitrios Katselis and Panos Papadimitratos

Abstract— **The complexity of cryptographic key management and the wireless medium salient features motivated a number of works that generate secret keys. Simply put, two nodes can estimate their wireless channel and derive common information to generate a key that other nodes cannot obtain. A gamut of methods, each drawing this information in a different manner, has been proposed. In this landscape, this paper contributes a few findings. First, we propose a method that renders channel impulse response magnitude samples roughly uniform, thus facilitating their quantization and agreement on the derived secret keys. We provide a characterization of the probability of successful agreement for this method, which could be useful for other related methods. Moreover, we consider the cost of the key agreement and we propose a trade-off to increase the probability of success while increasing local processing. With an appropriate configuration, a significant reduction in protocol rounds, and thus communication overhead, for key agreement can be achieved. Through simulations, we validate our approximation of the probability of success and demonstrate the reduced communication overhead.**

I. INTRODUCTION

Cryptographic protection of communication remains important, especially for wireless and mobile networked systems. Nonetheless, cryptographic key management is far from trivial. A gamut of recent works show how traditional key agreement methods can be complemented or substituted. Nodes (wireless devices) can leverage the wireless channel properties and their physical layer functionality to derive common randomness and thus generate secret keys.

Consider two nodes, A and B, seeking to agree on a shared secret key that a passive adversary, E, usually termed *eavesdropper*, cannot determine. Simply put, the wireless channel is location-, time-, and frequency-dependent and changes randomly. Thus, it is hard for any third party, and thus E, to determine the A, B channel (unless, e.g., practically at the same location as A or B). Moreover, within a short time interval, the channel does not vary, thus allowing both A and B to estimate it (both estimating the same channel, although not doing it simultaneously).

As a result, the channel (with its reciprocity, variability, and uniqueness for the given time, space, and frequency) provides A and B with a source of common randomness thus allowing them to generate shared keys, $K_{A,B}$. In principle, A and B engage in an exchange of predefined symbols, termed a training sequence, at the end of which they obtain each a channel estimate. Typically, at this stage, continuous observations are quantized and converted into bit strings. Accordingly, each node derives a key and communicates with its peer over the same public channel, checking if they both derived the same key; possibly, by correcting some errors. If this two-way exchange fails, the nodes repeat the process. The keys generated for different links, i.e., pairs of nodes, will be distinct with high probability, due to the statistical independence of the channels.

Along these lines, a multitude of schemes has been proposed, each method using different channel elements in different ways for various physical layers. The early [1] proposed transmission of tones across an urban UHF channel and estimation of the phase angles at the other end. Subsequently, a number of works used channel phase estimates [2], [3], [4] to derive keys. Schemes geared towards Ultra Wide Band (UWB) systems also leveraged channel reciprocity [5], [6]. Another line of works relied on the channel amplitude or more restrictive measurements (such as the Received Signal Strength): signal envelope sampling and deep fades [7], [8]; a level-crossing algorithm [9] to trace channel impulse response estimates within an index, and an IEEE 802.11 implementation-based evaluation; a solution geared towards reduced energy consumption in wireless sensor networks (WSNs) and IEEE 802.15.4 compliant radios [10].

Works aiming at practicality and applicability in mainstream systems, such as the IEEE 802.11 and .15.4, are constrained by the type of information the wireless transceivers can provide (at least, with small modifications). As those cannot easily provide estimates of channel phases, the corresponding group of schemes is not readily applicable [9], [11]. On the flip-side, channel phase has the convenient property of being a uniform random variable for usual fading assumptions, thus facilitating its quantization; unlike the magnitude. At the same time, the analytical treatment of methods that leverage the channel magnitude does not provide, to the best of our knowledge, a characterization of the probability that A and B generate the same string of bits, or in fact, key; unlike, for example, such a derivation for phase-based key generation [3].

These two observations motivate our first finding in this paper: we propose an approach to leverage the channel impulse response magnitude taps, while transforming those into approximately uniform samples. We derive an approximation of the probability that A and B succeed in obtaining their $K_{A,B}$. This can assist relevant schemes in need of such an estimate relating to the inherent channel randomness and the sought key size.

Our second finding in this paper follows from a simple observation: a relatively low probability of success implies a significant overhead for the nodes, re-engaging in a new

The authors are with the School of Electrical Engineering, KTH Royal Institute of Technology, SE 100 44 Stockholm, Sweden dimitrik@kth.se, papadim@kth.se

978-1-4799-4796-6/13/$31.00 © 2013 IEEE

channel estimation and key agreement; the exchange we term here, for brevity, a *handshake*. With a channel estimation completed, it is possible that A and B employ more than one methods to extract common randomness. In other words, they can compute multiple keys drawn from a single channel estimate. Then, the handshake can be augmented, allowing the two peers to check if *at least one of these keys* matches at both ends. Intuitively, this increases the probability of successful agreement, thus reducing the rounds of channel estimation and handshake. Of course, it achieves this at the expense of increased cost for the handshake. We outline further this trade-off and show its effectiveness through simulation.

In the rest of the paper, we first introduce the system model (Sec. II), we present our method (Sec. III) with our Proposition 1 providing the successful key agreement probability (Sec. III-A). Then, we discuss how the combination of two or more key generation methods can be beneficial (Sec. III-B). We validate our Proposition 1 approximation and demonstrate the effect of multi-key handshakes through simulations (Sec. IV) before concluding.

Notation: Vectors are denoted by bold letters. Superscript ^{T} stands for transposition. $|\cdot|$ is the complex modulus. For a vector $\boldsymbol{a}$, $[\boldsymbol{a}]_m$ denotes its *m-th* entry. The expectation operator is denoted by $E(\cdot)$. Furthermore, $1_{\mathcal{M}}$ is the indicator function of the set $\mathcal{M}$. Finally, $\mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{C})$ denotes the complex Gaussian vector distribution with mean $\boldsymbol{\mu}$ and covariance $\boldsymbol{C}$. $\mathcal{U}[a, b]$ denotes a uniform distribution on the interval $[a, b]$.

II. System Model

We do not dwell on a reference communication system. Without loss of generality, let the two nodes, A and B, at the end points of the desired link be the kth and lth. We assume a slowly varying $M \times 1$ vector channel with D coherence intervals and $M_c = M/D$ coefficients per such interval, i.e., $\boldsymbol{h}_{kl} = [[\boldsymbol{h}_{kl}]_1, \ldots, [\boldsymbol{h}_{kl}]_1, \ldots, [\boldsymbol{h}_{kl}]_D, \ldots, [\boldsymbol{h}_{kl}]_D]^T$. Depending on the nature of the communication system, the coherence intervals can correspond to time spans, frequency sub-bands or even spatial intervals. Letting $\tilde{\boldsymbol{h}}_{kl} = [[\boldsymbol{h}_{kl}]_1, \ldots, [\boldsymbol{h}_{kl}]_D]^T$, we assume that $\tilde{\boldsymbol{h}}_{kl} \sim \mathcal{CN}(\boldsymbol{0}_{D\times 1}, \boldsymbol{I}_D)$.

The multipath is assumed rich and nodes sufficiently separated in space, so that all channel vectors $\{\tilde{\boldsymbol{h}}_{kl}\}$ are statistically independent yet have D i.i.d. entries. To simplify our analysis, we assume that the channel estimate is $\widehat{\tilde{\boldsymbol{h}}}_{kl} = \tilde{\boldsymbol{h}}_{kl} + \boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{kl}$ with $\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{kl} \sim \mathcal{CN}(\boldsymbol{0}_{D\times 1}, \sigma^2 \boldsymbol{I}_D) = \mathcal{CN}(\boldsymbol{0}_{D\times 1}, \boldsymbol{I}_D/\text{SINR})$. Thus, $\widehat{\tilde{\boldsymbol{h}}}_{kl} \sim \mathcal{CN}(\boldsymbol{0}_{D\times 1}, (1+\sigma^2)\boldsymbol{I}_D)$ and $\left\{[\widehat{\tilde{\boldsymbol{h}}}_{kl}]_m\right\}_{m=1}^{D}$ i.i.d. Rayleigh distributed with parameter $\sqrt{(1+\sigma^2)/2}$ [12]. Here σ^2 is the variance of the combined interference and noise and $\text{SINR} = E\left[|\tilde{\boldsymbol{h}}_{kl}|^2\right] / E\left[|\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{kl}|^2\right] = 1/\sigma^2$ is the *signal-to-interference-and-noise ratio* (SINR) in the estimate of each channel coefficient.

Adversary model: We consider passive eavesdroppers, i.e., adversaries that silently intercept communications over the medium used by A and B without interfering with the channel estimation or the handshake. The adversaries seek to intercept communications, possibly by obtaining the generated $K_{A,B}$ keys, but they do *not* actively perturb the channel estimation or the subsequent handshake. This model is in-line with a significant body of the aforementioned PHY-based key generation works.

Protocol operation: We define here a generic three-step protocol we assume for the rest of the paper.

S1: A and B engage in a channel estimation step, exchanging in both directions an appropriate sequence of training (or probing) symbols. Let these be from a finite alphabet constellation $\mathcal{X}$ and each probing sequence having N symbols. At the end of this step, each node has its own channel estimate.

S2: A and B derive from their channel estimate a key $\hat{K}_{A,B}$ and $\hat{K}_{B,A}$ respectively.

S3: A message exchange:
$A \rightarrow B : A, B, n_1, H(n_1, A, B, \hat{K}_{A,B})$
and
$B \rightarrow A : A, B, n_2, H(n_1, n_2, A, B, \hat{K}_{B,A})$,
where n_1 and n_2 are randomly drawn previously not used numbers, and H is a cryptographic hash function (e.g., [13]). If $\hat{K}_{A,B} = \hat{K}_{B,A}$, both nodes verify their peer derived the same key; they set this as $K_{A,B}$. Otherwise, they re-start at S1.

III. Random Key Generation from Channel Estimate Magnitudes

The channel estimate magnitudes tend to the magnitudes of the true channel coefficients as the SINR increases. However, their Rayleigh distribution has two undesired characteristics: an infinite support and a concentration of different amounts of mass in different subintervals of the same length. The first one is not very important if we focus only on the essential support of the Rayleigh distribution. The second characteristic implies that we may have to carefully design the quantization cells within the aforementioned essential support. This is necessary so that the keys produced at the endpoints of the link coincide with high probability.

We can exploit the good behavior of the channel magnitudes with an increasing SINR, while dropping the two aforementioned characteristics by employing the following method:

Upon obtaining the channel estimates $\left\{[\widehat{\tilde{\boldsymbol{h}}}_{kl}]_m\right\}_{m=1}^{D}$, we generate a set of new random variables $\{[\gamma_{kl}]_m\}_{m=1}^{D}$ as follows:

$$[\gamma_{kl}]_m = F\left(\left|\left[\widehat{\tilde{\boldsymbol{h}}}_{kl}\right]_m\right|\right) \tag{1}$$

where $F(x) = 1 - e^{-x^2/(1+\sigma^2)}, x \in [0, +\infty)$ is the cumulative distribution function (CDF) corresponding to the Rayleigh distribution with parameter $\sqrt{(1+\sigma^2)/2}$. According to the probability integral transform [12], $[\gamma_{kl}]_m \sim \mathcal{U}[0, 1], \forall m$ are of course independent.

Let $f_Q : [0, 1] \rightarrow \{1, 2, \ldots, Q\}$ be the corresponding element-wise quantization mapping. Then for $\beta \in [0, 1]$, we have:

$$f_Q(\beta) = q \quad \text{if} \quad \beta \in \left[\frac{(q-1)}{Q}, \frac{q}{Q}\right), q = 1, 2, \ldots, Q \tag{2}$$

The corresponding vector mapping is defined as $\boldsymbol{f}_Q : [0,1]^D \rightarrow \{1,2,\ldots,Q\}^D$ and for the vector $\boldsymbol{\gamma} = [[\boldsymbol{\gamma}_{kl}]_1, [\boldsymbol{\gamma}_{kl}]_2, \ldots, [\boldsymbol{\gamma}_{kl}]_D]^T$, it gives

$$\boldsymbol{f}_Q(\boldsymbol{\gamma}) = [f_Q([\boldsymbol{\gamma}_{kl}]_1), f_Q([\boldsymbol{\gamma}_{kl}]_2), \ldots, f_Q([\boldsymbol{\gamma}_{kl}]_D)]^T \quad (3)$$

In this sense, we obtain a key with $b_{key} = D\log_2(Q)$ bits of information.

As far as the performance of this random key generation is concerned, Proposition 1 in [3] holds unchanged, i.e., the probability that the keys produced by nodes of different links are different equals to $1 - 1/Q^D$. Note that this probability tends to 1 as Q and/or as D increase. Therefore, the more the coherence subbands the better in terms of having different keys for different links, since this intuitively means that more randomness is introduced in our key generation process.

A. Secret Key for a Specific Link

Let p_{key} denote the probability that A and B generate the same $K_{A,B}$ in one handshake. Let n denote the number of independent handshakes and $p_{succ}(n)$ the probability that there is at least one successful handshake in n trials. Then, for a given p_{key} the number of handshakes needed to achieve a desired (sufficiently high) p_{succ} can be easily seen to be given by

$$n = \frac{\log(1 - p_{succ})}{\log(1 - p_{key})}. \quad (4)$$

If p is the probability that both users across a link generate the same quantization index for a particular channel coefficient, it also holds that $p_{key} = p^D$ if we assume that SINR is uniform across all channel coefficients[1]. We need to estimate p_{key} or, equivalently, p. The two channel estimates at the end points of a link are:

$$\widehat{\tilde{\boldsymbol{h}}}_{kl} = \tilde{\boldsymbol{h}}_{kl} + \boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{kl}, \quad \widehat{\tilde{\boldsymbol{h}}}_{lk} = \tilde{\boldsymbol{h}}_{kl} + \boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{lk}, \quad (5)$$

based on the reciprocity principle. Consider a specific channel coefficient of a single channel estimate $\left[\widehat{\tilde{\boldsymbol{h}}}\right]_m = \left[\tilde{\boldsymbol{h}}\right]_m + \left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}\right]_m$, where the specific link double subscript has been dropped. The magnitude $\left|\left[\widehat{\tilde{\boldsymbol{h}}}\right]_m\right|$ is:

$$\sqrt{\left|\left[\tilde{\boldsymbol{h}}\right]_m\right|^2 + \left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}\right]_m\right|^2 + 2\left|\left[\tilde{\boldsymbol{h}}\right]_m\right|\left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}\right]_m\right|\cos(\phi_m)}. \quad (6)$$

$\phi_m \sim \mathcal{U}[0, 2\pi)$ is the phase of $\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}\right]_m$ relative to $\left[\tilde{\boldsymbol{h}}\right]_m$.

p depends on the SINR at each end of the A, B link and on Q. In the rest of the discussion, we assume that the SINR is the same at both ends of the link.[2] Moreover, $\left|\left[\widehat{\tilde{\boldsymbol{h}}}\right]_m\right|^2$ is quantized to the nth index, when the corresponding $[\boldsymbol{\gamma}]_m$ falls in the nth quantization cell. Performing the computations, the corresponding condition turns out to be

$$a_n \leq \left|\left[\widehat{\tilde{\boldsymbol{h}}}\right]_m\right| \leq b_n \quad (7)$$

where $a_n = \sqrt{(1+\sigma^2)\ln(Q/(Q+1-n))}$ and $b_n = \sqrt{(1+\sigma^2)\ln(Q/(Q-n))}$.

Let $\mathcal{A}_m$ denote the set that the quantized $[\boldsymbol{\gamma}]$'s for the two reciprocal channels coincide. We also let $X_m^{kl} = \left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{kl}\right]_m\right| / \left|\left[\tilde{\boldsymbol{h}}_{kl}\right]_m\right|$ and $X_m^{lk} = \left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{lk}\right]_m\right| / \left|\left[\tilde{\boldsymbol{h}}_{lk}\right]_m\right|$ be the instantaneous inverse SINRs, while $\delta_m > 0$. Then:

$$p\,(\mathrm{SINR}, Q) = E[1_{\mathcal{A}_m}] = E\left[E[1_{\mathcal{A}_m}|X_m^{kl}, X_m^{lk}]\right] = \geq E[1_{\mathcal{A}_m}|X_m^{kl} \leq \delta_m, X_m^{lk} \leq \delta_m]P\{X_m^{kl} \leq \delta_m, X_m^{lk} \leq \delta_m\} \quad (8)$$

The lower bound can be made arbitrarily small since any of the complementary cases, e.g., $E[1_{\mathcal{A}_m}|X_m^{kl} \leq \delta_m, X_m^{lk} > \delta_m]P\{X_m^{kl} \leq \delta_m, X_m^{lk} > \delta_m\}$ etc, can be easily seen to be less than or equal to $P\{X_m > \delta_m\}$, where $X_m = X_m^{kl}$ or $X_m = X_m^{lk}$ accordingly.

$$P\{X_m > \delta_m\} = \frac{1}{\delta_m^2 \mathrm{SINR} + 1}, \quad (9)$$

which can be made arbitrarily small by making $\delta_m^2 \mathrm{SINR}$ sufficiently large. Here, we used the CDF of X_m in [3]

$$F_{X_m}(x) = Pr\{X_m \leq x\} = \frac{x^2}{x^2 + \sigma^2}. \quad (10)$$

We can choose the corresponding largest threshold in our case, i.e., the largest value of X_m that does not result in an error when the true channel magnitude falls in the middle of the n-th cell after being processed by F. Denoting by N_n, M_n the numbers $\ln(Q/(Q-n))/\ln(2Q/(2Q-2n+1))$ and $\ln(Q/(Q-n+1))/\ln(2Q/(2Q-2n+1))$, respectively, and by using (6), the maximum threshold $d_{\max}^n$ is given as the minimum of the root of the equation $\left(1 + X_m^2 + 2X_m\cos(\phi_m)\right) = N_n$ for $\cos(\phi_m) = 1$ and the root of the equation $\left(1 + X_m^2 + 2X_m\cos(\phi_m)\right) = M_n$ for $\cos(\phi_m) = -1$. Furthermore, this threshold can be made independent of n by simply choosing the final threshold equal to[3] $d_{\max} = \min_{n=1,2,\ldots,Q-1} d_{\max}^n$.

Combining the above results, we can now give a proposition for the approximation of p, notably when the SINR is sufficiently high:

Proposition 1: For sufficiently high SINR, the probability that the same quantization index is generated for a particular channel coefficient at both ends of a link can be approximated as

$$p \approx \frac{1}{Q}\sum_{n=1}^{Q}\frac{1}{2}\left[\mathrm{erf}\left(\frac{b_n'}{\sigma}\right) - \mathrm{erf}\left(\frac{a_n'}{\sigma}\right)\right]\frac{d_{\max}^2}{d_{\max}^2 + \sigma^2} \quad (11)$$

where $\mathrm{erf}(x)$ is the Gauss error function, $a_n' = (a_n^2 - m_n^2)/(a_n + b_n)$, $b_n' = (b_n^2 - m_n^2)/(a_n + b_n)$ and $m_n = (a_n + b_n)/2$.

[1]Note that the more the coherence subbands the worse the p_{key}. This is a clear tradeoff with the probability that the keys for different links should mismatch with the highest possible probability.

[2]Recall this is the SINR in the estimate of channel coefficients, defined in Sec. II.

[3]Remember that the term "maximum" threshold refers to the maximum possible X_m that does not result in an error. This is achieved by the min of $d_{\max}^n$'s. In the same sense, $d_{\max}^n$ is the minimum of two roots.

***Proof*:**

By definition, $\mathcal{A}_m = \{f_Q([\boldsymbol{\gamma}_{kl}]_m) = f_Q([\boldsymbol{\gamma}_{lk}]_m)\}$. Using (8), $p \geq E[1_{\mathcal{A}_m}|X_m^{kl} \leq d_{\max}, X_m^{lk} \leq d_{\max}]P\{X_m^{kl} \leq d_{\max}|X_m^{lk} \leq d_{\max}\}P\{X_m^{lk} \leq d_{\max}\}$. Additionally, $X_m << 1$ when the SINR is high with very high probability [3]. Therefore, based on the definition of the conditional probability, $P\{X_m^{kl} \leq d_{\max}|X_m^{lk} \leq d_{\max}\} \approx 1$ at high SINR.

We now focus on $E[1_{\mathcal{A}_m}|X_m^{kl} \leq d_{\max}, X_m^{lk} \leq d_{\max}] = P\{f_Q([\boldsymbol{\gamma}_{kl}]_m) = f_Q([\boldsymbol{\gamma}_{lk}]_m)|X_m^{kl} \leq d_{\max}, X_m^{lk} \leq d_{\max}\}$. Based on elementary properties of probability we have:

$$P\{f_Q([\boldsymbol{\gamma}_{kl}]_m) = f_Q([\boldsymbol{\gamma}_{lk}]_m)|X_m^{kl} \leq d_{\max}, X_m^{lk} \leq d_{\max}\} = \sum_{n=1}^{Q} P\{f_Q([\boldsymbol{\gamma}_{kl}]_m) = n|f_Q([\boldsymbol{\gamma}_{lk}]_m) = n, X_m^{kl} \leq d_{\max}, X_m^{lk} \leq d_{\max}\}P\{f_Q([\boldsymbol{\gamma}_{lk}]_m) = n\} \quad (12)$$

Clearly, $P\{f_Q([\boldsymbol{\gamma}_{lk}]_m) = n\} = 1/Q$. Furthermore, the events $\{f_Q([\boldsymbol{\gamma}_{kl}]_m) = n\}$ and $\{f_Q([\boldsymbol{\gamma}_{lk}]_m) = n\}$ are equivalent to $\left\{a_n \leq \left|\left[\widehat{\tilde{\boldsymbol{h}}}_{kl}\right]_m\right| \leq b_n\right\}$ and $\left\{a_n \leq \left|\left[\widehat{\tilde{\boldsymbol{h}}}_{lk}\right]_m\right| \leq b_n\right\}$, respectively. Additionally, $\left|\left[\widehat{\tilde{\boldsymbol{h}}}_{lk}\right]_m\right|$ belongs to $\left[\left|\left[\tilde{\boldsymbol{h}}\right]_m\right| - \left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{lk}\right]_m\right|, \left|\left[\tilde{\boldsymbol{h}}\right]_m\right| + \left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{lk}\right]_m\right|\right]$. Combining the above results, the event $\left\{a_n \leq \left|\left[\widehat{\tilde{\boldsymbol{h}}}_{lk}\right]_m\right| \leq b_n\right\}$ implies that $\left|\left[\tilde{\boldsymbol{h}}_{kl}\right]_m\right| = m_n = (a_n + b_n)/2$. Therefore:

$$P\{f_Q([\boldsymbol{\gamma}_{kl}]_m) = n|f_Q([\boldsymbol{\gamma}_{lk}]_m) = n, X_m^{kl} \leq d_{\max}, X_m^{lk} \leq d_{\max}\} = P\left\{a_n^2 \leq \left|\left[\widehat{\tilde{\boldsymbol{h}}}_{kl}\right]_m^2\right| \leq b_n^2 | \left|\left[\tilde{\boldsymbol{h}}_{kl}\right]_m\right| = (a_n + b_n)/2, X_m^{kl} \leq d_{\max}, X_m^{lk} \leq d_{\max}\right\} = P\left\{a_n^2 - m_n^2 \leq \left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{kl}\right]_m^2\right| + 2m_n\left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{kl}\right]_m\right|\cos(\phi_m^{kl}) \leq b_n - m_n^2 \,|\, X_m^{kl} \leq d_{\max}, X_m^{lk} \leq d_{\max}\right\} \approx P\left\{(a_n^2 - m_n^2)/(2m_n) \leq \left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{kl}\right]_m\right|\cos(\phi_m^{kl}) \leq (b_n - m_n^2)/(2m_n) \,|\, X_m^{kl} \leq d_{\max}, X_m^{lk} \leq d_{\max}\right\} \quad (13)$$

where in the last part we have used the fact that $\left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{kl}\right]_m\right|^2 \ll \left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{kl}\right]_m\right|$ at high SINR with very high probability. Here, ϕ_m^{kl} is the corresponding ϕ_m for the kl-th link. According to our assumptions, $\left|\left[\boldsymbol{\Delta}\tilde{\boldsymbol{h}}_{kl}\right]_m\right|\cos(\phi_m^{kl})$ is Guassian distributed with zero mean and variance $\sigma^2/2$ having a CDF equal to $0.5[1 + \text{erf}(x/\sigma)]$ [12].

Combining all the above results and using (10), the approximation (11) follows. ■

Remark 1: This approximation is not a guaranteed lower bound of p but simply a high SINR approximation, due to our intermediate approximations in the course of this derivation.

Remark 2: Instead of generating a key based on the modulus, we may generate keys based on the real or imaginary parts of the channel estimates by using $F(x) = 0.5[1 + \text{erf}(x/\sqrt{1+\sigma^2})]$, which is the corresponding CDF for the real and the imaginary parts of the channel estimates.

B. Reducing the Number of Handshakes

To reduce the number of protocol rounds, we augment the generic protocol in Sec. II as follows:

S1: Identical as before.

S2: A derives $\hat{K}_{A,B}^1$ and $\hat{K}_{A,B}^2$ and B derives $\hat{K}_{B,A}^2$ and $\hat{K}_{B,A}^2$; that is, each node derives two keys.

S3: A message exchange:
$A \rightarrow B$:
$A, B, n_1, H(n_1, A, B, \hat{K}_{A,B}^1), H(n_1, A, B, \hat{K}_{A,B}^2)$
and
$B \rightarrow A$:
$A, B, n_2, H(n_1, n_2, A, B, \hat{K}_{B,A}^1)$,
$H(n_1, n_2, A, B, \hat{K}_{B,A}^2)$.
If $\hat{K}_{A,B}^1 = \hat{K}_{B,A}^1$, or if $\hat{K}_{A,B}^2 = \hat{K}_{B,A}^2$, the two nodes set this as $K_{A,B}$.[4] Otherwise, they re-start at (S1).

In other words, additional processing is needed at each node for (S2), as each node generates an additional key. Moreover, each handshake message increases in size as two keys need to be confirmed. If at least one of the generated keys matches, A and B proceed accordingly with the derived common key; if both keys match, then the nodes may use either or both.[5] If no matching key was derived, the channel estimation, key derivation, and confirmation check steps are repeated.[6] One can easily generalize this to three or more keys.

Let the cost of the channel estimation, notably including the training, be denoted by C_T; the cost of a one-key derivation handshake step (S3) by C_H^1 and the cost of a two-key derivation handshake step (S3) by C_H^2. Moreover, let the probability of success for the first of the two combined methods to be p_1 and that for the second be p_2; assume the former method be the one used in the basic protocol. The enhanced protocol concludes successfully if *at least one* of the two methods results in a matching key.

The basic protocol succeeds with probability p_1 while the augmented one with probability $1 - (1 - p_1)(1 - p_2)$. Independently of whether p_2 is lower or higher than p_1, the augmented protocol success is more likely. Accordingly, the average number of rounds (handshakes) for each one would be $1/p_1$ and $1/(1 - (1 - p_1)(1 - p_2))$, assuming the numbers are geometrically distributed random variables $G(p_1)$ and $G(1 - (1 - p_1)(1 - p_2))$ respectively.

The advantage of the augmented over the basic protocol depends on the relative size of C_T compared to C_H^1 and C_H^2. Assume here, without loss of generality, that all fields in the handshake messages have the same size, c (e.g., 128 bits long each). Then, $C_H^2 = 1.25C_H^1$. The expected cost for having at least a key with the basic protocol would be $(1/p_1) \times (C_T + C_H^1)$ while the expected cost for the augmented protocol would be $(1/(1 - (1 - p_1)(1 - p_2))) \times (C_T + C_H^2)$. Clearly, the use

[4] If both keys match, the nodes can use both.

[5] The two keys can be correlated; we do not dwell here on how to use each of the matching keys, rather we assume each of the two combined methods can produce a good (i.e., random) key with the sought length.

[6] It possible to engage in a different type of handshake that allows A and B to identify disagreements and take corrective actions - we did not consider throughout this work this element.

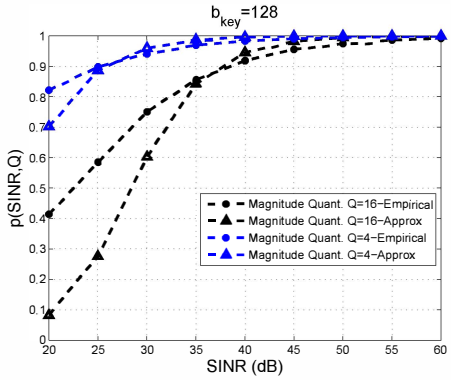

Fig. 1. Analytical vs. empirical values of $p(\text{SINR}, Q)$.

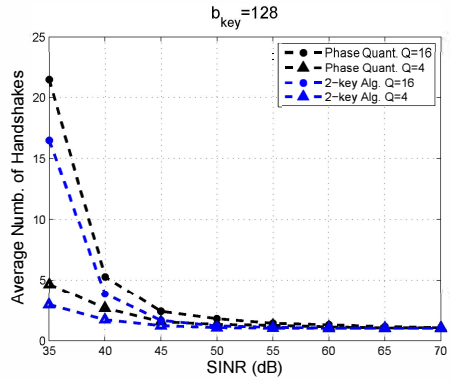

Fig. 2. Average number of handshakes for the 1-key phase quantization method in [3] and the proposed 2-key method.

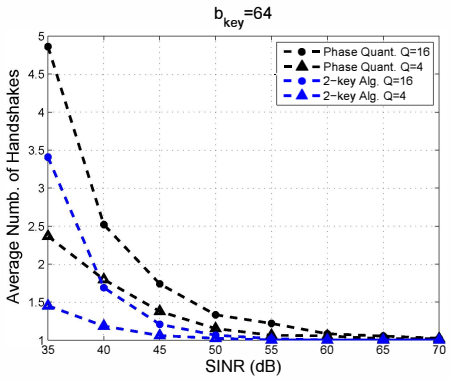

Fig. 3. Average number of handshakes for the 1-key phase quantization method in [3] and a 2-key method using the phase quantization method in [3] and the channel impulse response quantization method in [14].

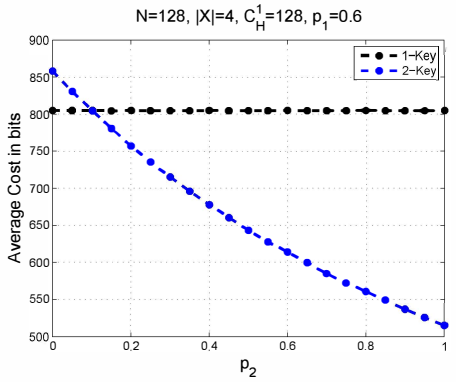

Fig. 4. Average Cost in bits for a 1-key and a 2-key method for a given p_1 versus p_2: $N = 128, |\mathcal{X}| = 4, C_H^1 = 128, p_1 = 0.6$.

of the 2-key is justified in terms of communication cost when

$$\frac{1}{p_1}(C_T + C_H^1) > \frac{1}{1-(1-p_1)(1-p_2)}(C_T + C_H^2),$$

which holds for the aforementioned protocol for a given p_1 when

$$p_2 > \frac{0.25 p_1 C_H^1}{(1-p_1)(C_T + C_H^1)}.$$

Assuming p_1 and p_2 are *a priori* known and $p_1 > p_2$, the better key generation method is used by the basic protocol. To reduce overhead further, It can be used first by the augmented protocol, with the second part of its S3 step sequentially only if needed (when the first part of the handshake fails). One can generalize this ordering for more than two keys.

IV. Evaluation

We validate here the derived approximation (Proposition 1) through simulations, we show the potential improvement from the use of two methods, and illustrate the communication cost trade-off.

p_1	0.1	0.8	0.9	0.91	0.92	0.94
$p_2 >=$	0.0074	0.2651	0.5964	0.67	0.7621	1.0382

TABLE I

$N = 128, \mathcal{X} = 4, C_H^1 = 128, C_H^2 = 1.25 C_H^1$: Threshold values for p_2 above which a 2-key method is better than the corresponding 1-key method in terms of cost.

Fig. 1 gives the approximation of the true p by Eq. (11) versus the SINR. Q is assumed fixed to either 4 or 16, while $b_{key} = 128$. Clearly, the approximation becomes tight as the SINR increases. Fig. 1 also demonstrates that the notion of the "high SINR" regime relates to the value of Q. For smaller Q values, the value of p is larger for smaller SINR values, as intuitively expected. The curves 'Approx.' correspond to (11), while the curves 'Empirical' correspond to a computation of the corresponding probabilities through Monte Carlo simulations.

The combination of two methods into a 2-key method (Sec. III-B) can be beneficial, compared to a 1-key method independently of the involved methods. To illustrate this, we provide two simulation-based outcomes: (i) we combine the CIR magnitude based method in this paper with the CIR phase method in [3], with the results in Fig. 2; and (ii) we combine [3] with [14] into a 2-key method, with the results in Fig. 3. In both cases, we see that the augmented protocol reduces the number of protocol rounds (handshakes), for the same values of Q and b_{key}. The relation of the "high SINR" regime with Q is also illustrated here, with the same intuition as for Fig. 1.

Figs. 4 and 5 illustrate the average communication cost analysis (Sec. III-B) for a generic 1-key and a generic 2-

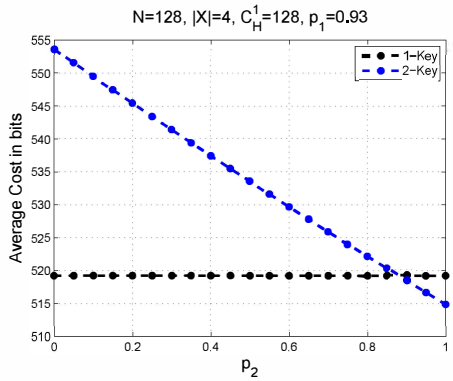

Fig. 5. Average Cost in bits for a 1-key and a 2-key method for a given p_1 versus p_2: $N = 128, |\mathcal{X}| = 4, C_H^1 = 128, p_1 = 0.93$.

key method. The first key of the 2-key method is assumed to coincide with the key of the 1-key method. The number of training symbols is $N = 128$ and the constellation cardinality is $\mathcal{X} = 4$. These are typical values, e.g., in orthogonal frequency division multiplexing (OFDM) systems with N subcarriers and quadrature phase shift keying (QPSK) symbols [15]. We follow the example described in Sec. III-B, where $C_H^1 = 128$ bits and $C_H^2 = 1.25C_H^1$ bits. Fig. 4 shows that for $p_1 = 0.6$, any 2-key method with p_2 roughly larger than 0.1 leads to lower average communication cost than the corresponding 1-key method, while delivering a common key with less average number of handshakes. For $p_1 = 0.93$, the corresponding threshold for p_2 is approximately equal to 0.89 as it appears in Fig. 5. To fully appreciate the rate at which the threshold for p_2 approaches 1, we provide Table I. For $p_1 \geq 0.94$ in this setup, no 2-key method can deliver a lower communication cost, but only a lower number of handshakes.

V. Discussion and Conclusions

It is usually assumed in the literature that as long as an eavesdropper E is not within a distance at the order of magnitude of the used radio wavelength, then it is impossible to derive the A, B channel estimate. As a result, it is assumed that the derived $K_{A,B}$ cannot be guessed by E. In this paper, we do not consider this aspect, we rather make the same assumption. Nonetheless, one has to be cautious, especially when dealing with the channel impulse response magnitude. An eavesdropper could also estimate the B, E and A, E channels, know the details A, B communication, and take advantage of fading correlations towards "guessing" the A, B channel and the resultant derived key. Different approaches are proposed to mitigate predicability and there is empirical evidence of significant variability, e.g., even across small displacements; yet, a rigorous treatment of how strong the produced keys are, overall, across all related schemes, would be welcome.

Looking at the communication overhead for the single and multiple key methods, we did not consider variations of the key lengths each one produces and adjust, for example, the probability of success. Moreover, we assumed that the two keys are independent and did not investigate what the overall key bit rate would be. Further exploration in these directions would be interesting. In addition, we could abstract away the generic protocol for the key check/confirmation, consider the amount of information A and B should exchange of their (public) channel.

In conclusion, this paper provided an analytic approximation of the probability of successful key agreement based on channel impulse response magnitude. It also outlined how to reduce communication overhead by extracting more than one keys out of the channel estimate, essentially succeeding in agreeing on a key if at least of one of the two (or more keys) match.

References

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

[2] H. Koorapaty, A. Hassan, and S. Chennakeshu, "Secure information transmission for mobile radio," *IEEE Comm. Letters*, vol. 4, no. 2, pp. 52–55, Feb. 2000.

[3] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *IEEE ICASSP*, Las Vegas, NV, USA, Mar. 2008.

[4] 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*, Shanghai, China, Apr. 2011.

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

[6] A. Kitaura, T. Sumi, K. Tachibana, H. Iwai, and H. Sasaoka, "A scheme of private key agreement based on delay profiles in uwb systems," in *IEEE Sarnoff Symposium*, Princeton, NJ, USA, Mar. 2006.

[7] M. Tope and J. McEachen, "Unconditionally secure communications over fading channels," in *IEEE MILCOM*, McLean, Virginia, USA, Oct. 2001.

[8] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *ACM Conference on Computer and Communications Security*, Alexandria, Virginia, USA, Oct.-Nov. 2007.

[9] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proceedings of the 14th ACM International Conference on Mobile Computing and Networking*, San Francisco, California, USA, Sept. 2008.

[10] J. Croft, N. Patwari, and S. Kasera, "Robust uncorrelated bit extraction methodologies for wireless sensors," in *ACM IPSN*, Stockholm, Sweden, Apr. 2010.

[11] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-rate uncorrelated bit extraction for shared secret key generation from channel measurements," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 17–30, 2010.

[12] H. Stark and J. W. Woods, *Probability and Random Processes with Applications to Signal Processing*. Prentice Hall.

[13] H. Krawczyk, M. Bellare, and R. Canetti, "Hmac: Keyed-hashing for message authentication, ietf rfc 2104," February 1997.

[14] J. Zhang, S. Kasera, and N. Patwari, "Mobility assisted secret key generation using wireless link signatures," in *IEEE INFOCOM*, San Diego, CA, March 2010.

[15] D. Katselis, "Some preamble design aspects in cp-ofdm systems," *IEEE Communications Letters*, vol. 16, no. 3, pp. 356–359, Mar. 2012.