# Cross-layer Wireless Information Security

Lixing Song, Shaoen Wu
Department of Computer Science
Ball State University
Email: {lsong, swu}@bsu.edu

***Abstract*—Wireless information security generates shared secret keys from reciprocal channel dynamics. Current solutions are mostly based on temporal per-frame channel measurements of signal strength and suffer from low key generate rate (KGR), large budget in channel probing, and poor secrecy if a channel does not temporally vary significantly. This paper designs a cross-layer solution that measures noise-free per-symbol channel dynamics across both time and frequency domain and derives keys from the highly fine-grained per-symbol reciprocal channel measurements. This solution consists of merits that: (1) the per-symbol granularity improves the volume of available uncorrelated channel measurements by orders of magnitude over per-frame granularity in conventional solutions and so does KGR; 2) the solution exploits subtle channel fluctuations in frequency domain that does not force users to move to incur enough temporal variations as conventional solutions require; and (3) it measures noise-free channel response that suppresses key bit disagreement between trusted users. As a result, in every aspect, the proposed solution improves the security performance by orders of magnitude over conventional solutions. The performance has been evaluated on both a GNU SDR testbed in practice and a local GNU Radio simulator. The cross-layer solution can generate a KGR of 24.07 bits per probing frame on testbed or 19 bits in simulation, although conventional optimal solutions only has a KGR of at most one or two bit per probing frame. It also has a low key bit disagreement ratio while maintaining a high entropy rate. The derived keys show strong independence with correlation coefficients mostly less than 0.05. Furthermore, it is empirically shown that any slight physical change, e.g. a small rotation of antenna, results in fundamentally different cross-layer frequency measurements, which implies the strong secrecy and high efficiency of the proposed solution.***

## I. Introduction

The information security in wireless mobile communication remains challenging. It confronts two main constraints: battery and mobility. The limited battery is weak in supporting conventional energy-hungry security architectures and algorithms. Meanwhile, mobility-incurred peer-to-peer wireless communications such as Wi-Fi Direct [1] and Mobile Ad-hoc Networking (MANET) lack of the key management infrastructure such as Public Key Infrastructure (PKI) required by conventional security. Wireless information security tackles these challenges by exploiting the uniqueness of wireless channel [2].

The classic system model of wireless information security is shown in Fig. 1 where Bob and Alice are trusted users with Eve being the malicious one. Channel reciprocity (a.k.a mutuality) refers to the fact that in wireless communication the wireless channel between Bob and Alice is symmetric to each other. As a result, both of them should ideally see the same channel response $h(t)$ independently at both sides.

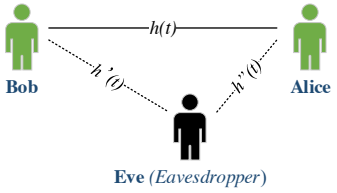


**Fig. 1: Classic Security Model**

Furthermore, because of uncorrelated stochastic variation over time, frequency and space, their channel reciprocity is unique and only known to themselves, not, at most partially, available to a third-party like Eve, because Eve has different channel response $h'(t)$ to Bob and $h''(t)$ to Alice from $h(t)$ unless her antenna to Bob's or Alice's is within half of carrier wavelength according to wireless information-theoretic security [3], [4]. Because a carrier wavelength in practice is too small (e.g. 0.125 $m$ in 2.4 GHz WLAN), it would never happen that Eve can directly detect the channel reciprocity between Bob and Alice. Thanks to these salient features of channel reciprocity, wireless information security enables Bob and Alice *independently* to generate shared secret keys out of their channel reciprocity for the cryptography of their communications.

Wireless information security solutions critically differ in extracting channel response. Bob and Alice use Time-Division Duplex (TDD) to exchange probing frames on their channel and then measure the received frames to formulate the channel response independently at both sides. The scheme obtaining channel response of a wireless information security system determines its performance in generating shared secret keys. The most popular metric currently used in wireless information security to reveal channel response is wireless signal strength including received signal strength indicator (RSSI) or signal-to-noise ratio (SNR) [5], [6]. A received signal can be formulated by:

$$r(t) = h(t)s(t) + n(t) \quad (1)$$

where $h(t)$ is channel response, $s(t)$ is the signal transmitted and $n(t)$ refers to noise. A frame is normally measured of its RSSI or SNR from the frame header at the physical layer upon the received signal $r(t)$ by a receiver. Signal strength based solutions confront three critical problems in wireless information security. **First**, because each frame can only result in one signal strength measurement, it takes long time for these solutions to generate hundreds of bits (commonly 128 to 512 bits) for a shared secret key. Currently secret key generation rate (KGR) based on signal strength is normally at the order of bit per probing. As a result, *(1) the channel resource overhead of key generation is too large to be acceptable because most of the link budget is spent on probing frames, (2) the battery overhead incurred by many rounds of probing transmission is disastrous, and (3) attackers are given plenty time in cracking a key.* **Second**, signal strength based measurements are not precise in revealing channel response because received signal

978-1-4799-3572-7/14/$31.00 ©2014 IEEE

$r(t)$ is polluted by noise $n(t)$. So, even though Bob and Alice transmits the same probing signal $s(t)$, the noise is very likely different along two directions. This exacerbates disagreement of key bits at both sides. An ideal solution would reveal the channel response without noise. **Third**, since the signal strength is measured upon a frame header, the remaining portion of the frame purely constitutes overhead to the measurement, which wastes precious wireless channel resources as well as the power in transmission and receiving.

In this paper, we design a cross-layer solution to wireless information security that has three merits: (i) channel response is measured upon the stochastic channel dynamics *at the granularity of symbol* for high KGR, (ii) channel measurements are *noise-free* to reveal the true channel response for high key agreement rate (KAR), and (iii) probing frames carry useful data, not garbage bits, that expedite the data collection to generate key bits. The main contributions of the work can be summarized as follows:

- We propose a cross-layer symbol-level channel measurement scheme that collects uncorrelated channel data over both frequency and time by taking advantage of frequency selective fading and fast fading. With this channel measurement at the finest granularity, the data collection, thus KGR, is improved by orders of magnitude over conventional wireless information security based on signal strength.
- We devise a novel channel probing that consists of a delicately designed training symbol sequence and an algorithm that can eliminate channel noise from channel measurements by working on the special symbol sequence. With this probing, we can obtain reliable noise-free channel measurements that solely relate to channel response. This improves KAR as well as the channel utilization because the probing frames are fully utilized.
- A key generation algorithm is proposed to quickly derive key bits out of the channel measurements.
- A universal evaluation metric is designed to comprehensively evaluate the secrecy performance of any wireless information security solution generating keys from channel response.

We have conducted extensive evaluation of the proposed cross-layer wireless information security solution on a local simulator as well as a GNU SDR testbed in real environment. The results show that (1) our solution can generate keys at a KGR of 24.07 bits per probing in testbed experiments; (2) derived shared secret keys demonstrate strong randomness and high independence across various channel scenarios; (3) the symbol-level channel measurements present no significant correlation with signal strength or *Doppler* shift, but sensitively response to channel multi-path variations, which implies reliable indication of channel response and thus improves key agreement.

The rest of paper is organized as follows. We start with a review of related works in Section II with a focus on their problems. Then, Section III presents the design of the cross-layer symbol-level channel measurement and the channel probing. Next, the key generation algorithm is discussed in Section IV. Comprehensive performance evaluation is presented in Section V and the paper is concluded by Section VI.

## II. Related Works

Inspired by theoretical analysis about *quantum cryptography* [7], the secret key extraction has been theoretically [2], [8] and experimentally [5], [6], [9]–[11] explored by wireless information security for years. Most popularly, signal strength based channel measurement is commonly used to collect data representing reciprocal channel dynamics from time-varying channel deep fading. Constrained by the limitation on granularity and accuracy of channel measurement, the literature wireless information security solutions are summarized as below:

1. **Low KGR:** Adopting signal strength as the channel measurement metric, Patwari *et al.* proposes an optimization method, called high-rate uncorrelated bit extraction (HRUBE), to address non-simultaneous directional measurement issues. It boosts the KGR from 1.2 *bits/sec.* in [5] up to 22 *bits/sec.* (note: it is per second, not per probing frame). Wei *et al.* designs an adaptive scheme based on Proportional-Integral-Derivative (PID) to make efficient probing, which gains a KGR of 72.34 *bits/sec.* at 100 $Hz$ probing rate.
2. **Mobility-dependent:** By evaluating the effectiveness of secret key extraction from RSSI, the work of [6] reveals that i) the quality of generated bits relies on the temporal variation of the channel, and ii) the mobility of nodes incurs temporal channel variations. It implies that the keys derived by signal strength based solutions have poor secrecy performance in static scenarios. For example, without mobility, the KGR of 72.34 *bits/sec.* in [9] drops to 58.9 *bits/sec.*.

Exploiting the channel potentials in frequency-domain, especially with orthogonal frequency-division multiplexing (OFDM), recent works attempt to find new channel measurement schemes to improve the performance in generating keys. [12] collects the RSSI of OFDM subcarriers and adopts the sampled channel coefficients as the source data to derive key bits. [13], [14] use phase change in multi-path wireless channels to generate secret keys. The most recent work [15] explores multiple-input and multiple-output (MIMO) technique with OFDM to provide more abundant channel measurement (e.g. Channel State Information). However, all those solutions are essentially still power-based strategies whose measurement accuracy is polluted by channel noise that hurts their key bit agreement.

## III. Cross-layer Channel Measurement and Probing

To exhaustively exploit wireless channel dynamics for fast key generation at high KGR, we have investigated the channel characteristics across both frequency and time at the smallest scale: per-symbol. Based on the investigation, we have designed a cross-layer symbols-level channel measurement to extract the channel dynamics reflecting channel response at the finest granularity. Then, a channel probing scheme has been developed to obtain noise-free channel data for key generation.

### A. Channel Characteristics Investigation

Conventional signal strength based wireless information security obtains channel data at the granularity of frame in that each frame can provide at most one uncorrelated channel measurement. However, a frame in transmission actually consists of hundreds, even thousands of signal symbols that are the smallest transmission units over wireless channel. Clearly, a frame-level channel measurement has smoothed out the small scale channel characteristics across the frame. If channel measurement can be taken at symbol level, it can reasonably improve the amount of available channel data by orders of magnitude with the same number of probing frames. We are so inspired to investigate the channel characteristics at nano scale across frequency and time.

We have conducted a transmission on a GNU SDR testbed consisting of two USRP2 N210 nodes. These two nodes are statically placed on the same level. The 800-bytes frames are delivered continuously from sender to receiver. In our SDR testbed configuration, each symbol takes $48\mu s$ to transmit. From the experiments, we have collected the Fast Fourier transform (FFT) power at the receiver and a snapshot is shown in Fig. 2. It is of utmost importance to observe that (1) the channel does have significant variations across frequency, which implies these variations can be exploited for channel measurement in generating keys, and (2) the channel shows similar trends in frequency domain at different moments, which implies that the channel response obtained across frequency domain is reliable to generate keys independently at the two communicators that have to use TDD to exchange probing frames, (3), even so, the channel also show some variations across time e.g. frequency drift (highlighted in the left rectangle in Fig. 2) and power attenuation (highlighted in the right rectangle), which implies that, with frequency domain measurements, the channel measurements across time also contain dynamics that can be exploited as the key source to generate fast key.

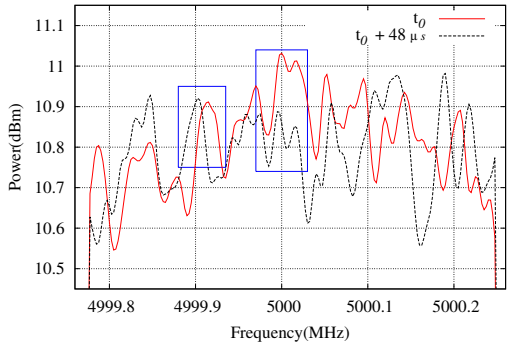


**Fig. 2: FFT powers at receiver. The left rectangle indicates a frequency drift across time. The right rectangle shows a power attenuation across time.**

### B. Design Principle of Noise-free Channel Measurement

Wireless channel always has random noise from thermal background or interference. Noise hurts the accuracy of channel measurement because it may change from one frame to another. We have designed a noise-free channel measurements that are purely determined by channel response and thus can promote the agreement of the keys independently derived at two trusted users from their mutual channel measurements. The following present the principle of our solution in obtaining noise-free channel measurements.

Denote $h(t)$ the channel response at the time $t$. A received copy of a source symbol $s_t$ through the channel with additive noise $n(t)$ is:

$$r_t = h(t) \cdot s_t + n(t) \tag{2}$$

Inspired by OFDM synchronization [16], we design a source symbol vector that consists of four back-to-back symbols in a special pattern: $(s, 0, \overline{s}, 0)$, where $\overline{s}$ is the conjugate of symbol $s$ and 0 is a silent symbol. Because the delivery time of a symbol is so small (only $\sim$83 $n$s in IEEE 802.11n) that it is reasonable to assume that both the channel $h(\cdot)$ and the noise $n(\cdot)$ are invariant across the transmission of these four symbols. Then, we can have four received symbols represented as:

$$\begin{aligned} r_0 &= h(\cdot) \cdot s + n(\cdot) \\ r_1 &= h(\cdot) \cdot 0 + n(\cdot) \\ r_2 &= h(\cdot) \cdot \overline{s} + n(\cdot) \\ r_3 &= h(\cdot) \cdot 0 + n(\cdot) \end{aligned}$$

With above equations, we can have the following derivations with the noise eliminated:

$$\begin{aligned} r_0 - r_1 &= h(\cdot) \cdot s \\ r_2 - r_3 &= h(\cdot) \cdot \overline{s} \end{aligned}$$

Since the training source symbol $s$ is known, the channel response has a relation to the received symbol vector $(r_0, r_1, r_2, r_3)$ as below:

$$h(t)^2 = \frac{(r_0 - r_1) \cdot (r_2 - r_3)}{|s|^2} \tag{3}$$

By measuring the amplitudes of received symbols, our noise-free channel measurement is calculated as $\frac{|r_0 - r_1| \cdot |r_2 - r_3|}{|s|^2}$, which reveals the mutual channel response.

### C. Cross-layer Noise-free Symbol-level Frequency-Time Channel Probing

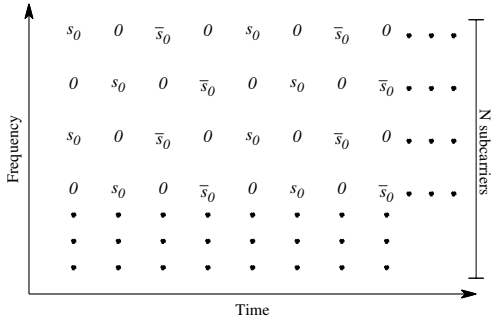


**Fig. 3: Symbol pattern design diagram.**

Since OFDM is widely used in today's wireless communication, we have designed a Frequency-Time channel probing that exploits not only the time variant channel dynamics, but also frequency selective channel dynamics. A challenge to noise-free channel measurement with OFDM is that it is not feasible in practice to generate an OFDM symbol with all subcarriers inserted of "0" symbols. Inspired by OFDM

piloting technique, we have designed a novel scheme that interlaces the source symbol vectors of $\boldsymbol{s} = (s, 0, \overline{s}, 0)$ in time domain as well as frequency domain. Fig 3 shows the Frequency-Time interlacing pattern of a source probing frame that consists of $M$ OFDM symbols with each containing $N$ subcarriers. To capture as many channel dynamics as possible across a probing frame, we suggest the probing frame size be at its maximum in standards, but yield the number OFDM symbol as a multiple of 4 for noise-free calculation as discussed next.

Once a probing frame of $M$ OFDM symbols is received through $N$ subcarriers with response $\boldsymbol{h} = (h_0, \ldots, h_{N-1})$, with the assumption that both the channel $h_i(\cdot)$ and the noise $n_i(\cdot)$ are invariant across the transmission of four consecutive symbols, we have a received symbol matrix $\boldsymbol{R}_{N\times M}$ as:

$$\begin{aligned}\boldsymbol{R} &= (\boldsymbol{r}_0 \ldots \boldsymbol{r}_{M-1}) \\ &= \begin{pmatrix} r_{0,0} & r_{0,1} & r_{0,2} & r_{0,3} & \ldots & r_{0,M-1} \\ r_{1,0} & r_{1,1} & r_{1,2} & r_{1,3} & \ldots & r_{1,M-1} \\ r_{2,0} & r_{2,1} & r_{2,2} & r_{2,3} & \ldots & r_{2,M-1} \\ r_{3,0} & r_{3,1} & r_{3,2} & r_{3,3} & \ldots & r_{3,M-1} \\ \vdots & \vdots & \vdots & \vdots & & \\ r_{N-1,0} & r_{N,-11} & r_{N-1,2} & r_{N-1,3} & \ldots & r_{N-1,M-1} \end{pmatrix} \\ &= \begin{pmatrix} h_0 \cdot s + n_0 & h_0 \cdot 0 + n_0 & h_0 \cdot \overline{s} + n_0 & h_0 \cdot 0 + n_0 & \ldots \\ h_1 \cdot 0 + n_1 & h_1 \cdot s + n_1 & h_1 \cdot 0 + n_1, & h_1 \cdot \overline{s} + n_1 & \ldots \\ h_2 \cdot s + n_2 & h_2 \cdot 0 + n_2 & h_2 \cdot \overline{s} + n_2 & h_2 \cdot 0 + n_2 & \ldots \\ h_3 \cdot 0 + n_3 & h_3 \cdot s + n_3 & h_3 \cdot 0 + n_3 & h_3 \cdot \overline{s} + n_3 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \end{pmatrix}\end{aligned}$$

Then, we partition $\boldsymbol{R}$ into $K = \frac{M}{4}$ sub-matrices $(\boldsymbol{P}_0 \ldots \boldsymbol{P}_{K-1})$ with $\boldsymbol{P}_i = (\boldsymbol{r}_{4i} \quad \boldsymbol{r}_{4i+1} \quad \boldsymbol{r}_{4i+2} \quad \boldsymbol{r}_{4i+3})$ contributing to a noise-free channel measurement vector for all $N$ subcarriers across the time of four symbols. By following the same process that derives Eq.(3), the measurement vector can be obtained as:

$$\boldsymbol{A}_i = \begin{pmatrix} \frac{|(r_{0,4i} - r_{0,4i+1})| \cdot |(r_{0,4i+2} - r_{0,4i+3})|}{|s_0|^2} \\ \frac{|(r_{1,4i} - r_{1,4i+1})| \cdot |(r_{1,4i+2} - r_{1,4i+3})|}{|s_0|^2} \\ \frac{|(r_{2,4i} - r_{2,4i+1})| \cdot |(r_{2,4i+2} - r_{2,4i+3})|}{|s_0|^2} \\ \frac{|(r_{3,4i} - r_{3,4i+1})| \cdot |(r_{3,4i+2} - r_{3,4i+3})|}{|s_0|^2} \\ \vdots \\ \frac{|(r_{N-1,4i} - r_{N-1,4i+1})| \cdot |(r_{N-1,4i+2} - r_{N-1,4i+3})|}{|s_0|^2} \end{pmatrix} \quad (4)$$

Therefore, for each probing, a channel measurement matrix $\boldsymbol{A}_{N\times K} = (\boldsymbol{A}_0 \quad \ldots \quad \boldsymbol{A}_{K-1})$ with $N \times K$ data elements can be obtained for key bit derivation, but signal strength based solutions can only generate at most one data element per probing.

**Implementation Challenge:** When the payload of a frame is loaded with the theoretically designed source symbol pattern, the entire frame cannot be correctly detected at a receiver due to frame acquisition failure because this special pattern inspired by the OFDM synchronization preamble pattern cannot be distinguished from the synchronization preamble. To remove this ambiguity, we enable a "guard band" that consists of a specific number of subcarriers that are used to transmit regular data symbols, rather than not the probing special symbols. For example, in our experiments, for total 256 subcarriers in an OFDM symbol, we only use the subcarriers [85:256] to load the probing symbols and leave [1:84] as the "guard band" for regular data. In this way, these 84 subcarriers help the OFDM synchronization recognize the separation between a preamble and a probing payload in the similar pattern.

## IV. Key Generation Algorithm Design

With the mutual channel measurements independently obtained at two trusted users, both users can now generate bits that constitute a key. Because of channel randomness, it is very likely that the channel measurements won't be exactly the same at both users and thus their keys independently derived from the channel measurements have to be reconciled for agreement before use. This section presents our design of key bit extraction, called *Quantization & Encoding*, out of the symbol-level noise-free Frequency-Time channel measurements, as well as *Bit Reconciliation & Key Generation*.

### A. Quantization & Encoding

In extracting bits from channel measurement, we adopt a level-crossing quantization as many conventional wireless information security solutions do [5]. However, to exploit the nano scale channel variations captured by our cross-layer symbol-level channel measurement, we design an XOR encoder after quantization.

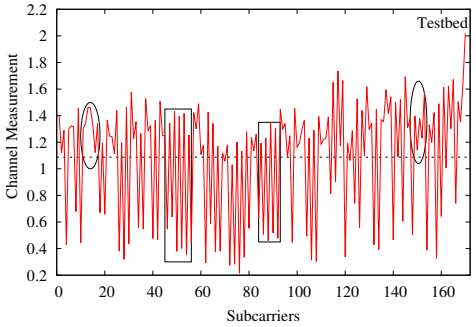


**Fig. 4: Channel measurement sample from testbed experiment. The dashed line indicates the mean value. Rectangles and ellipses indicate different types of observation.**

**Motivation.** In conventional wireless information security, the measured signal strength is actually a smoothened value across a probing frame and the measurements mostly have slow change over time because the channel does not normally vary dramatically among successive probing frames. That is also the reason why the measurements in static deployments result in large correlations. However, our channel measurements reveal nano-scale channel response across subcarriers, which are fundamentally different from signal strength measurements due to frequency selective fading among these subcarriers, which introduce large dynamics and thus maximize entropy. To obtain more insights into the dynamics in measurements, We plot a snapshot of channel measurements across subcarriers from our GNU SDR testbed in Fig. 4. The dashed line shows the mean of the measurements. From the results, the measurements show a highly dynamic variation across subcarriers in the frequency domain, which implies they have the quality to generate high entropy bits. It is interesting to observe that (i) mostly the measurement **crosses** the mean line up and down over a large block of neighboring subcarriers as highlighted by the rectangles, but (ii) occasionally it **remains** at one side (above or below) of the mean line for a few of subcarriers as marked by the ellipses. To exploit the information carried

by the measurement "spikes" across subcarriers, rather than using a plain multiple-level cross-level quantization, we design a hybrid quantization and encoding solution to extract bits from the channel measurements.

**Algorithm 1** Quantization&Encoding

**Alice&Bob:**
**Require:** Channel measurement matrix $A$ of size $N \times K$
  **for** $k = 0 : K-1$ **do**
    **for** $n = 0 : N-1$ **do**
      $m \leftarrow$MEAN$(A(0,k) : A(N-1,k))$ ▷ Calculate the mean for the $k$-th column in $A$.
      **if** $A_{n,k} > m$ **then**
        $Q \leftarrow [Q;\ 1]$
      **else**
        $Q \leftarrow [Q;\ 0]$
      **end if**
    **end for**
  **end for**
  **for** $k = 0 : K-1$ **do**
    **for** $n = 0 : N-2$ **do**
      $QE \leftarrow [QE;\ \text{XOR}(Q(n), Q(n+1))]$ ▷ XOR is the "exclusive or" operation.
    **end for**
  **end for**
  **return** $QE_A$ for Alice, $QE_B$ for Bob

**Algorithm Design.** Our hybrid key bit extraction is illustrated by Algorithm 1. The extraction process first calculates the mean of an $\boldsymbol{A}_k$ of channel measurement and uses the mean as a threshold to plainly quantify the channel measurement of each subcarrier in $\boldsymbol{A}_k$ into either "1" or "0". The result is a stream of $N$ binary bits stored in a list $Q$. Then, the bit stream pass through an *XOR encoder* that does XOR operation on every two consecutive bits. With the XOR encoding, the changes crossing the mean line either up or down, namely in the pattern of *...1,0,1,0...*, are transcoded into a block of "1"s and otherwise, namely in the pattern of *...1,1,1,...* or *...0,0,0,...*, results in a sequence of "0"s. After the transcoding, the $N \times K$ channel measurements in $\boldsymbol{A}_k$ are converted into $(N-1) \times K$ bits, labeled as $QE_A$ for Alice and $QE_B$ for Bob in Algorithm 1.

### B. Bits Reconciliation & Key Generation

The key bit sequences derived from the channel measurements independently collected at the trusted users Alice and Bob very likely disagree because of channel randomness and the half-duplex TDD probing. To reconcile the bit sequences for an agreed key, we design a reconciliation method similar to the *level-cross algorithm* in [5].

The reconciliation first indexes a bit sequence at Alice or Bob with $i_{n,k}$ denoting the $n$-th ($0 \le n \le N-2$) bit position of the bit sequence derived upon the $k$-th channel measurement vector $\boldsymbol{A}_k$ ($0 \le k \le M-1$) (as in Eq 4) of the measurement matrix $\boldsymbol{A}$ of a probing. Then the reconciliation proceeds as:

1. Following Algorithm 2, Alice parses the derived bits $QE_A$ to find any $\lambda$-length block of consecutive bits ($\{1,1,1,...\}$ or $\{0,0,0,...\}$) from $i_{start,k}$ to $i_{end,k}$ for a $\boldsymbol{A}_k$. Alice calculates the central index of a block of $\boldsymbol{A}_k$ as $i_{ctr,k} = \lfloor \frac{start+end+2k\cdot(N-1)}{2} \rfloor$, which indicates the location in the entire bit stream of the probing. The central indices of all $\lambda$-length blocks are then placed into a list $L_A$ that is sent to Bob. Since we focus on capturing the channel variation in frequency domain, the consecutive bits along time (i.e. $i_{n,start}$ to $i_{n,end}$) are not considered.
2. With the same algorithm, Bob also generates his list $L_B$. Based on the received list $L_A$ from Alice, Bob computes the intersection $L_{AB}$ of $L_A$ and $L_B$, i.e. $L_{AB} = L_A \cap L_B$. $L_{AB}$ indices the agreed central indices of $\lambda$-length blocks. Then, Bob sends back $L_{AB}$ to Alice.
3. Finally, Alice and Bob respectively generate a secret key by using the bits in $QE_A$ and $QE_B$ with indices $L_{AB}$. Even though, an adversary can acquire the index list $L_{AB}$ by eavesdropping, the key can not be cracked since the adversary has no idea about the corresponding data in source–$QE_A$ or $QE_B$.

**Algorithm 2** Central Indices Computation

**Alice&Bob:**
**Require:** The quantized and encoded bits $QE$ of size $(N-1) \times K$
  **for** $k = 0 : K-1$ **do**
    **for** $n = 0 : N-2$ **do**
      **if** $QE(n,k) = QE(n+1,k) = \cdots = QE(n+\lambda-1,k)$ **then**
        $n_{end} \leftarrow n + \lambda - 1$
        $L \leftarrow [L;\ \lfloor \frac{n+n_{end}+2k\cdot(N-1)}{2} \rfloor]$
      **end if**
    **end for**
  **end for**
  **return** $L_A$ for Alice, $L_B$ for Bob

### C. A Case Study of Key Generation

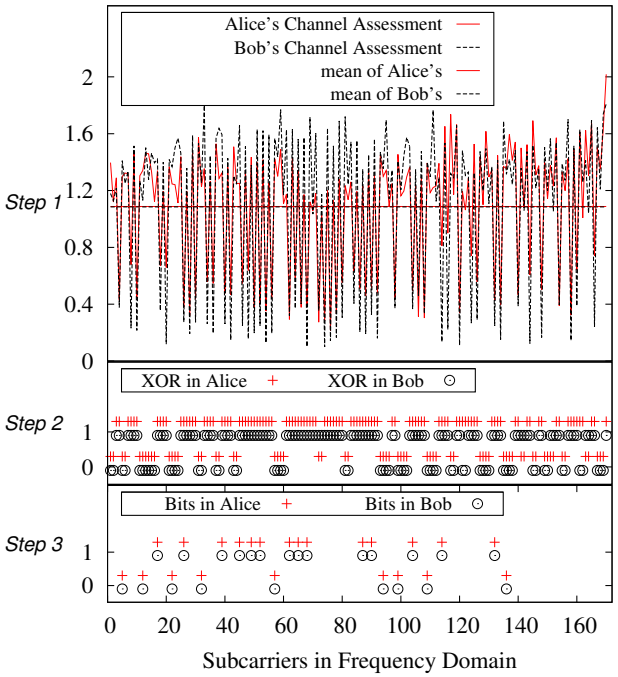


**Fig. 5: A case study showing key generation procedure.**

To illustrate the procedure of key generation, we have

conducted a case study with the algorithm. Fig 5 shows the procedure of key generation from an $\boldsymbol{A}_k$ of channel measurements from our GNU SDR testbed experiments. There are 172 subcarriers in total used to transmit the special probing symbols. We defer the testbed configuration to a section later. In this figure, *Step 1* shows the channel measurements in *quantization& encoding* phase at Alice and Bob. The extracted bits $L_A$ and $L_B$ are plotted in *Step 2* as the input to *bit reconciliation* where Alice and Bob generate the intersection list $L_{AB}$ according to Algorithm 2. Finally, based on $L_{AB}$, the secret key is formed as shown in *Step 3* that shows that Alice and Bob has the exactly the same key.

**Discussion of $\lambda$.** Parameter $\lambda$ plays an important role in Algorithm 2 that has significance on the key generation performance. A large $\lambda$ requires a large number of subcarriers to have close channel response, tends to miss the dynamics across subcarriers, and hurts KGR, which is against the original goal of fine-grained channel measurement. On the other hand, an extremely small $\lambda$ can result in significant key bit disagreement. For example, bit disagreement ratio is as high as $23\%$ with the data in Fig 5 if we set $\lambda = 1$. Through extensive experiments, we empirically find the optimal value for $\lambda$ is 3, which constantly yields the lowest bit disagreement ratios (e.g. $0\%$ with the data in Fig 5) while resulting in a high secret bit rate.

## V. Performance Evaluation

We have extensively evaluated the performance of the proposed cross-layer wireless information security on both a local GNU SDR simulator and a SDR testbed. The focus is on the robustness and secrecy performance in different channel environments. In experiments, $\lambda$ is configured to the optimal value 3 as discussed above and we use $s = (1 + j)$ as the source signal symbol in probing.

### A. Simulation Evaluation

**Settings:** We have implemented our proposed solution into GNURadio. To precisely control channel variations, we have also ported *Jake's* (1993) fading channel simulator into our simulator. We have conducted end-to-end transmissions between Alice and Bob with an IEEE 802.11-like physical layer. The frame length is of 1200 bytes with probing at 20 frames per second at each direction.

*1) Channel Variations on SNR:* We first comparatively evaluate the security performance of our solution and conventional solution under different SNR channel settings. To obtain the signal strength for conventional solutions, we use the received power in every subcarrier as the signal strength for an OFDM symbol. In this way, the signal strength data is collected per OFDM symbol that is already at higher resolution than per-frame solutions. For each channel condition, both our cross-layer solution and the optimal signal strength solution are tested with the same settings and algorithms to generate keys for fair performance comparison. We evaluate *key generation rate (KGR)*, *entropy rate*, and *bit disagreement ratio* at various SNR conditions and plot the results in Fig 6.

**Results & Analysis of the Proposed Cross-layer Solution:** For the top and center plots, we observe that KGR and entropy rate grow up to the maximal along with SNR, but then remain, which implies (i) improving channel condition favors KGR , but, ii) very high SNR does not surely boost KGR any more once it reaches the summit. The largest KGR is about 19 *bits/frame* or 380 *bps* in our configuration, which is improved by two orders of magnitude over the KGR of 1.2 *bps* in conventional solutions [5]. From the bottom plot, as expected, bit disagreement can be improved by high SNR. The minimal bit disagreement ratio is about $4\%$ at 30 $dB$.

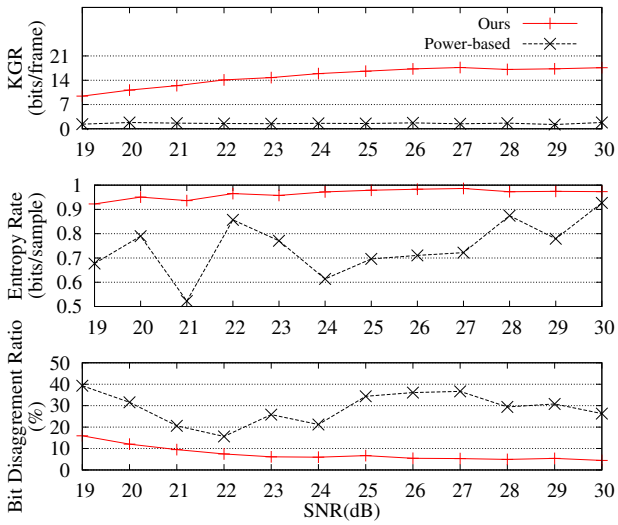


**Fig. 6: Performance under various channel conditions.**

**Comparative Results & Analysis:** As shown in Fig 6, our cross-layer Frequency-Time solution outperforms the optimal signal strength solution in every aspect, including KGR, entropy rate and bit disagreement ratio. The optimal signal strength solution merely has KGR about 1 *bits/frame* and its bit disagreement ratio can be as poor as 40%, which is surely unacceptable for any cryptography service. Signal strength solutions are feasible to measure large-scale channel deep fading as many prior works have shown, but they are incapable to capture small-scale or nano-scale channel dynamics, but the proposed cross-layer Frequency-Time solution has the merits of capturing not only the nano-scale variations, but also the frequency selective variations, which improves the secrecy performance over signal strength based solutions by orders of magnitude. We can also observe that the cross-layer Frequency-Time solution has exciting entropy performance of the derived key bits that is about $40\%$ improvement over the optimal signal strength solution. This is because the proposed solution measures the channel response of all subcarriers that are supposed to be very independent because of frequency selective fading, while signal strength solutions measure the temporal variations that will be largely correlated if the channel does not significantly change.

*2) Channel Variations on Doppler Shift:* We have also evaluated our solution under channel conditions with mobility by adjusting *Doppler* shift (DS) from 0 $Hz$ to 200 $Hz$ at a fixed SNR (30 $dB$). The results are plotted in Fig. 7.

**Results & Analysis:** Both KGR and entropy rate benefit from a certain degree of Doppler shift, e.g. $50Hz$. Similar observations are also reported in [6], [9]. However, even without mobility (Doppler shift = 0), our solution still can achieve high entropy rate (e.g. >0.96 bits/sample). Bit disagreement ratio always remains very low and does not change significantly along

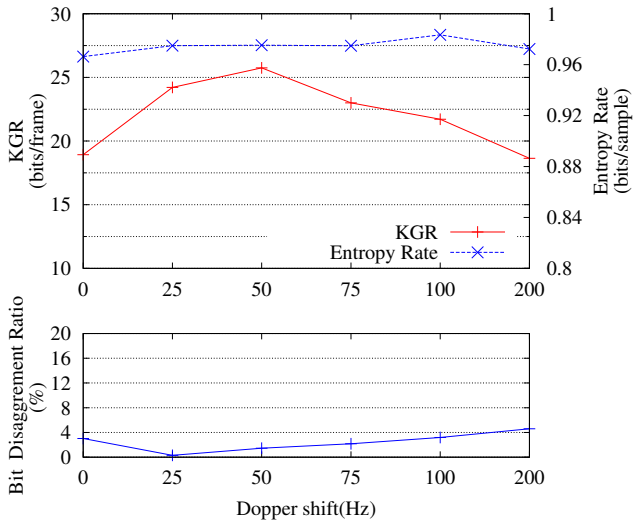


**Fig. 7: Performance under Doppler shifts at SNR=30 $dB$.**

with Doppler shift. This implies that our solution is highly effective regardless of mobility that is normally required by signal strength based solutions to generate keys of acceptable entropy.

*3) Secrecy:* A strong secret key is expected to possess two merits: *high randomness* and *strong independence*. High randomness protects the key from being predicted by proactive adversary, and strong independence across various channel environments makes it difficult to reproduce the key by mimicking channel. It is of interest to assess the performance of randomness and independence of the proposed cross-layer solution.

**Randomness:** We adopt a randomness test–*Runs. test* [17]––from the NIST test suite, because it determines if a two-value data set is from a random process that best fits out a case. We have conducted *Runs. test* upon the key bits obtained in above simulation experiments and the results (*p-value*) are summarized in Table I below:

**TABLE I:** *Runs. test* **results**

| SNR(dB) | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 |
|---|---|---|---|---|---|---|---|---|---|
| *p-value* | 0.28 | 0.48 | 0.23 | 0.45 | 0.64 | 0.33 | 0.09 | 0.23 | 0.60 |
| DS(Hz) | 0 | | 25 | | 50 | | 75 | 100 | 200 |
| *p-value* | 0.36 | | 0.64 | | 0.88 | | 0.65 | 0.48 | 0.70 |

A *p-value*$>$0.01 indicates that the key bits are random enough. As shown in the table, all key bits derived in different scenarios (SNR or DS) pass the randomness test and their randomness is large in most cases.

**Independence:** With the same data sets, we have evaluated the inter-dependence between the secret keys across different scenarios. We have computed the correlation coefficients of key bits derived in different SNR with DS=0 (no *Doppler* shift), as well as those derived in different Doppler shifts (DS) with SNR 30 $dB$. The correlation coefficient mean and its standard deviations of each scenario are plotted in Fig 8.

As observed, across all 16 data sets, the maximal coefficient is around $\pm 0.1$ with very small means, which implies the keys generated by our solution maintains strong independence across SNR variations as well as *Doppler* shifts.

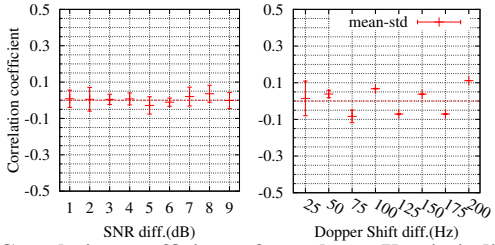


**Fig. 8: Correlation coefficient of two keys. X-axis indicates the SNR difference (SNR diff. =** $|SNR_1 - SNR_2|$**), or** *Doppler* **shift difference (Doppler shift diff. =** $|DS_1 - DS_2|$**), between any two scenarios where the keys are derived.**

## *B. Testbed Evaluation*

**Setting:** We have implemented a GNU SDR testbed consisting of two USRP2 N210 nodes (Alice and Bob) to evaluate our solution in practice. GNURadio USRP2 does not support complete IEEE 802.11 MAC layer and suffers from high latency in procuring RF sample and TR switch (transmit receive switch). Therefore, we have used different settings from simulation for testbed evaluation: probing frame size (800 bytes) and probing rate (1 probing/s) for each test in order to suppress errors due to testbed limitation. As mentioned earlier in Section III-C, among total 256 OFDM subcarriers, we take 84 of them as the "guard band" and use the rest 172 subcarriers to load the probing symbols. The testbed runs on 5.0 $GHz$ carrier frequency band in an indoor environment at late nights to avoid human interference.

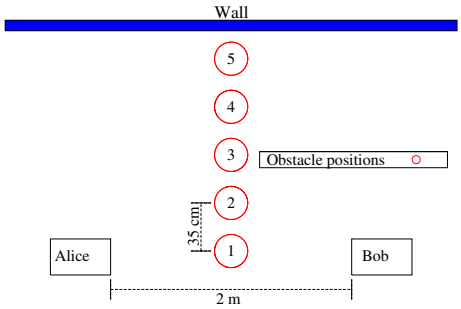


**Fig. 9: Testbed deployment**

**Test scenarios:** Our testbed evaluation environment is shown in Fig 9. To intrigue various channel conditions, we place a static object (a metal cup) at five locations between Alice and Bob. At location 1 that is in the middle of Alice and Bob, there is no Line-of-Sight (LOS). With this controllable setting with two adjacent locations being close, we can investigate the independence of keys with *slight* channel variations. The experiment at each position runs 14 seconds to generate key bits, and all experiments are finished within 2 minutes. Thus, we assume the channel background is nearly invariant, especially at midnights.

**Results & Analysis:** We have evaluated KGR, entropy rate and bit disagreement ratio of the proposed cross-layer solution and the results are shown in Table II. As we can observe, random channel dynamics in realistic environments actually help the solution achieve a large KGR up to 24.07 *bits/frame* with 8.8% bit disagreement at position *2*. The bit disagreement in testbed mostly results from long latency of the RF send-receive switch limited by the SDR hardware. Another observation is that, non-LOS or weak LOS at positions *1, 2*

**TABLE II: Testbed performance**

| Key | KGR (bits/frame) | Entropy Rate (bits/sample) | Bit Disagreement Ratio (%) |
|---|---|---|---|
| $K_1$ | 17.49 | 0.982 | 1.6 |
| $K_2$ | 24.07 | 0.988 | 8.8 |
| $K_3$ | 12.15 | 0.387 | 12.0 |
| $K_4$ | 12.72 | 0.928 | 15.0 |
| $K_5$ | 12.57 | 0.608 | 14.9 |

**TABLE III: Correlation coefficients**

| X,Y | $K_1,\ K_2$ | $K_1,\ K_3$ | $K_1,\ K_4$ | $K_1,\ K_5$ | $K_2,\ K_3$ |
|---|---|---|---|---|---|
| corr(X,Y) | -0.009 | -0.156 | 0.106 | 0.085 | -0.146 |
| X,Y | $K_2,\ K_4$ | $K_2,\ K_5$ | $K_3,\ K_4$ | $K_3,\ K_5$ | $K_4,\ K_5$ |
| corr(X,Y) | -0.037 | -0.032 | -0.099 | 0.082 | -0.099 |

results in better the performance than other positions *3, 4, 5*. Without LOS, the signal transverses through multiple paths each of which contributes significantly to the channel response. Thus key generation benefits form this diversity. A strong LOS dominates the channel response against other paths and yields worse KGR and entropy rate.

In addition, we also calculate the correlation coefficients between any pair of keys ($C_5^2$ pairs in total) derived at those five positions, which are summarized in Table III. Small correlation coefficients (ranging from -0.156 to 0.106) are observed, which implies these secret keys possess strong independence with even very small spatial separation, 35 $cm$. This also indicates that with the proposed solution, a key is difficult to be guessed by a malicious user Eve even if she is very close to a trusted user. Therefore, the proposed cross-layer solution is proved of, not only high efficiency with large KGR, but also strong secrecy in generated keys.

### C. Channel Measurement

It is important to evaluate and understand how reliable and robust the cross-layer channel measurement is, and what factor affects our channel measurement most. We have conducted experiments on both simulator and testbed to answer these questions.

**Measurements v.s. SNR/DS:** In the prior simulation experiments discussed earlier in Section V-A, we have also collected the channel measurement under various SNR and Doppler shift as shown in Fig 10. From the results, SNR and Doppler shift have very slightly impact on the channel measurement. Namely, the design cross-layer channel measurement is robust to SNR or Doppler shift. This is because based on the theoretical foundation of its design in Eq.(3), our channel measurement only relates to the instant noise-free channel response in frequency domain.

**Measurements v.s. Multi-path Fading:** Because multi-path fading affects the channel response, it is also expected to affect the channel measurements. To obtain insights, we have designed experiments to study the relation between multi-path fading and the cross-layer channel measurement. In simulation, the change of multi-path fading can be achieved by chaining the complex-coefficient of FIR filter in *Jake's* channel model.

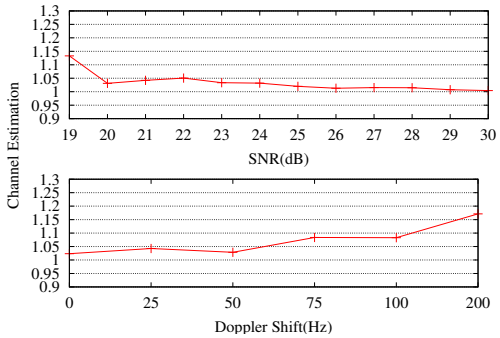


**Fig. 10: Channel measurement v.s. SNR(upper) and Doppler Shift(lower).**

On the testbed, we change the antenna direction to trigger the variation of multi-path components.

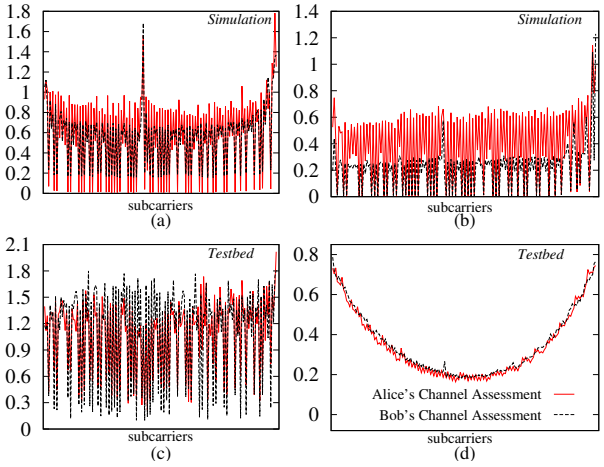


**Fig. 11: Channel measurement patterns under different channel environments. (a) is obtained by adding one more fading path to the simulated channel, (b) is a case with a stronger magnitude of the second fading path in simulator, (c) is a testbed scenario with two SDR antennas pointing to each other while (d) is a testbed case with antennas toward a wall.**

**TABLE IV: Measurement vs Secrecy**

| Scenario | Mean of Channel Measurement | p-value | Entropy Rate (bits/sample) |
|---|---|---|---|
| (a) | 0.68263 | 8.2e-9 | 0.77 |
| (b) | 0.24265 | 1.2e-8 | 0.82 |
| (c) | 1.08762 | 1.00 | 0.99 |
| (d) | 0.34588 | 0.17 | 0.15 |

Fig 11 plots the channel measurement patterns of four different channel scenarios. As we can observe, by changing the channel itself, the channel measurement shows a significant change too. With a controllable channel in simulation, by slightly tuning the magnitude of a fading path, the channel measurement sharply decreases from (a) to (b). A more dramatic change happens in the testbed scenarios where two completely different channel response measurement patterns are obtained as in (c) and (d) with only the antenna rotation. This implies that, in practice, the multi-path components of channel are very sensitive to any small spatial variation and our proposed channel measurement that can capture the resulted changes in frequency domain can produce high-quality keys.

**Measurement v.s. Secrecy:** We calculate the secrecy performance of the keys generated from the measurements

under those four scenarios in Figure 11 and summarize the secrecy performance in Table IV. From the data, a low channel measurement (e.g. 0.68, 0.24 0.34 in (a),(b),(d)) often yields a poor key: either poor randomness with p-value$<$0.01 (in (a),(b)) or unacceptable low entropy rate (in (d)). The is because a low channel measurement is not reliable or accurate any more to reveal channel response.

## VI. Conclusion

This paper proposes a cross-layer solution that generates shared secret keys from the noise-free per-symbol measurements of channel response in frequency domain. This solution improves the security performance by orders of magnitude over conventional solutions. The performance has been evaluated on both a GNU SDR testbed in practice and a local GNU Radio simulator. The proposed solution generates a KGR of 24.07 bits per probing frame on testbed or 19 bits in simulation, and has a low key bit disagreement ratio, less than 4% while maintaining a high entropy rate greater than 0.93. The derived keys show strong independence with low correlation coefficients around $\pm 0.1$ across various channel environments . Moreover, this solution shows strong secrecy and high efficiency because any minor physical change, e.g. a small antenna rotation, results in significant difference in frequency measurements.

## References


[1] R. Liu and W. Trappe, *Securing wireless communications at the physical layer*. Springer Publishing Company, 2009.

[2] U. Maurer, "Secret key agreement by public discussion from common information," *Information Theory, IEEE Transactions on*, vol. 39, no. 3, pp. 733–742, May 1993.

[3] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. McLaughlin, "Wireless information-theoretic security," *Information Theory, IEEE Transactions on*, vol. 54, no. 6, pp. 2515–2534, June 2008.

[4] Y. Liang and H. V. Poor, *Information theoretic security*. Foundations and Trends in Communications and Information Theory, 2009, vol. 5, no. 4.

[5] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," ser. MobiCom '08. New York, NY, USA: ACM, 2008, pp. 128–139.

[6] 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," ser. MobiCom '09. New York, NY, USA: ACM, 2009, pp. 321–332.

[7] C. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, pp. 3–28, 1992.

[8] A. Khisti and S. Diggavi, "A remark on secret-key generation over correlated fading channels," in *GLOBECOM Workshops (GC Wkshps), 2011 IEEE*, Dec 2011, pp. 864–868.

[9] Y. Wei, K. Zeng, and P. Mohapatra, "Adaptive wireless channel probing for shared key generation based on pid controller," *Mobile Computing, IEEE Transactions on*, vol. 12, no. 9, pp. 1842–1852, Sept 2013.

[10] 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, Jan 2010.

[11] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 401–410.

[12] Y. Liu, S. Draper, and A. Sayeed, "Secret key generation through ofdm multipath channel," in *Information Sciences and Systems (CISS), 2011 45th Annual Conference on*, March 2011, pp. 1–6.

[13] A. Sayeed and A. Perrig, "Secure wireless communications: Secret keys through multipath," in *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, March 2008, pp. 3013–3016.

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

[15] H. Liu, Y. Wang, J. Yang, and Y. Chen, "Fast and practical secret key extraction by exploiting channel response," in *INFOCOM, 2013 Proceedings IEEE*, April 2013, pp. 3048–3056.

[16] T. Schmidl and D. Cox, "Robust frequency and timing synchronization for ofdm," *Communications, IEEE Transactions on*, vol. 45, no. 12, pp. 1613–1621, Dec 1997.

[17] Bradley, *Distribution-Free Statistical Tests*, 1968, vol. Chapter 12.