Shared Secret Key Generation via Carrier Frequency Offsets

Waqas Aman*, Aneeqa Ijaz*, M. Mahboob Ur Rahman*, Dushanta Nalin K. Jayakody†‡, Haris Pervaiz§
*Electrical Engineering department, Information Technology University (ITU), Lahore, Pakistan
{waqas.aman,aneeqa.ijaz,mahboob.rahman}@itu.edu.pk
†School of Computer Science & Robotics, National Research Tomsk Polytechnic University, Russia (nalin@tpu.ru)
‡School of Postgraduate Studies and Research, Sri Lanka Technological Campus, Sri Lanka
§School of Computing and Communications, Lancaster University, UK (h.b.pervaiz@lancaster.ac.uk)

***Abstract*—This work presents a novel method to generate secret keys shared between a legitimate node pair (Alice and Bob) to safeguard the communication between them from an unauthorized node (Eve). To this end, we exploit the *reciprocal carrier frequency offset* (CFO) between the legitimate node pair to extract common randomness out of it to generate shared secret keys. The proposed key generation algorithm involves standard steps: the legitimate nodes exchange binary phase-shift keying (BPSK) signals to perform blind CFO estimation on the received signals, and do equi-probable quantization of the noisy CFO estimates followed by information reconciliation–to distil a shared secret key. Furthermore, guided by the Allan deviation curve, we distinguish between the two frequency-stability regimes—when the randomly time-varying CFO process i) has memory, ii) is memoryless; thereafter, we compute the key generation rate for both regimes. Simulation results show that the key disagreement rate decreases exponentially with increase in the signal to noise ratio of the link between Alice and Bob. Additionally, the decipher probability of Eve decreases as soon as either of the two links observed by the Eve becomes more degraded compared to the link between Alice and Bob.**

I. Introduction

Physical-layer security has its roots in 1950's when Shannon argued that perfect secrecy is possible provided that the entropy of the secret key is greater than the entropy of the to-be transmitted message [1]. Later on, Wyner, in his influential work introduced the notion of Gaussian wiretap channel to compute the so-called secrecy capacity in additive white Gaussian noise (AWGN) channels [2]. Csiszar [3] then extended the notion of secrecy capacity to the wireless fading channels. Maurer [4] was first to suggest to extract shared secret keys from a common source of randomness. Nevertheless, until last decade, the world had been accustomed to using higher-layer cryptographic protocols for authentication/security purposes. More recently, there is a growing interest in designing algorithms at the physical layer so as to complement/improve the existing security mechanisms, see, e.g., [5],[6] for a quick overview of recent development in the field.

In the literature on physical layer security, two popular models exist: i) Wyner's wiretap model, and ii) Basic source model. Wyner's wiretap model assumes that eavesdropper is using a degraded version of the main channel, and utilizes channel coding to approach the secrecy capacity. Having said this, much work has been done to design channel coding schemes which meet the absolute limits of secrecy capacity [7]. On the other hand, under the Basic source model, two legitimate nodes obtain multiple correlated observations from a shared random source. Both nodes then quantize their observations, do the information reconciliation [8] (to eradicate the bit mismatch at both ends) followed by privacy amplification [9] (to hash out the bits revealed during information reconciliation phase) to distil a shared secret key.

For the Basic source model, researchers have exploited the random and reciprocal nature of wireless medium in single-antenna and multiple-antenna settings to generate shared secret keys [10], [11]. Additionally, the feasibility of using the relays/friendly jammers to design high performance key generation algorithms is reported in [12], [13].

Apart from the medium, physical characteristics of the underlying device hardware can also be used for security, e.g., integrated circuits [14], oscillators [15–18], antennas [19], non-reciprocal hardware [20] etc. In this paper, we exploit *reciprocal carrier frequency offset* (CFO) between a node pair to generate secret keys shared between that node pair. To the best of authors' knowledge, there has been no work on this expect [15–17], which all use the CFO for authentication.

The main contributions of this paper are two-fold: i) a novel algorithm which constructs shared secret keys from the noisy CFO estimates ii) key generation rate of the CFO process.

The rest of this paper is organized as follows. Section II introduces the system model and the CFO models. The proposed, CFO based method for secret key generation is presented in Section III. Section IV studies the key generation rate of the CFO process. Section V provides some simulation results. Finally, Section VI concludes.

II. System Model & CFO Background

A. System Model

The system model consists of three nodes, Alice, Bob and Eve. As shown in Fig. 1, Alice and Bob make a legitimate node pair who intend to establish a secure wireless communication link in order to exchange confidential messages. Eve is a malicious node who passively eavesdrops in order to decipher the shared secret key being used by Alice and Bob. The legitimate node pair operates in half-duplex/time-division duplex (TDD) mode with T seconds long time-slots. Specifically, in order to

measure the CFO to learn a shared secret key, Alice and Bob exchange binary phase shift keying (BPSK)-modulated packets to each other. Finally, the center frequency of the channel is ω_c rad/sec.

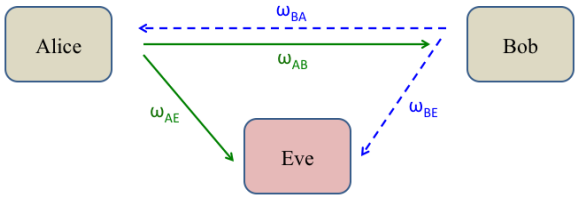

Fig. 1. System model.

B. CFO is Reciprocal

CFO is a measure of the speed of oscillations of a device's oscillator relative to that of another device. CFO arises due to manufacturing tolerance of oscillators; and may drift over time due to environmental/operating conditions. CFO is *reciprocal*: let $\omega_{AB} = \omega_A - \omega_B$ (rad/sec) be the CFO between "Alice and Bob", then reciprocity implies that $\omega_{AB} = -\omega_{BA}$. Therefore, the mutual CFO ω_{AB} can indeed be exploited by the legitimate node pair (Alice and Bob) to generate shared secret keys every once in a while. Fig. 2 plots the two CFO's ($f_{AB} = \omega_{AB}/2\pi$[1] and $-f_{BA} = -\omega_{BA}/2\pi$) against time. To obtain Fig. 2, an experiment was set up whereby two GNU Radio/USRP based software-defined radios (SDR) exchanged unmodulated tones/sinusoids with each other in frequency-division duplex (FDD) fashion to measure the (time-varying) CFO in both directions. Fig. 2 verifies that the CFO is indeed reciprocal.

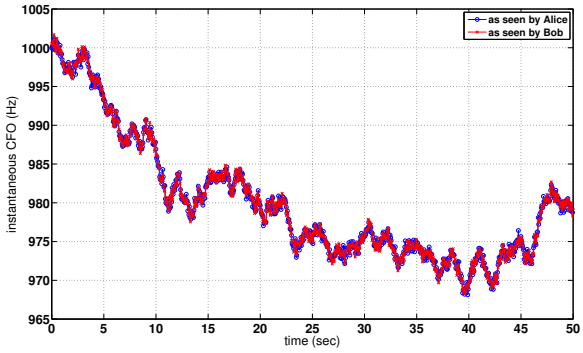

Fig. 2. Experimental validation: CFO between a node pair is reciprocal.

C. CFO Models

We now introduce the three fundamental models which govern the random, time-varying nature of the CFO.

Model M1: CFO is time-invariant. Under this model, the CFO ω_{AB} is treated as a random variable with distribution $U(-2\pi\Delta, 2\pi\Delta)$ where Δ could be derived from the parts-per-million (ppm) specs of the oscillators under consideration. This work considers the homogeneous case, i.e., when all the three nodes (Alice, Bob, Eve) of the considered system model use oscillators with same stability (ppm) specification. Let each of the three oscillators have an accuracy of x ppm, then $\Delta = f_c \times x$ Hz (f_c is the center frequency in MHz).

The construction of the remainig two models, model M2 and model M3 is based upon the so-called Allan Deviation[2]. So, Allan deviation first.

Allan deviation. Fig. 3 shows a typical plot of the Allan deviation $\sigma_y(\tau)$ against the observation interval τ. Fig. 3 indicates that there are two frequency-stability regions for the oscillators. In the short-term stability region (which lasts from few seconds to few minutes), white frequency noise dominates, while in the long-term stability region, random walk frequency noise dominates.

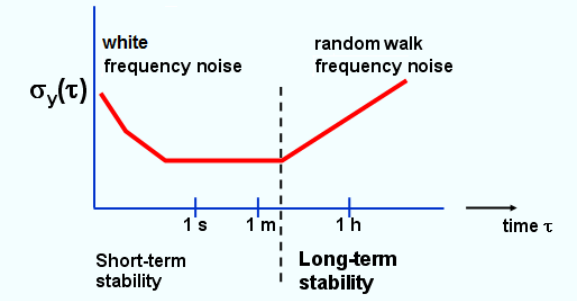

Fig. 3. Allan deviation $\sigma_y(\tau)$ as a function of the observation interval τ.

Model M2: CFO is time-varying and memory-full. Model M2 represents the long-term stability region of the Allan deviation curve. Here, aging/temperature effects cause the CFO to undertake a random walk over time [21], [22]:

$$\text{Model M2a: } \omega_{AB}(k+1) = \omega_{AB}(k) + n_{AB}(k) \qquad (1)$$

where $n_{AB}(k) \sim N(0, \sigma^2)$ is the random walk frequency noise. Let $t_k - t_{k-1} = T$ be the duration of a time-slot. Then, $\sigma^2 = \omega_c^2 q_2^2 T$ where $q_2^2 = 5.51 \times 10^{-18}$ for USRP N200 radios [23]. Re-arranging Eq. (1), we have:

$$\text{Model M2b: } n_{AB}(k) = \omega_{AB}(k+1) - \omega_{AB}(k) \qquad (2)$$

Note that the original stochastic process $\{\omega_{AB}\}_k$ of Eq. (1), Model M2a, is non-stationary auto-regressive moving average (ARMA) process, while the stochastic process $\{n_{AB}\}_k$ of Eq. (2), Model M2b, is stationary with independent and identically distributed (i.i.d) elements.

Model M3: CFO is time-varying and memoryless. Model M3 represents the short-term stability region of the Allan deviation curve. Here, the CFO $\{\omega_{AB}\}_k$ is a memoryless random process. That is, the CFO stays constant for the slot duration T; moreover, the CFO realizations across the slots

[1]We use the notation ω (rad/sec) and f (Hz) in interchangeable manner throughout the rest of the paper.

[2]Allan deviation is a well-known measure of frequency-stability of the oscillators [21], [22].

are i.i.d $U(-2\pi\Delta, 2\pi\Delta)$. This model resembles closely the well-acclaimed block-fading model for wireless channels.

At this point, some comments about the three CFO models are in order. Model M1, model M3 represent extreme/limiting cases whereby the CFO does not change at all, change independently during every time-slot, respectively. Furthermore, Model M1 represents an ideal oscillator (closest to which are the atomic clocks). On the other hand, all the commodity oscillators follow the Allan deviation curve which implies that they follow either model M2, or, model M3, depending upon the total time of their operation. Finally, we note that model M1 provides only 1 secret key during the life-time of an (ideal) oscillator; therefore, the rest of this paper will focus on model M2 and model M3 (and thus, commodity oscillators) only.

III. The Proposed Method

Due to two-way communication between Alice and Bob, four CFOs are of interest: $\omega_{AB}, \omega_{BA}, \omega_{AE}, \omega_{BE}$ (see Fig. 1). Appendix A describes a blind method for CFO estimation from BPSK-modulated data. Having obtained the noisy CFO estimates $\hat{\omega}_{AB}(k) = \omega_{AB}(k) + \nu_{AB}(k)$ and $\hat{\omega}_{BA}(k) = \omega_{BA}(k) + \nu_{BA}(k)$, Alice and Bob utilize them to generate secret keys. $\nu_{AB}(k) \sim N(0, \sigma^2_{AB})$ ($\nu_{BA}(k) \sim N(0, \sigma^2_{BA})$) is the estimation error at Alice (Bob). Specifically, with the CFO measurements in hand, the legitimate nodes need to do information reconciliation followed by privacy amplification. For information reconciliation, both nodes utilize linear block codes to exchange syndrome to eradicate the bit mismatch[3]. For privacy amplification, universal hash functions could be used to hash out the information revealed.

The essential steps of the proposed method are formally summarized below. Alice and Bob:

1) exchange BPSK signals to perform blind CFO estimation on the received signals to get $\hat{\omega}_{BA}$, $\hat{\omega}_{AB}$, respectively.
2) quantize their individual CFO estimates using equi-probable/uniform quantization to get K_A and K_B, respectively. K_A (K_B) is length-n binary key at Alice (Bob).
3) do information reconciliation using linear block codes to construct reconciled keys $\mathcal{K}_A$ and $\mathcal{K}_B$, respectively.

Note that uniform quantization in step 2 results in some entropy loss, while information reconciliation in step 3 reveals some information as well (due to public discussion). Thus, both steps 2,3 reduce the secret bit rate (SBR) to some extent.

Remark 1. Since model M2 is an ARMA process, both Alice and Bob implement a linear Kalman filter (LKF) (after step 1 and before step 2) to effectively track the drifting CFOs. Each of the two LKFs is fed by the noisy CFO estimate (outputted by the blind estimation method) and yields the filtered CFO estimate. Note that the LKF is the best linear unbiased estimator of the CFO. Therefore, once LKF is converged, each legitimate node utilizes its filtered estimate to implement step 2 and step 3. More details on using the LKF to track the drifting CFOs could be found in [16],[23].

[3]Note that when the public discussion for information reconciliation is not feasible, each of the legitimate nodes (Alice and Bob) could do majority decision decoding at its end for authentication. That is, Bob authenticates Alice if the received secret key and the local key have at most p ($0 < p < n$) mismatches, where n is the length of the shared secret key.

IV. Key Generation Rate of the CFO Process

A. Differential Entropy Rates

The differential entropy rate of model M2b is: $h_{M2b} = \frac{1}{2}\log_2(2\pi e \omega_c^2 q_2^2 T)$ bits/realization, thanks to $\{n_{AB}\}_k$ being a stationary process with i.i.d. elements, see Eq. (2). The differential entropy rate of model M3 is: $h_{M3} = \log_2(4\pi\Delta)$ bits/realization. Note that h_{M3} is non-negative when $\Delta \geq \frac{1}{4\pi} = 0.0796$ Hz which is satisfied easily by the low to medium-end temperature/voltage-controlled oscillators (which culminate in a CFO on the order of hundreds of Hz when tuned to a center frequency of few hundreds of MHz). Also, h_{M2b} is non-negative when $\omega_c^2 T \geq \frac{1}{2\pi e q_2^2} = 1.06 \times 10^{16}$ (this inequality is satisfied, say, with $T = 1$ ms, for $f_c = \frac{\omega_c}{2\pi} \geq \frac{1.03}{2\pi}$ GHz).

B. Key Generation Rate

The key generation rate (KGR) of the proposed method depends on the Auto-correlation function (ACF) of the CFO process $\{f_{AB}\}_k$. Specifically, with $1 \leq p \leq q$, let $f_{AB}(p)$ and $f_{AB}(q)$ represent the CFO at time p and q, respectively. Then, the ACF for model M2a (a first-order ARMA process) is: $\text{ACF}_{M2a}(p,q) = \sqrt{\frac{p}{q}}$. It is also straightforward to see that the ACF for model M2b (a stationary process with i.i.d. elements) is: $\text{ACF}_{M2b}(p,q) = \delta(p-q)$ where $\delta(p-q)$ is the Dirac delta function; $\delta(p-q)$ is 1 for $p = q$, and zero otherwise. Similarly, the ACF for model M3 is: $\text{ACF}_{M3}(p,q) = \delta(p-q)$. For model M2a, a new realization of the CFO process occurs when $\text{ACF}_{M2a} \leq \eta$ where $\eta > 0$ is a small threshold. Let T_{M2a} denote the time to obtain a new realization for model M2a. Then, $\text{KGR}_{M2a} \leq \frac{h_{M2a}}{T_{M2a}}$ bits/sec. For model M2b and model M3, a new realization of the CFO process occurs every T seconds. Therefore, or, $\text{KGR}_{M2b} \leq \frac{h_{M2b}}{T}$ bits/sec, and $\text{KGR}_{M3} \leq \frac{h_{M3}}{T}$ bits/sec.

V. Numerical Results

In this section, we assess the performance of the proposed CFO based secret key generation method by investigating the following metrics: auto-correlation function, key generation rate, key disagreement rate, and decipher probability of Eve.

Fig. 4 (a) plots the ACF for the models M2a, and M3. Note that the ACF for model M2a depends explicitly on the absolute time instants p and q. Thus, the ACF of model M2a does not decay unless p and q are quite far apart. Therefore, assuming that $f_{AB}(p)$ corresponds to M-th sample for i-th secret key, and $f_{AB}(q)$ corresponds to first sample for $(i+1)$-th secret key, one can see that the KGR for model M2a decays exponentially over time. For illustration, assume that $T = 50$ ms and required $ACF_{M2} < \eta = 0.3$. Then, Fig. 4 (b) shows that the time between generation of two successive keys increases exponentially for model M2a. In other words, due to non-stationary nature of model M2a, the CFO could provide only few (~ 10) secret keys within useful operating time. On the other hand, model M3 could provide 1 secret key every T seconds. In other words, KGR of model M3 is $\frac{1}{T}$ keys/sec.

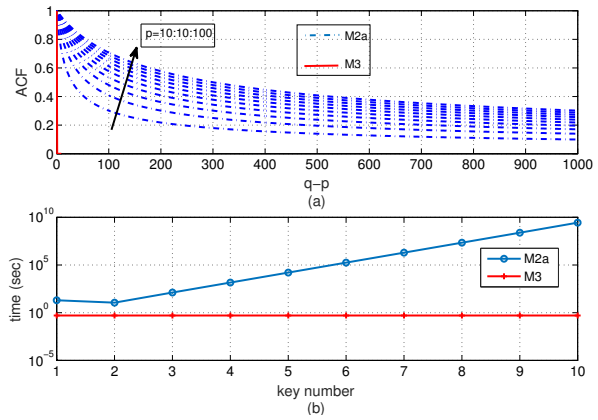

Fig. 4. (a) ACF of the CFO for models M2a, M3, (b) time between generation of two successive keys for models M2a, M3.

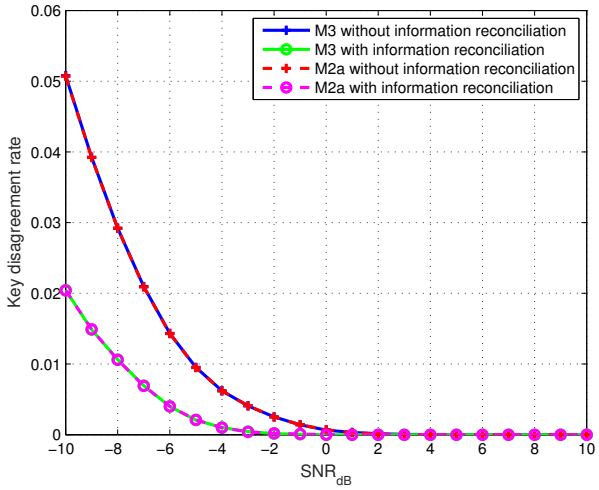

Fig. 5. Key disagreement rate vs. SNR.

Fig. 5 plots the average key disagreement rate (KDR)–a measure of the CFO reciprocity–against the signal-to-noise ratio (SNR) for models M2a, and M3. The average KDR is defined as: average number of bits mismatched between the (length-n) keys of Alice and Bob. That is, average KDR is computed as $\sum_N \frac{\#(K_A \neq K_B)}{n}$, or, $\sum_N \frac{\#(\mathcal{K}_A \neq \mathcal{K}_B)}{n}$, depending upon the stage, i.e., before or after information reconciliation. The $\#(A \neq B)$ operator outputs the number of bits mismatched between two length-n sequences A and B. Thus, for Monte-Carlo simulations, we set $N = 1e5$, use equi-probable quantization with 3 quantization levels, and utilize Hamming $(7, 4)$ code for information reconciliation. Fig. 5 reveals that the average KDR decreases exponentially fast with increase in SNR, for both models M2a, M3. Additionally, for any given SNR, the information reconciliation helps reduce the KDR (though the gap diminishes with increase in SNR), as expected.

Fig. 6 plots the average decipher probability of Eve (DPE) as a heat map for a range of pathloss values experienced by the two links (Alice to Eve, and, Bob to Eve) seen by Eve. The average DPE is defined as: average number of bits matched between the (length-n) key of Eve and the reconciled keys of Alice and Bob. That is, average DPE is computed as: $\frac{1}{2}\Big[\sum_N \frac{\#(K_E=\mathcal{K}_A)}{n} + \sum_N \frac{\#(K_E=\mathcal{K}_B)}{n}\Big]$ where K_E is the key at Eve. K_E was constructed by invoking the step 2 of the proposed method on $\hat{\omega}_{AE} - \hat{\omega}_{BE}$ (the Eve's belief about the shared secret key). One could see that the average DPE decreases from 0.9 to 0.5 as soon as either of the two links observed by the Eve becomes more degraded compared to the link between Alice and Bob.

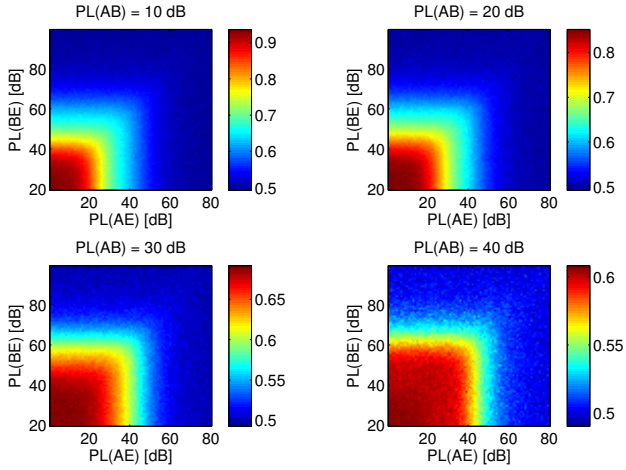

Fig. 6. Decipher probability of Eve for a range of pathloss values experienced by the two links seen by the Eve.

VI. Conclusion

We have proposed to utilize the reciprocal CFO to generate shared secret keys between a legitimate node pair in the presence of a malicious node. Simulation result have shown that the KDR decreases exponentially with increase in the SNR of the link between Alice and Bob. Furthermore, the average DPE decreases as soon as either of the two links observed by the Eve becomes more degraded compared to the link between Alice and Bob. We have also computed the KGR of the CFO process for the two frequency-stability regimes of oscillators.

Some comments about the proposed method are in order. CFO based key generation is appealing because CFO estimation is easily carried out, and already a mandatory operation for the modern cellular/WiFi receivers. Also, the average DPE could approach to zero when the legitimate node pair employs multiple-antenna/beamforming techniques to ensure that minimum power is radiated in unintended directions. Finally, high frequency bands such as milli-meter wave/60 GHz band and terahertz band could benefit from the proposed method because the KGR of the proposed method is proportional to the

center frequency of operation. In short, the proposed method could act as first line of defense against the malicious nodes who are either facing degraded/bad channels, or, don't have the computational resources for sophisticated, real-time signal processing. In near future, we aim to prototype the proposed algorithm on GNU radio/USRP based SDR platform.

APPENDIX A
BLIND CFO ESTIMATION FROM BPSK WAVEFORM

The BPSK baseband waveform at transmitter is: $x(t) = \sum_k a_k p(t-kT)$ where $a_k \in \{1, -1\}$, $p(t)$ is the pulse shape and T is symbol duration. Then, the signal received at the receiver is: $y(t) = x(t)\exp(j2\pi\Delta f t)$. To estimate the CFO Δf, one needs to perform a series of operations on $y(t)$. Specifically,

$$\begin{aligned} y^2(t) &= \{x(t)\exp(j2\pi\Delta f t)\}^2 \\ &= x^2(t)\exp(j4\pi\Delta f t) \\ &= \{\sum_k a_k p(t-kT)\}^2 \exp(j4\pi\Delta f t) \\ &= \{\sum_k p^2(t-kT)\}\exp(j4\pi\Delta f t) \end{aligned}$$

Let $f(t) = \sum_k p^2(t-kT)$. Then one can write:

$$f(t) = \frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n \cos\frac{2n\pi t}{T} + b_n \sin\frac{2n\pi t}{T}) \quad (3)$$

where a_0, a_n and b_n are the Fourier series coefficients given as: $a_0 = \frac{2}{T}\int_0^T f(t)\,dt$, $a_n = \frac{2}{T}\int_0^T f(t)\cos(\frac{2n\pi t}{T})\,dt$, and $b_n = \frac{2}{T}\int_0^T f(t)\sin(\frac{2n\pi t}{T})\,dt$. Then,

$$\begin{aligned} y^2(t) &= f(t)\exp(j4\pi\Delta f t) \\ &= \{\frac{a_0}{2} + \sum_{n=1}^{\infty}(a_n\cos\frac{2n\pi t}{T} + b_n\sin\frac{2n\pi t}{T})\}\exp(j4\pi\Delta f t) \end{aligned}$$

Let $\frac{1}{T} = F_{sym}$, the symbol rate. Let us now write the real and imaginary parts of $y^2(t)$ separately:

$$\begin{aligned} \Re(y^2(t)) = \frac{a_0}{2}\cos(4\pi\Delta f t) \\ + \sum_{n=1}^{\infty}(a_n\cos(2\pi n F_{sym}t)\cos(4\pi\Delta f t) \\ + b_n\sin(2\pi n F_{sym}t)\cos(4\pi\Delta f t)) \end{aligned} \quad (4)$$

$$\begin{aligned} \Im(y^2(t)) = \frac{a_0}{2}\sin(4\pi\Delta f t) \\ + \sum_{n=1}^{\infty}(a_n\cos(2\pi n F_{sym}t)\sin(4\pi\Delta f t) \\ + b_n\sin(2\pi n F_{sym}t)\sin(4\pi\Delta f t)) \end{aligned} \quad (5)$$

Passing the complex-valued signal $y^2(t)$ of Eqs. (4), (5) through a low-pass filter with cut-off frequency ω_c in the range $4\pi\Delta f << \omega_c << 2\pi F_{sym}$, we get:

$$z(t) = \frac{a_0}{2}\exp(j4\pi\Delta f t) \quad (6)$$

Finally, we take the fast Fourier transform (FFT) of $z(t)$, find the frequency $\widehat{2\Delta f}$ corresponding to the peak value, and divide it by 2 which gives us the CFO estimate.

REFERENCES

[1] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.

[2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975. [Online]. Available: http://dx.doi.org/10.1002/j.1538-7305.1975.tb02040.x

[3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *Information Theory, IEEE Transactions on*, vol. 24, no. 3, pp. 339–348, 1978.

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

[5] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," *CoRR*, vol. abs/1011.3754, 2010.

[6] Y.-S. Shiu, S.-Y. Chang, H.-C. Wu, S.-H. Huang, and H.-H. Chen, "Physical layer security in wireless networks: a tutorial," *Wireless Communications, IEEE*, vol. 18, no. 2, pp. 66–74, 2011.

[7] 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, 2008.

[8] M. Bloch, A. Thangaraj, S. McLaughlin, and J. M. Merolla, "Ldpc-based gaussian key reconciliation," in *Information Theory Workshop, 2006. ITW '06 Punta del Este. IEEE*, 2006, pp. 116–120.

[9] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, "Generalized privacy amplification," *Information Theory, IEEE Transactions on*, vol. 41, no. 6, pp. 1915–1923, 1995.

[10] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *Information Forensics and Security, IEEE Transactions on*, vol. 5, no. 2, pp. 240–254, 2010.

[11] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly gaussian random variables," in *Information Theory, 2006 IEEE International Symposium on*, 2006, pp. 2593–2597.

[12] L. Dong, Z. Han, A. Petropulu, and H. Poor, "Improving wireless physical layer security via cooperating relays," *Signal Processing, IEEE Transactions on*, vol. 58, no. 3, pp. 1875–1888, 2010.

[13] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *INFOCOM, 2011 Proceedings IEEE*, 2011, pp. 1125–1133.

[14] D. Lim, J. Lee, B. Gassend, G. Suh, M. van Dijk, and S. Devadas, "Extracting secret keys from integrated circuits," *Very Large Scale Integration (VLSI) Systems, IEEE Transactions on*, vol. 13, no. 10, pp. 1200–1205, 2005.

[15] W. Hou, X. Wang, and J. Chouinard, "Physical layer authentication in ofdm systems based on hypothesis testing of cfo estimates," in *Communications (ICC), 2012 IEEE International Conference on*, 2012, pp. 3559–3563.

[16] M. M. U. Rahman, A. Yasmeen, and J. Gross, "Phy layer authentication via drifting oscillators," in *2014 IEEE Global Communications Conference*, Dec 2014, pp. 716–721.

[17] M. M. U. Rahman, S. Kanwal, and J. Gross, "Simultaneous energy harvesting and sender-node authentication at a receiver node," in *2015 IEEE International Conference on Ubiquitous Wireless Broadband (ICUWB)*, Oct 2015, pp. 1–5.

[18] S. Dwivedi, J. O. Nilsson, P. Papadimitratos, and P. Händel, "Climex: A wireless physical layer security protocol based on clocked impulse exchanges," *arXiv preprint arXiv:1708.04774*, 2017.

[19] H. Imai, K. Kobara, and K. Morozov, "On the possibility of key agreement using variable directional antenna," 2006.

[20] M. M. U. Rahman, A. Yasmeen, and Q. H. Abbasi, "Exploiting lack of hardware reciprocity for sender-node authentication at the phy layer," in *2017 IEEE 85th Vehicular Technology Conference (VTC Spring)*, June 2017, pp. 1–5.

[21] C. Zucca and P. Tavella, "The clock model and its relationship with the allan and related variances," *Ultrasonics, Ferroelectrics and Frequency Control, IEEE Transactions on*, vol. 52, no. 2, pp. 289–296, 2005.

[22] L. Galleani, "A tutorial on the two-state model of the atomic clock noise," *Metrologia*, vol. 45, no. 6, p. S175, 2008.

[23] F. Quitin, M. M. U. Rahman, R. Mudumbai, and U. Madhow, "A scalable architecture for distributed transmit beamforming with commodity radios: Design and proof of concept," *Wireless Communications, IEEE Transactions on*, vol. 12, no. 3, pp. 1418–1428, 2013.