PHY Layer Authentication via Drifting Oscillators

Muhammad Mahboob Ur Rahman*, Aneela Yasmeen† and James Gross*
*Electrical engineering department, KTH (Royal Institute of Technology), Stockholm, Sweden
{mahboob.rahman, james.gross}@ee.kth.se
†u04181@yahoo.com

***Abstract*—PHY layer authentication of a wireless sender has gained much interest recently. In this paper, we consider the famous Alice, Bob and Eve model and investigate (for the first time) the feasibility of using *time-varying clock offsets* for sender-node-authentication at Bob. Specifically, we exploit the fact (and de-facto problem) that clock offset between every node pair is unique; moreover, the two clock offsets between any two node pairs drift independently and randomly over time. Therefore, an explicit mechanism is needed to track the time-varying clock offsets. To this end, we model oscillator drift as brownian motion frequency and phase drift, and present a novel framework which is based on interplay between a hypothesis testing device and a bank of two Kalman filters; one KF (KF_{H_0}) tracks Alice's clock while other KF (KF_{H_1}) tracks Eve's clock. Building on aforementioned framework, we then propose a novel sender-node-authentication method (so-called MHF method) by means of which Bob can automatically accept (reject) a received packet if it is sent by Alice (Eve). Finally, simulation results are presented which corroborate the efficiency of the proposed method.**

I. Introduction

Wireless systems, due to broadcast nature of wireless medium, are prone to attacks by intruders and eavesdroppers. Hence, there is always the need for robust security techniques so as to ensure secure communication between two legitimate parties. Ever since their advent and subsequent widespread, wireless networks have remained largely accustomed to using higher layer cryptographic protocols for authentication/security purposes. However, since the last decade, there has been growing interest in investigating physical (PHY) layer security techniques so as to complement/improve the existing higher layer security mechanisms. See, e.g., [1], [2] for a quick overview of recent development in the field.

Related work. A large body of work on PHY layer security is primarily concerned with various information theoretic models (of potential attacks) and corresponding performance limits (following the pioneer work by [3],[4]). Specifically, two main ingredients of PHY layer security are sender-node-authentication and shared secret key generation. With the recent surge of interest in exploiting PHY layer (medium/hardware) characteristics to implement security, the problem of shared secret key generation has been intensively investigated by researchers. Yet the problem of sender-node-authentication has received little attention so far.

In [5], authors exploit the spatio-temporal-filter property of channel frequency response (CFR) of the frequency-selective but time-invarient channel shared between legitimate node pair to authenticate the received packets at the designated receiver node. Same authors later extend this idea to time-varying channels; due to changes in scattering environment in [6], and due to node mobility in [7]. Authors in [8] investigate this concept further in MIMO/OFDM settings. On the other hand, [9] exploits properties of channel impulse response (CIR) of frequency-selective but time-invarient channels between node pairs to do the authentication. Liu et. al. then extend this idea to time-varying channels in [10], [11]. Finally, [12] takes a different approach where so-called tags are used for authentication purposes (a tag is a function of shared secret key and to-be transmitted message which is then superimposed on the message). [13], [14] extend this idea to MIMO systems.

Other than radio channel, clock offsets which arise due to manufacturing tolerances and environmental conditions of underlying oscillators can also serve as source of common randomness; and therefore, are the subject of this work. To the best of authors' knowledge, to date, there has been no work on this interesting topic except [15]. There, the authors utilize frequency offsets for sender-node-authentication via hypothesis testing under the idealistic assumption that frequency offsets between node pairs remain constant all the time which is not the case in practice.

Contributions. We consider the famous Alice, Bob and Eve model [5] and investigate the feasibility of using *time-varying clock offsets* for sender-node-authentication at Bob. Specifically, we exploit the fact (and de-facto problem) that clock offset between every node pair is unique; moreover, clock offsets between any two node pairs drift independently and randomly over time. To this end, we present a novel framework which is based on interplay between a hypothesis testing device and a bank of two Kalman filters; one KF (KF_{H_0}) tracks Alice's clock while the other KF (KF_{H_1}) tracks Eve's clock. Building on aforementioned framework, we then propose a novel node-authentication method, the so-called measurement-hypothesis-filtering (MHF) method, by means of which Bob can automatically accept (reject) a received packet if it is sent by Alice (Eve). By means of simulations, we demonstrate that the proposed MHF method provides superior performance in terms of detection rate (Bob discarding Eve's packet) P_d. Specifically, we obtain $P_d \leq 3 \times 10^{-4}$ for a wide range of pre-specified false alarm rate values (Bob discarding Alice's packet) P_{fa}, i.e., $10^{-6} \leq P_{fa} \leq 10^{-1}$, which is orders of magnitude better than the previous techniques reported in the literature [5]-[11],[15].

At the same time, this work is a contribution to Kalman filter as detector (KFaD) problem. Kalman filters have been extensively used for multi-object detection and tracking in the fields

of oceanic engineering and image processing. Specifically, researchers in the two fields have considered the KFaD problem under different acronyms such as multiple target tracking (MTT) [16], joint probabilistic data association (JPDA) [17], multi-hypothesis tracking (MHT) algorithms [18], probabilistic multi-hypothesis tracking (PMHT) algorithms [19], and interacting multiple model (IMM). Nevertheless, each of the aforementioned methods assumes that at every given time instant, measurements from multiple targets are available. However, this is not the case in the scenario under consideration in this work where simultaneous transmission by both Alice and Eve results in collision at Bob. Therefore, methods presented in [16]-[19] are not directly applicable to our situation. Another interesting work which we have become aware of very recently is [20] where authors use normalized innovation sequence of Kalman filter to detect faults in power systems.

Outline. The rest of this paper is organized as follows. Section II introduces system model. Section III describes the novel PHY layer authentication framework and the proposed node-authentication method (the MHF method). Section IV provides some simulation results which corroborate the efficiency of the MHF method proposed in section III. Finally, Section V concludes the paper.

II. System model

We consider a one-way authentication system as shown in Fig. 1. Specifically, Alice and Bob are the two legitimate nodes while Eve is an intruder which sends malicious packets to Bob from time to time while trying to impersonate Alice. Therefore, Bob needs a systematic framework to authenticate the sender of every packet it receives. This way, Bob can reject packets from illegal sender Eve. In this paper, we develop one such framework at the PHY layer which provides the springboard for proposed (so-called MHF) method which Bob can utilize for sender-node authentication.

We assume that the one-way authentication channel in Fig. 1 is time-slotted. That is, packets arrive at Bob at discrete-time instants t_m where $t_m - t_{m-1} = T$ is the time-gap between two successively received packets at Bob. Moreover, each received packet is $T_p < T$ seconds long.

Let f_A, f_B and f_E represent the center frequencies of Alice, Bob and Eve respectively. Ideally, $f_A = f_B = f_E = f_c$ (where f_c is the center frequency of common communication channel) but it is never the case due to oscillator manufacturing tolerances. As a quick example, the oscillators used in USRP N200 software-defined radios have an accuracy of ± 2.5 ppm [21]. Then, for $f_c = 2.4$ GHz, this implies each of f_A, f_B and f_E is uniformly distributed in the range $[2.4G - 6K, 2.4G + 6K]$ Hz initially. Moreover, each of the f_A, f_B and f_E drift randomly over time due to oscillator instability due to environmental conditions and aging. Let $\Delta f_{AB}(m) = f_A(m) - f_B(m)$ represent the frequency offset between Alice and Bob at time t_m. Similarly, define $\Delta f_{EB}(m) = f_E(m) - f_B(m)$ as the frequency offset between Eve and Bob at time t_m.

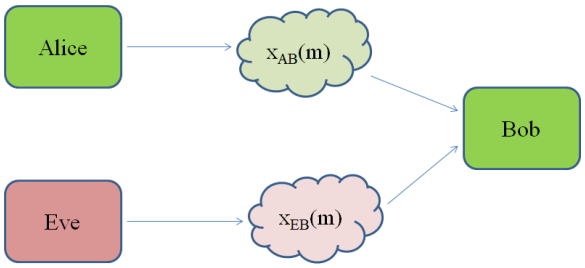

Fig. 1. One-way authentication system model.

More precisely, at time t_m, Bob either observes a random source $\mathbf{x}_{AB}(m)$ due to Alice's transmission; or, Bob observes a random source $\mathbf{x}_{EB}(m)$ due to Eve's attack (see Fig. 1). Each of the two random sources represents clock (phase and frequency) offset between corresponding node pair; moreover, the two random sources are correlated.

III. Proposed PHY layer authentication framework

In this section, we propose a novel PHY layer framework which exploits the random time-varying nature of clock offsets $\mathbf{x}_{AB}(m)$ and $\mathbf{x}_{EB}(m)$ for sender-node authentication. The proposed framework, employed by Bob, consists of a hypothesis testing device followed by a bank of two linear Kalman filters KF_{H_0} and KF_{H_1} which track Alice and Eve's clock respectively. Since every iteration in the proposed method consists of arrival of a new measurement (i.e., packet) followed by hypothesis testing followed by Kalman filtering, we dub the proposed node-authentication method as measurement-hypothesis-filtering (MHF) method in the sequel.

A. Kalman Filter Tracking of Drifting Clock Offsets

Process model for $\mathbf{KF_{H_0}}$. In precision oscillators, frequency and phase offsets drift is commonly modeled as random walk phase noise and random walk frequency noise. Using the famous two-state clock model [22], [23], we can write the time-evolution of the random source $\mathbf{x}_{AB}(m)$ in state-space as:

$$\mathbf{x}_{AB}(m+1) = \mathbf{F}\mathbf{x}_{AB}(m) + \mathbf{n}_{AB}(m) \tag{1}$$

where $\mathbf{x}_{AB}(m) = [\phi_{AB}(m), \omega_{AB}(m)]^T$ is the phase and frequency offset of Bob's oscillator with respect to Alice's oscillator at time t_m. The state transition matrix $\mathbf{F}$ is defined by:

$$\mathbf{F} = \begin{bmatrix} 1 & T \\ 0 & 1 \end{bmatrix}$$

where T is the time between two successively received packets by Bob. $\mathbf{n}_{AB}(m)$ is the process noise vector with $\mathbf{n}_{AB}(m) = [n_{AB,\phi}(m), n_{AB,\omega}(m)]^T$ and $\mathbf{n}_{AB}(m) \sim \mathcal{N}(0, \mathbf{Q}(T_s))$; T_s is the sampling period used by Bob. Basically, $\mathbf{n}_{AB}(m)$ is the phase and frequency noise that causes the phase and frequency offsets to deviate from their nominal values and drift randomly

with time. We adapt the following model for process noise covariance matrix [24]:

$$\mathbf{Q}(T_s) = \omega_c^2 q_1^2 \begin{bmatrix} T_s & 0 \\ 0 & 0 \end{bmatrix} + \omega_c^2 q_2^2 \begin{bmatrix} \frac{T_s^3}{3} & \frac{T_s^2}{2} \\ \frac{T_s^2}{2} & T_s \end{bmatrix} \quad (2)$$

where q_1^2 and q_2^2 are the two model parameters extracted from Allan variance curve of a given oscillator [22], [23]. $q_1^2 = 8.47\times10^{-22}$, $q_2^2 = 5.51\times10^{-18}$ for the oscillators used in USRP N200 software-defined radios [24]; ω_c is the center frequency (in rad/s) of Bob's channel.

Process model for $\mathbf{KF_{H_1}}$. Bob utilizes the following process model to track Eve's clock:

$$\mathbf{x}_{EB}(m+1) = \mathbf{F}\mathbf{x}_{EB}(m) + \mathbf{n}_{EB}(m) \quad (3)$$

where $\mathbf{x}_{EB}(m) = [\phi_{EB}(m), \omega_{EB}(m)]^T$ is the phase and frequency offset of Bob's oscillator with respect to Eve's oscillator at time t_m. $\mathbf{n}_{EB}(m)$ is the process noise vector with $\mathbf{n}_{EB}(m) = [n_{EB,\phi}(m), n_{EB,\omega}(m)]^T$ and $\mathbf{n}_{EB}(m) \sim \mathcal{N}(0, \mathbf{Q}(T_s))$. $\mathbf{n}_{EB}(m)$ represents the phase and frequency noise between Eve and Bob's clocks; $\mathbf{Q}(T_s)$ is the same as in Equation (2).

B. Hypothesis Testing

We formulate the hypothesis testing problem on top of the shared measurement model employed by Bob which is as follows:

$$\begin{cases} H_0: & \mathbf{z}(m) = \mathbf{H}\mathbf{x}_{AB}(m) + \epsilon(m) \\ H_1: & \mathbf{z}(m) = \mathbf{H}\mathbf{x}_{EB}(m) + \epsilon(m) \end{cases} \quad (4)$$

where $\mathbf{H}$ is the measurement matrix. We assume that access to unwrapped phase ($\phi_{AB}(m)$ or $\phi_{EB}(m)$) is available; therefore, we set $\mathbf{H} = \mathbf{I_2}$ in this work. $\mathbf{z}(m)$ is the (noisy) clock offset estimate vector obtained via running the algorithms in [25],[26] on received packet (at time t_m) which in our case is a sinusoidal burst of duration T_p. $\epsilon(m)$ is the estimation error with distribution $\epsilon(m) \sim \mathcal{N}(\mathbf{0}, \mathbf{R})$. Then, $\mathbf{z}(m) \sim \mathcal{N}(\mathbf{x}_{AB}(m), \mathbf{R})$ under H_0 and $\mathbf{z}(m) \sim \mathcal{N}(\mathbf{x}_{EB}(m), \mathbf{R})$ under H_1. If $H_0 = 1$, received packet is accepted by Bob; if $H_1 = 1$, received packet is rejected by Bob.

All in all, by the virtue of Equations (1)-(4) and KF_{H_0} and KF_{H_1}, Bob is able to track the two random sources (i.e., clock offsets $\mathbf{x}_{AB}(m)$ and $\mathbf{x}_{EB}(m)$) simultaneously and independently.

C. Proposed MHF Method

The method consists of two distinct phases, Phase-I and Phase-II. Since the purpose of hypothesis testing is to check whether or not the new measurement $\mathbf{z}(m)$ is consistent with the believed truth $\mathbf{x}_{AB}(m)$, one needs an estimate $\hat{\mathbf{x}}_{AB}(m)$ of the truth. Under linear Gaussian assumptions, KF_{H_0} provides the best estimate/prediction of the truth which is $\hat{\mathbf{x}}_{AB}(m) = \mathbf{x}_{AB}(m|m-1)$. Therefore, during Phase-I, KF_{H_0} is trained by Alice's transmissions on a secure channel. Usually, it only takes few iterations until KF_{H_0} converges. Once KF_{H_0} is converged, proposed MHF method enters Phase-II where Bob can authenticate all the received packets on its own. Below, both Phase-I and Phase-II are described in more detail.

Phase-I. KF_{H_0} is trained by Alice and Bob on a secure channel.

Phase-II. Packets are received by Bob at times t_m; since each packet can be from Alice or Eve, measurement-to-filter association is important. Therefore, the hypothesis testing device does two things in one-shot; first and foremost, it provides device authentication; secondly, it assigns each measurement to appropriate KF, i.e., KF_{H_0} or KF_{H_1}. On the other hand, KF_{H_0} (KF_{H_1}) tracks the time-varying clock offset $\mathbf{x}_{AB}(m)$ ($\mathbf{x}_{EB}(m)$), and thus, provides inputs (p-step-ahead prediction of its respective clock offset, $p \geq 1$) to the hypothesis testing device. Specifically, upon reception of a packet, Bob first obtains the noisy clock offset estimate $\mathbf{z}(m) = [z_\phi(m)\ z_\omega(m)]'$. At the same time, KF_{H_0} provides the p-step-ahead predication vector $\mathbf{x}_{AB}(m|m-p) = [\phi_{AB}(m|m-p)\ \omega_{AB}(m|m-p)]'$. The hypothesis testing device then applies the following test:

$$\|\mathbf{z}(m) - \mathbf{H}\mathbf{x}_{AB}(m|m-p)\|_\omega \underset{H_0}{\overset{H_1}{\gtrless}} \delta(m) \quad (5)$$

In Equation (5), let $\mathbf{y}(m) = \mathbf{z}(m) - \mathbf{H}\mathbf{x}_{AB}(m|m-p)$ with $\mathbf{y}(m) = [y_\phi(m)\ y_\omega(m)]'$. Then, $\|\mathbf{y}(m)\|_\omega$ is the so-called ω-norm defined as $\|\mathbf{y}(m)\|_\omega = |y_\omega(m)| = |z_\omega(m) - \omega_{AB}(m|m-p)|$; $\delta(m)$ is the decision threshold whose value is to be determined. If the above test results in $H_0 = 1$, measurement $\mathbf{z}(m)$ is passed as input to KF_{H_0}; otherwise, if $H_1 = 1$, $\mathbf{z}(m)$ is passed as input to KF_{H_1}. $\mathbf{y}(m)$ is commonly known as innovation sequence in Kalman filtering literature [27]. Specifically, $\mathbf{y}(m) \sim \mathcal{N}(\mathbf{0}, \mathbf{S}_{AB}(m))$ under H_0 and $\mathbf{y}(m) \sim \mathcal{N}(\mathbf{x}_{EB}(m) - \mathbf{x}_{AB}(m|m-p), \mathbf{S}_{AB}(m))$ under H_1. Essentially, Equation (5) is the whiteness test of $\mathbf{y}(m)$, where $E[\mathbf{y}(m)] = 0$ implies H_0 and hence Alice, while $E[\mathbf{y}(m)] \neq 0$ implies H_1 and hence Eve. $\mathbf{S}_{AB}(m)$ is given as:

$$\mathbf{S}_{AB}(m) = \mathbf{H}\mathbf{P}_{AB}(m|m-p)\mathbf{H}' + \mathbf{R} \quad (6)$$

Since $\mathbf{H} = \mathbf{I_2}$, Equation (6) is simplified as: $\mathbf{S}_{AB}(m) = \mathbf{P}_{AB}(m|m-p) + \mathbf{R}$. Similarly, we can simplify Equation (5) as:

$$|z_\omega(m) - \omega_{AB}(m|m-p)| \underset{H_0}{\overset{H_1}{\gtrless}} \delta(m) \quad (7)$$

Since $y_\omega(m) = z_\omega(m) - \omega_{AB}(m|m-p)$, then, $y_\omega(m) \sim \mathcal{N}(\mu_{y_\omega|H_0}(m), \mathbf{S}_{AB,22}(m))$ under H_0; $\mu_{y_\omega|H_0}(m) = 0$. $\mathbf{S}_{AB,22}(m)$ is the (2,2) element of $\mathbf{S}_{AB}(m)$, the covariance matrix of $\mathbf{y}(m)$. Then, the probability of false alarm P_{fa} (i.e., incorrectly identifying Alice's packet as if it is from Eve) is given as:

$$\begin{aligned} P_{fa} &= Pr(|y_\omega(m)| > \delta(m)|H_0) \\ &= 2Q\left(\frac{\delta(m)}{\sqrt{\mathbf{S}_{AB,22}(m)}}\right) \end{aligned} \quad (8)$$

where $Q(.)$ is the standard Q-function: $Q(x) = \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{t^2}{2}}dt$.

By setting P_{fa} to our desired value, $\delta(m)$ can be calculated using Equation (8) which is given as follows:

$$\delta(m) = \sqrt{\mathbf{S}_{AB,22}(m)}Q^{-1}\left(\frac{P_{fa}}{2}\right) \tag{9}$$

The complete MHF-based node-authentication procedure is summarized in Algorithm 1.

D. Performance of Proposed MHF Method

The probability of missed detection P_{md} (success probability of Eve) can be calculated as follows:

$$P_{md} = Pr(|y_\omega(m)| < \delta(m)|H_1) \tag{10}$$

Then, $y_\omega(m) \sim \mathcal{N}(\mu_{y_\omega|H_1}(m), \mathbf{S}_{AB,22}(m))$ under H_1 where $\mu_{y_\omega|H_1}(m) = \omega_{EB}(m) - \omega_{AB}(m|m-p)$. Assuming that unknown frequency offset is uniformly distributed within its ppm range $\omega_{EB}(m) \sim \mathcal{U}(-\Delta, \Delta)$, we have the following:

$$P_{md,tr} = \frac{1}{2\Delta}\int_{-\Delta}^{\Delta}\left[Q\left(\frac{-\delta(m) - \omega_{EB}(m) + \omega_{AB}(m|m-p)}{\sqrt{\mathbf{S}_{AB,22}(m)}}\right) - Q\left(\frac{\delta(m) - \omega_{EB}(m) + \omega_{AB}(m|m-p)}{\sqrt{\mathbf{S}_{AB,22}(m)}}\right)\right]d\omega_{EB}(m) \tag{11}$$

The closed-form solution of Equation (11) cannot be obtained because it involves the integration of Q function as well as $\omega_{AB}(m|m-p)$ which can only be obtained from KF_{H_0} at run-time. In case, KF_{H_1} is converged as well (due to Eve being a weak intruder, and hence, unable to decipher the authentication scheme being used by Bob), we have the following expression for P_{md} in steady-state:

$$P_{md,ss} = Q\left(\frac{-\delta(m) - \omega_{EB}(m|m-q) + \omega_{AB}(m|m-p)}{\sqrt{\mathbf{S}_{AB,22}(m)}}\right) - Q\left(\frac{\delta(m) - \omega_{EB}(m|m-q) + \omega_{AB}(m|m-p)}{\sqrt{\mathbf{S}_{AB,22}(m)}}\right) \tag{12}$$

E. Discussions

At this point, it is worth highlighting the role of KF_{H_1} in the proposed PHY layer authentication framework. Once (and if) converged, it provides two valuable pieces of information. 1) We can calculate the Kullback-Leibler divergence $D(\mathbf{r}\|\mathbf{s})$ between the two prior densities $\mathbf{r} = p(\mathbf{x}_{AB}(m)|\mathbf{z}(1:m-p)) \sim \mathcal{N}(\mathbf{x}_{AB}(m|m-p), \mathbf{P}_{AB}(m|m-p))$ provided by KF_{H_0} and $\mathbf{s} = p(\mathbf{x}_{EB}(m)|\mathbf{z}(1:m-q)) \sim \mathcal{N}(\mathbf{x}_{EB}(m|m-q), \mathbf{P}_{EB}(m|m-q))$ provided by KF_{H_1}. $D(\mathbf{r}\|\mathbf{s})$ when compared to $f(\mathbf{P}_{AB}(m|m-p))$ provides us information about reliability of hypothesis testing mechanism; $f(\mathbf{P}_{AB}(m|m-p))$ is some suitably chosen function of $\mathbf{P}_{AB}(m|m-p)$ which is the covariance of estimate/prediction $\mathbf{x}_{AB}(m|m-p)$ provided by KF_{H_0}. As an example, under the extreme case when $D(\mathbf{r}\|\mathbf{s}) - f(\mathbf{P}_{AB}(m|m-p))$ is so small that it results in 45° straight line on receiver operating characteristic (ROC) plot, hypothesis testing can't be relied upon. 2) By means of $\omega_{EB}(m|m-q)$, a new expression for P_{md} is obtained in (12) which is more precise than the expression in (11).

Algorithm 1 The MHF method.

Phase-I: $\mathbf{KF_{H_0}}$ training
//$H_0 = 1$
Initialize KF_{H_0}
while $\|\mathbf{z}(m) - \mathbf{H}\mathbf{x}_{AB}(m|m-1)\|_\omega > \epsilon$ **do**
  do measurement update using the new measurement $\mathbf{z}(m)$ to get $\mathbf{x_{AB}}(m|m)$
  do time update to get $\mathbf{x_{AB}}(m+1|m)$
end while
//KF_{H_0} is now converged
Phase-II: Sender-node-authentication
while (1) **do**
  KF_{H_0}: do time update to get $\mathbf{x_{AB}}(m|m-p)$
  KF_{H_1}: do time update to get $\mathbf{x_{EB}}(m|m-q)$
  compute threshold $\delta(m)$ from equation (9)
  if $\|\mathbf{z}(m) - \mathbf{H}\mathbf{x}_{AB}(m|m-p)\|_\omega < \delta(m)$ **then**
    $H_0 = 1$ //Accept. Packet came from Alice, the authentic sender
    //$\mathbf{z}(m)$ is associated with KF_{H_0}.
    KF_{H_0}: do measurement update using the new measurement $\mathbf{z}(m)$ to get $\mathbf{x_{AB}}(m|m)$
  else
    $H_1 = 1$ //Reject. Packet came from Eve, the intruder
    //$\mathbf{z}(m)$ is associated with KF_{H_1}.
    KF_{H_1}: do measurement update using the new measurement $\mathbf{z}(m)$ to get $\mathbf{x_{EB}}(m|m)$
  end if
end while

IV. Numerical Results

We assume that for Bob, having received a packet, the probabilities that the packet came from Alice or Eve are equal (i.e., $P(H_0) = P(H_1) = 0.5$). Furthermore, we assume that there are no collisions in the shared time-slotted channel.

For simulation purposes, we have used $f_c = 2.4$ GHz, $T = 50$ ms, $T_p = 5$ ms, $F_s = 20$ KSps. The specific values of T_p and T were guided by the CRLB-based rule of thumb in [24] so as to make sure that the two KF's (KF_{H0} and KF_{H1}) remain converged throughout the authentication operation. Moreover, assuming that the (noisy) frequency and phase estimates meet CRLB, we have the following covariance matrix for measurement noise [25],[26]:

$$\mathbf{R} = \begin{bmatrix} \frac{2}{\gamma} & 0 \\ 0 & \frac{6}{T_p^2\gamma} \end{bmatrix}$$

where γ represents the SNR at Bob.

Fig. 2 plots together the L.H.S. $\|\mathbf{z}(m) - \mathbf{H}\mathbf{x}_{AB}(m|m-p)\|_\omega$ and R.H.S. $\delta(m)$ of Equation (5) against time (received packet number) at Bob. Essentially, Fig. 2 demonstrates the real-time working of hypothesis testing device employed by Bob. We can easily and visually identify the packets sent by Eve which result in spikes (much larger than decision threshold $\delta(m)$) in the ω-norm of $\mathbf{y}(m)$. For this plot, frequency offset $\omega_{AB}(m)$ was initialized to 1000 Hz while frequency offset $\omega_{EB}(m)$

was initialized to 1050 Hz; moreover, a target P_{fa} = 0.1 was used to derive the threshold $\delta(m)$ and γ was set to 20 dB.

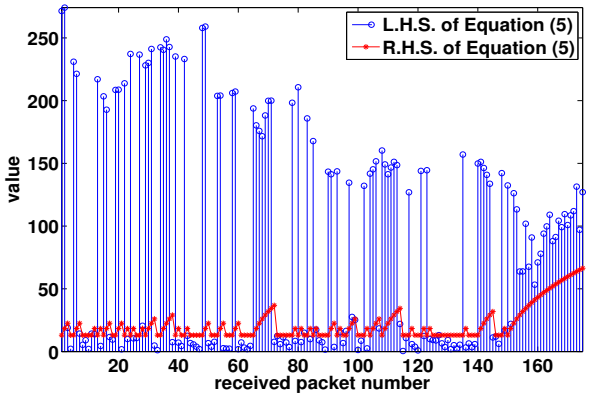

Fig. 2. Hypothesis testing device in action.

Fig. 3 is a plot between probability of false alarm P_{fa} vs. γ for two different P_{fa} values, i.e., $P_{fa} \epsilon \{0.1, 0.01\}$. Since we keep $T_p^2\gamma$ =constant, the detector proposed in Section III is a constant false alarm rate (CFAR) detector; therefore, we expect to see P_{fa} to be invariant to γ. This is indeed the case for P_{fa} = 0.1 as can be seen in Fig. 3. However, for P_{fa} = 0.01, the numerically obtained values $P_{fa,n}$ oscillate more about the target $P_{fa,t}$ that is set during calculation of the decision threshold $\delta(m)$. We believe this discrepency is due to less amount of averaging in Monte Carlo simulations.

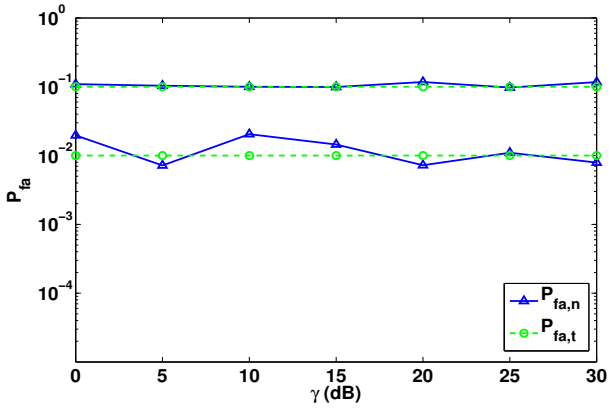

Fig. 3. Probability of false alarm vs. γ.

Let us define $\Delta f_0 = |f_{AB}(0) - f_{EB}(0)|$. That is, Δf_0 is the separation between the two frequency offsets $\omega_{AB}(m)$ and $\omega_{EB}(m)$ at time t_m = 0. Then, Fig. 4 shows a plot between $P_{fa,n}$ and Δf_0 for three different values of γ at Bob. From Fig. 4, we learn that the lower bound $\Delta f_{0,lb}$ on Δf_0 for which target $P_{fa,t}$ is respectably met is around 150 Hz. Actually, this lower bound $\Delta f_{0,lb}$ is inversely proportional to $P(H_0)$ which means better resolution (a.k.a detection performance) can be achieved in situations when Eve attacks Bob less frequently than Alice talks to Bob (and vice versa).

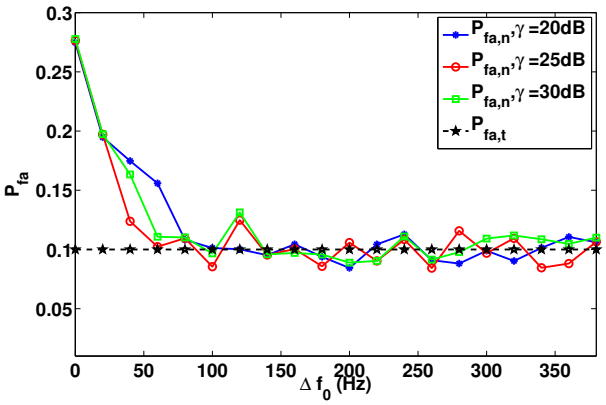

Fig. 4. Probability of false alarm vs. Δf_0.

Fig. 5 shows a plot between $P_{md,n}$ and Δf_0 for three different values of γ at Bob. From Fig. 5, we learn that the lower bound $\Delta f_{0,lb}$ on Δf_0 for which target $P_{md,t}$ is respectably met is again around 150 Hz. Specifically, for $P_{fa,t}$ = 0.1, corresponding $P_{md,t}$ is 10^{-4} (which is not visible in Fig. 5 though).

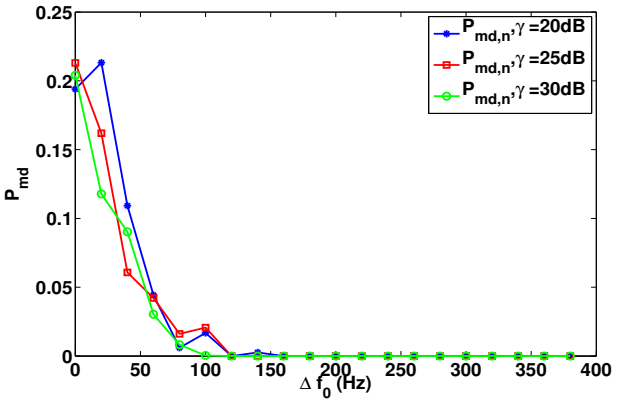

Fig. 5. Probability of missed detection vs. Δf_0.

A. Comparison with Other Authentication Schemes

Fig. 6 shows an ROC plot between P_d (probability of detection) and P_{fa} for three different values of γ at Bob. Note that P_d = 1 – P_{md}. Fig. 6 clearly demonstrates that $P_{md} \leq 3 \times 10^{-4}$ over the full practical range-of-interest of pre-specified P_{fa} values, i.e., $10^{-6} \leq P_{fa} \leq 10^{-1}$; which is (at least) an order of magnitude better than the previous techniques reported in the literature [5]-[11],[15]. Moreover, the proposed MHF method requires only one-time training in the beginning to obtain the ground truth, while other channel-based authentication schemes in [5]-[11] require training once every channel coherence interval which might be too much overhead in case of time-varying channels. Finally, frequency offset estimation is already a mandatory operation in modern receivers while channel impulse response estimation and

channel frequency response estimation are not. Therefore, schemes in [5]-[11] need additional (hardware/radio spectrum) resources for their implementation which will substantially increase the complexity and cost of the underlying system.

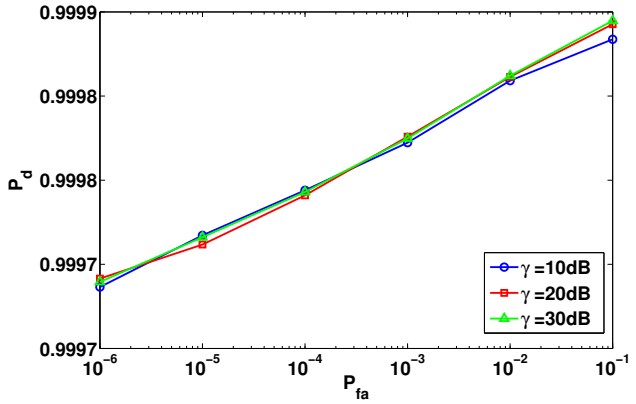

Fig. 6. Probability of detection vs. probability of false alarm.

V. Conclusion

In this paper, we investigated the feasibility of using *time-varying clock offsets* for sender-node-authentication at Bob. Specifically, we exploited the fact that clock offset between every node pair is unique; moreover, clock offsets between any two node pairs drift independently and randomly over time. To this end, we presented a novel PHY layer authentication framework which is based on interplay between a hypothesis testing device and a bank of two Kalman filters; one KF (KF_{H_0}) tracks Alice's clock while other KF (KF_{H_1}) tracks Eve's clock. Building on aforementioned framework, we then provided a novel sender-node-authentication method (so-called MHF method) by means of which Bob can automatically accept (reject) a received packet if it is sent by Alice (Eve). An immediate follow-up work will be to analyze the network-layer performance (i.e., stochastic delay bounds etc.) for the one-way authentication channel introduced in Fig. 1.

Acknowledgements

Mahboob acknowledges fruitful discussions with Prof. Raghu Mudumbai, Prof. Soura Dasgupta, Prof. Upamanyu Madhow and Dr. Francois Quitin.

References

[1] 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.

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

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

[4] 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

[5] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Fingerprints in the ether: Using the physical layer for wireless authentication," in *Proc. of IEEE International Conference on Communications (ICC)*, June 2007, pp. 4646–4651.

[6] L. Xiao, L. Greenstein, N. B. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, July 2008.

[7] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "A physical-layer technique to enhance authentication for mobile terminals," in *Proc. of IEEE International Conference on Communications, (ICC)*, May 2008, pp. 1520–1524.

[8] P. Baracca, N. Laurenti, and S. Tomasin, "Physical layer authentication over mimo fading wiretap channels," *IEEE Transactions on Wireless Communications*, vol. 11, no. 7, pp. 2564–2573, July 2012.

[9] J. Tugnait and H. Kim, "A channel-based hypothesis testing approach to enhance user authentication in wireless networks," in *Proc. of Second International Conference on Communication Systems and Networks (COMSNETS)*, Jan 2010, pp. 1–9.

[10] F. Liu, X. Wang, and H. Tang, "Robust physical layer authentication using inherent properties of channel impulse response," in *Proc. of IEEE MILITARY COMMUNICATIONS CONFERENCE, (MILCOM)*, Nov 2011, pp. 538–542.

[11] F. Liu, X. Wang, and S. Primak, "A two dimensional quantization algorithm for cir-based physical layer authentication," in *Proc. of IEEE International Conference on Communications (ICC)*, June 2013, pp. 4724–4728.

[12] P. Yu, J. Baras, and B. Sadler, "Physical-layer authentication," *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 1, pp. 38–51, March 2008.

[13] N. Goergen, W. Lin, K. Liu, and T. Clancy, "Extrinsic channel-like fingerprint embedding for authenticating mimo systems," *IEEE Transactions on Wireless Communications*, vol. 10, no. 12, pp. 4270–4281, December 2011.

[14] P. Yu and B. Sadler, "Mimo authentication via deliberate fingerprinting at the physical layer," *IEEE Transactions on Information Forensics and Security*, vol. 6, no. 3, pp. 606–615, Sept 2011.

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

[16] D. Reid, "An algorithm for tracking multiple targets," *IEEE Transactions on Automatic Control*, vol. 24, no. 6, pp. 843–854, Dec 1979.

[17] T. E. Fortmann, Y. Bar-Shalom, and M. Scheffe, "Sonar tracking of multiple targets using joint probabilistic data association," *IEEE Journal of Oceanic Engineering*, vol. 8, no. 3, pp. 173–184, Jul 1983.

[18] S. Blackman, "Multiple hypothesis tracking for multiple target tracking," *IEEE Aerospace and Electronic Systems Magazine*, vol. 19, no. 1, pp. 5–18, Jan 2004.

[19] R. L. Streit and T. E. Luginbuhl, "Probabilistic multi-hypothesis tracking," DTIC Document, Tech. Rep., 1995.

[20] F. Chowdhury, J. Christensen, and J. Aravena, "Power system fault detection and state estimation using kalman filter with hypothesis testing," *IEEE Transactions on Power Delivery*, vol. 6, no. 3, pp. 1025–1030, Jul 1991.

[21] USRP products, http://www.ettus.com, 2014.

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

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

[24] 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," *IEEE Transactions on Wireless Communications*, vol. 12, no. 3, pp. 1418–1428, 2013.

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

[26] S. Kay, "A fast and accurate single frequency estimator," *IEEE Transactions on Acoustics, Speech and Signal Processing*, vol. 37, no. 12, pp. 1987–1990, Dec 1989.

[27] B. Anderson and J. Moore, *Optimal Filtering*. Englewood Cliffs, New Jersey: Prentice-Hall, 1979.