Simultaneous Energy Harvesting and Sender-Node Authentication At a Receiver Node

Muhammad Mahboob Ur Rahman*, Sanobia Kanwal†, James Gross*
*School of Electrical engineering, KTH Royal Institute of Technology, Stockholm, Sweden
{mahboob.rahman,james.gross}@ee.kth.se
†Computer engineering department, BZ University, Multan, Pakistan
sanobiakanwal@gmail.com

***Abstract*—We consider a system with three single-antenna nodes; Alice talks to Bob over a time-slotted AWGN channel, while Eve's objective is to impersonate Alice. We then consider a setting where, for every received packet, Bob needs to do simultaneous energy harvesting (EH) and sender-node authentication. To this end, Bob employs *frequency offset* as the decision metric for binary hypothesis testing based authentication framework. Then, assuming separate receive chains for energy harvesting and information decoding, Bob implements two *deterministic* energy harvesting schemes: i) time-switching (TS) based, ii) static power-splitting (SPS) based. For both EH schemes, we analyze the trade-off between detection performance of the authentication scheme and amount of energy harvested. Numerical results suggest that for the same detection performance, SPS scheme outperforms TS scheme in terms of amount of energy harvested. We also consider a *random* energy harvesting scheme, the so-called opportunistic EH scheme, whereby Bob utilizes Eve's packets (as labeled by authentication scheme) to harvest energy. There, it is straightforward to see that the normalized mean throughput of EH receive chain increases linearly with an increase in Eve's attack rate.**

I. Introduction

The last decade has witnessed the unprecedented growth of wireless communication technology and its omniwhere adaptation within the society. This gigantic progress, as expected, has culminated in a new set of research challenges never addressed before, within the wireless research community. Among them, physical-layer security and energy harvesting are two novel avenues which did not get any significant attention by the researchers until very recently.

The need for physical-layer security arises mainly due to the broadcast nature of the wireless medium. Therefore, mechanisms (at the physical-layer) which could ensure secure communication between a legitimate node pair (Alice and Bob) in the presence of an active/passive malicious node (Eve) are needed. Sender-node authentication is one such mechanism whereby the receiver node (Bob) authenticates each and every packet it receives from the channel (Alice or Eve). Traditionally, sender-node authentication in wireless systems has been implemented via higher-layer cryptographic protocols; however, there is an increasing interest to complement/improve it via physical-layer mechanisms [1], [2]. To this end, reseachers have considered different physical-layer attributes such as wireless channel [3],[4],[5],[6], frequency offsets [7],[8], angle-of-arrival [9], received signal strength etc. to use them as device/node fingerprint.

Energy harvesting (EH), on the other hand, collectively represents a broad set of techniques which scavenge energy from ambient sources (sun-light, RF signals etc.) with the aim of prolonging the battery life-time of sensor-type wireless devices [10]. Nevertheless, for the sake of clarity, energy harvesting in this work primarily refers to the mechanisms of scavenging energy from the received in-band RF signals (data packets) at a receiver node (Bob). This concept is commonly known as simultaneous wireless information and power transfer (SWIPT) in the literature [11]. Then, two kinds of energy harvesting receiver architectures are proposed in the literature: i) receiver with separate energy receiver (ER) chain and information receiver (IR) chain, ii) receiver with ER and IR integrated into one RF receive chain [11],[12].

In this work, we assume that Bob has separate ER and IR chains. We then implement two deterministic energy harvesting schemes (first proposed in [12]) at Bob: i) time-switching (TS) based, ii) static power-splitting (SPS) based. For both EH schemes, we analyze the trade-off between detection performance of the (frequency offset based) authentication scheme and amount of energy harvested. We then consider a random energy harvesting scheme, the so-called opportunistic EH scheme, whereby the packets labeled as from Eve (by the authentication scheme) are sent to ER chain of Bob for opportunistic energy harvesting. There, we examine the normalized throughput of ER chain as a function of Eve's attack rate.

Outline. The rest of this paper is organized as follows. Section-II introduces the system model. We describe a frequency offset based sender-node authentication framework in section-III. Then, in section-IV, we discuss the three energy harvesting mechanisms implemented by Bob. Section V provides numerical results followed by some discussions. Finally, Section VI concludes the paper.

II. System Model

In this work, we have a system with three single-antenna nodes; Alice transmits to Bob over a time-slotted AWGN channel, while Eve is an intruder whose objective is to impersonate Alice (see Fig. 1). As an example, in 802.11 deployment, Alice could be thought of an AP, Bob is then STA, while Eve is an illegal AP. Then, traditionally, the goal of Bob has been to do sender-node authentication (either channel

based [3], or, frequency offset based [8]) for every packet it receives. In this work, we extend the previous works where, for every received packet, Bob employs an energy harvesting framework, in addition to (and not significantly degrading the performance of) sender-node authentication framework.

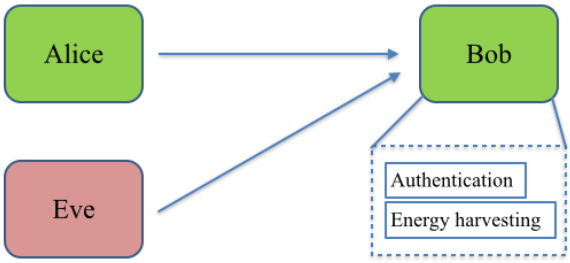

Fig. 1. Simultaneous energy harvesting and authentication by Bob.

III. Background: Frequency Offset based Sender-Node Authentication Framework

In this section, we describe a simple yet effective, sender-node authentication framework based on frequency offset metric. This section closely follows (and is inspired by) the works in [7] and [8]; nevertheless, the considered system model (of Fig. 1) is distinct from both [7] and [8]. Specifically, [7] deals with fixed frequency offsets in a wideband (OFDM) system setting, while [8] considers time-varying frequency offsets in a narrow-band system setting. On the other hand, this work considers a narrow-band system setting where: i) transmit nodes (Alice/Eve) send out unmodulated sinusoids, ii) frequency offsets are time-invarient. As will become clear later, the main motivation to consider such simplistic and fundamental system model is the clarity of exposition since the focus of this work is rather on analyzing the impact of energy harvesting mechanism, when super-imposed on the authentication mechanism.

A. The Hypothesis Testing based Authentication Framework

During m^{th} timeslot (T seconds long), either Alice, or, Eve will have dedicated access to the channel (assuming no collisions). Therefore, it will transmit a packet (which in our case is a sinusoidal burst of duration $T_p < T$) to Bob. Having received the packet, Bob runs the one-shot frequency offset estimation algorithms in [13],[14] to generate a measurement $z(m)$. Bob then casts the sender-node authentication problem as a binary hypothesis testing problem:

$$\begin{cases} H_0: & z(m) = \omega_{AB} + \epsilon(m) \\ H_1: & z(m) = \omega_{EB} + \epsilon(m) \end{cases} \tag{1}$$

where $\epsilon(m)$ is the estimation error, and ω_{AB} (ω_{EB}) is the frequency offset between Alice (Eve) and Bob (in rad/sec). Assuming that the considered frequency offset estimate meets the Cramer-Rao lower bound, $\epsilon(m)$ has the distribution $\epsilon(m) \sim \mathcal{N}(0, \sigma^2(m))$ where $\sigma^2(m) = \frac{6}{T_p^2 \gamma(m)}$. $\gamma(m) = \frac{A^2(m)T_p}{2N_0}$ is the link SNR where $A(m) = A$ is the signal amplitude and N_0 is the power spectral density of the receiver noise. Then, $z \sim \mathcal{N}(\omega_{AB}, \sigma^2)$ under H_0 and $z \sim \mathcal{N}(\omega_{EB}, \sigma^2)$ under H_1. If $H_0 = 1$, received packet is accepted by Bob; if $H_1 = 1$, received packet is rejected by Bob.

Next, assuming that: i) ω_{AB} is known with sufficient accuracy (via prior training in the beginning, on a secure channel), ii) both priors are equal (i.e., $P(H_0) = P(H_1)$), Bob applies the following test:

$$|z - \omega_{AB}| \underset{H_0}{\overset{H_1}{\gtrless}} \delta \tag{2}$$

where δ is the comparison threshold whose value is to be determined. Let $y = z - \omega_{AB}$. Then, $y \sim \mathcal{N}(0, \sigma^2)$ under H_0 and $y \sim \mathcal{N}(\omega_{EB} - \omega_{AB}, \sigma^2)$ under H_1. Then, the probability of false alarm P_{fa} (i.e., incorrectly identifying Alice's packet as if it is from Eve) is given as:

$$\begin{aligned} P_{fa} &= Pr(|y| > \delta | H_0) \\ &= 2Q\left(\frac{\delta}{\sigma}\right) \end{aligned} \tag{3}$$

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, δ can be calculated using Equation (3):

$$\delta = \sigma Q^{-1}\left(\frac{P_{fa}}{2}\right) \tag{4}$$

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

$$P_{md} = Pr(|y| < \delta | H_1) \tag{5}$$

Assuming that unknown frequency offset is uniformly distributed within its ppm range $\omega_{EB} \sim \mathcal{U}(-\Delta, \Delta)$, we have the following expression:

$$\begin{aligned} P_{md} = \frac{1}{2\Delta} \int_{-\Delta}^{\Delta} \Bigg[& Q\left(\frac{-\delta - \omega_{EB} + \omega_{AB}}{\sigma}\right) \\ & - Q\left(\frac{\delta - \omega_{EB} + \omega_{AB}}{\sigma}\right)\Bigg] d\omega_{EB} \end{aligned} \tag{6}$$

A closed-form solution of Equation (6) cannot be obtained because it involves the integration of the Q-function.

IV. Energy Harvesting Schemes Investigated

In this section, we discuss the specifics of each of the three EH schemes which could be employed by Bob.

A. Time Switching (TS) based Energy Harvesting

In this scheme, for every received packet, Bob utilizes initial part (of pre-determined length αT_p) for energy harvesting by ER, while the rest of the packet (of length $(1-\alpha)T_p$) is used for information decoding (hypothesis testing) by IR (see Fig. 2). In other words, $T_p = T_{p,IR} + T_{p,ER} = (1-\alpha)T_p + \alpha T_p$ where $0 < \alpha < 1$. Therefore, the total energy harvested by the TS scheme is: $E_h = \eta A^2 \alpha T_p$ (Joules) where $0 < \eta < 1$ is the energy conversion efficiency of ER [12].

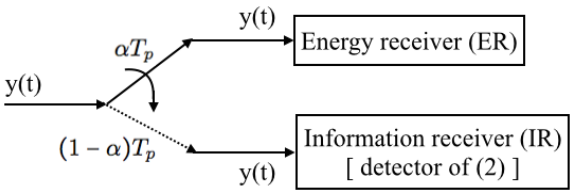

Fig. 2. Time switching scheme (at Bob).

We are then interested in studying the trade-off between probability of detection P_d and amount of energy harvested E_h, per packet received. Since E_h has a linear relationship with α, $(P_d\text{-}E_h)$ trade-off is equivalent to $(P_d\text{-}\alpha)$ trade-off. Then, to analyze the $(P_d\text{-}\alpha)$ trade-off, we first write down the probability of missed detection P_{md} as a function of α (see Equation (7) at the top of reverse side of the page). Then, $P_d(\alpha) = 1 - P_{md}(\alpha)$.

B. Static Power Splitting (SPS) based Energy Harvesting

In this scheme, for every received packet, Bob splits the received RF power/SNR (by means of an RF power splitter with adjustable splitting ratio ρ) between ER and IR receivers (see Fig. 3). Then, $\gamma = \gamma_{IR} + \gamma_{ER} = (1-\rho)\gamma + \rho\gamma$ where $0 < \rho < 1$. Therefore, the total energy harvested by the SPS scheme is: $E_h = \eta\rho A^2 T_p$ (Joules).

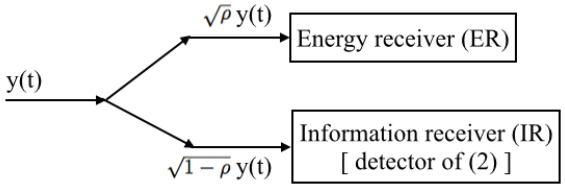

Fig. 3. Static power splitting scheme (at Bob).

Again, we are interested in studying the $(P_d\text{-}E_h)$ trade-off, for every packet received. Again, E_h has a linear relationship with ρ; therefore, $(P_d\text{-}E_h)$ trade-off is equivalent to $(P_d\text{-}\rho)$ trade-off. Then, to analyze the $(P_d\text{-}\rho)$ trade-off, we first write down the probability of missed detection P_{md} as a function of ρ (see Equation (8) at the top of reverse side of the page). Then, $P_d(\rho) = 1 - P_{md}(\rho)$.

C. Opportunistic Energy Harvesting

Succinctly speaking, the main idea behind opportunistic energy harvesting is to feed the rest of the (current) packet to ER whenever H_1 is true. Let us illustrate this idea further by means of 802.11 standard example. In this case, Bob first utilizes the well-known Cox and Schmid algorithm for coarse frequency offset estimation using short preamble. Then, hypothesis testing is carried out. Traditionally, P_d (plus P_{fa}) times the incoming packet is declared to be from Eve; and therefore, is discarded by IR. But now, after H_1 is true, it is noted that only (short) preamble of the 802.11 packet is gone. Hence, rest of the (current) packet is taken to ER for energy harvesting. On the other hand, when the sender is detected as Alice, this option is not available; hence called opportunistic EH scheme. Collisions between Alice and Eve also help; i.e., Bob exploits this opportunity to harvest energy (not considered in this work though).

By definition, hypothesis testing for sender-node authentication will result in throughput loss at Bob (compared to the case when Eve is absent). However, Opportunistic EH transforms the throughput loss at information receiver into an equivalent/proportional throughput gain at energy receiver. Let $R_P = 1/T$ be the number of transmission slots per second of the shared channel, and let $\beta = P(H_1)$ be the Eve's attack rate. Then, the normalized mean throughput for ER branch of Bob is[1]:

$$\begin{aligned} T_{ER} &= \frac{P_d\mathbb{E}[R_{P,E}] + P_{fa}\mathbb{E}[R_{P,A}]}{R_P} \\ &= \frac{P_d(\beta)R_P + P_{fa}(1-\beta)R_P}{R_P} \\ &= P_d\beta + P_{fa}(1-\beta) \end{aligned} \tag{9}$$

where $\mathbb{E}[R_{P,A}]$ ($\mathbb{E}[R_{P,E}]$) is the mean transmission rate of Alice (Eve).

Similarly, the (raw) normalized mean throughput for IR branch of Bob is:

$$\begin{aligned} T_{IR} &= \frac{(1-P_d)\mathbb{E}[R_{P,E}] + (1-P_{fa})\mathbb{E}[R_{P,A}]}{R_P} \\ &= \frac{(1-P_d)(\beta)R_P + (1-P_{fa})(1-\beta)R_P}{R_P} \\ &= (1-P_d)\beta + (1-P_{fa})(1-\beta) \end{aligned} \tag{10}$$

However, actual (effective) normalized throughput of IR branch is:

$$\begin{aligned} T_{IR,act} &= \frac{(1-P_{fa})(1-\beta)R_P}{R_P} \\ &= (1-P_{fa})(1-\beta) \le T_{IR} \end{aligned} \tag{11}$$

Note that $T_{ER} + T_{IR} = 1$. This implies that each of the incoming packet is now utilized by Bob; either through its IR branch, or, through its ER branch.

V. Numerical Results and Discussions

A. Numerical Results

As a quick reference, the oscillators used in USRP N200 software-defined radios have an accuracy of ±2.5 ppm [15]. Then, for carrier frequency $f_c = 2.4$ GHz, this implies each of ω_{AB} and ω_{EB} is uniformly distributed in the range $2\pi \times [2.4G - 6K, 2.4G + 6K]$ rad/sec. Moreover, we set $T_p = 5$ ms, $T = 50$ ms, $\gamma = 5$ dB. Finally, throughout this section, we assume that for every packet received at Bob, $P(H_0) = P(H_1) = 0.5$, (except Fig. 8 where $P(H_1) = \beta$ is variable).

[1]The mapping of T_{ER} to physical energy harvested (in Joules) is provided in Table I (on last page).

$$P_{md}(\alpha, P_{fa}) = \frac{1}{2\Delta}\int_{-\Delta}^{\Delta}\left[Q\left(\frac{-\sqrt{\frac{6}{(1-\alpha)^2T_p^2\gamma}}Q^{-1}(\frac{P_{fa}}{2}) - \omega_{EB} + \omega_{AB}}{\sqrt{\frac{6}{(1-\alpha)^2T_p^2\gamma}}}\right) - Q\left(\frac{\sqrt{\frac{6}{(1-\alpha)^2T_p^2\gamma}}Q^{-1}(\frac{P_{fa}}{2}) - \omega_{EB} + \omega_{AB}}{\sqrt{\frac{6}{(1-\alpha)^2T_p^2\gamma}}}\right)\right]d\omega_{EB} \tag{7}$$

$$P_{md}(\rho, P_{fa}) = \frac{1}{2\Delta}\int_{-\Delta}^{\Delta}\left[Q\left(\frac{-\sqrt{\frac{6}{(1-\rho)\gamma T_p^2}}Q^{-1}(\frac{P_{fa}}{2}) - \omega_{EB} + \omega_{AB}}{\sqrt{\frac{6}{(1-\rho)\gamma T_p^2}}}\right) - Q\left(\frac{\sqrt{\frac{6}{(1-\rho)\gamma T_p^2}}Q^{-1}(\frac{P_{fa}}{2}) - \omega_{EB} + \omega_{AB}}{\sqrt{\frac{6}{(1-\rho)\gamma T_p^2}}}\right)\right]d\omega_{EB} \tag{8}$$

Fig. 4 (Fig. 5) plots P_d against α (ρ), while Fig. 6 (Fig. 7) plots ROC curve in the presence of TS (SPS) based EH scheme. From Figs. (4)-(7), we learn that SPS is more suited EH scheme (compared to the TS scheme) for the considered system. This can be explained as follows. As is mentioned before, $\epsilon(m)$ is the estimation error with distribution $\epsilon(m) \sim \mathcal{N}(0, \sigma^2(m))$ where $\sigma^2(m) = \frac{6}{T_p^2\gamma(m)}$. Clearly, from the σ^2 expression, one can verify that for same increase in α (ρ) (or equivalently, for same decrease in T_p (γ)), increase in σ^2 is quadratic (linear) for the case of α (ρ).

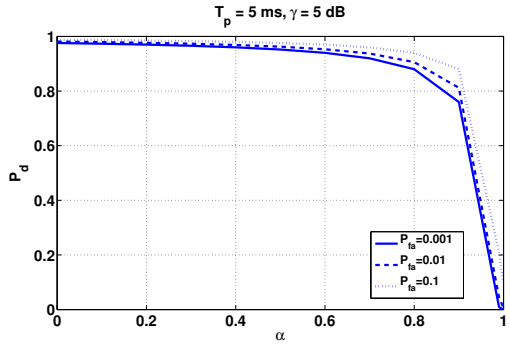

Fig. 4. Impact of TS based EH scheme on detetcion performance.

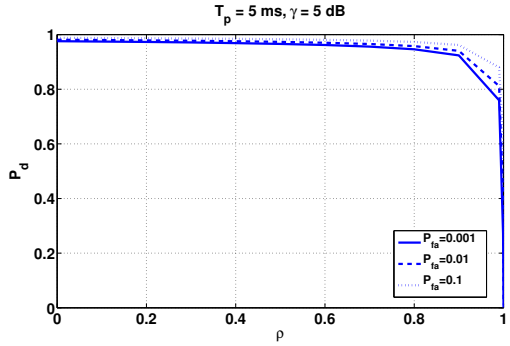

Fig. 5. Impact of SPS based EH scheme on detetcion performance.

Fig. 8 plots the normalized throughputs of ER and IR receivers, from Equation (9) and Equation (11) respectively, against Eve's attack rate β. To compute T_{ER}, first P_{md} was computed numerically from Equation (6). Then, $P_d = 1 - P_{md}$ was plugged into Equation (9).

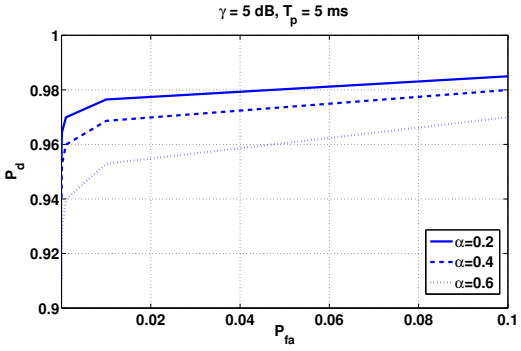

Fig. 6. ROC plot with TS based EH scheme.

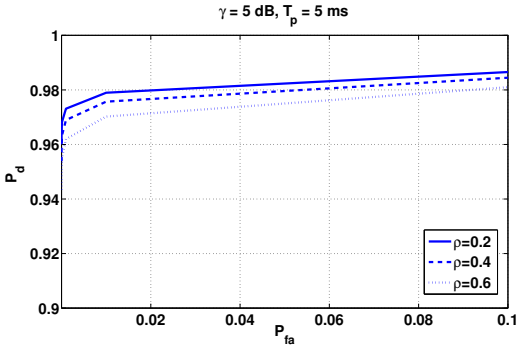

Fig. 7. ROC plot with SPS based EH scheme.

B. Discussions

- The TS based EH scheme implies that we are effectively reducing the sample size used to compute the estimate $z(m)$ in Equation (1). On the other hand, the SPS based EH scheme implies that we are effectively reducing the link SNR. Therefore, this suggests the need for *robust detector* design whereby the designed test meets the detection specifications in the face of increasingly small sample sizes and poor SNR conditions.
- In case ω_{EB} is also known to Bob, the integral is omitted from both Equations (7), (8); therefore, a closed-form

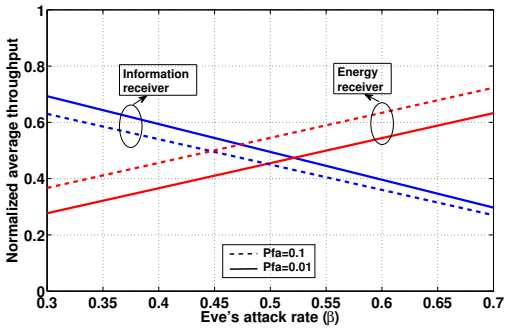

Fig. 8. Opportunistic EH scheme: impact of β on $T_{IR,act}$ and T_{ER}.

TABLE I
ENERGY HARVESTED (PER TIME-SLOT) BY THE THREE EH SCHEMES

EH scheme	Energy harvested (Joules)
TS	$\eta A^2 \alpha T$
SPS	$\eta A^2 \rho T$
Opportunistic	$\eta A^2 [P_d \beta + P_{fa}(1-\beta)]T$

expression for P_{md} as a function of energy harvesting ratio α, ρ is obtained. ω_{EB} could be known to/estimated by Bob in case Eve is a weak intruder which remains oblivious of authentication scheme being used by Bob. Alternatively, ω_{EB} could be known to Bob when the problem at hand is a sender-node classification problem instead of sender-node authentication problem.

- When TS and SPS schemes are implemented for full packet length T (instead of only preamble length T_p), then one can directly do the the performance comparison (i.e., energy harvested per time-slot) of the three EH schemes (see Table I). Basically, the energies harvested by the TS scheme and the SPS scheme are equal (for $\alpha = \rho$). Moreover, the energy harvested by opportunistic scheme could be lesser/greater than the energy harvested by TS and SPS schemes, depending upon the Eve's attack rate $\beta = P(H_1)$.
- The test in Equation (2) assumes equal priors. When this is not the case, i.e., when $P(H_0) \gg P(H_1)$ or vice versa, then the test will perform poorly. This calls for the design of another test which explicitly incorporates prior probability β for threshold δ computation. Then, P_{md} in Equations (6)-(8) and P_d in Equations (9)-(11) will also be dependent on prior probability β.

VI. CONCLUSION

In this preliminary work, we considered a system with three nodes; Alice talks to Bob, while Eve tries to impersonate Alice. We then considered a setting where for every received packet, Bob needs to do simultaneous energy harvesting (EH) and sender-node authentication. To this end, Bob implemented two deterministic EH schemes: i) time-switching (TS) based, ii) static power-splitting (SPS) based. For both EH schemes, we analyzed the trade-off between detection performance of the authentication scheme and amount of energy harvested. Numerical results suggested that for the same detection performance, SPS scheme outperforms TS scheme in terms of amount of energy harvested. We then considered a random EH scheme, the so-called opportunistic EH scheme, which harvests energy from (supposedly) Eve's packets. There, we observed a linear increase in the normalized mean throughput of ER chain with an increase in Eve's attack rate.

We foresee several different directions this work can grow into; some of which are the following: queuing-theoretic analysis of the considered system; extention to the scenario of multi-antenna, multi-user systems (with multiple Alice and multiple Eve nodes); tackling the time-varying frequency offsets (using Kalman-like filtering mechanisms); finding optimal values for energy harvesting parameters (α, ρ) given constraints on detection performance as well as battery power of Bob node.

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] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

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

[9] J. Xiong and K. Jamieson, "Secureangle: Improving wireless security using angle-of-arrival information," in *Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks*, ser. Hotnets-IX. New York, NY, USA: ACM, 2010, pp. 11:1–11:6. [Online]. Available: http://doi.acm.org/10.1145/1868447.1868458

[10] S. Priya and D. J. Inman, *Energy harvesting technologies*. Springer, 2009, vol. 21.

[11] I. Krikidis, S. Timotheou, S. Nikolaou, G. Zheng, D. W. K. Ng, and R. Schober, "Simultaneous wireless information and power transfer in modern communication systems," *Communications Magazine, IEEE*, vol. 52, no. 11, pp. 104–110, 2014.

[12] X. Zhou, R. Zhang, and C. K. Ho, "Wireless information and power transfer: Architecture design and rate-energy tradeoff," in *Global Communications Conference (GLOBECOM), 2012 IEEE*, Dec 2012, pp. 3982–3987.

[13] 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.

[14] 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.

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