User's Deception Mechanisms against Jammers in Wireless Energy Harvesting Networks

Dusit Niyato[1], Ping Wang[1], Dong In Kim[2], Zhu Han[3], and Joseph Chee Ming Teo[4]
[1] School of Computer Engineering, Nanyang Technological University (NTU), Singapore
[2] School of Information and Communication Engineering, Sungkyunkwan University (SKKU), Korea
[3] Department of Electrical and Computer Engineering, University of Houston, Texas, USA
[4] Institute for Infocomm Research (I2R) - A*STAR, Singapore

***Abstract*—In wireless energy harvesting communication networks, a user harvests energy from an environment and uses the energy for data transmission. However, the user's data transmission is susceptible to a jamming attack by jammers, which also harvest energy from the environment. To address this problem, therefore we introduce a user's deception mechanism in which the user can transmit fake signals (i.e., blank transmission) to trigger the jammers to perform the attack, wasting their energy. We propose an analysis of the network with the deception mechanism based on a Markov chain. The performance evaluation reveals some interesting results. For example, the user can adjust the number of blank transmissions to achieve the highest throughput. We provide a benchmarking scheme based on an optimization. The benchmarking is useful for developing an effective deception mechanism with minimum complexity and knowledge about the network and jammers.**

***Index Terms*—Wireless harvesting communication networks, jamming attack, deception mechanism.**

I. Introduction

Wireless energy harvesting communication networks can be deployed and used for many applications, e.g., sensor networks and ad hoc networks. In the networks, nodes or users harvest energy from an environment (e.g., renewable sources such as solar and RF signals [1]) to collect and transmit data. However, the networks, especially in military applications, are vulnerable to jamming by jammers deployed by adversaries [2]. The jammers can be made to harvest energy from the environment, reducing reliance on infrastructure, working in a distributed and concealed fashion, and avoiding detection and any countermeasure. Additionally, many jammers can be deployed in the network, increasing the chance of attack success. To circumvent the jamming attack by energy harvesting jammers, the user can employ deception mechanisms by luring the jammers into ineffective attacks. For example, the user can transmit fake signal and observe the jamming to identify active jammers in the networks.

In this paper, we consider the wireless energy harvesting communication networks with a user and multiple jammers. Both user and jammers harvest energy from the environment for data transmission and jamming, respectively. The user takes advantage of the fact that the jammers have limited energy to perform jamming, and the jammers have to spend some time to harvest the energy for the next attack (e.g., reloading). In particular, the user can implement deception mechanisms in which the user will transmit blank signals with small energy consumption to attract the jammers to attack. As some jammers will become inactive when harvesting energy, the user can transmit real data with a higher chance of success. We propose an analysis of the networks with the energy harvesting user and jammers based on a Markov chain. The user's deception mechanism can be analyzed using the Markov chain to obtain some important performance measures (e.g., user throughput). Additionally, we consider the case that the user has complete information about the network and introduce an optimization based on a Markov decision process to obtain an optimal deception policy. The performance obtained from the optimization provides an upper bound for the user to develop effective deception mechanisms. We perform performance evaluation and reveal some interesting results. For example, if the jammers perform the attacks without coordination, there could be an optimal attack probability such that the throughput of the legitimate user is minimized.

The rest of this paper is organized as follows. Section II reviews related work. Section III describes the system model and states the assumptions used in this paper. Section IV presents the Markov chain analysis and derives performance measures. Section V presents the performance evaluation. Section VI summarizes the paper. Appendix presents an optimization formulation for obtaining the optimal deception policy.

II. Related Work

A jamming attack remains one of the most critical threats to wireless networks with a goal to disrupt data transmission of legitimate users. Very little work addresses jamming attack problems. For example, the authors of [3] considered that a jammer can adjust jamming power to a training period of packet transmission, resulting in incorrect transmission information (e.g., synchronization). Consequently, a user can adjust transmit power to overcome the jamming. A game theoretic model was developed to obtain a Nash equilibrium strategy. The authors of [4] analyzed the IEEE 802.11 networks under different jamming attack strategies (e.g., periodic and random jamming). A Markov chain model was developed to investigate the effect of jamming. The authors of [5] considered an

978-1-4673-6432-4/15/$31.00 ©2015 IEEE

incomplete information environment. A user has to build the belief about jammers to adapt transmission parameters accordingly. The authors of [6] presented an analytical model of jamming attack in time-critical wireless applications. The jamming attack detection based on estimation (JADE) scheme was also proposed to achieve robust jamming detection for the user. A Markov decision process was used in [8] to find an optimal transmission policy under the attack. The number of jammers was estimated, such that the user can optimize a transmission strategy to achieve the highest throughput. Deception mechanisms were adopted to tackle jamming. The authors of [9] introduced a deception mechanism to mitigate smart jammer attacks. The mechanism attracts jammers to attack on vacant channels so that the data transmission on the other channel will be successful. The authors of [10] considered a deception mechanism in a network layer. In particular, users can transmit fake data on different routes to let jammers attack. As a result, the route for actual data transfer can escape such a threat. The jamming attack was considered in a wireless energy harvesting communication network [11], with multi-antenna energy-harvesting cooperative jammers. The performance in the MIMO wiretap channel was analyzed under an energy constraint.

However, none of the work in the literature considered jamming in wireless energy harvesting communication network with deception mechanisms. Therefore, it is the scenario considered in this paper in which its analysis is presented.

III. System Model

A. Network Model

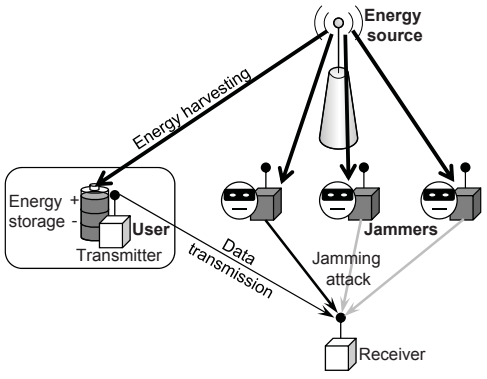


Fig. 1. System model.

We consider a wireless energy harvesting communication network as shown in Fig. 1. A user in the network is capable of harvesting energy from an environment (e.f., RF sources for wireless energy harvesting). The user uses the energy for transmission to a receiver. However, the network is susceptible to jamming attacks by multiple jammers. The jammers also harvest energy from the environment. The jammers use the harvested energy to perform jamming to the transmission by the user.

The user is aware of energy harvesting jammers in the network. Therefore, the user employs a deception mechanism to defend its own data transmission. In the deception mechanism, the user can perform blank transmission to deceive the jammers. The blank transmission can be the transmission of a fake signal with a relatively short period of time such that the active jammers (i.e., the jammers with enough energy harvested from the environment) can detect the signal and start the jamming attacks, wasting their energy. Since the blank transmission can use lower energy, the user can reserve some energy for its real data transmission later. After performing the jamming attacks, the jammers have to harvest energy from environment, which makes the jammers inactive for a certain period of time. As a result, the user can transmit data with a lower chance of being attacked. Figure 2 shows an example of the deception mechanism.

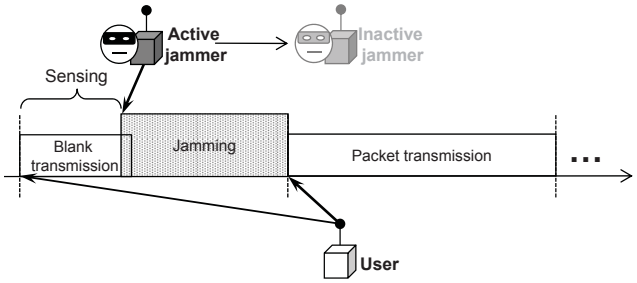


Fig. 2. Blank and data transmissions.

B. Assumptions of the Analysis

Based on the above system model of the wireless energy harvesting communication network and user's deception mechanism against jammers, it is important to analyze the user performance. In the next section, we will propose an analysis of the network based on a Markov chain. To make the analysis tractable, we make the following assumptions.

- We consider a time slot based system. The transmission of the user aligns to a time slot structure.
- The user has an energy storage (e.g., a battery) with the capacity of B units of energy. In each time slot, the user can harvest h units of energy from the environment with probability λ_h, where $h = 0, 1, \ldots, H$ and H is the maximum units of harvested energy.
- The user requires one unit of energy to perform blank transmission and requires E units of energy to perform data transmission, where $E > 1$.
- The user generates a data packet for transmission with probability α. The user must transmit the packet within a frame which is composed of F time slots. Otherwise, the packet will be discarded.
- For the deception mechanism, at time slot f in a frame, the user does not transmit anything (i.e., remains idle), performs blank transmission and data transmission with probabilities ϕ_f^{I}, ϕ_f^{B}, and ϕ_f^{D}, respectively, where $\phi_f^{\mathrm{I}} + \phi_f^{\mathrm{B}} + \phi_f^{\mathrm{D}} = 1$ for $f = 1, \ldots, F$.

- There are J identical jammers in the network. Each jammer can harvest energy sufficiently for the jamming attack with probability γ (i.e., it requires $1/\gamma$ time slots to collect enough energy for jamming).
- When the jammer is active (i.e., having enough energy), it performs the jamming attack with probability β. After jamming, the jammer becomes inactive, and cannot perform the jamming attack until it harvests enough energy again.

Without loss of generality, we assume that if at least one jammer performs the jamming attack, the data transmission by the user will be corrupted and the user has to transmit the data again. Note that the analysis can be easily extended for some general cases. For example, the successful data transmission probability of the user is a function of the number of jammers performing the attack. Additionally, the jammers can perform coordinated attacks (e.g., a set of jammers attacks). We omit the analysis for these cases due to space limit.

IV. Analysis

In this section, we develop a Markov chain to analyze the user performance with deception mechanisms. We first describe a state space and derive transition matrices. Then we obtain some important performance measures.

A. State Space and Transition Matrix

The discrete-time Markov chain has the state space defined as follows:

$$\begin{aligned}\Omega &= \Big\{(\mathscr{F},\mathscr{B},\mathscr{J}); \mathscr{F}\in\{0,1,\ldots,F\},\\ &\qquad \mathscr{B}\in\{0,1,\ldots,B\},\mathscr{J}\in\{0,1,\ldots,J\}\Big\}, \quad (1)\end{aligned}$$

where $\mathscr{F}$ represents the index of a time stage in a frame for a user to transmit a generated packet, $\mathscr{B}$ represents the energy level of the energy storage of the user, and $\mathscr{J}$ represents the number of active jammers. The time stage is zero when there is no generated data to be transmitted.

Next we derive the transition matrix of the Markov chain. We first consider the transition matrix for the number of active jammers. There are three cases. Firstly, we consider the transition when there is no transmission of the user. The transition matrix is expressed as follows:

$$\mathbf{J}_{\mathrm{I}} = \begin{bmatrix} J^{\mathrm{I}}_{0,0} & J^{\mathrm{I}}_{0,1} & J^{\mathrm{I}}_{0,1} & \cdots & J^{\mathrm{I}}_{0,J} \\ 0 & J^{\mathrm{I}}_{1,1} & J^{\mathrm{I}}_{1,2} & \cdots & J^{\mathrm{I}}_{1,J} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & J^{\mathrm{I}}_{J-1,J-1} & J^{\mathrm{I}}_{J-1,J} \\ 0 & \cdots & 0 & 0 & 1 \end{bmatrix} \quad (2)$$

where $J^{\mathrm{I}}_{j,j'}$ is the probability that the current number of active jammers is j and it changes to j'. This probability follows binomial distribution as follows:

$$J^{\mathrm{I}}_{j,j'} = \binom{J-j}{j'-j}\gamma^{j'-j}(1-\gamma)^{J-j'}. \quad (3)$$

Secondly, we consider the transition when there is transmission by the user, but none of jammers attacks. The transition matrix, denoted by $\mathbf{J}_{\mathrm{N}}$, has the element obtained from

$$J^{\mathrm{N}}_{j,j'} = (1-\beta)^j \binom{J-j}{j'-j}\gamma^{j'-j}(1-\gamma)^{J-j'}. \quad (4)$$

Thirdly, we consider the transition when there is transmission by the user, and at least one jammer attack. The transition matrix, denoted by $\mathbf{J}_{\mathrm{A}}$, has the element obtained from

$$\begin{aligned}J^{\mathrm{A}}_{j,j'} &= \sum_{a-i=j'-j}\left\{\binom{J-j}{a}\gamma^a(1-\gamma)^{J-j-a}\right\}\\ &\quad\times\left\{\binom{j}{i}\beta^i(1-\beta)^{j-i}\right\}, \quad (5)\end{aligned}$$

for $j>0$ where $a\in\{0,1,\ldots,J-j\}$ is the number of inactive jammers that become active (i.e., harvesting enough energy) and $i\in\{1,\ldots,j\}$ is the number of active jammers that become inactive (i.e., perform a jamming attack). Note that, for $j=0$, we have $J^{\mathrm{A}}_{0,j'}=0$ for all j' since there is no active jammer.

Then we consider the transition matrix for the energy level of the energy storage of the user. The energy transition can be divided into 3 major cases based on the action of the user (i.e., does nothing, performs blank transmission, and performs data transmissions). For the "doing nothing" case, the energy level can increase or remain the same. The transition matrix is expressed as follows:

$$\mathbf{B}_{\mathrm{I}} = \begin{bmatrix} \lambda_0\mathbf{J}_{\mathrm{I}} & \cdots & \lambda_H\mathbf{J}_{\mathrm{I}} & & \\ & \lambda_0\mathbf{J}_{\mathrm{I}} & \cdots & \lambda_H\mathbf{J}_{\mathrm{I}} & \\ & & \ddots & \ddots & \ddots \\ & & & \lambda_0\mathbf{J}_{\mathrm{I}} & \sum_{h=1}^{H}\lambda_h\mathbf{J}_{\mathrm{I}} \\ & & & & \sum_{h=0}^{H}\lambda_h\mathbf{J}_{\mathrm{I}} \end{bmatrix}, \quad (6)$$

where each row corresponds to the energy level $b=0,1,\ldots,B$ of the energy storage.

For the "blank transmission" case, the energy level can decrease by one unit, remain the same, or increase. The transition matrix is expressed as follows:

$$\mathbf{B}_{\mathrm{B}} = \begin{bmatrix} \lambda_0\mathbf{J}_{\mathrm{N}} & \cdots & \lambda_H\mathbf{J}_{\mathrm{N}} & & \\ \lambda_0\hat{\mathbf{J}} & \cdots & \lambda_H\hat{\mathbf{J}} & & \\ & \ddots & \ddots & \ddots & \\ & & \lambda_0\hat{\mathbf{J}} & \lambda_1\hat{\mathbf{J}} & \sum_{h=2}^{H}\lambda_h\hat{\mathbf{J}} \\ & & & \lambda_0\hat{\mathbf{J}} & \sum_{h=1}^{H}\lambda_h\hat{\mathbf{J}} \end{bmatrix} \quad (7)$$

where $\hat{\mathbf{J}}=\mathbf{J}_{\mathrm{N}}+\mathbf{J}_{\mathrm{A}}$ (i.e., the active jammers can perform a jamming attack).

For the "data transmission" case, the energy level will decrease by E units, if the current energy level is larger than or equal to E. Otherwise, it will not decrease (no data transmission due to lack of enough energy). We consider two subcases, i.e., successful and unsuccessful data transmission. The former happens when no active jammers performs the jamming attack (i.e., $\mathbf{J}_{\mathrm{N}}$ applies), and the latter happens when

at least one active jammers performs the jamming attack (i.e., $\mathbf{J}_{\mathrm{A}}$ applies). For the "successful data transmission" subcase, we have the transition matrix defined as follows:

$$\mathbf{B}_{\mathrm{S}} = \begin{bmatrix} 0 & & & & \\ & \ddots & & & \\ & & 0 & & \\ \hline \lambda_0\mathbf{J}_{\mathrm{N}} & \cdots & \lambda_H\mathbf{J}_{\mathrm{N}} & & \\ \ddots & \ddots & \ddots & \ddots & \\ & \lambda_0\mathbf{J}_{\mathrm{N}} & \cdots & \lambda_H\mathbf{J}_{\mathrm{N}} & \\ & & \lambda_0\mathbf{J}_{\mathrm{N}} & \cdots & \sum_{h=E}^{H}\lambda_h\mathbf{J}_{\mathrm{N}} \end{bmatrix}, \tag{8}$$

where in the first E rows, the probability is zero. For the "unsuccessful data transmission" subcase, we have the transition matrix defined as follows:

$$\mathbf{B}_{\mathrm{U}} = \begin{bmatrix} \lambda_0\mathbf{J}_{\mathrm{N}} & \cdots & \lambda_H\mathbf{J}_{\mathrm{N}} & & \\ & \ddots & \ddots & \ddots & \\ & \lambda_0\mathbf{J}_{\mathrm{N}} & \cdots & \lambda_H\mathbf{J}_{\mathrm{N}} & \\ \hline \lambda_0\mathbf{J}_{\mathrm{A}} & \cdots & \lambda_H\mathbf{J}_{\mathrm{A}} & & \\ & \ddots & \ddots & \ddots & \\ & & \lambda_0\mathbf{J}_{\mathrm{A}} & \cdots & \sum_{h=E}^{H}\lambda_h\mathbf{J}_{\mathrm{A}} \end{bmatrix}. \tag{9}$$

Next, we combine the transition of a time stage in a frame. The transition matrix $\mathbf{P}$ of the entire Markov chain is expressed as in (10), where $\mathbf{0}$ is a matrix of zeros with an appropriate size. Each row of matrix $\mathbf{P}$ corresponds to the time stage $f = 0, 1, \ldots, F$ in a frame. The time stage will start counting when there is an arriving packet (i.e., with probability α). Then if the data packet is not successfully transmitted, the time stage will increase until reaching the end of the frame. Otherwise, the time stage will be reset and return to an initial stage.

B. Steady State Probability and Performance Measures

To obtain the performance measure of the user, we obtain the steady state probability of the Markov chain. Let $\pi(f, b, j)$ denote the steady state probability at state (f, b, j), where f is the time stage in a frame, b is the energy level, and j is the number of active jammers. The vector of steady state probability is denoted by $\vec{\boldsymbol{\pi}}$, which is obtained from solving $\vec{\boldsymbol{\pi}}^{\top}\mathbf{P} = \vec{\boldsymbol{\pi}}^{\top}$ and $\vec{\boldsymbol{\pi}}^{\top}\vec{\mathbf{1}} = 1$, where $\vec{\mathbf{1}}$ is a vector of ones with an appropriate size.

The user throughput can be obtained from

$$\tau = \sum_{f=1}^{F}\sum_{b=E}^{B}\sum_{j=0}^{J}\phi_f^{\mathrm{D}}\pi(f, b, j)(1-\beta)^j. \tag{11}$$

The data is successfully transmitted if there is enough energy and none of active jammers perform the jamming attack.

The probability that the data is successfully transmitted after f time stages is obtained from

$$\theta_f = \frac{\sum_{b=E}^{B}\sum_{j=0}^{J}\phi_f^{\mathrm{D}}\pi(f, b, j)(1-\beta)^j}{\sum_{f'=1}^{F}\sum_{b=E}^{B}\sum_{j=0}^{J}\phi_f^{\mathrm{D}}\pi(f', b, j)(1-\beta)^j}. \tag{12}$$

Therefore, the average delay is $\overline{f} = \sum_{f=1}^{F} f\theta_f$.

V. Performance Evaluation

A. Parameter Setting

We consider a wireless energy harvesting communication network. The user and jammers in the network harvest wireless energy (e.g., from ambient RF sources). The user has the energy storage with the capacity of 20 units of energy, and the maximum time stage for each packet is 7. The user requires one unit of energy for blank transmission and three units of energy for a data transmission. The packet arrival probability is 0.3. Unless otherwise stated, the energy harvesting rate of the user (i.e., the rate to harvest one unit of energy) is 0.7 units per time slot. There are 5 jammers. The energy harvesting rate of the jammers (i.e., the rate to harvest enough energy to perform one jamming attack) is 0.1. In other words, the jammers need 10 time slots to harvest enough energy. If the user performs either blank or data transmission, each jammer performs the jamming attack with probability 0.5. We consider a simple deception mechanism where the user performs blank transmission at the beginning of a frame, and the user transmits data for rest of the frame. For example, if the user applies one blank transmission, then $\phi_1^{\mathrm{B}} = 1$, $\phi_1^{\mathrm{I}} = \phi_1^{\mathrm{D}} = 0$, and $\phi_f^{\mathrm{D}} = 1$, $\phi_f^{\mathrm{I}} = 0$, $\phi_f^{\mathrm{B}} = 0$ for $f = 2, \ldots, F$. The number of blank transmissions is varied depending on evaluation scenarios. Additionally, we consider the optimal jammer deception mechanism which assumes that the user performs blank and data transmission knowing all the network states. This is for benchmarking purpose. Appendix presents the optimization to obtain the optimal deception policy.

B. Numerical Results

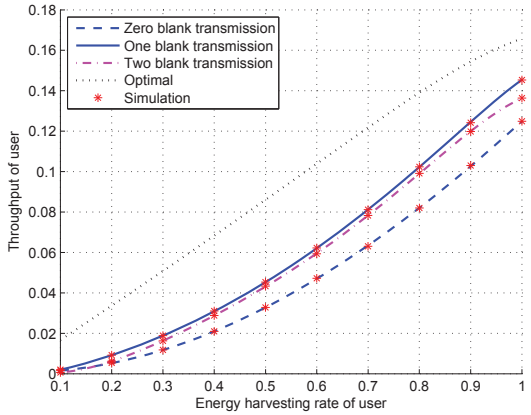


Fig. 3. Throughput of a user under different energy harvesting rate of the user.

Figures 3 and 4 show the user throughput when the energy harvesting rate of the user and jammers are varied. As expected, the user throughput increases as its energy supply increases. By contrast, the throughput decreases as the energy

$$\mathbf{P} = \begin{bmatrix} (1-\alpha)\mathbf{B}_{\mathrm{I}} & \alpha\mathbf{B}_{\mathrm{I}} & & & \\ \phi_1^{\mathrm{D}}\mathbf{B}_{\mathrm{S}} & \mathbf{0} & \phi_1^{\mathrm{I}}\mathbf{B}_{\mathrm{I}} + \phi_1^{\mathrm{B}}\mathbf{B}_{\mathrm{B}} + \phi_1^{\mathrm{D}}\mathbf{B}_{\mathrm{U}} & & \\ \vdots & & \ddots & \ddots & \\ \phi_{F-1}^{\mathrm{D}}\mathbf{B}_{\mathrm{S}} & & \cdots & \mathbf{0} & \phi_{F-1}^{\mathrm{I}}\mathbf{B}_{\mathrm{I}} + \phi_{F-1}^{\mathrm{B}}\mathbf{B}_{\mathrm{B}} + \phi_{F-1}^{\mathrm{D}}\mathbf{B}_{\mathrm{U}} \\ \phi_F^{\mathrm{D}}(\mathbf{B}_{\mathrm{S}} + \mathbf{B}_{\mathrm{U}}) + \phi_F^{\mathrm{I}}\mathbf{B}_{\mathrm{I}} + \phi_F^{\mathrm{B}}\mathbf{B}_{\mathrm{B}} & & \cdots & \cdots & \mathbf{0} \end{bmatrix}. \quad (10)$$

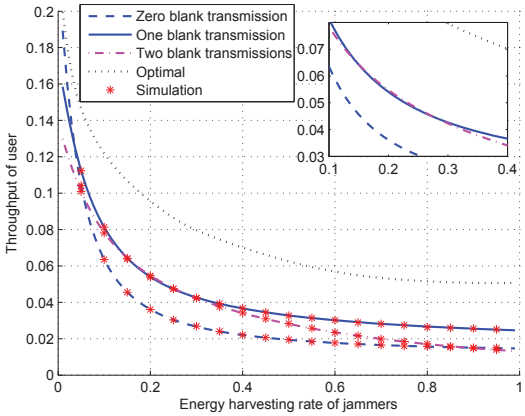


Fig. 4. Throughput of a user under different energy harvesting rate of the jammer.

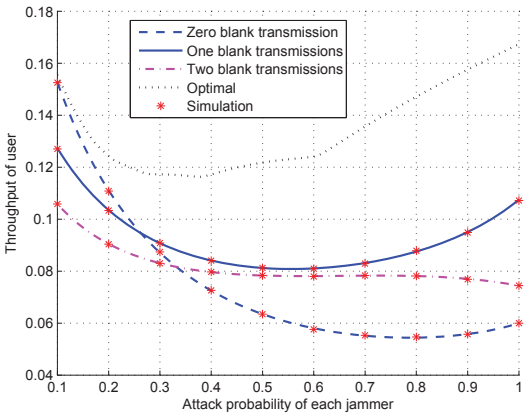


Fig. 5. Throughput of a user under different attack probability.

supply to the jammers increases. We also vary the number of blank transmissions in the deception mechanism. We observe that different numbers of blank transmissions result in different throughput behaviors. From Fig. 3, the highest throughput is achieved when we adopt one blank transmission. However, from Fig. 4, the highest throughput is achieved for different numbers of blank transmissions depending on the energy harvesting rate of the jammers. For example, one blank transmission mostly yields the higher throughput except some range as shown in a subfigure (top right), where two blank transmissions yield slightly higher throughput. Additionally, we perform a simulation to validate the analysis. The simulation results agree with that of analysis.

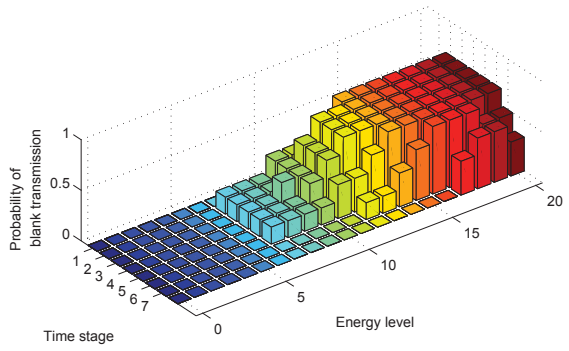
We then vary the attack probability of the jammers and show the user throughput in Fig. 5. Here we observe some interesting result. Firstly, there is the attack probability of the jammers that achieves minimum throughput (most successfully jamming). For zero and one blank transmission, the throughput first decreases and then increases. This is due to the fact that with a small attack probability, the throughput is high since the user is marginally affected by the fewer jamming attacks performed by the jammers. By contrast, with a high attack probability, the throughput improves since many jammers perform jamming attack and they have to wait for energy harvesting, leaving an opportunity for the user to successfully transmit data.

However, for two blank transmissions, we observe that the user throughput first decreases, then increases, and decreases again when the attack probability increases. The same reason as zero and one blank transmission cases applies. However, with two blank transmissions, the user also consumes more energy. Therefore, when the attack probability is large, the user also cannot transmit data, resulting in a detrimental throughput performance. The similar phenomenon is also observed when the number of blank transmissions increases.

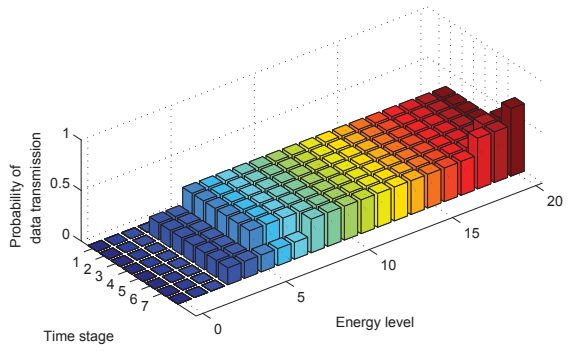
In the above results, we observe that the optimal deception policy always yields the highest user throughput. This is due to the fact that the optimal policy assumes the user to know the number of active jammers. To gain some insight, we evaluate the detail of the optimal policy. Figures 6(a) and (b) show the probabilities of blank and data transmissions by the user, averaged over all number of active jammers. We observe that the user will perform blank transmission when the energy level is high. The user spreads data transmission over all time stages in a frame, and again prefers to transmit data when the energy level is high. This result suggests that the jammer deception mechanism can be optimized to achieve the optimal throughput performance for the user, and this deserves further studies.

VI. Summary

We have considered a wireless energy harvesting communication network. Not only a user, but also jammers in the network can harvest energy from the environment for data transmission and jamming attacks, respectively. To alleviate the adverse effect of jamming, we have introduced a deception mechanism for the user by performing blank transmission to lure the jammers into ineffective attacks so as to waste their en-



(a)



(b)

Fig. 6. Probabilities of blank and data transmissions.

ergy. We have analyzed the network by formulating a Markov chain, which is able to obtain some important performance measures for the user. Additionally, for benchmarking purpose, we have extended the Markov chain by optimizing the user's deception mechanism based on a Markov decision process assuming that all the states are known. The user performance of this optimization serves as an upper bound.

For future work, the deception policy will be optimized assuming partially observable states of the network.

ACKNOWLEDGEMENTS

This work was supported in part by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIP) (2014R1A5A1011478), U.S. National Science Foundation under Grants US NSF CNS-1443917, ECCS-1405121, CNS-1265268, CNS-0953377, and NSFC 61428101, and Singapore MOE Tier 1 (RG18/13 and RG33/12).

APPENDIX A
OPTIMAL USER'S DECEPTION MECHANISM

We formulate a Markov decision process (MDP) for the user to optimize the deception mechanism, i.e., to perform blank or data transmission. Although this MDP requires complete information of the network's states (e.g., the number of active jammers), which may not be practical, it can serve as a benchmark for the optimal performance of the user. The state space of the MDP is defined as in (1). The action space is defined as $\mathcal{A} = \{0, 1, 2\}$ for when the user does nothing, performs blank transmission, and data transmission, respectively. The immediate reward function given states $(f, g, j) \in \Omega$ and action $a \in \mathcal{A}$ is defined as follows:

$$\mathscr{R}(f, b, j|a) = \begin{cases} (1-\beta)^j, & f > 0 \text{ and } b > E \text{ and } a = 2, \\ 0, & \text{otherwise.} \end{cases} \tag{13}$$

The MDP is defined as follows:

$$R(\chi) = \lim_{t' \to \infty} \frac{1}{t'} \sum_{t=1}^{t'} E_{\chi}\Big(\mathscr{R}(f_t, b_t, j_t|a_t)\Big), \tag{14}$$

where (f_t, g_t, j_t) is the state and a_t is the action at time t, and χ is a policy (i.e., a mapping from the state to action). The optimal policy χ^* can be obtained by solving the MDP (e.g., using a linear programming approach [12]).

REFERENCES

[1] X. Lu, P. Wang, D. Niyato, D. I. Kim, and Z. Han, "Wireless Network with RF Energy Harvesting: A Contemporary Survey" (available online at *arXiv: 1406.6470*)

[2] A. Mpitziopoulos, D. Gavalas, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs," *IEEE Communications Surveys & Tutorials*, vol. 11, no. 4, pp. 42-56, Fourth Quarter 2009.

[3] X. Zhou, D. Niyato, and A. Hjørungnes, "Optimizing training-based transmission against smart jamming," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 6, pp. 2644-2655, July 2011.

[4] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "On the Performance of IEEE 802.11 under Jamming," in *Proceedings of IEEE INFOCOM*, April 2008.

[5] Y. E. Sagduyu, R. A. Berry, and A. Ephremides, "Jamming games in wireless networks with incomplete information," *IEEE Communications Magazine*, vol. 49, no. 8, pp. 112-118, August 2011.

[6] Z. Lu, W. Wang, and C. Wang, "Modeling, evaluation and detection of jamming attacks in time-critical wireless applications," *IEEE Transactions on Mobile Computing*, vol. 13, no. 8, pp. 1746-1759, August 2014.

[7] Q. Zhu, H. Li, Z. Han, and T. Basar, "A Stochastic Game Model for Jamming in Multi-Channel Cognitive Radio Systems," in *Proceedings of IEEE International Conference on Communications (ICC)*, 23-27 May 2010.

[8] Y. Wu, B. Wang, and K. J. R. Liu, "Optimal defense against jamming attacks in cognitive radio networks using the Markov decision process approach," in *Proceedings of Global Telecommunications Conference (GLOBECOM)*, 6-10 Dec. 2010.

[9] J. Jeung, S. Jeongm, and J. Lim, "Adaptive rapid channel-hopping scheme mitigating smart jammer attacks in secure WLAN," in *Proceedings of Military Communications Conference (MILCOM)*, pp. 1231-1236, 7-10 November 2011.

[10] Q. Zhu; A. Clark, R. Poovendran, and T. Basar, "Deceptive routing games," in *Proceedings of IEEE Conference on Decision and Control (CDC)*, pp. 2704-2711, 10-13 December 2012.

[11] A. Mukherjee and J. Huang, "Deploying multi-antenna energy-harvesting cooperative jammers in the MIMO wiretap channel," in *Conference Record of Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, pp. 1886-1890, 4-7 November 2012.

[12] M. L. Puterman, *Markov Decision Processes: Discrete Stochastic Dynamic Programming*, Wiley-Interscience, April 1994.