Noname manuscript No.
(will be inserted by the editor)

Quality of Protection in Cloud-Assisted Cognitive Machine-to-Machine Communications for Industrial Systems

Li Jiang · Hui Tian · Jian Shen · Sabita Maharjan · Yan Zhang

Received: date / Accepted: date

Abstract Cloud-assisted cognitive machine-to-machine communications (CM2M) is a new paradigm to improve the mobile services, which have drawn considerable attention in industry and academia. In this paper, we consider the quality of protection (QoP) of information transmission in cloud-assisted CM2M communications. In such an environment, the secondary M2M system intends to share the primary spectrum on the condition that the secondary transmitter (ST) has to relay the primary message. However, the ST is a low-energy device which adopts the energy harvesting technique to power itself. In particular, we focus on secure information transmission for the primary system when the secondary users (SUs) are the potential eavesdroppers. We aim to jointly design power splitting and secure beamforming to maximize the secondary M2M system data rate subject to the secrecy requirement of the primary system and the ST power constraint. To solve this non-convex problem, we propose a computationally efficient two-stage optimization approach. Simulation results demonstrate that our proposed scheme achieves a significant transmission rate of the secondary M2M system while provides a high secrecy rate for the primary system compared to the scheme without energy harvesting.

Li Jiang and Hui Tian
State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, and Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory, Beijing, China.
E-mail: jill@bupt.edu.cn and tianhui@bupt.edu.cn

Jian Shen
Nanjing University of Information Science and Technology, Nanjing, China.
E-mail: s_shenjian@126.com

Sabita Maharjan and Yan Zhang
Simula Research Laboratory, Oslo 1325, Norway.
E-mail: sabita@simula.no and yanzhang@simula.no

Keywords Cloud-assisted cognitive machine-to-machine · quality of protection · energy harvesting · power splitting · secure beamforming

1 Introduction

Machine-to-machine (M2M) communications is an emerging communication paradigm that provides ubiquitous connectivity between devices with automatically data generation, exchange, processing and actuation requiring no humans intervention [1]. Cognitive M2M (CM2M) is proposed [2] to tackle the spectrum congestion problems in conventional M2M, in which cognitive radio [3] enabled machines are able to sense and utilize unused frequency bands in their surroundings. By adding a cognitive radio technology, the CM2M is more intelligent and adaptable than conventional M2M. However, the inherent limitations of devices including low battery life, weak processing rate, and limited local storage, have significantly impeded the improvement of mobile service utilities and brings new challenges to CM2M. CM2M may integrate with cloud computing [4] and are evolving toward cloud-assisted CM2M networks.

In cloud-assisted CM2M networks, there are many mobile applications in connected and cognitive devices, e.g., security and public safety (surveillance systems, object/human tacking, etc.), smart grids (grid control, industrial metering), vehicular telematics (fleet management, enhanced navigation), healthcare (telemedicine, remote diagnosis) [5]. An enormous amount of sensitive and confidential information will be transmitted via wireless channels in these mobile applications. The security and privacy issues related to the devices information transmission are becoming a rising concern. To achieve secure communication and provide quality of protection (QoP) service, physical-layer security based on information theory has been receiving growing interest

recently [7]. Differing from the traditional approach which protects data security through cryptographic techniques, physical layer security is identified as a promising strategy that provides secure wireless transmissions by smartly exploiting the imperfections of the communication medium. Using this strategy, the quality of signal received at unauthorized receivers and devices can effectively be degraded so as to secure the confidential information.

In this paper, we consider the cooperation transmission scheme between the primary system and the secondary M2M system which is a win-win strategy in the sense that the secondary transmitter (ST) helps to relay the traffic from the primary transmitter (PT) to the primary user (PU), and in return the ST can utilize the primary spectrum to serve its own secondary users (SUs) [6]. Since the primary system is the licensed spectrum holder, its information should be protected. Existing literatures have investigated the physical layer security to avoid primary information leakage to the external eavesdroppers (illegitimate users) [8] and [9]. There is another security issues where the SUs try to decode the primary information from the spectrum sensing results without permission. Authors in [10], [11] considered such case, while [10] focused on the characterization of an achievable secrecy rate for cooperative model in single-input single-output (SISO) channel and [11] characterized the achievable secrecy rate region for the cooperative model with multiple SUs, and it also considered the SISO channel.

Furthermore, it is a commonly seen situation when the ST is an energy-constrained device, such as sensors, which makes the cooperation between the primary system and the secondary M2M system difficult. Recently, harvesting energy from radio frequency (RF) signals is emerging as an attractive solution to power energy-constrained wireless communication devices [12]. The idea of utilizing RF signals from the PT to power the secondary devices has first been proposed in [13]. In RF-powered cooperative cognitive radio networks, the PT will transmit both information and energy to the energy-constrained ST, in exchange for the ST to relay the primary information and simultaneously transmits its own data, which creates even stronger incentives for both the primary system and the secondary system to cooperate and substantially improves the system overall spectrum efficiency [14].

Nevertheless, there exists several security problems in such scenario. Since the ST performs energy harvesting to forward the PT's information, the SUs may be the potential eavesdroppers and eavesdrop the PT's information without permission. It gives rise to a question: how about the security performance for the primary system in cloud-assisted cooperative CM2M networks when the ST is an energy-constrained device and the SUs are the potential eavesdroppers? This is a practical problem in the QoP guaranteed cloud-assisted mobile services.

The main contributions of this paper can be summarized as follows: first, we consider a cloud-assisted CM2M scenario in which the primary system cooperates with an energy-constrained secondary M2M system. We assume that the ST-SUs pairs in the secondary M2M system are the multiple-input single-output (MISO)links. Furthermore, we observe a new case when the SUs are potential eavesdroppers. This gives a new challenge in studying secure performance of the primary system. Second, we propose a new joint scheme by considering both power splitting and secure beamforming and formulate an optimization problem to maximize the secondary M2M system data rate subject to the secrecy rate requirement of the primary system and the power constraint of the ST. Then a computationally efficient two-stage optimization algorithm is proposed to solve the non-convex optimization problem. Finally, simulation results demonstrate that our proposed scheme achieves a significant transmission rate of the secondary M2M system while provides a high secrecy rate for the primary system compared to the scheme without energy harvesting.

The rest of this paper is organized as follows. The system model and the problem formulation are described in Section 2. Section 3 proposes the computationally efficient optimal algorithm based on a two-stage procedure. The simulation examples are provided to demonstrate the performance of the proposed algorithm in Section 4. Finally, Section 5 concludes the paper.

2 System model and problem formulation

2.1 Cloud-assisted CM2M networks

Fig.1 shows a cloud-assisted CM2M networks consists of two-tier network architecture. The first tier contains a heterogeneous wireless machines communications. Specifically, the large primary cells provide ubiquitous coverage to M2M devices; while smaller network elements such as relays and access points (APs) including femto- and pico-enhanced base stations sense the idle spectrum of the primary cells and bring connectivity closer to the devices so as to improve link reliability and increase system spectrum efficiency. The second tier involves service cloud which collects and processes data from machines and manage their operation.

2.2 Secure information transmission in cloud-assisted CM2M networks

Fig.2 shows the system model of the secure information transmission in a cloud-assisted CM2M networks. We consider cooperation between a primary system and an energy-constrained secondary M2M system. The primary system

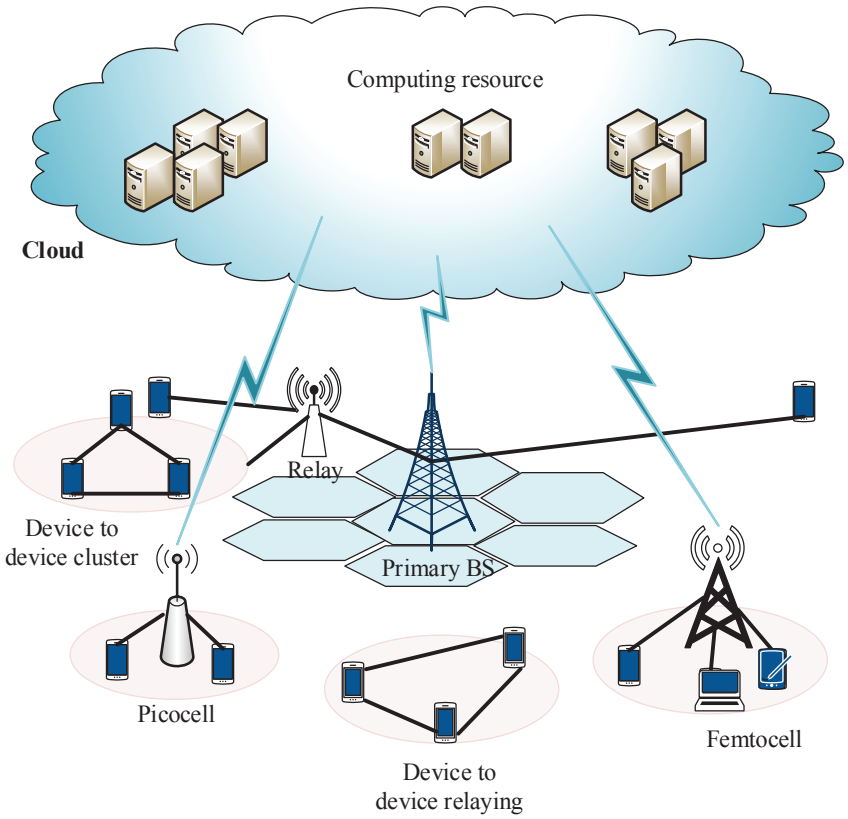

Fig. 1: Cloud-assisted CM2M networks

consists of a PT and a PU, while the secondary M2M system has a ST who serves one desired SU. There exists K-1 legitimate SUs. All terminals have a single antenna except that the ST has N antennas. The PT intends to send a confidential message, s_p, to the PU while the ST transmits a non-confidential message, s_s, to the desired SU. We consider a case that the ST intends to share the spectrum occupied by the primary system on the condition that the ST has to relay the PT's message. However, when the ST is a low-energy relay node, the cooperation is difficult. In this paper, we consider a two-phase transmission. At the first phase, the PT transmits signal. Then the ST adopts the power splitting technique [15] which splits the received PT's signal into two separate signal streams with different power levels, one sent to the energy harvester and the other to the information receiver. The power splitting technique is an intuitive and feasible scheme to demonstrate the energy harvesting principle where the RF receiver is the crucial device [16]. It has been noticed that all key components comprising of a receiver are available in the market, e.g., the power splitter [17] and the energy harvester [18]. Hence, it is possible to implement an energy harvesting system based on the power splitting technique. At the second phase, the ST concurrently transmits both the primary message and its own data by using the harvested energy, the amount of which is sufficient for powering the ST, such as a short-range sensor. Nevertheless, the K SUs may eavesdrop the PT's confidential message. The potential applications of the considered scenario include cognitive sensor networks or the indoor environment (e.g., smart buildings) where WiFi and ZigBee coexist and they both operate at 2.4 GHz. WiFi is the primary system for Internet access while ZigBee is the secondary system for industrial monitoring. In this case, ZigBee has limited power supply and can harvest energy from the primary transmitter to extend lifetime. At the same time, the ZigBee users can be potential eavesdroppers. The related data computing and storage are performed by local cloud server.

The channel coefficients of the PT-PU and the PT-SU$_k$ ($k \in \{1,\ldots,K\}$) links are denoted by the complex scalar h_{pp} and h_{ps_k}, respectively. The $N\times 1$ complex channel vectors of the PT-ST, ST-PU, ST-SU and ST-SU$_k$ links are represented by $\mathbf{g}$, $\mathbf{h}_{sp}$, $\mathbf{h}_{ss}$ and $\mathbf{h}_{ss_k}$, respectively. Although the legitimate SUs may misbehave and eavesdrop the primary confidential message, these legitimate SUs are active and also need to interact with the ST. Thus, the ST knows the full channel state information (CSI) of all the receivers.

As depicted in Fig. 2, at the first phase, the PT transmits s_p with power P_p, the received signal at the PU, the ST and

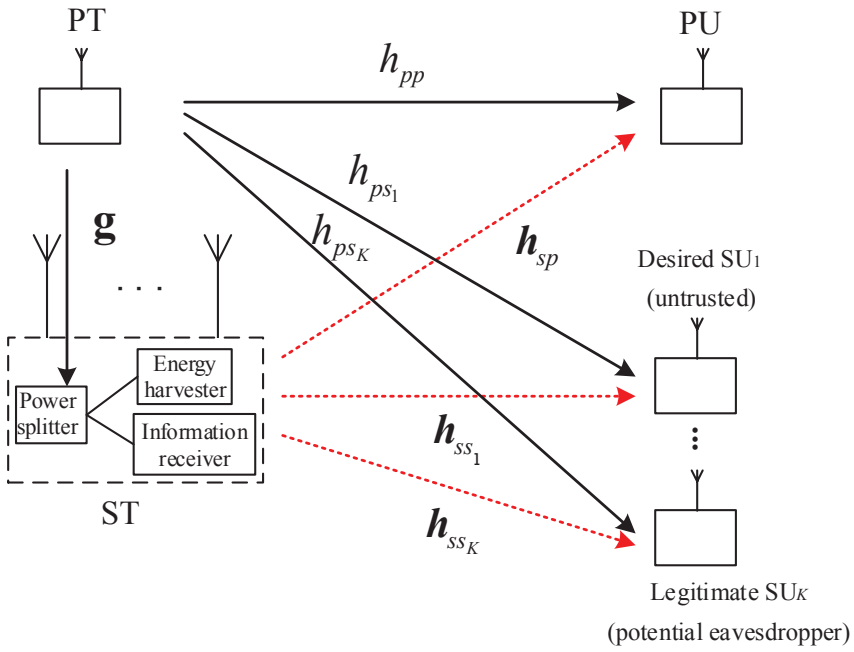

Fig. 2: Model of secure information transmission in a cloud-assisted CM2M networks, where the solid line denotes the first transmission phase and the dotted line denotes the second transmission phase

the SU_k are given by, respectively,

$$y_{PU} = \sqrt{P_p} h_{pp} s_p + n_{PU}, \tag{1}$$

$$\mathbf{y}_{ST} = \sqrt{P_p} \mathbf{g} s_p + \mathbf{n}_{ST}, \tag{2}$$

and

$$\mathbf{y}_{SU_k} = \sqrt{P_p} h_{ps_k} s_p + n_{SU_k}, \tag{3}$$

where n_{PU}, $\mathbf{n}_{ST}$ and n_{SU_k} are the received thermal noise at the PU, the ST and the SU_k, respectively, and are modeled as zero-mean additive white Gaussian noise (AWGN) with variance of N_0, $n_{PU} \in CN(0, N_0)$, $\mathbf{n}_{ST} \in CN(0, N_0\mathbf{I})$ and $n_{SU_k} \in CN(0, N_0)$.

The ST splits the received signal into two portions: one for forwarding to the PU after amplify-and-forward (AF) processing and the other for harvesting energy with relative power splitting ratio of ρ and 1-ρ, respectively. Hence, the signal for AF processing is written as

$$\breve{y}_{ST} = \sqrt{\rho}(\sqrt{P_p}\mathbf{g}^\dagger \mathbf{g} s_p + \mathbf{g}^\dagger \mathbf{n}_{ST}) + \mathbf{g}^\dagger \tilde{\mathbf{n}}_{ST}, \tag{4}$$

where $\tilde{\mathbf{n}}_{ST}$ is the noise due to the RF to baseband conversion and modeled as zero-mean AWGN with variance of N_C, $\tilde{\mathbf{n}}_{ST} \in CN(0, N_C\mathbf{I})$.

The amount of the harvested energy at the ST is given by

$$P_{EH} = \eta \left[(1-\rho) P_p \|\mathbf{g}\|^2 + (1-\rho) N_0 \right], \tag{5}$$

where η denotes the energy conversion efficiency from signal power to circuit power.

At the second phase, the ST concurrently transmits both the primary confidential message and its own data by using the forwarding beamforming vector $\mathbf{w}_p \in \mathbb{C}^{N\times 1}$ and the cognitive beamforming vector $\mathbf{w}_s \in \mathbb{C}^{N\times 1}$. The resulting transmit signal vector at the ST is given by

$$\mathbf{t} = \mathbf{w}_p \breve{y}_{ST} + \mathbf{w}_s s_s, \tag{6}$$

and the transmit power of the ST can be expressed as

$$\left(\rho P_p \|\mathbf{g}\|^4 + \rho N_0 \|\mathbf{g}\|^2 + N_C \|\mathbf{g}\|^2\right) \left|\mathbf{w}_p\right|^2 + \left|\mathbf{w}_s\right|^2, \tag{7}$$

By applying maximal ratio combining (MRC), the achievable signal-to-interference ratio (SINR) of the primary confidential message at the PU is the sum of signal transmission in two phases, which is expressed as

$$\mathrm{SINR}_p = \frac{P_p \left|h_{pp}\right|^2}{N_0} + \frac{\rho P_p \left|\mathbf{h}_{sp}^\dagger \mathbf{w}_p\right|^2 \|\mathbf{g}\|^4}{\left|\mathbf{h}_{sp}^\dagger \mathbf{w}_p\right|^2 (\rho \|\mathbf{g}\|^2 N_0 + \|\mathbf{g}\|^2 N_C) + \left|\mathbf{h}_{sp}^\dagger \mathbf{w}_s\right|^2 + \tilde{N}_0}, \tag{8}$$

where $\tilde{N}_0 = N_C + N_0$ is the combined received noise power. The achievable SINR of the secondary message at the desired SU is expressed as

$$\mathrm{SINR}_s = \frac{\left|\mathbf{h}_{ss}^\dagger \mathbf{w}_s\right|^2}{\left(\rho P_p \|\mathbf{g}\|^4 + \rho \|\mathbf{g}\|^2 N_0 + \|\mathbf{g}\|^2 N_C\right) \left|\mathbf{h}_{ss}^\dagger \mathbf{w}_p\right|^2 + \tilde{N}_0}, \tag{9}$$

The eavesdropping SINR of the primary confidential message during two phases at the SU_k is given by

$$\mathrm{SINR}_{SU_k} = \frac{P_p\left|\mathrm{h}_{ps_k}\right|^2}{N_0} + \frac{\rho P_p\left|\mathbf{h}_{ss_k}^{\dagger}\mathbf{w}_p\right|^2\|\mathbf{g}\|^4}{\left|\mathbf{h}_{ss_k}^{\dagger}\mathbf{w}_p\right|^2(\rho\|\mathbf{g}\|^2N_0+\|\mathbf{g}\|^2N_C)+\left|\mathbf{h}_{ss_k}^{\dagger}\mathbf{w}_s\right|^2+\tilde{N}_0}, \tag{10}$$

Thus, the achievable secrecy rate of the primary confidential message can be expressed as

$$R_s = \frac{1}{2}\left[\log(1+\mathrm{SINR}_p)-\log(1+\max_{k\in\{1,\ldots,K\}}\left\{\mathrm{SINR}_{SU_k}\right\})\right]^+, \tag{11}$$

where the factor $\frac{1}{2}$ is added due to the two-phase transmission process.

The joint power splitting and secure beamforming is designed to maximize the desired SU rate subject to the secrecy rate requirement for the PU and the power constraint of the ST. Due to the monotonicity between the received SINR and the achievable rate, the optimization problem can be formulated as (P1):

$$\begin{aligned}
&\max_{\rho,\mathbf{w}_s,\mathbf{w}_p}\ \frac{\left|\mathbf{h}_{ss}^{\dagger}\mathbf{w}_s\right|^2}{\left(\rho P_p\|\mathbf{g}\|^4+\rho\|\mathbf{g}\|^2N_0+\|\mathbf{g}\|^2N_C\right)\left|\mathbf{h}_{ss}^{\dagger}\mathbf{w}_p\right|^2+N_0}\\
&\text{s.t.}\\
&\mathrm{C1}: \frac{P_p\left|h_{pp}\right|^2}{N_0}+\frac{\rho P_p\left|\mathbf{h}_{sp}^{\dagger}\mathbf{w}_p\right|^2\|\mathbf{g}\|^4}{\left|\mathbf{h}_{sp}^{\dagger}\mathbf{w}_p\right|^2(\rho\|\mathbf{g}\|^2N_0+\|\mathbf{g}\|^2N_C)+\left|\mathbf{h}_{sp}^{\dagger}\mathbf{w}_s\right|^2+N_0}\geqslant\Gamma_p,\\
&\mathrm{C2}: \frac{P_p\left|h_{ps_k}\right|^2}{N_0}+\frac{\rho P_p\left|\mathbf{h}_{ss_k}^{\dagger}\mathbf{w}_p\right|^2\|\mathbf{g}\|^4}{\left|\mathbf{h}_{ss_k}^{\dagger}\mathbf{w}_p\right|^2(\rho\|\mathbf{g}\|^2N_0+\|\mathbf{g}\|^2N_C)+\left|\mathbf{h}_{ss_k}^{\dagger}\mathbf{w}_s\right|^2+N_0}\leqslant\Gamma_{SU_k},\quad\forall k,\\
&\mathrm{C3}: \left(\rho P_p\|\mathbf{g}\|^4+\rho N_0\|\mathbf{g}\|^2+N_C\|\mathbf{g}\|^2\right)\left|\mathbf{w}_p\right|^2+\left|\mathbf{w}_s\right|^2\leqslant P_{s0}+\eta\left[(1-\rho)P_p\|\mathbf{g}\|^2+(1-\rho)N_0\right],\\
&\mathrm{C4}: \quad 0\leqslant\rho\leqslant 1.
\end{aligned} \tag{12}$$

In C1, $\Gamma_p>0$ denotes the minimum SINR required at the PU for decoding PT's message. In C2, $\Gamma_{SU_k}>0$ denotes the maximum allowable SINR threshold for the kth SU to eavesdrop the PT's message. C1 and C2 guarantee that the lower bound of the secrecy rate for the PT's message is positive: $\frac{1}{2}\log(1+\Gamma_p)-\frac{1}{2}\log(1+\max_{k\in\{1,\ldots,K\}}\left\{\Gamma_{SU_k}\right\})\geqslant 0$. C3 denotes the transmit power constraint at the ST, P_{s0} is the initial power at the ST. C4 denotes the power splitting ratio constraint. Problem (P1) is non-convex and it is difficult to solve (P1) with three variables (ρ, $\mathbf{w}_s$, $\mathbf{w}_p$), simultaneously.

3 Optimal solution

In this section, we propose a computationally efficient optimization scheme based on a two-stage procedure to solve the non-convex problem (P1). First, for any power splitting ratio ρ in the interval of $[0,1]$, we solve (P1) to attain the optimal secure beamforming ($\mathbf{w}_s^*$, $\mathbf{w}_p^*$); then the globally optimal solution ($\mathbf{w}_s^*$, $\mathbf{w}_p^*$, ρ^*) can be found by performing one-dimension search over ρ.

For a given ρ, by changing of $\mathbf{w}_p$ in terms of

$$\mathbf{w}_p := \sqrt{\rho P_p\|\mathbf{g}\|^4+\rho\|\mathbf{g}\|^2N_0+\|\mathbf{g}\|^2N_C}\,\mathbf{w}_p, \tag{13}$$

problem (P1) can be reformulated as (P2):

$$\begin{aligned}
&\max_{\rho,\mathbf{w}_s,\mathbf{w}_p}\ \frac{\left|\mathbf{h}_{ss}^{\dagger}\mathbf{w}_s\right|^2}{\left|\mathbf{h}_{ss}^{\dagger}\mathbf{w}_p\right|^2+\tilde{N}_0}\\
&\text{s.t.}\quad \mathrm{C1}: \frac{\left|\mathbf{h}_{sp}^{\dagger}\mathbf{w}_p\right|^2}{\left|\mathbf{h}_{sp}^{\dagger}\mathbf{w}_s\right|^2+\tilde{N}_0}\geqslant\tilde{\Gamma}_p,\\
&\qquad \mathrm{C2}: \frac{\left|\mathbf{h}_{ss_k}^{\dagger}\mathbf{w}_p\right|^2}{\left|\mathbf{h}_{ss_k}^{\dagger}\mathbf{w}_s\right|^2+\tilde{N}_0}\leqslant\tilde{\Gamma}_{SU_k},\\
&\qquad \mathrm{C3}: \left|\mathbf{w}_p\right|^2+\left|\mathbf{w}_s\right|^2\leqslant P_{s0}+\eta\left[(1-\rho)P_p\|\mathbf{g}\|^2+(1-\rho)N_0\right],
\end{aligned} \tag{14}$$

where $\tilde{\Gamma}_p=\frac{\left(\rho P_p\|\mathbf{g}\|^2+\rho N_0+N_C\right)\left(\Gamma_p-P_p\left|\mathrm{h}_{pp}\right|^2/N_0\right)}{\rho P_p\|\mathbf{g}\|^2-\left(\Gamma_p-P_p\left|\mathrm{h}_{pp}\right|^2/N_0\right)(\rho N_0+N_C)}$,
and $\tilde{\Gamma}_{SU_k}=\frac{\left(\rho P_p\|\mathbf{g}\|^2+\rho N_0+N_C\right)\left(\Gamma_{SU_k}-P_p\left|\mathrm{h}_{ps_k}\right|^2/N_0\right)}{\rho P_p\|\mathbf{g}\|^2-\left(\Gamma_{SU_k}-P_p\left|\mathrm{h}_{ps_k}\right|^2/N_0\right)(\rho N_0+N_C)}$.

Define $\mathbf{H}_{ss}=\mathbf{h}_{ss}\mathbf{h}_{ss}^{\dagger}$, $\mathbf{H}_{ss_k}=\mathbf{h}_{ss_k}\mathbf{h}_{ss_k}^{\dagger}$, $\mathbf{H}_{sp}=\mathbf{h}_{sp}\mathbf{h}_{sp}^{\dagger}$, $\mathbf{W}_p=\mathbf{w}_p\mathbf{w}_p^{\dagger}$, $\mathbf{W}_s=\mathbf{w}_s\mathbf{w}_s^{\dagger}$. By applying the Charnes-Cooper transformation [19], problem (P2) can be equivalently formulated as the following semi-definite relaxation (SDR) problem (P3):

$$\max_{\mathbf{w}_s,\,\mathbf{w}_p,\,\tau} \ \mathrm{Tr}\left(\mathbf{H}_{ss}\mathbf{W}_s\right)$$
$$\begin{aligned} s.t.\ \ & \mathrm{C1}: \mathrm{Tr}\left(\mathbf{H}_{ss}\mathbf{W}_p\right)+\tau\tilde{N}_0 = 1, \\ & \mathrm{C2}: \mathrm{Tr}\left(\mathbf{H}_{sp}\mathbf{W}_p\right)-\tilde{\Gamma}_p\mathrm{Tr}\left(\mathbf{H}_{sp}\mathbf{W}_s\right) \geqslant \tau\tilde{\Gamma}_p\tilde{N}_0, \\ & \mathrm{C3}: \mathrm{Tr}\left(\mathbf{H}_{ss_k}\mathbf{W}_p\right)-\tilde{\Gamma}_{e_k}\mathrm{Tr}\left(\mathbf{H}_{ss_k}\mathbf{W}_s\right) \leqslant \tau\tilde{\Gamma}_{e_k}\tilde{N}_0, \\ & \mathrm{C4}: \mathrm{Tr}\left(\mathbf{W}_p\right)+\mathrm{Tr}\left(\mathbf{W}_s\right) \leqslant \tau P_{s0}+ \\ & \qquad \tau\eta\left[(1-\bar{\rho})P_p\|\mathbf{g}\|^2+(1-\bar{\rho})N_0\right], \\ & \mathrm{C5}: \mathbf{W}_p \succeq 0, \mathbf{W}_s \succeq 0, \tau \geqslant 0. \end{aligned} \tag{15}$$

Note that SDR can't guarantee the optimal solution with rank-one. Nevertheless, we provide the method for constructing the optimal solutions with rank-one. Let λ, β, ∂_k and θ denote the dual variables of (P3) associated with C1-C4 respectively. Then the Lagrangian of problem (P3) is

$$L\left(\mathbf{W}_s,\mathbf{W}_p,\lambda,\beta,\partial_k,\theta\right) = \mathrm{Tr}\left(A_1\mathbf{W}_s\right)+\mathrm{Tr}\left(B_1\mathbf{W}_p\right)+\varsigma_1, \tag{16}$$

where

$$A_1 = \mathbf{H}_{ss}-\beta\tilde{\Gamma}_p\mathbf{H}_{sp}+\sum_{k=1}^{K}\partial_k\tilde{\Gamma}_{e_k}\mathbf{H}_{ss_k}-\theta\mathbf{I}, \tag{17}$$

$$B_1 = -\lambda\mathbf{H}_{ss}+\beta\mathbf{H}_{sp}-\sum_{k=1}^{K}\partial_k\mathbf{H}_{ss_k}-\theta\mathbf{I}, \tag{18}$$

We have the following proposition.

Proposition 3.1: The optimal solutions ($\mathbf{W}_s^*$, $\mathbf{W}_p^*$, τ^*) to problem (P3) for given ρ satisfy the following conditions:

1. $\mathrm{rank}\left(\mathbf{W}_p^*\right) = 1$;

2. $\mathbf{W}_s^* = \sum_{t=1}^{N-r} a_t\pi_t\pi_t^{\dagger} + buu^{\dagger}$, where $a_t \geqslant 0$, $\forall t$, $b > 0$ and $u \in \mathbb{C}^{N\times 1}$, $\|u\| = 1$, $u^{\dagger}\Upsilon = 0$;

3. According to 2, if $\mathrm{rank}\left(\mathbf{W}_s^*\right) > 1$, then we have the following sufficient condition to yield an optimal solution of $\mathbf{W}_s^*$ with rank-one:

$$\tilde{\mathbf{W}}_s^* = \mathbf{W}_s^* - \sum_{t=1}^{N-r} a_t\pi_t\pi_t^{\dagger}, \tag{19}$$

$$\tilde{\mathbf{W}}_p^* = \mathbf{W}_p^*, \tag{20}$$

$$\tilde{\tau}^* = \tau^*. \tag{21}$$

Proof Please refer to Appendix A.

Then, one-dimension search over ρ is performed to obtain the globally optimal solution (ρ^*, $\mathbf{W}_s^*$, $\mathbf{W}_p^*$) for (P3). The optimal secure beamforming ($\mathbf{w}_s^*$, $\mathbf{w}_p^*$) can be obtained by the eigenvalue decomposition (EVD) of $\mathbf{W}_s^*$ and $\mathbf{W}_p^*$. The detailed procedure is described in **Algorithm 1**.

Algorithm 1 The proposed optimal algorithm for problem (P3)

Define $\Delta\rho$ as the search step and **Initialize** $\rho = \bar{\rho}$.
1: **for** the given $\rho \in [0,1]$ **do** S_1-S_3
S_1: Solve problem (P3) and denote ($\mathbf{W}_s^*$, $\mathbf{W}_p^*$, τ^*) as the optimal solution to (P3);
S_2: Do the following procedures to obtain the rank-one solution $\mathbf{W}_s^*$ and $\mathbf{W}_p^*$,
if $\mathrm{rank}\left(\mathbf{W}_s^*\right) = 1$ and $\mathrm{rank}\left(\mathbf{W}_p^*\right) = 1$
The optimal value of problem (P3) is $(\mathbf{W}_s^*/\tau^*, \mathbf{W}_p^*/\tau^*)$;
else
Resort to Proposition (3.1) to construct a new solution ($\tilde{\mathbf{W}}_s^*$, $\tilde{\mathbf{W}}_p^*$, $\tilde{\tau}^*$) with $\mathrm{rank}\left(\tilde{\mathbf{W}}_s^*\right) = 1$ and $\mathrm{rank}\left(\tilde{\mathbf{W}}_p^*\right) = 1$ according to (19)-(21). Then, $(\tilde{\mathbf{W}}_s^*/\tilde{\tau}^*, \tilde{\mathbf{W}}_p^*/\tilde{\tau}^*)$ will be the optimal solution to (P3).
end if
S_3: Update $\rho = \rho + \Delta\rho$;
end for
2: **Choose** the optimal solution from the following equation (ρ^*, $\mathbf{W}_s^*$, $\mathbf{W}_p^*$) = arg $\max_{\rho\in[0,1]}$ problem(P3).
3: **Perform** the EVD of $\mathbf{W}_s^*$ and $\mathbf{W}_p^*$ to obtain the optimal solution (ρ^*, $\mathbf{w}_s^*$, $\mathbf{w}_p^*$).

4 Numerical results

In this section, we evaluate the performance of the proposed joint power splitting and secure beamforming design scheme. We assume that the ST is equipped with $N = 4$ antennas. We consider a scenario where the distances from the ST to all the other terminals are 2 m, while the distance from the PT to the PU is 4 m. The channel between a transmit-receive antenna pair is modeled as $h = (d)^{-\frac{\partial}{2}}e^{jw}$ [14], where d is the distance, ∂ is the path loss exponent, chosen as 3.5, and w is uniformly distributed over $[0, 2\pi)$. The variance of noise are normalized to unity, i.e., $N_0 = N_C = 1$. The primary power is set to be $P_p = 20$ dBm. The minimum SINR requirement for the PU is set to be $\Gamma_p = 10$ dBm. The maximum allowable SINR for the kth SU is set to be $\Gamma_{SU_k} = 0$ dBm, $\forall k = 1,\ldots,K$.

Fig. 3 shows the impact of the ST's initial energy on the average rate of the desired SU, when the energy conversion efficiency η is 0.5. Substantial rate gain is achieved by using the proposed scheme compared with the scheme without energy harvesting when the ST's initial energy is at the low energy region. The achievable rate of the schemes without energy harvesting is close to that of the proposed schemes when the ST's initial energy is at the high energy region. This is because the ST has sufficient energy to meet the communication requirement. We can conclude that the energy harvesting technique is useful in the energy-constrained case. It is also observed that the achievable rate of the de-

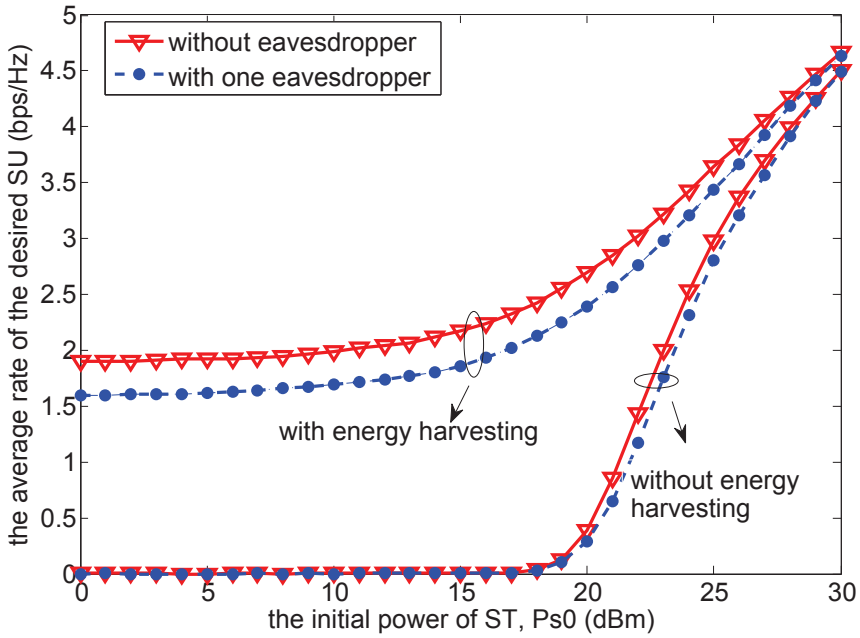

Fig. 3: the average rate of the desired SU vs the ST initial power

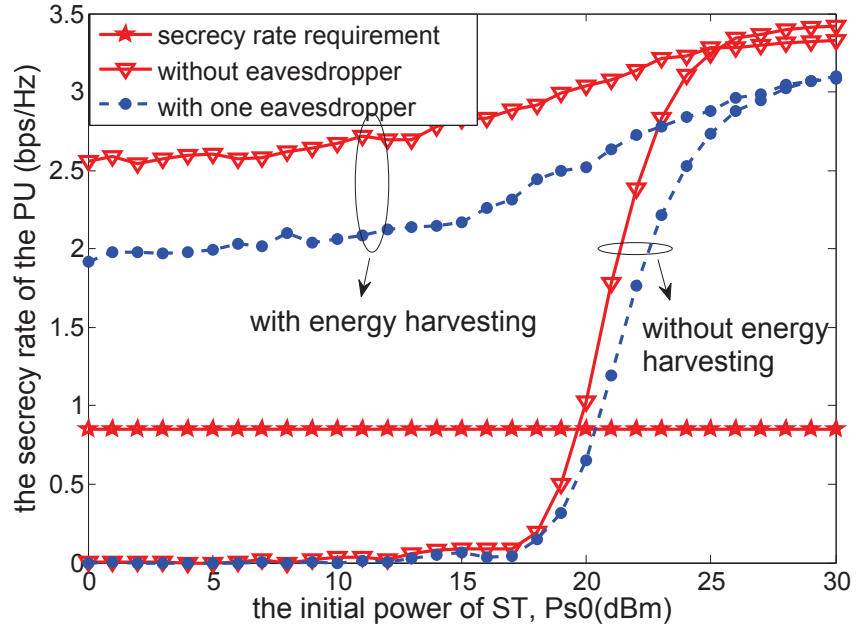

Fig. 4: the secrecy rate of the PU vs the ST initial power

sired SU without eavesdropper is higher than the case with one eavesdropper.

Fig. 4 shows the average secrecy rate of the PU corresponding to the ST's initial energy. The PU's secrecy rate requirement is 0.85 bps/Hz. It is noted that the PU's secrecy rate of the proposed schemes meets the requirement in the whole range of the ST's initial energy. In the schemes without energy harvesting, the PU's secrecy rate can't meet the requirement when the ST's initial energy is at the low energy region. The PU's secrecy rate is close to that of the proposed schemes with the increasing ST's initial energy, which further verifies the effectiveness of the proposed scheme. It is also observed that the PU secrecy rate without eavesdropper is higher than the case with one eavesdropper.

Fig.5 shows the average rate of the desired SU versus the number of potential eavesdroppers for the ST's initial power

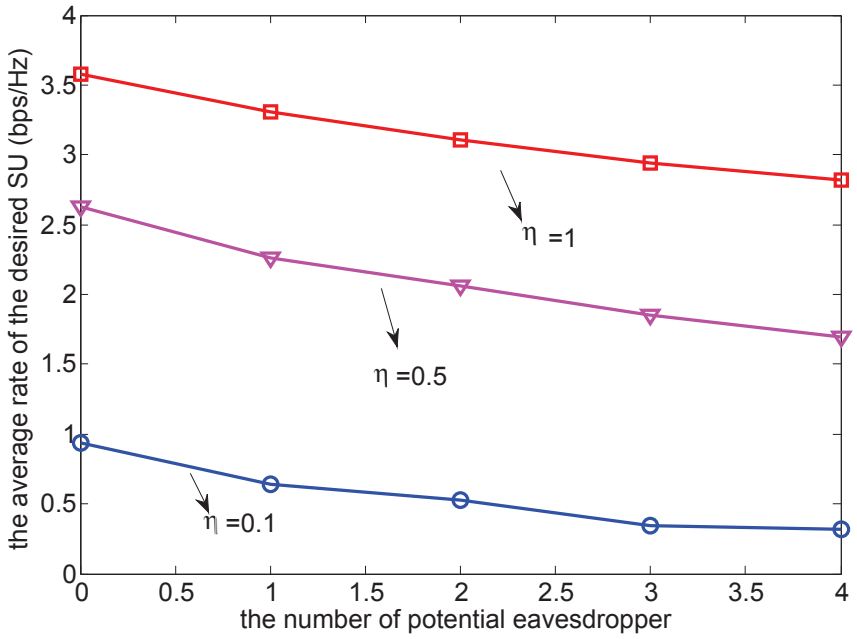

Fig. 5: the average rate of the SU vs the number of potential eavesdroppers

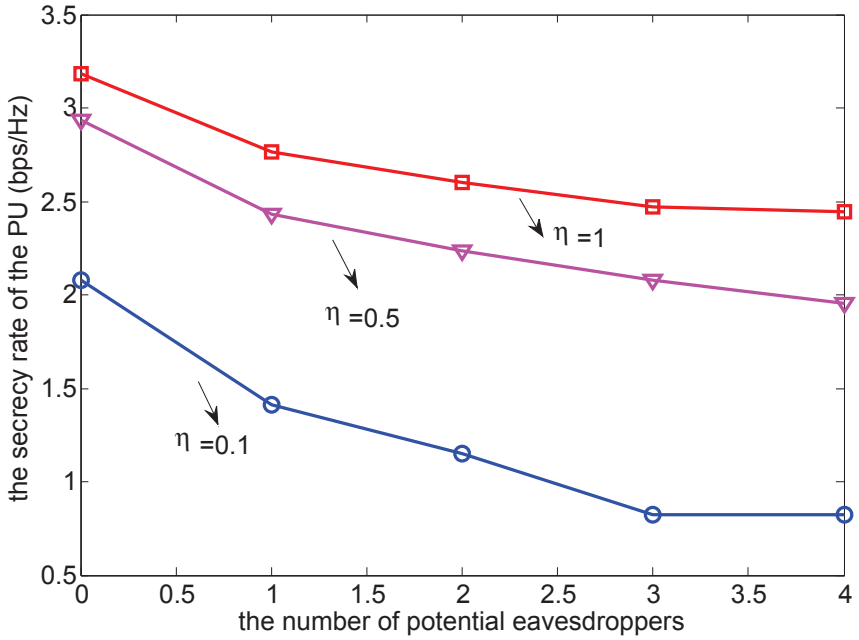

Fig. 6: the secrecy rate of the PU vs the number of potential eavesdroppers

$P_{s0} = 20$dBm and energy transfer efficiency η, takes values, 0.1, 0.5 and 1. We can see that the achievable rate of the desired SU decreases with the increasing number of eavesdroppers. This is because the probability that there exists much better wiretap links is high with the increasing number of eavesdroppers. As a result, more power is needed to defend against the eavesdroppers attack in order to guarantee the secrecy rate requirement. Furthermore, with the increasing of the energy transfer efficiency η, the ST can harvest more energy used to relay the primary confidential message and simultaneously transmit its own data, thus the average rate of the desired SU is improved.

Fig.6 depicts that the average secrecy rate of the PU decreases with the increasing number of potential eavesdrop-

pers. The higher energy transfer efficiency η can efficiently improve the PU's secrecy rate.

5 CONCLUSION

In this paper, we studied the security performance of the primary system in cloud-assisted CM2M networks when the ST is a low-energy device and the SUs are the potential eavesdroppers. We aimed to jointly design power splitting and secure beamforming to maximize the secondary M2M system data rate subject to the secrecy rate requirement of the primary system and the ST power constraint. An optimization algorithm based on a two-stage procedure was proposed to solve the complicated non-convex problem. Numerical results demonstrated that, when the ST's initial energy is at the low energy region, the proposed scheme achieves a significant transmission rate of the secondary M2M system while provides a high secrecy rate for the primary system compared to the scheme without energy harvesting.

Appendix A
PROOF OF PROPOSITION 3.1

The Karush-Kuhn-Tucker (KKT) conditions of problem (P3) are expressed as

$$A_1^*\mathbf{W}_s^* = 0,\ B_1^*\mathbf{W}_p^* = 0, \tag{22}$$

First, we show that rank $\left(\mathbf{W}_p^*\right) = 1$. The ST power constraint in (P3) is active with equality, it follows that the optimal dual variable $\theta^* > 0$. Since $\mathbf{H}_{ss} \succeq 0$ and $\mathbf{H}_{ss_k} \succeq 0$, we obtain rank $\left(-\lambda^*\mathbf{H}_{ss} - \partial_k^*\mathbf{H}_{ss_k} - \theta^*\mathbf{I}\right) = N$. Moreover, since rank$(\mathbf{H}_{sp}) \leqslant 1$, it follows from (18) that rank $(B_1^*) \geqslant N-1$. According to (22), we have rank $\left(\mathbf{W}_p^*\right) = 1$.

Next, we prove the second part of Proposition 3.1. Define

$$C_1^* = -\lambda^*\mathbf{H}_{ss} - \beta^*\tilde{\Gamma}_p\mathbf{H}_{sp} + \sum_{k=1}^{K}\partial_k^*\tilde{\Gamma}_{e_k}\mathbf{H}_{ss_k} - \theta^*\mathbf{I}, \tag{23}$$

Then we have

$$A_1^* = C_1^* + (\lambda^* + 1)\,\mathbf{H}_{ss}, \tag{24}$$

since $\theta^* > 0$, $\mathbf{H}_{ss} \succeq 0$, $\mathbf{H}_{ss_k} \succeq 0$ and $\mathbf{H}_{sp} \succeq 0$, we have rank $\left(-\lambda^*\mathbf{H}_{ss} - \beta^*\tilde{\Gamma}_p\mathbf{H}_{sp} - \theta^*\mathbf{I}\right) = N$. Without loss of generality, we define $r =$ rank (C_1^*) and the orthonormal basis of the null space of C_1^* as $\Upsilon \in \mathbb{C}^{N\times(N-r)}$ such that $C_1^*\Upsilon = 0$ and rank $(\Upsilon) = N-r$. Let $\pi_t \in \mathbb{C}^{N\times 1}$, $1 \leqslant t \leqslant N-r$, denote the tth column of Υ. We can express the optimal solution of W_s^* as

$$\mathbf{W}_s^* = \sum_{t=1}^{N-r} a_t\pi_t\pi_t^\dagger + buu^\dagger, \tag{25}$$

where $a_t \geqslant 0$, $\forall t$, $b > 0$ and $u \in \mathbb{C}^{N\times 1}$, $\|u\| = 1$, $u^\dagger\Upsilon = 0$.

Last, we prove the third part. For rank $(\mathbf{W}_s^*) > 1$, we construct another solution of the relaxed version of (P3), $\tilde{\mathbf{W}}_s^* = \mathbf{W}_s^* - \sum_{t=1}^{N-r} a_t\pi_t\pi_t^\dagger$, $\tilde{\mathbf{W}}_p^* = \mathbf{W}_p^*$, $\tilde{\tau}^* = \tau^*$. Then substituting them into the objective function and constraints in (P3) which achieves the same optimal value as the optimal solution and satisfies all the constrains. Thus, $\left(\tilde{\mathbf{W}}_s^*, \tilde{\mathbf{W}}_p^*, \tilde{\tau}^*\right)$ is also an optimal solution to (P3) but with rank $(\mathbf{W}_s^*) = 1$.

References

1. S. Whitehead (2004) Adopting wireless machine-to-machine technology. IEE Computing and Control Engineering J., 23(2):201-20
2. Y. Zhang et al. (2012) Cognitive machine-to-machine communciations: Visions and potentials for the smart grid. IEEE Netw., 26(3):6-13
3. S. Haykin (2005) Cognitive radio: Brain-empowered wireless communciations. IEEE JSAC, 23(2):201-220
4. J. F. Ding, R. Yu, Y. Zhang, S. Gjessing and D. H. K. Tsang (2015) Service provider competition and cooperation in cloud-based software defined wireless networks. IEEE Commun. Mag., 53(11):134-140
5. G. Wu, S. Talwar, K. Johnsson, N. Himayat and K. Johnson (2011) M2M:From mobile to embedded Internet. IEEE Commun. Mag., 49(4):36-43
6. A. K. Sadek, K. J. R. Liu and A. Ephremides (2007) Cognitive multiple access via coopeation: Protocol design and stability analysis. IEEE Trans. Inf. Theory, 53(10):3677-3696
7. X. Zhou, L. Song and Y. Zhang (2013) Physical layer security in wireless communications. CRC Press
8. I. Stanojev and A. Yener (2013) Improving secrecy rate via spectrum leasing for friendly jamming. IEEE Trans. Wireless Commun., 12(1):134-145
9. N. Zhang, N. Lu and X.S. Shen (2013) Cooperative spectrum access towards secure information transfer for CRNs. IEEE Jour. Select. Areas in Comm., 31(11):2453-2464
10. H. Jeon, S. W. Mclaughlin, I. M. Kim and J. Ha (2014) Secure communications with untrusted secondary nodes in cognitive radio networks. IEEE Trans. Wireless Commun., 13(4):1790-1805
11. F. Gabry, N. Schrammar, M. Girnyk, N. Li and R. Thobaben (2012) Cooperation for secure broadcasting in cognitive radio networks. IEEE ICC:1-8
12. A. A. Nasir, X. Y. Zhou, S. Durrani and R. A. Kennedy (2013) Relaying protocols for wireless energy harvesting and information processing. IEEE Trans. Wireless Commun., 12(7):3622-3636
13. S. Lee, R. Zhang and K.Huang (2013) Opportunistic wireless energy harvesting in cognitive radio networks. IEEE Trans. Wireless Comm., 12(9):4788-4799
14. G. Zheng, H. Z. Jorswieck and B. Ottersten (2014) Information and energy cooperation in cognitive radio networks. IEEE Trans. Signal Process., 62(9):2290-2303
15. A. A. Nasir, X. Y. Zhou, S. Durrani and R. A. Kennedy (2013) Relaying protocols for wireless energy harvesting and information processing. IEEE Trans. Wireless Commun., 12(7):3622-3636
16. R. Zhang and C. K. Ho (2013) MIMO broadcasting for simultaneous wireless information and power transfer. IEEE Trans. Wireless Comm., 12(5):1989-2001
17. Product Datasheet, 11667A Power Splitter, Agilent Technologies.
18. R. J. M. Vullers, R. V. Schaijk, I. Doms, C. V. Hoof and R. Mertens (2009) Micropower energy harvesting. Solid-State Electronics, 53(7):675-814
19. A. Charnes and W. W. Cooper (1962) Programming with linear fractional functions. Naval Res. Logist. Quarter., 9:181-186