SCHOOL of ELECTRONIC ENGINEERING and COMPUTER SCIENCE

Secure D2D Communication in Large-Scale Cognitive Cellular Networks with Wireless Power Transfer

Speaker: Yuanwei Liu

Email: yuanwei.liu@qmul.ac.uk

Queen Mary
University of London

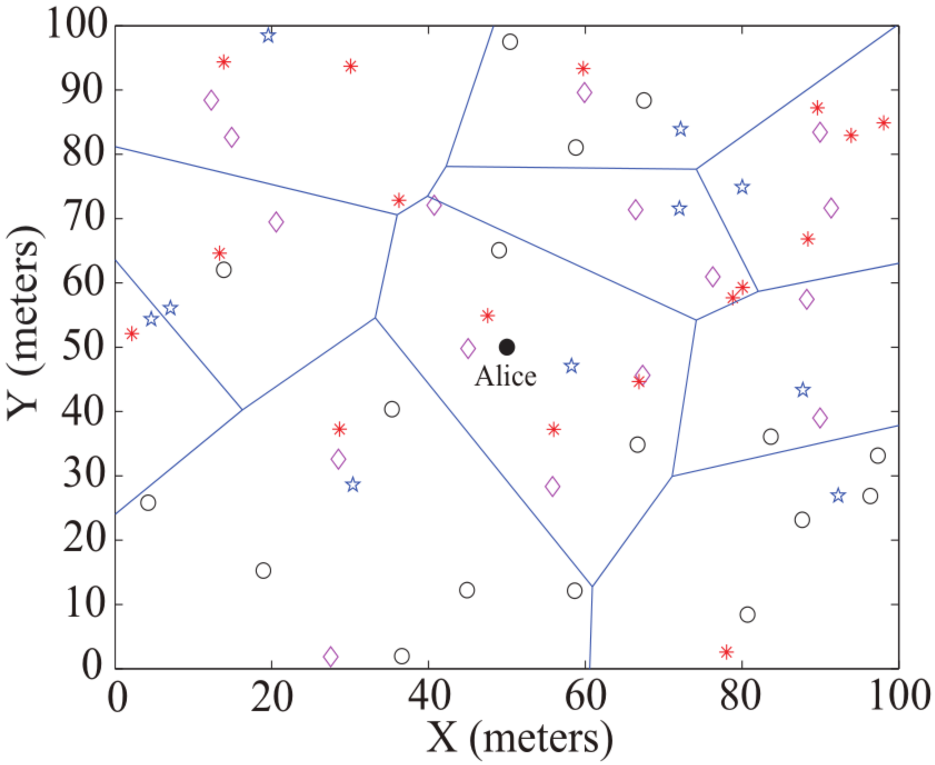
Outlines of Presentation

- Introduction
- System Model
- Analytical Results
- Numerical Examples
- Conclusions

Introduction

- Secure device-to-device (D2D) communication in energy harvesting large-scale cognitive cellular networks.
- New power transfer policy: best power beacon (BPB) power transfer.
- Two receiver selection schemes: 1) best receiver selection (BRS), and 2) nearest receiver selection (NRS).
- New closed-form expressions for the exact power outage probability and the asymptotic power outage probability with large antenna arrays at PBs.
- New expressions for the secrecy throughput considering the two receiver selection schemes using the BPB power transfer policies.

System Model



An example of a part of a network snapshot considering that the spatial distributions of

PBs： pink diamonds

Bobs：empty circles

BSs： blue five-pointed stars

Eves： red stars

follow homogeneous Poisson point processes (PPP).

Power Transfer Model

The harvested energy of Alice from the PB can be obtained as follows

$$E_H = \eta P_S \max_{p \in \Phi_p} \left\{ \left\| \mathbf{h}_p \right\|^2 L\left(r_p\right) \right\} (1-\beta) T,$$

The maximum transmit power at Alice is given by

$$P_H = \max_{p \in \Phi_p} \left\{ \left\| \mathbf{h}_p \right\|^2 L\left(r_p\right) \right\} \frac{\eta P_S \left(1-\beta\right)}{\beta}.$$

Information Signal Model

The transmit power at Alice is strictly constrained by the maximum transmit power at Alice and the peak interference power at cellular BSs according to

$$P_A = \min\left\{ \frac{I_p}{\max\limits_{\ell \in \Phi_\ell} \left\{ |h_\ell|^2 L\left(r_\ell\right) \right\}}, P_{\mathrm{t}} \right\},$$

The instantaneous signal-to-noise ratio (SNR) at the selected Bob for BRS and NRS is expressed as

$$\gamma_{\mathrm{B}} = \frac{P_A}{N_0} \max_{b \in \Phi_b} \left\{ |h_b|^2 L\left(r_b\right) \right\} \quad \gamma_{\mathrm{B}^*} = \frac{P_A}{N_0} |h_{b^*}|^2 \max_{b \in \Phi_b} L\left(r_b\right)$$

Power Outage Probability

- **Exact analysis for power transfer**

$$H_{out} = e^{\frac{-\lambda_p \pi \delta}{\mu^{\delta}} \sum_{m=0}^{M-1} \left(\frac{\Gamma(m+\delta)}{m!} \right)},$$

- **Large antenna array analysis for power transfer with** $M \to \infty$

$$H_{out}^{large} = e^{-\frac{\lambda_p \pi}{\theta^{\delta}}},$$

With the help of using law of large numbers below

$$||\mathbf{h}_p||^2 \overset{a.s.}{\to} M,$$

Queen Mary
University of London

Secrecy Throughput

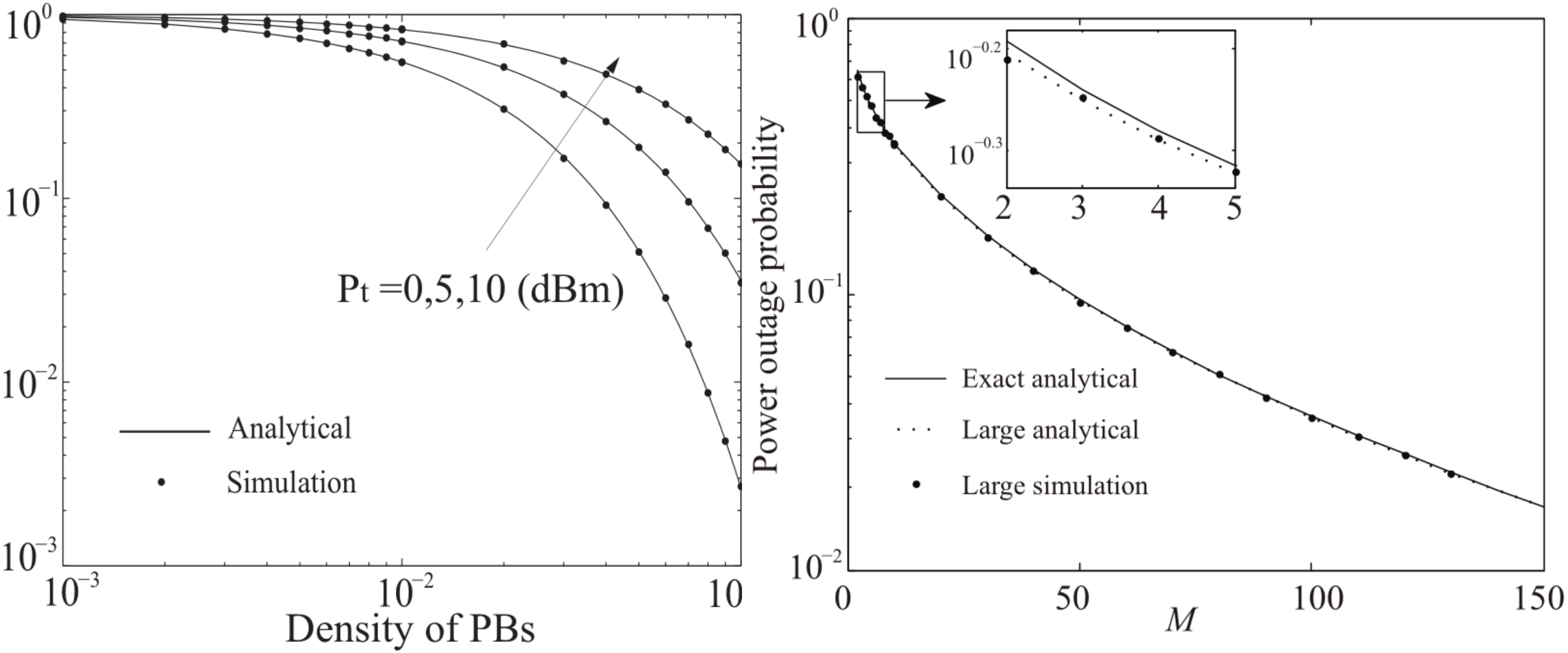
- **The instantaneous secrecy rate is defined as**

$$C_s^{\mathrm{BRS}} = \left[\log_2\left(1+\gamma_B\right) - \log_2\left(1+\gamma_E\right)\right]^+$$

- **The secrecy throughput using BPB power transfer policy is given by**

$$C_s^{\mathrm{BRS}} = \left(1-H_{out}\right)\frac{\beta}{\ln 2}$$
$$\times\left(\int_0^\infty \frac{\omega_\ell}{\overline{\gamma}_p^{\,\delta}\left(1+x_2\right)}\left(\frac{1}{Q_2}-\frac{1}{Q_3}+\frac{e^{-\overline{\gamma}_0^{\,\delta}Q_3}}{Q_3}-\frac{e^{-\overline{\gamma}_0^{\,\delta}Q_2}}{Q_2}\right)+\frac{e^{-\frac{\omega_\ell\overline{\gamma}_0^{\,\delta}}{\overline{\gamma}_p^{\,\delta}}-\frac{\omega_E\overline{\gamma}_0^{\,\delta}}{x_2^\delta}}}{1+x_2}\left(1-e^{-\frac{\omega_B\overline{\gamma}_0^{\,\delta}}{x_2^\delta}}\right)dx_2\right)$$

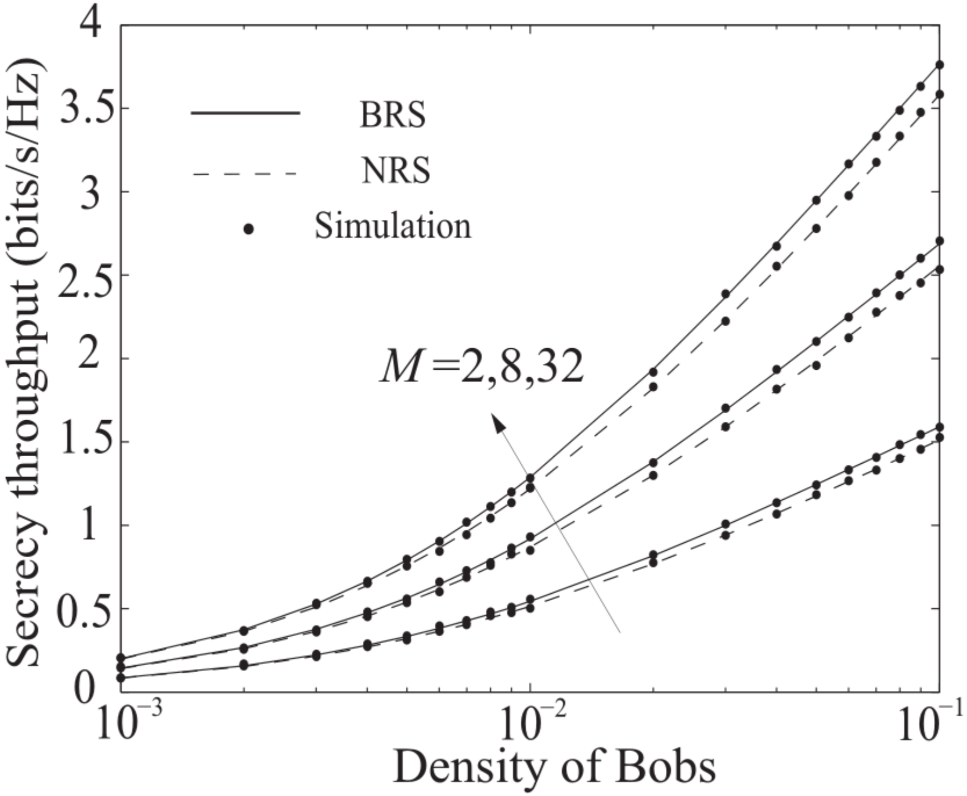
Numerical Results

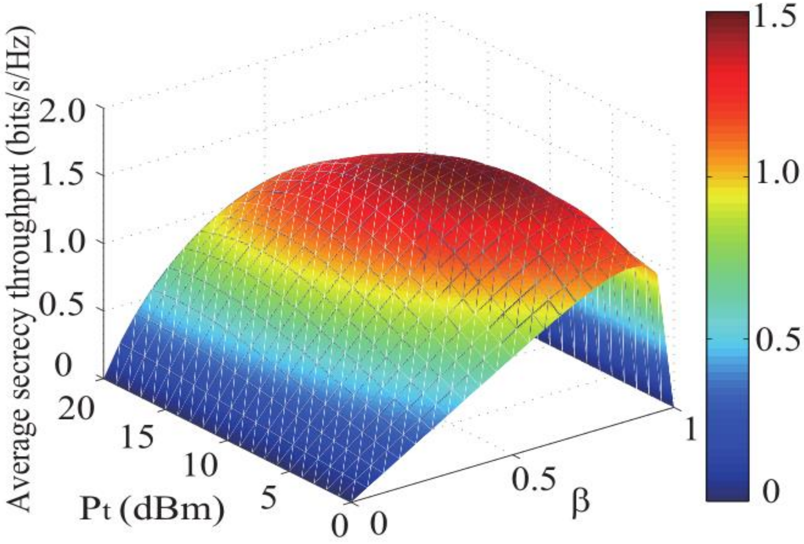


- Power outage probability versus density of PBs
- Power outage probability versus M for large antenna array analysis

`

Numerical Results





(a) BRS scheme

- Secrecy throughput versus density of Bobs

- Secrecy throughput of BRS versus and power threshold

Conclusions

- We proposed a novel wireless power transfer policy in the power transfer model, namely, best power beacon power transfer. We also considered best receiver selection and nearest receiver selection schemes in the information signal model.
- New analytical expressions in terms of power outage probability and secrecy throughput are derived to determine the system security performance.
- We show that secrecy performance improves with increasing densities of PBs and D2D receivers because of a larger multiuser diversity gain.
- A pivotal conclusion is reached that BRS achieves better secrecy performance than NRS but demands more instantaneous feedback and overhead.

Thank you!