Security Analysis of Cooperative Jamming in Internet of Things with Multiple Eavesdroppers

Xin **Fan**, Yan **Huo**

Beijing Jiaotong University, Beijing, China

E-mail: {fanxin, yhuo}@bjtu.edu.cn

Outline

Introduction

- **Why do we exploit Physical Layer Security in IoT?**
  - ***High complexity*** of cryptography-based methods is not inapplicable in the IoT devices with limited computation and communication capabilities;
  - ***Difficulties in key management*** exist in cryptography-based security mechanisms due to high heterogeneous and dynamic IoT systems;
  - ***Inflexible security-level configuration*** is hard to support different security levels of various devices.

Introduction

- **What is Physical Layer Security?**
  - Achieve the **error-free** transmission between users in the network;
  - Exploit the **characteristics** of wireless medium to ensure that eavesdroppers cannot obtain the transmission information;
  - Provide **an additional layer of protection** without compromising the existing cryptographic-technique-based security protection.

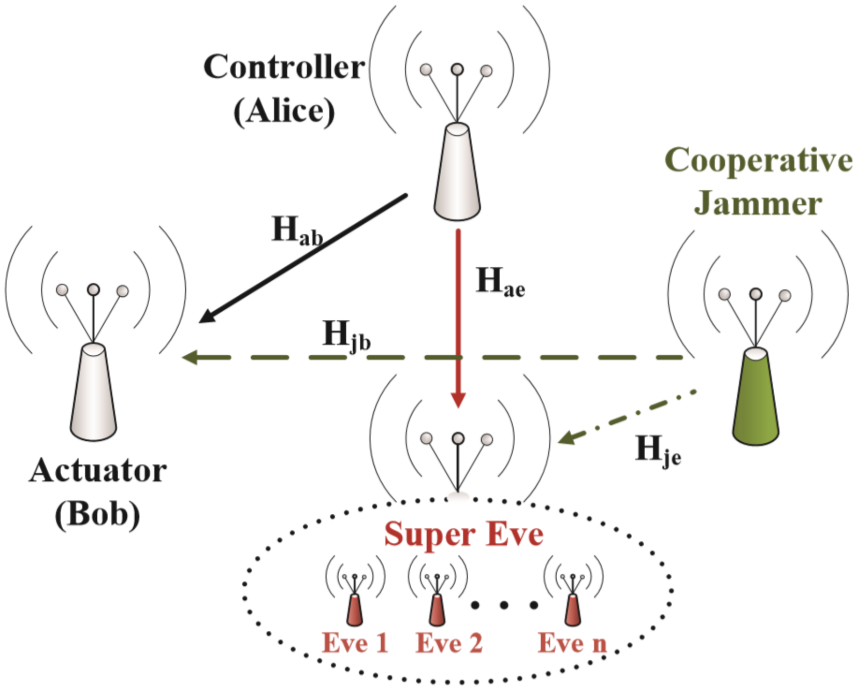
Cooperative Jamming: use artificial noise (**AN**) generated by friendly neighboring nodes to degrade the quality of received signals at eavesdroppers.

Introduction

- **What are the characteristics of our work compared with the existing schemes?**
  - All the considered nodes are equipped with **multi-antenna**;
  - **Multiple passive collusive eavesdroppers** that they can work together to the ability to eavesdrop;
  - The channel state information (**CSI**) of the eavesdroppers **cannot be obtained**.
- For the above meaningful scenarios, we design a secure transmission scheme and analyze the security performance.

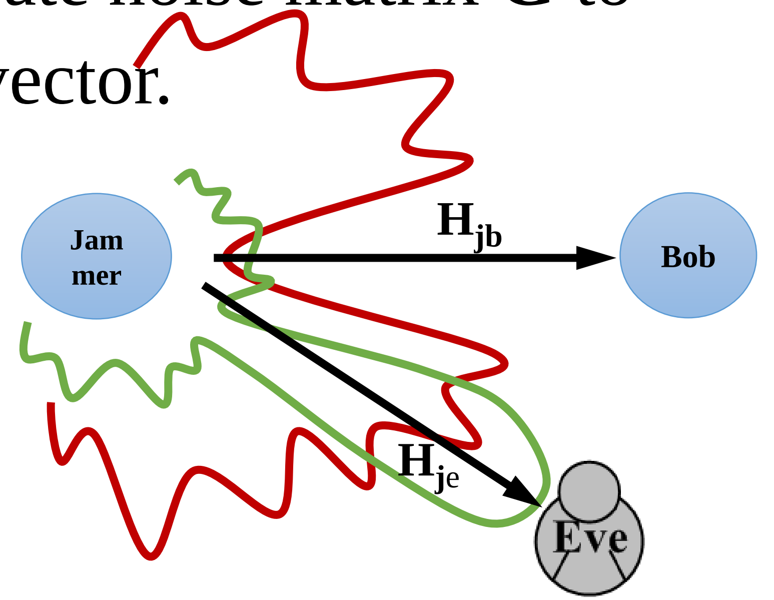
System Model

- A controller (Alice) sends private information to an actuator (Bob).
- One or more passive eavesdroppers (Eves) can conspire to eavesdrop on the information.
- A selected node (called as Jammer) broadcasts AN to confuse the eavesdroppers.
- Alice, Bob and Jammer are equipped with N_a, N_b and N_j antennas.
- These collusive eavesdroppers are treated as a super eavesdropper (S-Eve) with N_e antennas.
- Perfect CSIs from Alice and Jammer to Bob are available, but to S-Eve cannot be known.
- How to design a secure transmission scheme?



System Model

- **Challenges**
  - Without Eves’ CSI, we can't generate directional jamming (i.e., **Green**)
  - The jamming should be injected into the null-subspace of the intended receiver's channel (**Red**)
  - If single-antenna, we can generate noise matrix **G** to make $\mathbf{G}\mathbf{h}_{jb}=\mathbf{0}$, because $\mathbf{h}_{jb}$ is a vector.
  - However, with multiple antenna, we can’t make $\mathbf{G}\mathbf{H}_{jb}=\mathbf{0}$.



System Model

- Received signals at Bob:

AWGN at Bob

$$\mathbf{y}_b = \sqrt{P_a}\mathbf{H}_{ab}\mathbf{w}s_a + \sqrt{P_j}\mathbf{H}_{jb}\mathbf{z}s_z + \mathbf{n}_b, \qquad (1)$$

The transmit power of Alice

The AN vector transmitted by Jammer

The transmit power of Jammer

The precoding vector transmitted by Alice

- To eliminate the effect of AN:

The decoding vector used by Bob

$$r_b = \mathbf{d}_b\mathbf{y}_b = \sqrt{P_a}\mathbf{d}_b\mathbf{H}_{ab}\mathbf{w}s_a + \sqrt{P_j}\mathbf{d}_b\mathbf{H}_{jb}\mathbf{z}s_z + \mathbf{d}_b\mathbf{n}_b, \quad (3)$$

- SINR at Bob are given by

$$SINR_b = \frac{P_a \mid \mathbf{d}_b\mathbf{H}_{ab}\mathbf{w} \mid^2}{P_j \mid \mathbf{d}_b\mathbf{H}_{jb}\mathbf{z} \mid^2 + 1}. \qquad (4)$$

System Model

- To maximize Bob's SINR, a joint optimization problem **P1** needs to be solved

$$\textbf{P1:}\quad \{\mathbf{d}_b, \mathbf{w}, \mathbf{z}\} = \arg \max_{\mathbf{d}_b, \mathbf{w}, \mathbf{z}} \frac{P_a \mid \mathbf{d}_b \mathbf{H}_{ab} \mathbf{w} \mid^2}{P_j \mid \mathbf{d}_b \mathbf{H}_{jb} \mathbf{z} \mid^2 + 1}. \tag{5}$$

- The solutions can be given by the following **Lemma 1**.

Lemma 1. *When* $\mathbf{H}_{ab}$ *has a form of SVD as* $\mathbf{H}_{ab} = \mathbf{USV}^H$, *the solution of* $\{\mathbf{d}_b, \mathbf{w}, \mathbf{z}\}$ *can be calculated as follows.*

$$\mathbf{d}_b = \text{the first row of } \mathbf{U}^H, \tag{6}$$

$$\mathbf{w} = \text{the first column of } \mathbf{V}, \tag{7}$$

$$\mathbf{z} = \left(\mathbf{I}_{N_j} - \frac{\mathbf{H}_{jb}^H \mathbf{d}_b^H \mathbf{d}_b \mathbf{H}_{jb}}{\| \mathbf{d}_b \mathbf{H}_{jb} \|^2} \right) \mathbf{a}, \tag{8}$$

System Model

- The maximum ratio combining (MRC) weight can be given by

$$\boldsymbol{\varpi} = (\mathbf{H}_{ae}\mathbf{w})^H = \mathbf{w}^H\mathbf{H}_{ae}^H. \tag{10}$$

- Then the output signal after MRC at S-Eve is given by

$$\mathbf{r}_e = \boldsymbol{\varpi}\mathbf{y}_e = \sqrt{P_a}\boldsymbol{\varpi}\mathbf{H}_{ae}\mathbf{w}s_a + \sqrt{P_j}\boldsymbol{\varpi}\mathbf{H}_{je}\mathbf{z}s_z + \boldsymbol{\varpi}\mathbf{n}_e. \tag{11}$$

- Accordingly, we can get the SINR at S-Eve

$$\begin{aligned} SINR_e &= \frac{P_a \mid \boldsymbol{\varpi}\mathbf{H}_{ae}\mathbf{w} \mid^2}{P_j \mid \boldsymbol{\varpi}\mathbf{H}_{je}\mathbf{z} \mid^2 + \mid \boldsymbol{\varpi} \mid^2} \\ &= \frac{P_a \mid \boldsymbol{\varpi} \mid^2}{P_j \mid \boldsymbol{\psi} \mid^2 + 1} = \frac{X}{Y+1}, \end{aligned} \tag{12}$$

Secrecy Analysis

- Exploiting the well-known Wyners wiretap code, the achievable secrecy rate for Bob can be given by

$$R_s = \max\{R_b - R_e, 0\}, \qquad (13)$$

- where

$$R_b = \log(1 + SINR_b) \text{ and } R_e = \log(1 + SINR_e), \qquad (14)$$

are the achievable rate of Bob and S-Eve.

We employ **Secrecy Outage Probability** (SOP) to evaluate the secrecy performance

Secrecy Analysis

- The SOP is

$$\begin{aligned}\varepsilon &= Pr\{R_s < R_{th}\} = Pr\{R_b - R_e < R_{th}\}\\ &= Pr\{R_e > R_b - R_{th}\} = Pr\{SINR_e > 2^{R_b - R_{th}} - 1\}\\ &= \overline{F}_{SINR_e}(2^{R_b - R_{th}} - 1),\end{aligned} \tag{15}$$

- where $\overline{F}_{SINR_e}(x) \triangleq Pr(SINR_e > x)$ is the complementary cumulative distribution function (CCDF) of $SINR_e$.
- **Challenge:** It is very difficult to calculate the multiple integrals to derive the closed-form expressions of the SOP.

Secrecy Analysis

Proposition 1. *The closed-form of the CCDF of $SINR_e$ can be calculated as*

$$\begin{aligned}\overline{F}_{SINR_e}(\tau) =& \frac{1}{P_j}\exp\left(-\frac{\tau}{P_a}\right)\sum_{k=0}^{N_e-1}\frac{1}{k!}\left(\frac{\tau}{P_a}\right)^k \\ &\times\sum_{i=0}^{k}C_k^i\left(\frac{\tau}{P_a}+\frac{1}{P_j}\right)^{-i-1}\Gamma(i+1),\end{aligned} \quad (16)$$

where $\tau > 0$ *and* $C_k^i = \frac{k!}{i!(k-i)!}$.

- The SOP: $\varepsilon(\mu) = \overline{F}_{SINR_e}(\mu)$. (17)

Proposition 2. *The closed-form expression for SOP without Jammer can be calculated as*

$$\varepsilon^{NJ}(\mu) = \exp\left(-\frac{\mu}{P_a}\right)\sum_{k=0}^{N_e-1}\frac{1}{k!}\left(\frac{\mu}{P_a}\right)^k. \quad (18)$$

Secrecy Analysis

Property 1. *The asymptotic expressions of* $\varepsilon(N_e)$ *and* $\varepsilon^{NJ}(N_e)$ *for the infinite value of* N_e *can be given by*

$$\varepsilon(N_e) \xrightarrow[N_e]{a.s.} 1, \tag{21}$$

$$\varepsilon^{NJ}(N_e) \xrightarrow[N_e]{a.s.} 1. \tag{22}$$

- ***Remark 1*: Property 1** implies that secure transmission can be completely interrupted, even with a Jammer, as long as the number of antennas of S-Eve is sufficient.

Secrecy Analysis

Property 2. *The asymptotic expressions of* $\varepsilon(P_a)$ *and* $\varepsilon^{NJ}(P_a)$ *for the infinite value of* P_a *can be given by*

$$\varepsilon(P_a) \xrightarrow[P_a]{a.s.} \frac{\sum_{k=0}^{Ne-1}\sum_{i=0}^{k}\frac{\overrightarrow{\varsigma}^{k-i}}{(k-i)!}\overrightarrow{\zeta}^{i}}{e^{N_e\overrightarrow{\varsigma}}P_j}, \tag{23}$$

$$\varepsilon^{NJ}(P_a) \xrightarrow[P_a]{a.s.} \exp\left(-\overrightarrow{\varsigma}\right)\sum_{k=0}^{N_e-1}\frac{1}{k!}\overrightarrow{\varsigma}^{k}, \tag{24}$$

where $\overrightarrow{\varsigma} = \frac{\lambda_{\max}^2}{2^{R_{th}}}$ *and* $\overrightarrow{\zeta} = \frac{\overrightarrow{\varsigma}}{\overrightarrow{\varsigma}+\frac{1}{P_j}}$.

- ***Remark 2:*** **Property 2** demonstrates that only increasing transmit power of Alice is not always beneficial to the secrecy performance of the network.

Secrecy Analysis

Property 3. *When* $\mu > 0$, $\varepsilon(P_j)$ *decreases monotonously as the increase of* P_j *and finally converges to 0 for the infinite value of* P_j, *i.e.,*

$$\varepsilon(P_j) \xrightarrow[P_j]{a.s.} 0. \tag{25}$$

- ***Remark 3*: Property 3** theoretically confirms that SOP can be significantly reduced as long as the cooperative jamming power is sufficient.

Numerical Results

- We set the power of AWGN to 1 mw,
- Na = Nb = Nj = 4,
- Rth = 6 bit/s/Hz.

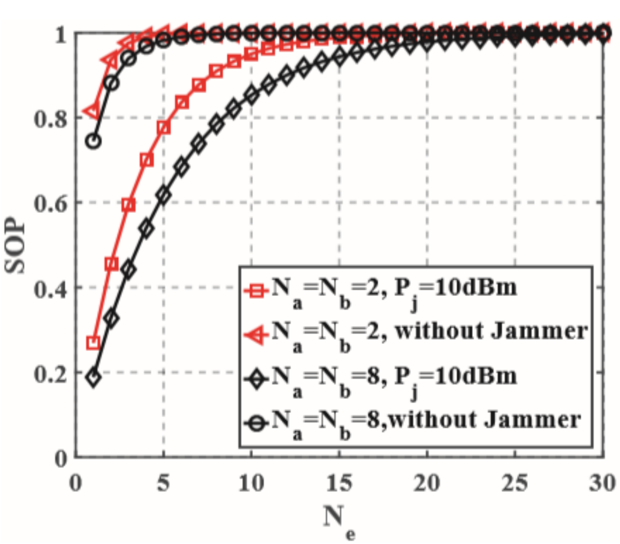


Fig. 2: SOP *vs.* N_e with $P_a = 30dBm$.

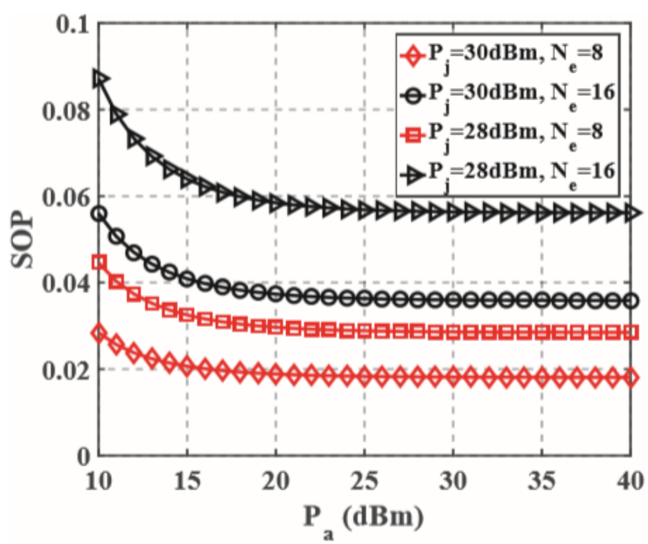


Fig. 3: ε *vs.* P_a with Jammer.

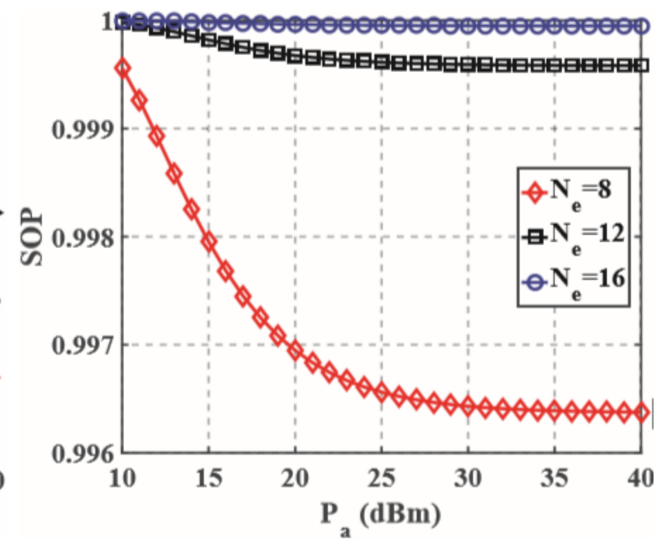


Fig. 4: ε^{NJ} *vs.* P_a without Jammer.

Numerical Results

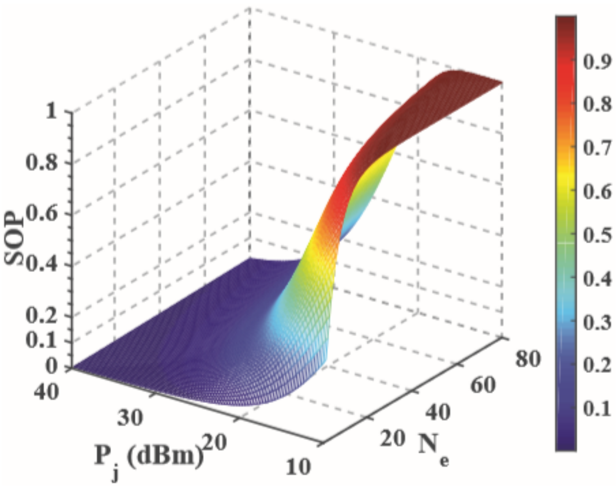


Fig. 5: ε over (P_j, N_e) with $P_a = 30$dBm.

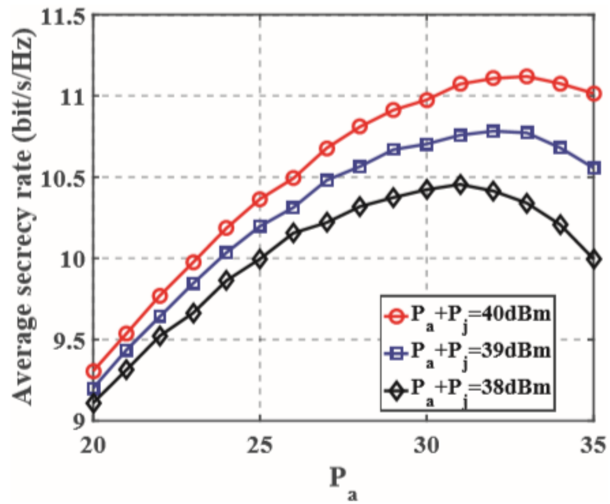


Fig. 6: ASR *vs.* P_a with $N_e = 16$.

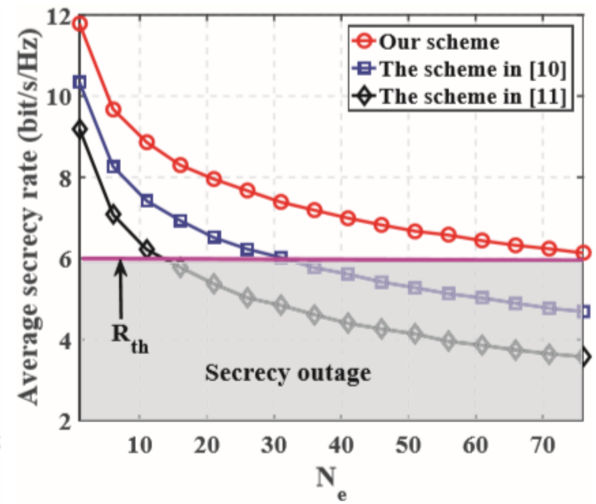


Fig. 7: Comparison of performance.

[10] L. Hu, H. Wen, B. Wu, F. Pan, R. Liao, H. Song, J. Tang, and X. Wang, "Cooperative jamming for physical layer security enhancement in Internet of Things," IEEE Internet of Things Journal, vol. 5, no. 1, pp. 219–228, Feb 2018.
[11]Y. Zhang, Y. Shen, H. Wang, J. Yong, and X. Jiang, "On secure wireless communications for IoT under eavesdropper collusion," IEEE Transactions on Automation Science and Engineering, vol. 13, no. 3, pp. 1281–1293, July 2016.

Conclusion

- We propose a CJ scheme for IoT systems to fight against multiple passive and collusive eavesdroppers of unknown CSIs.
- The actuator maximizes its receiving SINR by using SVD and ZFBF while the collusive eavesdroppers enhance their SINR by utilizing the MRC technology.
- We derive the closed-form expressions of the SOP with and without CJ, respectively.
- We provide the asymptotic analysis to explore the impact of various system parameters on the SOP.
- In the future, we intend to study the optimization problem of power allocation with the constraint of the limited total power since IoT devices are generally energy-constrained.

THANK YOU

Xin FAN

Wireless Network and Information Perception Center (WNIP)

School of Electronic and Information Engineering, Beijing Jiaotong University

Telephone: 86 15652955761

Email: fanxin@bjtu.edu.cn