Proactive Wireless Surveillance Techniques with Cooperative Jamming

Professor Inkyu Lee

Wireless Communication Lab
School of Electrical Engineering
Korea University

February 18, 2020

Speaker Profile

Education

- 90' BSEE, Seoul National University, Dept. of Control & Inst.
- 92' MS, Stanford University, Dept. of Elec. Eng.
- 95' Ph.D, Stanford University, Dept. of Elec. Eng.

Experience

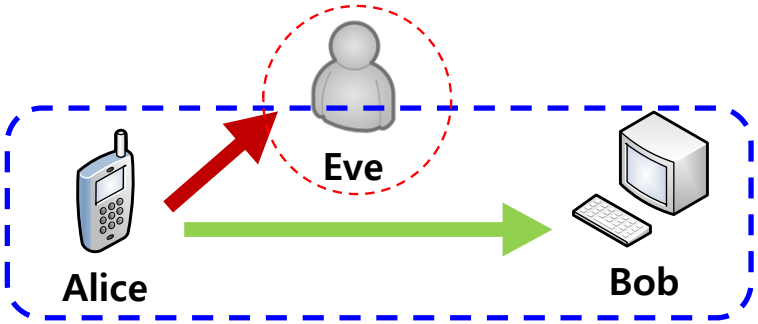
- '95~'02 Member of Technical Staff, AT&T Bell Lab, Lucent Technologies
- '02~present Professor, School of Elec. Eng., Korea University
- '01~'11 IEEE Transactions on Communications, Associate Editor
- '07~'11 IEEE Transactions on Wireless Communications, Associate Editor
- '06 IEEE Journal on Selected Areas in Communications, Chief Editor (Special issue on 4 G systems)
- '17~present IEEE Distinguished Lecturer
- '19~present Department Head, School of Elec. Eng., Korea University

Awards

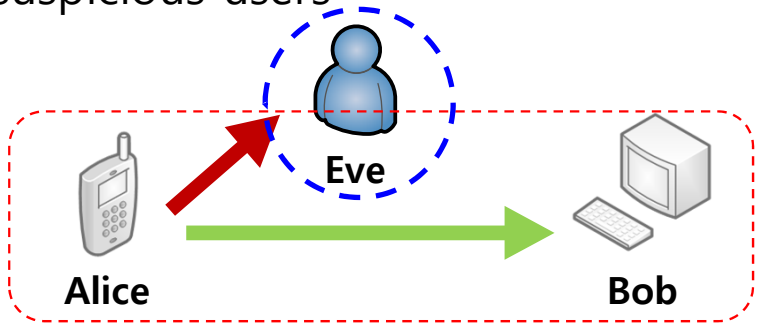
- Fellow, IEEE
- Member, National Academy of Engineering in Korea
- Korea Engineering Award, National Research Foundation of Korea (NRF)

Motivation

- **Conventional secrecy in wireless communications**
  - Exponentially growth of interest in securing data transmission over the last few years.
    - Decentralized networks
    - Massive connections in the upcoming 5G
    - Advanced cyber terrorism (e.g., DoS and Ransomware)
  - Physical layer security techniques
    - To achieve perfect wireless secrecy against malicious eavesdropping attacks
    - To preserve the confidentiality of wireless communications
  - Assumptions in the system model so far
    - Communication users → legitimate nodes
    - Eavesdroppers → Illegitimate nodes



- **A new line of secrecy: Legitimate eavesdropping**
  - Paradigm shift
    - Communication links possibly used for illegal purpose (e.g. criminals or terrorists)
    - Growing need for government agencies to legitimately monitor the suspicious communication links
    - Communication users → Illegitimate nodes
    - Eavesdroppers → legitimate monitoring nodes
  - Purpose of legitimate eavesdropping
    - To intercept as much information as possible from suspicious users
    - To proactively react to the potential illegal activities

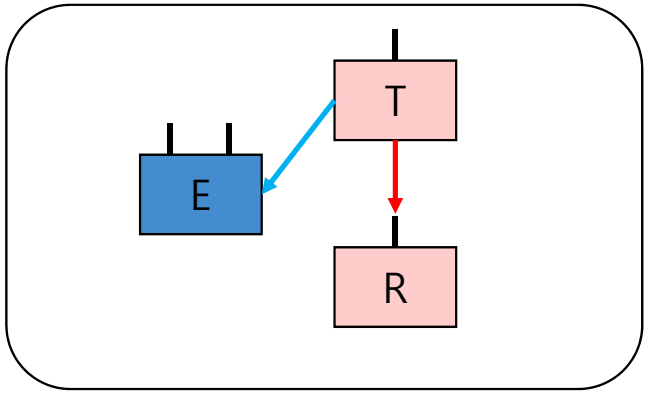


- **Methods of eavesdropping**
  - Passive eavesdropping
    - A legitimate monitor only listening to the suspicious communications
    - Effective only when $C_{Eavesdropping} \geq R_{Suspicious}$
    - Not always feasible…
      (e.g. a monitor located far away from the suspicious pair, $C_{Eavesdropping} < R_{Suspicious}$)
  - Proactive eavesdropping
    - A legitimate monitor proactively changing the channel condition by jamming
    - Purpose of conventional jamming:
      - To disrupt or disable enemy communications
    - Purpose of jamming for proactive eavesdropping:
      - To control the channel condition so that the monitor can reliably decode the eavesdropped data.

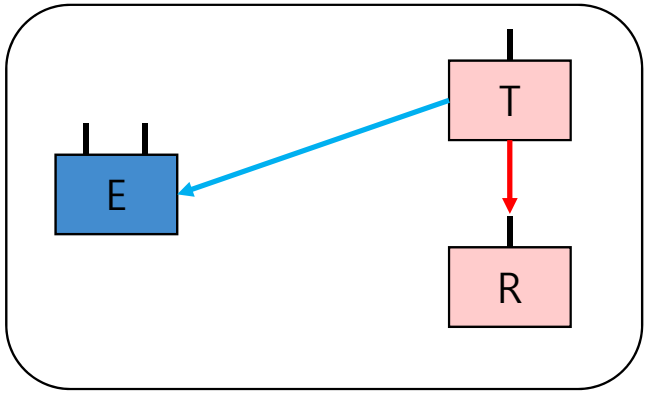
$$C_{Eavesdropping} < R_{Suspicious} \Rightarrow \text{Jamming} \Rightarrow R_{Suspicious} \downarrow \Rightarrow C_{Eavesdropping} \geq R_{Suspicious}$$

- **Role of jamming in proactive eavesdropping**

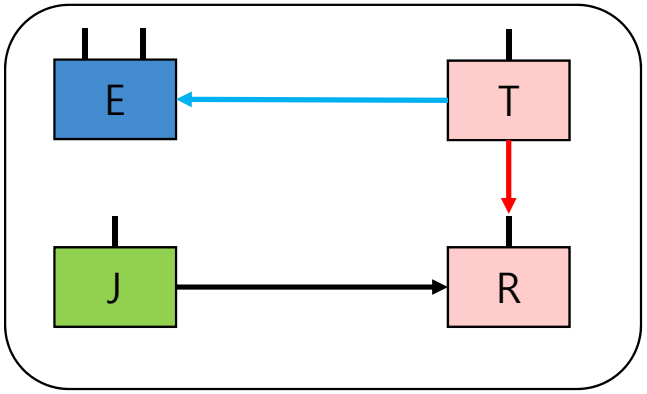
Close eavesdropping



Passive distant eavesdropping



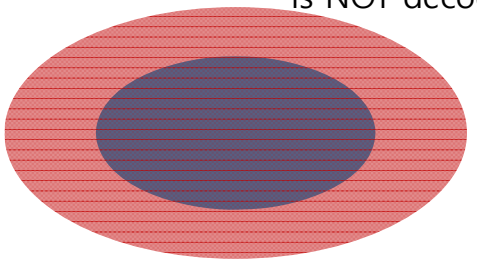
"Proactive" distant eavesdropping



Eavesdropping channel capacity

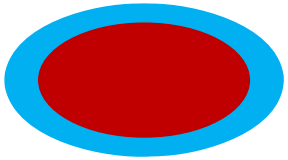
$C_{Eavesdropping} \geq R_{Suspicious}$

Eavesdropped info.
Is NOT decodable…



$C_{Eavesdropping} < R_{Suspicious}$

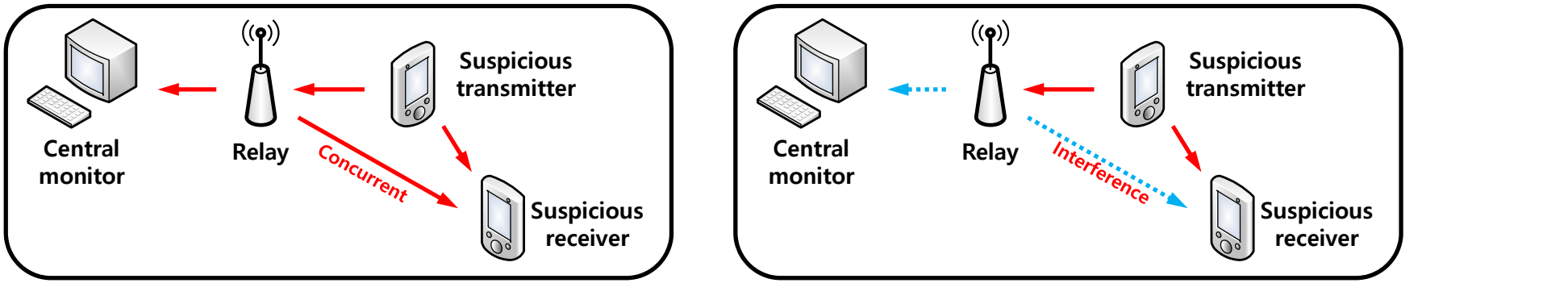
Eavesdropped info.
becomes decodable!



$C_{Eavesdropping} \geq R_{Suspicious}$

Introduction

- **Relay-assisted proactive eavesdropping**
  - Common assumptions in literature [JXu:17b, CZhong:17]
    - Existence of a direct link between the monitor and the suspicious users
      - Possibly infeasible in practice (e.g., covert surveillance operation from a far distance)
      - → Intermediate relays required
  - Two practical considerations for relays [TRiihonen:09]



Negligible relay processing delay [YZeng:16]

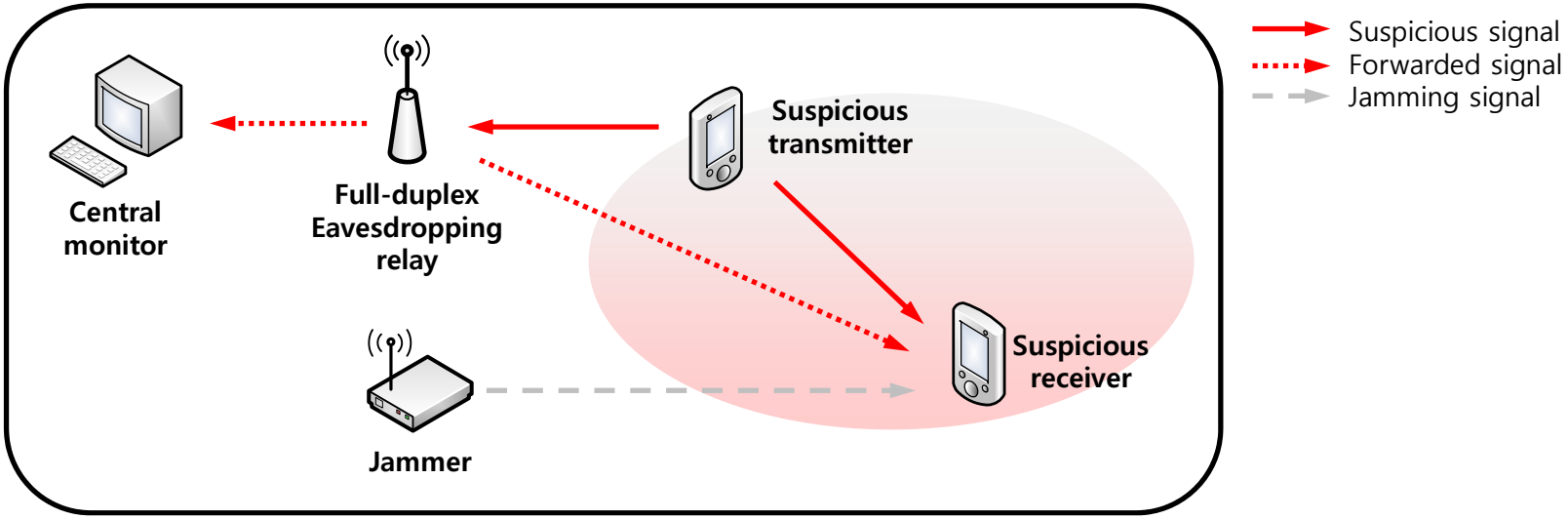
e.g.) delay ≪ a symbol time period

Non-negligible relay processing delay

e.g.) delay > a symbol time period

Introduction

- **Proposed relay-assisted proactive eavesdropping with a cooperative jammer**
  - Goal
    - Eavesdropping rate maximization by optimizing the power allocation of the relay and the jammer



Outline

- System model
- Case 1: Negligible relay processing delay
  - Eavesdropping rate maximization
- Case 2: Non-negligible relay processing delay
  - Eavesdropping rate maximization
- Extension
  - Multi-antenna multi-relay system
- Numerical results
- Conclusion

System Model

- **Case 1: Negligible relay processing delay**
  - Received signals
    - At the eavesdropping relay E

Cooperative jamming

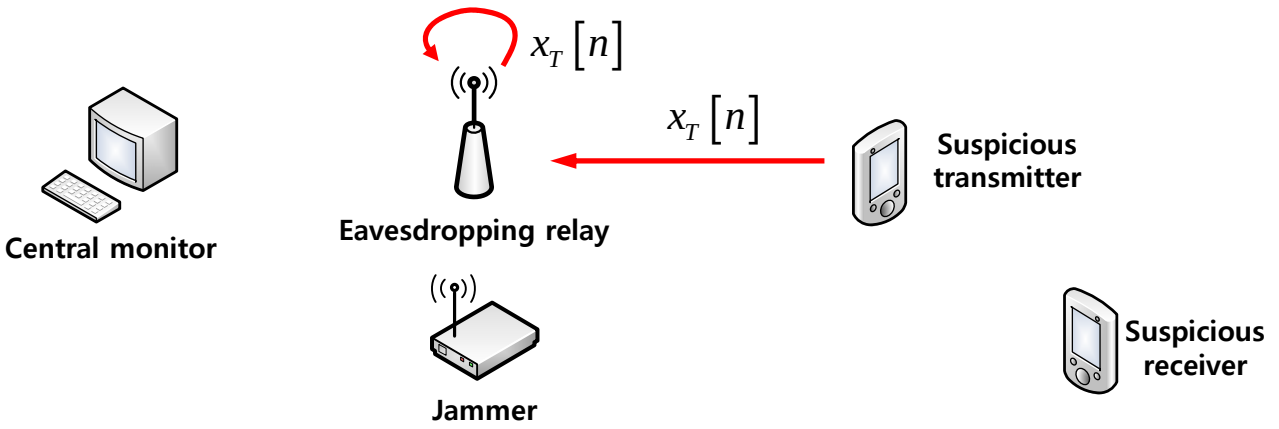
$$y_E[n] = h_{TE}x_T[n] + \tilde{h}_{EE}x_E[n] + h_{JE}x_J[n] + z_E[n]$$

where $x_E[n] = G_E y_E[n]$

$$\Rightarrow \quad x_E[n] = \frac{G_E h_{TE}}{\left(1 - G_E \tilde{h}_{EE}\right)} x_T[n] + \frac{G_E}{\left(1 - G_E \tilde{h}_{EE}\right)} z_E[n]$$

Notations

- x_X : Transmit signal at node **X**
- h_{XY} : Channel coefficient from node **X** to node **Y**
- $\tilde{h}_{XX}$: Residual self-interference at node **X**
- P_X : Transmit power at node **X**
- G_E : Amplification factor
- z_X : AWGN at node **X** with power σ_X^2



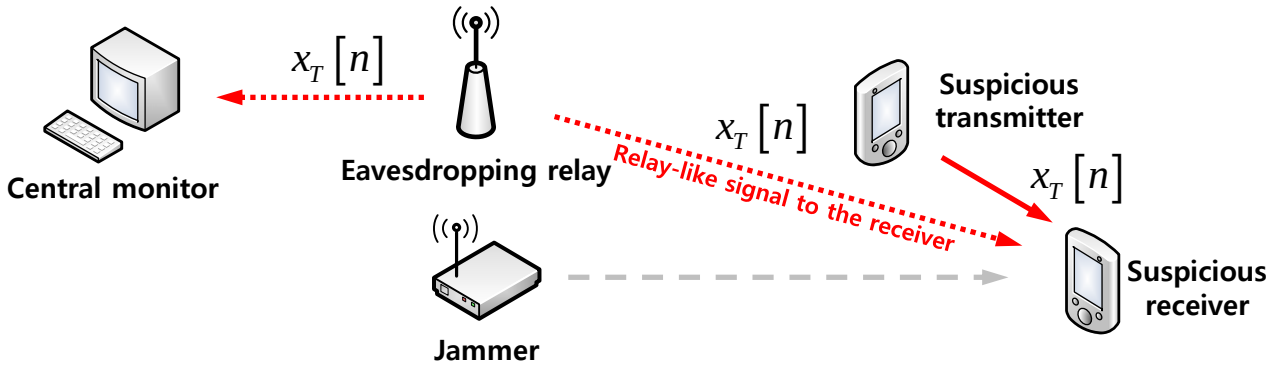
System Model

- **Case 1: Negligible relay processing delay**
  - Received signals
    - At the central monitor M

$$y_M[n] = \underbrace{h_{EM}\frac{G_E h_{TE}}{(1-G_E h_{EE})}x_T[n]}_{\text{Desired}} + h_{EM}\frac{G_E}{(1-G_E h_{EE})}z_E[n] + z_M[n]$$

    - At the suspicious receiver R

$$y_R[n] = \underbrace{\left(h_{TR} + h_{ER}\frac{G_E h_{TE}}{(1-G_E h_{EE})}\right)x_T[n]}_{\text{Desired}} + h_{ER}\frac{G_E}{(1-G_E h_{EE})}z_E[n] + h_{JR}x_J[n] + z_R[n]$$



System Model

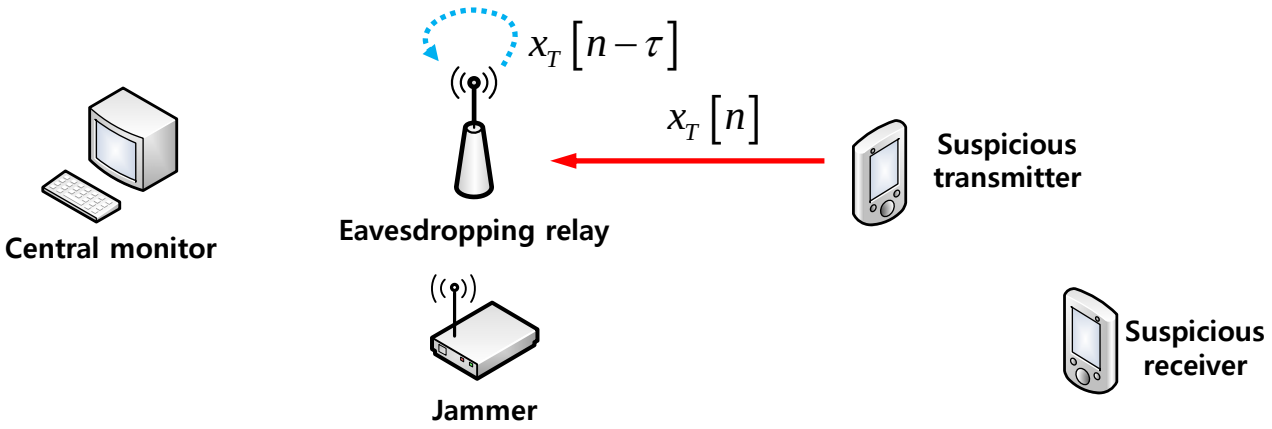
- **Case 2: Non-negligible relay processing delay**
  - Received signals
    - At the eavesdropping relay E

Cooperative jamming

$$y_E[n] = h_{TE}x_T[n] + \tilde{h}_{EE}x_E[n] + h_{JE}x_J[n] + z_E[n]$$

where $x_E[n] = G_E y_E[n-\tau]$ $\Rightarrow$ $\mathrm{E}\left[\left|x_E[n]\right|^2\right] = |G_E|^2\left(|h_{TE}|^2 P_T + |\tilde{h}_{EE}|^2 P_E + \sigma_E^2\right) = P_E$

$$|G_E|^2 = \frac{P_E}{|h_{TE}|^2 P_T + |\tilde{h}_{EE}|^2 P_E + \sigma_E^2}$$



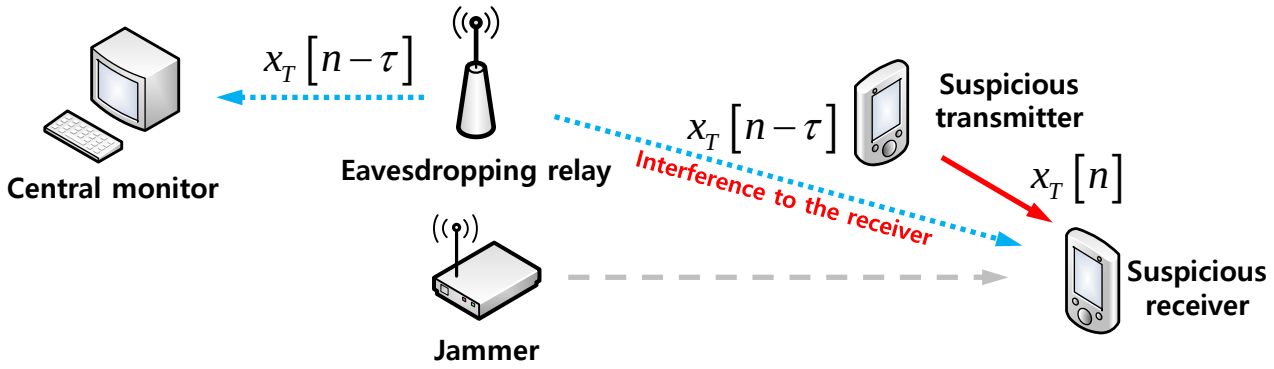
System Model

- **Case 2: Non-negligible relay processing delay**
  - Received signals
    - At the central monitor M

$$y_M[n] = \underbrace{h_{EM} G_E h_{TE} x_T[n-\tau]}_{\text{Desired}} + h_{EM} G_E \tilde{h}_{EE} x_E[n-\tau] + h_{EM} G z_E[n-\tau] + z_M[n]$$

    - At the suspicious receiver R

$$y_R[n] = \underbrace{h_{TR} x_T[n]}_{\text{Desired}} + h_{ER} G h_{TE} x_T[n-\tau] + h_{ER} G \tilde{h}_{EE} x_E[n-\tau] + h_{ER} G z_E[n-\tau] + h_{JR} x_J[n] + z_R[n]$$



Case 1: Negligible relay processing delay

- **Signal-to-interference-plus-noise ratio (SINR)**
  - $\gamma_M\left(\Omega_E\right)=\dfrac{\left|h_{EM}\Omega_E h_{TE}\right|^2 P_T}{\left|h_{EM}\Omega_E\right|^2\sigma_E^2+\sigma_M^2}$ and $\gamma_R\left(\Omega_E,\theta_E,P_J\right)=\dfrac{\left|h_{TR}+h_{ER}\Omega_E\angle\theta_E\tilde{h}_{TE}\right|^2 P_T}{\left|h_{ER}\Omega_E\right|^2\sigma_E^2+\left|h_{JR}\right|^2 P_J+\sigma_R^2}$

    where $\Omega_E\angle\theta_E=\dfrac{G_E}{\left(1-G_E\tilde{h}_{EE}\right)}$

- **Problem formulation**

Problem 3. Eavesdropping rate maximization for case 1

$$(\mathrm{P3}):\ \max_{\Omega_E,\theta_E,P_J}\ \gamma_R\left(\Omega_E,\theta_E,P_J\right)$$
$$\text{s.t.}\ \ \gamma_M\left(\Omega_E\right)\geq\gamma_R\left(\Omega_E,\theta_E,P_J\right)$$
$$\gamma_M\left(\Omega_E\right)\geq\bar{\gamma}_M$$
$$\left|\Omega_E h_{TE}\right|^2 P_T+\left|\Omega_E\right|^2\sigma_E^2\leq\bar{P}_E\ \text{and}\ 0\leq P_J\leq\bar{P}_J$$

Non-convex

Intercepting as much data as possible

Eavesdropping channel link ≥ Data rate of the suspicious users

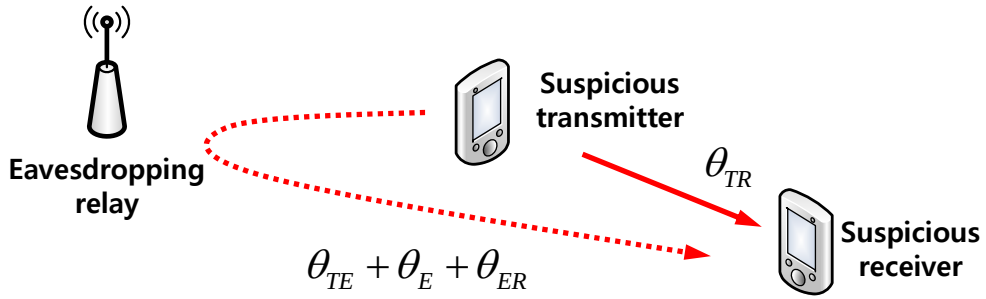
- Optimal solution recovered by $G_E^{\star}=\dfrac{\Omega_E^{\star}\angle\theta_E^{\star}}{\left(1+\Omega_E^{\star}\angle\theta_E^{\star}\tilde{h}_{EE}\right)}$

Case 1: Negligible relay processing delay

- **Properties of** $\gamma_R\left(\Omega_E,\theta_E,P_J\right)$

$$\gamma_R\left(\Omega_E,\theta_E,P_J\right)=\frac{\left(\left|h_{ER}h_{TE}\right|^2\Omega_E^2+2\left|h_{TR}h_{ER}h_{TE}\right|\Omega_E\cos\left(\theta_{TR}-\theta_{ER}-\theta_E-\theta_{TE}\right)+\left|h_{TR}\right|^2\right)P_T}{\left|h_{ER}\right|^2\sigma_E^2\Omega_E^2+\left|h_{JR}\right|^2P_J+\sigma_R^2}$$

  - Constructive relay
    - Maximum achievable $\gamma_R\left(\Omega_E,\theta_E,P_J\right)$ when $\cos\left(\theta_{TR}-\theta_{ER}-\theta_E-\theta_{TE}\right)=1$
    - $\theta_{E,\max}=\theta_{TR}-\theta_{ER}-\theta_{TE}$
  - Destructive relay
    - Minimum achievable $\gamma_R\left(\Omega_E,\theta_E,P_J\right)$ when $\cos\left(\theta_{TR}-\theta_{ER}-\theta_E-\theta_{TE}\right)=-1$
    - $\theta_{E,\min}=\theta_{TR}-\theta_{ER}-\theta_{TE}-\pi$



Case 1: Negligible relay processing delay

- **Optimal solution for (P3)**

Theorem 2. Three operation modes

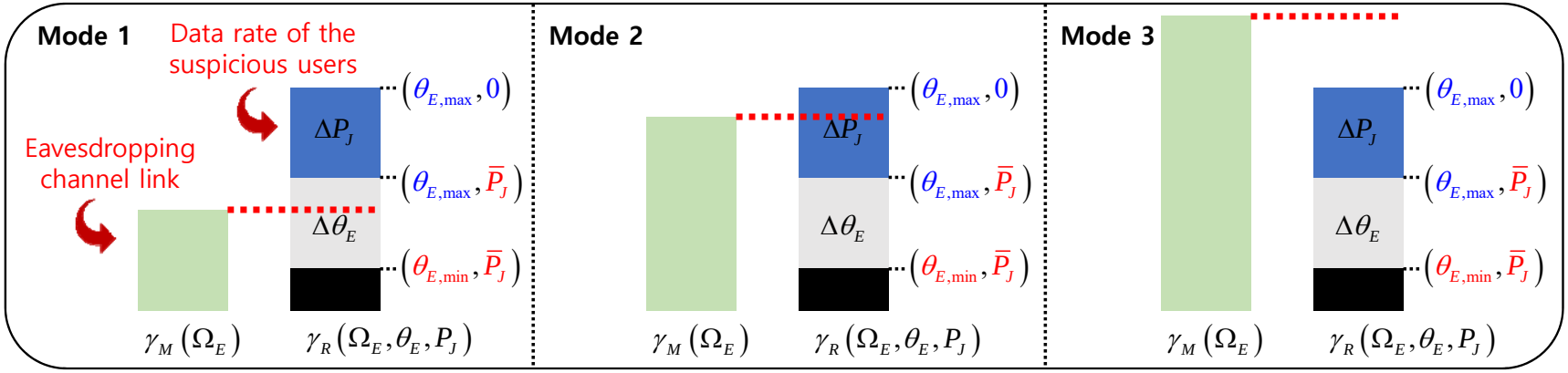
The optimal solution $(\Omega_E^\star, \theta_E^\star, P_J^\star)$ for (P3) falls into one of the following three modes:

1) Destructive relaying with full jamming: $\theta_{E,\min} \le \theta_E^\star < \theta_{E,\max}$ and $P_J^\star = \bar{P}_J$

2) Constructive relaying with jamming: $\theta_E^\star = \theta_{E,\max}$ and $0 < P_J^\star \le \bar{P}_J$

3) Constructive relaying without jamming: $\theta_E^\star = \theta_{E,\max}$ and $P_J^\star = 0$

Closed-form solutions available



Case 2: Non-negligible relay processing delay

- **Signal-to-interference-plus-noise ratio (SINR)**
  - $\gamma_M(P_E) = \dfrac{\gamma_{TE}\gamma_{EM}}{\gamma_{TE}+\gamma_{EM}+1}$ and $\gamma_R(P_E,P_J) = \dfrac{\gamma_{TR}}{\gamma_{ER}+\gamma_{JR}+1}$

    where $\gamma_{TE} \triangleq \dfrac{|h_{TE}|^2 P_T}{|\tilde{h}_{EE}|^2 P_E + \sigma_E^2}$, $\gamma_{EM} \triangleq \dfrac{|h_{EM}|^2 P_E}{\sigma_M^2}$, $\gamma_{TR} \triangleq \dfrac{|h_{TR}|^2 P_T}{\sigma_R^2}$, $\gamma_{ER} \triangleq \dfrac{|h_{ER}|^2 P_E}{\sigma_R^2}$, $\gamma_{JR} \triangleq \dfrac{|h_{JR}|^2 P_J}{\sigma_R^2}$

- **Problem formulation**

Problem 4. Eavesdropping rate maximization for case 2

$$
\begin{aligned}
(\mathrm{P4}): \quad & \max_{P_E,P_J} \quad \gamma_R(P_E,P_J) \\
& \text{s.t.} \quad \gamma_M(P_E) \geq \gamma_R(P_E,P_J) \quad \left.\right\} \text{ Non-convex} \\
& \qquad \gamma_M(P_E) \geq \bar{\gamma}_M \\
& \qquad 0 \leq P_E \leq \bar{P}_E \text{ and } 0 \leq P_J \leq \bar{P}_J
\end{aligned}
$$

Case 2: Non-negligible relay processing delay

- **Two-step approach**
  - Step 1: Unconstrained solution by first relaxing the jammer power constraint

Problem 4.1. Unconstrained problem for case 2

$$(\text{P4.1}): \quad \max_{P_E, P_J} \ \gamma_R(P_E, P_J)$$
$$\text{s.t.} \quad \gamma_M(P_E) \geq \gamma_R(P_E, P_J)$$
$$\gamma_M(P_E) \geq \bar{\gamma}_M$$
$$0 \leq P_E \leq \bar{P}_E \ \text{and} \ 0 \leq P_J \leq \bar{P}_J$$

Solved by the two-layer algorithm (Part I.)

  - Step 2: Retrieving the true optimal solution if the obtained jamming power from (P4.1) is $\hat{P}_J > \bar{P}_J$

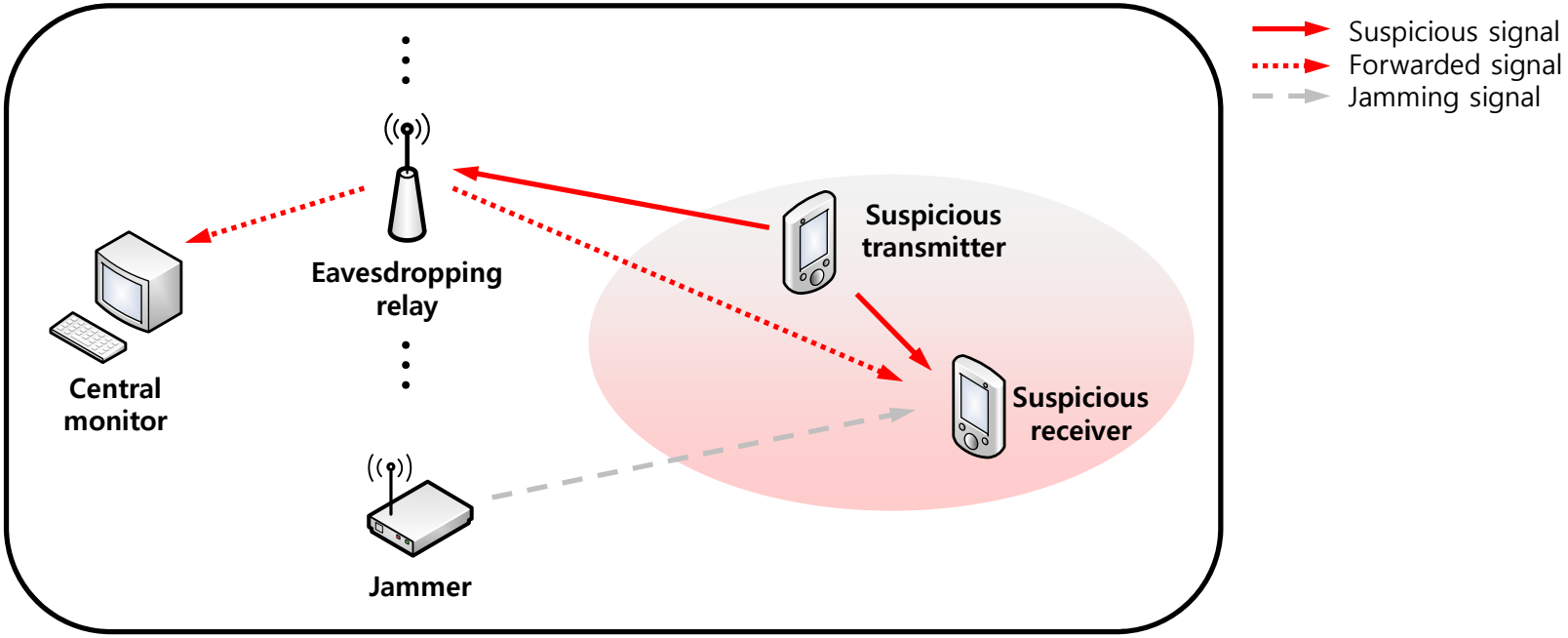
Theorem 3. The optimal jamming power for the original problem (P4)

If $\hat{P}_J > \bar{P}_J$, the optimal jamming power for the original problem (P4) is $P_J^\star = \bar{P}_J$

    - Closed-form solution available

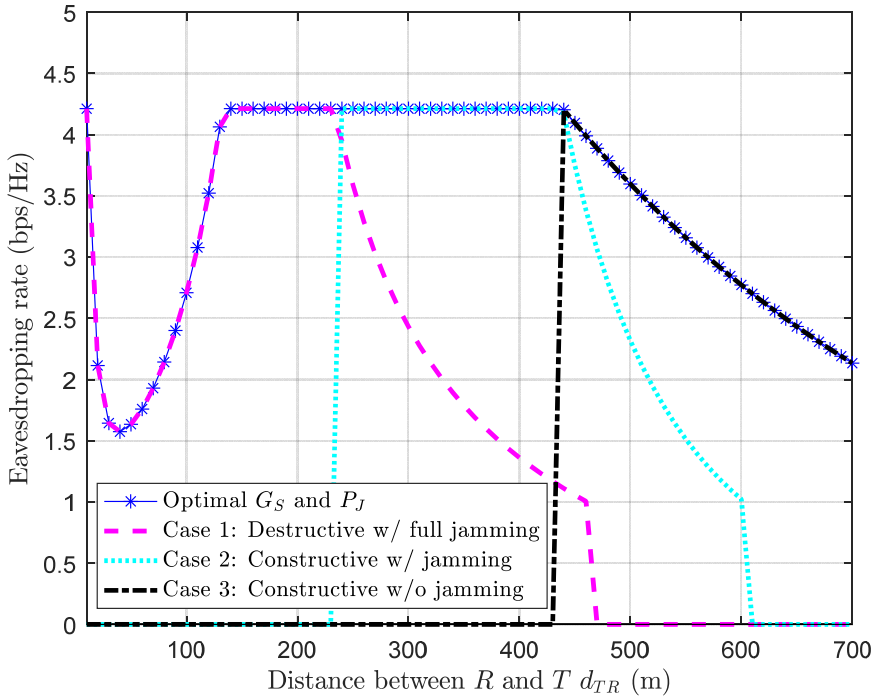
Extension

- **Multi-antenna multi-relay system**
  - Goal
    - Eavesdropping rate maximization by jointly optimizing the receive combining vector at the central monitor, the precoders at the relays and the transmit covariance matrix at the jammer



Numerical Results

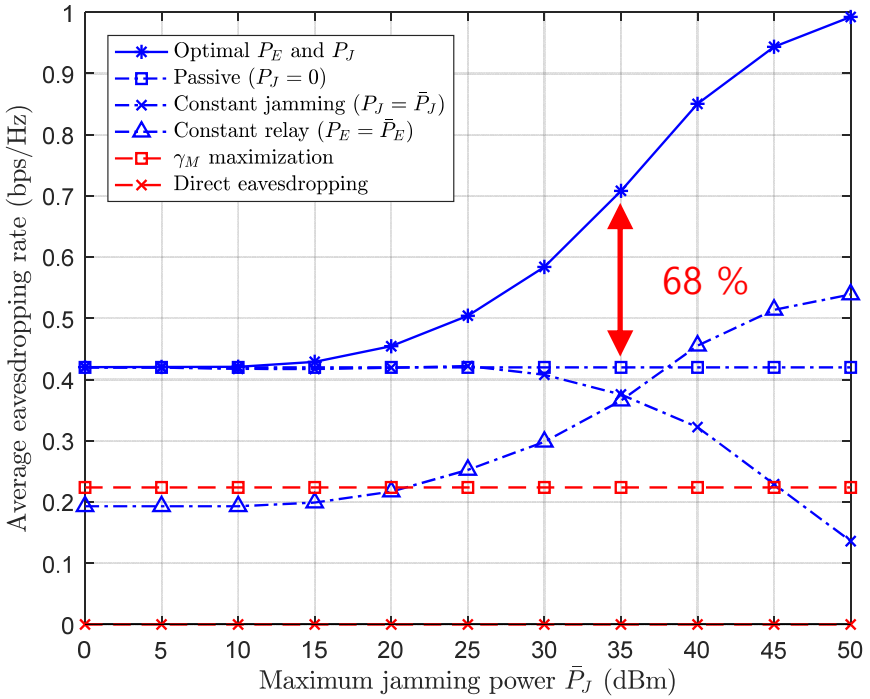
Case 1: Negligible relay processing delay



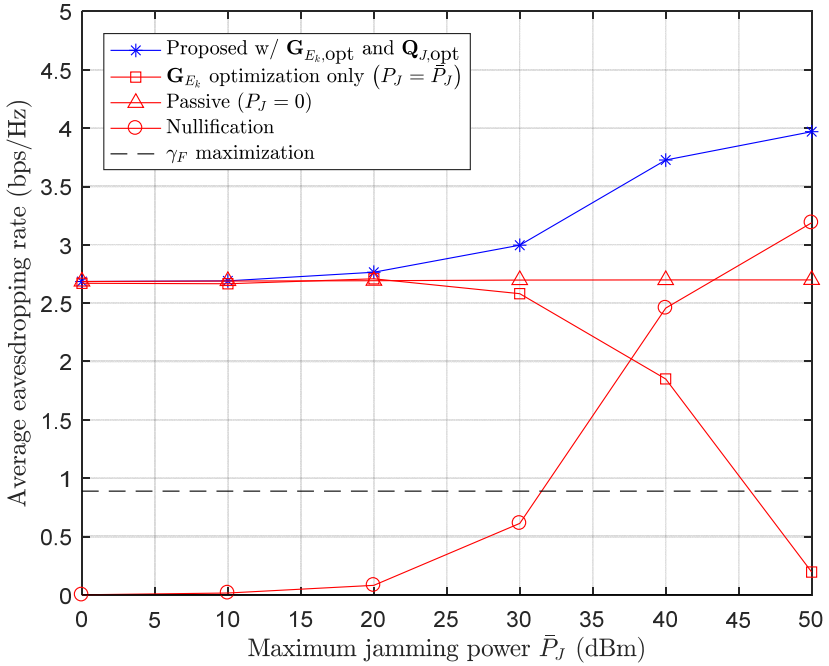
High ← → Low

Channel condition of the suspicious users

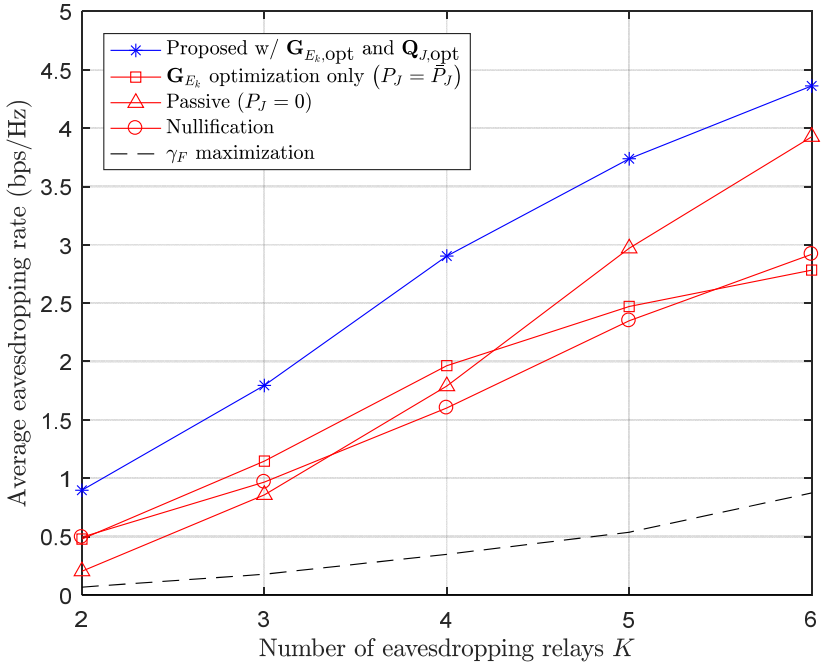
Case 2: Non-negligible relay processing delay



Maximum Transmit Power of The Jammer



Number of Eavesdropping Relays



Conclusion

- **Conclusion**
  - A scenario where a distant central monitor covertly wiretaps the communication between a pair of suspicious users via a full-duplex relay and a cooperative jammer
  - Two different cases
    - Negligible relay processing delay
      - Three optimal operation modes with the closed-form optimal solutions
    - Non-negligible relay processing delay
      - Two-step optimization approach for the optima power optimization
  - Extension to multi-antenna multiple relay scenarios
- **Future works**
  - Absence of global channel state information
  - Active suspicious users with anti-eavesdropping or anti-jamming capabilities

Reference

- [LLiu:14] Liang Liu, Rui Zhang and Kee-Chaing Chua, "Secrecy wireless information and power transfer with MISO beamforming," IEEE Trans. Signal Process. vol. 64, pp. 1850-1863, Apr. 2014.
- [DWKNg:14] Derrick Wing Kwan Ng, Ernest S. Lo and Robert Schober, "Robust beamforming for secure communication in systems with wireless information and power transfer," *IEEE Trans. Wireless Commun*. vol. 13, pp. 4599-4615, Aug. 2014.
- [HXing:16a] Hong Xing, Liang Liu and Rui Zhang, "Secrecy wireless information and power transfer in fading wiretap channel," *IEEE Trans. Veh. Technol*. vol.65, pp. 180-190, Jan. 2016.
- [WLiu:16] Wanchun Liu, Xiangyun Zhou, Salman Durrani and Petar Popovski, "Secure communication with a wireless-powered friendly jammer," *IEEE Trans. Wireless Commun*. vol. 15, pp. 401-415, Jan. 2016.
- [HXing:15b] Hong Xing and Kai-Kit Wong and Zheng Chu and Arumugam Nullanathan, "To harvest and jam: a paradigm of self-sustaining friendly jammers for secure AF relaying," *IEEE Trans. Signal Process*. vol. 63, pp. 6616-6631, Dec. 2015.
- [JXu:17a] Jie Xu, Lingjie Duan and Rui Zhang, "Surveillance and intervention of infrastructure-free mobile communications: a new wireless security paradigm," *IEEE Wireless Commun*. vol. 24, pp. 152-159, Aug. 2017.
- [JXu:17b] Jie Xu, Lingjie Duan and Rui Zhang, "Proactive eavesdropping via cognitive jamming in fading channels," I*EEE Trans. Wireless Commun*. vol. 16, pp. 2790-2806, May 2017.
- [CZhong:17] Caijun Zhong, Xin Jiang, Fengzhong Qu and Zhaoyang Zhang, "Multi-antenna wireless legitimate surveillance systems: design and performance analysis," *IEEE Trans. Wireless Commun*. vol. 16, pp. 4585-4599, Jul. 2017.
- [YZeng:16] Yong Zeng and Rui Zhang, "Wireless information surveillance via proactive eavesdropping with spoofing relay," *IEEE J. Sel. Topics Signal Process*., vol. 10, pp. 1449-1461, Dec. 2016.
- [Jmoon:18] J. Moon, H. Lee, C. Song, S. Kang, and I. Lee, "Relay-assisted proactive eavesdropping with cooperative jamming and spoofing," IEEE Trans. Wireless Commun., vol. 17, pp. 6958-6971, Oct. 2018.