# Single Relay Selection for Secure Communication in a Cooperative System with Multiple Full-Duplex DnF Relays

**Binh Nguyen**

School of Information and Communications
Gwangju Institute of Science and Technology
Gwangju, Republic of Korea

November $19^{th}$, 2015

# List of Contents

## Cooperative Communication

- Recent developments on MIMO systems show that the channel capacity can dramatically increases by using multiple transmit and receive antennas.
  - Given perfect CSI, we have $\lim_{SNR \to \infty} \frac{C(SNR)}{\log(SNR)} = \min\{M_t, M_r\}$, where $M_t$ and $M_r$ respectively are numbers of transmit and receive antennas.
- However, deployment of multiple antennas in a limited space, i.e., hand-held devices, is difficult and costly.
- This motivates the introduction of Cooperative Communications, in which single antenna systems can obtain spatial diversity by exploiting distributed antennas to create virtual MIMO channels [Cuba'12].

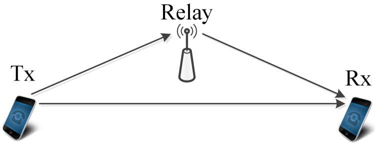


*Fig. 1: An example of a cooperative communication system*

## Half-Duplex versus Full-Duplex Relay

- In cooperative systems, relays can operate either in half-duplex (HD) or in full-duplex (FD) mode.
- Half-duplex mode: a relay receives and transmits in two separate time slots.
  - Easy to implement.
  - However, it suffers from high bandwidth and spectral efficiency loss.
- Full-duplex mode: a relay receives and transmit simultaneously.
  - Recovers the bandwidth and spectral efficiency loss associated with HD mode.
  - However, it suffers from loop interference due to the signal leakage between relay's input and output.
- With recent advances on antenna technologies and signal processing, FD mode has attracted much attention recently.

# Single Relay Selection

- In multi-relay scenarios, relays can be utilized according to
  - Orthogonal transmission approach.
  - Distributed space-time coding approach.
  - Beamforming approach.
  - Single relay selection approach.
- Among which single relay selection is a good option for practical implementation [Jing'09].

| Schemes | Description | Pros | Cons |
|---|---|---|---|
| **Orthogonal transmission** | Transmission in orthogonal channels | Low complexity receiver | Spectrally inefficient |
| **Distributed space-time coding** | Simultaneous transmission using a space-time code | Spectrally efficient | Requires strict synchronization<br>Challenging code design |
| **Beamforming** | Simultaneous transmission with phase adjustment of transmitted signals | Best performance | Requires transmit-site channel knowledge at relays<br>Sensitive to mismatches in carrier and timing synchronization |
| **Single relay selection** | Only the 'best' relay transmits | Simplifies signaling and network synchronization<br>Low complexity receiver | Design of selection mechanism and associated overhead |

*Table 1. A comparison of approaches that can be used in multi-relay scenarios*

# Physical Layer Security

- Even though the broadcast nature of wireless medium facilitates cooperative communication, it make wireless data transmission vulnerable to eavesdropping attack.
- Traditionally, secure wireless data transmission has been relied on cryptographic which suffers from very high communication overhead and computational complexity.
- As an alternative, physical layer security (PLS) is emerging as a promising prototype relying on exploiting the physical characteristic of wireless channels for protection against eavesdropping attack [Mukhehee'14].
- In addition, and importantly, PLS approach can operate essentially independent of higher layers, so it can be used to augment existing security schemes.

# Motivation and Objective

- Motivation
  - Applying relay selection techniques to improve robustness against eavesdropping attack has gained a lot of interest in research community recently.
  - Secure communication in multi-HD-relay systems have extensively studied in [Krikidis'09]-[Wang'15].
  - There are only a few works consider security issues in FD relay systems [Alves'14]-[Lee'15].
  - Importantly, [Alves'14]-[Lee'15] focus on single relay configuration which may be inadequate in reality because many relays could be available.

- Objective:
  - Investigating single relay selection schemes for a multi-FD-relay system under eavesdropping attack.

# System Model

- The considered system consist a source $S$, a destination $D$, $K$ FD DnF relays, and an eavesdropper $E$.
- $h_{ij}$ denotes the channel gain of $i-j$ link and $h_{kk}$ is the self-interference channel of the relay $k$. $h_{ij}$ and $h_{kk}$ are subject to Rayleigh fading.
- Capacities obtained at $D$ and $E$ are

$$C_D^{R_k} = \log_2\left(1+\min\left\{\frac{\gamma_{SR_k}}{\gamma_{kk}+1}, \gamma_{R_kD}\right\}\right), \quad (1)$$

$$C_E^{R_k} = \log_2\left(1+\gamma_{R_kE}\right), \quad (2)$$

where $\gamma_{ij} = \frac{P}{N_0}h_{ij}^2$.

- The system secrecy capacity is

$$C^{R_k} = \max\left\{0, \log_2\left(\frac{1+\min\left\{\frac{\gamma_{SR_k}}{\gamma_{kk}+1}, \gamma_{R_kD}\right\}}{1+\gamma_{R_kE}}\right)\right\}. \quad (3)$$

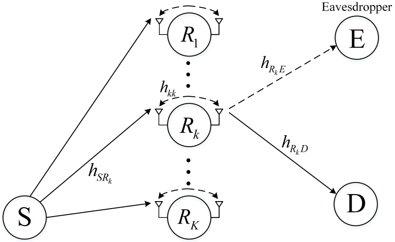


*Fig. 2: A multi-FD-DnF-relay system is under eavesdropping attack*

## Single Relay Selection Schemes

- According to the conventional Max-Min relay selection (MRS) scheme, the relay $R_m$ is selected if it satisfies

$$m = \arg \max_{k=1,\cdots,K} \left[ \min \left\{ \frac{\gamma_{SR_k}}{\gamma_{kk} + 1}, \gamma_{R_k D} \right\} \right]. \quad (4)$$

- It is obvious that the MRS scheme is suboptimal for our considered system.
- We propose an optimal relay selection (ORS) scheme which selects a relay as follows

$$o = \arg \max_{k=1,\cdots,K} \left[ \frac{1 + \min \left\{ \frac{\gamma_{SR_k}}{\gamma_{kk}+1}, \gamma_{R_k D} \right\}}{1 + \gamma_{R_k E}} \right]. \quad (5)$$

- Because the ORS scheme takes the eavesdropper channels into account, it is expected to provide better system performance compared to the MRS counterpart.

# Secrecy Outage Probability Analysis (1)

- We now analyze the performance of the proposed scheme by deriving its secrecy outage probability (SOP).
- As a comparison, the SOP of the conventional MRS scheme is also given.
- In addition, by considering the SOPs in the high region of average SNR of the main channels (source-to-relay and relay-to-destination), novel insights on the system behaviour are revealed.

# Secrecy Outage Probability Analysis (2)

- The SOP of the MRS scheme is given by

$$SOP_m = \Pr\left[C^{R_m} < R_S\right]$$

$$= \frac{\lambda_{SR}}{b\lambda_R\lambda_{RE}} \sum_{k=1}^{K} \binom{K}{k} (-1)^k \frac{e^{-ak\left(\frac{1}{\lambda_{SR}}+\frac{1}{\lambda_{RD}}\right)} E_k\left(\left(1+\frac{a\lambda_R}{\lambda_{SR}}\right)A\right)}{\left(1+\frac{a\lambda_R}{\lambda_{SR}}\right)^{k-1} e^{-\left(1+\frac{a\lambda_R}{\lambda_{SR}}\right)A}}, \qquad (6)$$

where $A = \frac{\lambda_{SR}}{b\lambda_R}\left(\frac{bk}{\lambda_{SR}} + \frac{kb}{\lambda_{RD}} + \frac{1}{\lambda_{RE}}\right)$, $a = 2^{R_s} - 1$, $b = 2^{R_s}$, $\lambda_{ij} = P\delta_{ij}^2/N_0$, $\lambda_R = P\delta_{kk}^2/N_0$, $\delta_{ij}^2$ is variance of $h_{ij}$, $P$ is transmit power of source and relays, $N_0$ is power of AWGN, $R_s$ is pre-defined secure rate, and $E_k(x)$ is the exponential integral function.

- When $\lambda_{R_kE} = \lambda_E$ is fixed and $\lambda_{SR_k} = \lambda_{R_kD} = \lambda_M \to \infty$, we have

$$SOP_m \approx O\left(\frac{1}{\lambda_M^K}\right). \qquad (7)$$

- When $\lambda_E = \lambda_M/L$ and $\lambda_M \to \infty$, we derive

$$SOP_m \approx \sum_{k=0}^{K} \binom{K}{k} \frac{(-1)^k}{(1+2bk/L)}. \qquad (8)$$

# Secrecy Outage Probability Analysis (3)

- The SOP of the optimal scheme is given by

$$SOP_o = \Pr\left[C^{R_o} < R_S\right] = \left(1 - \frac{\lambda_{SR} e^{-a\left(\frac{1}{\lambda_{SR}} + \frac{1}{\lambda_{RD}}\right) + B} E_1(B)}{b\lambda_R \lambda_{RE}}\right)^K, \quad (9)$$

where $B = \frac{\lambda_{SR}}{b\lambda_R}\left(1 + \frac{a\lambda_R}{\lambda_{SR}}\right)\left(\frac{b}{\lambda_{SR}} + \frac{b}{\lambda_{RD}} + \frac{1}{\lambda_{RE}}\right)$.

- When $\lambda_E$ is fixed and $\lambda_M \to \infty$, we obtain

$$SOP_o \approx \frac{(2a + a\lambda_R + 2b\lambda_{RE} + b\lambda_R\lambda_{RE})^K}{\lambda_M^K}. \quad (10)$$

- When $\lambda_E = \lambda_M / L$ and $\lambda_M \to \infty$, we derive

$$SOP_o \approx \left(1 - \frac{L}{L + b(2 + \lambda_R)}\right)^K. \quad (11)$$

## Secrecy Outage Probability Analysis (4)

- Remarks
  - When $\lambda_E$ is fixed and $\lambda_M \to \infty$, both MRS and ORS can provide a diversity order equal to the number of relays.
  - When $\lambda_E = \lambda_M / L$ and $\lambda_M \to \infty$, the SOPs of both MRS and ORS schemes converge to well-defined saturated values.

# Simulation Results (1)

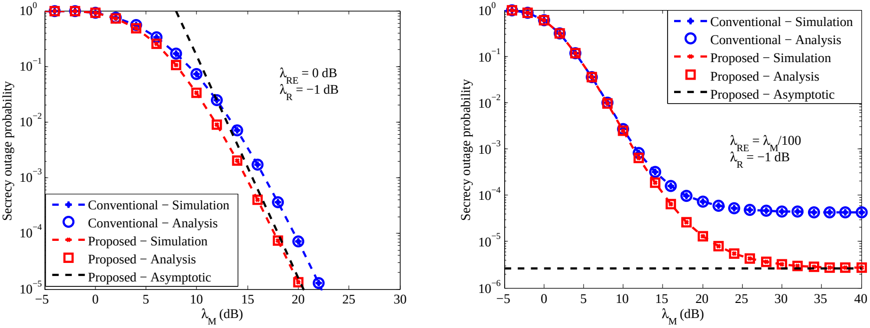


Fig. 3. Secrecy outage probability as a function of $\lambda_M$ with $K = 4$ relays.

- The simulated results confirm that the MRS and ORS schemes follow the same trend in the high region of $\lambda_M$. In addition, the proposed scheme always outperform the conventional one.

# Simulation Results (2)

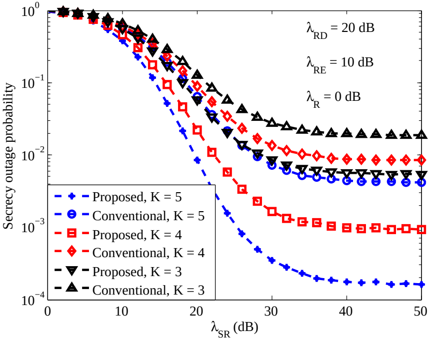


Fig. 4. Effect of the number of relays on the system performance.

- Increasing the number of relays significantly enhances performance of both MRS and ORS schemes.
- As the number of relays increases, the gap between performance of the ORS scheme and that of the MRS scheme is enlarged.

# Conclusions

- In this work, we investigated single relay selection schemes for a multi-FD-DnF-relay system which is under eavesdropping attack.
- We proposed the ORS scheme which selects the relay that maximizes the system secrecy capacity.
- We derived the secrecy outage probabilities of the ORS and the conventional MRS schemes in closed-form expressions, which can help system designers quickly obtain system performance without doing complex computer simulations.
- We showed that ORS and MRS follow the same trend in the high region of average SNR of the main channels.
  - When average SNR of the eavesdropper channels is fixed, both schemes can provide a diversity order equal to the number of relays.
  - When average SNR of the eavesdropper channels is linear proportion to that of the main channels, the SOPs of the two schemes are saturated.

# References


1. [Cuba′12] F. G. Cuba, R. A. Cacheda, and F. J. G. Castaño, "A Survey on Cooperative Diversity for Wireless Networks,"*IEEE Commun. Surveys Tuts.*, vol. 14, N0. 3, pp. 822-835, Third Quarter 2012.
2. [Jing′09] Y. Jing, and H. Jafarkhani, "Single and Multiple Relay Selection Schemes and their Achievable Diversity Orders," *IEEE Trans. Wireless Commun.*, vol. 8, N0. 3, pp. 1414-1423, March 2009.
3. [Mukhejee′14] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurt, "Principles of Physical Layer Security in Multiuser Wireless Networks: A Survey,"*IEEE Commun. Surveys Tuts.*, vol. 16, N0. 3, pp. 1550-1573, Third Quarter 2014.
4. [Krikidis′09] I. Krikidis, J. S. Thompson, and S. McLaughlin, "Relay Selection for Secure Cooperative Networks with Jamming," *IEEE Trans. Wireless Commun.*, vol. 8, no. 10, pp. 5003-5011, Aug. 2009.
5. [Wu′13] N. Wu and H. J. Li, "Effect of Feedback Delay on Secure Cooperative Networks with Joint Relay and Jammer Selection," *IEEE Commun. Lett.*, vol. 2, no. 4, pp. 415-418, Aug. 2013.
6. [Jindal′14] A. Jindal, C. Kundu, and R. Bose, "Secrecy Outage of Dual-Hop AF Relay System with Relay Selection Without Eavesdropper's CSI," *IEEE Commun. Lett.*, vol. 18, no. 10, pp. 1759-1762, Oct. 2014.
7. [Wang′15] L. Wang, K. J. Kim, T. Q. Duong, M. Elkashlan, "Security Enhancement of Cooperative Single Carrier Systems," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 1, pp. 90-113, Jan. 2015.

## References


8. [Alves′14] H. Alves, G. Brante, R. D. Souza, D. B. da Costa, and M. Latva-aho, "On the Performance of Full-Duplex Relaying Under Physical Security Constraints," *IEEE ICASSP*, 2014.

9. [Huang′14] X. Huang, J. He, Q. Li, Q. Zhang, and J. Qin, "Optimal Power Allocation for Multicarrier Secure Communication in Full-Duplex Decode-and-Forward Relay Networks," *IEEE Commun. Lett.*, vol. 18, no. 12, pp. 2169-2172, Dec. 2014.

10. [Chen′15] G. Chen, Y. Gong, P. Xiao, and J. A. Chambers, "Physical Layer Network Security in the Full-Duplex Relay System," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 3, pp. 574-583, March 2015.

11. [Lee′15] J. H. Lee, "Full-Duplex Relay for Enhancing Physical Layer Security in Multi-Hop Relaying Systems," *IEEE Commun. Lett.*, vol. 19, no. 4, pp. 525-528, April 2015.

# Thank You

==========================================

Any questions or comments are appreciated.

Binh Nguyen