Full-Duplex Two-Way MIMO Relaying System: Transceiver Design and Review of Physical Layer Security

Nachiket Ayir and Dr. P. Ubaidulla

Signal Processing and Communications Research Center (SPCRC),
International Institute of Information Technology, Hyderabad, India.

Full-Duplex Wireless Communication

Introduction

- In most of current systems, communication is in half-duplex, i.e., transmission and reception happen in different times slots or in different frequency bands, etc.
- In in-band full-duplex wireless, all the communicating nodes receive and transmit on the same frequency band at the same time !

Benefits

- An in-band full-duplex radio can achieve better spectral efficiency, viz., twice the efficiency of half-duplex or out-of-band full-duplex wireless.
- Along with enhanced data rates, full-duplex would also free up a lot of spectrum, which would result in increase in number of supported users.

Challenges

- Transmit signal power >>> Received signal power (80dB or more).
- User's own transmit signal can completely overwhelm the intended received signal from other nodes. .

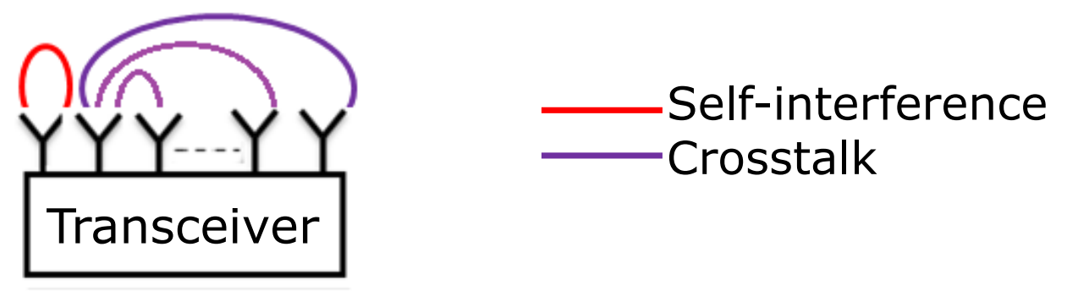
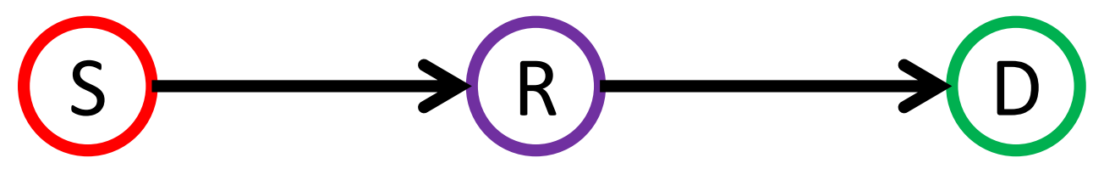


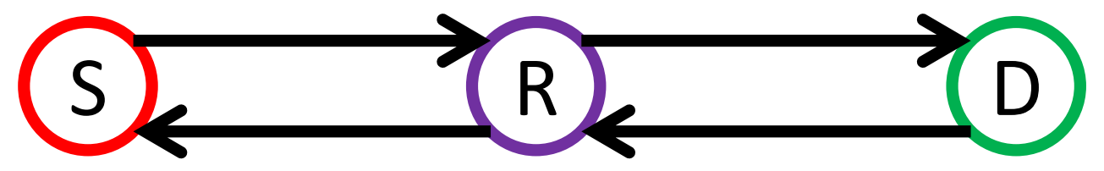
Fig. 1

Use of Relays in Wireless Communication

- Recent research in FD relays involves use cases in physical layer security, wherein the relay transmits jamming signals towards the eavesdropper to improve secrecy.
- Based on mode of operation , relays can be classified as: 1. Amplify-and –Forward (AF), 2. Decode-and-Forward (DF), etc.
- Based on relaying schemes, we have the following classification (Source-Relay-Destination):



One-way-relaying,



Two-way-relaying .

- **Two-way in-band full-duplex relaying** combines the benefits of both these technologies and has the potential to be a driving technology for next generation cellular networks.

Abstract

In this paper, we consider the design of optimal transceiver and relay processing algorithms for a full-duplex (FD) two-way amplify-and-forward (AF) multiple-input multiple-output (MIMO) relaying system. We assume the channel state information of loopback self-interference (SI) channels to be imperfect. The nodes employ precoders and receive filters for suppressing the residual SI. The optimal precoders at transceivers are designed by equalising the signal-to-interference-plus-noise ratio at the relay and transceiver. Using the transceiver precoders thus designed, we then design the optimal relay precoder and transceiver receive filters by minimizing the sum of mean square error (SMSE) at the transceivers. The optimal precoders and receive filters are continuously updated to account for the cumulative interference effect caused by AF operation of the FD relay. The secrecy performance of this system in the presence of a passive eavesdropper is analyzed by considering the relay signal to be artificial noise (AN) for the eavesdropper. The effectiveness of the proposed design is demonstrated in our simulation results.

Problem statement

- None of the previous work in literature considers the problem of residual SI mitigation, simultaneously, at the transceivers and at the relay.
- One of the solution proposed in literature to mitigate the residual SI in a FD two-way MIMO relaying system is computationally too complex and also does not scale well with time.
- Simultaneous transmission and reception on the same frequency makes a FD system inherently secure due to the presence of multiple signals combined on the same frequency ! However this inherent secrecy has not been analyzed yet in literature.

Accumulating above problems into a possible solution, we propose:

1. The design of optimal precoders and receive filters for a FD two-way AF MIMO relaying system in the presence of a passive eavesdropper.
2. A technique to secure the data transmission from the eavesdropper which exploits the fact the precoded relay transmission is unknown to the eavesdropper and can hence act as artificial noise (AN).

System model

- **# antennas at the users = N_S**
- **# antennas at the Eavesdropper= N_E**
- **# antennas at the relay = N_R**

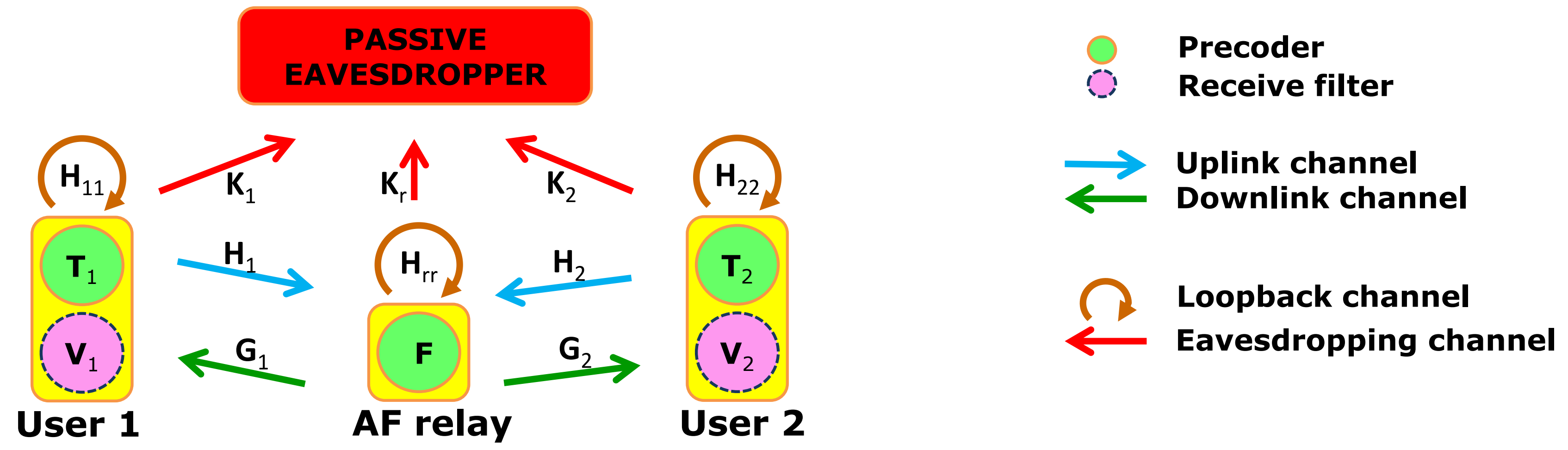


Fig. 2

Contributions

- Precoding at end-user transceivers for mitigating residual SI.
- We computed the feedback term (Γ_p), required for residual SI mitigation at the AF relay, in a recursive manner with minimal memory requirements. It is given as:

$$\Gamma_p = \sigma_{er}^2[tr(\mathbf{F}^{(t-1)}\Delta^{(t-2)}\mathbf{F}^{(t-1)^H})\mathbf{I}_{N_s} + \Gamma_p^{(t-1)}tr(\mathbf{F}^{(t-1)}\mathbf{F}^{(t-1)^H})]$$

- Analysis of physical layer security of the proposed FD system in terms of the achievable sum-secrecy rate.

Review of Physical layer security

- Consider the worst case scenario where Eavesdropper is able to decode the signals from transceivers using blind channel estimation techniques.
- Even in this case, Eavesdropper will not have CSI of relay-transceiver channels $\mathbf{G}_1$ and $\mathbf{G}_2$.
- Now, the relay precoder **F** is a function of relay-transceiver channels. Hence, the Eavesdropper won't be able to decode the signal received from the relay, which is precoded with **F**.
- So, even in the worst case scenario, the relay signal acts as artificial noise (AN) for the Eavesdropper.
- Also, we observed that for optimality, the relay always transmits at full power $P^r_{max.}$ This makes the relay signal a strong interferer for the Eavesdropper. We found the sum-secrecy rate for this case.
- Please note that in this case we do not use separate dedicated antennas at the relay for generating AN, neither do we pump in additional power for the purpose.

Simulation results

For simulations, we have set:
$N_S = N_E = 2$, $N_R = 4$.

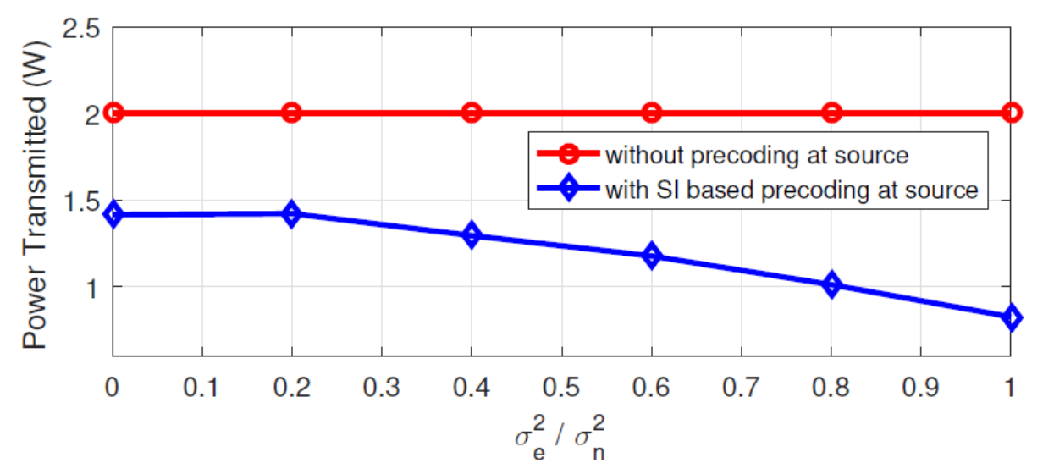


Fig. 3

- Shows the transmitted power for User 1 for varying interference-to-noise ratio (INR) or residual SI.
- Without any precoding at transceivers, the User always transmits at fixed power irrespective of the residual SI.
- **Our precoder designs result in reduced transmit power as the residual SI increases.**
- Also with out any residual SI, the proposed precoder design results in much lesser transmit power

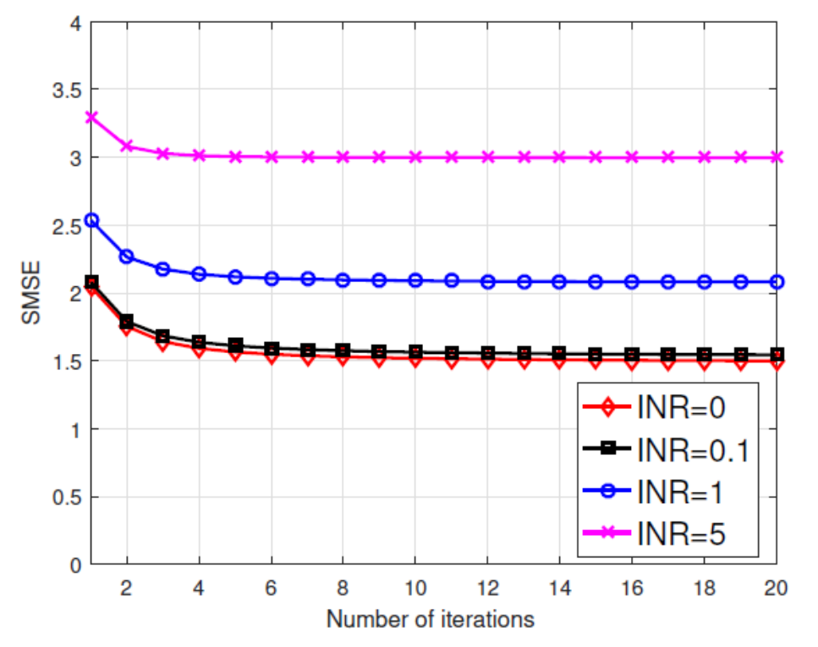


Fig. 4

- Shows the number of iterations required for the transceiver and relay processing algorithm to converge.
- **The proposed algorithm converges quickly signifying its suitability for practical implementation**

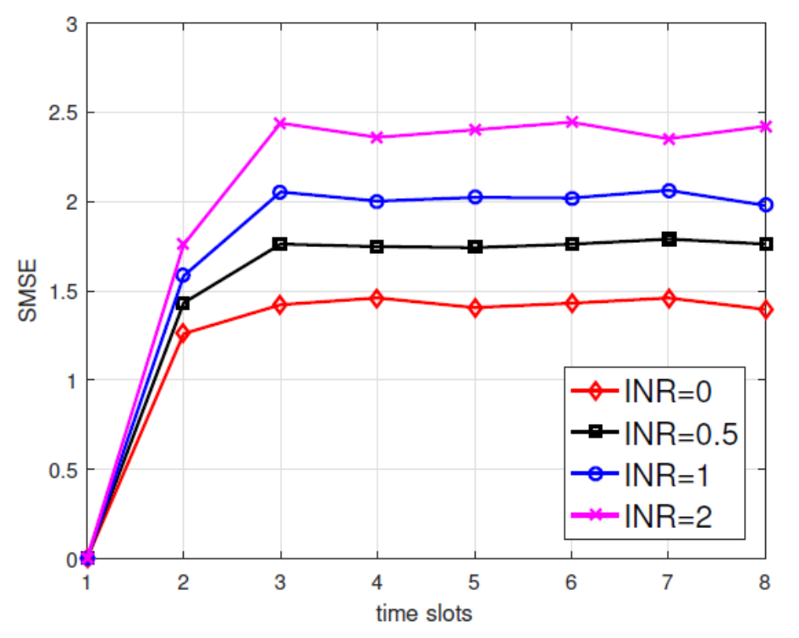


Fig. 5

- Shows the variation of SMSE over time at SNR = 10dB, for different values of INR.
- The SMSE starts to stabilize from the 3rd time slot.
- This is due to the effect of feedback term Γ_p which begins from t = 3.

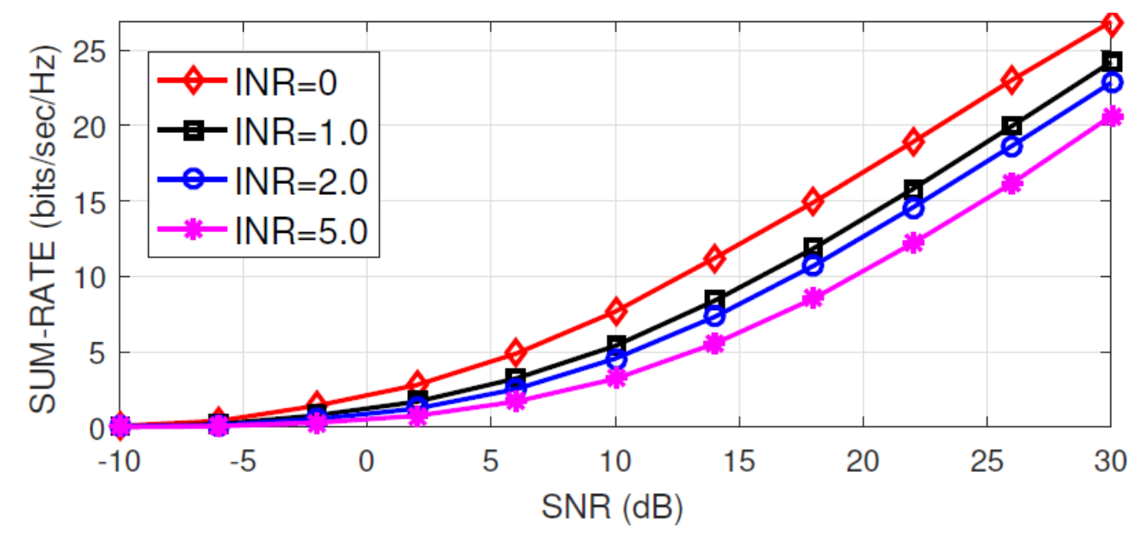


Fig. 6

- Shows the variation of sum-secrecy rate for varying SNR and INR.
- It can be observed that, with sufficient suppression of residual SI, this system achieves good sum-secrecy rate.
- The high rate is also due the strong interference from the relay signal to the Eavesdropper.
- **This result demonstrates the effectiveness of the inherent security of a FD system, without any use of additional power or separate antennas to generate artificial noise.**

Conclusions

- We proposed an iterative algorithm for mitigating the residual SI in a FD two-way MIMO relaying system.
- The iterative algorithm converges in about 5 iterations, as a result of which our transceiver and relay processing algorithm is practically feasible in a real world system.
- The proposed transceiver precoder designs ensure that the transmit power is adjusted as per the instantaneous residual SI, so as to minimize SI at the transceivers.
- Our analysis of Physical layer security for our system reveals that the precoded relay signal can itself act as artificial noise (AN) for the Eavesdropper. This results in savings on power and also relay antennas as compared to traditional methods of AN generation.

Paper id: 1408 FDX-O.2 - Signal Processing for Interference Cancellation and Full-Duplex Communication Systems Posters Wednesday, November 15, 14:00 - 15:30

If you have any queries on this paper, please contact: **ayir.nachiket@research.iiit.ac.in**