Project plan for degree project

ET2606 : MASTER'S THESIS IN TELECOMMUNICATION SYSTEMS

March 18, 2021

Title	Secrecy Capacity in Beamforming Transmission of Amplify and Forward Relaying Network	
Classification	*Beamforming Transmission, Relaying Transmission, Amplify and Forward, Secrecy Capacity*	
Student 1	Name	Rachakonda SVA Karthik
	E-Mail	sarc19@student.bth.se
	Person nr	9409158392
	Program	Masters in Telecommunication Systems
Student 2	Name	Mahesh Chowdary Karumanchi
	E-Mail	makc17@student.bth.se
	Person nr	9412232952
	Program	Masters in Telecommunication Systems
Supervisor	Name & title	Thi My Chinh Chu
	E-Mail	thi.my.chinh.chu@bth.se
	Department	Department of Computer Science

1 Introduction

Wireless network communication has played a major role in data transmission and communication. By principle, wireless communication works by transmitting the electromagnetic signals from the enabled device through an open-air environment [1]. The main advantages of wireless communication are ease of setup, freedom from wires, flexibility, cost effectiveness, and more. For this reason, wireless network communication offer's a great potential for exploitation while the communications of normal wired networks travel along fixed paths with a covered copper wire or by using an optical fiber cable. However, coming to the disadvantage of wireless communications, there are two main drawbacks that wireless network communication need to address, i.e., security issues due to broadcast nature of open-air environment and the variation of the received signals due to the effect of fading channel.

In recent years, there have been increasing attacks on the physical layer security [2]. Due to the nature of the broadcast environment of the wireless network within the open air, the communication is completely exposed to any kind of attacks of eavesdroppers within the coverage range [3]. Thus, guaranteeing secure communication in the presence of eavesdroppers has been a major challenge with mobile radio systems [4]. This gives a motivation to find a better solution to increase the secrecy capacity of transmission and enhance the reliability of the transmitted signal under different environmental conditions [5]. Here, security plays a primary aspect, so it's important to introduce the secrecy capacity [6] in the physical layer.

When deploying of physical layer security [7], there is a constraint in the transmit power of the source in order to reduce the risk that an eavesdropper can decode the secret signal. For this reason, the transmitter cannot send the signal with very high-power level. Therefore, the receiver may confront a lot of difficulties when decoding signal, especially, when the transmission range is too far. Because of this constraint in physical layer, so we need to find a solution that is able to provide reliability transmission for the main communication while can still guarantee the security for the wireless transmission.

To enhance the reliability of communication and extend transmission range, relaying transmission is a very powerful method. The principle of relaying transmission is to deploy an additional node, also called an intermediate node or relaying node, to assist the main transmission by forwarding the signal received from the source to the final destination. Thereby, when the relay cooperates with a network consisting of the source-destination pair and the relay will be configured [8]. By this way, the received signal is strengthen at the receiver and the transmission range can be extended even if the signal is transmitted with not too high-power level at the source.

There are two most popular protocols of relaying transmissions [8], which are decode-and-forward (DF) and amplify-and-forward (AF) [10]. In the DF protocol, the received signal from the source is decoded, re-modulated, and then re-transmitted to the final destination while the AF protocol simply amplifies and re-transmit the received signal from the source to the final destination without decoding. Thus, the complexity of AF relaying is significantly reduced but it comes to the cost of also magnifying the noise at the AF relaying node.

Another method that can apply to boost the reliability of communication is to deploy multiple-input multiple-output (MIMO) antennas for wireless communication systems. MIMO has been proved in [6] to be able to provide spatial diversity to enhance transmission reliability and to provide multiplexing diversity to enhance throughput. In this work, we aim for find the solution to enhance the reliability of the wireless communication in the context that there is a constraint of limited transmit power due to the deployment of the physical layer security. Therefore, the system will deploy the beamforming to direct the signal toward the destination as such the spatial diversity is achieve. In order to deploy the beamforming [2], the transmitter and receiver need to know the channel state information (CSI) to design the transmit and receive beamforming vectors. This CSI is obtained by periodically recorded at the received and feedbacks to the transmitter.

2 Related Works

Several relevant research papers have been studied for better awareness regarding the pros and cons of a wireless network, about the security measures taken against eavesdroppers and different techniques already implemented on different models to enhance the transmission reliability. In [4], few physical layer security schemes such as discrete Fourier transform spread orthogonal frequency division multiplexing (DFT-s-OFDM) and Radio Frequency Fingerprinting (RF Fingerprinting) have been proposed. A novel physical layer encryption scheme has also been introduced to secure the signal from the eavesdropper. In [7], Xiao Chen et al. attempt to degrade the eavesdropper's channel and secure the channel by producing an "artificial noise" at

the transmitter. In [13], two conditions are provided in order to optimize beamforming globally and hence ensure a secure transmission. The first condition states that the difference between the Gram matrices of legitimate and eavesdropper channel matrices has exactly one positive eigenvalue and the second condition involves convex optimization.

In [11], a collaboration of AF relays have been used to form a beamforming system and provide an improved physical-layer security. In order to maximise the secrecy rates, the experiments are carried out with different designs of networks and under total and individual relay power constraints when perfect CSI is available. In [2], the effect of feedback delay on outage probability (OP) and symbol error rate (SER) of cognitive AF relay networks with beamforming transmission is investigated under the condition of a Rayleigh fading environment. In [10], the performance of a dual-hop AF multi-antenna relay network, with an end-to-end best antenna selection, is investigated and the average symbol/bit error rate (SER/BER) for a large class of practical modulation schemes have been analysed.

In [8], the secrecy capacity of a full-duplex underlay cognitive cooperative radio network (CCRN) is analysed in the presence of an eavesdropper and under the interference power constraint of a primary network. Various network parameters are calculated and the secrecy capacity is analysed under different circumstances. In [5], the secrecy capacity of an underlay CCRN is studied with multiple relays assisting the secondary transmission. To obtain the maximum secrecy capacity under the condition of an interference power constraint, an optimal power allocation algorithm is also proposed for the secondary transmitter and secondary relays. In [9], the use of transmit antenna selection (TAS) and maximal ratio combining (MRC) for a cognitive MIMO AF relay network is studied. Finally, [6] summarizes the recent developments and challenges faced during the practical deployment of Cooperative multiple-input multiple-output (CMIMO).

3 Aim and objectives

Aim

The aim of this thesis is to find effective solutions to boost security and to enhance the reliability transmission of the signal from a source to a receiver while ensure secure transmission under various environment conditions. We achieve this by deploying the physical layer security and quantifying the secrecy capacity and implement beamforming transmission in combination with relaying transmission to further enhance the reliability of the transmission in term of outage probability and symbol error rate.

Objectives

The main objectives of the thesis are as follows.

1. To deploy the security in the physical layer of the wireless communication system.
2. To implement AF relaying transmission to enhance the transmission reliability and extend the transmission distance of the wireless communication system to cope with the signal variation due to fading.
3. To analyse the obtained performance metrics of the wireless communication system in terms of OP, SER and secrecy capacity.

4. To simulate the obtained performance metrics of the considered wireless communication system over fading channels in MATLAB simulation.

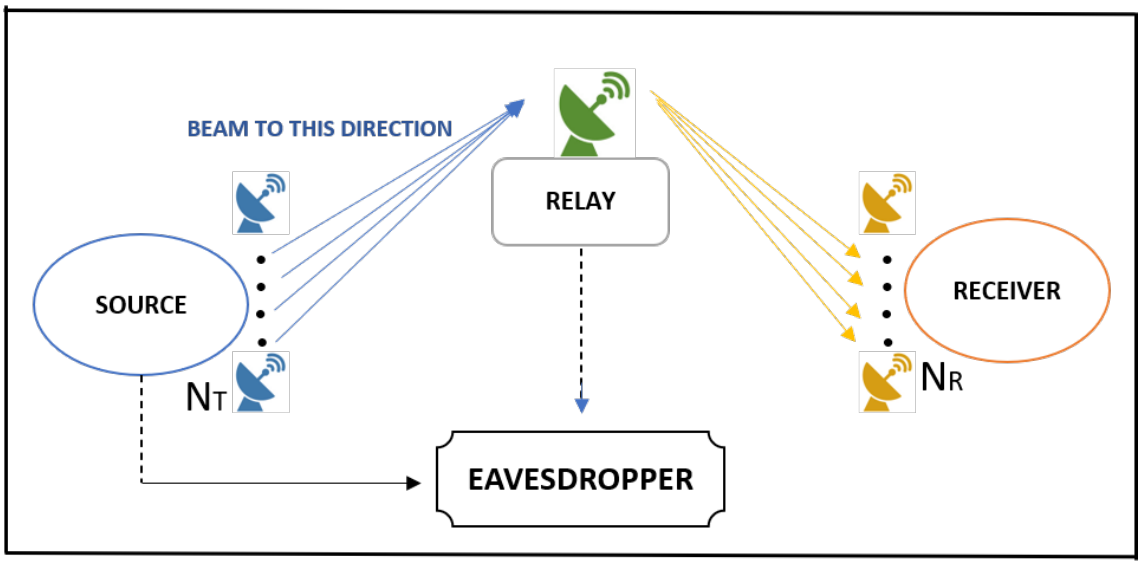

Figure 1: System Model

4 Research questions

RQ1: How does the wireless system deploy secrecy capacity of the system in physical layer?

RQ2: What is the benefit when we deploy AF relaying transmission for wireless communication using beam forming?

RQ3: How does beamforming technique enhance the transmission reliability of the signal?

RQ4: What is the obtained performance in terms of outage probability, symbol error rate and secrecy capacity of the system?

5 Method

1. A literature review has been carried out on relevant papers from acclaimed databases such as IEEE, SpringerLink, ACM digital library, Diva and so on. Research papers with keywords such as Wireless communication, Beamforming transmission, Physical layer security, Relaying protocol etc. were searched to understand fundamental concepts regarding the background of the topic. It is therefore found that by attempting to enhance the secrecy capacity of this system comprising AF relays, we could achieve the aim of this research.
2. A mathematical framework is proposed for deriving signal expressions to analyse the performance of the system.
3. MATLAB Simulations will be performed to generate fading channels and transmitted signals. Then, some performance metrics are also obtained through Matlab Simulations.

6 Expected outcomes

The following outcomes are expected out of this research.

1. To derive some expressions for the performance of the system in terms of outage probability and symbol error rate.
2. Beamforming transmissions can comparatively enhance the reliability of the system.
3. Relaying transmission can enhance reliability and extend the transmission distance.

7 Time and Activity Plan

The expected activity plan for the thesis is as shown in the table. Following the activity plan, the thesis is expected to be carried out for approximately 25 weeks. Each week, the supervisor would updated with the progress on the thesis work and changes will be made according to the provided suggestions. The execution of the plan may differ to that of actual plan depending on the obstacles in work.

Table 1: Time and Activity Plan

Task	**Period**
Background and literature	Week 5-Week 11
Project plan submission	Week 11
Preparation work for experiment	Week 12-Week 13
Experimental setup	Week 14
Experiment	Week 15-Week 24
Data analysis, interpretation and discussions	Week 24-Week27
Documentation	Week14-Week 34
Unexpected delay	Week 35
Thesis draft submission	Week 36
Opponent report	Week 37
Final thesis submission	Week 38

8 Limitations and risk management

Table 2: Risk Management

RISK	IMPACT	PLAN OF ACTION
Time constraints	Moderate	Modify plans if necessary.
Deviation from the main objective	High	Updating information to the supervisor time to time as per the project plan.
Inaccurate results	Moderate	Checking and repetition of the experiment.
Health problems	Moderate	Adjusting the time plan to overcome the lost time.

References

[1] H. Leung and Z. Zhu, Signal processing for RF impairment mitigation in wireless communications , Artech, 2014.

[2] T. M. Chinh Chu, H. Phan, T. Q. Duong, M. Elkashlan and H. Zepernick, "Beamforming transmission in cognitive AF relay networks with feedback delay," in *Proc. IEEE International Conference on Computing, Management and Telecommunications*, Ho Chi Minh City, Vietnam, Jan. 2013, pp.117-122.

[3] N. Xie, J. Chen, and L. Huang, "Physical-layer authentication using multiple channel based features," in *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 2356-2366, Jan. 2021.

[4] P. Ramabadran, D. Malone, S. Madhuwantha, P. Afanasyev, R. Farrell, J. Dooley, and B. O'Brien, "A novel physical layer encryption scheme to counter eavesdroppers in wireless communications," in *Proc. IEEE International Conference on Electronics, Circuits and Systems*, Bordeaux, France, Dec. 2018, pp. 69-72.

[5] T. M. C. Chu, H.-J. Zepernick, and H. Phan, "Optimal secrecy capacity of underlay cognitive radio networks with multiple relays," in Proc. *IEEE International Conference for Military Communications*, Baltimore, USA, Nov. 2016, pp. 162-167.

[6] D. N. Nguyen and M. Krunz, "Cooperative MIMO in wireless networks: recent developments and challenges," in *IEEE Network*, vol. 27, no. 4, pp. 48-54, Jul. 2013.

[7] X. Chen, L. Pang, Y. Tang, H. Yang and Z. Xue, "Security in MIMO wireless hybrid channel with artificial noise," in *Proc. IEEE International Conference on Cyber Security of Smart Cities, Industrial Control System and Communications*, Shanghai, China, Aug. 2015, pp. 1-4.

[8] T. M. C. Chu and H.-J. Zepernick, "On secrecy capacity of full-duplex cognitive cooperative radio networks," in *IEEE International Conference on Communications Workshops*, Kansas City, USA, May 2018, pp. 1-6.

[9] T. M. C. Chu, H. Phan, and H.-J. Zepernick, "Cognitive MIMO AF relay network with TAS/MRC under peak interference power constraint" in *Proc. IEEE International Confer-*

ence on Advanced Technologies for Communications, Ho Chi Minh City, Vietnam, Oct. 2013, pp.1-6.

[10] H. A. Suraweera, G. K. Karagiannidis, Y. Li, H. K. Garg, A. Nallanathan and B. Vucetic, "Amplify-and-forward relay transmission with end-to-end antenna selection," in *Proc. IEEE Wireless Communication and Networking Conference*, Sydney, Australia, Apr. 2010, pp. 1-6.

[11] J. Zhang and M. C. Gursoy, "Relay beamforming strategies for physical-layer security," in *Proc. IEEE Annual Conference on Information Sciences and Systems*, Princeton, USA, Mar. 2010, pp. 1-6

[12] M. Xu, H. Zhu, H. Xu, B. Wang and S. Zhu, "Joint optimization of packet length and transmission energy in amplify-and-forward relay networks," in *Proc. IEEE International Conference on Computational Intelligence and Security*, Hangzhou, China, Nov. 2018, pp. 259-263.

[13] J. Li and A. P. Petropulu, "Optimality of beamforming for secrecy capacity of MIMO wiretap channels," in *Proc. IEEE International Workshop on Information Forensics and Security*, Costa Adeje, Spain, Dec. 2012, pp. 276-281.