WARP-based Experiments of Configurable Beamforming on Physical Layer Security

Yuanrui Zhang*, Roger Woods*, Alan Marshall‡, Youngwook Ko*
* ECIT, Queen's University Belfast
Belfast, Northern Ireland, UK
Email: {yzhang31, r.woods, y.ko}@qub.ac.uk
‡ Electrical Engineering and Electronics, University of Liverpool
Liverpool, England, UK
Email: Alan.Marshall@liverpool.ac.uk

Abstract

This work investigates a novel approach called configurable beamforming on wireless physical layer security against passive eavesdroppers with Wireless Open-Access Research Platform (WARP). The aim is to create physical regions surrounding the intended user by configuring antenna array. By adapting the array configuration according to the intended user's channel state information, it allows the vulnerability of the physical regions to eavesdropping to be reduced. The theory analysis and implementation on WARP is examined in this work. Two WARP boards are deployed in a room where one with an antenna array serves as the access point and the other one serves as a general user. A range of antenna array configurations are investigated. Results using the real studies are then used to advise on the optimum array configuration for a user traversing a coverage area.

I. Introduction

While the recent developments of wireless technologies lead us to the era of the 5th generation, it is a remaining issue that wireless communications are vulnerable in an adversarial environment. For example, One common scenario in the indoor WiFi network is passive eavesdroppers attempting to intercept the message in the open air. The physical layer security rises in response to this challenge. While many encryption-based methods that are implemented in the layers above physical layer have their shortages, the security provided in physical layer acts as an extra layer of protection.

The authors in [1] proposed *configurable beamforming technique* that adapts the array configuration to the intended user's channel state information (CSI) in such a way that the surrounding region of the intended user is minimized. A correct reception is only possible when a receiver is inside this region. Thus, the chance that a passive eavesdropper of which the location is random to the access point (AP) is inside the region is reduced.

The configurable beamforming technique is proposed based on the analysis of different systematic factors in a free-space environment. This work further investigates the implementation of this algorithm on WARP. Several difficulties are dealt with regarding to the real implementation of this algorithm. The real measurements both in anechoic chamber and a normal indoor environment are carried out and more results are anticipated to come in the few week.

In Fig. 1, Alice is the transmitter who wishes to send messages to the intended receiver Bob in the presence of a passive eavesdropper Eve. In the context of an 802.11n network, if we envisage that the access point (AP) equipped with an antenna array acts as Alice, then *beamforming* can be used to restrict the eavesdroppers' access to the signals. In [2], a metric called exposure region (ER) was introduced to refer the area within which an eavesdropper can access and decode the signals being transmitted.

The received power of Bob can be adjusted using beamforming with CSI at the transmitter. However, the AP does not have knowledge of Eve, or of her CSI, thus Eve could be located within the ER. In order to decrease the possibility of Eve being able to receive the signal correctly, the ER should be minimized. The problem can be formulated to minimizing the area of the ER A according to Bob's location p_B on the condition that Bob's received power P_{rB} must be guaranteed to be above a threshold power P_{th}. The ER is affected by the array configuration, i.e., the number of antenna elements N and their spacing Δd, and Bob's location p_B which affects the channel condition. Thus, the problem can be posed as follows.

$$\begin{aligned} &\min A(N, \Delta d) \\ &\text{s.t. } P_{rB}(p_B) \geq P_{th} \end{aligned} \tag{1}$$

We first try to measure the received signal strength (RSS) across a room with two WARP boards. One board is equipped with a 4-element antenna array and serves as the transmitter, while the other is a general user which has only one antenna. To start with, we use a single element in the array (an omni-directional antenna) to transmit and move the receive antenna across a grid with 0.5 meter interval in an open space with light-of-sight (LOS) path. In Figure 2 the measured RSS of this area is given.

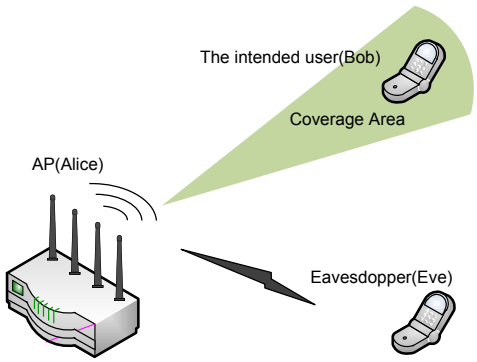


Fig. 1. A three-party communication model: Alice, Bob and Eve. The shadow area surrounding Bob illustrates the ER.

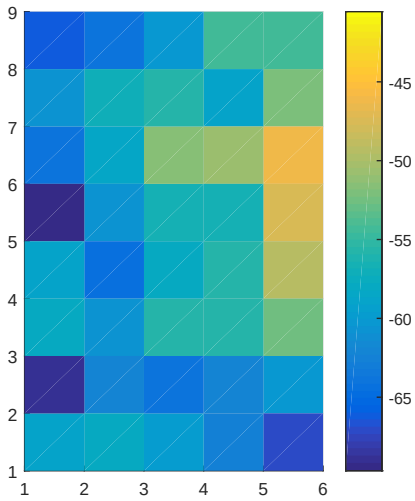
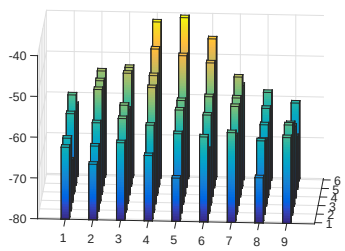
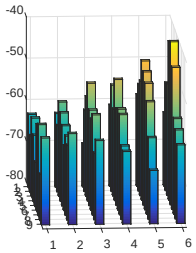


Fig. 2. RSS across a 9×6 gird, top view.

The transmitter's coordinate is (5,6). It can be seen that the RSS decreases as the receiver is further away from the transmitter. It can be better observed in Figure 3 that the decrease along X- and Y-axis fits an exponential decay profile.



A view along Y-axis



A view along X-axis

Fig. 3. RSS across a 9×6 gird

REFERENCES

[1] Y. Zhang, A. Marshall, R. Woods, and Y. Ko, "Creating secure wireless regions using configurable beamforming," in *Proc. of the 25th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications(PIMRC)*, Washington, USA, Sep. 2014.

[2] S. Lakshmanan, C. Tsao, R. Sivakumar, and K. Sundaresan, "Securing wireless data networks against eavesdropping using smart antennas," in *Proc. of The 28th International Conference on Distributed Computing Systems(ICDCS)*, Beijing, China, Jun. 2008, pp. 19–27.