Physical Layer Security based on Time Reversal Technique for Urban Radio Channels

Hassan El-Sallabi*, Yahia Basahl and Abdulaziz Aldosari
Emiri Signal Corps and Information Technology, QAF
Qatar

***Abstract*— This work presents experimental characterization of feasibility of physical layer security based on time reversal technique for radio channels. The investigation is for outdoor urban microcellular radio channels for both scenarios of fixed and mobile receivers. The investigation is at frequency range of 2.4 GHz and bandwidth of measurement system is 100 MHz. A metric based on difference between strongest and 2nd strongest peak on power delay profile is proposed and presented as performance indicator.**

Keywords— Physical Layer Security, Time Reversal, Outdoor, Radio Channels.

I. Introduction

The aim of physical layer security is to prevent eavesdropping to ensure secure communications [1]. Physical layer (PHY) is the first layer of the seven layers of Open System Interconnect (OSI) model. The upper layers of the network protocol stack handles authentications, privacy, and confidentiality using private-key and public-key cryptosystems. Different network layers used different techniques [2]. The upper layer usually assumes the eavesdroppers have limited computational resources, which is not anymore true due to advanced technology of modern computers. This makes encryption/decryption algorithms to be not very difficult to break. The proposed approach applies for slow fading radio channels, when the propagation delays, processing delay Tx to construct a pulse shaping and at Rx for channel state estimation is less than coherence time of the channel.

I. Physical Layer Security

Research results in information theory, signal processing, and cryptography highlighted the security that can be obtained by utilizing the imperfections of physical layer (IoPL) to design secure system. The information-theoretic research results show that IoPL can be harnessed to hide messages from eavesdropper and/or for authentications with "security keys" [3] that can be obtained from spatio-temporal properties of the radio channel. The fundamental principal of physical layer security is to exploit random nature and reciprocity of wireless channel without considering specific knowledge to computational capability of eavesdroppers. There are different techniques to achieve PHY security, e.g., Preprocessing Scheme (coding, key generation, and artificial noise scheme), game theoretic scheme, cooperation communications, signal processing time reversal technique, etc. The time reversal technology has the capability to focus energy both in time and spatial domains [4], [5]. This energy harvesting may have an important role in high spatial resolution that secures data transmission between transmitter and intended receiver and become very difficult to detect for eavesdropper. The idea is based on the fact that each receiver, either intended or eavesdropper, has a unique spatial and temporal channel impulse response relative to the position of the transmitter.

II. System Model

Figure 1 shows system level scenario of legitimate channel between transmitter (Alice) and receiver (Bob) and illegitimate channel between transmitter and eavesdropper (Eve) [6]. Eve does not make any active attack but passively tries to extract information from transmission between Alice and Bob. For a MIMO communication system with M transmit antennas and N receive antennas; whose approximate capacity is given in [7], the impulse response at time t from transmit antenna at $\overline{r_m}$ to receive antenna at $\overline{r_n}$ is $h_{n,m}(t,\tau,\ \overline{r_m} \to \overline{r_n})$, with τ denoting the propagation delay of multipath components. The receiver estimates the channel impulse response (CIR) based on known transmitted sequence and sends back to the transmitter the time reversed CIR. Details of the system model can be traced in [4].

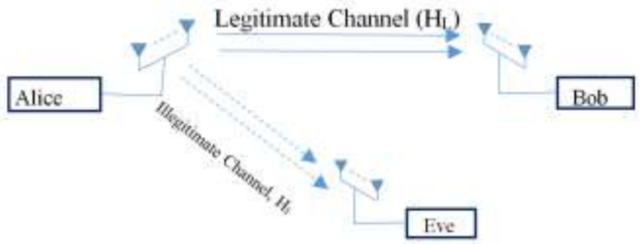

Figure 1. System model.

III. Performance Metrics and results

The measurement setup is: 1) A 120-deg sector transmit antenna mounted on top of a tripod of 4 m height, located on street level, this yields a microcellular type of antenna deployment; 2) Receiver antenna array on omnidirectional antennas mounted on a trolley with variable spacing of up to a few lambdas. The measurement data were collected in outdoor environment in Ilmenau, Germany during participation of first author in testing of wideband channel sounder described in

978-1-5386-7102-3/18/$31.00 ©2018 IEEE

[4]. The performance of wideband PHY time reversal system depends on time reversal properties: 1) temporal compression; 2) spatial focusing; and 3) channel hardening. These can be reflected in a measure based on difference between strongest peak to second strongest peak in dB scale for the antenna of Bob's receiver and antenna of Eve's receiver. The high difference indicates highly temporally compressed and focused energy (see Figure 2), which has to be at Bob's antenna and noise like signal at Eve's antenna (see Figure 3). Temporal compression shows reduction in effective delay window where most of energy is aggregated. The spatial focusing implies energy is concentrated at Bob's antenna and become noise like at Eve's antenna. This is the key feature that can be used for physical layer security. Collecting large number of CIR snapshots for both static receiver and transmitter and moving receiver, at pedestrian speed, allows us to statistically study the performance of time reversal technique for physical layer security. Figure 4 and Figure 5 show histogram of data of aforementioned metric at both Eve's antenna and Bob's antennas for both static and mobile receivers, respectively. We can see the focusing energy at Bob's antenna for both channels. This can be seen in large difference between strongest peak and 2nd strongest peak. The higher the difference is the more focused energy to intended Bob's receiver. The spread (noise like) energy at Eve's antenna can also clearly be observed. One can notice a small difference between strongest peak and 2nd strongest peak value. The smaller the difference values the noise like spread of energy in delay domain. This makes it more difficult for eavesdroppers to detect as signals become weak.

IV. Conclusion

This work presents empirical characterization of time reversal channels for physical layer security applications for outdoor channels. Both scenarios fixed and mobile receivers are tested. The difference between strongest peak and second strongest peak is used as a focusing metric to measure energy focusing at Bob's antenna and Eve's antenna. It has been shown experimentally that the time reversal technique can used for physical layer security as it focuses energy at intended antenna and minimize energy at eavesdropping antenna.

References

[1] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE communications Surveys and Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[2] H. Bidgoli, Handbook of Information Security, Threats, Vulnerabilities, prevention, Detection and Management, vol. 3, John Wiley, 2006.

[3] M. Bloch and J. Barros, Physical-Layer Security: from Information Theory to Security Engineering, 2011, Cambridge University Press

[4] H. El-Sallabi, P. Kyritsi, A. Paulraj, and G. Papanicolaou, "Experimental Investigation on Time Reversal Precoding for Space Time Focusing in Wireless Communications," *IEEE Trans. Instr. Measur.,* vol. 59, no. 6, pp. 1537–1543, 2010.

[5] M. E. Yavuz and F. L. Teixeira, "Ultrawideband Microwave Sensing and Imaging Using Time-Reversal Techniques: A Review," *Remote Sensing* 1(3), Sep. 2009.

[6] R. Liu and W. Trappe, Securing Wireless Communications at the Physical Layer, 2010, Springer

[7] J Salo, etal, "Approximate distribution of capacity of Rayleigh fading MIMO channels," *Electronic Letters* 40 (12), 741-742.

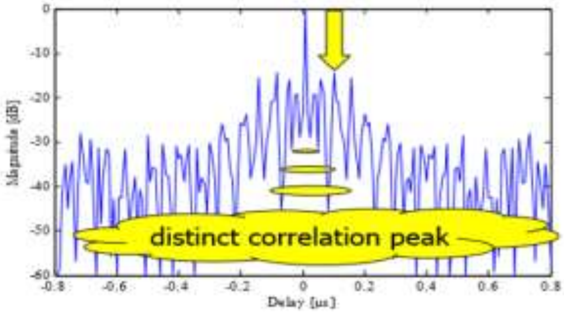

Figure 2. Snapshot at Bob's antenna.

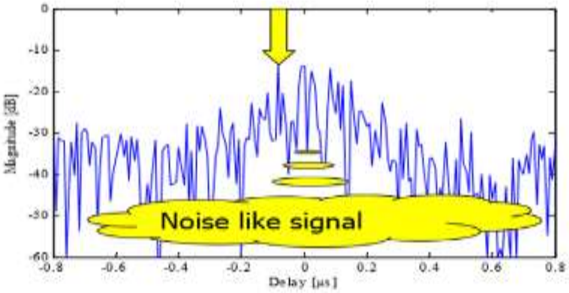

Figure 3. Snapshot at Eve's antenna.

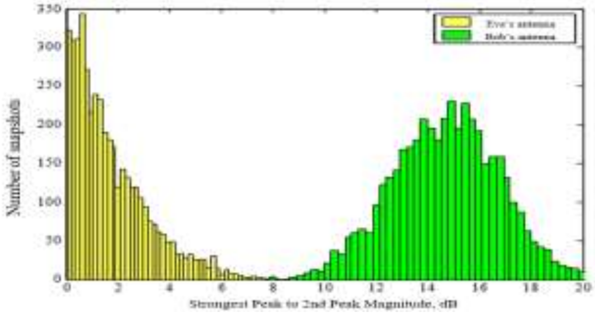

Figure 4. Fixed receiver scenario.

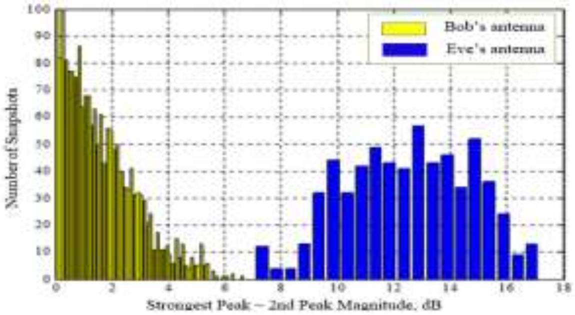

Figure 5. Mobile receiver scenario.