IITB-Monash Research Academy

Indian Institute of Technology Bombay | MONASH University

An Indian-Australian research partnership

Project Title:	**Wireless secret communications**	
Project Number	**IMURA0339**	
Monash Supervisor(s)	Yi Hong	*Full names and titles*
Monash Primary Contact:	Yi.Hong@monash.edu	*Email, phone*
Monash Head of Department:	Jamie Evans	*Full name, email*
Monash Department:	Electrical and Computer Systems	*Full name*
Monash ADRT:	Emanuele Viterbo	*Full name, email*
IITB Supervisor(s)	Virendra Sule	*Full names and titles*
IITB Primary Contact:	vrs@ee.iitb.ac.in	*Email, phone*
IITB Head of Department:	Abhay Karandikar, head@ee.iitb.ac.in	*Name, Email,*
IITB Department:	Department of Electrical Engineering	*Full name*

Research Academy Themes:

Highlight which of the Academy's Theme(s) this project will address?

(Feel free to nominate more than one. For more information, see www.iitbmonash.org)

1. **Advanced computational engineering, simulation and manufacture**
2. Infrastructure Engineering
3. Clean Energy
4. Water
5. Nanotechnology
6. Biotechnology and Stem Cell Research

The research problem

Define the problem

A wireless communication system can be assessed from the following three aspects: 1) Efficiency; 2) Reliability; 3) Security. By nature, wireless channels offer a shared medium, particularly favourable to eavesdroppers and jammers. In this project, we concern about the problem howsecure the communication system using physical layer techniques when the system is jammed and eavesdropped by the intruders. We will target at different possible solutions against eavesdropping problems.

A direction for research in security can also be explored for wireless channels from the point of view of providing features such as key management, authentication and more generally public key facility. Cryptographic features are usually provided at the data layer of any communication. However if

cryptographic functions are feasible at physical layer, this would have possible advantages over the cryptographic schemes operating at the data layer. A part of this research would be devoted to explore these directions.

Project aims

Define the aims of the project

Traditionally, security is an issue independent from physical layer in the 7 layers of the OSI Model and it relies heavily on the upper-layer operation. The symmetric data encryption/decreption algorithm has been widely used in networks. In this project we target at physical layer security to further enhance the wireless security. Currently several attempts to PHY security include artificial noise technique which is designed to transmit a noisy signal to confuse eavesdropper but remains orthogonal to the channels between transmitter and receiver. Other approaches including secure key distributions are proposed to maximize the secrecy capacity. Since they are still in initial status, in the project, we will be aiming at investigating those practical wireless physical layer approaches (such as artificial noise and secure key distributions, etc …) to improve the performance of wireless communications against eavesdropping.

Expected outcomes

Highlight the expected outcomes of the project

The outcomes of the project is to have robust PHY wireless communications and networking against eavesdropping with high transmission data rate.

How will the project address the Goals of the above Themes?

Describe how the project will address the goals of one or more of the 6 Themes listed above.

The research will make a significant contribution to the physical layer security for wireless communications and networking.

Capabilities and Degrees Required

List the ideal set of capabilities that a student should have for this project. Feel free to be as specific or as general as you like. These capabilities will be input into the online application form and students who opt for this project will be required to show that they can demonstrate these capabilities.

Student shall have background of communication theory, signal processing, wireless communications, cryptography and some basic Matlab and SAGE programming skills.