PHYSICAL LAYER SECURITY

(Short Course)

Assistant Prof. Lorenzo Mucchi
Dept of Electronics and Telecommunications
University of Florence
Via santa marta 3, 50139 Firenze, Italy

28 - 29 May 2012 at the University of Oulu

Description:

Along with the rapid development of wireless communication networks, wireless security has become a critical concern. Unfortunately, security risks are inherent in any wireless technology. Some of these risks are similar to those of wired networks, some are exacerbated by wireless connectivity and some other are completely new. First, the most significant source of risks in wireless networks is that the technology's underlying communications medium, the airwave, is open to intruders. Second, mobile and handheld wireless devices are resource constrained (e.g.: battery life); hence such devices have limited transmission power and may use weaker cryptographic mechanisms for saving power, thereby making them easy targets for powerful adversaries. Third, the lack of trusted third party (TTP) or certification authority (CA) in ad hoc wireless networks pose serious challenges to identity and trust management. Fourth, multi-hop wireless network inherently assumes cooperation between nodes for packet routing and forwarding, whereas a compromised node may refuse to cooperate (by being greedy or malicious). Fifth, handheld mobile devices cannot afford the same level of physical security as an enterprise server and thus, may be easily stolen. A direct consequence of these risks is the loss of data confidentiality and integrity and the threat of denial of service (DoS) attacks to wireless communications. Unauthorized users may gain access to agency's system and information, corrupt the agency's data, consume network bandwidth, degrade network performance, launch attacks that prevent authorized users from accessing the network, or use agency's resources to launch attacks on other networks. These problems are even exacerbated in future unstructured sensors and ad-hoc networks with dynamically and rapidly varying topology.

One of the fundamental issues for physical-layer built-in security is the capacity of the transmission channel when built-in security is guaranteed without relying on upper layer data encryption. Such capacity is named secret channel capacity (SCC). The secrecy is defined as information-theoretic secrecy, i.e., the adversary's received signal gives no more information for eavesdropping than purely guessing. Information-theoretic secrecy is in fact equivalent to perfect secrecy. Practically, it means null or negligibly low interception probability (LPI).

The course will give the essential knowledge on physical layer security techniques for wireless networks.

Brief Bio:
Lorenzo Mucchi was born in Rome, Italy, in 1971. He received the Dr. Eng. Degree (*Laurea*) in Telecommunications Engineering from the University of Florence (Italy) in 1998 and the Ph.D. in Telecommunications and Information Society in 2001. Since 2001 he has been with the Department of Electronics and Telecommunications of the University of Florence as a Research Scientist. During the academic year 2000-2001, he spent a 12-months period of research at the Centre for Wireless Communications, University of Oulu, Finland. His main research areas are spread spectrum techniques (UWB, CDMA), cooperative communication systems, cognitive radio, wireless security, MIMO and diversity techniques and multi-satellite communications. He is involved in several national and international projects. Currently, he has published 6 chapters in 6 different international books, 16 papers in international journals and several papers (~54) in international conference proceedings during his research activity. Since 2004 he has been TPC of about 30 international conferences all around the world. Since 2008 he is professor of Information Technologies at the University of Florence. Lorenzo Mucchi is also a full member of the Institute of Electrical and Electronics Engineers (IEEE) and permanent member of the International Association of Science and Technology for Development (IASTED) Technical Committee on Telecommunications.

Conduction:
Written Exam, no material can be used during the exam.
Students need to attend the lectures, to be eligible for the exam.

The amount of credits is yet to be confirmed.

Literature:
Bloch Matthieu; Barros Joao
PHYSICAL-LAYER SECURITY
FROM INFORMARION THEORY TO SECURITY ENGINEERING
Cambridge University Press, 2011

Liu Ruoheng; Trappe Wade (Eds.)
Securing Wireless Communications at the Physical Layer
Springer, 2010

Yingbin Liang, H. Vincent Poor, Shlomo Shamai (Shitz)
Information Theoretic Security
Now Publishers, 2009

Course Contents:

Day	Topics	Classes (45 min)
1. Mo 28.5.	1. Introduction to physical layer security (8:30-10:00)	2
	2. Information-theoretic approach (10:15-11.00 and 12:00-12:45)	2
	3. Secrecy capacity (13:00-14:30)	2
2. Tu 29.5.	4. Coding for security (8:30-10:00)	2
	5. System aspects (10:15-11:00 and 12:00-12:45)	2
	6. Advanced techniques (13:00-14:30)	2
3. Date T.B.A	Exam (9:00-12:00)	3