PHYSICAL LAYER WIRELESS SECURITY
(Short Course)
Assistant Prof. Lorenzo Mucchi
Dept. of Information Engineering (DINFO), University of Florence, Italy
June 9-11, 2014, University of Oulu

Description:
Nowadays the domination of wireless communications (as universal way to access information anytime anywhere) presents a major risk to society, because of widely recognized security leaks in the current wireless radio access technologies. Basically, the security today relies on bit-level cryptographic techniques and associated protocols at various levels of the data processing stack. These solutions have drawbacks, which are currently a concrete delay to the progress of the digital society. The protocols which are currently considered secure use complex cryptographic schemes, either asymmetric or symmetric. The security level, which can be reached with these techniques, relies on the amount of complex calculations required to perform decrypting analysis on the eavesdropped data. There is no cryptographic algorithm that is mathematically demonstrated to be unbreakable. The security is based on the (huge) amount of time to perform decrypting analysis. The robustness of encryption algorithms against eavesdropping becomes day by day more critical due to the increase in computing power of current devices, requiring more frequent updating and simplified cryptographic keys. The distribution of the secret keys is also another hard task for current and future wireless networks, since the keys has to be changed frequently over an always accessible (and crowded) resource as the radio channel.

Recently, researchers came up with a new security approach, from information theory fundamentals, which is focused on the exploitation of the intrinsic property of the radio environment and of the electromagnetic waves to produce security at physical layer, with no assumption on the computational capabilities of eavesdroppers and with the added benefit of reducing the load on the security protocols at the upper levels.

The course will give the fundamentals of physical layer security approach for wireless networks, and in particular, how it can help not only by adding security at one layer, but also in other aspects like key distribution.

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 physical layer 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, 21 papers in international journals and several papers (~60) in international conference proceedings during his research activity. Since 2004 he has been TPC of about 45 international conferences all around the world. Since 2008 he is professor of Information Technologies at the University of Florence. Lorenzo Mucchi is also a senior 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.

Course Contents:

<table>
<thead>
<tr>
<th>Day</th>
<th>Topics</th>
<th>Classes (à 45 min)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>1. Review of existing security in wireless networks (8:30-10:00)</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>2. Introduction to physical layer security (10:15-11.00 and 12:00-12:45)</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>3. Information-theoretical approach to security I (13:00-14:30)</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>4. Information-theoretical approach to security II (8:30-10:00)</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>5. Secrecy Capacity (10:15-11:00 and 12:00-12:45)</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td>6. Coding schemes for approaching secrecy capacity (13:00-14:30)</td>
<td>2</td>
</tr>
<tr>
<td>2.</td>
<td>Recent advances (8:15-10:45)</td>
<td>3</td>
</tr>
</tbody>
</table>
Exam:
2 weeks after the end of the course.

Conduction:
Written Exam (3h), no material can be used during the exam.
Students need to attend the course, to be eligible for the exam.

The amount of credits is yet to be confirmed.

Literature:

Xiangyun Zhou, Lingyang Song, Yan Zhang
Physical Layer Security in Wireless Communications
CRC Press, 2013

BLOCH MATTHIEU; BARROS JOAO
PHYSICAL-LAYER SECURITY
FROM INFORMATION 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