Interplay between Information-Theoretic and Computational Security in Wireless Channels

Manuel Barbosa
DI/CCTC, U.Minho

João Barros
IT Porto/DCC U.Porto

January 2008

Context

This dissertation proposal results from the collaboration between the Cryptography and Information Security group at CCTC and the Networking and Information Processing Group of IT Porto in the FCT Project titled Wireless Information-Theoretic Security (WITS). The project duration is three-years and kick-o will take place in early 2008.

The goals of the WITS (Wireless Information-Theoretic Security) project are (1) to help lay the information-theoretic foundations of secure communications over unreliable wireless networks with multiple users, and (2) develop secure protocols based on novel physical layer security technologies (most notably, secrecy capacity achieving channel codes) in combination with standard cryptographic primitives.

Wireless communication technologies offer the promise of low-cost pervasive access and exchange of information over increasingly widespread data networks. Although much has been accomplished in terms of how to design, construct, and manage such networks, the fundamental mechanisms that allow full confidentiality and assure the authenticity of the transported data are not yet well understood. Wireless security thus remains a formidable challenge. Today, standard approaches to security are based on cryptographic protocols at a higher layer. Realizing that data security is too important to be left to one layer only - particularly if it can be done in a cost effective manner at other layers, as well - we propose a different paradigm:

to design communication protocols that combine physical layer and higher layer encryption technologies and thus provide security levels well beyond those of cryptographic protocols alone. Inspired by foundational research on information-theoretic security (widely accepted as the strictest level of security) we envision a network security sub-system that relies not only on the computational intractability of certain functions but also on the physical properties and natural randomness of the wireless communication channels that compose the network.

This dissertation will be integrated into either *Task 1: Interplay between Information-Theoretic Security and Classical Cryptography* and *Task 3:Secure Communication Protocols and System Aspects of Wireless Information-Theoretic Security*. The WITS project aims at achieving a security level in wireless communication networks beyond the standards offered by public-key encryption, whose assumptions of computational hardness of certain functions remain unproven. Instead, as outlined above, we propose information-theoretically secure protocols over wireless channels, relying on physical-layer technologies such as secure channel coding. The objective of Task 1 is to explore the differences and possible synergies between the two aforementioned approaches, which are very fundamental and not yet well understood. The main results of Task 3 will be communication protocols that combine end-to-end encryption and physical layer methods, as well as system architectures for wireless comunications featuring multi-layered security. The development of secure protocols is essential towards providing the proof of concept for the security technologies that are proposed.

References

[1] U. M. Maurer, "Secret key agreement by public discussion from common information", IEEE Trans. on Information Theory, vol. 39-3, 1993.

[2] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels", Proc. IEEE Symposium on Information Theory, Seattle, WA, July 2006.