Physical layer security for IoT applications

Miroslav Mitev

Supervisors: Martin Reed, Arsenia Chorti

A thesis submitted for the degree of PhD

School of Computer Science and Electronic Engineering

University of Essex

August 2020

Abstract

The increasing demands for Internet of things (IoT) applications and the tremendous increase in the volume of IoT generated data bring novel challenges for the fifth generation (5G) network. Verticals such as e-Health, vehicle to everything (V2X) and unmanned aerial vehicles (UAVs) require solutions that can guarantee low latency, energy efficiency, massive connectivity, and high reliability. In particular, finding strong security mechanisms that satisfy the above is of central importance for bringing the IoT to life.

In this regards, employing physical layer security (PLS) methods could be greatly beneficial for IoT networks. While current security solutions rely on computational complexity, PLS is based on information theoretic proofs. By removing the need for computational power, PLS is ideally suited for resource constrained devices. In detail, PLS can ensure security using the inherit randomness already present in the physical channel. Promising schemes from the physical layer include physical unclonable functions (PUFs), which are seen as the hardware fingerprint of a device, and secret key generation (SKG) from wireless fading coefficients, which provide the wireless fingerprint of the communication channel between devices.

The present thesis develops several PLS-based techniques that pave the way for a new breed of latency-aware, lightweight, security protocols. In particular, the work proposes: i) a fast multi-factor authentication solution with verified security properties based on PUFs, proximity detection and SKG; ii) an authenticated encryption SKG approach that interweaves data transmission and key generation; and, iii) a set of countermeasures to man-in-the-middle and jamming attacks. Overall, PLS solutions show promising performance, especially in the context of IoT applications, therefore, the advances in this thesis should be considered for beyond-5G networks.

Acknowledgments

I would like to thank the University of Essex, School of Computer Science and Electronic Engineering (CSEE) Doctoral Training Programme for sponsoring my studies and made my dream of pursuing a PhD degree reality.

I would like to sincerely thank my supervisors, Dr Martin Reed and Dr Arsenia (Ersi) Chorti for their valued advice and motivation while conducting this research, thanks to their continuous guidance I enjoyed a stress-free working environment. They let me freely choose my research directions and demonstrated a great deal of support. Our meetings and discussions were the key that brought this thesis to life. Furthermore, I would like to express my gratitude for the networking and travelling opportunities which greatly contributed in enhancing my research experience.

My sincere thanks also go to the members of staff of the School of Computer Science and Electronic Engineering and the Department of Mathematical Sciences, University of Essex who provided me the opportunity to become a Graduate teaching assistant and Graduate lab assistant. This was an amazing experience which helped me to advance with my PhD studies.

I would like to thank my co-authors Dr. Leila Musavian and Dr. Veronica Belmega for their insightful comments and support. I would also like to thank Dr. Mahdi Herfeh for our ongoing collaboration and future publication on the short-block length solution which is not fully contained in this thesis.

Finally, I wish to express my deepest gratitude to my family members, my friends, my colleagues, and my life-partner Elena, for their constant support throughout writing this thesis.

Contents