

## CALL FOR BOOK CHAPTER

# Title: Security in RFID and Sensor Networks

(to be published by Auerbach Publications, Taylor&Francis Group)

### Introduction

Radio Frequency Identification (RFID) gains a recent explosion of interest in both industry and academia. A variety of applications include supply chain management, electronic payment, RFID passport, environmental monitoring and control, office access control, intelligent labels, earthquake monitoring, target detection and tracking, port management, food production control, animal identification, airports, and so on. It is strongly believed that many more scenarios will be identified when RFID principle is thoroughly understood, cheap components are available and, most importantly, RFID is sufficiently secured. Security is one of the open issues before the wide deployment of RFID systems. On the other hand, recent advances in digital electronics, embedded systems, and wireless communications have motivated significant interest in Wireless Sensor Networks (WSNs). A WSN consists of a large number of small sensors with sensing, data processing, as well as communication and networking capabilities. WSNs are characterized of dense node deployment, unreliable sensor, frequent topology change, and severe power, computation, and memory constraints. These unique characteristics pose new challenges to the design of WSNs. Because sensor networks usually transmit sensitive data and operate in hostile unattended environments, it is imperative that the security issues be addressed from the beginning of the system design. However, due to inherently limited resource and computing capability, security mechanisms in sensor networks are significantly different from traditional computer security. In practice, there is an increasing trend in integrating RFID and WSNs due to their complementary nature, flexible combination and demand for ubiquitous computing. The two technologies integration can exponentially increase visibility and monitoring capability. Comparing with RFID or sensor networks alone, integrated RFID&WSN has more diversity of security and privacy challenges.

### Recommended Topics (not limited to)

#### Part 1: Fundamentals of RFID and Wireless Sensor Networks

- RFID
- Wireless Sensor Networks (WSNs)
- Integrated RFID and WSNs

#### Part 2: Security in RFID

- Threats, attacks and vulnerabilities
- RFID reader security, identification and protocols
- Authenticity, authentication and privacy
- Public-key Infrastructure; key update protocols
- Encryption techniques
- DDoS attack detection
- Tag database security
- Sort signature techniques for RFID
- Scalability issues
- Hardware implementation

#### Part 3: Security in Wireless Sensor Networks

- Digital signature transponder
- Data protection & privacy, contract agreements
- Key update protocols
- Asymmetric and symmetric key-based approach
- DDoS attack detection, intrusion detection
- Hardware implementation
- Authenticated, anonymous Routing

- Wormhole attacks
- Wireless terrorism
- Link layer cryptography
- Message authentication codes (MACs)
- Physical tampering
- High-level security services
- Secure group management
- Policy management

#### Part 4: Security in RFID and WSN Integrated Networks

- Smart home security issues, models and services
- WSNs and RFID secure application for smart home
- Secure applications, like Personal health care, Business meetings, Near field communications, Systems surveillances
- Secure routing protocols
- Node capture
- Secure localization
- Hardware implementation

#### Important Dates

- You are invited to submit a 1-2 pages proposal describing the topic of your chapter. The proposal should include the chapter organization, number of pages of the final manuscript and contact authors. Deadline: 30, August 2007
- Notification of proposal acceptance: 30, September 2007
- Full chapter submission: 30, December 2007
- Review report received: 31, Feb. 2008
- Final version submission: 31, April 2008

#### Manuscript Submission

- Estimated, each chapter should has about 35 pages with 12 font size, double-space format.
- Name figure files consecutively (Fig001.eps, Fig002.eps, etc.). Do not use descriptive names.
- Do not embed figures; please add all the figures at the end of the document.
- Using the reference format as follows:
- `\begin{thebibliography}{50}`
- `\bibitem{XXXXX}`
- Author, Title, publication, publishing time;
- .....
- `\end{thebibliography}`

**Note: each lead chapter author will get a free copy of the book.**

#### Contact

Please make correspondence and paper submissions to:

Dr. Yan ZHANG  
 Simula Research Laboratory, Norway  
 Email: yanzhang@ieee.org

Dr. Paris KITSOS  
 School of Science & Technology,  
 Hellenic Open University (HOU), Greece  
 Email: pkitsos@ieee.org