Recent Advances in Security and Privacy for Wireless Sensor Networks

Fei Yu,1 Chin-Chen Chang,2 Jian Shu,3 Iftikhar Ahmad,4 Jun Zhang,5 and Jose Maria de Fuentes6

1Peoples’ Friendship University of Russia, Moscow 117198, Russia
2Feng Chia University, Taichung 40724, Taiwan
3Nanchang Hangkong University, Nanchang 330000, China
4King Saud University, Riyadh 92144, Saudi Arabia
5Deakin University, Burwood, VIC 3125, Australia
6Universidad Carlos III de Madrid, Madrid 28036, Spain

Correspondence should be addressed to Fei Yu; hunanyufei@126.com

Received 20 May 2015; Accepted 27 May 2015

Copyright © 2015 Fei Yu et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Wireless networks have experienced explosive growth during the last few years. Nowadays, there are a large variety of networks spanning from the well-known cellular networks to noninfrastructure wireless networks such as mobile ad hoc networks and sensor networks. Communication security is essential to the success of wireless sensor network applications, especially for those mission-critical applications working in unattended and even hostile environments. However, providing satisfactory security protection in wireless sensor networks has ever been a challenging task due to various network and resource constraints and malicious attacks.

In this special issue, we concentrate mainly on security and privacy as well as the emerging applications of wireless sensor networks. It aims to bring together researchers and practitioners from wireless and sensor networking, security, cryptography, and distributed computing communities, with the goal of promoting discussions and collaborations. We are interested in novel research on all aspects of security in wireless sensor networks and tradeoff between security and performance such as QoS, dependability, and scalability. The special issue covers industrial issues/applications and academic research into security and privacy for wireless sensor networks.

This special issue includes a collection of 14 papers selected from 74 submissions to 9 countries or districts (China, India, South Korea, Chennai, USA, Pakistan, Saudi Arabia, Malaysia, and Taiwan). All submitted papers followed the same standard (peer-reviewed by at least three independent reviewers) as applied to regular submissions.

In the paper entitled “Accurately Identifying New QoS Violation Driven by High-Distributed Low-Rate Denial of Service Attacks Based on Multiple Observed Features,” J. Kang et al. propose using multiple observed features of network traffic to identify new high-distributed low-rate Quality of Services (QoS) violation so that detection accuracy may be further improved.

In the paper entitled “A Self-Adaptive Wireless Sensor Network Coverage Method for Intrusion Tolerance Based on Trust Value” Z. Chen et al. propose a network coverage method for invasive tolerance based on trust value of nodes by combining the trust value model with the reliable coverage optimization.

The paper entitled “Trust-Aware and Low Energy Consumption Security Topology Protocol of Wireless Sensor Network” by Z. Chen et al. tries to take node trust into consideration when building a network topology, so as to ensure the security of the network communication. The TLES algorithm is based on the analysis of node behavior. It develops a variety of trust factors and then performs comprehensive analysis with direct information and recommended information.
In the paper entitled "A Data Processing Middleware Based on SOA for the Internet of Things" by F. Wang et al., based on characteristics of the architecture and challenges of information fusion in the IoT, the paper designs a middleware platform based on SOA architecture for the integration of multisource heterogeneous information.

In the paper entitled "Survey of Security Technologies on Wireless Sensor Networks" Q. Yang et al. summarized research progress of sensor network security issues in key management, authentication, and secure routing as three aspects, by analyzing and commenting on these results advantages and disadvantages, and pointed out the future direction of the hot research field.


In the paper entitled "Parking Query in Vehicular Delay-Tolerant Networks with Privacy Protection Based on Secure Multiparty Computation" H. Huang et al. design the routing protocol RPAD from the direction and distribution density of the vehicle and the base station is considered to be a reference.

In the paper entitled “A Novel Digital Certificate Based Remote Data Access Control Scheme in WSN” by W. Liang et al. a digital certificate based remote data access control scheme is proposed for safe authentication of accessor in wireless sensor network (WSN).

The paper entitled "Distributed Software-Attestation Defense against Sensor Worm Propagation" by J.-W. Ho proposed on-demand software-attestation based scheme to stop worm propagation in sensor network.


The paper entitled "Bi-iTRS: A Bio-Inspired Trusted Routing Scheme for Wireless Sensor Networks" by M. Zhang et al. presents a novel bio-inspired trusted routing scheme (BiTRS) based on ant colony optimization (ACO) and Physarum autonomic optimization (PAO).

The paper entitled "Research on Handoff Delay and Mobility Management Cost of Mobility Protocols in Wireless Sensor Networks" by A. Q. Zhao and Y. Hu focused on the research of mobility management cost of mobility support protocols and made analysis and comparison of mobility management cost among various mobility support protocols.

The paper entitled "Sequence Alignment with Dynamic Divisor Generation for Keystroke Dynamics Based User Authentication" by J. Ho and D.-K. Kang proposed sequence alignment with dynamic divisor generation (SADD) for user authentication by using the keystroke dynamics.

Acknowledgments
In particular, we would like to acknowledge the program committee members of Seventh International Symposium on Information Processing (ISIP 2014). This issue contains most of the revised and expanded versions of the selected quality papers presented at the Seventh International Symposium on Information Processing (ISIP 2014). We wish to express our deepest thanks to the program committee members for their help in selecting papers for this issue and especially the referees of the extended versions of the selected papers for their thorough reviews under a tight time schedule. ISIP 2014 took place on October 25-26, 2014, in Changsha, China, and was cosponsored by Jiangxi University of Science and Technology, China; Peoples’ Friendship University of Russia, Russia; South China University of Technology, China; Feng Chia University, Taiwan; Henan Polytechnic University, China; Nanchang Hangkong University, China; and Jiangxi University of Science and Technology, China. In closing, we would like to take this opportunity to thank the authors for the efforts they put in the preparation of the manuscripts and in keeping the deadlines set by editorial requirements. We hope that you will enjoy reading this special issue as much as we did putting it together.

Fei Yu
Chin-Chen Chang
Jian Shu
Iftikhar Ahmad
Jun Zhang
Jose Maria de Fuentes