Fei Yu, Chin-Chen Chang, Jian Shu, Iftikhar Ahmad, Jun Zhang, Jose Maria de Fuentes, "Recent Advances in Security and Privacy for Wireless Sensor Networks 2016", *Journal of Sensors*, vol. 2017, Article ID 3057534, 3 pages, 2017

DOI: 10.1155/2017/3057534

Hindawi
Journal of Sensors
Volume 2017, Article ID 3057534, 3 pages
https://doi.org/10.1155/2017/3057534

Editorial

Recent Advances in Security and Privacy for Wireless Sensor Networks 2016

Fei Yu,[1] Chin-Chen Chang,[2] Jian Shu,[3] Iftikhar Ahmad,[4] Jun Zhang,[5] and Jose Maria de Fuentes[6]

[1] *Peoples' Friendship University of Russia, Moscow, Russia*
[2] *Feng Chia University, Taichung, Taiwan*
[3] *Nanchang Hangkong University, Nanchang, China*
[4] *King Saud University, Riyadh, Saudi Arabia*
[5] *Deakin University, Melbourne, Australia*
[6] *Universidad Carlos III de Madrid, Madrid, Spain*

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

Received 8 February 2017; Accepted 8 February 2017; Published 23 February 2017

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 network. 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 25 papers selected from 97 submissions to 21 countries or districts (Australia, China, Croatia, France, India, Iraq, Jordan, Korea, Malaysia, Morocco, Oman, Pakistan, Poland, Russia, Saudi Arabia, Spain, Taiwan, Tunisia, Turkey, UK, and USA).

In the paper entitled "Multitask Learning-Based Security Event Forecast Methods for Wireless Sensor Networks," H. He et al. propose a sensor network security event forecast method named Prediction Network Security Incomplete Unmarked Data (PNSIUD) method to forecast missing attack data in the target region according to the known partial data in similar regions.

In the paper entitled "Prediction Approach of Critical Node Based on Multiple Attribute Decision Making for Opportunistic Sensor Networks" by Q. Chen et al., the conceptions of critical nodes, region contribution, and cut-vertex in multiregion OSN are defined; then an approach to predict critical node for OSN is proposed, which is based on multiple attribute decision making (MADM).

The paper entitled "Information Security of PHY Layer in Wireless Networks" by W. Fang et al. firstly identifies and summarizes the threats and vulnerabilities in PHY layer of wireless networks. Then, we give a holistic overview of PHY layer secure schemes, which are divided into three categories: spatial domain-based, time domain-based, and frequency domain-based.

The paper entitled "Enhancing Energy Efficiency of Wireless Sensor Network through the Design of Energy Efficient

Routing Protocol" by N. Zaman et al. proposes a new routing protocol entitled "Position Responsive Routing Protocol (PRRP)" and compares its performance with the well-known LEACH and CELRP protocols. The simulation results show a significant improvement over the aforementioned protocols in terms of energy efficiency and the overall performance of the WSN.

In the paper entitled "Study of Wireless Authentication Center with Mixed Encryption in WSN," Y. Lu et al. propose a wireless authentication center with mixed encryption named "MEWAC" according to shortcomings of the current schemes. MEWAC has the advantages of low cost, low power consumption, good performance, and stability; moreover, the authentication protocol improves the security of sensor nodes and reduces the overhead in node authentication.

The paper entitled "Multilevel Modeling of Distributed Denial of Service Attacks in Wireless Sensor Networks" by K. Mazur et al. proposes a model of a structural health monitoring network, being disturbed by one of the most common types of DDoS attacks, the flooding attack.

The paper entitled "RESH: A Secure Authentication Algorithm Based on Regeneration Encoding Self-Healing Technology in WSN" by W. Liang et al. considers the regeneration encoding self-healing and secret sharing techniques and proposes an effective scheme to authenticate data in WSN. The data is encoded by regeneration codes and then distributed to other redundant nodes in the form of fragments.

In the paper entitled "Security Analysis and Improvements of Session Key Establishment for Clustered Sensor Networks" J. Kim et al. propose a session key establishment scheme for clustered sensor networks that is based on elliptic curve Diffie-Hellman (ECDH) key exchange and hash chain. The proposed scheme eliminates vulnerabilities of existing schemes for WSN and has improved security.

The paper entitled "Adaptive Cross-Layer Multipath Routing Protocol for Mobile Ad Hoc Networks" by Z. Iqbal et al. proposes a cross-layer multipath routing protocol for MANET. The proposed protocol has two important features, that is, security and adaptive nature. These important features are achieved by multipath framework using cross-layer interface.

The paper entitled "System for Malicious Node Detection in IPv6-Based Wireless Sensor Networks" by K. Grgic et al. proposes a system for detecting malicious nodes in an IPv6-based WSN. The proposed system is designed for the IPv6 environment and it supports the IPv6 stack in a WSN. It is implemented into the sensor network that uses the IEEE 802.15.4 standard and the 6LoWPAN adaptation layer.

The paper entitled "Disjoint Key Establishment Protocol for Wireless Sensor and Actor Networks" by A. Ghafoor et al. presents a Disjoint Key Establishment Protocol (DKEP) that does not require transmitting keys across the nodes. In DKEP, each node is preloaded with one row and one column from a matrix.

The paper entitled "An Improved μTESLA Protocol Based on Queuing Theory and Benaloh-Leichter SSS in WSNs" by H. Huang et al. proposes a novel secret key release scheme based on the data flow, which addresses some problems of traditional key release schemes based on the fixed time interval, effectively improves the efficiency of the utilization of keys, prolongs the life cycle of hash chain, and reduces the network communication overhead and computational cost.

The paper entitled "AR-RBFS: Aware-Routing Protocol Based on Recursive Best-First Search Algorithm for Wireless Sensor Networks" by F. Kiani proposes the design of an AR-RBFS based routing protocol in two different scenarios on WSN. It is used to evaluate the power consumption and packet delivery rate of wireless sensor nodes. The algorithm computes an optimized path to route the packets from the sink to the destination node.

In the paper entitled "A Novel Nonlinear Multitarget k-Degree Coverage Preservation Protocol in Wireless Sensor Networks" by Z. Sun et al., due to the existence of a large number of redundant data in the process of covering multiple targets, the effective coverage of monitored region decreases, causing the network to consume more energy. To solve this problem, this paper proposes a multitarget k-degree coverage preservation protocol.

The paper entitled "Low Complexity Signed Response Based Sybil Attack Detection Mechanism in Wireless Sensor Networks" by M. S. and N. M. Khan proposes a low complexity sybil attack detection scheme that is based on signed response (SRES) authentication mechanism developed for Global System for Mobile (GSM) communications. A probabilistic model is presented which analyzes the proposed authentication mechanism for its probability of sybil attack.

In the paper entitled "Routing Algorithm with Uneven Clustering for Energy Heterogeneous Wireless Sensor Networks" by Y. Zhang et al. in order to solve the problem of "hotspots" in sensor networks, a kind of routing algorithm named EDEUC based on energies and distances was proposed by using the idea of uneven clustering. This method adopts double selection mechanism for cluster-heads and optimizes the competition radius of cluster-heads.

The paper entitled "A Passenger Flow Risk Forecasting Algorithm for High-Speed Railway Transport Hub Based on Surveillance Sensor Networks" by Z. Xie and Y. Qin considered the passenger flow risk forecasting problem in high-speed railway transport hub. Based on the surveillance sensor networks, a passenger flow risk forecasting algorithm was developed based on spatial correlation.

The paper entitled "R-bUCRP: A Novel Reputation-Based Uneven Clustering Routing Protocol for Cognitive Wireless Sensor Networks" by M. Zhang et al. proposes a reputation-based uneven clustering routing protocol (R-bUCRP) considering both energy saving and reputation assessment.

In the paper entitled "WDARS: A Weighted Data Aggregation Routing Strategy with Minimum Link Cost in Event-Driven WSNs" by O. A. Mahdi et al., a comprehensive weight for tradeoff between different objectives has been employed, the so-called weighted data aggregation routing strategy (WDARS) which aims to maximize the overlap routes for efficient data aggregation and link cost issues in cluster-based WSNs simultaneously.

The paper entitled "Supporting Business Privacy Protection in Wireless Sensor Networks" by N. Feng et al. proposes a business privacy-protection system (BPS) that is modeled as a hierarchical profile in order to filter sensitive information with respect to enterprise-specified privacy requirements. The BPS is aimed at solving a tradeoff between metrics that are defined to estimate the utility of information and the business privacy risk.

The aim of the paper entitled "WSN-DS: A Dataset for Intrusion Detection Systems in Wireless Sensor Networks" by I. Almomani et al. is to design an intelligent intrusion detection and prevention mechanism that could work efficiently to limit DoS attacks with reasonable cost in terms of processing and energy. To achieve this aim, a specialized dataset for WSN was constructed to classify four types of DoS attacks.

In the paper entitled "A Lightweight Authentication and Key Management Scheme for Wireless Sensor Networks" by D. Qin et al., a lightweight authentication and key management protocol AKMS have been proposed for wireless sensor networks. It uses the symmetric cryptographic primitives with keyed-hash functions (HMAC) and bidirectional encryption algorithm to provide message confidentiality and authenticity for WSN and reduces the encryption overhead to the minimum as well with just a few bytes to be performed for once per authentication attempt.

The paper entitled "Privacy Models in Wireless Sensor Networks: A Survey" by J. M. de Fuentes et al. proposes a set of guidelines to build comprehensive privacy models so as to foster their comparability and suitability analysis for different scenarios.

The paper entitled "Identity Recognition Using Biological Electroencephalogram Sensors" by W. Liang et al. proposes several brain wave-based identity recognition techniques for further studies.

The paper entitled "An Intelligent and Secure Health Monitoring Scheme Using IoT Sensor Based on Cloud Computing" by J.-X. Hu et al. proposes a scheme with IoT sensor based on cloud computing to make the elder safely and conveniently monitored.

Acknowledgments

In particular, we would like to acknowledge the program committee members of Ninth International Symposium on Information Processing (ISIP 2016). This issue contains revised and expanded versions of selected quality papers presented at the Ninth International Symposium on Information Processing (ISIP 2016). ISIP 2016 took place on August 20-21, 2016, in Changsha, China, and was cosponsored by Jishou University, 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. 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. 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