Modern information and communication technologies have created unprecedented opportunities in wireless communication, which has enabled the large-scale deployment and applications of wireless sensor networks (WSNs). The widespread proliferation of WSNs in several important and critical areas, such as military, critical infrastructure monitoring, healthcare, environment monitoring, and manufacturing, has also opened the doors to vulnerabilities and security pitfalls. Therefore, security and privacy are of paramount concern for many sensor network applications and for the ultimate growth of WSNs. Preserving security and privacy in WSNs is quite a big obstacle due to the open nature of wireless communication and limited competencies of sensor nodes.

In this special issue, we aim at bringing forward the latest development in the design, implementation, and evaluation in the areas of trust, security, and privacy of WSNs. The accepted papers of this special issue present novel theories, frameworks, and solutions to the challenging problems of trust, security, and privacy. This special issue contains a diverse collection of 11 high-quality papers contributed by academicians and researchers from diversified background and locations.

The paper by P. Castillejo et al. presents SensoTrust, a novel security model for WSN based on the definition of trustworthy domains, which is adaptable to a wide range of applications and scenarios where services are published as a way to distribute the acquired data.

The paper by C. Cheng et al. proposes an access control method based on elliptic curve cryptography and the chameleon hash function. This method addresses the security problems in existing research. It also has additional advantages since it does not require time synchronization between communication nodes nor does it require node verification tables. The results of the study demonstrate that their scheme has outstanding performance and fulfills the main requirements for secure communication in WSNs.

The paper by Y. Weiwei et al. studies opportunistic decode-and-forward relaying transmission in cooperative cluster-based WSN. The system performance in terms of the secrecy outage probability and the probability of nonzero secrecy capacity is analyzed and the exact closed-form expressions are derived over Rayleigh fading channels. They also performed analysis to verify the theoretical results and depict that node cooperation has a great potential to enhance physical layer security against eavesdropping.

The paper by Z. Zhenjing et al. proposes a solution to address the selfish and security issues (selfish nodes and malicious nodes) in social DTNs. Based on nodes’ social characteristics, a dynamic trust model is proposed to prevent bad-mouthing and ballot stuffing attacks and the Shannon entropy function is introduced to avoid blackhole and greyhole attacks. The simulation results show that their proposed scheme can significantly improve the performance of social DTNs including delivery ratio and average end-to-end delay.
The paper by A. Esfahani et al. presents a new homomorphic MAC-based scheme, called Dual-Homomorphic MAC (Dual-HMAC), for network coding-enabled wireless sensor networks. The proposed scheme makes use of two types of tags (i.e., MACs and D-MACs) to provide resistance against data pollution attacks and partially tag pollution attacks. Their scheme achieves low communication overhead and low computational complexity compared to other existing schemes.

The paper by H. Haiping et al. aims at providing two novel and secure two-party distance computation protocols based on a semihonest model, the first with aid of a third party and the second based on randomization technique. Both of these protocols can extend the calculated value into a real number field. The output of the distance computation and the intermediate values in the proposed protocols are also private and not accessible to a third party or any other attackers. They also proved that their scheme is secure and robust against different attacks.

The paper by L. You et al. proposes a pairwise key distribution schemes (DKH-KD) based on deployment knowledge and hash chains. The authors analyze in detail the performance of their scheme in terms of local connectivity, security, storage, and energy consumption, and it shows that their DKH-KD scheme can be realized with the local connection probability reaching 1 and the security can be significantly improved.

The paper by Z. Jun et al. investigates the joint resource management for orthogonal frequency division multiple access (OFDMA) security two-way relay networks in next-generation wireless sensor networks. A security satisfaction ratio model is introduced as the objection function to evaluate the information security of users. Meanwhile, in order to guarantee diverse information security requirements and fairness for different users, secrecy ratio and CDF are also presented in this paper.

The paper by M. A. T. AlSudiairy presents perspectives of managing mobile service security risks. The objective of this paper is to bring into light the explicit and implicit assumptions on the nature of technological change and how they could raise security issues, discuss the technology and management perspectives on the security issues, and present them through a methodology-oriented taxonomy.

The paper by H. Young Lee proposes a fuzzy-based centralized method for detecting and adaptively countering FEIAs in dense WSNs, where two fuzzy rule-based systems are used to detect an FEIA and to select the most effective countermeasure against the FEIA. A major benefit of the proposed method is that the fuzzy systems can be optimized automatically by combining a genetic algorithm and a simulation. Thus, users only need to write a model of the WSN to apply the proposed method to a WSN. The improved performance with this method is also demonstrated by simulation results.

L. Zhihong et al. contribute one of the papers of this special issue. In this paper, the authors focus on the problem of developing key agreement schemes for secure communication across wireless channels and propose a key evolution scheme to alleviate the assumption. They present a strategy for legitimate parties to send artificial noise if the eavesdropper cannot distinguish the sources of messages. They also discuss a k-resistant encryption scheme that can use different keys to encrypt and decrypt messages if there is no more than k bits difference between the encryption and decryption keys.