Annals of Telecommunications (2019) 74:373–374
https://doi.org/10.1007/s12243-019-00718-6

EDITORIAL

Security and privacy in IoT communication

Jin Li[1] · Xiaofeng Liao[2] · Nicolas Puech[3]

Published online: 29 June 2019

In recent years, with the popularity of smart devices, the Internet of things (IoT) has become a buzzword to describe the smart device objects. It has opened up entirely new ways to revolutionize our daily lives in a more automatic, efficient, and convenient way. As a core component, IoT communication is the key to IoT environment. However, due to the open nature of wireless communication in the sensor networks and the limited ability including storage, bandwidth, and energy, security and privacy issues are not well addressed. It is vulnerable to hacker attacks in IoT communication. Thus, addressing security and privacy challenges in IoT communication is of crucial importance in IoT environment.

In this special issue, we selected 13 high-quality research papers with rigorous review process. Our selection is based on the relevance to the special issue topics, paper quality, methods, and research contributions.

Access control is a vital issue to ensure trust in the IoT, which makes security and privacy an increasing concern for users.

The paper entitled "Access control in the Internet of Things: a survey of existing approaches and open research questions" provides a comprehensive survey of the existing different models, focused both on access control models (e.g., DAC, MAC, RBAC, ABAC) and on access control architectures and protocols (e.g., SAML and XACML, OAuth 2.0, ACE, UMA, LMW2M, AllJoyn). Authors also provide future directions for research on access control for the IoT.

For mobile healthcare, the paper entitled "Fine-grained multi-authority access control in IoT-enabled mHealth" by Li et al. proposes a secure and efficient multi-authority access control system for IoT-enabled mHealth (SEMAAC). In their SEMAAC scheme, there are multiple independently working attribute authorities (AAs). A new entity could be an AA without re-building the system. The AAs can help the user to check if the partial decryption ciphertext (PDC) is correctly computed. Additionally, a restricted user can delegate his/her key to someone to outsource the decryption and check the returned result, without exposing the plaintext file.

The paper entitled "Efficient and privacy-preserving traceable attribute-based encryption in blockchain" presents an efficient privacy-preserving traceable attribute-based encryption scheme. Blockchain technologies are used to guarantee both integrity and non-repudiation of data. The ciphertext can be quickly generated by using the pre-encryption technology. Moreover, attributes are hidden in anonymous access control structures by using the attribute bloom filter.

Another important issue in IoT is to ensure the security and the privacy of data.

In this respect, the efficiency of keyword search should be taken into consideration in resource-constrained IoT scenarios. The article "Secure and flexible keyword search over encrypted data with outsourced decryption in Internet of things" describes a flexible keyword search scheme able to search over encrypted data in IoT.

In the work "Certificateless searchable public key authenticated encryption with designated tester for cloud-assisted medical Internet of Things," authors present a certificateless searchable public key authenticated encryption scheme with designated tester (CL-dPAEKS), which is suitable for cloud-assisted medical Internet of things (mIoT). They prove that the proposed scheme can resist various types of attacks and that it is more secure than other schemes built on certificateless cryptography without significant loss in efficiency.

✉ Jin Li
jinli71@gmail.com

Xiaofeng Liao
xfliao@cqu.edu.cn

Nicolas Puech
redaction@annals-of-telecommunications.com

[1] School of Computer Science and Cyber Engineering, Guangzhou University, Guangzhou, China

[2] College of Computer Science, Chongqing University, Chongqing, China

[3] Institut Mines-Télécom, Paris, France

In the paper entitled "Certificateless public key encryption with conjunctive keyword search and its application to cloud-based reliable smart grid system," authors prove that their scheme is secure against adaptive chosen keyword attacks in the random oracle model under bilinear Diffie-Hellman (BDH) problem assumption.

The next two papers address an interesting common topic: data replication and restoration.

In "Recovering SQLite Data from Fragmented Flash Pages," authors present a new method to recover SQLite data records from fragmented flash pages. Instead of investigating the whole *.db file or the journal file, the suggested method focuses on the analysis of the B-tree leaf page structure, which is the basic storage unit in which one may locate and extract existing and deleted data records with the help of the structures of the page header and cells in the leaf page. Then, the method uses the SQLite master structure to translate hex data records into meaningful SQLite tables.

In the work "Optimizing the restoration performance of deduplication systems through an energy-saving data layout," authors introduce a selective deduplication algorithm (SDD) to perform data replication and restoration. A new CGDL-based disk scheduling algorithm (LDP) is also proposed that predicts location dependence to save energy by eliminating the redundant disk read/write operations.

Network traffic analysis and data streaming are fundamental areas used in IoT environment. Classification and authentication are enabling techniques for network security and management.

The paper entitled "Statistical network protocol identification with unknown pattern extraction" describes a learning scheme with unknown pattern extraction for statistical protocol identification. This scheme is designed with a more realistic setting, in which the training data only consists of labeled samples from a limited number of protocols. The goal is to identify these known patterns out of arbitrary traffic mixture of both known and unknown protocols. For data streaming, authors define and construct a new primitive, namely, dimension-increasing vector commitment (DIVC), and present the definition of constant verifiable data streaming (CVDS), which is an extension of the original verifiable data streaming (VDS) scheme presented in the article "New efficient constructions of verifiable data streaming with accountability."

There are some other security issues for IoT environment such as data collection, wireless sensor network (WSN) deployment, and anonymous authentication.

In the paper entitled "On the rewards of self-adaptive IoT honeypots," authors present a novel approach on collecting relevant data about IoT attacks. They detail a SSH/Telnet honeypot system that leverages reinforcement learning algorithms in order to interact with the attackers, and present the results obtained in view of defining optimal reward functions to be used.

A novel deployment algorithm for 3D wireless sensor networks (WSNs) based on the Voronoi diagrams is described in the paper "Three-dimensional Voronoi diagram-based self-deployment algorithm in IoT-sensor networks." This algorithm uses the characteristics of adjacency and fast partition of the Voronoi diagram to realize a fast division of the 3D monitoring area. It repeatedly builds the Voronoi diagram to maximize the coverage of the monitoring area and maximize the availability and the integrity of data.

In the study entitled "Lattice-based dynamic group signature for anonymous authentication in IoT," a new group signature scheme is proposed: it allows any user to dynamically join the group while achieving efficient revocation. Furthermore, it is shown that the new scheme can achieve the security of non-frameability. The security of non-frameability guarantees that any user's signature cannot be forged by other users in the system.

Hence, this special issue presents a large sample of current research in IoT. We believe this area will attract more and more researchers who will pay attention to the security and privacy issues in IoT communication.

Finally, the Guest Editors and the Board of the journal would like to warmly thank the authors who contributed to this special issue as well as the reviewers for their helpful remarks and suggestions.