Hindawi
Wireless Communications and Mobile Computing
Volume 2019, Article ID 2627938, 2 pages
https://doi.org/10.1155/2019/2627938

Editorial

Physical Layer Security for Internet of Things

Ning Zhang[1], **Dajiang Chen**[2], **Feng Ye**[3], **Tong-Xing Zheng**[4] and **Zhiqing Wei**[5]

[1]*Department of Computing Sciences, Texas A&M University-Corpus Christi, TX, USA*
[2]*School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu, China*
[3]*Department of Electrical and Computer Engineering, University of Dayton, Ohio, USA*
[4]*School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an, China*
[5]*School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing, China*

Correspondence should be addressed to Ning Zhang; ning.zhang@tamucc.edu

Received 2 April 2019; Accepted 2 April 2019; Published 18 April 2019

Internet of Things (IoT) enables physical objects to sense, communicate, and perform certain actions on demand, which can facilitate a multitude of applications, such as smart home, smart city, and intelligent transportation system [1, 2]. Along with the advantages of IoT is the security issue. In IoT, the security threats are even extended from the cyberworld to cyberphysical world [3, 4]. To ensure security, the typical approach is through upper-layer cryptographic algorithms/protocols. However, they heavily rely on the availability of key management system and might be comprised as the computation power of adversaries keeps increasing [5].

As a complement, information-theoretic security can be provided by exploiting the characteristics of the physical (PHY) layer, even though adversaries have infinite computational capabilities [6–9]. With recent advances in computing, artificial intelligence, signal processing, coding, and so on, PHY security can be further enhanced to protect data and authenticate legitimate users in IoT. The interest and application of PHY security in IoT are also growing [10, 11]. The purpose of this special issue is to publish original efforts describing theoretical and practical research endeavors in the domain of PHY layer security for IoT. In this special issue, there are 13 submissions in total. After peer review, 6 papers are selected for published.

Cloud computing plays an important role in IoT. The premise of securing the cloud-based IoT context is to evaluate the security and compliance of cloud service. To this end, Xiang Li et al. propose a secure and compliant continuous assessment framework (SCCAF), to facilitate cloud service customers to select an optimal cloud service provider (CSP) which satisfies their desired security requirements. Moreover, it also enables cloud service customers to evaluate the compliance of the selected CSP in the process of using cloud services.

Xiaohui Shang et al. study the secure uplink transmission scenario in Internet of Things (IoT), where one of multiple sensors communicates with the controller aided by the cooperative relay. An energy-efficient transmission scheme (EET) is proposed, which can be suitable for the resource-constrained devices and applications in IoT communication. Moreover, the secrecy outage probability (SOP) and secure energy efficiency (SEE) of different transmission strategies are derived, which contributes to the design of energy-efficient secure transmission.

In order to ensure the security of the IoT communication system, Tao Hong et al. propose a machine learning based antenna design scheme, which can achieve directional communication from the relay tag to the receiving reader by combining patch antenna with log-periodic dual-dipole antenna (LPDA). From the simulation results, it is demonstrated that he proposed antenna design can work well in physical layer security communication, where signal-to-noise ratio of the wiretap channel is reduced, communication quality of the main channel is ensured, and information leakage is prevented.

As for securing IoT applications, Tingting Yang et al. target maritime security, where unmanned surface vessels (USV) are utilized to collect information on the sea for intelligent monitoring. To enhance the security of the unmanned

video monitoring system, an improved Hill encryption algorithm is proposed. The improved Hill encryption algorithm is integrated into the process of video compression and regulates the parameters of the encryption process according to the content of the video image. Mingsheng Cao et al. focus on wireless body area networks (WBANs), which is one of the most important IoT applications. WBANs allow patients demographics to be collected by tiny wearable and implantable sensors. These data can be used to analyze and diagnose for healthcare. In order to protect the security and privacy, Mingsheng Cao et al. propose a lightweight fine-grained search over encrypted data in WBANs, considering the limited resource of WBANs devices.

Jiefan Qiu et al. study security for over-the-air reprogramming to improve the security of reprogramming by changing the physical-level communication mode. Unidirectional Visible Light Communication (VLC) is applied to the over-the-air reprogramming and commercial off-the-shelf devices such as smartphone and sensor node are used to improve applicability. Moreover, a reprogramming approach named ReVLC is proposed. The experiment results demonstrate the effectiveness of ReVLC at the cost of extra 49.1% energy overhead compared with a traditional reprogramming approach.

With this special issue, we hope that readers will be interested in physical layer security for IoT and they find this special issue is helpful to their research.

Conflicts of Interest

Editors have no conflicts of interest to the assigned manuscripts when handling them and making decisions.

Ning Zhang
Dajiang Chen
Feng Ye
Tong-Xing Zheng
Zhiqing Wei

References

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: a survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015.

[2] D. Zhang, Y. Qiao, L. She, R. Shen, J. Ren, and Y. Zhang, "Two time-scale resource management for green internet of things networks," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 545–556, 2019.

[3] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: the road ahead," *Computer Networks*, vol. 76, pp. 146–164, 2015.

[4] F. Ye and Y. Qian, "A security architecture for networked internet of things devices," in *Proceedings of the 2017 IEEE Global Communications Conference (GLOBECOM 2017)*, pp. 1–6, Singapore, 2017.

[5] D. Chen, N. Zhang, Z. Qin et al., "S2M: a lightweight acoustic fingerprints-based wireless device authentication protocol," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 88–100, 2017.

[6] A. Mukherjee, S. A. A. Fakoorian, J. Huang, and A. L. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: a survey," *IEEE Communications Surveys & Tutorials*, vol. 16, no. 3, pp. 1550–1573, 2014.

[7] H.-M. Wang, T.-X. Zheng, J. Yuan, D. Towsley, and M. H. Lee, "Physical layer security in heterogeneous cellular networks," *IEEE Transactions on Communications*, vol. 64, no. 3, pp. 1204–1219, 2016.

[8] H. V. Poor, "Information and inference in the wireless physical layer," *IEEE Wireless Communications Magazine*, vol. 19, no. 1, pp. 40–47, 2012.

[9] N. Zhang, N. Cheng, N. Lu, X. Zhang, J. W. Mark, and X. Shen, "Partner selection and incentive mechanism for physical layer security," *IEEE Transactions on Wireless Communications*, vol. 14, no. 8, pp. 4265–4276, 2015.

[10] L. Sun and Q. Du, "A Review of Physical Layer Security Techniques for Internet of Things: Challenges and Solutions," *Entropy*, vol. 20, no. 10, p. 730, 2018.

[11] A. Mukherjee, "Physical-layer security in the internet of things: sensing and communication confidentiality under resource constraints," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1747–1761, 2015.