Annals of Telecommunications (2021) 76:117–118
https://doi.org/10.1007/s12243-021-00842-2

EDITORIAL

Security and trust in ubiquitous systems

Samia Bouzefrane[1] · Jenny Gabriela Torres Olmedo[2] · Gongxuan Zhang[3] · Nicolas Puech[4]

Published online: 7 April 2021

5G will enable massive Internet of Things (IoT) applications and domains such as connected cars, smart cities, smart homes, wearables, health care devices, smart factories, smart farming, and other IoT devices. One of the IoT-applications requirements that 5G must meet is the security/cybersecurity. Security must be delivered from design to protect the networks, the applications and the services. By extending the vision to IoT devices that are resource-constrained, new types of security threats are introduced, hence increasing the attack surface. In addition to the traditional security properties that are required to secure networks, platforms, services and users, trust and reputation are the other concerns in ubiquitous environments either in business or in mission-critical applications. While trust can rely on hardware trusted platforms and secure elements, reputation is built upon recommendation systems which may use artificial-intelligence mechanisms. Ubiquitous systems may refer to any pervasive system such as IoT, cyber physical systems, edge computing, mobile computing, cloud computing, and distributed computer systems. Designing secure and data-protected solutions for these systems requires to meet key constraints such as scalability, maintainability, and performance.

This special edition is dedicated to security and trust mechanisms that are investigated to help provide reliable services and more trustable infrastructures in any connecting system that relies on new technologies. A wide range of topics are covered such as trust and reputation of messaging systems, blockchain for appropriate technical infrastructure, outlier characterization in IoT context, authentication, SIM and EMV protocols, and mobile payment.

✉ Samia Bouzefrane
samia.bouzefrane@cnam.fr

[1] Conservatoire National Des Arts Et Métiers, Paris, France

[2] Escuela Politécnica Nacional, Quito, Ecuador

[3] Nanjing University of Science and Technology (NJUST), Nanjing, China

[4] Institut Mines Telecom, Paris, France

Every paper has been evaluated by at least two experts and, after a thorough selection process, nine papers have been accepted. We provide a summary of each paper in this special issue.

The paper by David Jelenc entitled "Towards unified trust and reputation messaging in ubiquitous systems" deals with the design of a protocol and the development of a framework that allow the exchange of trust and reputation information (such as ratings) enhancing the trust and reputation of the applications.

In a paper entitled "A Decision Tree for Building IT Applications—What to choose: Blockchain or Classical Systems?", Nour El Madhoun and her colleagues discuss the use of blockchain in the appropriate technical infrastructure for a given IT application by relying on a decision tree.

The paper "A modified LOF based approach for outlier characterization in IoT" by Lynda Boukela and her colleagues proposes to modify the Local Outlier Factor (LOF) algorithm to characterize the outliers in Internet of Things (IoT) with the objective of enhancing the IoT security and reliability.

José David Vega Sánchez and his colleagues propose a "Survey on Physical Layer Security for 5G Wireless Netwoks", which consists in a review of the physical layer security over several enabling 5G technologies.

The paper entitled "Novel user authentication method based on body composition analysis" by Paweł Łąka and his colleagues investigates authentication based on the analysis of body composition. A trusted system, that relies on the biometric authentication, has been designed, implemented, and evaluated.

In the article entitled "Transparency of SIM Profiles for the Consumer Remote SIM Provisioning Protocol", Abu Shohel Ahmed and his colleagues present a SIM Profile Transparency Protocol (SPTP) to detect malicious provisioning of SIM profiles. They evaluated security guarantees using a formal model as well as a prototype.

To enhance the security of mobile transactions, Nour El Madhoun and her colleagues address two dangerous vulnerabilities known in the EMV protocol. They prove the

accuracy of the solution by using the Scyther security verification tool. Their paper is entitled "Towards More Secure EMV Purchase Transactions—A New Security Protocol Formally Analyzed by the Scyther Tool".

The following article entitled "Mobile Money Traceability and Federation Using Blockchain Services" by Edem Kodjo Agbezoutsi and his colleagues is related to mobile payment. The authors present a mobile-money solution based on blockchain technology that aims at increasing security and trust in the federated platforms.

In the paper entitled "Understanding Cyberbullying as an Information Security Attack—Life Cycle Modeling", Patricio Zambrano and his colleagues deal with the problem of cyberbullying. They propose a cyberbullying life cycle model and conceptualize the different stages of the attack considering criteria associated with computer attacks.

The last paper of this Special Issue is by Jorge Merchan-Lima and his colleagues. "Information Security Management Frameworks and Strategies in Higher Education Institutions: a Systematic Review" describes a process to develop information security management for high-education institutions, in addition to recommendations that should be considered for the framework implementation in an era of ever-evolving security threats.

Acknowledgements The Guest Editors would like to express their deep appreciation to the Editor-in-Chief, Prof. Guy Pujolle, for giving them the opportunity to publish this special issue. The Guest Editors also thank the Managing Editor, Laurence Monéger, as well as the journal editorial staff for their continuous support during the publishing process. Lastly, the Guest Editors would like to thank all the authors for submitting quality articles. We also would like to thank the reviewers for helping in the selection of papers and improving the accepted papers.