applied sciences

MDPI

Editorial

Trustworthiness in Mobile Cyber-Physical Systems

Hyo-Joong Suh [1], Junggab Son [2] and Kyungtae Kang [3,*]

[1] School of Computer Science and Information Engineering, The Catholic University of Korea, Bucheon 14662, Korea; hjsuh@catholic.ac.kr

[2] Department of Computer Science, Kennesaw State University, Marietta, GA 30060, USA; json@kennesaw.edu

[3] Department of Applied Artificial Intelligence, Hanyang University, Ansan 15588, Korea

[*] Correspondence: ktkang@hanyang.ac.kr; Tel.: +82-31-400-5235

1. Introduction

As they continue to become faster and cheaper, devices with enhanced computing and communication capabilities are increasingly incorporated into diverse objects and structures in the physical environment. Harnessing these capabilities will provide the basis for applications offering enormous societal impact and economic benefit, linking the cyber world of computing and communications with the physical world. Such applications are called cyber-physical systems (CPSs). It is evident that as direct interactions between real-world entities (including human activities) and cyber systems become more commonplace, the trustworthiness of such systems will become an increasingly important issue. Here, we use the term system trustworthiness in a broad sense to describe systems that demonstrate reliable functionality and are worthy of user confidence, such that they guarantee continuous service in response to internal errors or external attacks [1].

While CPSs traditionally involve static equipment and stable networks, the development of increasingly pervasive mobile devices has generated considerable attention in mobile CPSs (MCPSs). By exploiting the advantages of CPSs through mobile devices, such as the iPhone and Android phones, with their increasing processing power, range of sensors, and pervasive cellular connections, MCPSs provide expanded applicability, including access to networks comprising multiple mobile devices, such as vehicle networks. Owing to the instability of mobile networks and the variable computing power of individual mobile devices, many studies have been performed to address various aspects supporting the efficient cooperation and performance of MCPSs. In particular, the timeliness of data transferal is essential because delays and failures due to bottlenecks stemming from variable network environments can adversely affect the entire system.

The objective of this Special Issue is to contribute to the advancement of research on a wide variety of topics involved in the development of modern and future trustworthy MCPSs, including design, modeling, verification and validation, dependability, resilience, security, safety, and run-time resource optimization. It is imperative to address the issues that are critical to the mobility of MCPSs, report significant advances in the underlying science, and discuss the challenges facing the development and implementation of specific MCPS applications, including those associated with aerospace, autonomous automotive systems, automatic pilot avionics, smart grids, and distributed robotics. Such applications will empower the true vision of MCPSs, driving the evolution of human interactions with the physical world. Moreover, technologies utilizing CPSs will emerge as key drivers in the development of a future autonomous and smart-connected world.

As a side note, we focus on methods for integrating MCPSs with artificial intelligence (AI) without compromising the trustworthiness of the system. AI-enabled CPSs combine computational capabilities with the ability to control and sense physical space. For example, the behavior of autonomous CPSs, such as self-driving cars and autonomous drones in open environments is often determined by AI and machine learning algorithms. However, the use of data-driven deep learning techniques for perception and control in autonomous

check for updates

Citation: Suh, H.-J.; Son, J.; Kang, K. Trustworthiness in Mobile Cyber-Physical Systems. *Appl. Sci.* **2021**, *11*, 1676. https://doi.org/10.3390/app11041676

Received: 8 February 2021
Accepted: 9 February 2021
Published: 13 February 2021

CPSs has raised concerns regarding the safety and robustness of autonomous systems. When operating in a physical environment, the unexpected action of AI-enabled CPSs can inflict critical damage on the surrounding environment, including the potential endangerment of humans. Therefore, AI-enabled MCPSs should satisfy stringent regulations regarding their trustworthiness. Although sophisticated testing plays an important role in ensuring the safety and robustness of such systems, the complexity of modern autonomous CPSs means that evaluating trustworthiness via testing alone is insufficient. Formal verification reduces the burden on the testing process by ruling out large classes of errant behaviors at the design stage. Nevertheless, the introduction of a standard methodology for developing formal methods for autonomous AI-enabled CPSs is essential.

2. Review of Issue Contents

This Special Issue presents nine original papers covering the latest advances and technologies involved in the design of reliable, resilient, secure, and intelligent MCPSs. Moreover, each paper contributes research that offers insights regarding trustworthiness in MCPSs.

Artificial intelligence models, especially deep neural networks such as convolutional neural nets (CNNs), tend to have many learning parameters, thus making their integration into small embedded CPSs, such as mobile phones, challenging. In response to this issue, Lee et al. in [2] suggested a new model compression framework based on sparse coding and knowledge distillation with adversarial training, thereby producing compact CNN architectures that maintain robustness against adversarial perturbed inputs. Furthermore, the authors provide training algorithms based on the alternating direction method of multipliers (ADMM), which is more memory-efficient than existing CNN pruning methods and, therefore, more suitable for AI-enabled MCPSs.

In [3], Kim et al. propose two novel data quality measures suitable for large-scale high-dimensional data. As low-quality data can degrade prediction accuracy and inference bias, measuring the data quality is an important first step in successful AI applications. In MCPS, the use of AI often requires regular updates, while detecting inference bias when operating at the AI runtime is difficult; therefore, a data quality check is essential. This study also proposes efficient algorithms based on random projections and bootstrapping, enabling the suggested measures to be computed for large-scale and high-dimensional data, thus representing a departure from existing data quality measures.

Automotive systems are typical examples of CPSs in which embedded software is the main element controlling the mechanical components of the vehicle. Internet-connected software components can be victims of security attacks at any time, and CAN (Controller Area Networks), an in-vehicle network system connecting individual electronic control units (ECUs), serves as a breach point to break vehicle safety.

MAuth-CAN [4] is a new CAN authentication technique that protects ECUs from attacking messages based on a centralized node called an authenticator. It is secure against masquerade attacks by a compromised node and protects the authenticator node from bus-off attacks that can temporarily force an ECU to leave CAN. However, the use of a central node causes an additional authentication delay. Thus, in accordance with regulations such as ISO 26262, the efficacy of the MAuth-CAN must be formally verified before it can be used for commercial vehicles.

Cho et al. [5] present formal proof that MAuth-CAN is consistently resistant against message flooding and Bus-Off attacks and provide formal CAN models at various levels, which can be used to analyze CAN applications. Via model checking, the complicated behavior of CAN in the media access control level of the data link layer connecting to MAauth-CAN was checked exhaustively to prove its resilience and sustainability under such attacks. These results can be used to obtain safety certificates from regulatory authorities, while the methodology and the CAN models can be used to secure safety certificates regarding CAN applications.

Public key encryption with keyword search (PEKS) functionality enables users to search for encrypted data that has been outsourced to an untrusted server. Unfortunately, updates to the outsourced data may cause information leakage by exploiting the queries previously submitted in PEKS. Yoon et al. [6] address this by proposing a novel forward private PEKS scheme based on software guard extension (SGX), a trusted execution environment provided by Intel. By utilizing SGX, the proposed scheme presents substantial performance improvements compared with prior work. Owing to the readiness with which a trusted platform such as SGX can be integrated with many current CPSs, this research also has implications for security enhancements in CPS environments.

Event-based systems (EBSs) are prevalent in MCPS applications owing to their communication model, which uses implicit invocation and concurrency between components. However, the non-determinism of EBSs during event processing can introduce inherent security vulnerabilities into the system. Many types of attack can incapacitate and/or damage a target EBS by exploiting this event-based communication model. To minimize the security risks to EBSs, the security flaws of such systems, the relationships between these flaws, and feasible techniques for dealing with each flaw must be determined. However, existing security flaw taxonomies do not appropriately reflect the inherent security issues of EBSs. Therefore, Lee et al. [7] introduced a new taxonomy that defines and classifies the inherent security flaws of EBSs, which can serve as a basis for resolving its specific security problems. Moreover, the authors correlated their taxonomy with security attacks designed to target specific flaws and identified existing solutions for the prevention of such attacks.

In [8], Ali et al. describe an energy minimization technique for mixed-criticality real-time scheduling on a single-core system. The main contribution of the proposed technique is that it allows the processor frequency to be controlled dynamically depending on the system criticality mode. Through a series of simulations, they demonstrated and analyzed the effects caused by both low-and high-criticality modes in power-aware mixed-criticality systems. As safety and power awareness are both issues for MCPSs, this study offers valuable insights for power-aware safety-critical CPSs.

Safety and efficiency provide the focus in [9], in which Kwon et al. propose a system that dynamically controls the all-red signal length based on the driving characteristics of vehicles identified as red-light runners (RLRs) to improve the overall safety and efficiency of intersections in road networks. The proposed system uses a multi-channel deep convolutional neural network (MC-DCNN) to enable the online detection and classification of RLRs, which can be defined using clustering results acquired via dynamic time wrapping (DTW) and hierarchical clustering analysis (HCA). For dynamic all-red signal control, the proposed system uses a multi-level regression model to estimate the necessary all-red signal extension time more accurately, thereby improving the overall safety for intersection traffic as well as efficiency of the traffic flow.

By contrast, the study conducted by Oh et al. [10] concerns real-time data transmission to mobile equipment used by groups of workers, termed a mobile sink group (MSG), for which rapid and reliable data are vital to ensure the efficient operation of groups working on collaborative projects, which often involve multiple pieces of equipment where miscommunication could result in an industrial accident. The authors proposed a real-time data delivery mechanism based on a virtual grid structure to support MSGs. The main idea is to determine the farthest distance and calculate the minimum real-time data transmission speed required.

First, the proposed scheme models the MSG as a single center point and radius, and defines the end-to-end distance based on the member sink located furthest from the source node. Thus, the source node can calculate the transmission speed, which is maintained during the data transmission. The data transmission process is divided into two main phases: the main forwarding phase, which passes through the center of the mobile sinks from the source node, and the branch forwarding phase at the branch point, which receives data via the main forwarding phase. In addition, even if some mobile sinks deviate from the initial radius owing to environmental factors associated with MCPSs, the connection of the sinks is ensured through the inner/outer agent concept. Thus, the proposed scheme can deliver data to all member sinks in a timely manner and is superior to existing schemes in terms of real-time communication for MSGs.

Finally, in [11], Choi et al. address an important system optimization problem faced by automotive control systems. More specifically, a control application based on AUTOSAR (AUTomotive Open System Architecture) [12] is assumed, whereby fine granular schedule entities (i.e., runnables) are used to compose a control application. For this purpose, the authors propose a Lagrange multiplier-based runnable period optimization method that maximizes the level of system control, which is useful for the development of future MCPSs, where design optimization is a fundamental consideration.

3. Conclusions

This Special Issue presents new and innovative research addressing some of the many scientific challenges associated with improving the trustworthiness of MCPSs. We emphasize the need for a better understanding of the security and reliability of MCPS as well as the impacts of AI, and demonstrate procedures for solving the adverse effects caused by these impacts. As such, the studies contained within this volume provide a valuable basis for the protection and promotion of resilient MCPSs.

Author Contributions: Conceptualization, H.-J.S., J.S. and K.K.; methodology, H.-J.S. and K.K.; validation, J.S.; investigation, K.K.; writing—original draft preparation, K.K.; writing—review and editing, H.-J.S.; supervision, J.S. and K.K.; funding acquisition, H.-J.S. and K.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was supported by the National Research Foundation of Korea (2016R1D 1A1B01006716) and the Catholic University of Korea, Research Fund, 2020. This research was also supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (Ministry of Science and ICT) (No.2020-0-01343, Artificial Intelligence Convergence Research Center (Hanyang University ERICA)).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Acknowledgments: This issue would not have been possible without the help of a variety of talented authors, professional reviewers, and the dedicated editorial team of Applied Sciences. First, we express our gratitude to the authors for their excellent contributions to this Special Issue on trustworthiness in mobile cyber-physical systems. We are also grateful to all the reviewers for their time and effort in examining these papers, and for their valuable comments and constructive suggestions. Finally, we appreciate the advice and support of the editorial team of Applied Sciences for their help in the publication process. We hope that this Special Issue will serve as a valuable reference for academicians, scientists, engineers, and practitioners working toward the design and implementation of trustworthy mobile cyber-physical systems.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Romanovsky, A.; Ishikawa, F. *Trustworthy Cyber-Physical Systems*, 1st ed.; Chapman & Hall/CRC: London, UK, 2017; pp. 2–22.
2. Lee, J.; Lee, S. Robust CNN Compression Framework for Security-Sensitive Embedded Systems. *Appl. Sci.* **2021**, *11*, 1093. [CrossRef]
3. Kim, J.H.; Jo, H.J.; Lee, I. Model Checking Resiliency and Sustainability of In-Vehicle Network for Real-Time Authenticity. *Appl. Sci.* **2021**, *11*, 1068. [CrossRef]
4. Jo, H.J.; Kim, J.H.; Choi, H.-Y.; Choi, W.C.; Lee, D.H.; Lee, I. MAuth-CAN: Masquerade-Attack-Proof Authentication for In-Vehicle Networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 2204–2218. [CrossRef]
5. Yoon, H.; Moon, S.; Kim, Y.; Hahn, C.; Lee, W.; Hur, J. SPEKS: Forward Private SGX-Based Public Key Encryption with Keyword Search. *Appl. Sci.* **2021**, *11*, 1068. [CrossRef]
6. Cho, H.; Lee, S. Data Quality Measures and Efficient Evaluation Algorithms for Large-Scale High-Dimensional Data. *Appl. Sci.* **2021**, *11*, 472. [CrossRef]
7. Yoon, H.; Moon, S.; Kim, Y.; Hahn, C.; Lee, W.; Hur, J. SPEKS: Forward Private SGX-Based Public Key Encryption with Keyword Search. *Appl. Sci.* **2020**, *10*, 7842. [CrossRef]

8. Lee, K.L.; Kim, D.A. Taxonomy for Security Flaws in Event-Based Systems. *Appl. Sci.* **2020**, *10*, 7338. [CrossRef]
9. Ali, I.; Jo, Y.-I.; Lee, S.; Lee, W.L.; Kim, K.H. Reducing Dynamic Power Consumption in Mixed-Critical Real-Time Systems. *Appl. Sci.* **2020**, *10*, 7256. [CrossRef]
10. Kwon, S.K.; Jung, H.; Kim, K.-D. Dynamic All-Red Signal Control Based on Deep Neural Network Considering Red Light Runner Characteristics. *Appl. Sci.* **2020**, *10*, 6050. [CrossRef]
11. Oh, S.; Choi, Y.; Kim, S.; Kim, C.; Jung, K.; Kim, S.-H. A Real-Time Data Delivery for Mobile Sinks Group on Mobile Cyber-Physical Systems. *Appl. Sci.* **2021**, *10*, 5950. [CrossRef]
12. Choi, D.; Kim, T.-W.; Kim, J.-K. AUTOSAR Runnable Periods Optimization for DAG-Based Complex Automobile Applications. *Appl. Sci.* **2021**, *10*, 5829. [CrossRef]