CIT. Journal of Computing and Information Technology, Vol. 29, No. 2, June 2021, i–ii
doi: 10.20532/cit.2021.1005424

Editorial

The June 2021 issue (Vol. 29, No. 2) of *CIT. Journal of Computing and Information Technology* brings four papers from the areas of control systems, network security and privacy, and natural language processing.

The development of networking technology enabled the diversification of controlled objects as well as the growth of control systems leading to the emergence and rapid development of closed-loop feedback control systems as a sort of overlay networks, known as Network Control Systems (NCS), themselves finding application especially in complex industrial control and in the military sector. Within such a framework, the event-triggered mechanism for exchanging data is increasingly being chosen over the traditional time-triggered one, because of its inherent advantages related to eliminating the impact of time delay and packet dropouts, while also reducing the amount of data transmission in the system and saving network resources. Since the network states are randomly changed, NCSs can be accurately described by Markov chains, specifically Markov jumping systems. In their paper, titled *Event-triggered Observer-based Robust H∞ Fault-tolerant Control for Markov Jumping NCSs*, Xingjian Fu and Xinyao Geng describe the design of an NCS with time delay, communication constraints, and other network faults, as a parameter uncertainty random time-delay Markov jumping system. They designed both the respective observer and H∞ fault-tolerant controller, which ensures stability in the event of NCS failures. The authors provided sufficient condition for the existence of the fault-tolerant controller under the event-triggered mechanism and verified the effectiveness and feasibility of the proposed method by simulation.

The second paper of the issue, titled *Signal Processing-based Model for Primary User Emulation Attacks Detection in Cognitive Radio Networks*, addresses security problems in cognitive radio networks (CRNs). Namely, technology developments in recent years spawned an increased use of wireless-based transmission, which has been followed by a growth of malicious activities trying to disrupt its use. The limited transmission spectrum is usually managed in such a way as to allow unlicensed users, known as secondary users (SUs), to opportunistically occupy the spectrum left free by licensed, so-called primary users (PUs). On the other hand, the basic operational rules of CRNs assume SUs sensing the surrounding environment in order to access and/or leave the spectrum. This mechanism is however exploited in the *Primary User Emulation Attack* (PUEA), in which the malicious attacker emulates the behavior of PUs effectively blocking SUs' attempts to access/use some otherwise available spectrum, the result of which are dropped calls and increased delay times, effectively leading to QoS degradation and bandwidth waste. Thus, the authors – Diafale Lafia, Mistura Laide Sanni, Rasheed Ayodeji Adetona, Bodunde Odunola Akinyemi and Ganiyu Adesola Aderounmu – introduce a novel mechanism to detect PUE attackers, which is based on position detection of the transmitter and analysis of the signal detected, and can be used even in sparse networks and mobile users CRNs. The results of the MATLAB simulation of the proposed model, as well as of the OMNET++ 4.6 one of the CRN, demonstrate the model's effectiveness.

In order to support the mobility of users, access networks are nowadays commonly implemented using wireless technology. Such a medium has an open nature, the respective wireless links being more prone to physical layer attacks compared to their wired counterparts. Because of this, implementing security in the physical layer presents an outstanding problem, especially when the devices to be wirelessly networked do not possess sufficient resources to support the application of conventional cryptographic approaches providing security, which is especially true for Inter-

net-of-Things (IoT) sensors/actuators. In fact, these simple devices must allocate most of the available energy and computation to the execution of their core application functionality, with little to be left over for supporting security. Therefore, Hong Zhao and Paul Ratazzi propose a novel physical layer security system that includes secure transmitting of messages at the waveform level, as well as hardware-assisted device authentication. In their paper, titled *Providing Physical Layer Security for IoTs in the Last Mile*, they address the issue by using a number of mechanisms, here including hiding data in chaotic carrier signals, using the initial conditions and spreading factor as keys, and *Physically Unclonable Function*s (PUF) based authentication, which rely on the intrinsic uniqueness of the physical microstructure of semiconductor devices. The results of performed simulations show high resistance to interference and more immunity against multipath effects, while security performance is analyzed in terms of key space and statistical property of the chaos signal. The authors note that the proposed approach can be implemented as a single subsystem providing all the basic processing, thus making it a promising way of providing physical layer security for IoTs in the last mile.

The paper *Natural Language Processing Using Neighbor Entropy-based Segmentation* by Jianfeng Qiao, Xingzhi Yan and Shuran Lv addresses the processing of a characteristic kind of semi-structured text found in accident prevention procedures in workplaces denoted as hazard text. Such texts are generated by workers within reports submitted before hazards occur, enabling hazard rectification and/or mitigation of similar events. Hazard report records consist of a number of predefined fields of free text, contain some logging data (checking time and other parameters) along with professional words describing the threats, the free text within the individual fields being further subdivided into shorter units. Since present regulations in China emphasize hazard identification as the most critical task for safety management, the amount of hazard texts recorded within enterprises is understandably huge, thus leading to the automatization of their analysis through word segmentation. As Asian language texts do not easily provide themselves for segmentation, since these texts consist of character strings without obvious boundaries between words, the authors propose a novel segmentation model specifically developed for Chinese Word Segmentation (CWS), which is based on a statistical approach using entropies as a means to assess the loss, along with the benefit, of segmentation choices, wherefrom the name *Neighbor Entropy-based Segmentation* (NES). Applying this segmentation model to the Beijing Municipal Administration of Work Safety (Q4/2018) text corpus, the authors report higher performances regarding precision, recall, and F-measure than using existing tools and popular statistical models.

Vlado Glavinić
Editor-in-Chief