Annals of Telecommunications (2022) 77:455–456
https://doi.org/10.1007/s12243-022-00918-7

EDITORIAL

Enabling technologies for running IoT applications on the cloud

Diogo Menezes Ferrazani Mattos[1] · Dianne Scherly Varela de Medeiros[1] · Daniel Mosse[2]

Published online: 9 July 2022

The Internet of Things generates myriad new applications supported by vehicles connected to roadside units, home appliances connected to the cloud, and many resource-constrained devices. Despite IoT devices' lack of computational power, they are numerous and spread over Internet access networks. Furthermore, IoT devices are a main target of current cyber-attacks and are susceptible to being easily compromised. Therefore, security enforcement and network optimization are key techniques for enabling IoT applications. Moreover, cloud, fog, and edge computing are the computational environments that make it feasible to run complex algorithms alongside resource-constrained IoT devices. This special edition is dedicated to these new research areas that shape the world to have more secure and optimized computer networks while enabling new distributed, mobile, and trustworthy IoT applications. The articles cover a wide range of topics, such as cyber-physical system security, vehicular ad hoc network optimizations, consensus mechanisms for the blockchain, distributed intrusion detection systems, and analysis of current network-security datasets.

After a thorough reviewing process, in which experts have evaluated every paper, seven papers have been accepted for publication. Reviewers' comments were helpful and productive to select the most meaningful contributions as well as to improve the content, quality, and presentation of the accepted papers. Hereafter, we provide a summary of each article published in this special issue.

The first one from Silvio E. Quincozes and his colleagues is entitled "An extended assessment of metaheuristics-based feature selection for intrusion detection in CPS perception layer." Quincozes et al. address the intrusion detection challenges in cyber-physical systems (CPS). They propose a feature selection scheme for a machine learning–based intrusion detection system (IDS). They deploy the F1-score metric as a criterium for a randomized adaptive search metaheuristic to improve the performance of traffic classifiers. The results show that the proposed metaheuristic succeeded in accurately detecting denial of service attack classes and variations of traffic injection attacks in networks underlying cyber-physical systems.

The second paper is from Kirti A. Yadav and P. Vijayakumar, who propose the "LPPSA: an efficient lightweight privacy-preserving signature-based authentication protocol for a vehicular ad-hoc network." The authors claim that malicious vehicles in vehicular ad hoc networks (VANET) lead to severe security and safety issues, as the malicious vehicle may prevent legitimate information exchange. Besides, the authors argue that privacy preservation of vehicle information is mandatory in VANETs and requires securely transferring and maintaining the integrity of all messages. The authors propose a lightweight privacy–preserving signature-based authentication (LPPSA) for VANETs. The proposal deploys elliptic-curve Diffie-Hellman (ECDH) as the key exchange algorithm to generate shared secret keys and shares the trust authority (TA) processing load with the roadside units (RSU). The results show that the proposed scheme reduces the communication costs and the computational complexity in vehicle authentication.

The following paper from Melody Jamalzadeh and her colleagues is entitled "EC-MOPSO: an edge computing-assisted hybrid cluster and MOPSO-based routing protocol for the Internet of Vehicles." In this paper, the authors claim that RSU in vehicular ad hoc network (VANET) architectures play the role of an edge computing device and assist in the routing process. Moreover, they state that bioinspired metaheuristic optimization algorithms are feasible solutions to routing problems in VANETS. Furthermore, clustering algorithms are also a possible solution for reducing the routing complexity in these networks. Therefore, the authors propose MOPSO, an edge computing-assisted cluster-based routing algorithm utilizing multi-objective particle swarm optimization for Internet of Vehicle (IoV) applications. The RSU is responsible for the computation of the optimization procedure, and the particles represent a unique path for

✉ Diogo Menezes Ferrazani Mattos
diogo_mattos@id.uff.br

[1] Universidade Federal Fluminense, Niteroi, Brazil

[2] University of Pittsburgh, Pittsburgh PA, USA

routing between a specific source and destination. Simulation results prove that the proposal outperforms the AQRV (adaptive QoS-based routing for VANETs) method when comparing distance, hop count, packet delivery rate, delay, and computational complexity.

The fourth paper from Renato S. Silva and Luís F. M. Moraes is entitled "A balanced prior knowledge model based on beta function for evaluating DIDS performance." The authors ponder that a distributed intrusion detection system (DIDS) based on federation is a platform of autonomous IDS instances that cooperate to improve the overall system performance. The authors claim that evaluating DIDS performance is a non-trivial task. Thus, they propose an analytic model blending Bayesian inference with beta distribution to evaluate the functional performance of DIDS platforms. The results show that the performance metrics the proposal provides for an evaluated DIDS are closer to those obtained in practical deployment scenarios than metrics obtained from previous analytical performance models.

The ensuing paper from Gabriel Antonio F. Rebello and his colleagues is entitled "A security and performance analysis of proof-based consensus protocols." The authors posit that consensus protocols of public blockchain present vulnerabilities and performance limitations that hinder the adoption of blockchain technology. The paper discusses the centralization issue of Proof of Work (PoW) and Proof of Stake (PoS) and compares proof-based alternative protocols, such as Proof of Elapsed Time (PoET), Proof of Burn (PoB), Proof of Authority (PoA), and Delegated Proof of Stake (DPoS). The authors also provide a security evaluation of the IOTA protocol.

The sixth paper from Lucas C. B. Guimaraes and his colleagues proposes "A threat monitoring system for intelligent data analytics of network traffic." The authors claim that the high number of low-power computing devices, such as IoT devices connected to the Internet, augment the impact of distributed attacks, as these devices are easily compromised on a large scale. Moreover, the time to discover a cyberattack may be longer than weeks to months, exponentially increasing the risk of financial losses and irreparable damage. The authors propose TeMIA-NT (ThrEat Monitoring and Intelligent data Analytics of Network Traffic), a real-time flow analysis system that uses parallel flow processing. TeMIA-NT introduces an architecture for real-time detection of network intrusions that uses the structured streaming library and provides two modes of operation: offline and online. The results show that hyperparametric optimization on algorithm performance positively affected the proposed system, exemplified by a 30% reduction in false negative rate for the best evaluated tree-based models.

The last paper from Joao Vitor V. Silva and his colleagues introduces "A statistical analysis of intrinsic bias of network security datasets for training machine learning mechanisms." The authors note that network security–intended machine learning mechanisms lack accurate evaluation, comparison, and deployment due to the scarcity of well-constructed datasets. Thus, the authors propose a statistical analysis of the features in four highly used security datasets: NSL-KDD, CIC-IDS 2017, UNSW-NB15, and CIC-Botnet2014. The study shows that the evaluated datasets introduce bias when applying machine learning classification models because most of the features in the datasets derive from different probability distributions for attack and benign traffic. Moreover, the study also demonstrates that the random forest classifier, associated with the recursive feature elimination (RFE) as a feature selection procedure, is the machine learning technique that best performs for the evaluated network-security datasets.

Acknowledgements The guest editors would like to express their deep appreciation to the Editor-in-Chief, Prof. Guy Pujolle, for the opportunity to produce 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 process of this publication. Last, but certainly not least, the guest editors would like to express their thanks to all the authors for submitting quality articles and the reviewers for helping in the selection of papers and improving the accepted papers.