Guest Editorial Special Issue on Intrusion Detection for the Internet of Things

THE PROLIFERATION of IoT devices in everyday life has made their security a critical requirement. Currently, those devices are not secure enough because of several reasons. First, manufacturers do not account much for security, releasing products that are vulnerable to attacks, thus leaving security issues that are unlikely to be resolved. Second, many IoT devices lack the processing power to run antivirus software or even permit its installation. Finally, the heterogeneity, which characterizes the IoT in terms of applications, hardware, and software, expands the attack surface, while at the same time increasing the difficulty of deploying all-encompassing security solutions.

Despite some sort of security provided by IoT-enabling technologies or intrusion prevention systems, attackers still find ways to compromise devices. Unlike laptop and desktop computers which have frequent on–off cycles, many IoT devices, such as webcams and wireless routers, operate 24/7 unattended. This makes IoT devices prone to various attacks, such as those aiming at recruiting devices for the creation of botnets, or to leakage of private data, such as health data. An important building block for IoT protection is intrusion detection. Intrusion detection is critical to detect signs of known attacks and/or detect behavioral anomalies in IoT devices and the networks connecting them.

This special issue focuses on the recent advances in the area of intrusion detection for the IoT. It consists of 25 papers that were selected by experts via a peer-review process. In the following, we summarize these articles and highlight their major contributions.

Geng et al. [A1] propose PLC-READER, a memory attacks detection and response framework to secure cyber–physical systems. PLC_READER includes a comprehensive semantic analysis approach specifically designed for programmable logic controllers' proprietary protocol based on software reverse engineering and network traffic difference analysis, and a fine-grained memory structure analysis approach to identify the critical memory data. Experimental results demonstrate that PLC-READER can detect all memory attacks with an accuracy of 100% and timely execute corresponding emergency responses.

Malik et al. [A2] propose a framework to analyze the spread of ransomware and its impact on connected vehicles. The authors analyze the business impact of ransomware on a ride-hailing service and propose a fog computing architecture to reduce latency in vehicle-to-vehicle communication and vehicle-to-base station communication. Experimental results show that ransomware can have a debilitating impact on connected vehicle businesses due to their high mobility and connectivity with attacks on average impacting earnings by 45% per hour.

Bhale et al. [A3] propose OPTIMIST, a transparent, optimally placed, distributed IDS which can handle both high-rate and low-rate DDoS attacks. The placement problem is formulated as the weighted minimum vertex cover problem of a K-uniform hypergraph and solved with an approximation algorithm. The IDS module is based on an LSTM model where a novel offline training method for LSTM is proposed using WGAN-generated artificial flows. Extensive experimentation on simulation and testbed shows that OPTIMIST can best achieve the balance between DDoS detection and energy overhead.

Carrillo-Mondejar et al. [A4] propose HALE-IoT, a systematic approach to harden legacy IoT non-low-end devices by retrofitting defensive firmware modifications without access to the original source code. HALE-IoT approaches this nontrivial task via binary firmware reversing and modification. Experimental results show good performance and reliability with a remarkably accurate detection and prevention rate for attacks coming from both real vulnerabilities and synthetic exploits.

Fouda et al. [A5] propose an IDS for the Internet of Healthcare Things based on deep subclass dispersion one-class support vector machine (OSVM), a variation of the standard OSVM, which considers subclasses in the target class, in order to minimize the data dispersion within and between subclasses, thereby improving the discriminative power and classification performance of the IDS. Experimentation results show that the proposed approach outperforms the other relevant one-class classifiers for network intrusion detection.

Celdrán et al. [A6] propose a host-based and federated learning (FL)-oriented IDS for IoT spectrum sensors that consider unsupervised ML/DL and fingerprints based on system calls. The framework detection performance and consumption of resources are analyzed in both local and federated scenarios with six spectrum sensors deployed on Raspberry Pis. The obtained results significantly improve with respect to previous approaches for detecting SSDF attacks while protecting sensors privacy, and reducing the usage of CPU, memory, and storage at sensors.

Digital Object Identifier 10.1109/JIOT.2023.3244636

Uhřícek et al. [A7] propose BOTA, a botnet analysis system which uses the concepts of weak indicators and heterogeneous meta-classifiers to achieve higher accuracy compared with state-of-the-art systems, while also providing explainable results that are easy to understand. The authors provide an implementation capable to work on top of extended bidirectional flow data, making it deployable on large 100-Gb/s large-scale networks at the level of Internet service providers. The architecture is tested with various real-world and lab-created datasets, and it correctly identifies 94.3% of infected IoT devices without false positives.

Yumlembam et al. [A8] propose VGAEMalGAN, a generative adversarial network-based algorithm to attack the graph-based GNN Android malware classifier. The VGAE-MalGAN generator generates adversarial malware API graphs, and the VGAE-MalGAN substitute detector tries to fit the detector. The experimental analysis shows that VGAE-MalGAN can effectively reduce the detection rate of GNN malware classifiers, and that retraining the model with generated adversarial samples helps to combat adversarial attacks.

Heidari et al. [A9] propose a blockchain-based radial basis function neural networks model which improves data integrity and storage for smart decision making across different Internet of Drones. The authors discuss the use of blockchain to create decentralized predictive analytics, and a model for effectively applying and sharing deep learning (DL) methods in a decentralized fashion. They also assess the model using a variety of datasets to demonstrate the viability and efficacy of implementing the blockchain-based DL technique in the Internet of Drones contexts. Experimental results show that the proposed model is an excellent option for developing classifiers while adhering to the constraints placed by network intrusion detection.

Fadhilla et al. [A10] propose a botnet attack detection system for the IoT based on meta-learning ensemble models and evaluated the capability of a single-board system in addressing cyber-attack threats. Experiments show that the deployment of the proposed methodologies on edge devices exhibits similar results to PC-based desktop CPU-trained models.

Khan et al. [A11] propose Federated-SRUs, an IDS model based on simple recurrent units for the security of IoT-based industrial control systems (ICSs), which improves simple recurrent units architecture by reducing computational cost and alleviating the gradient vanishing issue in recurrent networks. Experimental results show that the proposed model outperforms existing state-of-the-art approaches. The performance is validated through experiments using real-world gas pipeline-based ICS network data, which indicates that Federated-SRUs is able to accurately detect intrusions in real time without compromising privacy and security.

Anyanwu et al. [A12] propose an intrusion detection model to identify Distributed Denial-of-Service (DDoS) attacks in SDN-based vehicular networks (VANET). The proposed solution employs the radial basis function kernel of the support vector machine classifier and an exhaustive parameter search. The proposed scheme shows an overall accuracy of 99.33%, a detection rate of 99.22%, and an average squared error of 0.007, outperforming existing benchmarks.

Zainudin et al. [A13] present XGBoost, a feature selection method for determining the most relevant data features with a hybrid convolutional neural network and long short-term memory (CNN-LSTM) for DDoS attack classification in software-defined networking (SDN)-based Industrial Internet of Things (IIoT) networks. The authors evaluate the proposed model on the CICDDoS2019 dataset, showing improved accuracy and low-complexity capability for low-latency IIoT requirements. Performance results show that the proposed model achieves a high accuracy of 99.50% with a time cost of 0.179 ms.

Lopez-Martin et al. [A14] propose an intrusion detection model for IoT networks based on a shallow-neural-network architecture with a light resource footprint. The model is based on a contrastive learning architecture that contrasts features and labels in an expanded latent space. The experimental results show a higher ability of the proposed model to detect unknown attacks than similar models and alternative machine learning models.

Meidan et al. [A15] propose CADeSH, a two-step collaborative anomaly detection method which first uses an autoencoder to differentiate benign and possibly malicious traffic flows, and then uses clustering to analyze only the infrequent flows and classify them as either benign or malicious. The method is evaluated using 21 days of real-world traffic data from eight IoT devices deployed on various networks. Experimental results show a macro-average area under the precision–recall curve of 0.841, an F1 score of 0.929, and an FPR of 0.014.

Rondon et al. [A16] present PoisonIvy, a series of generalized proof-of-concept attacks used to demonstrate that an attacker can use a malicious driver to perform denial of service, gain remote control, and abuse IoT system resources. Then they propose IVYCIDE, an IDS for the drivers used to integrate devices into complex IoT environments, such as smart buildings, government offices, private offices, and conference rooms. IVYCIDE detects unexpected network traffic operating as a passive monitoring system using machine learning and signature-based classification. Experimental results show that IVYCIDE achieves an average accuracy of 97% in classifying the type of POISONIVY attack and operates without modifications or operational overhead to existing IoT systems.

Roy et al. [A17] propose PLAKE, a physically unclonable function (PUF)-based authentication and key exchange protocol for IoT, which leverages cryptographic XOR, hash function for secure communication, and PUF for unique device-dependent identity generation and lightweight security solution to prevent physical attacks. The protocol performs device-to-device and device-to-server authentication without incurring additional communication and computation resources.

Musikawan et al. [A18] present AMDIDroid a deep neural network for the detection and identification of Android malware. AMDI-Droid is tested in six different scenarios on three datasets concerning static and dynamic analysis cases,

and the experimental results show that AMDI-Droid outperforms the competitors in terms of the accuracy, precision, recall, F1-score, and MCC metric.

Khoa et al. [A19] propose a collaborative learning framework for intrusion detection in IoT networks, which leverages transfer learning (TL) to overcome the unavailability of labeled data and dissimilarity of data features for training. Experiments on recent real-world cybersecurity datasets show that the proposed framework can improve more than 40% as compared to the state-of-the-art deep-learning-based approaches.

Fan et al. [A20] propose to use of machine unlearning, a technique that quickly updates machine learning models without retraining, to update DL-based models for traffic anomaly detection in IoT systems. The method, called ViFLa, groups training data based on estimated unlearning probability and treats each group as a virtual client in an FL framework. ViFLa also uses a new state transition ring mechanism into the statistical query learning framework to update the local model of each virtual client quickly.

Yang et al. [A21] propose a traceable privacy-preserving data-sharing method for fog-based smart logistics, which achieves data access control, data integrity protection, key escrow and abuse resistance, user privacy preserving, and scalability. The access policy hiding mechanism is used for user privacy preserving, while white-box tracing and certificateless public data integrity auditing techniques are employed to resist key abuse and escrow problems. The authors formally prove the security of the proposed scheme for indistinguishability of chosen plaintext attack security and traceability.

Zhang et al. [A22] show that small attacks could effectively mislead the predictions of well-trained ML monitors and proposed a monitor for predicting the fault condition of IIoT systems using the adversarial training technique. The model is designed to be formally robust to attacks with restricted magnitude. The authors also present a novel false data injection attack-generating method that utilizes the concept of adversarial perturbations to mislead well-trained monitors.

Zhang et al. [A23] propose a protocol-agnostic radio frequency fingerprinting identification system for open-set recognition, based on a slicing-enhanced preprocessing with noise augmentation. The proposed technique solves the problem of rogue device intrusion by rejecting access to unregistered transmitters and correctly identifying the registered ones.

Zhao et al. [A24] propose an intrusion detection method based on the semi-supervised FL scheme to address known FL issues, such as the privacy risk of having model parameters used to recover private data, not independent and identically distributed private data that adversely affects the training of FL, and high communication overhead caused by the large model size which hinders the actual deployment of the solution. Experiments on real-world traffic dataset show that the proposed method can achieve better detection performance as well as lower communication overhead than state-of-the-art methods.

Kamaldeep et al. [A25] propose a feature engineering and machine learning framework to detect DDoS attacks in the IoT-CIDDS dataset. The authors propose a complexity analysis of the feature-engineered dataset with five machine-learning techniques by creating training, validation, and testing datasets from IoT-CIDDS. The experimental results show that substantial feature reduction optimizes the performance of ML-based IDS for detecting DDoS attacks in standardized IoT networks employing a 6LoWPAN stack.

APPENDIX: RELATED ARTICLES

[A1] Y. Geng et al., "Defending cyber–physical systems through reverse-engineering-based memory sanity check," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8331–8347, 15 May 2023.

[A2] A. W. Malik, Z. Anwar, and A. U. Rahman, "A novel framework for studying the business impact of ransomware on connected vehicles," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8348–8356, 15 May 2023.

[A3] P. Bhale, D. R. Chowdhury, S. Biswas, and S. Nandi, "OPTIMIST: Lightweight and transparent IDS with optimum placement strategy to mitigate mixed-rate DDoS attacks in IoT networks," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8357–8370, 15 May 2023.

[A4] J. Carrillo-Mondéjar, H. Turtiainen, A. Costin, J. L. Martínez, and G. Suarez-Tangil, "*HALE-IoT*: Hardening legacy Internet of Things devices by retrofitting defensive firmware modifications and implants," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8371–8394, 15 May 2023.

[A5] M. Fouda, R. Ksantini, and W. Elmedany, "A novel intrusion detection system for Internet of Healthcare Things based on deep subclasses dispersion information," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8395–8407, 15 May 2023.

[A6] A. H. Celdrán, P. M. S. Sánchez, C. Feng, G. Bovet, G. M. Pérez, and B. Stiller, "Privacy-preserving and syscall-based intrusion detection system for IoT spectrum sensors affected by data falsification attacks," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8408–8415, 15 May 2023.

[A7] D. Uhřícek, K. Hynek, T. Čejka, and D. Kolář, "BOTA: Explainable IoT malware detection in large networks," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8416–8431, 15 May 2023.

[A8] R. Yumlembam, B. Issac, S. M. Jacob, and L. Yang, "IoT-based android malware detection using graph neural network with adversarial defense," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8432–8444, 15 May 2023.

[A9] A. Heidari, N. J. Navimipour, and M. Unal, "A secure intrusion detection platform using blockchain and radial basis function neural networks for Internet of Drones," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8445–8454, 15 May 2023.

[A10] C. A. Fadhilla, M. D. Alfikri, and R. Kaliski, "Lightweight meta-learning BotNet attack detection," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8455–8466, 15 May 2023.

[A11] I. A. Khan, D. Pi, M. Z. Abbas, U. Zia, Y. Hussain, and H. Soliman, "Federated-SRUs: A federated-simple-recurrent-units-based IDS for accurate detection of cyber attacks against IoT-augmented industrial control systems," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8467–8476, 15 May 2023.

[A12] G. O. Anyanwu, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim, "Optimization of RBF-SVM kernel using grid search algorithm for DDoS attack detection in SDN-based VANET," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8477–8490, 15 May 2023.

[A13] A. Zainudin, L. A. C. Ahakonye, R. Akter, D.-S. Kim, and J.-M. Lee, "An efficient hybrid-DNN for DDoS detection and classification in software-defined IIoT networks," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8491–8504, 15 May 2023.

[A14] M. Lopez-Martin, A. Sanchez-Esguevillas, J. I. Arribas, and B. Carro, "Contrastive learning over random Fourier features for IoT network intrusion detection," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8505–8513, 15 May 2023.

[A15] Y. Meidan, D. Avraham, H. Libhaber, and A. Shabtai, "CADeSH: Collaborative anomaly detection for smart homes," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8514–8532, 15 May 2023.

[A16] L. P. Rondon, L. Babun, A. Aris, K. Akkaya, and A. S. Uluagac, "IVYCIDE: Smart intrusion detection system against E-IoT driver threats," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8533–8546, 15 May 2023.

[A17] S. Roy, D. Das, A. Mondal, M. H. Mahalat, B. Sen, and B. Sikdar, "PLAKE: PUF-based secure lightweight authentication and key exchange protocol for IoT," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8547–8559, 15 May 2023.

[A18] P. Musikawan, Y. Kongsorot, I. You, and C. So-In, "An enhanced deep learning neural network for the detection and identification of android malware," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8560–8577, 15 May 2023.

[A19] T. V. Khoa et al., "Deep transfer learning: A novel collaborative learning model for cyberattack detection systems in IoT networks," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8578–8589, 15 May 2023.

[A20] J. Fan, K. Wu, Y. Zhou, Z. Zhao, and S. Huang, "Fast model update for IoT traffic anomaly detection with machine unlearning," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8590–8602, 15 May 2023.

[A21] Y. Yang et al., "A scalable and auditable secure data sharing scheme with traceability for fog-based smart logistics," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8603–8617, 15 May 2023.

[A22] X. Zhang, H. Tian, X. Zheng, and D. D. Zeng, "Robust monitor for industrial IoT condition prediction," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8618–8629, 15 May 2023.

[A23] X. Zhang, M. Lin, Y. Tian, Y. Huang, J. An, and T. Cui, "Data-enhancement-aided protocol-agnostic transmitter recognition for open-set in IoT," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8630–8644, 15 May 2023.

[A24] R. Zhao, Y. Wang, Z. Xue, T. Ohtsuki, B. Adebisi, and G. Gui, "Semi-supervised federated-learning-based intrusion detection method for Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8645–8657, 15 May 2023.

[A25] Kamaldeep, M. Malik, and M. Dutta, "Feature engineering and machine learning framework for DDoS attack detection in the standardized Internet of Things," *IEEE Internet Things J.*, vol. 10, no. 10, pp. 8658–8669, 15 May 2023.

ANTONINO RULLO, *Guest Editor*
Department of Informatics, Modelling, Electronics and Systems
University of Calabria
87036 Rende, Italy
(E-mail: n.rullo@dimes.unical.it)

ELISA BERTINO, *Guest Editor*
Department of Computer Science
Purdue University
West Lafayette, IN 47907 USA
(E-mail: bertino@purdue.edu)

KUI REN, *Guest Editor*
College of Computer Science and Technology
Zhejiang University
Hangzhou 310027, Zhejiang, China
(E-mail: kuiren@zju.edu.cn)