Hindawi
Security and Communication Networks
Volume 2022, Article ID 9804596, 4 pages
https://doi.org/10.1155/2022/9804596

Editorial

Identification of Attack Traffic Using Machine Learning in Smart IoT Networks

Muhammad Shafiq,[1] **Shah Nazir**,[2] **and Xiangzhan Yu**[3]

[1]*Guangzhou University, Guangzhou, China*
[2]*University of Swabi, Swabi, Pakistan*
[3]*Harbin Institute of Technology, Harbin, China*

Correspondence should be addressed to Muhammad Shafiq; srsshafiq@gmail.com

Received 18 March 2022; Accepted 18 March 2022; Published 11 April 2022

1. Introduction

Identifying attack traffic is very important for the security of Internet of Things (IoT) in smart cities by using machine learning (ML) algorithms. Recently, the IoT security research community has endeavoured to build anomaly, intrusion, and cyber-attack traffic identification models using machine learning algorithms for IoT security analysis. However, some critical and significant problems have not yet been studied in depth. One such problem is how to select an effective ML algorithm when there are a number of ML algorithms for a cyber-attack detection system for IoT security. Will early-stage traffic management give effective results if applied to IoT traffic management by using ML algorithms, or will this affect the performance of the ML model if several features are selected? Methods must avoid the risk of inaccuracy, inefficiency, and privacy leakage of machine learning techniques in IoT. The main objective of this Special Issue is to publish articles based on feature selection, algorithms, protocols, frameworks, and machine learning techniques in IoT that extend the current state of the art with innovative ideas and solutions in the broad area of security attack traffic detection and network traffic management. Theoretical and experimental studies for typical and newly emerging convergence technologies and cases enabled by recent advances are encouraged. High-quality review papers are also welcome.

1.1. Papers in This Special Section. A large number of papers were submitted to this Special Issue, and each paper was reviewed by three or more experts during the assessment process. After evaluating the overall scores, thirteen papers were selected for inclusion in this Special Issue.

Following is a brief description of the accepted papers:

(i) In paper [1], the Hybrid Monotone Empirical Mode Decomposition (HM-EMD) is a recent EMD-based method of generating intrinsic mode functions (IMFs) using the monotone property. The monotone property assumes that, at each IMF extraction step, local maxima and minima are either increasing or decreasing. Based on this property and along with the characteristics of EMD, the HM-EMD is a useful method for extracting hidden information in audio streams. This paper proposes an enhancement of HM-EMD based on the predicted correlation and periodicity between IMFs obtained from a modified intensity function. In addition, to prove its feasibility, they apply the method to detect short messages in music files. Experimental results show that, compared with traditional EMD and other recent EMD-based methods such as reduced iteration EMD, scalar-reduced iteration EMD, and modified iteration EMD, the proposed algorithm is superior to both nondominated sorting genetic algorithm II and fast nondominated sorting genetic algorithm II.

(ii) The sophisticated cyberattacks are evolving every day, and they are becoming difficult to be detected by conventional security measures. To defend the cyber-security of modern computer systems, researchers have been working on developing intelligent techniques to detect the cyberattacks. The AI techniques have been proved successful so far for many cybersecurity applications, such as intrusion detection, malware analysis, and attack forecasting. However, the complexity of these attacks grows rapidly and the AI techniques need to be continuously updated to detect these attacks. In this paper, the authors compare and analyze the approaches used in applying intelligent techniques in some applications of cybersecurity such as intrusion detection system (IDS), malware analysis, and network traffic monitoring. Based on the analysis, they define some open challenges in using AI for combating cybercrime. They also discuss the challenges and prospects by combing through over one hundred articles related to future research directions. Finally, they present their perspectives on how future research can improve the cyberattack detection system.

(iii) Paper [2] presents a communication cost optimization method based on security evaluation to address the problem of increased communication cost due to node security verification in the blockchain-based federated learning process. By studying the verification mechanism for useless or malicious nodes, they also introduce a double-layer aggregation model into the federated learning process by combining the competing voting verification methods and aggregation algorithms. The experimental comparisons verify that the proposed model effectively reduces the communication cost of the node security verification in the blockchain-based federated learning process.

(iv) In paper [3] entitled “Poor Coding Leads to DoS Attack and Security Issues in Web Applications for Sensors,” researchers from the Department of Computer Engineering at Konkuk University, South Korea, identify common web programming errors that could lead to a denial-of-service (DoS) attack in web applications for sensors. The research team developed a testbed for two kinds of applications: one for single sensor data collection and the other for data retrieval from a sensor network. Their findings reveal how easily common coding blunders can expose critical infrastructure to unfortunate circumstances.

(v) Study [4] presents that in edge computing environments, a dynamic network failure happens frequently due to factors like time-varying nodes and service fluctuations. This failure often affects the performance of applications or even causes crashes. With the emergence of the model-based anomaly detection method, previous work has proven its effectiveness in helping edge computing systems to detect anomalous behaviors and recover from failures at runtime. However, these techniques often require ad hoc model regeneration for each new state of the system and are not suitable for unpredictable edge computing environments. To address this problem, they present AdaGUM—an adaptive graph updating model-based anomaly detection method. The proposed method uses a multidimensional graph to capture the interdependency between different elements of edge computing systems (e.g., software components) and then generates the subsequent state transition paths through random walks over graphs. The system behavior is then compared with the transition path based on behavior space. They evaluate AdaGUM with three real-world open-source systems (e.g., Spark Streaming) using real failures as anomalies and two criteria: accuracy and performance overhead that measures system resource consumption. The evaluation results show that AdaGUM can correctly detect 99% of anomalies with an average overhead of 3%.

(vi) The authors in the paper “TBSMR: A Trust-Based Secure Multipath Routing Protocol for Enhancing the QoS of the Mobile Ad Hoc Network” proposed a trust-based multipath routing protocol called TBSMR to enhance the MANET’s overall performance. The main strength of the proposed protocol is that it considers multiple factors like congestion control, packet loss reduction, malicious node detection, and secure data transmission to intensify the MANET’s QoS. The performance of the proposed protocol is analyzed through the simulation in NS2. The simulation results justify that the proposed routing protocol exhibits superior performance than the existing approaches.

(vii) The paper entitled “Compressed Wavelet Tensor Attention Capsule Network” proposes the compressed wavelet tensor attention capsule network (CWTACapsNet), which integrates multiscale wavelet decomposition, tensor attention blocks, and quantization techniques into the framework of capsule neural network. Specifically, the multilevel wavelet decomposition is in charge of extracting multiscale spectral features in the frequency domain; in addition, the tensor attention blocks explore the multidimensional dependencies of convolutional feature [5] channels, and the quantization techniques make the computational storage complexities be suitable for edge computing requirements. The proposed CWTACapsNet provides an efficient way to explore spatial-domain features, frequency-domain features [6], and their dependencies which are useful for most texture classification tasks. Furthermore, CWTACapsNet benefits from quantization techniques and is suitable for edge computing applications. Experimental results on several texture datasets show that the proposed CWTACapsNet outperforms the state-of-the-art texture classification methods not only in accuracy but also in robustness.

(viii) In the paper entitled "Employing Deep Learning and Time Series Analysis to Tackle the Accuracy and Robustness of the Forecasting Problem," the authors apply time series to predict the crime rate to facilitate practical crime prevention solutions. Machine learning [7, 8] can play an important role in better understanding and analysis of the future trend of violations. Different time-series forecasting models have been used to predict the crime. These forecasting models are trained to predict future violent crimes. The proposed approach outperforms other forecasting techniques for daily and monthly forecast.

(ix) In the paper entitled "Cuckoo Search-based SVM (CS-SVM) Model for Real-Time Indoor Position Estimation in IoT Networks," the authors proposed a hybrid technique using Cuckoo Search-based Support Vector Machine (CS-SVM) for real-time position estimation. Cuckoo search is a nature-inspired optimization algorithm, which solves the problem of slow convergence rate and local minima of other similar algorithms. The Wi-Fi [9] RSSI fingerprint dataset of the UCI repository having seven classes is used for simulation purposes. The dataset is preprocessed by min-max normalization to increase accuracy and reduce computational speed. The proposed model is simulated using MATLAB and evaluated in terms of accuracy, precision, and recall with K-nearest neighbor (KNN) and support vector machine (SVM). Moreover, the simulation results show that the proposed model achieves a high accuracy of 99.87%.

(x) Although access control is one of the most important and effective methods for time-series data security, most existing access control models focus on the function of holding or managing data. However, the method of controlling transmission path is ignored. To maximize data security, the authors proposed an IoT time-series data security model based on thermometer encoding and proposed a new hyper-chaotic system as the source-generating system to build an adversarial attack model by using input parameter sensitivities detection. The authors designed a new adversarial attack model which can prevent input parameter sensitivity detection for realizing the maximum data security in the transmission process.

(xi) Due to the development of the digital economy, Internet of Things (IoT) has been widely used in various fields. The data security of IoT has become a hot research topic. Generally, the data security of IoT cannot be guaranteed without encryption. Time series encryption can better protect IoT data, but it is still a challenge for time-series encryption, especially in the case that there is an adversary attack. Therefore, the authors design an adversarial attack model and then propose an IoT time-series data security model based on thermometer encoding. Finally, the authors evaluate the performance of the proposed model through experiments and compare it with other encryption algorithms.

(xii) The last paper proposes an anomaly detection [10] algorithm selection service (ADS) with genetic algorithm (GA) and tsfresh tool. For IoT stream data, it requires that the anomaly detection algorithm can provide good recommendation for easy operation for IoT devices in factory automation systems. Moreover, the proposed method can compare suitable detection models from 28 candidates that are introduced by tsfresh tool with suitable input parameters which are determined by GA methods. The experiments are conducted and ADS system has achieved good results for anomaly detection which can be a good reference for other researchers or users for their solutions.

Conflicts of Interest

The editors declare that they have no conflicts of interest.

Acknowledgments

The editors would like to express their sincere thanks to all the authors who made this Special Issue possible and to the reviewers for their thoughtful contributions.

Muhammad Shafiq
Shah Nazir
Xiangzhan Yu

References

[1] J. Lou, Z. Xu, D. Zuo, and H. Liu, "Feature Extraction Method for Hidden Information in Audio Streams Based on HM-EMD," *Security and Communication Networks*, vol. 2021, Article ID 5566347, 12 pages, 2021.

[2] S. Xuan, M. Jin, X. Li, Z. Yao, W. Yang, and D. Man, "DAM-SE: A Blockchain-Based Optimized Solution for the Counterattacks in the Internet of Federated Learning Systems," *Security and Communication Networks*, vol. 2021, Article ID 9965157, 14 pages, 2021.

[3] K. B. Jalbani, M. Yousaf, M. S. Sarfraz, R. Jamili Oskouei, A. Hussain, and Z. Memon, "Poor Coding Leads to DoS Attack and Security Issues in Web Applications for Sensors," *Security and Communication Networks*, vol. 2021, Article ID 5523806, 11 pages, 2021.

[4] X. Yu, C. Shan, J. Bian, X. Yang, Y. Chen, and H. Song, "AdaGUM: An Adaptive Graph Updating Model-Based Anomaly Detection Method for Edge Computing Environment," *Security and Communication Networks*, vol. 2021, Article ID 9954951, 12 pages, 2021.

[5] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, "Selection of effective machine learning algorithm and Bot-IoT attacks traffic identification for internet of things in smart city," *Future Generation Computer Systems*, vol. 107, pp. 433–442, 2020.

[6] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CorrAUC: a malicious bot-IoT traffic detection method in IoT network using machine-learning techniques," *IEEE Internet of Things Journal*, vol. 8, no. 5, pp. 3242–3254, 2020.

[7] A. Krysovatyy, H. Lipyanina-Goncharenko, S. Sachenko, and O. Desyatnyuk, "Economic crime detection using support vector machine classification," *CEUR Workshop Proceedings*, vol. 2917, pp. 830–840, 2021.

[8] N. Usman, S. Usman, F. Khan et al., "Intelligent dynamic malware detection using machine learning in IP reputation for forensics data analytics," *Future Generation Computer Systems*, vol. 118, pp. 124–141, 2021.

[9] M. F. Khan, G. Wang, and M. Z. A. Bhuiyan, "Wi-Fi frequency selection concept for effective coverage in collapsed structures," *Future Generation Computer Systems*, vol. 97, pp. 409–424, 2019.

[10] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016.