Hindawi
Security and Communication Networks
Volume 2019, Article ID 4529757, 4 pages
https://doi.org/10.1155/2019/4529757

Editorial

Intrusion Detection and Prevention in Cloud, Fog, and Internet of Things

Xuyun Zhang,[1] Yuan Yuan,[2] Zhili Zhou,[3] Shancang Li,[4] Lianyong Qi,[5] and Deepak Puthal[6]

[1] *Department of Electrical, Computer and Software Engineering, University of Auckland, Auckland 1023, New Zealand*
[2] *Department of Computer Science and Engineering, Michigan State University, Michigan, MI 48824, USA*
[3] *Nanjing University of Information Science and Technology, Nanjing, 210044, China*
[4] *FET-Computer Science and Creative Technologies, University of the West of England, Bristol BS16 1QY, UK*
[5] *School of Information Science and Engineering, Chinese Academy of Education Big Data, Qufu Normal University, Qufu 276826, China*
[6] *Faculty of Engineering and IT, University of Technology Sydney, Ultimo, NSW 2007, Australia*

Correspondence should be addressed to Xuyun Zhang; xuyun.zhang@auckland.ac.nz

Received 9 April 2019; Accepted 9 April 2019; Published 23 May 2019

We are pleased to announce the publication of the special issue focusing on intrusion detection and prevention in cloud, fog, and Internet of Things (IoT). Internet of Things (IoT), cloud, and fog computing paradigms are as a whole provision a powerful large-scale computing infrastructure for many data and computation intensive applications. Specifically, the IoT technologies and deployment can widely perceive our physical world at a fine granularity and generate sensing data for further insight extraction. The fog computing facilities can provide computing power near the IoT devices where data are generated, aiming to achieve fast data processing for time critical applications or save the amount of data transmitted into cloud for storage or further processing. The cloud computing platforms can offer big data storage and large-scale processing services for cheap long-term storage or data intensive analytics with more advanced data mining models. Hence, it can be seen that the IoT/fog/cloud computing infrastructures can support the whole lifecycle of large-scale applications where big data collection, transmission, storage, processing, and mining can be seamlessly integrated. However, these state-of-the-art computing infrastructures still suffer from severe security and privacy threats because of their built-in properties such as the ubiquitous-access and multitenancy features of cloud computing, or the limited computing capability of IoT devices. The expanded attack surface and the lack of effective security and privacy protection measures are still one of the barriers of widely deploying applications on the IoT/fog/cloud infrastructure.

Intrusion detection and prevention systems that monitor the devices, networks, and systems for malicious activities and policy violations are one of the key countermeasures against cybersecurity attacks. With a wide spectrum, the detection and prevention systems vary from antivirus software to hierarchical systems monitoring the traffic of an entire backbone networks. In general, intrusion detection systems can be categorized into two groups, that is, signature-based detection (malicious patterns are already known) and anomaly-based detection (no patterns are given). Traditional methods and systems might fail to be directly applicable to the state-of-the-art computing paradigms and infrastructure as mentioned above. Novel intrusion detection and prevention algorithms and systems are in demand to cater for the new computing infrastructure and newly emerging cybersecurity attacks and threats, taking into account the factors such as algorithmic scalability, computing environment heterogeneity, data diversity, and complexity. Extensive research is required to conduct more scalable and effective intrusion detection and prevention in IoT/fog/cloud. Many relevant theoretical and technical issues have not been answered well yet. As such, it is high time to investigate the related issues in intrusion detection and prevision in IoT, fog, and cloud computing by examining intrusion detection and prevision algorithms, methods, architecture, systems, platforms, and applications in detail. This special issue gained substantial interests of researchers from all over the world and our editorial team consisting of six researchers in this field have rigorously selected 20 articles out of 60 submissions for publication. The research topics include intrusion detection system, intrusion prevention systems, DDoS attack detection, network/IoT anomaly detection, anomaly detection in cloud, malware detection, privacy-preservation technologies, and other closely related works on data deduplication, cloudlet placement, and fault analysis.

In the paper entitled "Fingerprinting Network Entities Based on Traffic Analysis in High-speed Network Environment", *X. Gu et al.* studied the entity identification problem in high-speed network environment to detection potential intruders and proposed to use the PFQ kernel module and Storm to capture high-speed packet and analyse online traffic, respectively. Based on this, they further proposed a novel device fingerprinting technology based on the runtime environment analysis that employs a logistic regression model and the sliding window mechanism to implement online identification.

In the paper entitled "Test Sequence Reduction of Wireless Protocol Conformance Testing to Internet of Things", *W. Lin et al.* investigated the wireless protocol conformance testing problems which just judge whether a wireless protocol has been performed as expected and proposed an improved method based on an overlapping technique that makes use of invertibility and multiple unique input/output sequences. Specifically, the method consists of two steps: the maximum-length invertibility-dependent overlapping sequences (IDOSs) are constructed in the first step, and a minimum-length rural postman tour covering the just constructed set of maximum-length IDOSs is generated. Finally, a test sequence is extracted from the tour.

In the paper entitled "Flow Correlation Degree Optimization Driven Random Forest for Detecting DDoS Attacks in Cloud Computing", *J. Cheng et al.* investigated the Distributed Denial-of-Service (DDoS) attacks in cloud computing and proposed a DDoS attack detection method with the enhanced random forest (RF) technique optimized by a genetic algorithm based on the flow correlation degree (FCD) features. Specifically, the features of attack flow and normal flows are described by the two-tuple FCD feature consisting of package-statistical degree (PSD) and semidirectivity interaction abnormality (SDIA). A genetic algorithm based on the FCD feature sequences is used to optimize two key parameters of the decision tree in the RF, and the trained RF model with the optimized parameters is employed to generate the classifier for DDoS attack detection.

In the paper entitled "A Cooperative Denoising Algorithm with Interactive Dynamic Adjustment Function for Security of stacker in Industrial Internet of Things", *D. Huang et al.* studied the problem of security monitoring of stacker in Industry IoT (IIoT) and proposed a cooperative denoising algorithm with interactive dynamic adjustment function. Specifically, the denoising framework named as IDVSLMS-EEMD was constructed based on the advantages of LMS, VSLMS, and improved VSLMS-EEMD. Real-world data applied in Power Grid of China was used to verify and simulate the effectiveness of the proposed algorithms.

In the paper entitled "A Constraint-aware Optimization Method for Concurrency Bug Diagnosis Service in a Distributed Cloud Environment", *L. Bo and S. Jiang* investigated the performance problems in concurrency bug diagnosis services which analyse concurrent software and detect concurrency bugs and proposed a static constraint-aware method to simplify concurrent program buggy traces. Specifically, the maximal sound dependence relations of original buggy traces are calculated based on the constraint models. The simplified traces can be obtained after checking the dependent constraints iteratively and forwarding current events to extend thread execution intervals.

In the paper entitled "Applying Catastrophe Theory for Network Anomaly Detection in Cloud Computing Traffic", *L. Khatibzadeh et al.* examined the network traffic anomaly detection problems in cloud computing environments and proposed a catastrophe theory based approach aiming to depict sudden change processes of the network effectively caused by the dynamic nature of the cloud. Exponential Moving Average (EMA) was applied for the state variable in sliding window to better show the dynamicity of cloud network traffic, and entropy was used as one of the control variables in catastrophe theory to analyse the distribution of traffic features.

In the paper entitled "A Privacy Protection Model of Data Publication Based on Game Theory", *L. Kuang et al.* investigated the user privacy protection problem in sensor acquisition technology because the attacker may identify the user based on the combination of user's quasi-identifiers and the fewer quasi-identifier fields result in a lower probability of privacy leaks. Specifically, they tried to determine an optimal number of quasi-identifier fields under the constraint of trade-offs between service quality and privacy protection. To this aim, the service development process is modelled as a cooperative game between the data owner and consumers, and the Stackelberg game model is leveraged to determine the number of quasi-identifiers that are published to the data development organization. Experiment showed that the data loss of our model is less than that of the traditional k-anonymity especially when strong privacy protection is applied.

In the paper entitled "A Quantum-based Database Query Scheme for Privacy Preservation in Cloud Environment", *W. Liu et al.* studied the privacy protection problems when users access sensitive cloud data and proposed a quantum-based database query scheme for privacy preservation in cloud environment to achieve privacy preservation and reduce the communication complexity. Specifically, all the data items of a database are encrypted by different keys for protecting server's privacy, and the server is required to transmit all these encrypted data items to the client with the oblivious transfer strategy to guarantee the users' privacy. Moreover, two oracle operations, i.e., modified Grover iteration and special offset encryption mechanism, are combined together to ensure that a user can correctly query a desirable data item.

In the paper entitled "Application of Temperature Prediction based on Neural Network in Intrusion Detection of IoT", *X. Liu et al*. studied the security of network information in IoT and proposed to use a neural network to construct the farmland Internet of Things intrusion detection system to detect anomalous intrusion. They used the temperature data from an IoT acquisition system as the case study and adopted different time granularities for feature analysis. Results showed that the neural network can predict the temperature sequence of varying time granularities better and ensure a small prediction error.

In the paper entitled "Semantic Contextual Search based on Conceptual Graphs over Encrypted Cloud", *Z. Wang et al*. explored the problem of ignorance of context information of the topic sentence when constructing conceptual graph in cloud searchable encryption. To address this problem, the authors defined and constructed semantic search encryption scheme for context-based conceptual graph (ESSEC). The contextual contact was associated with the central key attributes in the topic sentence and its semantic information was extended, so as to improve the accuracy of the retrieval and semantic relevance. Experiments on real data showed that the scheme is effective and feasible.

In the paper entitled "Adaptive DDoS attack detection method based on multiple-kernel learning", *J. Cheng et al*. investigated the distributed denial of service (DDoS) attack problems for Internet security and proposed an adaptive DDoS attack detection method (ADADM) based on multiple-kernel learning (MKL). Five features from the burstiness of DDoS attack flow, the distribution of addresses and the interactivity of communication, were employed to describe the network flow characteristics. A classifier was established to identify an early DDoS attack by training simple multiple-kernel learning (SMKL) models with two characteristics including interclass mean squared difference growth (M-SMKL) and intraclass variance descent (S-SMKL). The sliding window mechanism is used to coordinate the S-SMKL and M-SMKL to detect the early DDoS attacks. The experimental results indicate that this method can detect DDoS attacks early and accurately.

In the paper entitled "A Sequence Number Prediction based Bait Detection Scheme to Mitigate Sequence Number Attacks in MANETs", *R. H. Jhaveri et al*. explored the sequence number attacks which can degrade the network functioning and performance by attracting the sender to establish a path through the adversary node and proposed a proactive secure routing mechanism which makes use of linear regression mechanism to predict the maximum destination sequence number that the neighbouring node can insert in the RREP packet. As an additional security checkpoint, a bait detection mechanism is used to establish the confidence in marking a suspicious node as a malicious node. Results showed that the approach improves the network performance in the presence of adversaries as compared to previous schemes.

In the paper entitled "RoughDroid: Operative Scheme for Functional Android Malware Detection", *K. Riad and L. Ke* studied the malware problems in mobile applications and proposed a floppy analysis approach *RoughDroid*, which can discover Android malware applications directly on a smartphone. *RoughDroid* is based on seven feature sets from the XML manifest file of an Android application and three feature sets from the Dex file. Those feature sets are fed to the Rough Set algorithm to classify the Android application as either benign or malicious elastically. The experimental results showed that *RoughDroid* has 95.6% detection performance for the malware families at 1% false-positive rate.

In the paper entitled "Secure Deduplication Based on Rabin Fingerprinting over Wireless Sensing Data in Cloud Computing", *Y. Zhang et al*. explored the data deduplication problem in cloud computing because existing data deduplication technologies still suffer security and efficiency drawbacks and proposed two secure data deduplication schemes based on Rabin fingerprinting over wireless sensing data in cloud computing. The first scheme is based on deterministic tags and the other one adopts random tags. The proposed schemes realize data deduplication before the data is outsourced to the cloud storage server, and hence both the communication cost and the computation cost are reduced. Our security analysis shows that the proposed schemes are secure against offline brute-force dictionary attacks, and the random tag makes the second scheme more reliable.

In the paper entitled "Enhanced Adaptive Cloudlet Placement Approach for Mobile Application on Spark", *Y. Zhang et al*. investigated the cloudlet placement problem for facilitating mobile computation offloading and proposed an enhanced adaptive cloudlet placement approach named EACP-CA (Enhanced Adaptive Cloudlets Placement approach based on Covering Algorithm) for mobile applications in a given network area. The CA (Covering Algorithm) was used to adaptively cluster the mobile devices based on their geographical locations, and the cloudlet destination locations were also determined according to the clustering centres. The algorithms were implemented on Apache Spark, and the experiment results showed the effectiveness and efficiency of the proposed approach.

In the paper entitled "A Security Sandbox Approach of Android Based on Hook Mechanism", *X. Jiang et al*. studied the security problems in the Android systems and proposed a new security sandbox approach of Android based on hook mechanism to further enrich Android malware detection techniques. The sandbox monitors the behaviours of a target application by using a process hook-based dynamic tracking method during its running period. It can create an isolated virtual space where *apk* can be installed, run, and uninstalled and builds a risk assessment approach based on behaviour analysis. Experiments on malware and normal application samples verified the security of the sandbox.

In the paper entitled "Towards Optimized DFA Attacks on AES under Multibyte Random Fault Model", *R. Wang et al*. investigated the Differential Fault Analysis (DFA) attack problems and pointed out that the state-of-the-art attack is not fully optimized since no clear optimization goal was set. Accordingly, the authors proposed two optimization goals, i.e., the fewest ciphertext pairs and the least computational complexity, for optimization. To achieve these goals, the corresponding optimized key recovery strategies are identified to further increase the efficiency of DFA attacks on AES. Then, a more accurate security assessment of AES can be completed.

In the paper entitled "Street-Level Landmark Evaluation Based on Nearest Routers", *R. Li et al.* examined the evaluation issues of street-level landmarks for IP geolocation and proposed a street-level landmark evaluation approach based on the nearest router given that the location organization declared is regarded as an area not a point. Specifically, the declared location of preevaluated landmark is verified by IP location databases, and landmarks are grouped according to their nearest routers. The distance constraint is obtained using the delay value between a landmark and its nearest router by delay-distance correlation, based on which a relation model is established among distance constraint, organization's region radius, and distance between two landmarks. The experiment results showed that geolocation errors decrease obviously using evaluated landmarks.

In the paper entitled "Energy-Efficient Cloudlet Management for Privacy Preservation in Wireless Metropolitan Area Networks", *X. Xu et al.* investigated the energy and privacy protection problems in cloudlet based wireless metropolitan area networks (WMAN) and proposed an energy-efficient cloudlet management method, named ECM, for privacy preservation in WMAN. The problem was formulated with an optimization model. Based on the live virtual machine (VM) migration technique, a corresponding privacy-aware VM scheduling method for energy saving was designed to determine which VMs should be migrated and where they should be migrated. Experimental results demonstrated that the proposed method is both efficient and effective.

In the paper entitled "Scheduling Parallel Intrusion Detecting Applications on Hybrid Clouds", *Y. Zhang et al.* examined the scheduling problems in Parallel Intrusion Detection (PID) which can be regarded as a Bag-of-Tasks (BoT) application and proposed to construct an Iterated Local Search (ILS) algorithm which uses an effective heuristic to obtain the initial task sequence and an insertion-neighbourhood-based local search method to explore better task sequences with lower makespans. Specifically, the authors constructed a Fast Task Assignment (FTA) method by integrating an existing Task Assignment (TA) method with an acceleration mechanism to achieve efficiency without loss of any effectiveness. The experiment results showed that the proposed method can outperform the state-of-the-arts.

We strongly believe that this special issue will advance the understanding and research of various intrusion detection and prevention techniques and the closely related privacy and security technologies in cloud, edge/fog and IoT. We hope that the audience will enjoy reading these novel contributions.

Conflicts of Interest

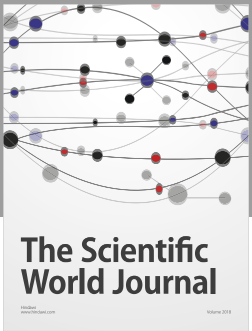
The editors declare that they have no conflicts of interest regarding the publication of this special issue.

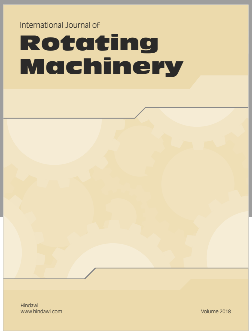
Acknowledgments

We would also like to cordially thank all the reviewers who have participated in the review process of the articles submitted to this special issue and the special issue coordinators and the technical supports from the publishing team.

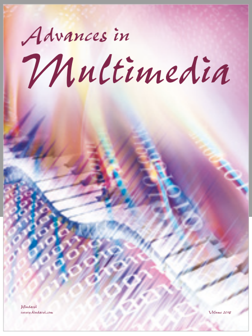
Xuyun Zhang
Yuan Yuan
Zhili Zhou
Shancang Li
Lianyong Qi
Deepak Puthal

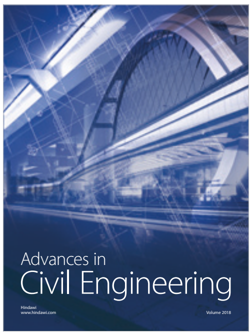
Journal of
Engineering


The Scientific
World Journal

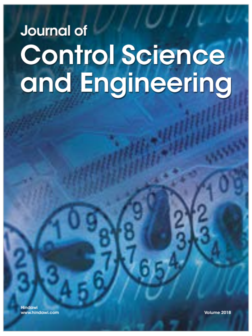

International Journal of
Rotating
Machinery

Journal of
Sensors

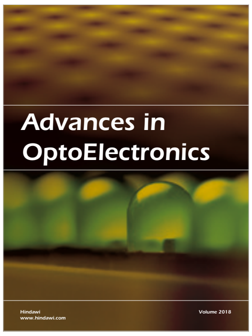

Advances in
Multimedia


Advances in
Civil Engineering

Journal of
Robotics

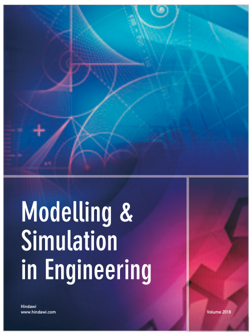

Journal of
Control Science
and Engineering

Journal of
Electrical and Computer
Engineering

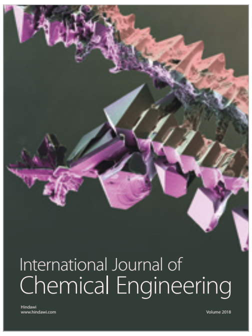

Advances in
OptoElectronics

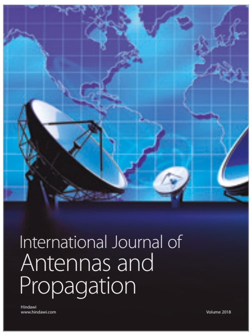
VLSI Design

International Journal of
Navigation and
Observation

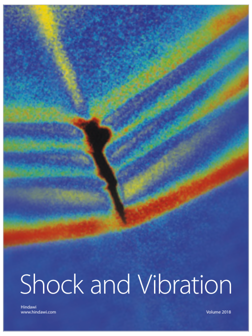

Modelling &
Simulation
in Engineering

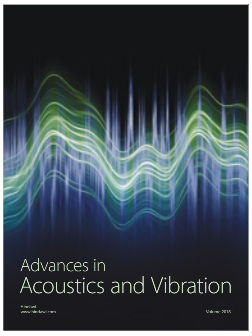
International Journal of
Aerospace
Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and
Propagation

Active and Passive
Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration