Hindawi Publishing Corporation
Journal of Electrical and Computer Engineering
Volume 2016, Article ID 2093790, 2 pages
http://dx.doi.org/10.1155/2016/2093790

Editorial

System and Network Security: Anomaly Detection and Monitoring

Michele Vadursi,[1] Andrea Ceccarelli,[2] Elias P. Duarte Jr.,[3] and Aniket Mahanti[4]

[1] *University of Naples "Parthenope", 80143 Napoli, Italy*
[2] *University of Florence, 50134 Florence, Italy*
[3] *Federal University of Paraná, 19018 Curitiba, PR, Brazil*
[4] *University of Auckland, Auckland 1142, New Zealand*

Correspondence should be addressed to Michele Vadursi; vadursi@uniparthenope.it

Received 9 May 2016; Accepted 9 May 2016

Large-scale systems and networks often operate under variable and unpredictable conditions, thus requiring efficient and adaptive monitoring and error detection solutions. Furthermore, the increasing complexity and dynamicity of current systems and networks ask for solutions that infer the status by looking for anomalies rather than directly detecting errors. Anomalous behavior is an indication not only of hardware and software faults, but also of security threats including intrusion attempts and frauds, which represent an increasingly relevant challenge from both scientific and socioeconomic point of view. The timely identification of anomalies in dependable systems allows timely error and security threat detection which can trigger appropriate reactions.

This special issue covers a wide range of topics that are of interest to researchers and practitioners in the field of security and anomaly detection in computer systems and networks. The papers contained in this special issue include research articles focused on network intrusion detection, malware detection in mobile devices, clock synchronization vulnerabilities in industrial networks, privacy preservation in IP version 6, and abrupt changes of the available bandwidth.

Distributed Denial of Service (DDoS) attacks are constructed by malicious entities by flooding the target host with traffic thus denying it from servicing legitimate requests. Network intrusion detection systems are deployed to identify and thwart such attacks. Several techniques based on signatures and observed anomalies have been proposed in the literature. The paper by Ö. Cepheli et al. entitled "Hybrid Intrusion Detection System for DDoS Attacks" proposes a hybrid framework combining signature-based and anomaly-based methods for improved DDoS attack detection.

Intrusion detection involves sifting through large amounts of network traffic. Data compression can improve the efficacy of the intrusion detection system. The paper entitled "SVM Intrusion Detection Model Based on Compressed Sampling" by S. Chen et al. presents a Support Vector Machine (SVM) intrusion detection model based on compressive sampling. The paper shows that by using compressed sensing theory the proposed SVM intrusion detection system can utilize a small sample of the network data for training its classifiers and detection time is reduced.

With mobile device sales surpassing those of desktop devices, more people are connecting to the Internet through their smartphones and tablets. This shift to a new platform has attracted the attention of attackers to target mobile devices. O. Somarriba et al. in their paper entitled "Detection and Visualization of Android Malware Behavior" present a monitoring architecture to identify malicious Android applications.

Clock synchronization is an important requirement in several industrial networks such as automation, stock market, and telecommunications. The IEEE 1588 standard allows clock synchronization across the nodes in an Ethernet network; however, this standard does not provide adequate security. In the paper entitled "Protecting Clock Synchronization: Adversary Detection through Network Monitoring" E. Lisova et al. describe clock synchronization vulnerabilities and evaluate solutions to mitigate these attacks.

Entities sharing sensitive information over the Internet should remain anonymous. Address rotation of the sender and receiver can prevent an attacker from discovering the identities of the communicating parties. The Moving Target IPv6 Defense (MT6D) architecture implements user anonymity by automatically changing IP version 6 addresses. D. Basam et al. in their paper entitled "Strengthening MT6D Defenses with LXC-Based Honeypot Capabilities" extend their work on MT6D to study suspicious activity on the discarded addresses and strengthen the MT6D parameters.

Available bandwidth is an important network performance metric, which helps in routing, Quality of Service (QoS), and traffic engineering on the Internet. D. Santoro and M. Vadursi in their paper entitled "Performance Analysis of a DEKF for Available Bandwidth Measurement" present a characterization of a measurement algorithm based on a Discrete-time Extended Kalman Filter (DEKF) for tracking abrupt changes of the available bandwidth.

We sincerely believe this special issue has highlighted relevant emerging issues in security of computer systems and networks, in particular the Internet. We hope the research results presented in this special issue will enable the research community to further the field, by proposing novel and efficient solutions to challenges facing the computer systems and network security community.

Acknowledgments

We thank the authors who made submissions to this special issue and the reviewers for their support and detailed reviews in making this special issue possible.

Michele Vadursi
Andrea Ceccarelli
Elias P. Duarte Jr.
Aniket Mahanti

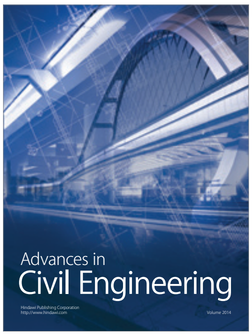
Journal of
Engineering

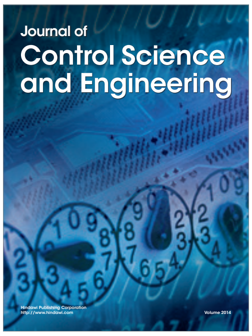
The Scientific World Journal

International Journal of
Rotating Machinery

Journal of
Sensors

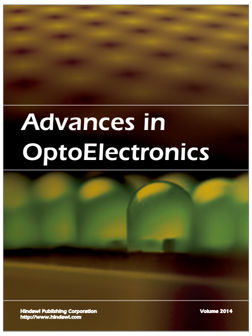
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering


Journal of
Control Science and Engineering

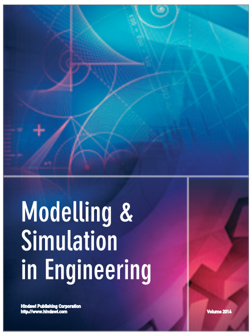
Journal of
Robotics

Journal of
Electrical and Computer Engineering

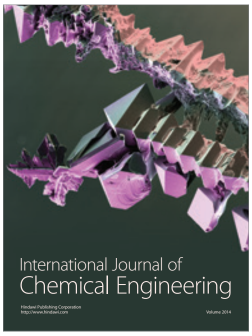

Advances in
OptoElectronics

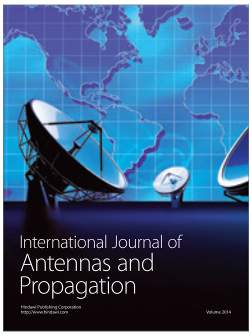
VLSI Design

International Journal of
Navigation and Observation

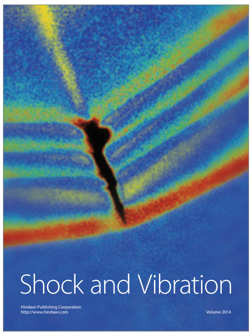

Modelling & Simulation in Engineering

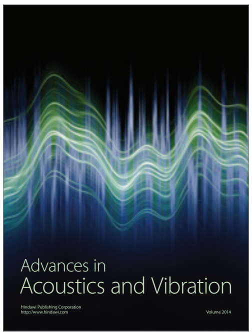
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration