Hindawi Publishing Corporation
EURASIP Journal on Advances in Signal Processing
Volume 2009, Article ID 527689, 2 pages
doi:10.1155/2009/527689

Editorial

Signal Processing Applications in Network Intrusion Detection Systems

Chin-Tser Huang,[1] Rocky K. C. Chang,[2] and Polly Huang[3]

[1] *Department of Computer Science and Engineering, University of South Carolina, Columbia, SC 29208, USA*
[2] *Department of Computing, The Hong Kong Polytechnic University, Hung Hom, Kowloon, Hong Kong SAR, China*
[3] *Department of Electrical Engineering, National Taiwan University, Taipei 10617, Taiwan*

Correspondence should be addressed to Chin-Tser Huang, huangct@cse.sc.edu

Received 25 February 2009; Accepted 25 February 2009

In recent years, the problem of network intrusion detection has attracted a lot of attention in the field of network security. Network intrusions carried out in various forms, such as worms, virus, spamming, Trojan horse, and many others, pose two major threats and damage on the victims. First, the intruders probe, gather, and deduce sensitive information about target hosts in an effort to gain unauthorized access to them and their networks. Second, the intruders inject unwanted packets into the target networks, aiming to disrupt the normal communications and services provided by the target networks. It is therefore critically important to implement effective network intrusion detection systems (NIDSs) to monitor the network and detect the intrusions in a timely manner.

Signal processing techniques have found applications in NIDS, because of their ability of detecting novel intrusions and attacks, which cannot be achieved by signature-based NIDS. Therefore, the primary objective of an NIDS based on signal processing techniques is to profile the normal network traffic pattern or application-level behavior and to classify intrusions or unwanted traffic as anomalies. Wavelets, entropy analysis, and data mining techniques are examples in this regard. However, the major challenges of the signal processing-based approaches lie in the adaptive modeling of normal network traffic and the high false alarm rate due to the inaccuracy of the modeled normal traffic pattern. The emergence of a variety of wireless networks and the mobility of nodes in such networks only add to the complexity of the problems.

The goal of this special issue is to present some of the state-of-the-art techniques of applying signal processing techniques to the intrusion detection problems. This issue features seven papers which cover generic issues in designing NIDS, such as improving the false-positive performance, speed performance, and quality of the training data (the first two papers), applying wavelet analysis to detect attacks on wired networks and wireless networks (the third and fourth papers), detecting flooding-based and low-rate denial-of-service attacks (the fifth and sixth papers), and detecting game bots in massively multiplayer online role playing games (the seventh paper).

In the paper "Detecting network intrusions using signal processing with query-based sampling filter," coauthored by Liang-Bin Lai et al., the authors take a joint signal processing and neural network approach toward the intrusion detection problem. Learning-based solutions are known vulnerable to noise in the training data. The proposed quantization method overcomes this problem by screening the training data and comparing to the "known attacks" classified by the neural network. Such a treatment results in a more robust classification of intrusions, allowing potential discovery of rare (new) attacks. This interesting combination of signal processing and learning techniques is shown effective, and the choice of the query-based sampling filter is justified using the 1999 DARPA intrusion detection dataset.

In the paper "An adaptive approach to granular real-time anomaly detection," coauthored by Chin-Tser Huang and Jeff Janies, the authors propose a framework allowing flexible granular examination of network traffic for individual hosts. Given the diversity of Internet use today, with heterogeneous applications and usage, an everyday norm of Internet access for one host might be anomaly for others. Such observation

of instruction being relative is addressed in the Fates system proposed. In that, traffic can be classified by the source or destination addresses (or port numbers) at different granularity before a score-based anomaly detection mechanism is applied. The Fates system is implemented utilizing libpcap library and shown effective capturing anomalies using an extensive set of traffic data.

In the paper "Network anomaly detection based on wavelet analysis," coauthored by Wei Lu and Ali Ghorbani, the authors propose a new network anomaly detection model based on wavelet approximation and system identification theory. The uniqueness of the proposed approach lies in that the observed network traffic first goes through a feature analysis stage which derives fifteen features to characterize the network traffic behaviors, and then the derived features are used as the input signals to the wavelet analysis and finally a decision on the intrusion is made. The authors evaluate their system against the data from the 1999 DARPA intrusion detection dataset and from a real WiFi ISP network to show its ability to detect both attack types and attack instances.

In the paper "Multilayer statistical intrusion detection in wireless networks," coauthored by Mohamed Hamdi et al., a vertical stack, from physical to transport layer, of traffic anomaly detection mechanisms is detailed. What is unique in this work is the use of maximum overlap discrete wavelet transform (MODWT) to detect pattern shift in fractal processes. This form of DWT discounts variance change due to temporal shift in the aggregated signal, thus highlights the fractality changes that should really be attracting network administrators' attention. The authors apply the MODWT on multiple levels, including wireless signal strength transition detection (MAC address spoofing) and the traffic rate process anomaly detection (network intrusion) which are the key components of the multilayer NIDS described in the paper.

In the paper "Detecting distributed network traffic anomaly with network-wide correlation analysis," coauthored by Zong-Lin Li et al., the authors propose to detect DDoS attacks using a network-wide correlation analysis of instantaneous parameters. The idea is that anomalies caused by the same attack source will exhibit a strong correlation in the time and frequency domains. They have applied a principal component analysis-based method to detect anomalies with strong correlations. Their simulation results based on real-network traces have shown that the network-wide correlation analysis is effective on detecting distributed network traffic anomaly even when the attack does not induce detectable anomaly in individual link.

In the paper "Detecting pulsing denial-of-service attacks with nondeterministic attack intervals" coauthored by Xiapu Luo et al., the authors address the problem of detecting a class of low-rate DoS attacks, called pulsing denial of service (PDoS) attacks, which send a sequence of attack pulses to reduce TCP throughput. The authors propose and implement a new anomaly-based detection scheme, Vanguard, which uses a CUSUM algorithm to detect three traffic anomalies induced by PDoS attacks. Unlike the previous approaches, Vanguard is designed to detect the traditional flooding-based DoS attacks as well as the PDoS attacks which may be launched with nondeterministic attacks periods. Their experiment results show that Vanguard is more effective in detecting PDoS attacks than previous anomaly detection methods.

In the paper "Identifying MMORPG bots: A traffic analysis approach," coauthored by Kuan-Ta Chen et al., the authors address an important and interesting problem of detecting game bots. In the world of online games, these game bots are often considered as "intrusions," because the bots, unlike human players, never get tired. They have proposed a number of methods based on game traffic analysis to identify these game bots automatically. Using Ragnarok Onlineas a case study, they have shown that the traffic corresponding to bots and human players is distinguishable in various respects, such as the regularity in client response times, the trend and magnitude of traffic burstiness in multiple time scales, and user sensitivity to network conditions.

Acknowledgments

The guest editors of this special issue would like to thank all the authors for submitting their latest research works, and thank all the reviewers for their time and effort in suggesting improvements during successive iterations. They would like also to express their thankfulness to the publisher, its staff, and the Editor-in-Chief for their patience and helpful suggestions during the preparation of this issue. They hope that readers will find this collection of papers interesting, instructive, and inspiring for further research on applying signal processing methods to the problem of detecting network intrusions.

Chin-Tser Huang
Rocky K. C. Chang
Polly Huang