Network Traffic Anomaly Detection And Prevention

The State of the Art in Intrusion Prevention and Detection analyzes the latest trends and issues surrounding intrusion detection systems in computer networks, especially in communications networks. Its broad scope of coverage includes wired, wireless, and mobile networks; next-generation converged networks; and intrusion in social networks. Presenting cutting-edge research, the book presents novel schemes for intrusion detection and prevention. It discusses tracing back mobile attackers, secure routing with intrusion prevention, anomaly detection, and AI-based techniques. It also includes information on physical intrusion in wired and wireless networks and agent-based intrusion surveillance, detection, and prevention. The book contains 19 chapters written by experts from 12 different countries that provide a truly global perspective. The text begins by examining traffic analysis and management for intrusion detection systems. It explores honeypots, honeynets, network traffic analysis, and the basics of outlier detection. It talks about different kinds of IDSs for different infrastructures and considers new and emerging technologies such as smart grids, cyber physical systems, cloud computing, and hardware techniques for high performance intrusion detection. The book covers artificial intelligence-related intrusion detection techniques and explores intrusion tackling mechanisms for various wireless systems and networks, including wireless sensor networks, WiFi, and wireless automation systems. Containing some chapters written in a tutorial style, this book is an ideal reference for graduate students, professionals, and researchers working in the field of computer and network security.

Cybersecurity is a growing research area with direct commercial impact to organizations and companies in every industry. With all other technological advancements in the Internet of Things (IoT), mobile devices, cloud computing, 5G network, and artificial intelligence, the need for cybersecurity is more critical than ever before. These technologies drive the need for tighter cybersecurity implementations, while at the same time act as enablers to provide more advanced security solutions. This paper will discuss a framework that can predict cybersecurity risk by identifying normal network behavior and detect network traffic anomalies. Our research focuses on the analysis of the historical network traffic data to identify network usage trends and security vulnerabilities. Specifically, this thesis will focus on multiple components of the data analytics platform. It explores the big data platform architecture, and data ingestion, analysis, and engineering processes. The experiments were conducted utilizing various time series algorithms (Seasonal ETS, Seasonal ARIMA, TBATS, Double-Seasonal Holt-Winters, and Ensemble methods) and Long Short-Term Memory Recurrent Neural Network algorithm. Upon creating the baselines and forecasting network traffic trends, the anomaly detection algorithm was implemented using specific thresholds to detect network traffic trends that show significant variation from the baseline. Lastly, the network traffic data was analyzed and forecasted in various dimensions: total volume, source vs. destination volume, protocol, port, machine, geography, and network structure and pattern. The experiments were conducted with multiple approaches to get more insights into the network patterns and traffic trends to detect anomalies.

This book was prepared as the Final Publication of COST Action IC0703 "Data Traffic Monitoring and Analysis: theory, techniques, tools and applications for the future networks". It contains 14 chapters which demonstrate the results, quality,and the impact of European research in the field of TMA in line with the scientific objective of the Action. The book is structured into three parts: network and topology measurement and modelling, traffic classification and anomaly detection, quality of experience.

Unsupervised Network Anomaly Detection

First Euro-NF Workshop, FITraMEn 2008, Porto, Portugal, December 11-12, 2008, Revised Selected Papers

Exploring the Timeliness Requirement of Artificial Neural Networks in Network Traffic Anomaly Detection

Network Traffic Analysis

Machine Learning for Cyber Physical Systems

Concepts, Techniques, and Tools

This indispensable text/reference presents a comprehensive overview on the detection and prevention of anomalies in computer network traffic, from coverage of the fundamental theoretical concepts to in-depth analysis of systems and methods. Readers will benefit from invaluable practical guidance on how to design an intrusion detection technique and incorporate it into a system, as well as on how to analyze and correlate alerts without prior information. Topics and features: introduces the essentials of traffic management in high speed networks, detailing types of anomalies, network vulnerabilities, and a taxonomy of network attacks; describes a systematic approach to generating large network intrusion datasets, and reviews existing synthetic, benchmark, and real-life datasets; provides a detailed study of network anomaly detection techniques and systems under six different categories: statistical, classification, knowledge-base, cluster and outlier detection, soft computing, and combination learners; examines alert management and anomaly prevention techniques, including alert preprocessing, alert correlation, and alert post-processing; presents a hands-on approach to developing network traffic monitoring and analysis tools, together with a survey of existing tools; discusses various evaluation criteria and metrics, covering issues of accuracy, performance, completeness, timeliness, reliability, and quality; reviews open issues and challenges in network traffic anomaly detection and prevention. This informative work is ideal for graduate and advanced undergraduate students interested in network security and privacy, intrusion detection systems, and data mining in security. Researchers and practitioners specializing in network security will also find the book to be a useful reference.

Network Intrusion Detection and Prevention: Concepts and Techniques provides detailed and concise information on different types of attacks, theoretical foundation of attack detection approaches, implementation, data collection, evaluation, and intrusion response. Additionally, it provides an overview of some of the commercially/publicly available intrusion detection and response systems. On the topic of intrusion detection system it is impossible to include everything there is to say on all subjects. However, we have tried to cover the most important and common ones. Network Intrusion Detection and Prevention: Concepts and Techniques is designed for researchers and practitioners in industry. This book is suitable for advanced-level students in computer science as a reference book as well.

This book presents papers on various problems of dependability in computer systems and networks that were discussed at the 14th DepCoS-RELCOMEX conference, in Brunów, Poland, from 1st to 5th July 2019. Discussing new ideas, research results and developments in the design, implementation, maintenance and analysis of complex computer systems, it is of interest to researchers and practitioners who are dealing with dependability issues in such systems. Dependability analysis came as a response to new challenges in the evaluation of contemporary complex systems, which should be considered as systems of people – with their needs and behaviours –interacting with technical communication channels (such as mobile activities, iCloud, Internet of Everything) and online applications, often operating in hostile environments. The diversity of topics covered, illustrates the variety of methods used in this area, often with the help of the latest results in artificial and computational intelligence.

15th International Conference, WASA 2020, Qingdao, China, September 13–15, 2020, Proceedings, Part I

Concepts and Techniques

Network Traffic Characterization and Network Anomaly Detection

11th International Conference, KES 2007, Vietri sul Mare, Italy, September 12-14, 2007, Proceedings, Part I

Network Classification for Traffic Management

Network Traffic Anomaly Detection Using EMD and Hilbert-Huan Transform

This book constitutes the proceedings of the 14th International Symposium on Recent Advances in Intrusion Detection, RAID 2011, held in Menlo Park, CA, USA in September 2011. The 20 papers presented were carefully reviewed and selected from 87 submissions. The papers are organized in topical sections on application security; malware; anomaly detection; Web security and social networks; and sandboxing and embedded environments.

5th International Conference on Communication and Electronics Systems (ICCES 2020) is being organized on 10 12, June 2020 ICCES will provide an outstanding international forum for sharing knowledge and results in all fields of Engineering and Technology ICCES provides quality key experts who provide an opportunity in bringing up innovative ideas Recent updates in the in the field of technology will be a platform for the upcoming researchers The conference will be Complete, Concise, Clear and Cohesive in terms of research related to Communication and Electronics systems

The two-volume set LNCS 12385 + 12386 constitutes the proceedings of the 15th International Conference on Wireless Algorithms, Systems, and Applications, WASA 2020, which was held during September 13-15, 2020. The conference was planned to take place in Qingdao, China; due to the COVID-19 pandemic it was held virtually. The 67 full and 14 short papers presented in these proceedings were carefully reviewed and selected from 216 submissions. These submissions cover many hot research topics, including machine-learning algorithms for wireless systems and applications, Internet of Things (IoTs) and related wireless solutions, wireless networking for cyber-physical systems (CPSs), security and privacy solutions for wireless applications, blockchain solutions for mobile applications, mobile edge computing, wireless sensor networks, distributed and localized algorithm design and analysis, wireless crowdsourcing, mobile cloud computing, vehicular networks, wireless solutions for smart cities, wireless algorithms for smart grids, mobile social networks, mobile system security, storage systems for mobile applications, etc.

A Machine Learning Perspective

Proceedings of the Ninth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX. June 30 – July 4, 2014, Brunów, Poland

Knowledge-Based Intelligent Information and Engineering Systems

The State of the Art in Intrusion Prevention and Detection

Real-time Analysis of Aggregate Network Traffic for Anomaly Detection

Recent Advances in Intrusion Detection

The work presents new approaches to Machine Learning for Cyber Physical Systems, experiences and visions. It contains some selected papers from the international Conference ML4CPS – Machine Learning for Cyber Physical Systems, which was held in Karlsruhe, September 29th, 2016. Cyber Physical Systems are characterized by their ability to adapt and to learn: They analyze their environment and, based on observations, they learn patterns, correlations and predictive models. Typical applications are condition monitoring, predictive maintenance, image processing and diagnosis. Machine Learning is the key technology for these developments.

Anomaly detection has become a vital component of any network in today's Internet. Ranging from non-malicious unexpected events such as flash-crowds and failures, to network attacks such as denials-of-service and network scans, network traffic anomalies can have serious detrimental effects on the performance and integrity of the network. The continuous arising of new anomalies and attacks create a continuous challenge to cope with events that put the network integrity at risk. Moreover, the inner polymorphic nature of traffic caused, among other things, by a highly changing protocol landscape, complicates anomaly detection system's task. In fact, most network anomaly detection systems proposed so far employ knowledge-dependent techniques, using either misuse detection signature-based detection methods or anomaly detection relying on supervised-learning techniques. However, both approaches present major limitations: the former fails to detect and characterize unknown anomalies (letting the network unprotected for long periods) and the latter requires training over labeled normal traffic, which is a difficult and expensive stage that need to be updated on a regular basis to follow network traffic evolution. Such limitations impose a serious bottleneck to the previously presented problem.We introduce an unsupervised approach to detect and characterize network anomalies, without relying on signatures, statistical training, or labeled traffic, which represents a significant step towards the autonomy of networks. Unsupervised detection is accomplished by means of robust data-clustering techniques, combining Sub-Space clustering with Evidence Accumulation or Inter-Clustering Results Association, to blindly identify anomalies in traffic flows. Correlating the results of several unsupervised detections is also performed to improve detection robustness. The correlation results are further used along other anomaly characteristics to build an anomaly hierarchy in terms of dangerousness. Characterization is then achieved by building efficient filtering rules to describe a detected anomaly. The detection and characterization performances and sensitivities to parameters are evaluated over a substantial subset of the MAWI repository which contains real network traffic traces.Our work shows that unsupervised learning techniques allow anomaly detection systems to isolate anomalous traffic without any previous knowledge. We think that this contribution constitutes a great step towards autonomous network anomaly detection.This PhD thesis has been funded through the ECODE project by the European Commission under the Framework Programme 7. The goal of this project is to develop, implement, and validate experimentally a cognitive routing system that meet the challenges experienced by the Internet in terms of manageability and security, availability and accountability, as well as routing system scalability and quality. The concerned use case inside the ECODE project is network anomaly.

With the rapid rise in the ubiquity and sophistication of Internet technology and the accompanying growth in the number of network attacks, network intrusion detection has become increasingly important. Anomaly-based network intrusion detection refers to finding exceptional or nonconforming patterns in network traffic data compared to normal behavior. Finding these anomalies has extensive applications in areas such as cyber security, credit card and insurance fraud detection, and military surveillance for enemy activities. Network Anomaly Detection: A Machine Learning Perspective presents machine learning techniques in depth to help you more effectively detect and counter network intrusion. In this book, you'll learn about: Network anomalies and vulnerabilities at various layers The pros and cons of various machine learning techniques and algorithms A taxonomy of attacks based on their characteristics and behavior Feature selection algorithms How to assess the accuracy, performance, completeness, timeliness, stability, interoperability, reliability, and other dynamic aspects of a network anomaly detection system Practical tools for launching attacks, capturing packet or flow traffic, extracting features, detecting attacks, and evaluating detection performance Important unresolved issues and research challenges that need to be overcome to provide better protection for networks Examining numerous attacks in detail, the authors look at the tools that intruders use and show how to use this knowledge to protect networks. The book also provides material for hands-on development, so that you can code on a testbed to implement detection methods toward the development of your own intrusion detection system. It offers a thorough introduction to the state of the art in network anomaly detection using machine learning approaches and systems.

Security in Smart Cities: Models, Applications, and Challenges

Cyber Security Risk Analysis Framework

Automatic Network Traffic Anomaly Detection and Analysis Using Supervised Machine Learning Techniques

Combining Statistical and Spectral Analysis Techniques in Network Traffic Anomaly Detection

Network Anomaly Detection

Statistical Analysis of Network Traffic for Anomaly Detection and Quality of Service Provisioning

This textbook collects a series of research papers in the area of Image Processing and Communications which not only introduce a summary of current technology but also give an outlook of potential feature problems in this area. Image Processing and Communications have undergone an impressive development. Recent evolutions in this area have led to a pervasive spread in many areas of human life and have become such a critical component in contemporary science and technology. The book is divided into two parts. The first part contains recent research results in image processing, whilst the second part contains recent research results in communications.

Network-wide traffic analysis and monitoring in large-scale networks is a challenging and expensive task. In this thesis work we have proposed to analyze the traffic of a large-scale IP network from aggregated traffic measurements, reducing measurement overheads and simplifying implementation issues. We have provided contributions in three different networking fields related to network-wide traffic analysis and monitoring in large-scale IP networks. The first contribution regards Traffic Matrix (TM) modeling and estimation, where we have proposed new statistical models and new estimation methods to analyze the Origin-Destination (OD) flows of a large-scale TM from easily available link traffic measurements. The second contribution regards the detection and localization of volume anomalies in the TM, where we have introduced novel methods with solid optimality properties that outperform current well-known techniques for network-wide anomaly detection proposed so far in the literature. The last contribution regards the optimization of the routing configuration in large-scale IP networks, particularly when the traffic is highly variable and difficult to predict. Using the notions of Robust Routing Optimization we have proposed new approaches for Quality of Service provisioning under highly variable and uncertain traffic scenarios. In order to provide strong evidence on the relevance of our contributions, all the methods proposed in this thesis work were validated using real traffic data from different operational networks. Additionally, their performance was compared against well-known works in each field, showing outperforming results in most cases. Taking together the ensemble of developed TM models, the optimal network-wide anomaly detection and localization methods, and the routing optimization algorithms, this thesis work offers a complete solution for network operators to efficiently monitor large-scale IP networks from aggregated traffic measurements and to provide accurate QoS-based performance, even in the event of volume traffic anomalies.

The frequent and large-scale network attacks have led to an increased need for developing techniques for analyzing network traffic. If efficient analysis tools were available, it could become possible to detect the attacks, anomalies and to appropriately take action to contain the attacks before they have had time to propagate across the network. In this dissertation, we suggest a technique for traffic anomaly detection based on analyzing the correlation of destination IP addresses and distribution of image-based signal in postmortem and real-time, by passively monitoring packet headers of traffic. This address correlation data are transformed using discrete wavelet transform for effective detection of anomalies through statistical analysis. Results from trace-driven evaluation suggest that the proposed approach could provide an effective means of detecting anomalies close to the source. We present a multidimensional indicator using the correlation of port numbers as a means of detecting anomalies. We also present a network measurement approach that can simultaneously detect, identify and visualize attacks and anomalous traffic in real-time. We propose to represent samples of network packet header data as frames or images. With such a formulation, a series of samples can be seen as a sequence of frames or video. This enables techniques from image processing and video compression such as DCT to be applied to the packet header data to reveal interesting properties of traffic. We show that "scene change analysis" can reveal sudden changes in traffic behavior or anomalies. We show that "motion prediction" techniques can be employed to understand the patterns of some of the attacks. We show that it may be feasible to represent multiple pieces of data as different colors of an image enabling a uniform treatment of multidimensional packet header data. Measurement-based techniques for analyzing network traffic treat traffic volume and traffic header data as signals or images in order to make the analysis feasible. In this dissertation, we propose an approach based on the classical Neyman-Pearson Test employed in signal detection theory to evaluate these different strategies. We use both of analytical models and trace-driven experiments for comparing the performance of different strategies. Our evaluations on real traces reveal differences in the effectiveness of different traffic header data as potential signals for traffic analysis in terms of their detection rates and false alarm rates. Our results show that address distributions and number of flows are better signals than traffic volume for anomaly detection. Our results also show that sometimes statistical techniques can be more effective than the NP-test when the attack patterns change over time.

Advances in Fuzzy Logic and Technology 2017

Network Traffic Anomaly Detection and Evaluation

Anomaly Detection as a Service

Image Processing and Communications Challenges 4

Wireless Algorithms, Systems, and Applications

Network Intrusion Detection and Prevention

This authored book investigates network traffic classification solutions by proposing transport-layer methods to achieve better run and operated enterprise-scale networks.

This volume constitutes the proceedings of two collocated international conferences: EUSFLAT-2017 – the 10th edition of the flagship Conference of the European Society for Fuzzy Logic and Technology held in Warsaw, Poland, on September 11–15, 2017, and IWIFSGN–2017 – The Sixteenth International Workshop on Intuitionistic Fuzzy Sets and Generalized Nets, held in Warsaw on September 13–15, 2017. The conferences were organized by the Systems Research Institute, Polish Academy of Sciences, Department IV of Engineering Sciences, Polish Academy of Sciences, and the Polish Operational and Systems Research Society in collaboration with the European Society for Fuzzy Logic and Technology (EUSFLAT), the Bulgarian Academy of Sciences and various European universities. The aim of the EUSFLAT-2017 was to bring together theoreticians and practitioners working on fuzzy logic, fuzzy systems, soft computing and related areas and to provide a platform for exchanging ideas and discussing the l atest trends and ideas, while the aim of IWIFSGN–2017 was to discuss new developments in extensions of the concept of a fuzzy set, such as an intuitionistic fuzzy set, as well as other concepts, like that of a generalized net. The papers included, written by leading international experts, as well as the special sessions and panel discussions contribute to the development the field, strengthen collaborations and intensify networking.

Anomaly detection has been a long-standing security approach with versatile applications, ranging from securing server programs in critical environments, to detecting insider threats in enterprises, to anti-abuse detection for online social networks. Despite the seemingly diverse application domains, anomaly detection solutions share similar technical challenges, such as how to accurately recognize various normal patterns, how to reduce false alarms, how to adapt to concept drifts, and how to minimize performance impact. They also share similar detection approaches and evaluation methods, such as feature extraction, dimension reduction, and experimental evaluation. The main purpose of this book is to help advance the real-world adoption and deployment anomaly detection technologies, by systematizing the body of existing knowledge on anomaly detection. This book is focused on data-driven anomaly detection for software, systems, and networks against advanced exploits and attacks, but also touches on a number of applications, including fraud detection and insider threats. We explain the key technical components in anomaly detection workflows, give in-depth description of the state-of-the-art data-driven anomaly-based security solutions, and more importantly, point out promising new research directions. This book emphasizes on the need and challenges for deploying service-oriented anomaly detection in practice, where clients can outsource the detection to dedicated security providers and enjoy the protection without tending to the intricate details.

Anomaly Detection in Network Traffic

7th International Symposium, RAID 2004, Sophia Antipolis, France, September 15-17, 2004, Proceedings

Traffic Anomaly Detection

Selected papers from the International Conference ML4CPS 2016

From Measurement, Classification, and Anomaly Detection to Quality of Experience

A New Approach to Network Traffic Anomaly Detection

This post proeedings volume contains a selection of research contributions presented at FITraMEn 2008, held during December 11-12, 2008 in Porto, Portugal. The papers contained in this book provide a general view of the ongoing research on traffic management and traffic engineering in the Euro-NF Network of Excellence, and give a representative example of the problems currently investigated in this area, that spans topics such as bandwidth allocation and traffic control, statistical analysis, traffic engineering, and optical networks and video communications.

This book offers an essential guide to IoT Security, Smart Cities, IoT Applications, etc. In addition, it presents a structured introduction to the subject of destination marketing and an exhaustive review on the challenges of information security in smart and intelligent applications, especially for IoT and big data contexts. Highlighting the latest research on security in smart cities, it addresses essential models, applications, and challenges. Written in plain and straightforward language, the book offers a self-contained resource for readers with no prior

background in the field. Primarily intended for students in Information Security and IoT applications (including smart cities systems and data heterogeneity), it will also greatly benefit academic researchers, IT professionals, policymakers and legislators. It is well suited as a reference book for both undergraduate and graduate courses on information security approaches, the Internet of Things, and real-world intelligent applications.

With the rapid rise in the ubiquity and sophistication of Internet technology and the accompanying growth in the number of network attacks, network intrusion detection has become increasingly important. Anomaly-based network intrusion detection refers to finding exceptional or nonconforming patterns in network traffic data compared to normal behavior. Finding these anomalies has extensive applications in areas such as cyber security, credit card and insurance fraud detection, and military surveillance for enemy activities. Network Anomaly Detection: A Machine Learning Perspective presents machine learning techniques in depth to help you more effectively detect and counter network intrusion. In this book, you'll learn about: Network anomalies and vulnerabilities at various layers The pros and cons of various machine learning techniques and algorithms A taxonomy of attacks based on their characteristics and behavior Feature selection algorithms How to assess the accuracy, performance, completeness, timeliness, stability, interoperability, reliability, and other dynamic aspects of a network anomaly detection system Practical tools for launching attacks, capturing packet or flow traffic, extracting features, detecting attacks, and evaluating detection performance Important unresolved issues and research challenges that need to be overcome to provide better protection for networks Examining numerous attacks in detail, the authors look at the tools that intruders use and show how to use this knowledge to protect networks. The book also provides material for hands-on development, so that you can code on a testbed to implement detection methods toward the development of your own intrusion detection system. It offers a thorough introduction to the state of the art in network anomaly detection using machine learning approaches and systems.

Traffic Anomaly Detection and Diagnosis on the Network Flow Level

Proceedings of the Fourteenth International Conference on Dependability of Computer Systems DepCoS-RELCOMEX, July 1-5, 2019, Brunów, Poland

14th International Symposium, RAID 2011, Menlo Park, CA, USA, September 20-21, 2011, Proceedings

Proceedings of: EUSFLAT- 2017 - The 10th Conference of the European Society for Fuzzy Logic and Technology, September 11-15, 2017, Warsaw, Poland IWIFSGN'2017 - The Sixteenth International Workshop on Intuitionistic Fuzzy Sets and Generalized Nets, September 13-15, 2017, Warsaw, Poland, Volume 2

Anomaly Detection, Feature Selection, Clustering and Classification

Challenges, Advances, and Opportunities

With the growing number of attacks and malicious threats on the Internet services and network infrastructures, the need for techniques to identity and detect attacks is increasing. Therefore, using machine learning techniques along traditional security mechanisms such as firewall and cryptography, can improve the performance of intrusion detection systems (IDSs). Network anomaly detection has become a very important area for both industrial application and academic research in the recent years. It is involved widely in a broad spectrum of domains and many research areas. Detection anomalies (attacks are detected as anomalies) in data is a crucial problem to diverse real-world applications. The goal of anomaly detection is to identify anomalous behavior, events based on deviations from expected normal usage. Hidden Markov Models (HMM) have been applied to anomaly detection since 1996. The previous researches applying HMM were limited to small data sets. In our work, we have used the term anomaly detection to describe the process of differentiating abnormal behavior from normal behavior on datasets available in this study. In this dissertation, we describe our research contributions for detecting anomalous patterns in network traffic data using HMM. We built HMM correlates the observation sequences and state transitions to predict the most probable intrusion state sequences that are capable of reducing false positive rate.

This book presents an overview of traffic anomaly detection analysis, allowing you to monitor security aspects of multimedia services. The author's approach is based on the analysis of time aggregation adjacent periods of the traffic. As traffic varies throughout the day, it is essential to consider the concrete traffic period in which the anomaly occurs. This book presents the algorithms proposed specifically for this analysis and an empirical comparative analysis of those methods and settle a new information theory based technique, named "typical day analysis". A new information-theory based technique for traffic anomaly detection (typical day analysis) Introductory chapters to anomaly detection methods including control charts, tests of goodness-of-fit Mutual Information Contains comparative analysis of traffic anomaly detection methods

This book constitutes the refereed proceedings of the 7th International Symposium on Recent Advances in Intrusion Detection, RAID 2004, held in Sophia Antipolis, France, in September 2004. The 16 revised full papers presented were carefully reviewed and selected from 118 submissions. The papers are organized in topical sections on modelling process behavior, detecting worms and viruses, attack and alert analysis, practical experience, anomaly detection, and formal analysis for intrusion detection.

Network Traffic Anomaly Detection Using Modified Hidden Markov Model

Network Traffic Anomaly Detection and Prevention

Network Traffic Anomaly Detection

New Methods for Network Traffic Anomaly Detection

Traffic Management and Traffic Engineering for the Future Internet

Engineering in Dependability of Computer Systems and Networks

A worldwide Internet usage growth rate of 380% larger than the period from 2000, the year of the dot-com bubble burst, until present indicates that Internet technology has become a foundation of our daily life. In the same period, cyber-crime has seen an incredible that makes sophisticated protection device for computers and networks an absolute necessity. Firewalls as the major defense of the last decade do not give sufficient protection anymore. This fact has given rise to the expansion of intrusion detection and prevention systems. Traditional intrusion detection systems are hasty in the sense that they use a s signatures, which raise at the same rate as new technique are discovered, to identify malicious traffic patterns. Anomaly detection systems are another branch of intrusion detection systems that act more proactively. They get a model of the normal system performance and issue alerts whenever the behavior changes; making an appropriate assumption that such changes are frequently caused by malicious or disruptive events. Anomaly detection has been a ground of exhaustive research over the last years as it poses several challenging problems.

DepCoS – RELCOMEX is an annual series of conferences organized by Wroc?aw University of Technology to promote a comprehensive approach to evaluation of system performability which is now commonly called dependability. In contrast to classic analyses which were concentrated on reliability of technical resources and structures built from them, dependability is based on multi-disciplinary approach to theory, technology and maintenance of a system considered to be a multifaceted amalgamation of technical, information, organization, software and human (users, administrators, supervisors, etc.) resources. Diversity of processes being realized (data processing, system management, system monitoring, etc.), their concurrency and their reliance on in-system intelligence often severely impedes construction of strict mathematical models and calls for application of intelligent and soft computing methods. This book presents the proceedings of the Ninth International Conference on Dependability and Complex Systems DepCoS-RELCOMEX, which took place in Brunów Palace, Poland, from 30th June to 4th July, 2014. The articles selected for this volume illustrate the variety of topics that must be included in system dependability analysis: tools, methodologies and standards for modelling, design and simulation of the systems, security and confidentiality in information processing, specific issues of heterogeneous, today often wireless, computer networks or management of transportation networks.

This book is part of a three-volume set that constitutes the refereed proceedings of the 11th International Conference on Knowledge-Based Intelligent Information and Engineering Systems, KES 2007. Coverage in this first volume includes artificial neural networks and connectionists systems, fuzzy and neuro-fuzzy systems, evolutionary computation, machine learning and classical AI, agent systems, and information engineering and applications in ubiquitous computing environments.

Data Traffic Monitoring and Analysis

Anomaly Detection and Some Implications of Neutrality

2020 5th International Conference on Communication and Electronics Systems (ICCES)

A Statistical Approach ; Flood and Flash Crowd Anomaly in Network Traffic

Sampling Network Traffic for Anomaly Detection

Visualizing Network Traffic as Images for Network Anomaly Detection

Today, internet has become an important tool for the entire public. It is the source of information, education, entertainment, and convenience. To maintain the efficiency and performance of the large computer networks supporting the internet, it is important to monitor and analyze the overall network traffic. During evening hours, when most people access internet at the same time for social media browsing, accessing their data or watching Netflix, with the increase in utilization, the network traffic can become congested and therefore the speed decreases. This research aims to identify network variables that cause these disturbances, thus impacting the overall speed of the network and leading it to a state of "congestive collapse". Machine learning models can be built using data passively collected in the network's logs and can be used in real-time to predict the traffic in the next time frame so network administrators could tune the network variables that are causing these disturbances. The models proposed here are able to quickly detect large intervals of low performing network transfers, which requires attention from network engineers.