Network Anomaly Detection A Machine Learning Perspective

The scope of conference papers and exhibits including but not limited to the following area related to ELECTRONICS AND COMMUNICATION ENGG, ELECTRICAL ENGINEERING , INFORMATION TECHNOLOGY COMPUTER ENGINEERING WIRELESS NETWORKING COMPUTATIONAL INTELLIGENCE ADVANCED COMPUTING ELECTRONICS AND INTERDISCIPLINARY DATA COMMUNICATION AND NETWORKING RENEWABLE AND SUSTAINABLE ENERGY POWER ENGINEERING AND CONTROL SYSTEM SIGNAL AND IMAGE PROCESSING COMMUNICATION SYSTEM BIOMEDICAL ENGINEERING DESIGN, MATERIALS AND MANUFACTURING FLEET TECHNOLOGIES ADVANCES IN CIVIL AND ENVIRONMENTAL ENGINEERING SPECIAL CALL FOR PAPERS CONVERGENCE IN TECHNOLOGY

Data networking now plays a major role in everyday life and new applications continue to appear at a blinding pace. Yet we still do not have a sound foundation for designing, evaluating and managing these networks. This book covers topics at the intersection of algorithms and networking. It builds a complete picture of the current state of research on Next Generation Networks and the challenges for the years ahead. Particular focus is given to evolving research initiatives and the architecture they propose and implications for networking. Topics: Network design and provisioning, hardware issues, layer-3 algorithms and MPLS, BGP and Inter AS routing, packet processing for routing, security and network management, load balancing, oblivious routing and stochastic algorithms, network coding for multicast, overlay routing for P2P networking and content delivery. This timely volume will be of interest to a broad readership from graduate students to researchers looking to survey recent research its open questions.

This book is concerned with the automatic detection of unknown attacks in network communication. Based on concepts of machine learning, a framework for self-learning intrusion detection is proposed which enables accurate and efficient identification of attacks in the application layer of network communication. The book is a doctoral thesis and targets researchers and postgraduate students in the area of computer security and machine learning.

This volume constitutes the thoroughly refereed post-conference proceedings of the 11th International Conference on Security and Privacy in Communication Networks, SecureComm 2015, held in Dallas, TX, USA, in October 2015. The 29 regular and 10 poster papers presented were carefully reviewed and selected from 107 submissions. It also presents 9 papers accepted of the workshop on Applications and Techniques in Cyber Security, ATCS 2015. The papers are grouped in the following topics: mobile, system, and software security; cloud security; privacy and side channels; Web and network security; crypto, protocol, and model.

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.

Applications of AI, computer security, computer networking, ICT4D

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.

Finding Data Anomalies You Didn't Know to Look For Anomaly detection is the detective work of machine learning: finding the unusual, catching the fraud, discovering strange activity in large and complex datasets. But, unlike Sherlock Holmes, you may not know what the puzzle is, much less what “suspects” you’re looking for. This O’Reilly report uses practical examples to explain how the underlying concepts of anomaly detection work. From banking security to natural sciences, medicine, and marketing, anomaly detection has many useful applications in this age of big data. And the search for anomalies will intensify once the Internet of Things spawns even more new types of data. The concepts described in this report will help you tackle anomaly detection in your own project. Use probabilistic models to predict what’s normal and contrast that to what you observe Set an adaptive threshold to determine which data falls outside of the normal range, using the t-digest algorithm Establish normal fluctuations in complex systems and signals (such as an EKG) with a more adaptive probablistic model Use historical data to discover anomalies in sporadic event streams, such as web traffic Learn how to use deviations in expected behavior to trigger fraud alerts

This book constitutes the refereed proceedings of the 5th European Workshop on Wireless Sensor Networks, EWSN 2008, held in Bologna, Italy, in January/February 2008. The 23 revised full papers presented were carefully reviewed and selected from 110 submissions. The papers are organized in topical sections on localization, detection of space/time correlated events, network coding, ZigBee, topology, software, as well as deployment and application development.

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.

The development of computer science is now so rapid that we, the readers, in-creasingly receive technology news about new solutions and applications which very often straddle the border between the real and the virtual worlds. Computer science is also the area in which cognitive science is witnessing a renaissance, be-cause its combination with technical sciences has given birth to a broad scientific discipline called cognitive informatics. And it is this discipline which has become the main theme of this monograph, which is also to serve as a kind of guide to cognitive informatics problems. This book is the result of work on systems for the cognitive analysis and inter-pretation of various data. The purpose of such an analytical approach is to show that for an in-depth analysis of data, the layers of semantics contained in these sets must be taken into account. The interdisciplinary nature of the solutions proposed means that the subject of cognitive systems forming part of cognitive informatics becomes a new challenge for the research and application work carried out. The authors of this monograph hope that it will guide Readers on an interesting and accurate journey through the intricacies of information and cognitive science.

Security Analytics for the Internet of Everything compiles the latest trends, technologies, and applications in this emerging field. It includes chapters covering emerging security trends, cyber governance, artificial intelligence in cybersecurity, and cyber challenges. Contributions from leading international experts are included. The target audience for the book is graduate students, professionals, and researchers working in the fields of cybersecurity, computer networks, communications, and the Internet of Everything (IoE). The book also includes some chapters written in a tutorial style so that general readers can easily grasp some of the ideas.

This book contains the best papers of the 10th International Conference on Enterprise Information Systems (ICEIS 2008), held in the city of Barcelona (Spain), organized by the Institute for Systems and Technologies of Information, Control and Com- nication (INSTICC) in cooperation with AAAI and co-sponsored by WfMC. ICEIS has become a major point of contact between research scientists, engineers and practitioners in the area of business applications of information systems. This year, five simultaneous tracks were held, covering different aspects related to enterprise computing, including: “Databases and Information Systems Integration,” “Artificial Intelligence and Decision Support Systems,” “Information Systems Analysis and Specification,” “Software Agents and Internet Computing” and “Human–Computer Interaction.” All tracks focused on real-world applications and highlighted the benefits of information systems and technology for industry and services, thus making a bridge between academia and enterprise. Following the success of 2007, ICEIS 2008 received 665 paper submissions from more than 40 countries. In all, 62 papers were published and presented as full papers, i.e., completed work (8 pages in proceedings / 30-min oral presentations), and 183 papers, reflecting work-in-progress or position papers, were accepted for short pr- entation and another 161 for poster presentation.

This book reports on advanced theories and methods in two related engineering fields: electrical and electronic engineering, and communications engineering and computing. It highlights areas of global and growing importance, such as renewable energy, power systems, mobile communications, security and the Internet of Things (IoT). The contributions cover a number of current research issues, including smart grids, photovoltaic systems, wireless power transfer, signal processing, 4G and 5G technologies, IoT applications, mobile cloud computing and many more. Based on the proceedings of the Second International Conference on Emerging Trends in Electrical, Electronic and Communications Engineering (ELECOM 2018), held in Mauritius from November 28 to 30, 2018, the book provides graduate students, researchers and professionals with a snapshot of the state-of-the-art and a source of new ideas for future research and collaborations.

This book discusses a variety of methods for outlier ensembles and organizes them by the specific principles with which accuracy improvements are achieved. In addition, it covers the techniques with which such methods can be made more effective. A formal classification of these methods is provided, and the circumstances in which they work well are examined. The authors cover how outlier ensembles relate (both theoretically and practically) to the ensemble techniques used commonly for other data mining problems like classification. The similarities and (subtle) differences in the ensemble techniques for the classification and outlier detection problems are explored. These subtle differences do impact the design of ensemble algorithms for the latter problem. This book can be used for courses in data mining and related curricula. Many illustrative examples and exercises are provided in order to facilitate classroom teaching. A familiarity is assumed to the outlier detection problem and also to generic problem of ensemble analysis in classification. This is because many of the ensemble methods discussed in this book are adaptations from their counterparts in the classification domain. Some techniques explained in this book, such as wagging, randomized feature weighting, and geometric subsampling, provide new insights that are not available elsewhere. Also included is an analysis of the performance of various types of base detectors and their relative effectiveness. The book is valuable for researchers and practitioners for leveraging ensemble methods into optimal algorithmic design.

The two-volume set LNCS 6640 and 6641 constitutes the refereed proceedings of the 10th International IFIP TC 6 Networking Conference held in Valencia, Spain, in May 2011. The 64 revised full papers presented were carefully reviewed and selected from a total of 294 submissions. The papers feature innovative research in the areas of applications and services, next generation Internet, wireless and sensor networks, and network science. The first volume includes 36 papers and is organized in topical sections on anomaly detection, content management, DTN and sensor networks, energy efficiency, mobility modeling, network science, network topology configuration, next generation Internet, and path diversity.

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.

Utilize this easy-to-follow beginner's guide to understand how deep learning can be applied to the task of anomaly detection. Using Keras and PyTorch in Python, the book focuses on how various deep learning models can be applied to semi-supervised and unsupervised anomaly detection tasks. This book begins with an explanation of what anomaly detection is, what it is used for, and its importance. After covering statistical and traditional machine learning methods for anomaly detection using Scikit-Learn in Python, the book then provides an introduction to deep learning with details on how to build and train a deep learning model in both Keras and PyTorch before shifting the focus to applications of the following deep learning models to anomaly detection: various types of Autoencoders, Restricted Boltzmann Machines, RNNs & LSTMs, and Temporal Convolutional Networks. The book explores unsupervised and semi-supervised anomaly detection along with the basics of time series-based anomaly detection. By the end of the book you will have a thorough understanding of the basic task of anomaly detection as well as an assortment of methods to approach anomaly detection, ranging from traditional methods to deep learning. Additionally, you are introduced to Scikit-Learn and are able to create deep learning models in Keras and PyTorch. What You Will Learn Understand what anomaly detection is and why it is important in today's world Become familiar with statistical and traditional machine learning approaches to anomaly detection using Scikit-Learn Know the basics of deep learning in Python using Keras and

PyTorch Be aware of basic data science concepts for measuring a model's performance: understand what AUC is, what precision and recall mean, and more Apply deep learning to semi-supervised and unsupervised anomaly detection Who This Book Is For Data scientists and machine learning engineers interested in learning the basics of deep learning applications in anomaly detection

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.

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.

This book introduces the latest research on advanced control charts and new machine learning approaches to detect abnormalities in the smart manufacturing process. By approaching anomaly detection using both statistics and machine learning, the book promotes interdisciplinary cooperation between the research communities, to jointly develop new anomaly detection approaches that are more suitable for the 4.0 Industrial Revolution. The book provides ready-to-use algorithms and parameter sheets, enabling readers to design advanced control charts and machine learning-based approaches for anomaly detection in manufacturing. Case studies are introduced in each chapter to help practitioners easily apply these tools to real-world manufacturing processes. The book is of interest to researchers, industrial experts, and postgraduate students in the fields of industrial engineering, automation, statistical learning, and manufacturing industries.

This book, drawing on recent literature, highlights several methodologies for the detection of outliers and explains how to apply them to solve several interesting real-life problems. The detection of objects that deviate from the norm in a data set is an essential task in data mining due to its significance in many contemporary applications. More specifically, the detection of fraud in e-commerce transactions and discovering anomalies in network data have become prominent tasks, given recent developments in the field of information and communication technologies and security. Accordingly, the book sheds light on specific state-of-the-art algorithmic approaches such as the community-based analysis of networks and characterization of temporal outliers present in dynamic networks. It offers a valuable resource for young researchers working in data mining, helping them understand the technical depth of the outlier detection problem and devise innovative solutions to address related challenges.

The growing presence of smart phones and smart devices has caused significant changes to wireless networks. With the ubiquity of these technologies, there is now increasingly more available data for mobile operators to utilize. Big Data Applications in the Telecommunications Industry is a comprehensive reference source for the latest scholarly material on the use of data analytics to study wireless networks and examines how these techniques can increase reliability and profitability, as well as network performance and connectivity. Featuring extensive coverage on relevant topics, such as accessibility, traffic data, and customer satisfaction, this publication is ideally designed for engineers, students, professionals, academics, and researchers seeking innovative perspectives on data science and wireless network communications.

COMMUNICATION NETWORKS AND SERVICE MANAGEMENT IN THE ERA OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING Discover the impact that new technologies are having on communication systems with this up-to-date and one-stop resource Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning delivers a comprehensive overview of the impact of artificial intelligence (AI) and machine learning (ML) on service and network management. Beginning with a fulsome description of ML and AI, the book moves on to discuss management models, architectures, and frameworks. The authors also explore how AI and ML can be used in service management functions like the generation of workload profiles, service provisioning, and more. The book includes a handpicked selection of applications and case studies, as well as a treatment of emerging technologies the authors predict could have a significant impact on network and service management in the future. Statistical analysis and data mining are also discussed, particularly with respect to how they allow for an improvement of the management and security of IT systems and networks. Readers will also enjoy topics like: A thorough introduction to network and service management, machine learning, and artificial intelligence An exploration of artificial intelligence and machine learning for management models, including autonomic management, policy-based management, intent based management, and network virtualization-based management Discussions of AI and ML for architectures and frameworks, including cloud systems, software defined networks, 5G and 6G networks, and Edge/Fog networks An examination of AI and ML for service management, including the automatic generation of workload profiles using unsupervised learning Perfect for information and communications technology educators, Communication Networks and Service Management in the Era of Artificial Intelligence and Machine Learning will also earn a place in the libraries of engineers and professionals who seek a structured reference on how the emergence of artificial intelligence and machine learning techniques is affecting service and network management.

In recent years, the need for smart equipment has increased exponentially with the upsurge in technological advances. To work to their fullest capacity, these devices need to be able to communicate with other devices in their network to exchange information and receive instructions. Computational Intelligence in the Internet of Things is an essential reference source that provides relevant theoretical frameworks and the latest empirical research findings in the area of computational intelligence and the Internet of Things. Featuring research on topics such as data analytics, machine learning, and neural networks, this book is ideally designed for IT specialists, managers, professionals, researchers, and academicians.

The intrusion detection in computer networks is a complex research problem, which requires the understanding of computer networks and the mechanism of intrusions, the configuration of sensors and the collected data, the selection of the relevant attributes, and the monitor algorithms for online detection. It is critical to develop general methods for

data dimension reduction, effective monitoring algorithms for intrusion detection, and means for their performance improvement. This dissertation is motivated by the timely need to develop statistics-based machine learning methods for effective detection of computer network anomalies. Three fundamental research issues related to data dimension reduction, control charts design and performance improvement have been addressed accordingly. The major research activities and corresponding contributions are summarized as follows:(1) Filter and Wrapper models are integrated to extract a small number of the informative attributes for computer network intrusion detection. A two-phase analyses method is proposed for the integration of Filter and Wrapper models. The proposed method has successfully reduced the original 41 attributes to 12 informative attributes while increasing the accuracy of the model. The comparison of the results in each phase shows the effectiveness of the proposed method.(2) Supervised kernel based control charts for anomaly intrusion detection. We propose to construct control charts in a feature space. The first contribution is the use of multi-objective Genetic Algorithm in the parameter pre-selection for SVM based control charts. The second contribution is the performance evaluation of supervised kernel based control charts.(3) Unsupervised kernel based control charts for anomaly intrusion detection. Two types of unsupervised kernel based control charts are investigated: Kernel PCA control charts and Support Vector Clustering based control charts. The applications of SVC based control charts on computer networks audit data are also discussed to demonstrate the effectiveness of the proposed method. Although the developed methodologies in this dissertation are demonstrated in the computer network intrusion detection applications, the methodologies are also expected to be applied to other complex system monitoring, where the database consists of a large dimensional data with non-Gaussian distribution.

In the era of Internet of Things (IoT), and with the explosive worldwide growth of electronic data volume and the associated needs of processing, analyzing, and storing this data, several new challenges have emerged. Particularly, there is a need for novel schemes of secure authentication, integrity protection, encryption, and non-repudiation to protect the privacy of sensitive data and to secure systems. Lightweight symmetric key cryptography and adaptive network security algorithms are in demand for mitigating these challenges. This book presents state-of-the-art research in the fields of cryptography and security in computing and communications. It covers a wide range of topics such as machine learning, intrusion detection, steganography, multi-factor authentication, and more. It is a valuable reference for researchers, engineers, practitioners, and graduate and doctoral students working in the fields of cryptography, network security, IoT, and machine learning.

This study presents the correlational paraconsistent machine (CPM), a tool for anomaly detection that incorporates unsupervised models for tra?c characterization and principles of paraconsistency, to inspect irregularities at the network tra?c ?ow level.

This book constitutes the refereed proceedings of the International Conference on Advances in Security of Information and Communication Networks, Sec Net 2013, held in Cairo, Egypt, in September 2013. The 21 revised full papers presented were carefully reviewed and selected from 62 submissions. The papers are organized in topical sections on networking security; data and information security; authentication and privacy; security applications.

Introduces the concept of intrusion detection, discusses various approaches for intrusion detection systems (IDS), and presents the architecture and implementation of IDS. This title also includes the performance comparison of various IDS via simulation.

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.

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.

The book focuses on both theory and applications in the broad areas of communication technology, computer science and information security. This two volume book contains the Proceedings of International Conference on Advanced Computing and Intelligent Engineering. These volumes bring together academic scientists, professors, research scholars and students to share and disseminate information on knowledge and scientific research works related to computing, networking, and informatics to discuss the practical challenges encountered and the solutions adopted. The book also promotes translation of basic research into applied investigation and convert applied investigation into practice.

Can machine learning techniques solve our computer security problems and finally put an end to the cat-and-mouse game between attackers and defenders? Or is this hope merely hype? Now you can dive into the science and answer this question for yourself! With this practical guide, you'll explore ways to apply machine learning to security issues such as intrusion detection, malware classification, and network analysis. Machine learning and security specialists Clarence Chio and David Freeman provide a framework for discussing the marriage of these two fields, as well as a toolkit of machine-learning algorithms that you can apply to an array of security problems. This book is ideal for security engineers and data scientists alike. Learn how machine learning has contributed to the success of modern spam filters Quickly detect anomalies, including breaches, fraud, and impending system failure Conduct malware analysis by extracting useful information from computer binaries Uncover attackers within the network by finding patterns inside datasets Examine how attackers exploit consumer-facing websites and app functionality Translate your machine learning algorithms from the lab to production Understand the threat attackers pose to machine learning solutions

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

Security of Information and Networks includes invited and contributed papers on information assurance, security, and public policy. It covers Ciphers, Mobile Agents, Access Control, Security Assurance, Intrusion Detection, and Security Software.

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.

The use of informatics and Internet of Things (IoT) is gradually and effectively blending into our lives Millions of terminals and devices seamlessly generate data and exchange information through heterogeneous IoT networks to monitor the surroundings and control specific functional modules The IoT technology is rapidly developing, and various techniques will be widely applied and further improved in the coming years The intelligence of an IoT application is mostly determined by the methods used for data processing and analysis in IoT systems The current mainstream research is related to techniques including big data, artificial intelligence (AI), and cloud computing