# Intrusion Detection In Computer Network Using Genetic





**ELAINE ALANI**

*The State of the Art in Intrusion Prevention and Detection* Springer Science & Business Media
This book constitutes the proceedings of the First International Conference on Intelligent Robotics and Manufacturing, IRAM 2012, held in Kuala Lumpur, Malaysia, in November 2012. The 64 revised full papers included in this volume were carefully reviewed and selected from 102 initial submissions. The papers are organized in topical sections named: mobile robots, intelligent autonomous systems, robot vision and robust, autonomous agents, micro, meso and nano-scale automation and assembly, flexible manufacturing systems, CIM and micro-machining, and fabrication techniques.

*Computer Network Intrusion Detection* Springer Science & Business Media
This book is a training aid and reference for intrusion detection analysts. While the authors refer to research and theory, they focus their attention on providing practical information. New to this edition is coverage of packet dissection, IP datagram fields, forensics, and snort filters.

*Intrusion Detection and Prevention for Mobile Ecosystems* Springer Science & Business Media
This book constitutes the refereed proceedings of the 11th Asia-Pacific Network Operations and Management Symposium, APNOMS 2008, held in Beijing, China, in October 2008. The 43 revised full papers and 34 revised short papers presented were carefully reviewed and selected from 195 submissions. The papers are organized in topical sections on routing and topology management; fault management; community and virtual group management; autonomous and distributed control; sensor network management; traffic identification; QoS management; policy and service management; wireless and mobile network management; security management; short papers.

Computer Networks, Big Data and IoT Elsevier
This book presents state-of-the-art research on intrusion detection using reinforcement learning, fuzzy and rough set theories, and genetic algorithm. Reinforcement learning is employed to incrementally learn the computer network behavior, while rough and fuzzy sets are

utilized to handle the uncertainty involved in the detection of traffic anomaly to secure data resources from possible attack. Genetic algorithms make it possible to optimally select the network traffic parameters to reduce the risk of network intrusion. The book is unique in terms of its content, organization, and writing style. Primarily intended for graduate electrical and computer engineering students, it is also useful for doctoral students pursuing research in intrusion detection and practitioners interested in network security and administration. The book covers a wide range of applications, from general computer security to server, network, and cloud security.

*Analysis of Machine Learning Techniques for Intrusion Detection System: A Review* New Riders Publishing

Security is a key issue to both computer and computer networks. Intrusion detection System (IDS) is one of the major research problems in network security. IDSs are developed to detect both known and unknown attacks. There are many techniques used in IDS for protecting computers and networks from network based and host based attacks. Various Machine learning techniques are used in IDS. This study analyzes machine learning techniques in IDS. It also reviews many related studies done in the period from 2000 to 2012 and it focuses on machine learning techniques. Related studies include single, hybrid, ensemble classifiers, baseline and datasets used.

Cisco Security Professional's Guide to Secure Intrusion Detection Systems Springer Science & Business Media

Details how intrusion detection works in network security with comparisons to traditional methods such as firewalls and cryptography Analyzes the challenges in interpreting and correlating Intrusion Detection alerts

Intrusion Detection Systems IGI Global

The menace of illegal access to data resources is a growing concern of researchers in the field of computer science. A significant amount of effort is required to monitor the activities in a computer network with a view to detect any attempt for intrusion. From this perspective, the main motivation behind this research is to design an efficient intrusion detection system using some novel data mining approaches that have the capability to detect intrusions with high detection rate with low false positive rate. In this work, we take multiple supports Apriori algorithm with various interestiness measures to obtain the most significant rules in detecting network intrusions. Further, we propose some novel ensemble of classifiers in order to enhance the detection rate of network attacks. Some unsupervised clustering algorithms have been proposed to further increase the detection rate of new or unseen attacks that fall under rare attacks categories. Finally, certain hybrid data mining approaches have been employed in order to design an efficient anomaly based network intrusion detection system that can achieve high detection rate and low false positive rate.

**2021 10th IEEE International Conference on Communication Systems and Network Technologies (CSNT)** Springer

Network and System Security provides focused coverage of network and system security technologies. It explores practical solutions to a wide range of network and systems security issues. Chapters are authored by leading experts in the field and address the immediate and long-term challenges in the authors' respective areas of expertise. Coverage includes building a secure organization, cryptography, system intrusion, UNIX and Linux security, Internet security, intranet security, LAN security; wireless network security, cellular network security, RFID security, and more. Chapters contributed by leaders in the field covering foundational and practical aspects of system and network security, providing a new level of technical expertise not found elsewhere Comprehensive and updated coverage of the subject area allows the reader to put current technologies to work Presents methods of analysis and problem solving techniques, enhancing the reader's grasp of the material and ability to implement practical solutions

**Challenges for Next Generation Network Operations and Service Management** World Scientific

At its core, information security deals with the secure and accurate transfer of information. While information security has long been important, it was, perhaps, brought more clearly into mainstream focus with the so-called "Y2K" issue. Te Y2K scare was the fear that c- puter networks and the systems that are controlled or operated by sofware would fail with the turn of the millennium, since their clocks could lose synchronization by not recognizing a number (instruction) with three zeros. A positive outcome of this scare was the creation of several Computer Emergency Response Teams (CERTs) around the world that now work - operatively to exchange expertise and information, and to coordinate in case major problems should arise in the modern IT environment. Te terrorist attacks of 11 September 2001 raised security concerns to a new level. Te - ternational community responded on at least two fronts; one front being the transfer of reliable information via secure networks and the other being the collection of information about - tential terrorists. As a sign of this new emphasis on security, since 2001, all major academic publishers have started technical journals focused on security, and every major communi- tions conference (for example, Globecom and ICC) has organized workshops and sessions on security issues. In addition, the IEEE has created a technical committee on Communication and Information Security. Te ?rst editor was intimately involved with security for the Athens Olympic Games of 2004.

Intrusion Detection Newnes

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.

Network Intrusion Detection and Prevention CRC Press
A typical problem that arises when deploying intrusion detection sensors is their affinities of producing high rate of false alerts. Thus, it needs huge analysis efforts and time consuming odd jobs at higher levels. In this study, we have investigated an approach to anomaly intrusion detection based on causal knowledge reasoning. The approach is anomaly-based and utilizes causal knowledge inference based fuzzy cognitive maps (FCM) and self organizing maps (SOM). A set of parallel neural network classifiers (SOM) are used to do an initial recognition of the network traffic flow to detect abnormal behaviors. The FCM is incorporated to eliminate ambiguities of odd neurons and making final decisions. Based on the domain knowledge of network data the SOM/FCM combination presents quantitative and qualitative matching correspondences which in turn reduce the number of suspicious neurons i.e. reduce the number of false alerts. This method works as a unique fuzzy clustering approach and we have demonstrated its performance using DARPA 1999 network traffic data set. The method has also the flexibility of features selection for further exploration.

**Trends in Intelligent Robotics, Automation, and Manufacturing** CRC Press
The ubiquity of modern technologies has allowed for increased connectivity between people and devices across the globe. This connected infrastructure of networks creates numerous opportunities for applications and uses. As the applications of the internet of things continue to progress so do the security concerns for this technology. The study of threat prevention in the internet of things is necessary as security breaches in this field can ruin industries and lives. Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications is a vital reference source that examines recent developments and emerging trends in security and privacy for the internet of things through new models, practical solutions, and technological advancements related to security. Highlighting a range of topics such as cloud security, threat detection, and open source software, this multi-volume book is ideally designed for engineers, IT consultants, ICT procurement managers, network system integrators, infrastructure service providers, researchers, academics, and professionals interested in current research on security practices pertaining to the internet of things.

**Threat Forecasting** Springer
To defend against computer and network attacks, multiple, complementary security devices such as intrusion detection systems (IDSs), and firewalls are widely deployed to monitor networks and hosts. These various IDSs will flag alerts when suspicious events are observed. This book is an edited volume by world class leaders within computer network and information security presented in an easy-to-follow style. It introduces defense alert systems against computer and network attacks. It also covers integrating intrusion alerts within security policy framework for intrusion response, related case studies and much more.

**Computer and Information Security Handbook** GRIN Verlag
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.

**Privacy, Intrusion Detection and Response: Technologies for Protecting Networks** Springer
Presenting cutting-edge research, Intrusion Detection in Wireless Ad-Hoc Networks explores the security aspects of the basic categories of wireless ad-hoc networks and related application areas. Focusing on intrusion detection systems (IDSs), it explains how to establish security solutions for the range of wireless networks, including mobile ad-hoc networks, hybrid wireless networks, and sensor networks. This edited volume reviews and analyzes state-of-the-art IDSs for various wireless ad-hoc networks. It includes case studies on honesty-based intrusion detection systems, cluster oriented-based intrusion detection systems, and trust-based intrusion detection systems. Addresses architecture and organization issues Examines the different types of routing attacks for WANs Explains how to ensure Quality of Service in secure routing Considers honesty and trust-based IDS solutions Explores emerging trends in WAN security Describes the blackhole attack detection technique Surveying existing trust-based solutions, the book explores the potential of the CORIDS algorithm to provide trust-based solutions for secure mobile applications. Touching on more advanced topics, including security for smart power grids, securing cloud services, and energy-efficient IDSs, this book provides you with the tools to design and build secure next-generation wireless networking environments.

*Network Intrusion Detection* Syngress
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.

*Intrusion Detection Networks* Pearson Education
This book covers the basic statistical and analytical techniques of computer intrusion detection. It is the first to present a data-centered approach to these problems. It begins with a description of the basics of TCP/IP, followed by chapters dealing with network traffic analysis, network monitoring for intrusion detection, host based intrusion detection, and computer viruses and other malicious code.

*Intrusion Detection* Springer Science & Business Media

The rapidly increasing sophistication of cyber intrusions makes them nearly impossible to detect without the use of a collaborative intrusion detection network (IDN). Using overlay networks that allow an intrusion detection system (IDS) to exchange information, IDNs can dramatically improve your overall intrusion detection accuracy. Intrusion Detection Networks: A Key to Collaborative Security focuses on the design of IDNs and explains how to leverage effective and efficient collaboration between participant IDSs. Providing a complete introduction to IDSs and IDNs, it explains the benefits of building IDNs, identifies the challenges underlying their design, and outlines possible solutions to these problems. It also reviews the full-range of proposed IDN solutions—analyzing their scope, topology, strengths, weaknesses, and limitations. Includes a case study that examines the applicability of collaborative intrusion detection to real-world malware detection scenarios Illustrates distributed IDN architecture design Considers trust management, intrusion detection decision making, resource management, and collaborator management The book provides a complete overview of network intrusions, including their potential damage and corresponding detection methods. Covering the range of existing IDN designs, it elaborates on privacy, malicious insiders, scalability, free-riders, collaboration incentives, and intrusion detection efficiency. It also provides a collection of problem solutions to key IDN design challenges and shows how you can use various theoretical tools in this context. The text outlines comprehensive validation methodologies and metrics to help you improve efficiency of detection, robustness against malicious insiders, incentive-compatibility for all participants, and scalability in network size. It concludes by highlighting open issues and future challenges.

**Handbook of Research on Intrusion Detection Systems** Springer Science & Business Media

Master's Thesis from the year 2013 in the subject Computer Science - IT-Security, grade: C, Lovely Professional University, Punjab (School Of Computer Science and Engineering), course: M.Tech(CSE), language: English, abstract: The rapid proliferation of Mobile ad hoc network has changed the landscape of network security. The recent DOS attacks on major Internet sites have shown us, no open computer network is immune from intrusions. The ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology and cooperative algorithms, lack of centralized monitoring and management point and lack of a clear line of defense. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective. There are many intrusion detection techniques have been developed on Ad hoc network but have been turned to be inapplicable in this new environment. Here we need to search for new architecture and mechanisms to protect Mobile Ad hoc network. In the above all technique of intrusion detection is applied on the only one layer and that is probably on routing layer. But here we apply this intrusion detection system in the MAC layer for the more security, efficiency and high speed compare to other technique those whose apply in the network layer.

*Intrusion Detection* Springer Science & Business Media

This book constitutes the proceedings of the 4th International Conference on Network Security and Applications held in Chennai, India, in July 2011. The 63 revised full papers presented were carefully reviewed and selected from numerous submissions. The papers address all technical and practical aspects of security and its applications for wired and wireless networks and are organized in topical sections on network security and applications, ad hoc, sensor and ubiquitous computing, as well as peer-to-peer networks and trust management.