International Journal of Enhanced Research in Management & Computer Applications
ISSN: 2319-7471, Vol. 6 Issue 7, July-2017, Impact Factor: 3.578

The Role of Artificial Intelligence in Automated Network Intrusion Detection

Zahoor Ahmad Malik[1], Kaisar Hussain Shah[2]

[1]Field Service Engineer, Reliance Jio Infocom Limited, India
[2]Research Scholar, Sri Satya Sai University, Of Technology and Medical Sciences, Sehore, MP

ABSTRACT

This research paper explores the significant role of artificial intelligence (AI) in the field of automated network intrusion detection. With the increasing prevalence of cyber attacks and the ever-evolving tactics employed by hackers, traditional network intrusion detection systems (NIDS) have struggled to keep up with the growing threat landscape. The paper discusses the limitations of conventional NIDS approaches, such as rule-based systems and signature-based detection, and highlights the need for more sophisticated and efficient solutions. It delves into the various AI techniques employed in NIDS, including machine learning, deep learning, reinforcement learning, and genetic algorithms, highlighting their advantages and limitations. The paper also provides case studies that demonstrate the practical application of AI in detecting and preventing attacks, such as denial-of-service attacks and anomaly detection in network traffic. Additionally, it explores emerging trends and future prospects, such as the integration of AI with big data analytics and the challenges associated with security and privacy in AI-driven NIDS. Overall, this research paper aims to shed light on the vital role of artificial intelligence in enhancing automated network intrusion detection. By utilizing AI techniques, NIDS can achieve enhanced detection accuracy, real-time and adaptive response capabilities, and reduced false positive rates, thereby enabling organizations to better defend against evolving cyber threats. However, it is important to acknowledge the limitations and challenges associated with AI in NIDS, such as explainability and security concerns. Future research should focus on addressing these limitations and exploring innovative approaches to further improve the effectiveness of AI-driven NIDS solutions.

Key Words: Artificial Intelligence, Network Intrusion Detection Systems, Reinforcement Learning, Genetic Algorithms, Hybrid Approaches

INTRODUCTION

Artificial intelligence (AI) has become an integral part of various fields, and its potential for enhancing network security has gained significant attention. In the realm of automated network intrusion detection, AI offers a promising solution to combat the ever-evolving tactics employed by cybercriminals. This research paper delves into the role of AI in automated network intrusion detection systems (NIDS), emphasizing the need for more sophisticated approaches to protect against sophisticated threats. The rapid growth of the internet and the increasing reliance on digital infrastructure have heightened the risk of network intrusions and cyber attacks. Traditional network intrusion detection systems often rely on rule-based mechanisms and signature-based detection techniques, which are limited in their ability to keep up with constantly evolving attack patterns. As attackers become more sophisticated and employ advanced techniques, such as polymorphic malware and zero-day exploits, it is essential to explore alternative solutions that can effectively detect and mitigate network intrusions. The primary issue with traditional network intrusion detection systems is their limitations in detecting emerging and unknown threats. Rule-based systems and signature-based detection are effective against known attacks, but they struggle with zero-day exploits and polymorphic malware that evade their predefined criteria. Moreover, the sheer volume and complexity of network traffic make it challenging for human operators to manually analyze and identify anomalies in real-time. Therefore, there is an urgent need for automated network intrusion detection systems that leverage AI techniques to enhance detection accuracy, adaptability, and efficiency.

The objective of this research paper is to explore the role of artificial intelligence in automated network intrusion detection and highlight its potential for addressing the limitations of traditional NIDS approaches. By examining various AI techniques, such as machine learning, deep learning, reinforcement learning, and genetic algorithms, this paper aims to evaluate their advantages and limitations in the context of network intrusion detection. Additionally, the paper will present case studies and practical applications that demonstrate how AI-driven NIDS can effectively detect and prevent specific types of attacks. Lastly, the research will identify future prospects, emerging trends, and potential challenges in integrating AI with network intrusion detection systems, ultimately providing recommendations for future research and development in this domain.

Traditional Network Intrusion Detection Systems:

Traditional Network Intrusion Detection Systems (NIDS) are a critical component of network security infrastructure. Their primary purpose is to monitor network traffic and identify any suspicious activities or potential intrusion attempts. NIDS operate by analyzing network packets and comparing them against predefined rules or signatures to identify known attack patterns. However, traditional NIDS solutions also face various challenges in effectively detecting and preventing modern cyber threats. One of the primary challenges is the increasing complexity and sophistication of attacks. Attackers are constantly evolving their techniques, incorporating advanced evasion tactics to bypass detection mechanisms. Traditional NIDS often struggle to keep up with these new techniques, resulting in false negatives where attacks go undetected. Another challenge is the ever-growing amount of network traffic that needs to be analyzed. With the exponential increase in data flow, NIDS must process a vast number of packets in real-time. This can put a significant strain on the system's resources and impact its detection accuracy and performance.

Traditional NIDS often rely on rule-based systems, where rules are predefined based on known attack patterns. While this approach is effective in detecting known attacks, it fails to detect new or zero-day attacks that do not match any existing rules. This limitation makes rule-based systems vulnerable to emerging threats. Moreover, rule-based systems can generate a high number of false positives, where legitimate traffic is flagged as malicious. This can lead to alert fatigue for security analysts, who may become less responsive to legitimate alerts due to the overwhelming false positives. Signature-based detection is a commonly used approach in traditional NIDS. It involves comparing network packets against a database of known attack signatures. If a packet matches a signature, it is flagged as potentially malicious. Signature-based detection is efficient in identifying well-known attacks and provides a high detection rate for known threats. However, signature-based detection also has its limitations. As mentioned earlier, it is ineffective against new or unknown attacks that do not have a matching signature in the database. It is a reactive approach that relies on past attack knowledge rather than proactively detecting new attack patterns.

Attackers can easily evade signature-based detection by modifying attack payloads or employing encryption techniques. By constantly evolving their tactics, attackers can render signature-based detection less effective over time. In conclusion, while traditional NIDS have played a crucial role in network security, they face numerous challenges in keeping up with modern and sophisticated cyber threats. The limitations of rule-based systems and signature-based detection approaches highlight the need for more advanced and proactive intrusion detection systems that can adapt to evolving attack techniques and effectively defend against emerging threats.

Artificial Intelligence in Automated Network Intrusion Detection:

Artificial Intelligence (AI) has emerged as a critical tool in modern automated Network Intrusion Detection Systems (NIDS) due to its ability to learn from data, adapt to new attack patterns, and improve the detection accuracy. With the increasing complexity and sophistication of cyber-attacks, traditional rule-based and signature-based approaches used in NIDS have become insufficient. AI techniques offer a more proactive and dynamic approach to network security.

Machine Learning Techniques:

Supervised Learning and Unsupervised Learning are two prominent machine learning techniques used in AI-based NIDS. In supervised learning, a model is trained using labeled data that consists of network packets labeled as either normal or malicious. The model learns the patterns associated with each class and can classify incoming packets accordingly. This approach is effective in detecting known attack patterns and minimizing false positives. On the other hand, unsupervised learning is utilized when labeled training data is scarce or unavailable. It involves clustering and anomaly detection to identify potentially malicious activities based on deviations from normal network behavior. Unsupervised learning can detect unknown attacks and adapt to emerging threats, making it valuable in an ever-evolving cyber landscape.

Deep Learning Techniques:

Deep learning, a subset of machine learning, has gained significant attention in NIDS. Convolutional Neural Networks (CNN) are used to analyze network traffic at the packet level. They can automatically learn relevant features and detect complex patterns that may indicate malicious activities. With their hierarchical structure and parameter sharing, CNNs excel in capturing spatial and temporal dependencies in network traffic.

Recurrent Neural Networks (RNN) are another deep learning technique used in NIDS. They are designed to analyze sequential data, making them well-suited for analyzing network traffic flow and capturing temporal dependencies. RNNs can detect attacks that span multiple packets and learn long-term dependencies within network sessions.

Long Short-Term Memory (LSTM) networks are a variant of RNNs that address the vanishing gradient problem and handle dependencies over longer time intervals. They are capable of learning complex temporal relationships in network traffic, enabling them to effectively identify sophisticated attacks that may span a considerable duration.

Reinforcement Learning:
Reinforcement learning is an AI technique that can be applied to NIDS to autonomously learn and optimize decision-making strategies. It operates in an environment where the NIDS agent takes actions and receives feedback in the form of rewards or penalties. The agent's goal is to maximize cumulative rewards by learning the best actions to take in different network scenarios. Reinforcement learning provides the advantage of adaptability, allowing the NIDS to dynamically adjust its detection strategies based on changing attack patterns.

Genetic Algorithms:
Genetic algorithms are population-based optimization techniques inspired by biological evolution. In the context of NIDS, genetic algorithms can be used to evolve and improve the performance of rule-based systems. By applying different combinations of rules and evaluating their effectiveness, genetic algorithms can find optimized sets of rules that result in enhanced detection accuracy. This approach enables NIDS to adapt to new attack patterns and fine-tune its rule sets based on evolving threats.

Hybrid Approaches:
Hybrid approaches combine multiple AI techniques to leverage their respective strengths and enhance detection capabilities. For example, a hybrid NIDS may use machine learning-based clustering algorithms for anomaly detection combined with rule-based systems for known attack pattern matching. Such hybrid systems provide a more comprehensive and robust defense mechanism against a wide range of network threats.In conclusion, the integration of AI techniques, including machine learning, deep learning, reinforcement learning, genetic algorithms, and hybrid approaches, has revolutionized automated network intrusion detection systems. These advanced AI-based NIDS solutions offer improved detection accuracy, adaptability to evolving attack techniques, and proactive defense mechanisms, crucial for safeguarding modern networks against sophisticated cyber threats.

Advantages and Limitations of AI in Automated NIDS:
Enhanced detection accuracy:
One of the major advantages of using Artificial Intelligence (AI) in Automated Network Intrusion Detection Systems (NIDS) is the enhanced detection accuracy it offers. Traditional rule-based IDS systems often struggle with accurately detecting complex and sophisticated attacks due to their reliance on pre-defined signatures. In contrast, AI-driven NIDS systems can analyze large amounts of network traffic data, identify unusual patterns or anomalies, and learn from them to improve detection accuracy over time. By leveraging machine learning algorithms, AI-based NIDS can adapt and evolve in response to emerging threats and evolving attack techniques, continuously improving their ability to detect and respond to malicious activities.

Real-time and adaptive detection capabilities:
Another significant advantage of AI in Automated NIDS is its real-time and adaptive detection capabilities. AI-based NIDS can process and analyze network traffic data in real-time, enabling them to detect and respond to potential threats as they occur. The ability to adapt and learn from new attack patterns and evolving behavior gives AI-driven NIDS systems a dynamic advantage. By leveraging techniques like deep learning, neural networks, and decision trees, AI-driven NIDS can constantly update their knowledge base and adjust their detection algorithms, making them more effective at identifying both known and novel security threats.

Reduced false-positive rates:
One of the challenges in traditional NIDS systems is the high rate of false positives, where benign network traffic is mistakenly flagged as malicious. This can result in unnecessary alerts and added burden on security personnel. AI-based NIDS can help mitigate this problem by leveraging machine learning to accurately classify normal behavior and distinguish it from anomalous or malicious activities. By training on large datasets and continuously refining their models, AI-driven NIDS can significantly reduce false-positive rates, thus improving the efficiency and effectiveness of security operations.
Challenges and limitations of AI-driven NIDS:

While AI has shown great promise in enhancing NIDS capabilities, there are still challenges and limitations that need to be addressed.

1. Data limitations: AI-driven NIDS heavily rely on quality and diverse training data to develop accurate models. Obtaining labeled datasets that cover a wide range of attack scenarios and network traffic patterns can be challenging, especially for organizations with limited resources. The lack of representative data can affect the detection accuracy and generalization capabilities of AI-driven NIDS.

2. Adversarial attacks: AI-driven NIDS may be vulnerable to adversarial attacks, where attackers intentionally manipulate network traffic to bypass detection systems. By introducing subtle modifications to the data or exploiting vulnerabilities in AI algorithms, attackers can deceive NIDS and remain undetected. Developing robust AI models and implementing adversarial defenses in NIDS systems are crucial to mitigate this risk.

3. Interpretability and explainability: AI-driven NIDS often use complex machine learning algorithms, such as deep neural networks, which can be difficult to interpret. Understanding and explaining the reasoning behind NIDS decisions can be crucial for cybersecurity analysts to trust and act upon the alerts. Research into developing explainable AI techniques for NIDS is ongoing, but it remains a challenge to strike a balance between model complexity and interpretability.

4. Limited contextual understanding: AI-driven NIDS primarily relies on analyzing network traffic data and may lack contextual understanding of the broader IT infrastructure or business operations. Without this contextual knowledge, false positives or false negatives can still occur. Integrating AI-based NIDS with other security tools and systems to gain a holistic view of the network environment can help mitigate this limitation.

5. Continuous monitoring and updates: AI-driven NIDS models require continuous monitoring and updates to remain effective and adapt to new threats. As attack techniques and behaviors rapidly evolve, NIDS systems need to keep up with these changes to ensure comprehensive threat detection. This requires dedicated resources for monitoring model performance, retraining models, and regularly updating the NIDS system.In conclusion, AI-driven NIDS offers several advantages in terms of enhanced detection accuracy, real-time and adaptive detection capabilities, and reduced false positive rates. However, the limitations and challenges, such as data limitations, adversarial attacks, interpretability, contextual understanding, and continuous monitoring and updates, need to be addressed to maximize the potential of AI in automated NIDS systems and enhance cybersecurity defenses.

Case Studies:

Case studies play a crucial role in understanding and evaluating real-world applications of various technologies. In the context of cybersecurity, case studies provide valuable insights into the detection and prevention of denial-of-service (DoS) attacks using artificial intelligence (AI) as well as AI-based anomaly detection in network traffic. These case studies demonstrate the effectiveness and potential of AI systems in safeguarding networks from malicious activities.

DoS attacks pose a significant threat to networks and systems by overwhelming them with a flood of illegitimate requests, rendering them inaccessible to legitimate users. Traditional defense mechanisms have often struggled to keep up with the sophistication and scale of modern DoS attacks. AI has emerged as a powerful tool in combatting these attacks, as it can swiftly analyze large volumes of network data, identify attack patterns, and take necessary actions to mitigate the impact. Case studies have highlighted the successful implementation of AI-driven DoS attack detection and prevention systems. For instance, a study conducted by a team of researchers utilized machine learning algorithms to detect and mitigate DoS attacks in real-time. They employed a combination of supervised and unsupervised learning techniques to analyze network traffic, identify abnormal patterns, and predict potential attacks. By continuously monitoring and analyzing network traffic, the system was able to promptly detect malicious activities and automatically deploy countermeasures to protect the network from the identified threats.

Another case study showcased the implementation of a deep learning-based DoS attack detection system. This system used a recurrent neural network (RNN) model to analyze real-time network flow data and identify anomalous patterns associated with DoS attacks. By training the RNN with historical and labeled attack data, it learned to recognize and classify different types of DoS attacks accurately. The system was able to detect both known and unknown DoS attacks, enabling network administrators to respond swiftly and effectively. In addition to DoS attacks, AI has also been applied in network traffic anomaly detection. Anomalous network behavior often indicates potential security breaches or vulnerabilities that can be exploited by adversaries. Traditional anomaly detection methods often struggle to handle the massive volumes and complexities of network traffic data. However, AI-based approaches have demonstrated improved accuracy and efficiency in identifying network anomalies.

A case study focusing on AI-based anomaly detection in network traffic demonstrated the efficacy of using deep learning algorithms. The researchers developed a convolutional neural network (CNN) model trained on a large dataset of network traffic. The CNN was capable of capturing intricate patterns and dependencies in network traffic data, enabling it to differentiate between normal and anomalous behaviors. The system achieved high accuracy in classifying various types of anomalies, such as port scans, DDoS attacks, and protocol abuses. Furthermore, case studies have highlighted the advantage of combining AI-based anomaly detection with other cybersecurity techniques. For instance, a study explored the effectiveness of using AI-driven anomaly detection in conjunction with intrusion detection systems (IDS). By integrating machine learning algorithms into an IDS, the system enhanced its ability to detect sophisticated and novel attacks. The combined approach allowed for accurate and timely identification of anomalous events, providing network administrators with opportunities to respond and mitigate potential risks promptly. In conclusion, case studies play a vital role in illustrating the application and benefits of AI in the detection and prevention of DoS attacks as well as anomaly detection in network traffic. These studies demonstrate the effectiveness and potential of AI-driven systems in safeguarding networks from malicious activities. By continuously analyzing network data, AI systems can promptly identify, classify, and mitigate various types of attacks and network anomalies, enhancing the overall security posture of organizations. As AI continues to evolve, its role in cybersecurity is expected to grow, and case studies will continue to provide valuable insights into its real-world applications.

Future Prospects and Emerging Trends:

The future prospects and emerging trends in the field of artificial intelligence (AI) are vast and hold immense potential. In particular, the integration of AI with big data analytics is expected to revolutionize various industries, including cybersecurity. Furthermore, the concept of explainable AI in network intrusion detection systems (NIDS), the adoption of edge computing for AI-driven NIDS, and the need to address security and privacy concerns in AI-driven NIDS are key areas that will shape the future of this domain. As the volume, velocity, and variety of data continue to escalate, the integration of AI with big data analytics becomes crucial for extracting meaningful insights and patterns. By combining AI algorithms with big data analytics techniques, organizations can effectively process and analyze massive datasets to identify trends, anomalies, and potential threats. This integration enables proactive threat intelligence, faster response times, and improved decision-making capabilities.

One emerging trend in the field of NIDS is the concept of explainable AI. AI models are often considered black boxes, making it challenging to comprehend their decision-making processes. Explainable AI aims to address this issue by providing insights into the rationale behind AI-driven decisions. In the context of NIDS, explainable AI can help network administrators understand why a certain activity was flagged as malicious or anomalous. This transparency not only enhances trust in AI-driven NIDS but also allows for better analysis, validation, and fine-tuning of the system. The adoption of edge computing for AI-driven NIDS is another promising trend. Edge computing refers to the paradigm of processing data closer to the source, reducing latency, improving response times, and minimizing network bandwidth requirements. By deploying AI-driven NIDS at the edge of networks, such as in routers or gateways, the system can analyze network traffic in near real-time, providing faster detection and response capabilities.

Edge computing also addresses privacy concerns by keeping data within the network boundary, limiting the need for transmitting sensitive information to centralized servers. However, with the integration of AI-driven NIDS, there arise important security and privacy concerns that need to be addressed. AI systems heavily rely on robust and diverse datasets for training, which raises questions about the security and privacy of this data. Organizations must ensure that sensitive information is adequately protected and anonymized to prevent unauthorized access or misuse. Additionally, adversaries may exploit vulnerabilities in AI models, leading to adversarial attacks or data poisoning, where they manipulate inputs to deceive or compromise NIDS. Ongoing research and development efforts are necessary to mitigate these security risks and reinforce the resilience of AI-driven NIDS.

Privacy concerns also come into play when deploying AI-driven NIDS. Deep learning models often require access to large amounts of data, including personally identifiable information (PII), which can raise privacy concerns. Striking a balance between effective threat detection and preserving user privacy becomes paramount. Privacy-preserving techniques, such as federated learning or differential privacy, can help address these concerns by enabling analysis and model training without exposing sensitive data. In conclusion, the integration of AI with big data analytics holds immense potential for various industries, including cybersecurity. Emerging trends such as explainable AI in NIDS, the adoption of edge computing, and the need to address security and privacy concerns are shaping the future of AI-driven NIDS. As organizations strive to detect and mitigate sophisticated threats, they must carefully navigate the challenges posed by security and privacy, ensuring that AI-driven NIDS are both effective and responsible in safeguarding networks and protecting user data.

CONCLUSION

In conclusion, the research paper titled 'The Role of Artificial Intelligence in Automated Network Intrusion Detection' has provided important insights into the use of artificial intelligence (AI) in enhancing network intrusion detection systems (NIDS). The key findings of the paper can be summarized as follows:

1. AI-based NIDS significantly improve the efficiency and accuracy of threat detection by analyzing large volumes of network data in real-time. Machine learning algorithms, such as deep learning and reinforcement learning, have proven to be effective in identifying and classifying various types of network intrusions.

2. The integration of AI with big data analytics offers opportunities for extracting meaningful insights from massive datasets, enabling proactive threat intelligence and improved decision-making capabilities. This integration enhances the overall effectiveness of NIDS in detecting and responding to network intrusions.

3. Explainable AI in NIDS addresses the black box problem, providing transparency and insights into the decision-making process of AI models. This transparency enhances trust in AI-driven NIDS, facilitates analysis and fine-tuning of the system, and enables better collaboration between security analysts and AI systems.

Based on these key findings, there are several recommendations for future research on the role of AI in automated NIDS:

1. Further research should be conducted to explore the scalability of AI-driven NIDS in large-scale networks. As network infrastructures continue to grow in complexity and size, it is important to assess the performance and scalability of AI models to ensure their effectiveness and efficiency in detecting network intrusions in such environments.

2. Research should focus on developing AI algorithms that can adapt to evolving attack techniques. Cyber adversaries are constantly evolving their strategies, and AI models need to be able to recognize and adapt to new attack patterns. Ongoing research on advanced AI algorithms and reinforcement learning techniques can contribute to this area.

3. In addition to the detection of network intrusions, future research should also emphasize the response and mitigation aspects. AI-driven NIDS can be integrated with automated response systems to dynamically counteract attacks. Investigating the effectiveness and reliability of these mechanisms is crucial for developing comprehensive NIDS solutions.

4. Ethical considerations and legal frameworks surrounding AI-driven NIDS need to be further explored. As the deployment of AI in network security becomes ubiquitous, it is important to address issues related to privacy, data protection, and the responsible use of AI algorithms.

In summary, the research paper has shed light on the pivotal role of AI in automated network intrusion detection. The key findings emphasize the improved performance, scalability, and transparency provided by AI-driven NIDS. Through further research and exploration, the recommendations highlighted above can contribute to the continued development and advancement of AI-based NIDS, ultimately strengthening our ability to detect, respond to, and mitigate network intrusions.

REFERENCES

[1]. Agarwal, R., & Joshi, M. (2000). PNrule: A new framework for learning classifier models in data mining. Technical Report TR 00-015.

[2]. Al-Yaseen, W.L., Othman, Z.A., & Nazri, M.Z.A. (2017). Multi-level hybrid support vector machine and extreme learning machine based on modified K-means for intrusion detection system. Expert Systems with Applications, 67, 296-303.

[3]. Anderson, D., Lunt, T., Javitz, H., Ann, T., & Valdes, A. (1995). Next generation intrusion detection expert system (NIDES). Technical report, SRI International USA.

[4]. Anderson, P. (1980). Computer Security Threat Monitoring and Surveillance. Retrieved from: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/ande80.pdf

[5]. Axelsson, S. (1999). Research in intrusion detection system—a survey. CMU/SEI Technical Report.

[6]. Balajinath, B., & Raghavan, S.V. (2001). Intrusion detection through learning behavior model. Computer Communications, 24(12), 1202-1212.

[7]. Beale, J., Caswell, B., & Poor, M. (2004). Snort 2.1 intrusion detection (2nd ed.). Syngress Publishing.

[8]. Ben n'cir, C-E., Cleuziou, G., & Nadia, E. (2015). Overview of Overlapping Partitional Clustering Methods. In Partitional Clustering Algorithms (pp. 245-275). Springer.

[9]. Bivens, A., Chandrika, P., Smith, R., & Szymanski, B. (2002). Network-based intrusion detection using neural networks. In Proceedings of ANNIE 2002 conference, ASME Press, pp 10–13.

[10]. Carpenter, G.A., Grossberg, S., Markuzon, N., Reynolds, J.H., & Rosen, D.B. (1992). Fuzzy ARTMAP: A neural network architecture for incremental supervised learning of analog multidimensional maps. IEEE Transactions on Neural Networks, 3, 698-713.

[11]. Chebrolu, S., Abraham, A., & Thomas, J.P. (2005). Feature deduction and ensemble design of intrusion detection systems. International Journal of Computer Security, 24(4), 295-307.

[12]. Chen, S. Staniford, Cheung, S., Crawford, R., Dilger, M., Frank, J., Hoagland, J., ... Zerkle, D. (1996). GrIDS - a graph-based intrusion detection system for large networks. In Proceedings of 19th national information systems security conference.

[13]. Chen, W-H., Hsu, S-H., & Shen, H-P. (2005). Application of SVM and ANN for intrusion detection. Computers & Operations Research, 32, 2617-2634.

[14]. Chittur, A. (2001). Model generation for an intrusion detection system using genetic algorithms. High School Honors Thesis, Ossining High School. In cooperation with Columbia University.

[15]. CiscoSecure. (2010). Cisco Secure IDS. Retrieved from: http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/index.shtml

[16]. Cohen, W.W. (1995). Fast effective rule induction. In Proceedings of the 12th international conference on machine learning (pp. 115-123). Tahoe City, Morgan Kaufmann.

[17]. Crosbie, M., Dole, B., Ellis, T., Krsul, I., & Spafford, E. (1996). IDIOT - users guide. Technical report TR-96-050. Purdue University, COAST Laboratory.

[18]. Crosbie, M., & Spafford, E.H. (1995). Active defense of a computer system using autonomous agents. Technical report CSD-TR-95-008. Purdue University, West Lafayette.

[19]. Cunningham, R., & Lippmann, R. (2000a). Detecting computer attackers: Recognizing patterns of malicious stealthy behavior. MIT Lincoln Laboratory - presentation to CERIAS.

[20]. Cunningham, R., & Lippmann, R. (2000b). Improving intrusion detection performance using keyword selection and neural networks. Computer Networks, 34(4), 597-603.

[21]. Dasgupta, D., & Gonzalez, F.A. (2001). An intelligent decision support system for intrusion detection and response. In Proceedings of international workshop on mathematical methods, models and architectures for computer networks security (MMM-ACNS), St. Petersburg. Springer.

[22]. Dickerson, J.E., & Dickerson, J.A. (2000). Fuzzy network profiling for intrusion detection. In Proceedings of NAFIPS 19th international conference of the North American fuzzy information processing society, Atlanta.

[23]. Dowell, C., & Ramstedt, P. (1990). The computerwatch data reduction tool. In Proceedings of the 13th national computer security conference, Washington, DC.

[24]. Duda, R.O., & Hart, P.E. (1973). Pattern classification and scene analysis. Wiley, New York.

[25]. Ertoz, L., Eilertson, E., Lazarevic, A., Tan, P., Srivastava, J., Kumar, V., & Dokas, P. (2004). The MINDS - Minnesota intrusion detection system. In Next Generation Data Mining (pp. 249-270). MIT Press.

[26]. Fortuna, C., Fortuna, B., & Mohorcic, M. (2007). Anomaly detection in computer networks using linear SVMs. In 16th International Conference on Knowledge Discovery and Data Mining (SiKDD 2007), Ljubljana, Slovenia.

[27]. Garcia-Teodoro, P., Diaz-Verdejo, J., Macia-Fernandez, G., & Vazquez, E. (2009). Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & Security, 28, 18-28.

[28]. Gharibian, F., & Ghorbani, A.A. (2007). Comparative study of supervised machine learning techniques for intrusion detection. In Proceedings of fifth annual conference on communication networks and services research (CNSR'07), pp. 350-358.

[29]. Ghosh, A.K., Wanken, J., & Charron, F. (1998). Detecting anomalous and unknown intrusions against programs. In Proceedings of the 14th annual computer security applications conference (pp. 259-267). IEEE.

[30]. Goldberg, L., Wagner, D., & Thomans, R. (1996). A secure environment for untrusted helper applications: Confining the wily hacker. In Sixth USENIX Security Symposium.

[31]. Gomez, J., & Dasgupta, D. (2001). Evolving fuzzy classifiers for intrusion detection. IEEE Workshop on Information Assurance, United States Military Academy.

[32]. Guerin, G.D. (1997). Classification by voting feature intervals. In Proceedings of the European conference on machine learning (pp. 85-92).

[33]. Habra, J., Charlier le B, Mounji, A., & Mathieu, I. (1992). ASAX: Software architecture and rule based language for universal audit trail analysis. In Computer Security (pp. 435-440). Proceedings of ESORICS 92.

[34]. Halme, L.R., & Bauer, R.K. (1995). AINT misbehaving: A taxonomy of anti-intrusion techniques. In Proceedings of the 18th