Network Intrusion Detection Through Classification Methods and Machine Learning Techniques

Conference Paper · October 2023

DOI: 10.1109/ICAI58806.2023.10339029

Pavel Petrov
University of Economics Varna
63 PUBLICATIONS **274** CITATIONS

Jordan Jordanov
University of Economics Varna
7 PUBLICATIONS **17** CITATIONS

International Conference AUTOMATICS AND INFORMATICS`2023, October 05 - 07, 2023, Varna, Bulgaria (ICAI'23)

Network Intrusion Detection through Classification Methods and Machine Learning Techniques

Dimitrios Simeonidis
Department of Informatics
University of Economics - Varna
Varna, Bulgaria
simeonidis@ue-varna.bg

Pavel Petrov
Department of Informatics
University of Economics - Varna
Varna, Bulgaria
petrov@ue-varna.bg

Jordan Jordanov
Department of Informatics
University of Economics - Varna
Varna, Bulgaria
jordanov.jordan@ue-varna.bg

2023 International Conference Automatics and Informatics (ICAI) | 979-8-3503-1291-1/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICAI58806.2023.10339029

***Abstract*—The field of network attacks is rapidly evolving, which makes it particularly difficult to grasp a universal picture of the problem. Intrusion detection is one of the most important tools for securing and protecting computer systems from malicious attackers by enabling detection of attacks and reducing their impact. In this research, we study the problem of cyberattacks and approach the possibility of securing computer and network communications by proposing intrusion detection approaches based on classification and machine learning mechanisms. Considering that intrusion detection is not simply a matter of predicting the most likely classification (attack-"normal" behavior), since different types of errors incur different costs, we propose the implementation of a cost-sensitive approach to intrusion detection and apply it to some well-known and efficient classification algorithms for both wired and wireless networks. The research method used in the study employs a research design focused on evaluating the effectiveness of intrusion detection systems using classification algorithms. Statistical analysis could be applied as necessary to analyze the data, and the research is designed to be reproducible for future studies.**

Keywords*—computer network, intrusion detection, machine learning, classification

I. Introduction

As the connectivity of computers is constantly increasing, the need for security of computer systems and networks becomes imperative. The security of computer systems can be described as how well a system is able to protect the system's information from attackers. To have security in a network communication it is necessary to meet the following basic principles availability, confidentiality, integrity, authentication, and nonrepudiation [1]:

- Availability ensures the continued functioning of network services to participants when needed.
- Confidentiality confirms that the information transmitted is accessible only to authorized participants and is never disclosed to unauthorized users.
- Authentication confirms the identity of the participant who transmits information.
- Integrity ensures the secure transfer of information without amendments.
- Nonrepudiation confirms that an entity can demonstrate the flow of information from one entity to another (sender / recipient) and cannot refute the fact that it received or sent specific data.

However, often the above basic safety principles are not followed resulting in computer systems / networks being exposed to many threats. McNab [2] classified the threats against a computer system in the following categories:

- Risk: Unintentional or unanticipated information reporting or violation of operational integrity because of hardware breakdown, incomplete or wrong software design.
- Vulnerability: A known or suspected defect in a system's hardware, software, or operation that exposes the system to successful attacks or unintentional disclosure of its information.
- Attack: A thorough plan's execution in order to make a threatening attempt.
- Penetration: An effective attack characterized by the ability to gain unapproved and unnoticeable access to records and projects, as well as the control status of a PC framework.

According to Kizza et al. [3]: "intrusion is defined as any set of actions that attempt to undermine the integrity, confidentiality, or availability of a computer resource". This definition does not distinguish between the success or failure of these actions.

II. Detection of Intrusion Using Classification Algorithms

To achieve the required security goals and protect computer systems, many security mechanisms have been proposed and implemented. Intrusion prevention through encryption and authentication can be used as the **first line of defense** to limit intruders, but it certainly cannot eliminate them. No matter how many protections are implemented in a network, there are always some vulnerabilities and security holes that can be exploited by a malicious user. To prevent or mitigate an attack, a second firewall is required.

Intrusion detection systems (IDS) could be used as the **second line of defense** against evil attackers because they help detect attacks, limit their impact and are necessary to achieve great functionality in a network. Intrusion detection can be described as the method of determining inappropriate, false, or abnormal activity. An intrusion detection system's purpose is to discern between illegal ("abnormal") and legitimate ("normal") conduct. As a result, an intrusion detection system is a classification system capable of analyzing system behavior or security events and detecting harmful behavior.

979-8-3503-1291-1/23/$31.00 ©2023 IEEE

The two basic categories of intrusion detection are intrusion based on **anomaly detection** and intrusion based on **misuse detection**. These types of intrusion detection could be supported by using **classification algorithms**. Most intrusion detection systems have some difficulty in successfully classifying and distinguishing intrusions from "normal" network behavior, which makes it difficult to develop a robust system for real-time intrusion detection. Classification algorithms are used in intrusion detection to improve the performance of data search and analysis from previously recorded computer system files. A classification-based intrusion detection system can be roughly defined as one that classifies the recorded data using a set of rules, standards, or another classification method.

Thus, we select classification algorithms and use their advantages to achieve reliable and effective intrusion detection. The classification algorithms are very simple in their operation and application, are automated, provide direct and accurate results, and have extensive applications, bibliographic coverage, and extensive experimental experience to prove their effectiveness.

The ideal application of intrusion detection with classification algorithms is based on the concentration of several "normal" and "abnormal" recorded data corresponding to the behavior of a user or a program. Then, the classification algorithm is applied to train the classifier and predict the class ("normal" or "abnormal") of the newly recorded data. A classifier is created when a learning algorithm is applied to a data set. The training dataset consists of several records and vectors, where each vector consists of a set of field attributes. The purpose of a classifier is to use a feature vector and assign each vector to a category. To use a classifier for a problem, we follow a pattern recognition process. The design of the pattern recognition system (Figure 1) usually involves the repetition of several different activities [4]: data collection, field attribute selection, model selection, classifier training, testing, and evaluation.

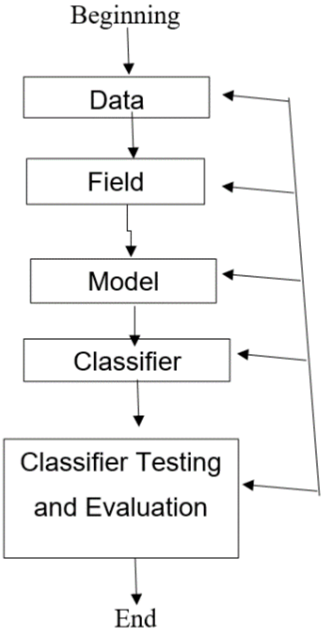

Fig. 1. Pattern Recognition Procedure

The basic steps in an intrusion detection system based on classification algorithms are the following:

- Data Collection: Data collection has to do with the problem that we want to solve, and it is especially important to collect a large and representative set of examples for the education and testing of the classifier.
- Field Selection: The selection of the appropriate fields to help separation of classes, which are representative of each problem, is a particularly important step.
- Model Selection: In order to select the appropriate model, we use specific methods to configure the training model in order to achieve a specific goal, for example to minimize the classification error.
- Classifier Training: Having selected the appropriate model and appropriate parameters we train our classifier.
- Classifier Testing and Evaluation: We test our classifier in a set of data tests, and we examine the effectiveness of our classifier. The results of the evaluation can lead to the repetition of several previous steps to obtain satisfactory results.

III. Self Organizing Maps for Intrusion Detection

Network traffic logs are undoubtedly a powerful weapon to secure our systems, but also to detect possible intruders. In particular, web traffic logs help us understand the cause of an unforeseen failure of our system, the extent of the damage caused by an attack, or even the discovery of an attack in real time.

On the other hand, maps have always provided us with a practical way to navigate and expand. Although almost everything is mapped today, we still observe cyber activities through the keyhole [5]. Network traffic maps can be very helpful in getting a comprehensive picture of what is going on in a computer network and, more importantly, in effectively detecting potential intruders.

We present an anomaly detection approach which uses eSOM to map network traffic, in order to relieve network managers of the extremely difficult and time-consuming chore of scrutinizing network traffic while avoiding excessive processing costs. In this regard, our approach exploits the human ability to effectively manage complexity. Monitoring traffic becomes user-friendly and displaying network information provides new opportunities for detecting and analyzing possible intrusions.

The ability of neural networks to accept erroneous data is a huge advantage. Although ESOMs are based on the straightforward Kohonen's SOM (KSOM), they have several benefits that we can use to improve intrusion detection performance. We can better understand networks by fusing tools for information visualization with machine learning. Regarding its capacity to distinguish between "normal" and "abnormal" behavior, the suggested strategy yields encouraging findings.

In the area of intrusion detection, KSOM is widely employed. The iSOM software package, which is a component of the INBOUNDS intrusion detection system, is described by Bakshi & Dujodwala [6]. This software application uses KSOM to find irregularities in network traffic. They proposed an intrusion detection approach based on a KSOM hierarchy and attempted to determine whether an intrusion detection approach based on a hierarchical KSOM sequence was effective using only 6 of the 41 fields in a dataset. Stevens & Rago [7] proposed a prototype anomaly detection system in a UNIX environment that is node-based and monitors network node users.

This system relies on KSOM to investigate whether a user's behavior is "abnormal." Dhakne & Chatur [8] use KSOM hierarchically to achieve node-based intrusion detection. Two levels make up the hierarchical KSOM design in use. Three maps make up the first level. A variety of data and time vectors are displayed on each map. The results of each map level are combined in the second level map to give a complete view of the network state. Creux et al.'s [9] anomaly detection system tries to classify real data using KSOM. Normal data is used to train KSOM before actual Ethernet data is used to test the system. If a winning neuron is not one of the identified neurons, an attack occurs. They employ KSOM to compare the outcomes of an unsupervised method (KSOM) for anomaly identification with those of a neuro-immune approach. This comparison does not have a clear winner. Qiao et al. [10] suggested a method for detecting assaults that makes use of several KSOMs. Their technique does not rely on a single KSOM to identify attacks, but rather on a multi-KSOM monitoring stack design, with each KSOM unique to detecting "abnormal" protocol behavior. Prasad [11] suggested a method based on KSOM and Resilient Propagation Neural Network (RPROP) to detect intrusions in regular traffic and invasions by combining imaging (with KSOM) and sorting (with RPROP). All methodologies described above for intrusion detection are based on simple KSOMs, which can be considerably improved by employing eSOMs.

IV. Intrusion Detection with eSOM

In intrusion detection with eSOM, we proceeded as follows:

The first step is to process the data to be used for web traffic classification. So, after collecting the data that describes the network traffic, we select the most relevant data fields and then normalize them. To avoid a large impact on the input vector fields, the input data must be normalized. The data was normalized using a variety of techniques. We used mean zero approach and variance one approach to normalize the data, which, according to the literature, typically produces very positive outcomes.

The next step in detecting intrusions is to classify the data. To classify the data, we perform clustering of the training dataset using eSOM. To avoid information loss, we train eSOMs with existing network traffic logs and take advantage of the key advantages of eSOMs, such as the huge number of neurons and the ability to obtain borderless maps.

After training the training dataset, a map was created that clearly shows the formation of classes of "normal" network traffic and attacks (creating classifiers). Each of these groups (classes) is then used to classify new datasets (applying classifiers to control datasets). By applying the classifiers to the new traffic datasets, we obtain a new visual representation that shows how the control data is classified into the existing classes.

V. Intrusion Detection in Wireless Networks Using Key Agreement Protocols

Effective and secure intruder response should be used in conjunction with effective [12] intrusion detection. For an effective and safe reaction to an intrusion, security measures like group key management and agreement should be the foundation. For wireless networks, several group key management techniques [13] have been developed, including numerous systems built on a tree structure [14]. However, most of these protocols cannot be used in casual networks or other environments with poor infrastructure or sensitive resource management.

For instance, four nodes form a 22-cube in the Octopus protocol [15], and the other network members are "edges" connected to one of the central nodes. It is difficult to keep such a topology in a network that occasionally experiences dynamic behavior. The IKA1 and IKA2 (Internet Key Agreement) protocols' performance is enhanced by the Tree-Group Diffie-Hellman (TGDH) protocol, which was proposed in [16]. However, it is based on modular exponentiation, which can necessitate computing the group session key in exponential steps, making it the most expensive computational operation.

Lv et al. [18] proposed a key agreement protocol based on a shared group password, the XOR operation, and a binary tree structure. Although this method works well in casual networks, it is vulnerable to password computation and replay attacks. Guo et al. [19] improved on the previous approach by incorporating mutual certification and a key renewal process on a regular basis. However, because it is password-based, their approach is vulnerable to dictionary and brute force attacks.

The Intrusion Response Machine consists of the following basic elements:

- Communication Unit: it is accountable for agreeing local keys (LK) and a global key (GK) based on a group key agreement protocol, which are utilized in the local response unit and in the universal response units.
- Local Response Unit: it is in charge of the creation of the eSOM Local Map Distribution Protocol.
- Universal Response Unit: it is responsible for the Universal Map Distribution Protocol.

The Intrusion Response Machine accepts as input the eSOM maps created by the Intrusion Detection Machine. These maps are created locally at each node of the wireless network from time to time and are protected from possible changes using a proposed watermarking technique.

The Local Response Unit ensures the secure distribution of the local eSOM maps in the local network using the local and universal key generated by the Secure Communication Unit. An eSOM Global Map is then created, which consists of the eSOM Local Maps of all nearby (one-step) node neighbors. The crated eSOM Global Map is used to indicate the security state of the local network on an occasion consisting of the immediate (one-step) neighbors of a node. The eSOM Universal Charter is also protected by the proposed watermarking technique. Depending on the size of the attack derived from the observation of the Universal Charter, the next step of the response engine is determined.

This map also assists nodes in determining the most suitable and secure neighbor node for message forwarding.

The Universal Response Unit is in charge of informing all neighbors within the attacker node's communication range. If the attack is not very severe, the appropriate node is selected for forwarding packet messages through the local network. If the attack is particularly severe, it is determined based on the extent of the eSOM map of a node covered (over 2/3) with attack markers. In this case, the Universal Response Unit is activated, which is responsible for deleting the attacked node from the appropriate routing tables and warning all nodes within the attacked node's range of a potential attack.

For the proposed approach to be effective, the local eSOM maps created at each node of the network, as well as the universal local map, must be protected from possible modification or violation. To this end, we propose an innovative watermarking technique that helps us ensure the integrity of the eSOM maps and detect possible modifications to them. The proposed watermarking technique is based on an effective combination of the lattice and block wise integration methods.

Watermarking is widely used in information security research. In the field of intrusion detection, Run et al. [20] proposed an intrusion detection framework for wired networks that allows watermarking packets and tracking the source IP address of the attacker only when the intrusion detection subsystem detects that an attack is in progress.

Despite the significant benefits of watermarking techniques, no application of watermarking techniques in casual wireless network security has yet been proposed. Given the vulnerability of image cards to forgery, watermarking techniques can be applied to eSOM cards to certify their authenticity and detect any card modifications. Watermarking techniques can be used to identify image components that have been illegally altered or transformed.

VI. Conclusion

While the paper does not provide specific empirical results, it highlights the potential benefits of adopting classification algorithms to assesses two categories of intrusion detection: anomaly detection and misuse detection. Classification algorithms are selected for their simplicity, automation, and proven effectiveness, while ethical considerations and limitations are acknowledged.

We integrate machine learning and information visualization approaches to acquire a clearer view of network activity, relieving network managers of the particularly difficult and time-consuming chore of monitoring network data [21] and avoiding excessive processing overhead [22]. We take advantage of neural networks that tolerate imprecise data, as well as the human ability to effectively manage complexity. We have succeeded in making traffic monitoring user-friendly, as the display of network information provides new opportunities [23] for detection and analysis [24] of possible intruders.

The approach suggested can be used to analyze both real-time and historical network traffic. The intrusion detection strategy based on eSOM produces excellent results with very low levels of false alarms. When the datasets used for training and testing include more attacks, the results are more optimistic when we employ 18 fields derived from the essential fields of each attack type and "normal" network traffic. The proposed approach analyzes and decodes network events that are not human readable and provides them in a readable form. The results of the proposed intrusion detection method through information visualization are easy to understand and facilitate the network administrator's task of detecting attacks.

It should also be noted that we need to update the trained eSOM maps as new standards of cyber-attacks emerge, as well as new network conditions, to ensure that our technique always yields dependable and precise results. The proposed intrusion detection method is simple to implement and can be easily applied to other architectures.

The key flaw in the suggested strategy is the high computational cost involved in training datasets with more than 10,000 records. But, of course, the eSOM computation does not prohibit its use, since it is performed only during training, which is not as frequent as checking with new network traffic data. Furthermore, the classes of classified data must be created manually by monitoring the map throughout the classification process, which may result in a procedural error.

Acknowledgment

This research is financially supported by NPI-67/2023 of University of Economics – Varna Science Fund.

References

[1] E. Cole, R. L. Krutz, and J. W. Conley, *Network security bible.* Indianapolis, In: Wiley, 2009.

[2] C. Mcnab, *Network security assessment : know your network*. Sebastopol, Ca: O'reilly Media, Inc, 2017.

[3] J. M. Kizza, *Guide to computer network Security*. 2017. doi: 10.1007/978-3-319-55606-2.

[4] A. Mitrokotsa and C. Dimitrakakis, "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection," *Ad Hoc Networks*, vol. 11, no. 1, pp. 226–237, Jan. 2013, doi: 10.1016/j.adhoc.2012.05.006.

[5] P. V. Ponangi, P. Kidambi, D. Rao, M. Fendley, M. Haas, and S. S. Narayanan, "ON THE OFFENSE: USING CYBER WEAPONS TO INFLUENCE COGNITIVE BEHAVIOR," *International Journal of Cyber Society and Education*, vol. 5, no. 2, pp. 127–150, Dec. 2012, doi: 10.7903/ijcse.1101.

[6] A. Bakshi and Y. B. Dujodwala, "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine," *2010 Second International Conference on Communication Software and Networks*, Singapore, 2010, pp. 260-264, doi: 10.1109/ICCSN.2010.56.

[7] W. R. Stevens and S. Rago, *Advanced Programming in the UNIX Environment, second edition*. Addison-Wesley 2013.

[8] A. R. Dhakne and P. N. Chatur, "Distributed Trust based Intrusion Detection approach in wireless sensor network," *2015 Communication, Control and Intelligent Systems (CCIS)*, Mathura, India, 2015, pp. 96-101, doi: 10.1109/CCIntelS.2015.7437886.

[9] V. K. BP, K. SM and P. LV, "Deep machine learning based Usage Pattern and Application classifier in Network Traffic for Anomaly Detection," *2023 International Conference on Advances in Electronics, Communication, Computing and Intelligent Information Systems (ICAECIS)*, Bangalore, India, 2023, pp. 50-54, doi: 10.1109/ICAECIS58353.2023.10169914.

[10] J. Qiao and H. Han, "An adaptive fuzzy neural network based on Self-Organizing Map (SOM)," in *InTech eBooks*, 2010. doi: 10.5772/9158.

[11] N. Prasad, R. Singh and S. P. Lal, "Comparison of Back Propagation and Resilient Propagation Algorithm for Spam Classification," *2013 Fifth International Conference on Computational Intelligence, Modelling and Simulation*, Seoul, Korea (South), 2013, pp. 29-34, doi: 10.1109/CIMSim.2013.14.

[12] I. O. Kuyumdzhiev, “Controls Mitigating the Risk of Confidential Information Disclosure by Facebook: Essential Concern in Auditing Information Security.” *TEM Journal 3*(2), 2014, pp.113-119.

[13] T. T. Mapoka, “Group Key Management Protocols for Secure Mobile Multicast Communication: A Comprehensive survey,” *International Journal of Computer Applications*, vol. 84, no. 12, pp. 28–38, Dec. 2013, doi: 10.5120/14629-2985.

[14] B. Wu, J. Wu, and Y. Dong, “An efficient group key management scheme for mobile ad hoc networks,” *International Journal of Security and Networks*, vol. 4, no. 1/2, p. 125, Jan. 2009, doi: 10.1504/ijsn.2009.023431.

[15] R. Melamed, I. Keidar, and Y. Barel, “Octopus: A fault-tolerant and efficient ad-hoc routing protocol,” *Wireless Networks*, vol. 14, no. 6, pp. 777–793, Jan. 2007, doi: 10.1007/s11276-006-0013-6.

[16] S. A. Mortazavi, A. N. Pour and T. Kato, "An efficient distributed group key management using hierarchical approach with Diffie-Hellman and Symmetric Algorithm: DHSA," *2011 International Symposium on Computer Networks and Distributed Systems (CNDS)*, Tehran, Iran, 2011, pp. 49-54, doi: 10.1109/CNDS.2011.5764584.

[17] J. A. Álvarez-Bermejo, A. Lodroman and J. A. López-Ramos, “Distributed Key Agreement for Group Communications Based on Elliptic Curves. An Application to Sensor Networks.” Mathematical Methods in the Applied Sciences. Vol. 39. John Wiley and Sons Ltd, 2016. pp.4797–4809. https://doi.org/10.1002/mma.3802

[18] C. Lv, X. Jia, L. Tian, J. Jing and M. Sun, "Efficient Ideal Threshold Secret Sharing Schemes Based on EXCLUSIVE-OR Operations," *2010 Fourth International Conference on Network and System Security*, Melbourne, VIC, Australia, 2010, pp. 136-143, doi: 10.1109/NSS.2010.82.

[19] H. Guo, X. Shen, W. L. Goh and L. Zhou, "Data Analysis for Anomaly Detection to Secure Rail Network," *2018 International Conference on Intelligent Rail Transportation (ICIRT)*, Singapore, 2018, pp. 1-5, doi: 10.1109/ICIRT.2018.8641555.

[20] R.-S. Run, S.-J. Horng, J.-L. Lai, T.-W. Kao, and R.-J. Chen, “An improved SVD-based watermarking technique for copyright protection,” *Expert Systems With Applications*, vol. 39, no. 1, pp. 673–689, Jan. 2012, doi: 10.1016/j.eswa.2011.07.059.

[21] J. Vasilev, Network Security by Analysis of Log Files of Apache Web Server. *SocioBrains: International Scientific Refereed Online Journal* , № 4, p. 66-88, 2014.

[22] S. A.-M. Ramona, C. M. Pompiliu, and M. Stoyanova, “Data mining algorithms for knowledge extraction,” in *Springer proceedings in business and economics*, 2020. doi: 10.1007/978-3-030-43449-6_20.

[23] P. Petrov, I. Kuyumdzhiev, R. Malkawi, G. Dimitrov, and J. Jordanov, “Digitalization of educational services with regard to policy for information security,” *TEM Journal*, pp. 1093–1102, 2022. doi:10.18421/tem113-14

[24] S. Stefanov, D. Georgieva, and J. Vasilev, “Issues in the disclosure of financial information by Multinational Enterprises,” *TEM Journal*, pp. 5–12, 2022. doi:10.18421/tem111-01