A Method for Determining the Credibility of Intrusion Detection based on a Probabilistic Graph Model in the Proactive Protection Subsystem of the Operational Cybersecurity Center

Andrey R. Ocheredko[a], Michael M. Putyato[b] and Alexander S. Makaryan[c]
Kuban State Technological University, 2 Moskovskaya St., Krasnodar, Russian Federation

Keywords: Cybersecurity, Machine Learning, Cyber Threats, Neural Networks, Bayes Theorem, Probability Theory, Probabilistic Analysis, Information Security, Network Attacks.

Abstract: The threat landscape is expanding rapidly, which has a number of consequences for most organizations and individuals. This is evidenced by a large number of cyber attacks which constantly occur in cyberspace. Although several defensive approaches have recently been proposed and implemented, the most of them are entirely theoretical. Others remain unfeasible due to the computational requirements of their implementation. The issue of computational complexity becomes extremely significant for methods which have proven to be implementable, because they often tend to consume a large amount of computational resources. Also most of these methods are reactive which means that they can only be initiated after an incident has already occurred. Moving from reactive approach to proactive one is currently one of the greatest challenges in the sphere of cybersecurity research.

1 INTRODUCTION

Cybersecurity is a serious problem for a large number of organizations, institutions, corporations and individuals around the world. Specialists (Buczak and Guven, 2016) argue that a set of technologies and processes for monitoring and preventing unauthorized access, modification, misuse and denial of service of computer networks and resources implies a concept such as cybersecurity. It also includes the tendency to authorize access to classified content and critical infrastructure that can be accessed through the network. Most networks are widely interconnected via the Internet and serve as means of exchanging data, information, intelligence, software and hardware. Although the sharing of valuable resources to improve operational efficiency is an inherent feature the computer networking paradigm, it has also created a way to easy distribution of malware. Therefore the escalation of cyber-attacks is taking place in cyberspace.

This expansion of the threat spectrum is a factor in the growing power of cybercrime, which is gradually entering the sphere of control over all domestic, business and industrial functions. The danger of cyberattacks consists in the possibility of altering system or database parameters to create a kinetic effect in escalating attacks, including the tendency to destroy classified content (Akyazi, 2014). Defense against cyber-attacks requires both proactive and reactive approaches, which can also be characterized as active and passive ones. They are relevant in the context of organizing direct defensive actions or methods to mitigate the effects of cyber threats. Therefore, it is important to understand the research gaps in current approaches to cybersecurity. That is why this article is going to review the methods that are in use now and the ones that will be used in the near future to detect and prevent incidents. The following sections will discuss cybersecurity approaches in terms of detection, prediction and prevention. Generally, attack detection and prediction can be achieved with the help of machine learning and

[a] https://orcid.org/0000-0002-1451-995X
[b] https://orcid.org/0000-0001-9974-7144
[c] https://orcid.org/0000-0002-1801-6137

Ocheredko, A., Putyato, M. and Makaryan, A.
A Method for Determining the Credibility of Intrusion Detection based on a Probabilistic Graph Model in the Proactive Protection Subsystem of the Operational Cybersecurity Center.
DOI: 10.5220/0010620400003170
In *Proceedings of the International Scientific and Practical Conference on Computer and Information Security (INFSEC 2021)*, pages 163-167
ISBN: 978-989-758-531-9; ISSN: 2184-9862

evolutionary algorithms, as well as statistical methods and association rules. Similarly, most approaches to attack prevention are achieved by analyzing traffic to detect and block (or stop) malicious activity.

2 APPROACHES TO DETECTING CYBER-ATTACKS

Cyber attack detection is a common attack mitigation technique. It involves responding to an anomalous connection to report the presence of an attack pattern or profile on the network. One of the main approaches to cyberattack detection is intrusion detection. Intrusion detection is the process of determining the signature of an intrusion or attack in a continuous stream of connections (Putjato and Makarjan, 2020) Intrusion detection systems (IDS, Intrusion detection system) operate based on three main approaches: the signature-based approach, the anomaly-based approach, and the hybrid approach. While misuse detection takes into account signatures of known attacks to help detect intrusions, anomaly detection uses profiles of normal network activity to flag intrusions in which a deviation from the normal profile is detected. Combining these two approaches results in a hybrid approach (Putjato, et al., 2020). However, some approaches based on these 3 main approaches have proven to be largely ineffective in terms of attack detection, while some have resulted in high consumption of computing resources. Similarly, most of the approaches proposed in the extant literature are computationally infeasible and can only remain theoretical.

3 DETECTION WITH MACHINE LEARNING

Recently, machine learning techniques have become popular in the detection of cyber attacks. Machine learning is particularly effective for analyzing data and predicting the outcome of certain events based on the available sample inputs, which are used to build a suitable model to make the right decisions (Aissa and Guerroumi, 2016). The main tasks of machine learning algorithms are classifying and predicting the presence or absence of a known instance of an incident using data for learning. The application of machine learning in today's cyberattack detection scenario has helped to greatly improve the detection process. In this paper, we will look at the application of a Bayesian (probabilistic) model to information security incident detection. There are 3 main types of machine learning.

Machine Learning:

1. Supervised Learning

Good for tasks where every input data point is labeled or belongs to a certain category (Kim G., Lee and Kim S., 2014).

2. Unsupervised Learning

Good for tasks where all data are not labeled or do not belong to a certain category. Algorithms are used for clustering/grouping complex data into classes (Yoo et al., 2014).

3. Reinforcement Learning

Good for tasks where future actions are based on the results of current reactions, and the next actions need to be predicted (Rani and Xavier, 2015).

4 A PROBALISTIC METHOD FOR DETECTING INCIDENTS. BUILDING A BAYESIAN NETWORK

Bayesian networks form an important part of all types of machine learning, combining the fields of probability theory and graph theory to solve problems of uncertainty and complexity. They are one of the graphical probabilistic models that allow a compact representation of the probability distribution of simultaneous occurrences of controllable events (Lin, Ke and Tsai, 2015). The advantage of Bayesian networks is their relative intuitiveness for humans, as it is easier to understand the direct relationships between events and local probability distributions than the resulting probability distributions of multiple events occurring simultaneously. A Bayesian network (or causal network) is represented as an oriented acyclic graph (DAG) (Shapoorifard and Shamsinejad, 2017). Each node in this graph is a variable that has certain states. Directional edges in this graph represent relationships between variables - if there is a directional edge between two variables, then one depends on the other. If there is no relationship between two nodes, this does not mean that they are completely independent, because they can be connected through other nodes. However, they can become dependent or independent depending on the evidence set on the other nodes. Nodes and connections build the structure of a Bayesian network, and is called a structural specification (Song, 2013). This model consists of several parameters. The first is the a priori probability of parent nodes, which do not depend on any states.

Each child node has a conditional probability table (CPT), which specifies the prior relationship between the node and its parent. Each element of the conditional probability table is defined:

$$CPT_{ij} = P(daughter\ state = j | parental\ state = i)) \quad (1)$$

Some variables may have certain values that were obtained by observation. Let be the set of observed variables and Y_0 - be the corresponding set of values. Let X be the set of variables we are interested in. The conclusion is the process of calculating the posterior probability $P(X|Y = Y_0)$ (Abduvaliyev et al., 2013). The posterior probability $P(X|Y = Y_0)$ is determined using:

$$P(X|Y = Y_0) = \frac{P(X,Y=Y_0)}{P(Y=Y_0)} \quad (2)$$

In this paper we consider only a finite set $U = \{X_1, \dots, X_n\}$ of discrete random variables, where each variable X_i can take values 0 or 1. In our case, these random variables will be aggregate warnings or hyper-warnings. We define that each node in the causal network has a binary state, i.e., 1 or 0. A value of 1 represents a warning in the node being raised, while a value of 0 indicates that it does not. Because variables are discrete, conditional probability tables contain the probability that a variable will contain one of all possible values for each combination of its parent values. To generate a Bayesian network, causal relationships and conditional probabilities between hyper-alerts are required (Butun, Morgera and Sankar, 2014). Thus, the data from the previous subsection written in the table will be used causal_relationships. The procedure for creating a Bayesian network is shown below. The Bayesian network creation method accepts three input parameters: (I) agr_alerts_all, (II) correlated_alerts и (III) causal_relationships. The result of this process is a Bayesian hyper-alert network (Ashfaq et al., 2017). The stages of constructing a Bayesian network are as follows:

Step 1: For each causal relationship between hyper-alerts x_i and x_j in the correlated_alerts table, a directed edge $x_i > x_j$ is generated..

Step 2: Each node in the Bayesian network has a conditional probability table (CPT). This table displays the probability of a node given the values of its parent nodes (Han et al., 2016). After all edges were added to the network in step 1, a method was used to generate a conditional probability table for each node. This method was introduced in:

$$P\left(x_j \middle| P_a(x_j)\right) = \begin{cases} 0, \forall_{x_i} \in P_a(x_i), x_i = false \\ P\left(\cup_{x_{i=true}} t_i\right) = 1 - \sqcap_{x_i=true} (1 - P(t_i)) \end{cases} \quad (3)$$

In this function x_i indicates the values of the variables in the parent nodes $P_a(x_j)$ x_j. The variable t_i denotes a transition that changes the state of the network from x_i to x_j, where $x_i \in P_a(x_i)$. Using this formula, each field in the conditional probability table at node x_j is computed based on the values in the parent nodes. It follows from this procedure that if all parent nodes have a value of 0 and no such warnings have occurred, then the child node cannot receive a warning either, and the value in the corresponding field will be 0. This procedure resulted in a Bayesian network with conditional probability tables due to different parent states in each node.

Based on the Bayesian network created, we can then calculate the probability of a particular warning occurring given other warnings using Bayesian inference. After the intrusion system generates one or more warnings, we can calculate the so-called posterior probability, which is the probability that any other condition will occur. With this knowledge, the system administrator can take precautions to reduce the risk of a successful cyberattack that would otherwise cause more damage.

All steps can be represented as a Bayesian Web of Trust, which can help determine the necessary calculations to get a confidence value that an attack is underway and an alert needs to be sent out. Let's take the raw alert data from one of the modules with a standard value of 0.5. To calculate the reliability of data received from modules, we will use the classical Bayesian trust network construction methodology. Given that the notification is sent only when there is a positive signal from each of the modules, let us set the appropriate values for the matrix. (Figure 1).

aqr_alerts_all	correlated_alerts	causal_relationships	ALARM SYS = Alarr	ALARM SYS = Dont
alarm	alarm	alarm	1	0
alarm	alarm	no alarm	1	0
alarm	no alarm	alarm	1	0
alarm	no alarm	no alarm	1	0
no alarm	alarm	alarm	1	0
no alarm	alarm	no alarm	1	0
no alarm	no alarm	alarm	1	0
no alarm	no alarm	no alarm	0	1

Figure 1: Matrix of matching values.

Using a standard probability value of 0.5, we obtain the following results for the validity of the entire module network:

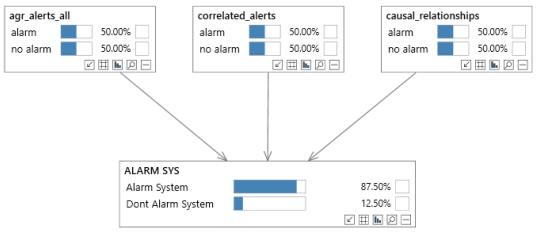

Figure 2: Bayesian trust network $P(X|Y = Y_0)$.

When using the classical trust network scheme, it is possible to specify the degree of interaction between the signals received from the modules. In this case, if at least one of the modules of the complex system receives an alert, a hyper-alert is formed for the specialist. When using the proposed scheme of processing and alerting, the reliability of the result is more than 80%.

5 CONCLUSIONS

In the context of cyberspace protection, it is important to have a reliable and stable mechanisms for detecting and predicting the likelihood of an attack in a typical network environment. Varying network configurations represent different activity profiles and behavioral attributes of users and software. To achieve an effective mechanism in this direction, a cascade of multiple layers of non-linear processing components is required, which can be useful for extracting and transforming attributes to interpret dynamic network profiles. Responding quickly to security incidents is necessary to minimize the damage caused by security incidents to the organization. The primary goal of the organization is to be as prepared as possible to handle security incidents, and to prevent them by proactive actions. Transitioning from reactive approach to proactive one is currently a challenge in the sphere of cybersecurity research.

The goal of constructing a Bayesian network was to develop a model that, based on an attack prediction, could determine the initial stages of an attack. The model proposed does not only include the aggregation of alerts, but also their correlation. We used the proposed attack model to predict the attack itself. This research can be extended in the future. There are several problems left to be solved in the future work. One of them is the processing and prediction of events even if there are cycles in the attack graph. This case is problematic, since many computational models accounting for acyclic graphs cannot be used. Therefore, it may be worthwhile to test another method. For example, using an attack graph simulation or a hidden Markov model. The second problem, which this study presents, is the creation of a complex and complete data set. To our knowledge, no suitable dataset has been created to date that emphasizes attacks. Therefore, it is important to form a dataset that would contain attacks covering all detectable attack stages.

REFERENCES

Buczak, A. L. and Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection, *IEEE Communications Surveys & Tutorials,* 18(2): 1153-1176.

Akyazi, U. (2014). Possible scenarios and maneuvers for cyber operational area. In *European Conference on Cyber Warfare and Security, Academic Conferences International Limited*, Greece.

Putjato, M.M. and Makarjan, A.S. (2020). Kiberbezopasnost' kak neot#emlemyj atribut mnogourovnevogo zaschischennogo kiberprostranstva. *Prikaspijskij zhurnal: upravlenie i vysokie tehnologii,* 3(51): 94-102

Putjato, M.M., Makarjan, A.S., CHerkasov, A.N. and Gorin, I.G. (2020). Adaptivnaja sistema kompleksnogo obespechenija bezopasnosti kak jelement infrastruktury situacionnogo centra. *Prikaspijskij zhurnal: upravlenie i vysokie tehnologii*, 4(52): 75-84

Denning, D. E. (2014). Framework and principles for active cyber defense. *Computers & Security*, 40: 108-113.

Aissa, N. B. and Guerroumi, M. (2016).Semi-supervised statistical approach for network anomaly detection. *Procedia Computer Science*, 83: 1090-1095.

Kim, G. Lee S. and Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection, *Expert Systems with Applications*, 41(4): 1690-1700.

Yoo, S. Kim, S., Choudhary, A., Roy, O.P. and Tuithung, T. (2014). Two-phase malicious web page detection scheme using misuse and anomaly detection. *International Journal of Reliable Information and Assurance*, 2(1): 1-9.

Rani, M. S. and Xavier, S.B. (2015). A Hybrid Intrusion Detection System Based on C5. 0 Decision Tree Algorithm and One-Class SVM with CFA. *International Journal of Innovative Research in Computer*, 3(6): 5526-5537.

Lin, W. C., Ke, S. W. and Tsai, C. F. (2015). CANN: An intrusion detection system based on combining cluster centers and nearest neighbors. *Knowledge-based systems*, 78: 13-21.

Shapoorifard, H. and Shamsinejad, P. (2017). A Novel Cluster-based Intrusion Detection Approach Integrating Multiple Learning Techniques. *International Journal of Computer Applications*, 166(3): 13-16.

Song, J., Takakura, H., Okabe, Y. and Nakao, K. (2013). Toward a more practical unsupervised anomaly detection system. *Information Sciences*, 231: 4-14.

Abduvaliyev, A., Pathan, A. S. K., Zhou, J., Roman, R. and Wong, W. C. (2013). On the vital areas of intrusion detection systems in wireless sensor networks. *IEEE Communications Surveys & Tutorials*, 15(3): 1223-1237.

Butun, I., Morgera S.D. and Sankar, R. (2014). A survey of intrusion detection systems in wireless sensor networks. *IEEE communications surveys & tutorials*, 16(1): 266-282.

Ashfaq, R. A. R., Wang, X. Z., Huang, J. Z., Abbas, H. and He, Y. L. (2017). Fuzziness based semi-supervised learning approach for intrusion detection system. *Information Sciences*, 378: 484-497.

Han, Y., Alpcan, T., Chan, J., Leckie, C. and Rubinstein, B. I. (2016). A game theoretical approach to defend against co-resident attacks in cloud computing: Preventing co-residence using semi-supervised learning. *IEEE Transactions on information Forensics and Security*, 11(3): 556-570.