Challenges and Issues of Modern Science, 3 (2024). ISSN: 3083-5704
URL: https://cims.fti.dp.ua/j/article/view/197
PURL: https://purl.org/cims/2403.021

Prediction of Network Threats and Attacks by Mathematical Simulation

Daniil Doroshenko

Purpose. The purpose of the article is a comprehensive study of modern methods of mathematical modeling of network threats and attacks, as well as studying their effectiveness. **Design / Method / Approach.** The research uses mathematical methods such as probability theory, game theory, graph models, and statistical approaches to build models that allow to reproduce the dynamics of threats in real networks. The methodology is based on modeling various attack scenarios, affecting information security. **Findings.** The study showed that mathematical models do not allow analyzing complex network processes, predicting the emergence of new threats and identifying vulnerabilities in networks. Using these models makes it possible to create precise algorithms to prevent attacks, which in turn achieve the reliability and security of the network infrastructure. **Theoretical Implications.** The research contributes to the development of theoretical knowledge about the application of mathematical methods in cyber security, especially in the conditions of the constant expansion of network threats. The models presented in the work offer new ways of assessing risks and analyzing attacks. **Practical Implications.** The proposed approaches can be used by network administrators and cyber security specialists to develop effective strategies for protecting information systems. Mathematical modeling allows not only to analyze existing threats, but also to predict the emergence of new ones. **Originality / Value.** The article is distinguished by its originality due to the integration of various mathematical approaches in the study of network threats. This research provides a unique opportunity to gain a deeper understanding of the nature of cyberattacks, making it a valuable resource for security professionals. **Research Limitations / Future Research.** The study has a limitation related to the fact that the presented models apply only to certain types of network threats. In future research, it is advisable to extend these models for other forms of attacks and explore the possibilities of their integration into different systems**. Article type.** Review of Methods.

Keywords:

mathematical modeling, network threats, cyberattacks, information security, critical infrastructure, threat prediction

Contributor Details:

Daniil Doroshenko, Undergraduate Student, Oles Honchar Dnipro National University: Dnipro, UA, daniil427dorosh@gmail.com

The work considers some basic methods of mathematical modeling, namely stochastic models, game theory and graph theory. Other techniques, such as neural networks or artificial intelligence techniques, were excluded not because they have no value, but because this study focuses on more established mathematical approaches. These approaches provide a strong theoretical foundation and are easier to integrate into existing cybersecurity systems without requiring complex computing resources. Mathematical modeling is a key tool in cyber security, as it allows creating abstract models of real network processes and, ultimately, better understanding attack mechanisms and developing strategies to prevent them. Among the main research methods that will be considered are stochastic models used to describe random processes in networks; probability theory for analyzing the probabilities of random events in networks; game theory, which models conflicts between attackers and defenders in the form of a game; and graph theory, which analyzes the structure of a network, particularly its nodes and connections.

Also, the study will be devoted to the simulation of DDoS type, which is one of the most progressive and destructive cyber threats. The use of mathematical approaches makes it possible to better check the mechanisms of such attacks and identify their weak points. Next, mass service theory techniques will be presented to analyze request flows that exceed normal downloads, as well as stochastic models to help estimate the probability of a successful attack. This will help to understand the system of behavior during an attack and develop effective defense strategies.

It will also explore the application of game theory, which is ready to model the interaction between the attacker and the defender as a strategy that allows finding optimal solutions for both sides. The models used in this study allow not only to better understand the nature of cyber threats, but also to develop new, more effective strategies for protecting network systems, which have important practical significance for modern information technologies.

Objectives and Tasks

The purpose of this research is to explore mathematical modeling techniques for assessing and mitigating network threats, with a particular focus on DDoS attacks. The main tasks are as follows. Overview of basic mathematical modeling techniques such as stochastic models, probability theory, game theory, and graph theory. Simulation of DDoS attacks and assessment of their impact on the network. Evaluation of the applicability of mass service theory for network traffic analysis during attacks. Development of models using game theory to simulate the interaction between attackers and defenders. Creation of effective defense strategies based on the proposed models.

Materials and Methods

The work uses several methods of mathematical modeling, in particular:

Stochastic models for estimating random processes in networks, such as traffic fluctuations during attacks.

Probability theory for analyzing the probabilities of various threats.

Game theory for modeling conflicts between attackers and defenders in the form of a mathematical game.

Graph theory for analyzing the structure of networks and identifying critical nodes and paths that may be vulnerable to attacks.

Mass service theory methods for analyzing the impact of large volumes of requests during DDoS attacks.

Basic methods of mathematical modeling

As is known from various sources, quite different mathematical approaches are used to model network threats. They can usually reproduce some abstract models of real network processes. It is clear that they help to better understand attack mechanisms and develop effective strategies to prevent them. I will give some examples of the main methods of mathematical modeling.

Stochastic models. They are used to describe random processes in networks, which may include communication interruptions, abnormal delays, or other random situations. I would like to point out that these models cannot be analyzed, in case random factors can affect the operation of the network and the preparation of attack scenarios. It is worth noting that stochastic models are particularly useful for studying dynamic processes, such as fluctuations in network traffic during attacks, which usually cause random or variable intensity of attacking actions. They also help conditionally predict how the network will behave in random scenarios and how it can be minimized.

Analysis of the system using state transitions aimed at identifying the intrusion has the advantage that it is independent of the signature analysis and is formed on individual transitions of the system. It is more effective especially if there is a modification of intrusions with a known signature (Литвинов et al., 2018).

The theory of probabilities. It is one of the most advanced mathematical approaches for the analysis of random events in networks.

Game theory. Used to simulate conflicts between an attacker and a defender as a game with two players. It allows you to simulate different options of attacks and determine the most likely strategies of attackers. It is entirely up to defenders to predict the actions of attackers and build optimal methods of protection.

Graph theory. Investigates the structure of a network in which the elements are various components, such as servers, routers, computers, and the connections between them are already data transmission channels (Петрик & Дубровін, 2021).

It is worth noting that each of these mathematical methods will help us to better understand attack mechanisms and develop effective strategies to protect network systems from threats.

Simulation of a DDoS attack

Let's consider what a DDoS attack is. Distributed Denial of Service is a certain type of cyberattack in which attackers try to overload a network system with

many requests, making it inaccessible to ordinary users. It is clear that different mathematical approaches are used to model such attacks, which allow us to better define the mechanism.

Let's consider some approaches.

Theory of mass service. This approach is used to model processes in systems that process a large volume of requests. In the context of DDoS attacks, the theory of mass serving allows us to analyze how request flows significantly exceeding the normal load can cause the system to fail.

In a DDoS attack, a system that was designed to handle requests from legitimate users suddenly stops doing so, or does so with significant back-ups, equivalent to a denial of service (Горобець et al., 2023).

Among the main factors that are considered in such modeling are the speed of the system response, the number of attackers and, of course, the traffic intensity.

Consider stochastic models. Stochastic models are used to analyze random processes occurring during the attack itself. They can estimate the probability of load distribution and the probability of a successful attack.

Thus, mathematical models help to better understand the behavior of the system during a DDoS attack and effectively defend against them, predicting the consequences and developing protection strategies.

Simulating attacks using graphs

Note that graph theory provides us with a powerful tool for modeling and analyzing network attacks. They represent networks as graphs, where nodes are servers, routers, or other infrastructure elements, and edges are data channels. This approach makes it possible to simulate attacks, assessing their impact on the network and identifying vulnerabilities.

Let's consider the main aspects of simulating attacks on graphs: Identification of critical nodes and paths. With the help of graphs, you can configure critical points in the network. If these elements are attacked, the effect on the network will be the most destructive (Хавер & Савченко, 2023).

Analysis of threats such as data interception or modification. By simulating attacks, it is possible to assess which parts of the network are most favorable for data interception or data modification.

Simulating attacks to identify vulnerabilities. With the help of graph models, it is possible to simulate various types of attacks - DDoS, data interception, routing attacks, etc. These are individual nodes or edges that are most at risk.

Defense strategy. After identifying vulnerable network elements, strategies can be developed to protect them. This may include isolating key nodes, reserving data transmission channels, and simulating an attack using graphs.

Using game theory to analyze attacks

It is clear that game theory provides us with a powerful tool for modeling and analyzing the interaction between an attacker and a defender in a system. This approach allows you to consider time as a mathematical game, where the player

has his own goals and strategies.

Game simulation. In this context, the game consists of two main players: the attacker and the defender. An attacker aims to penetrate or disrupt a system, while a defender aims to prevent such attacks and ensure the security of the system. Each player chooses strategies to achieve their goals (Яценко et al., 2022).

An attacker can choose different methods of attack, while a defender has many defense options, from changing access policies to implementing new technologies.

Analysis of Nash equilibrium. This analysis is a key aspect in this context. A Nash equilibrium is reached when one of the players cannot improve his outcome by changing his strategy while the other players' strategies are fixed. This allows you to determine the optimal strategies for both pages. In cases with attacks, Nash equilibrium analysis allows strategies to be set up that maximize the probability of a successful attack for the attacker while providing the best defense for the defender.

Mixed strategic planning. This is one of the approaches to the optimization of the defense strategy is the use of mixed strategies. The defender can change the access or routing policy in a way that complicates the attacker's task. For example, the defender can immediately change the network configuration, use different authentication methods, or implement new intrusion detection systems (Коробейнікова & Цар, 2023).

This creates a dynamic environment where attacks remain less predictable, making them more difficult to implement.

In general, the use of game theory in attack analysis can better understand the available attack scenarios and accordingly achieve a defense strategy, creating a system that is more resistant to the threat.

Forecasting threats using statistical methods

Let's consider some key aspects.

Data collection is the first stage of large amounts of data about network traffic, system events, and user activity.

Data analysis is the second stage. In this step, mathematical statistical methods, in particular machine learning methods, are used to analyze this data. One popular approach is to use algorithms to detect anomalies that may indicate a threat. For example, clustering techniques can help divide data into groups where normal traffic will be separated from abnormal traffic.

Modeling is the third stage, where models that learn from historical data are created to predict possible threats. Regression analysis allows you to assess how various factors can affect the probability of a threat (Мєшков, 2023).

Early warning is the fourth stage, where the results of modeling and design analysis are used to create an early warning system. This allows you to detect any threats in time before they lead to serious consequences. Such systems can automatically generate alarms or even initiate automatic measures for protection.

Adaptation and improvement are the fifth, last stage. Over time, as more data is collected and new types of threats emerge, the models can be updated and

refined to improve their accuracy and effectiveness. Regular retraining of models for new data supports maintaining their relevance and adaptability to new threats.

There is a reason to claim that it is practically impossible to get rid of the destructive influence of cyberattacks. However, certain general methods for mitigating their negative consequences are proposed (Толюпа et al., 2021).

Thus, statistical methods create a powerful tool for forecasting and early detection of threats that allow organizations to respond to your attacks in time and reduce risks to their information systems.

Results

The main results of this study are the following.

Development of new models based on stochastic processes for analysis of threats in networks and simulation of DDoS attacks. A personal contribution arose in the integration of mass service methods for traffic simulation during attacks, which allows more accurate assessment of the impact of congestion on network resources.

Using graph theory to model network attacks and identify critical points in the network structure. This work offers new approaches to identify bottlenecks and vulnerable network components that may be particularly vulnerable during a cyber-attack.

Analysis of the interaction between the attacker and the defender using game theory. A new model has been proposed that treats attack and defense as a strategic game where both sides can make optimal decisions based on mathematical modeling. This makes it possible to better predict the possibilities of action of the attacking side and optimize defense strategies.

Application of mass service theory to evaluate the effectiveness of network resources during reboot attacks. The analysis of the behavior of the network under load has been updated due to the introduction of new traffic estimation models that go beyond normal operating conditions.

Conclusion

So, after conducting an analysis and working on this topic, it can be stated that mathematical modeling is a powerful tool in the field of cyber security, and its application for analyzing and countering attacks will significantly strengthen the protection of information systems. This paper presents four key methods of mathematical modeling, each of which plays an important role in the development of security strategies.

First, modeling a DDoS attack allows you to study in detail the mechanisms and impact of such attacks on systems and networks. The author's contribution turns into the use of bulk service theory for a detailed analysis of network behavior during reboot attacks. This provides new insights into how denial-of-service attacks affect system resources and performance.

Secondly, modeling attacks using graphs allows you to visualize and analyze the structure and dynamics of attacks. New methods of assessing bottlenecks and

vulnerabilities in networks have been proposed to help design critical components that require special protection. This innovation achieves the accuracy and efficiency of network threat analysis.

The third important aspect is the use of game theory to analyze attacks. Game theory allows modeling the interaction between attackers and defenders as a game where each side tries to optimize its strategy. A personal contribution in this area works in the development of a new game model that allows you to place optimal defense strategies in the conditions of different attack scenarios.

Finally, is the prediction of statistical threats using methods. Statistical analysis of historical data on attacks and threats allows you to identify trends and the probability of the appearance of new threats. The contribution comes precisely in the integration of these methods to create accurate models for predicting threats and implementing proactive protection measures.

Thus, approaches to cyber threat modeling are proposed in the work to provide a comprehensive view of the problem and it is possible to create more accurate and effective protection strategies, develop new security technologies and ensure reliable protection of information systems in the conditions of a complex and dynamic cyber environment.

References

Горобець, В. І., Дубровін, В. І., & Твердохліб, Ю. В. (2023). Виявлення несанкціонованих дій та атак в мережах методом вейвлет-аналізу. *Applied Questions of Mathematical Modeling, 5*(1), 9–20. https://doi.org/10.32782/mathematical-modelling/2022-5-1-1

Коробейнікова, Т., & Цар, О. (2023). Аналіз сучасних відкритих систем виявлення та запобігання вторгнень. *Grail of Science, 27*, 317–325. https://doi.org/10.36074/grail-of-science.12.05.2023.050

Литвинов, В. В., Стоянов, Н., Скітер, І. С., Трунова, О. В., & Гребенник, А. Г. (2018). Аналіз систем та методів виявлення несанкціонованих вторгнень у комп'ютерні мережі. *Математические машины и системы*, (1), 31-40. http://dspace.nbuv.gov.ua/handle/123456789/132008

Мєшков, В. (2023). Аналіз систем інтелектуального моніторингу трафіку комп'ютерної мережі для систем виявлення атак. *Information Technology: Computer Science, Software Engineering and Cyber Security*, (1), 85-92. https://doi.org/10.32782/IT/2023-1-11

Петрик, Б. В., & Дубровін, В. І. (2023). Виявлення атак типу DOS в мережевому трафіку за допомогою вейвлет-перетворення. *Applied Questions of Mathematical Modeling, 4*(1), 186–196. https://doi.org/10.32782/kntu2618-0340/2021.4.1.20

Толюпа, С., Лукова-Чуйко, Н., & Шестяк, Я. (2021). Засоби виявлення кібернетичних атак на інформаційні системи. *Information and Communication Technologies, Electronic Engineering, 1*(2), 19–31. https://doi.org/10.23939/ictee2021.02.019

Хавер, А.В., Савченко, В. А. (2023). Математична модель захисту об'єкта критичної інфраструктури від троянських програм. *Modern Information Security, 55*(3), 12–21. https://doi.org/10.31673/2409-7292.2023.030002

Яценко, А. К., Дубровін, В. І., & Дейнега, Л. Ю. (2023). Аналіз трафіку програмно-визначених мереж за допомогою ентропії. *Applied Questions of Mathematical Modeling, 5*(1), 108–114. https://doi.org/10.32782/mathematical-modelling/2022-5-1-14