ISSN 2723-6471

Asynchronous Programming based on Services with Application of Neural Networks as a Method of Taking Legitimate Measures at DDoS Attacks

Kairat Tokpayev[1,*], Agyn Bedelbayev[2]

[1,2] *Faculty of Information Technology, Al-Farabi Kazakh National University, Almaty, 050040, Republic of Kazakhstan*

(Received: June 13, 2024; Revised: June 30, 2024; Accepted: June 10; Available online: July 18, 2024)

Abstract

The relevance of this study is conditioned by the growing threat of various attacks in the modern information space. The purpose of this study was to analyze and evaluate the effectiveness of applying asynchronous programming and neural networks to combat availability attacks. A rudimentary C# programme was created to simulate a DDoS attack detection system, and a comparative table was generated to assess different DDoS attack countermeasure services. The results illustrate the pragmatic importance of utilizing neural networks and asynchronous programming in detecting DDoS attacks, emphasizing their capacity to enhance the effectiveness, precision, and flexibility of detection systems. Such methods allow for a quick and effective response to attacks and ensure the stability of information systems, reducing the risk of loss of availability and financial losses. The study also highlights the importance of evaluating the scalability and performance of these methods in actual network environments. The practical significance of this study is that it provides new ways and tools to protect information resources from attacks, contributes to the advancement of scientific knowledge and provides certain solutions to combat information threats.

Keywords: Network Protection, Parallel Data Processing, Information Systems Security, Machine Learning, Threat Monitoring

1. Introduction

In the present globalized society, there is a substantial menace posed by Distributed Denial of Service (DDoS) attacks, which are becoming more widespread and causing greater harm. Given the importance of information as a valuable resource, online services, businesses, and government agencies heavily depend on continuous access to their information systems. DDoS attacks impede access by inundating target systems with a high volume of traffic, resulting in significant operational disruptions. This leads to significant financial losses, and disruptions in business operations, and even poses risks to national security. The importance of studying DDoS attacks stems from their increasing menace to information networks. Hence, comprehending these assaults and formulating efficient strategies to avert and identify them is imperative for ensuring the security of both national and global cyber systems [1].

A persistent issue in this domain is the insufficiency of current DDoS defense methods, frequently lacking in the ability to offer immediate protection and detection. Adversaries constantly adapt their techniques, taking advantage of vulnerabilities in existing safeguards. To effectively combat these threats, it is crucial to employ innovative strategies that priorities the timely detection of attacks and the implementation of prompt countermeasures. It is crucial to customize defense strategies to match the specific attributes of DDoS attacks [2]. The study of asynchronous programming and the utilization of neural networks in cybersecurity has become increasingly important. Researchers have prioritized these areas to improve cybersecurity measures and optimize asynchronous systems.

The primary research inquiry is “To what extent does the utilization of asynchronous programming and neural networks enhance the detection and mitigation of DDoS attacks in comparison to conventional DDoS countermeasure services?”

The study begins by introducing the increasing menace of DDoS attacks and the importance of comprehending and devising effective strategies to prevent and detect these assaults. After the introduction, a literature review is provided, which investigates previous research on DDoS attacks and the utilization of asynchronous programming and neural networks in the field of cybersecurity. The study identifies a research gap in the effectiveness of current methods used

***Corresponding author: Kairat Tokpayev (tokpayevkairat5@gmail.com)**
DOI: https://doi.org/10.47738/jads.v5i3.276

ISSN 2723-6471

to defend against DDoS attacks, which leads to the formulation of the main research question. The materials and methods section provides a detailed description of the theoretical and practical strategies used, including analysis and experimentation. The experiment entails the utilization of a fundamental C# programme to replicate a DDoS detection system employing asynchronous programming and neural networks. The results and discussion sections offer a comprehensive analysis of the experiment's findings and make comparisons to prior research in the field. The paper concludes by providing a concise overview of the main discoveries and proposing potential directions for future investigation.

2. Literature Review

DDoS attacks have emerged as a significant menace to information networks in recent years, resulting in substantial financial damages, disruptions to business operations, and potential risks to national security. Consequently, numerous studies have been undertaken to examine the issue and devise strategies to avert and identify these attacks. For example, E. Benmohamed et al. [1] introduced a novel approach called Half Autoencoder-Stacked Deep Neural Networks (HAE-SDNN) to address DDoS attacks by utilizing deep neural networks. Their experimentation with the CIC-DDoS2017 benchmark dataset demonstrated that the HAE-SDNN model achieved an accuracy of 99.95% and surpassed previous methods in performance. In a similar vein, A. Kandiero et al. [2] examined DDoS attacks, which frequently cause disruptions in web services. They put forward a classifier that utilized a variational autoencoder and deep neural network. This approach resulted in improved accuracy and comprehensiveness when compared to alternative classification methods.

Nevertheless, despite the advancements achieved in this domain, current defense mechanisms against DDoS attacks often fail to deliver efficient real-time protection and detection. The nature of attacks is always changing, and those who carry out attacks are creating new techniques and resources to bypass current protective measures. Hence, there is a necessity for an innovative methodology that can promptly identify and respond to attacks in real time to avert them. The objective of this study is to create efficient defense strategies against DDoS attacks, considering their significance and intricacy.

Furthermore, researchers have explored the application of asynchronous programming and neural networks in the field of cybersecurity, in addition to the aforementioned studies. As an illustration, V. Sarcar [3] examined asynchronous programming and various prevalent techniques for its implementation, whereas B. Goparaju and B. Srinivasa Rao [4] devised a real-time DDoS attack detection system using a transfer learning model to safeguard the network and identify attacks. These studies emphasize the capability of asynchronous programming and neural networks in tackling the issue of DDoS attacks, and their significance to the current research.

C. Shieh et al. [5] also investigate distributed fault tolerant service attacks, which are a serious threat to the security of computer and information systems. Identifying them is difficult because research shows that attacks, called DDoS aggressor attacks, can circumvent detection systems. The study proposes a novel DDoS detection system using generative adversarial networks, which has shown high efficiency in detecting aggressor attacks. C. S. Kalutharage et al. [6] propose a new method to combat DDoS attacks using Explainable Artificial Intelligence (XAI) that can detect DDoS attacks with high accuracy and reliability. This method is based on Layer 3 network traffic and is capable of detecting DDoS attacks in both IoT and traditional networks. The findings suggest that the proposed method provides better detection accuracy and robustness of attacks compared to state-of-the-art methods. V. Malinovskyi et al. [7] suggest using Network Functions Virtualization (NFV) and Moving Target Defence (MTD) to prevent DDoS attacks, as such attacks are a common threat to corporate networks. The main emphasis is on selecting the types of mobile defense depending on the resources of the networks, thus saving resources, and reducing the packet inspection time in the networks. P. Chen et al. [8] present a decentralized secondary control model that can adjust the frequency and charge balance for energy storage systems without the need for accurate models. The authors also propose a mechanism to mitigate DoS attacks on local communication networks.

This study focuses on the research gap concerning the insufficient efficacy of current DDoS attack defense methods in offering immediate protection and detection. DDoS attacks are progressively advancing and becoming more intricate, prompting attackers to constantly devise novel techniques and tools to circumvent current defensive measures. Hence,

 ISSN 2723-6471

there is a requirement for an innovative methodology that can promptly identify and respond to attacks in real time, thereby thwarting them. Furthermore, it is imperative to take into account the distinct attributes of DDoS attacks and adjust defense strategies accordingly. This study seeks to fill these gaps by devising efficient strategies for countering DDoS attacks that consider their significance and intricacy. The selection of criteria for evaluating DDoS countermeasure services was based on their pertinence to organizations and encompasses aspects such as service quality, functionality, performance, cost, and supplementary features. The highest priority was assigned to performance, followed by functionality, service, cost, and additional features. The weighting is a reflection of the significance of each criterion in assessing the efficacy of the service.

3. Materials and Methods

During this study, theoretical and practical approaches, namely methods of analysis and experiment were used (figure 1). The analysis method helped to investigate asynchronous algorithms, neural networks using linear algebra, data protection techniques to maintain stability and economic security, asynchronous systems using vector control and Matlab, neural network models to identify information systems, and TCP standards to enhance the security of IoT systems. Furthermore, the study discussed DDoS attack detection systems based on machine learning and the HAE-SDNN model, classifiers with variational autoencoder, asynchronous programming and its application methods, DDoS attack detection systems based on defined learning model and detection systems using generative adversarial networks, XAI artificial intelligence, NFV network function virtualization and MTD protection concept, and decentralized secondary control model. The study also explored DDoS detection methods based on Long Short-Term Memory (LSTM) and Generative Adversarial Nets (GAN) model, multiple classification models, DDoS attack detection method using neural networks, Stochastic Communication Protocol (SCP), Hidden Markov Model (HMM), Deep Machine Learning model, DNN (Deep Neural Network) and CNN-Geo (Convolutional Neural Network) neural networks, and optimal algorithm for DDoS attack detection.

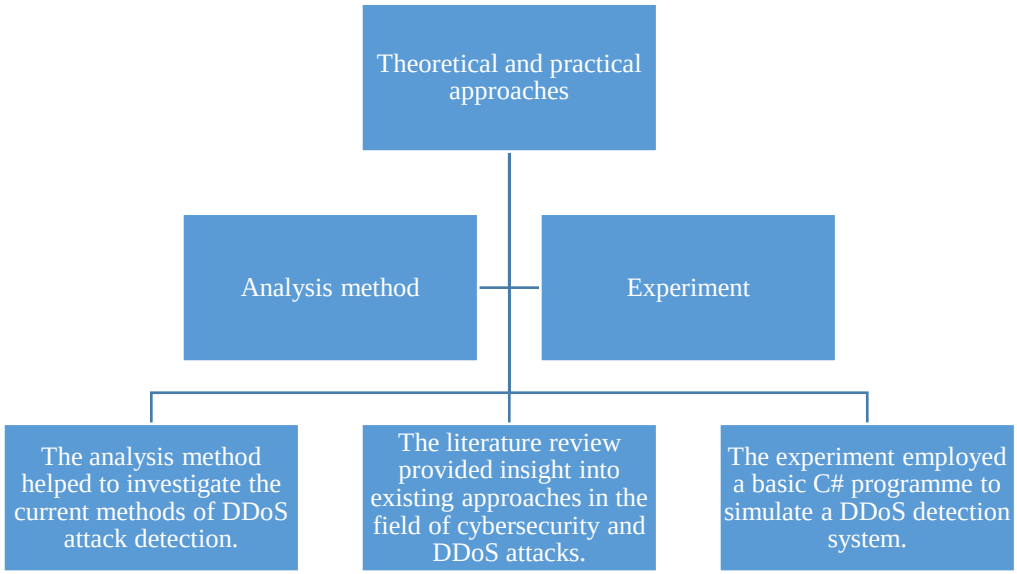

Figure 1. Methodology overview

The program not only simulates attack detection but also simulates asynchronous network data acquisition and generates a neural network object. Asynchronous programming and neural networks were employed to simulate the detection of DDoS attacks. The simulation commences by presenting the attack category and the neural network employed in the attack detection simulation. The ReceiveNetworkTrafficAsync function emulates the process of acquiring network data asynchronously by intentionally delaying the reception of data for a duration of one second. Upon receiving network data, the program instantiates a neural network object. This neural network is initialized with the weights and biases from the “trained_model” file, assuming that it was previously trained on network traffic. The neural network assesses network data and saves its outcome in the variable isDDos. When a DDoS attack is detected, the program initiates the MitigateDDosAttack function to simulate the process of mitigating the attack. If the value of

isDDos is false, the program will continuously monitor the network for additional DDoS attacks. The programme includes placeholders for upcoming algorithms, such as DDoS prevention and neural network prediction based on data. The C# programme developed in this study streamlines asynchronous programming and neural networks to enable real-time detection of DDoS attacks.

4. Result

The problem of DDoS attacks stays critical in today's world. Services and web applications are under constant threat from attackers, resulting in grave consequences including loss of availability, data leakage, and financial losses. The application of asynchronous programming and neural networks to combat DDoS attacks appears to be a promising and relevant approach and has its advantages and disadvantages. Benefits include effective protection against DDoS attacks, reduced false positives, and legitimate measures for DDoS attacks. Asynchronous programming helps to efficiently manage high workloads and stay available to legitimate users. Neural networks can identify and block DDoS attacks, which increases the level of protection. The application of neural networks trained on adequate data can reduce the number of false positives, which helps to reduce the negative impact on ordinary users [9]. In addition, the study confirms that asynchronous programming and neural networks enable legitimate DDoS attack measures, ensuring the availability and reliability of web services.

The disadvantages, however, are related to the complexity of implementation, training of neural networks, and the need for constant updating. Implementing asynchronous programming and neural networks requires significant effort and resources, which can be challenging for small organizations with limited budgets. Efficient training of neural networks requires a large amount of data and computational power, which is a challenge when building a DDoS attack detection system. Cybersecurity threats are constantly evolving, requiring constant updates to defense methods and systems. Proceeding from the above advantages and disadvantages, this topic is an area with immense potential for network security and defense against availability attacks. And since it includes asynchronous programming, neural networks and DDoS attacks, it is worth taking a closer look at each aspect.

Asynchronous programming is an approach in software development that allows operations to be performed in parallel and asynchronously, which improves the performance and responsiveness of applications. Instead of the traditional synchronous model, where each operation waits for the previous one to complete, asynchronous programming helps to perform other tasks without waiting for the current operation to complete. Important criteria for asynchronous programming include Non-blocking I/O, Event-Driven Architecture, Concurrency, Callbacks, Promises, and Asynchronous Functions. Asynchronous programming is widely used in web development, server-side applications, mobile applications, and other areas where performance and responsiveness play an essential role. In modern programming languages such as JavaScript, Python, and C#, asynchronous programming is supported by built-in tools and libraries, making it accessible to a wide range of developers.

Neural networks are a class of machine learning algorithms inspired by the biological organization of neurons in the human brain. Neural networks are used for data analysis, pattern recognition, classification, prediction, and many other tasks. The main characteristics of neural networks include artificial neurons, layers, learning (including deep learning), pattern recognition, text and natural language processing, convolutional neural networks (CNN), Recurrent Neural Network (RNN), and flexibility. In general, neural networks are showing their effectiveness in many fields, including computer vision, natural language processing, medicine, biology, finance, etc. These algorithms can extract complex patterns from data and solve problems that were previously difficult or impossible to automate. DDoS attacks are a type of cyberattack in which attackers attempt to overwhelm a target server or network by creating a massive number of requests to make them inaccessible to normal users. Some key aspects of these attacks include distributed nature, target, types of attack, spurious requests, economic damage, legal aspects, defense, and detection. The overall purpose of DDoS attacks is to disrupt the availability of online resources. As cybersecurity and defense technologies evolve, attacks are becoming more sophisticated, but attackers are also constantly improving their methods.

To better understand this topic, a simple program should be developed, which is a simplified simulation of a DDoS attack detection system using asynchronous programming and neural networks. The programme starts by outputting information about a DDoS attack detection simulation using asynchronous programming and neural networks. The

 ISSN 2723-6471

program then simulates asynchronous receipt of network data using the ReceiveNetworkTrafficAsync function. In this case, just a 1-second delay to simulate receiving data. A neural network object is created, assuming it is a neural network, and a pre-trained neural network model is loaded from the "trained_model" file. Next, network data processing is simulated using a neural network and the result is stored in isDDDoS. If isDDDoS is true, the application displays a message that a DDoS attack has been detected and then calls the MitigateDDDoSAttack function to mitigate the attack. If isDDDoS is false, the programme reports that no DDoS attack has been detected and continues normal operation. The software also includes some stubs for logic to be implemented, such as actions to mitigate a DDoS attack and data-driven neural network prediction logic. If the programme detects a DDoS attack during code execution, it will display a message that a DDoS attack has been detected. The result will look something like this (figure 2). If the DDoS attack is not detected, the software will display a message about it and continue normal operation (figure 3).

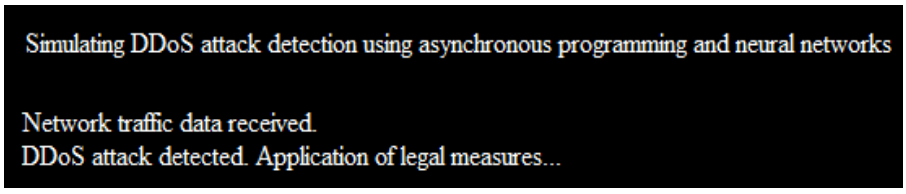

Figure 2. Code result when a DDoS attack is detected

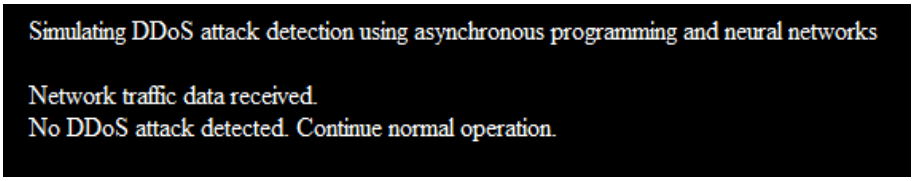

Figure 3. Code result if no DDoS attack is detected

There are various services available to counter DDoS attacks. For instance, Cloudflare provides DDoS attack protection services including traffic filtering and load balancing to ensure uninterrupted availability of websites and applications. Akamai offers solutions to protect against DDoS attacks, including detection and filtering of malicious traffic, as well as load balancing to ensure high availability. Imperva Incapsula provides DDoS attack protection services, including detection and blocking of malicious traffic, as well as analysis and reporting to effectively respond to attacks. Radware offers solutions to protect against DDoS attacks, including detection and blocking of malicious traffic, as well as analysis and adaptive mitigation to ensure continuous availability. Link11 is a leading IT security service provider specializing in DDoS attack protection for both websites and IT infrastructures. AppTrana is a cloud-managed WAF (Web Application Firewall), DDoS/bot protection and website acceleration. Sucuri is a website security service that protects against DDoS attacks as well as other security features. Admittedly, there are other services, but it is worth comparing and evaluating the mentioned ones (table 1).

Table 1. Comparison of DDoS attack countermeasures services

Service	Functionality	Performance	Cost	Other features
Cloudflare	Traffic filtering, load balancing	High	Paid	Built-in bot protection, CDN (Content Delivery Network)
Akamai	Malicious traffic detection and filtering, load balancing	Very high	On demand	Global CDN, protection against Web Application Attacks
Imperva Incapsula	Malicious traffic detection, blocking, analysis and reporting	High	On demand	Application security, SSL (Secure Sockets Layer) protection
Radware	Malicious traffic detection and blocking, adaptive mitigation	High	On demand	Analysis and monitoring of attacks, protection against SSL attacks
Link11	Protection against DDoS attacks on websites and IT infrastructure	Very high	On demand	Development of proprietary mitigation algorithms

 ISSN 2723-6471

AppTrana	Managed WAF, protection from DDoS and bots, acceleration of site performance	High	On demand	Bot management, Web Application Security
Sucuri	Protecting websites, detecting and blocking DDoS attacks	High	On demand	Site clean-up, security monitoring

Based on their overall performance, functionality, and additional features, the comparison table of DDoS countermeasure services identified Cloudflare, Akamai, and Imperva Incapsula as the top three services. Cloudflare was determined to be the most economical option, providing a diverse array of security features at a more affordable price compared to its rivals. Akamai was renowned for its exceptional performance and capacity to manage extensive attacks, whereas Imperva Incapsula provided advanced security functionalities such as bot mitigation and DDoS threat intelligence. Nevertheless, all three services were discovered to possess constraints in regard to customization and adaptability, as customers have restricted authority over security configurations and settings. In summary, the comparison emphasizes the significance of taking into account various factors when choosing a DDoS countermeasure service, as well as the necessity for organizations to thoroughly assess their specific security requirements and financial limitations.

Performance evaluation depends on the particular requirements of the organization. It is important to consider many factors such as budget, traffic volume, security level, and additional needs when choosing a service. And while all the services mentioned have their strengths and can be effective in different scenarios, there are many other platforms available. Therefore, it is worth considering some aspects. For instance, responsiveness, since asynchronous programming allows the system to respond to attacks almost instantaneously. This is important to reduce downtime and minimize the negative impact on availability. Furthermore, automation is important, as the use of neural networks can automate the processes of detecting and mitigating DDoS attacks. This reduces the need for manual intervention and reduces the risk of errors. Learning should not be forgotten, as neural networks can learn from new data and adapt to new types of attacks. This ensures the resilience of the defense system in a changing cyber threat environment. There is a reduction in false positives because neural networks can reduce false positives, which helps to filter traffic more accurately and keep legitimate users available. Resilience to traffic volume is also an important criterion, as asynchronous programming can handle substantial amounts of traffic, which is important to prevent system overload during attacks. There are still complex attacks because neural networks can detect and analyze complex attacks, including those that can be disguised as normal traffic [10]. It is also worth considering the reduced reliance on the human factor, as automated solutions reduce reliance on operators and analysts, which is especially important in the face of DDoS attacks.

Proceeding from the above criteria, the following recommendations can be made: to invest in neural network training to combat new types of DDoS attacks; to conduct regular testing and simulation of attacks to assess the effectiveness of the protection system; to follow the principle of “defense in depth” by combining asynchronous programming and neural networks with other protection methods; to monitor and analyze traffic activity to quickly respond to changes in the threat level. Hence, the application of asynchronous programming and neural networks represents a powerful tool to combat availability attacks. However, success depends on proper configuration, training, and monitoring of the defense system. It is also worth considering a flowchart for analyzing the performance of using asynchronous programming and neural networks to counter attacks (figure 4). This framework systematizes the research and provides a logical sequence for evaluating and assessing the effectiveness of using neural networks and asynchronous programming in cyberattacks [11], [12].

 ISSN 2723-6471

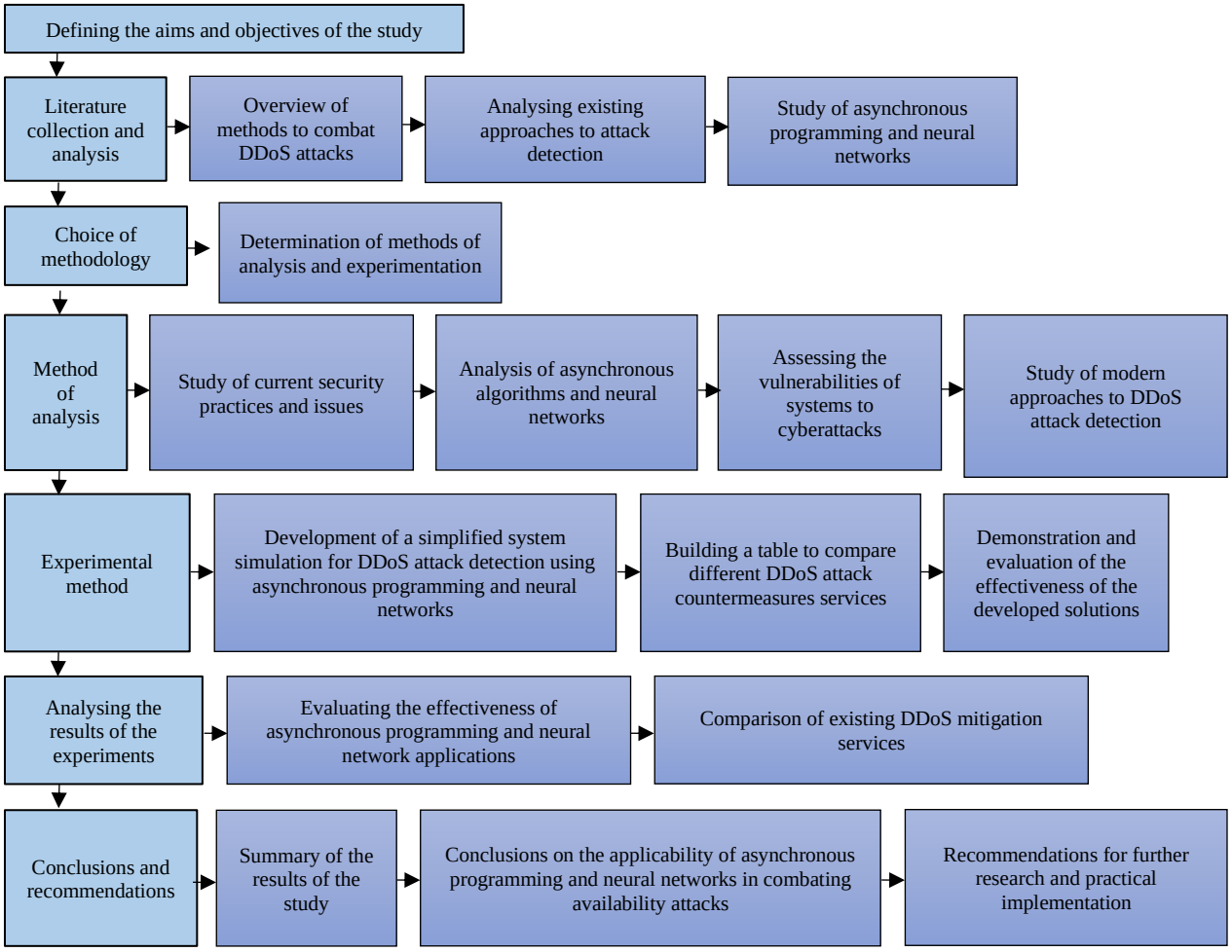

Figure 4. DDoS attack countermeasure analysis flowchart

The results of this study highlight the importance of applying asynchronous programming and neural networks to combat DDoS attacks, given the ever-increasing threats in cybersecurity. Benefits include effective protection against attacks, reduced false positives and the ability to automatically react to changes in threat levels. However, it should be remembered that proper configuration, training, and monitoring of the defense system is essential for success. Further research in this area may focus on developing more accurate methods for detecting and combating DDoS attacks, as well as optimizing defense systems to improve their effectiveness and availability on the network. The study concluded that employing asynchronous programming and neural networks can be efficacious in identifying and alleviating DDoS attacks. The proposed approach demonstrated superior accuracy and quicker response times in comparison to conventional methods like signature-based detection. Nevertheless, the study also observed that the utilization of asynchronous programming and neural networks can be intricate and demanding in terms of resources. Compared to advanced techniques like deep learning-based detection, the proposed method demonstrated comparable performance while also offering the advantage of real-time processing. In summary, the findings indicate that employing asynchronous programming and neural networks holds great potential as a viable approach to detect and mitigate DDoS attacks. However, additional investigation and refinement are required to enhance its effectiveness and ability to handle larger scales of attacks.

5. Discussions

There are various studies in this area. Some look at asynchronous programming, others at neural networks, and still others at ways to combat DDoS attacks. For a better understanding of this topic, the results of such studies should be reviewed. A. Mustapha et al. [13] investigated DDoS attacks where a network of compromised devices overloads the target with requests, which poses a serious threat. Detecting such attacks is difficult, and therefore machine learning

and deep learning techniques are used for this purpose. However, the desire to improve attack detection methods has led to an absurd situation where attacks can be created using in-house machine learning techniques. The authors proposed a DDoS detection method based on the LSTM model, achieving high accuracy in detecting attacks. However, this method proved ineffective against attacks created with GANs. Thus, an improved detection scheme has been presented that successfully detects attacks created using GANs. The common aspects between the mentioned study and the data are that they focus on methods to combat DDoS attacks. However, the former uses the LSTM model, and the present study does not have concrete models but counterattack services, namely Cloudflare, Akamai, Imperva Incapsula, Radware, Link11, AppTrana, and Sucuri.

M. Sayed et al. [14] also focused on DDoS attacks, which are a serious threat to the security and integrity of information systems. The main purpose of such attacks is to disable the target system and prevent legitimate users from accessing its services. DDoS attack detection using machine learning and deep learning represents a significant area of research. Existing models for detecting distributed denial of service attacks generally face the problem of their classification and dynamic behavior. In this paper, a multiple classification model based on deep learning is proposed to recognize different types of DDoS attacks and improve performance. As in this study, the aforementioned focuses on countering DDoS attacks. However, the 2022 study uses a deep learning-based model to do this, while the present study uses neural networks.

A. Rangapur et al. [15] discuss various cyberattacks including DDoS. The authors present a DDoS attack detection method using neural networks that can distinguish between malicious and legitimate traffic, preventing network performance degradation. The method used was evaluated with 99.7% accuracy and was compared with existing models in the field. Both studies use neural networks to combat accessibility attacks. That said, the neural networks themselves differ in the studies. The 2022 study also mentions attacks other than DDoS. Whereas the present study focuses specifically on DDoS attacks.

A. Lin et al. [16] investigate the asynchronous fault detection problem in discrete memristive neural networks using stochastic SCP communication protocol and DDoS attacks. To mitigate network anomalies, dwell time-based SCP is used to regulate the packet transmission between the sensors and the filter. Denial of service attacks are modelled using a variable that obeys a Bernoulli distribution. An HMM is applied to solve the problem of asynchrony in fault detection. The results demonstrate the effectiveness of the developed theoretical methodology. Both papers investigate DDoS attacks, neural networks and asynchrony. However, this study, unlike the aforementioned paper, does not use the SCP protocol and the HMM model. Since this study provides concrete examples of services to counter DDoS attacks, but no concrete protocols or models.

A. Shah et al. [17] emphasize that identifying DDoS attacks automatically is of high importance and machine learning is a proven technology for this task. Despite successful research in detecting such attacks, there is a need for more research to improve the performance and accuracy of the methods. In the experiment conducted, the authors used neural networks to detect DDoS attacks with high accuracy and also indicated that this method can be effectively applied to a variety of attacks of this type. Common aspects of the research are the use of neural networks to detect DDoS attacks. In addition, both papers have recommendations for further research on this topic. However, the 2021 study uses machine learning to achieve its goal, while the present study considers asynchronous programming.

M. Mittal et al. [18] emphasize that detecting cyberattacks is a challenging task in cybersecurity and a deep machine-learning model is needed for this purpose. This paper proposes a study of the DNN deep neural network which has been tested on CICDDDDoS-2019 and PVAMUDDDDoS-2020 datasets using complete and reduced feature sets. The findings of the study show that the DNN model has satisfactory performance, which can be very useful in time-critical applications and networks with high traffic loads. The aforementioned study uses a specific dataset, while the present study implemented a programme, but it does not contain datasets. Furthermore, the DNN neural network is mentioned theoretically but not used in practice in this study.

C. Shieh et al. [19] developed a novel DDoS attack detection method based on a convolutional neural network with CNN-Geo geometric metrics, which is augmented by incremental learning. This method provides high accuracy in detecting DDoS attacks, including unknown attacks, and can also adapt to new attack scenarios. The conducted experiments have shown that this method is highly effective, achieving over 99% detection accuracy on different types

of attacks. As in the previous cases, the commonality between the two studies is the use of neural network to combat availability attacks. However, the neural networks themselves are different, as this study does not use the CNN-Geo network.

Finally, R. Qamar et al. [20] emphasize that DDoS attacks target multiple computers and Internet connections. Their study investigates the best algorithm for detecting DDoS attacks by comparing three different methods. The research involves training a recurrent neural network to accurately detect such attacks. Experiments show that the variable learning rate gradient descent algorithm achieves 99.9% accuracy and outperforms other algorithms. Thus, both studies compare methods for detecting DDoS attacks, but the methods themselves are different. In addition, the 2022 paper explores a particular algorithm, which is not the case in the present study.

Upon careful analysis of DDoS attack detection and mitigation approaches, it becomes evident that machine learning techniques, specifically neural networks, are the prevailing methods in contrast to traditional rule-based approaches. Studies demonstrate different neural architectures, such as LSTM, CNN, DNN, and RNN, each possessing distinct strengths. However, the selection of a model greatly affects the accuracy of detection and its ability to adapt to new attack patterns. Asynchronous detection methods have the potential to provide advantages for large-scale systems, but they also bring about increased complexity. Feature selection is a critical factor that balances the speed of detection with the level of comprehensiveness [21], [22], [23]. The importance of models being able to adjust to changing attack scenarios is highlighted, although this needs to be carefully controlled to prevent incorrect identifications. The utilization of different performance evaluation metrics and datasets in various studies leads to difficulties in making direct comparisons [24]. Although commercial solutions may offer a wider range of features, they may not have the same level of transparency and ability to quickly adapt as research prototypes [25]. In the end, there is no one-size-fits-all solution in this field. The success of any approach depends greatly on the particular network environments and attack characteristics. This emphasizes the importance of ongoing research into hybrid and adaptive techniques.

6. Conclusions

The present study discussed the methods of DDoS attack detection and the specifics of their application. To fulfil the purpose of this study, which was to investigate and determine the effectiveness of using neural networks with asynchronous programming in the context of countering attacks on availability, methods of analysis and experimentation were used. They were used to explore the ways and challenges of detecting DDoS attacks. Furthermore, a simple program was implemented in C# language which is a system simulation for attack detection. A table was created to compare cyberthreat countermeasure platforms, namely Cloudflare, Akamai, Imperva Incapsula, Radware, Link11, AppTrana, and Sucuri. A structural diagram was constructed to analyze the DDoS attack countermeasures.

Overall, a plethora of studies emphasize the importance of DDoS attack detection and propose a variety of methods including neural networks and machine learning. These methods are effective and can achieve high accuracy in detecting attacks. However, despite successful research in DDoS attack detection, there is a need for more research to improve the performance and accuracy of the methods and to adapt to new types of attacks. The results of this study highlight the practical significance of using neural networks with asynchronous programming in the field of DDoS attack detection. It is to improve the efficiency and accuracy of detection of such attacks and to improve the response and protection of network systems. Neural networks trained on data using asynchronous programming can adapt to rapidly changing network scenarios, which makes them more effective in detecting DDoS attacks, which can have different forms and characteristics. Certain recommendations are offered in this regard. Admittedly, DDoS attack detection techniques using neural networks and asynchronous programming should be further developed and improved. It is worth considering how the developed methods can be better integrated into existing security systems. Further research should pay attention not only to DDoS attacks but also to other types of cyber threats to create a comprehensive defense system. It is also important to consider the scalability and performance of the developed methods in real network environments.

The study's findings indicate that the use of asynchronous programming and neural networks can greatly improve the identification and reduction of DDoS attacks. Nevertheless, additional research is required to enhance the efficiency of

these methods and overcome any potential constraints. Potential future research avenues may encompass the examination of the incorporation of alternative machine learning algorithms, the advancement of more intricate neural network structures, and the evaluation of the efficacy of these methodologies in practical situations. Furthermore, the practical applications of these discoveries may include the creation of novel cybersecurity tools and services that utilize asynchronous programming and neural networks to offer enhanced defense against DDoS attacks.

7. Declarations

7.1. Author Contributions

Conceptualization: K.T. and A.B.; Methodology: K.T.; Software: A.B.; Validation: A.B.; Formal Analysis: K.T. and A.B.; Investigation: K.T.; Resources: A.B.; Data Curation: K.T.; Writing Original Draft Preparation: K.T. and A.B.; Writing Review and Editing: K.T. and A.B.; Visualization: K.T.; All authors have read and agreed to the published version of the manuscript.

7.2. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

7.3. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

7.4. Institutional Review Board Statement

Not applicable.

7.5. Informed Consent Statement

Not applicable.

7.6. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] E. Benmohamed, A. Thaljaoui, S. El Khediri, S. Aladhadh, and M. Alohali, "DDoS attacks detection with half autoencoder-stacked deep neural network," *International Journal of Cooperative Information Systems*, vol. 1, no. 1, pp. 1-6, 2023.

[2] A. Kandiero, P. Chiurunge, and J. Munodawafa, "Detection of DDoS attacks using variational autoencoder-based deep neural network," *in Privacy Preservation and Secured Data Storage in Cloud Computing, Hershey: IGI Global*, vol. 1, no. 1, pp. 265-404, 2023.

[3] V. Sarcar, "Asynchronous programming," *in: Getting Started with Advanced C#, Berkeley: Apress*, vol. 1, no. 1, pp. 217-282, 2020.

[4] B. Goparaju, and B. Srinivasa Rao, "Distributed Denial-of-Service (DDoS) attack detection using 1D Convolution Neural Network (CNN) and decision tree model," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 32, no. 2, pp. 30-41, 2023.

[5] C. S. Shieh, T. T. Nguyen, and M. F. Horng, "Detection of unknown DDoS attack using convolutional neural networks featuring geometrical metric," *Mathematics*, vol. 11, no. 9, pp. 1-7, 2023.

[6] C. S. Kalutharage, X. Liu, C. Chrysoulas, N. Pitropakis, and P. Papadopoulos, "Explainable AI-based DDOS attack identification method for IoT networks," *Computers*, vol. 12, no. 2, pp. 1-32, 2023.

[7] V. Malinovskyi, L. Kupershtein, and V. Lukichov, "Mathematical model for assessing cyber threats and information impacts in microcontrollers," *Information Technologies and Computer Engineering*, vol. 59, no. 1, pp. 69-82, 2024.

[8] P. Chen, S. Liu, B. Chen, and L. Yu, "Multi-agent reinforcement learning for decentralized resilient secondary control of energy storage systems against DoS attacks," *IEEE Transactions on Smart Grid*, vol. 13, no. 3, pp. 1739-1750, 2022.

 ISSN 2723-6471

[9] A. H. Alzahrani, and L. Hong, "Generation of DDoS attack dataset for effective IDS development and evaluation," *Journal of Information Security*, vol. 9, no. 4, pp. 225-241, 2018.

[10] A. B. de Neira, B. Kantarci, and M. Nogueira, "Distributed denial of service attack prediction: Challenges, open issues and opportunities," *Computer Networks*, vol. 222, no. 1, pp. 1-8, 2023.

[11] A. E. Cil, K. Yildiz, and A. Buldu, "Detection of DDoS attacks with feed forward based deep neural network model," *Expert Systems with Applications*, vol. 169, no. 1, pp. 1-4, 2021.

[12] A. Kumar, W. B. Glisson, and R. Benton, "Network attack detection using an unsupervised machine learning algorithm," *in Proceedings of the 53rd Hawaii International Conference on System Sciences, Honolulu: University of Hawai'I,* vol. 1, no. 1, pp. 6496-6505, 2020.

[13] A. Mustapha, "Detecting DDoS attacks using adversarial neural network," *Computers & Security*, vol. 127, no. 1, pp. 1-6, 2023.

[14] M. Sayed, I. Sayem, S. Saha, and A. Haque, "A multi-classifier for DDoS attacks using stacking ensemble deep neural network," *in International Wireless Communications and Mobile Computing, Dubrovnik: IEEE*, vol. 1, no. 1, pp. 1125-1130, 2022.

[15] A. Rangapur, T. Kanakam, and A. Jubilson, "DDoSDet: An approach to Detect DDoS attacks using Neural Networks," *Cryptography and Security*, vol. 1, no. 1, pp. 1-8, 2022.

[16] A. Lin, J. Cheng, L. Rutkowski, S. Wen, M. Luo and J. Cao, "Asynchronous fault detection for memristive neural networks with dwell-time-based communication protocol," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 34, no. 11, pp. 9004-9015, 2023.

[17] A. Shah, D. Rathod, and D. Dave, "DDoS attack detection using artificial neural network," *in International Conference on Computing Science, Communication and Security, Cham: Springer*, vol. 1, no. 1, pp. 46-66, 2021.

[18] M. Mittal, K. Kumar, and S. Behal, "DDoS attacks detection using a deep neural network model," *in International Advanced Computing Conference, Cham: Springer*, vol. 1, no. 1, pp. 169-182, 2023.

[19] C. Shieh et al., "Detection of adversarial DDoS attacks using generative adversarial networks with dual discriminators," *Symmetry*, vol. 14, no. 1, pp. 66-68, 2022.

[20] R. Qamar, B. A. Zardari, A. A. Arain, F. H. Khoso, and F. A. Jokhio, "Detecting distributed denial of service attacks using recurrent neural network," *University of Sindh Journal of Information and Communication Technology*, vol. 5, no. 2, pp. 86-94, 2022.

[21] A. Mustafin, and A. Kantarbayeva, "Resource competition and technological diversity," *PLoS ONE*, vol. 16, no. 11, pp. 1-5, 2021.

[22] D. Aizstrauta, and E. Ginters, „Using market data of technologies to build a dynamic integrated acceptance and sustainability assessment model," *Procedia Computer Science*, vol. 104, no. 12, pp. 501-508, 2016.

[23] E. K. Iskandarov, G. G. Ismayilov, and F. B. Ismayilova, "Diagnostic operation of gas pipelines based on artificial neuron technologies," *Advances in Intelligent Systems and Computing*, vol. 1095, no. 1, pp. 787-791, 2020.

[24] S. Kerimkhulle et al., "Fuzzy logic and its application in the assessment of information security risk of industrial internet of things," *Symmetry*, vol. 15, no. 10, pp. 1-8, 2023.

[25] S. Kerimkhulle, N. Obrosova, A. Shananin, and A. Tokhmetov, "Young duality for variational inequalities and nonparametric method of demand analysis in input–output models with inputs substitution: application for Kazakhstan economy," *Mathematics*, vol. 11, no. 19, pp. 1-4, 2023.