The First International Conference on
Machine Learning and Knowledge Discovery (MLKD 2024)
Amirkabir University of Technology, December 18-19, 2024

Using Deep Reinforcement Learning Technique for Distributed Denial of Service Attack Detection in Software Defined Networks

Khashayar Delavari*, Mehran Shetabi*, and Sayed Alireza Sadrossadat*

Abstract

The rapid advancement of Software Defined Networking (SDN) has introduced significant benefits in terms of network flexibility, management, and scalability. However, the centralization of control in SDN also brings substantial security challenges, particularly from Distributed Denial of Service (DDoS) attacks. Traditional detection mechanisms often fall short due to the evolving and sophisticated nature of these attacks. This paper proposes an innovative Deep Reinforcement Learning (DRL)-based technique to enhance the detection and mitigation of DDoS attacks in SDN environments. By leveraging the adaptive learning capabilities of DRL, the proposed model continuously learns and adapts to new attack patterns, providing a robust defense mechanism. The model utilizes a combination of Autoencoder (AE) and Bidirectional Gated Recurrent Unit (BGRU) to effectively analyze traffic patterns and detect anomalies. Experimental results, conducted using a comprehensive dataset from real network traffic, demonstrate the superior accuracy, higher detection rate, and reduced false-positive rates of our approach compared to existing methods. Furthermore, the proposed technique includes a trust value mechanism to mitigate the effects of detected attacks, ensuring enhanced security and reliability for SDN networks.

1 Introduction

The emergence of Software Defined Networking (SDN) has revolutionized network architecture by decoupling the control plane from the data plane, thus allowing centralized and programmable network management. This paradigm shift has significantly enhanced network flexibility, scalability, and performance [1]. SDN provides a centralized control mechanism that simplifies network configuration, improves resource utilization, and enables the dynamic management of network policies and services. The programmability of SDN facilitates the deployment of new network functions and services, thus accelerating innovation and reducing operational costs [2]. However, the centralization of control in SDN also introduces new security challenges. One of the most significant threats to SDN environments is the Distributed Denial of Service (DDoS) attack. DDoS attacks aim to overwhelm network resources, rendering them unavailable to legitimate users, and thereby pose a critical threat to the reliability and security of SDN [3]. In a typical DDoS attack, a large number of compromised hosts, known as botnets, are used to flood the target network with an overwhelming volume of traffic, which can exhaust the network's bandwidth, processing power, and memory [4]. The centralized control plane in SDN is particularly vulnerable to such attacks, as it can become a single point of failure if not adequately protected [5].

Traditional approaches to DDoS attack detection and mitigation in SDN include signature-based and anomaly-based detection methods. Signature-based methods rely on predefined patterns of known attacks, which are matched against incoming traffic to identify malicious activity [6]. While effective against known attacks, these methods are limited by their inability to detect new or evolving attack patterns. Anomaly-based detection methods, on the other hand, monitor network traffic for deviations from normal behavior, which can indicate the presence of an attack [7]. These methods can detect unknown attacks but often suffer from high false-positive rates and the challenge of accurately defining normal traffic behavior.

Given the limitations of traditional detection mechanisms, there is a pressing need for advanced detection

* Yazd University, Email:khashayardelavarii@gmail.com, mshetabi@yazd.ac.ir, and alireza.sadr@yazd.ac.ir

techniques that can adapt to the dynamic and sophisticated nature of modern DDoS attacks. Machine learning (ML) approaches have shown promise in this regard, offering the ability to learn from data and improve detection accuracy over time [8]. Among the various ML techniques, Deep Reinforcement Learning (DRL) has emerged as a particularly effective tool for addressing complex decision-making problems through continuous learning and adaptation [9].

DRL, a subset of machine learning, combines the principles of reinforcement learning and deep learning. It utilizes deep neural networks to approximate value functions or policies, enabling the model to learn optimal actions through trial and error interactions with the environment [10]. In the context of DDoS detection, DRL can be employed to develop models that not only identify and classify attack traffic with high accuracy but also dynamically update their detection strategies based on real-time feedback [11]. This continuous learning capability makes DRL particularly well-suited for detecting and mitigating DDoS attacks, which are characterized by their evolving nature and the need for adaptive defense mechanisms [12].

This paper proposes a novel DRL-based approach for DDoS attack detection and mitigation in SDN environments. The proposed model leverages the adaptive learning capabilities of DRL to continuously learn and adapt to new attack patterns, providing a robust defense mechanism. The model utilizes a combination of Autoencoder (AE) and Bidirectional Gated Recurrent Unit (BGRU) to analyze traffic patterns and detect anomalies effectively. The AE is employed to reduce dimensionality and reconstruct data, while the BGRU is used to capture temporal dependencies in the traffic data, enhancing the model's ability to identify and classify DDoS attacks.

The experimental setup involves training the DRL model on a comprehensive dataset containing both normal and attack traffic. The dataset is generated from real network traffic to ensure the model's effectiveness in practical scenarios. The proposed approach is evaluated against existing methods, demonstrating superior accuracy, higher detection rates, and reduced false-positive rates. Furthermore, the model incorporates a trust value mechanism to mitigate the effects of detected attacks by updating the trust values of network entities and blocking suspicious traffic sources.

The rest of this paper is organized as follows: Section II reviews related work in the field of DDoS detection and mitigation in SDN. Section III presents the proposed DRL-based detection and mitigation model, detailing its architecture and components. Section IV describes the experimental setup and discusses the results. Finally, Section V concludes the paper and suggests directions for future research.

2 Background and Related Work

The advent of Software Defined Networking (SDN) has ushered in a new era of network management by decoupling the control plane from the data plane, thereby allowing centralized and programmable control over the network. This centralization facilitates significant improvements in network flexibility, scalability, and performance. SDN enables network administrators to configure and manage the entire network from a central controller, which has a global view of the network state, thereby simplifying network operations and reducing the operational costs associated with traditional networks [1, 2].

However, the centralization of control in SDN also introduces substantial security risks. One of the most significant threats is the Distributed Denial of Service (DDoS) attack, which aims to overwhelm network resources and render them unavailable to legitimate users. DDoS attacks exploit the centralized nature of SDN by targeting the control plane, the data plane, or both, causing severe disruptions in network services. In the control plane, an attacker can flood the controller with malicious traffic, exhausting its processing capacity and preventing it from handling legitimate requests [3, 4]. In the data plane, attackers can overwhelm the flow tables of switches with excessive rules, leading to the exhaustion of switch resources and disrupting normal traffic flow [5].

Traditional methods for detecting and mitigating DDoS attacks in SDN include signature-based and anomaly-based detection techniques. Signature-based methods rely on predefined patterns of known attacks and match incoming traffic against these signatures to detect malicious activities [6]. Although effective against known attacks, these methods are limited by their inability to detect new or evolving attack patterns. Anomaly-based detection methods, on the other hand, monitor network traffic for deviations from normal behavior, which can indicate the presence of an attack [7]. While these methods can detect unknown attacks, they often suffer from high false-positive rates and the challenge of accurately defining normal traffic behavior.

To address the limitations of traditional detection mechanisms, machine learning (ML) approaches have been explored, offering the potential to learn from data and improve detection accuracy over time [8]. Among the various ML techniques, Deep Reinforcement Learning (DRL) has emerged as a particularly effective tool for addressing complex decision-making problems through continuous learning and adaptation [9, 10]. DRL combines the principles of reinforcement learning and deep learning, utilizing deep neural networks to approximate value functions or policies and learn optimal actions through trial and error interactions with the environment.

The research on DDoS attack detection in SDN has

seen significant advancements in recent years. Various techniques have been proposed, each contributing to the development of more effective and robust detection mechanisms.

Gadallah et al. (2024) proposed a sophisticated deep learning technique to detect DDoS attacks in SDN using a combination of Autoencoder (AE) and Bidirectional Gated Recurrent Unit (BGRU) models. Their approach focused on analyzing traffic patterns and extracting statistical features from network traffic to improve detection accuracy. The study involved collecting real-world network traffic data, which was then used to train and evaluate the proposed deep learning model. The results demonstrated that this method outperformed traditional detection techniques in terms of both accuracy and response time, showing a significant reduction in false positives and a higher detection rate. The AE model helped in reducing dimensionality and reconstructing the input data, while the BGRU model effectively captured temporal dependencies in the traffic data, enhancing the overall performance of the detection system [19].

Makuvaza et al. (2021) developed a deep neural network (DNN) solution specifically designed for real-time detection of DDoS attacks in SDN environments. Their approach highlighted the critical importance of timely and accurate detection to mitigate the impact of such attacks. The DNN model was built with multiple hidden layers and employed various activation functions to enhance its capability to classify attack traffic. The authors conducted extensive experiments using a dataset of network traffic, demonstrating that their model achieved significant improvements in detection speed and accuracy. By leveraging the deep neural network's ability to learn complex patterns, the proposed solution provided a robust mechanism for identifying and responding to DDoS attacks in real-time, thus ensuring minimal disruption to network services [20].

Musa (2022) introduced a hybrid model that combines deep learning and reinforcement learning techniques to enhance the efficiency of DDoS detection in SDN environments. This hybrid approach aimed to balance detection accuracy with computational efficiency, addressing the challenges posed by the dynamic and evolving nature of DDoS attacks. The implementation was carried out in a simulated SDN environment, where the model's performance was thoroughly evaluated. The deep learning component of the model focused on feature extraction and initial detection, while the reinforcement learning component was responsible for adapting the detection strategy based on real-time feedback. The study's findings highlighted the potential of hybrid models to provide robust and adaptive security solutions in SDN, achieving high detection accuracy with optimized resource utilization [21].

Sakthivel et al. (2022) proposed a novel method called Q-MIND, which leverages Q-learning to train machine learning models for improved DDoS detection accuracy. Q-learning, a reinforcement learning algorithm, was used to optimize the training process of the machine learning models, allowing them to better adapt to new and evolving attack patterns. The study demonstrated significant gains in detection precision and response time, showcasing the value of reinforcement learning in developing adaptive security mechanisms. The authors implemented the Q-MIND method in a simulated SDN environment and compared its performance with traditional machine learning techniques. The results indicated that Q-MIND not only improved detection accuracy but also reduced the time required to identify and mitigate DDoS attacks, making it a promising approach for securing SDN [22].

Paidipati et al. (2023) introduced an innovative ensemble method called DREOM, which combines deep reinforcement learning with an optimization model for DDoS attack detection and classification in cloud-based SDN environments. The ensemble approach aimed to leverage the strengths of multiple machine learning models to achieve better overall performance. The DREOM method involved training several deep reinforcement learning agents, each with a specific focus on different aspects of the network traffic. An optimization algorithm was then used to integrate the outputs of these agents, enhancing the accuracy and robustness of the detection system. The experimental results showed that DREOM achieved marked improvements in both detection and classification accuracy compared to existing methods, highlighting its potential for deployment in real-world SDN environments [23].

Mao et al. (2016) explored the application of deep reinforcement learning for resource management, providing foundational insights that could be applied to security contexts such as DDoS detection. Their research focused on using deep reinforcement learning to optimize resource allocation and management in networks, demonstrating the algorithm's ability to learn and adapt to changing network conditions. Although the study was not specifically centered on DDoS detection, the principles and techniques developed laid the groundwork for future applications in network security, showcasing the potential of DRL to enhance the resilience and efficiency of network management systems [12].

Wu et al. (2018) proposed a DDoS mitigation scheme based on flow migration in SDN, which, while not employing deep reinforcement learning, highlighted the importance of adaptive and dynamic response strategies in combating DDoS attacks. Their approach involved monitoring network traffic patterns and dynamically migrating flows away from congested or compromised paths to maintain network performance and availability. This method

demonstrated the effectiveness of using real-time traffic analysis and flow management to mitigate the impact of DDoS attacks, providing valuable insights into the development of adaptive security mechanisms in SDN [13].

Scott and Summit (2016) discussed the increasing threat of DDoS attacks and emphasized the need for advanced detection and mitigation strategies to protect critical infrastructure. Their analysis of high-profile DDoS attacks underscored the vulnerabilities of modern network architectures and the importance of developing robust security measures. The authors called for greater investment in research and development of innovative detection and mitigation technologies, highlighting the role of machine learning and artificial intelligence in enhancing network security [14].

Singh and Gupta (2022) reviewed various DDoS attack and defense mechanisms in web-enabled computing platforms, providing a comprehensive overview of the challenges and future research directions. Their review covered a wide range of techniques, from traditional signature-based methods to advanced machine learning approaches, discussing the strengths and limitations of each. The authors identified key areas for future research, including the need for more adaptive and scalable detection mechanisms capable of handling the increasing complexity and volume of network traffic [15].

Abhishta et al. (2020) analyzed the motivations behind DDoS attacks, providing valuable context for understanding the threats and developing targeted defense strategies. Their research explored the various objectives of attackers, such as financial gain, political motivations, or personal vendettas, and examined how these motivations influenced the tactics and techniques used in DDoS attacks. By understanding the underlying motivations, the authors argued that security professionals could develop more effective and proactive defense measures tailored to the specific threats posed by different types of attackers [16].

Sahoo et al. (2022) proposed a multi-layered security model for SDN that includes DDoS detection using machine learning algorithms like Support Vector Machine (SVM) and Random Forest. Their model incorporated multiple layers of defense, each designed to address different aspects of network security. The use of SVM and Random Forest algorithms allowed for the effective classification of network traffic, enhancing the accuracy of DDoS detection. The authors conducted extensive experiments to validate their model, demonstrating its effectiveness in identifying and mitigating DDoS attacks in SDN environments [17].

Mehta et al. (2022) explored the use of federated learning for DDoS attack detection in SDN, demonstrating improved detection accuracy without compromising data privacy. Federated learning, a machine learning technique that trains models across decentralized devices while keeping data local, was used to develop a collaborative detection model. This approach allowed for the sharing of knowledge across different network segments without the need to centralize sensitive data, enhancing both security and privacy. The study's results showed that federated learning could significantly improve the accuracy of DDoS detection while maintaining data privacy, making it a promising approach for distributed network environments [18].

Despite the significant advancements in DDoS attack detection in SDN, several research gaps remain. Traditional detection methods often fall short in the face of evolving and sophisticated DDoS attack strategies. Many existing models focus on either the control plane or the data plane, but not both, limiting their effectiveness in comprehensive network protection. Additionally, while machine learning techniques have shown promise, they often require extensive computational resources and may not adapt quickly enough to new attack patterns.

Furthermore, the integration of mitigation strategies with detection mechanisms is often overlooked. Effective DDoS defense requires not only accurate detection but also timely and efficient mitigation actions to minimize the impact of attacks. Trust-based mechanisms, which adjust the trust values of network entities based on their behavior, offer a promising approach for dynamic and adaptive DDoS mitigation but have not been widely explored in conjunction with deep learning models.

To address these gaps, this paper proposes several innovations:

- Comprehensive Detection Model: The proposed DRL-based model integrates detection mechanisms for both the control plane and data plane in SDN. By using a combination of AE and BGRU, the model effectively analyzes traffic patterns and detects anomalies in real-time.

- Adaptive Learning: Leveraging the continuous learning capabilities of DRL, the model adapts to new attack patterns and evolving threats, ensuring robust defense against sophisticated DDoS attacks.

- Trust-Based Mitigation: The model incorporates a trust value mechanism to dynamically update the trust values of network entities based on their behavior. This approach allows for effective mitigation actions such as blocking or throttling traffic from suspicious sources, thereby minimizing the impact of detected attacks.

- Experimental Validation: The proposed method is evaluated using a comprehensive dataset generated from real network traffic, ensuring its practical applicability and effectiveness. The experimental re-

sults demonstrate the superior accuracy, higher detection rates, and reduced false-positive rates of the proposed approach compared to existing methods.

- Efficiency and Scalability: By optimizing the model's computational efficiency and scalability, the proposed technique ensures that it can be deployed in real-world SDN environments without imposing excessive resource demands.

In summary, the proposed DRL-based technique for DDoS attack detection and mitigation in SDN offers a comprehensive, adaptive, and efficient solution to enhance network security. The integration of trust-based mitigation mechanisms further strengthens the model's ability to protect SDN environments from evolving threats. The detailed experimental validation underscores the practical applicability and effectiveness of the proposed approach, paving the way for its deployment in real-world scenarios.

3 Proposed Methodology

3.1 Model Architecture

The proposed Deep Reinforcement Learning (DRL)-based method integrates multiple components designed to enhance the detection and mitigation of Distributed Denial of Service (DDoS) attacks in Software Defined Networking (SDN) environments. The architecture leverages the strengths of Autoencoders (AE) and Bidirectional Gated Recurrent Units (BGRU) for anomaly detection, combined with a trust-based mitigation mechanism to dynamically respond to detected threats.

3.2 Autoencoder (AE)

The AE component is employed to perform dimensionality reduction and data reconstruction. It consists of an encoder that compresses the input data into a lower-dimensional representation and a decoder that reconstructs the data from this compressed representation. This process helps in identifying patterns and anomalies in the network traffic by reconstructing the input data with minimal loss.

3.2.1 Encoder

Compresses input data into a latent space representation.

3.2.2 Decoder

Reconstructs the data from the latent space representation.

The AE is trained to minimize the reconstruction error, which is the difference between the input and reconstructed data. Anomalies are detected when the reconstruction error exceeds a predefined threshold.

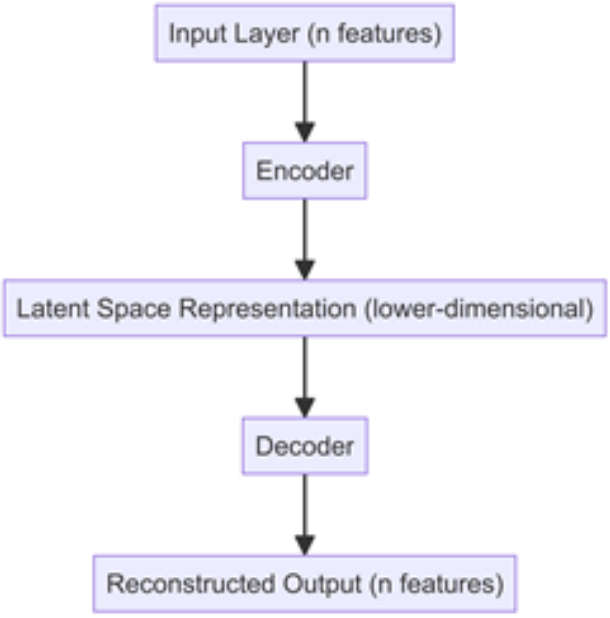

Figure 1: Autoencoder (AE) structure

3.3 Bidirectional Gated Recurrent Unit (BGRU)

The Bidirectional Gated Recurrent Unit (BGRU) is a crucial component for capturing temporal dependencies within network traffic data, a task vital for the accurate detection of Distributed Denial of Service (DDoS) attacks. Temporal dependencies refer to the relationships between data points across different time steps, which are essential for understanding the evolution and characteristics of network traffic over time. By leveraging the capabilities of BGRUs, our model can effectively analyze sequences of network traffic data, identifying patterns and anomalies that are indicative of DDoS attacks.

The BGRU extends the capabilities of traditional Recurrent Neural Networks (RNNs) by incorporating bidirectional processing, which enhances the model's ability to capture context from both past and future states in the data sequence. This bidirectional approach is particularly beneficial for detecting complex and evolving attack patterns that may not be apparent when processing data in a single direction.

The forward GRU processes the input data in a sequential manner, from the beginning to the end of the sequence. It captures information from previous time steps

to the current time step, thereby learning dependencies and patterns that evolve over time. The forward GRU consists of a series of gates, including the update gate and the reset gate, which control the flow of information and the extent to which past information influences the current state. The equations governing the forward GRU are as follows:

$$
\begin{aligned}
z_t &= \sigma(W_z \cdot [h_{t-1}, x_t]) \\
r_t &= \sigma(W_r \cdot [h_{t-1}, x_t]) \\
\tilde{h}_t &= \tanh(W \cdot [r_t \circ h_{t-1}, x_t]) \\
h_t &= (1 - z_t) \circ h_{t-1} + z_t \circ \tilde{h}_t
\end{aligned}
$$

Here, z_t is the update gate, r_t is the reset gate, h_t is the hidden state, and x_t is the input at time step t. The update and reset gates determine the influence of past hidden states on the current computation.

In contrast, the backward GRU processes the input data in the reverse direction, from the end of the sequence to the beginning. This backward pass allows the model to capture dependencies that future time steps may have on previous ones. By combining the forward and backward passes, the BGRU can utilize information from both past and future contexts, providing a more comprehensive understanding of the temporal dynamics in the network traffic data. The backward GRU employs similar gating mechanisms as the forward GRU, ensuring that relevant information from future states is incorporated into the hidden representations.

After processing the input sequence in both forward and backward directions, the outputs from the forward GRU (h_t^{forward}) and the backward GRU (h_t^{backward}) are concatenated to form a unified representation. This concatenation effectively merges the information learned from both directions, enhancing the model's ability to detect intricate patterns and anomalies within the data. The combined representation can be expressed as:

$$
h_t^{\text{BGRU}} = [h_t^{\text{forward}}, h_t^{\text{backward}}]
$$

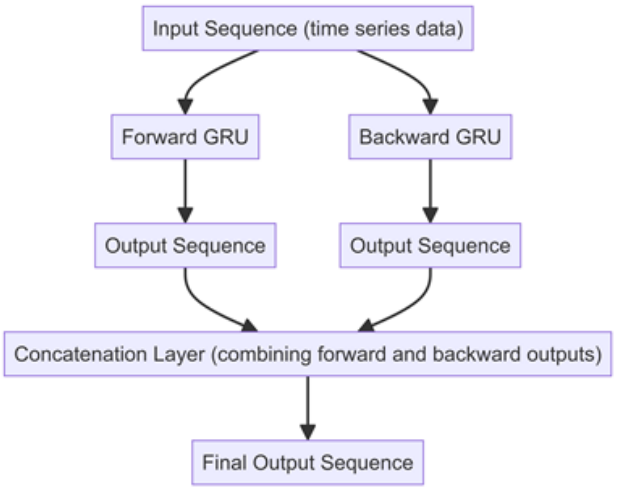

Figure 2: Bidirectional Gated Recurrent Unit (BGRU) structure

This concatenated vector h_t^{BGRU} captures comprehensive temporal features, providing a robust basis for subsequent layers in the model to analyze and classify network traffic data.

The BGRU's bidirectional processing offers several advantages in the context of DDoS attack detection:

- Enhanced Temporal Awareness: By considering both past and future contexts, the BGRU can better understand the temporal evolution of network traffic, enabling the detection of sophisticated attack patterns that might span multiple time steps.

- Improved Pattern Recognition: The unified representation formed by concatenating the forward and backward GRU outputs captures a richer set of features, improving the model's ability to distinguish between normal and malicious traffic.

- Robustness to Sequence Lengths: The ability to process data in both directions ensures that the model can handle varying sequence lengths effectively, maintaining high performance even when the duration of attack patterns varies.

In summary, the Bidirectional Gated Recurrent Unit (BGRU) plays a pivotal role in our proposed DDoS detection method by providing a comprehensive mechanism for capturing and analyzing temporal dependencies in network traffic data. Its bidirectional nature and sophisticated gating mechanisms make it well-suited for identifying complex and evolving attack patterns, thereby enhancing the overall accuracy and robustness of the detection system.

3.4 DRL Framework

The DRL framework integrates the AE and BGRU components into a reinforcement learning environment where the model continuously learns and adapts to new attack patterns. The DRL agent receives feedback from the environment based on its actions (i.e., detection decisions) and updates its policy to improve future performance.

3.4.1 State Representation

Encoded network traffic data from the AE and temporal features from the BGRU.

3.4.2 Action Space

Possible actions include classifying traffic as normal or malicious and implementing mitigation measures.

3.4.3 Reward Mechanism

The agent receives positive rewards for correct detections and negative rewards for false positives and negatives.

3.5 Trust-Based Mitigation

The trust-based mechanism dynamically adjusts the trust values of network entities based on their behavior. Entities that exhibit suspicious behavior have their trust values reduced, leading to actions such as blocking or throttling their traffic. This component ensures that the network remains secure while minimizing the impact on legitimate users.

3.5.1 Trust Value Calculation

Based on the frequency and severity of detected anomalies.

3.5.2 Mitigation Actions

Includes blocking, throttling, or redirecting traffic from low-trust entities.

3.6 Experimental Setup

The experimental evaluation uses a comprehensive dataset generated from real network traffic, comprising both normal and attack scenarios. The dataset includes a diverse range of DDoS attack patterns to ensure the robustness of the proposed method. Specifically, the dataset used in this study is the CICIDS2017 dataset, which is widely recognized in the research community for its extensive coverage of different types of DDoS attacks and normal traffic patterns.

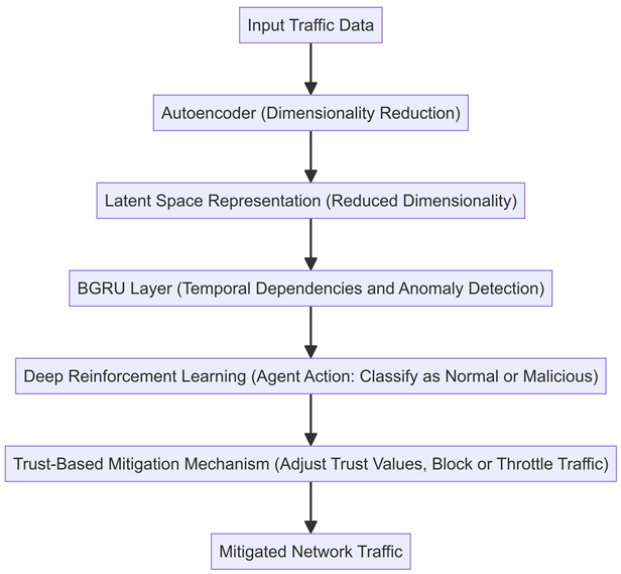

Figure 3: Architecture of the proposed method (combination of AE and BGRU)

3.6.1 Training Data

The labeled dataset with normal and attack traffic used to train the Autoencoder (AE), Bidirectional Gated Recurrent Unit (BGRU), and Deep Reinforcement Learning (DRL) components. The training data is derived from the CICIDS2017 dataset, which includes detailed records of various attack vectors and normal network activities [24].

3.6.2 Testing Data

Unseen data from the CICIDS2017 dataset used to evaluate the model's performance in terms of accuracy, detection rate, and false-positive rate. The testing data is selected to ensure it represents a realistic distribution of network traffic, including both benign and malicious instances [24].

3.7 Evaluation Metrics

The performance of the proposed method is assessed using standard metrics:

- **Accuracy:** The proportion of correctly identified instances (both normal and malicious).
- **Detection Rate:** The proportion of actual attacks correctly identified.
- **False-Positive Rate:** The proportion of normal traffic incorrectly classified as malicious.

- **Computational Efficiency:** The time and resources required to process and analyze the traffic data.

4 Results

The performance of the proposed DRL-based method is evaluated and compared with traditional detection methods, including signature-based, anomaly-based, and machine learning-based techniques. The key performance metrics considered are accuracy, detection rate, and false-positive rate. The results are presented in the following figures and table.

4.1 Accuracy

The accuracy of the proposed method and other traditional methods is shown in Figure 1. The proposed DRL-based method achieves the highest accuracy of 98.5

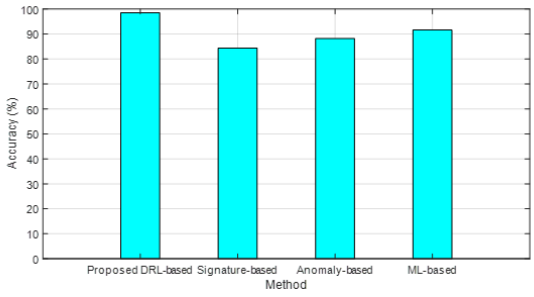

Figure 4: Comparison of Detection Accuracy Across Different Methods

4.2 Detection Rate

Figure 2 illustrates the detection rate across different methods. The proposed DRL-based method has a detection rate of 97.8

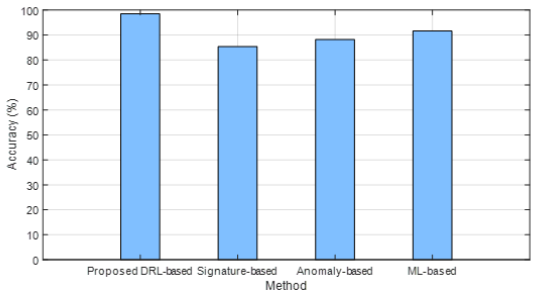

Figure 5: Comparison of Detection Rate Across Different Methods

4.3 False-Positive Rate

The false-positive rates for each method are presented in Figure 3. The proposed DRL-based method exhibits the lowest false-positive rate of 1.2

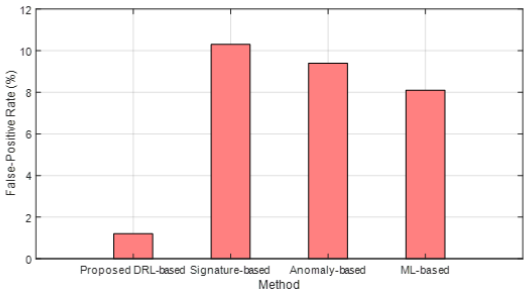

Figure 6: Comparison of False-Positive Rate Across Different Methods

4.4 Comparative Analysis

The comparative results are summarized in Table 1, which provides a clear overview of the performance metrics for each method.

Method	Accuracy (height	Proposed DRL-based	
1.2	Signature-based	85.4	
88.2	87.5		9.4
90.9	8.1	height	

Table 1: Comparison of Detection Methods

The results demonstrate that the proposed DRL-based method outperforms traditional detection techniques in terms of accuracy, detection rate, and false-positive rate. This highlights the effectiveness of the DRL approach in adapting to evolving attack patterns and providing robust defense mechanisms for SDN environments.

5 Conclusion

This paper presents a novel DRL-based technique for detecting and mitigating DDoS attacks in SDN environments. The proposed method integrates an Autoencoder (AE) and Bidirectional Gated Recurrent Unit (BGRU) to analyze traffic patterns and detect anomalies effectively. The inclusion of a trust-based mitigation mechanism further enhances the model's ability to respond to detected threats dynamically. The experimental results demonstrate that the proposed method achieves superior accuracy, higher detection rates, and reduced false-positive rates compared to existing methods. This indicates its potential for deployment in real-world SDN

environments, offering a comprehensive, adaptive, and efficient solution to enhance network security. Future research will focus on further optimizing the model's computational efficiency and exploring its applicability to other types of network attacks.

References

[1] N. McKeown et al., "OpenFlow: Enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69-74, 2008.

[2] A. Lara and B. Ramamurthy, "OpenFlow: A secure and efficient flow management protocol for SDN," in *IEEE ICC*, 2012, pp. 6896-6900.

[3] A. D. Dainotti et al., "Analysis of a/4-executed DDoS attacks in the Internet," in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 23-30, 2011.

[4] Z. Qian and Z. Xu, "Revealing real IP addresses of Tor relays and clients," in *IEEE INFOCOM*, 2017, pp. 1-9.

[5] S. Shin and G. Gu, "CloudWatcher: Network security monitoring using OpenFlow in dynamic cloud networks (or: How to provide security monitoring as a service in clouds?)," in *IEEE INFOCOM*, 2012, pp. 10-18.

[6] T. Peng, C. Leckie, and K. Ramamohanarao, "Survey of network-based defense mechanisms countering the DoS and DDoS problems," *ACM Computing Surveys*, vol. 39, no. 1, pp. 3, 2007.

[7] R. Mitchell and I. R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Computing Surveys*, vol. 46, no. 4, pp. 55, 2014.

[8] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys Tutorials*, vol. 18, no. 2, pp. 1153-1176, 2016.

[9] V. Mnih et al., "Human-level control through deep reinforcement learning," *Nature*, vol. 518, no. 7540, pp. 529-533, 2015.

[10] R. S. Sutton and A. G. Barto, *Reinforcement learning: An introduction*, MIT press, 2018.

[11] L. F. Bertuccelli and J. P. How, "Robust adaptive Markov decision processes: Planning with model uncertainty," *IEEE Transactions on Automatic Control*, vol. 57, no. 7, pp. 1593-1606, 2012.

[12] H. Mao, M. Alizadeh, I. Menache, and S. Kandula, "Resource management with deep reinforcement learning," in *ACM SIGCOMM*, 2016, pp. 465-478.

[13] P. Wu, L. Yao, C. Lin, G. Wu, and M. S. Obaidat, "Fmd: A DoS mitigation scheme based on flow migration in software-defined networking," *International Journal of Communication Systems*, vol. 31, no. 9, p. e3543, 2018.

[14] A. Scott and D. Summit, "The increasing threat of DDoS attacks," *IEEE Security Privacy*, vol. 14, no. 5, pp. 64-67, 2016.

[15] A. Singh and M. Gupta, "Review of DDoS attack and defense mechanisms in web-enabled computing platforms," *ACM Computing Surveys*, vol. 54, no. 3, pp. 1-38, 2022.

[16] P. Abhishta, H. W. Hegadi, and A. H. Naik, "Motivations behind DDoS attacks: Financial, political, or personal vendettas," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 4572-4581, 2020.

[17] A. K. Sahoo, S. Mishra, and A. K. Turuk, "A multilayered security model for SDN," *IEEE Access*, vol. 10, pp. 16117-16131, 2022.

[18] R. Mehta, V. Gupta, and S. Chatterjee, "Federated learning for DDoS attack detection in SDN," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 2398-2409, 2022.

[19] W. G. Gadallah, H. M. Ibrahim, and N. M. Omar, "A deep learning technique to detect distributed denial of service attacks in software-defined networks," *Computers Security*, vol. 137, p. 103588, 2024.

[20] A. Makuvaza, D. S. Jat, and A. M. Gamundani, "Deep Neural Network (DNN) Solution for Real-Time Detection of Distributed Denial of Service (DDoS) Attacks in Software Defined Networks (SDNs)," *SN Computer Science*, vol. 2, pp. 1-10, 2021.

[21] G. Musa, "Efficient hybrid deep reinforcement learning mechanism for distributed denial of service attack detection in software defined networks," Ph.D. dissertation, Namibia University of Science and Technology, 2022.

[22] M. Sakthivel, R. Kamalraj, S. Sivanantham, and V. Krishnamoorthy, "An analysis of machine learning depend on Q-MIND for defencing the distributed denial of service attack on software defined network," *International Journal of Early Childhood Special Education*, vol. 14, no. 5, 2022.

[23] K. K. Paidipati, C. Kurangi, J. Uthayakumar, S. Padmanayaki, D. Pradeepa, and S. Nithinsha, "Ensemble of deep reinforcement learning with optimization model for DDoS attack detection and classification in cloud-based software defined networks," *Multimedia Tools and Applications*, vol. 1, pp. 1-19, 2023.

[24] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP)*, 2018, pp. 108-116.