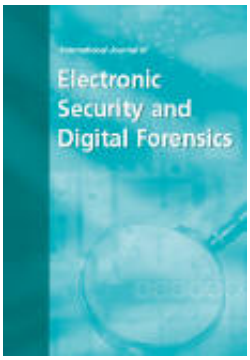


International Journal of Electronic Security and Digital Forensics

ISSN online: 1751-9128 - ISSN print: 1751-911X
https://www.inderscience.com/ijesdf

VLMDALP: design of an efficient VARMA LSTM-based model for identification of DDoS attacks using application-level packet analysis

Meghana Solanki, Sangita Chaudhari

DOI: 10.1504/IJESDF.2025.10061885

Article History:

Received:	15 May 2023
Last revised:	01 September 2023
Accepted:	21 September 2023
Published online:	23 December 2024

VLMDALP: design of an efficient VARMA LSTM-based model for identification of DDoS attacks using application-level packet analysis

Meghana Solanki* and Sangita Chaudhari

Ramrao Adik Institute of Technology,
D.Y. Patil (Deemed to be University),
Nerul, Navi Mumbai,
Maharashtra, India
Email: meghanasolanki2020@gmail.com
Email: sangita.chaudhari@rait.ac.in
*Corresponding author

Abstract: A novel approach for detecting application-level distributed denial-of-service (DDoS) attacks in networks is introduced. By merging vector autoregressive moving average (VARMA) and long short-term memory (LSTM) techniques, our hybrid model efficiently analyses packet data across time, frequency, and spatial domains. Initially utilising VARMA, the model extracts hierarchical features from raw packets, further refined by LSTM. These combined features form a succinct representation fed into a neural network for classifying diverse attack types. Experimenting with real-world datasets, including application-layer DDoS samples, our model demonstrates superior accuracy, precision, and recall compared to contemporary methods. Its use of VARMALSTM not only enhances performance but also ensures high efficiency in training and testing, making it well-suited for real-time applications. This innovation significantly advances forensic analysis in networks, crucial for fortifying communication systems' security and reliability.

Keywords: network forensics; attacks; analysis; application layer DDoS; vector autoregressive moving average; VARMA; long short-term memory; LSTM; samples.

Reference to this paper should be made as follows: Solanki, M. and Chaudhari, S. (2025) 'VLMDALP: design of an efficient VARMA LSTM-based model for identification of DDoS attacks using application-level packet analysis', *Int. J. Electronic Security and Digital Forensics*, Vol. 17, Nos. 1/2, pp.149–168.

Biographical notes: Meghana Solanki is a research scholar at the Ramrao Adik Institute of Technology, D.Y. Patil (Deemed to be University), Nerul, Navi Mumbai. Her main areas of research interest are digital forensics, cyber forensics, information security, and data mining.

Sangita Chaudhari is a Professor at the Ramrao Adik Institute of Technology, D.Y. Patil (Deemed to be University), Navi Mumbai, holds a PhD in Geospatial Data Security from IIT Bombay (2016). With 23 years of teaching and research, she specializes in digital forensics, cybersecurity,

image processing, and geospatial analytics. A senior IEEE member involved with IEEE GRSS, IEEE WIE, ACM, CSI, ISRS, and ISTE, she chaired IEEE WIE Affinity Group Bombay Section and Vice-Chaired IEEE GRSS Bombay Chapter. Her expertise covers GIS, image processing, cyber security, satellite image processing, pattern recognition, information security, databases, data analytics, and high-performance computing.

1 Introduction

The safety and reliability of communication systems are vulnerable to variety of threats that can cause significant damage. Network forensics is a critical aspect of computer security aimed at enhancing investigative capabilities within existing networks. It involves specialised infrastructure for the collection and analysis of network packets and events, specifically designed for investigative purposes. Network forensics is proposed as a complementary approach to the existing network security model. In today's organisations, network forensics holds significant importance in multiple ways. Firstly, it helps in understanding the patterns of external attacks, enabling organisations to prevent similar attacks in the future. Secondly, it plays a pivotal role in investigating insider abuses, which constitute the second-most expensive type of attack within organisations. Lastly, law enforcement agencies rely on network forensics to investigate crimes involving computers or digital systems as targets or tools for committing the crime. Forensic analysis models (FAMs) are essential for detecting and preventing these attacks. Traditional FAMs rely on hand-crafted features and rule-based systems, often proving ineffective in detecting new and unknown attacks. Deep learning-based models have shown promising results in the field of network forensics by automatically learning features from raw data samples (Almulhem, 2009).

One of the most significant threats and complex security challenges on the internet is the DDoS attack. With little to no notice, a DDoS attack can quickly exhaust the computational and communication capabilities of its target. To address this issue, various statistically-based protection measures have been developed to mitigate these attacks. However, the safeguards used at the network layer can provide only limited defence against DDoS attacks. At the transport (or network) layer, there is not always sufficient information available to make informed judgements about application attacks. Additionally, flaws in the designs of network hardware and lower-layer services on the provider's side can lead to complications. A denial-of-service (DoS) attack involves flooding an internet server with an enormous amount of legitimate or incorrect packets, thereby congesting its bandwidth and denying requests from other clients. DoS attempts to exploit various protocols across the network layer, transport layer, and application layer. Attackers often utilise protocols like the transport control protocol (TCP), user datagram protocol (UDP), and network layer protocols such as the internet control message protocol (ICMP), along with features like the SYN flag, to launch sophisticated DDoS attacks. To carry out DoS attacks at the application layer, attackers use application-layer protocols like HTTP, domain name service (DNS), etc. as metrics. DDoS attacks are launched from multiple geographic locations with the goal of taking down a server. While web servers on the internet are vulnerable to application-layer

DDoS attacks, forensic mechanisms play a crucial role in identifying them (Liu et al., 2022).

Most of these web servers are now centralised and have direct access to network backbones. DDoS attacks are more potent than DoS attacks because they are more targeted and involve a larger number of devices spread across different parts of the globe. Each device serves as a denial-of-service agent. In comparison to a DoS attack, a DDoS attack requires much less time to achieve its objective of rendering a target website inoperable. It affects all layers, including the application and network layers. A botmaster spreads harmful code and recruits malicious clients, forming a group of bots known as a botnet. These command-and-control centres, each located in a distinct geographical region, work in conjunction with the botmaster to communicate with bot clients and gather information from them. The botmaster expeditiously acquires bots by coercing individual customers into downloading software or files (Chen et al., 2022).

DDoS attacks generally impact layer three and layer four protocols, thereby consuming server bandwidth and affecting internet control. Additionally, it has been observed that application layer attacks utilise protocols such as HTTP, SMTP, FTP, and DNS. These attacks are designed to disrupt the functionality of applications. Due to the various methods employed to launch DDoS attacks, determining the specific type of DDoS attack without a focused network flow analysis is challenging. Attackers commonly target application-layer services like web servers and firewalls. DDoS attacks can severely disrupt web servers and potentially lead to a complete website shutdown. Moreover, attackers employ seemingly legitimate application layer requests, making it difficult for current defence mechanisms to identify them. These attacks can bring down a server much more swiftly and discreetly than network-layer DDoS attacks, as they target multiple assets at the application layer (Chen et al., 2022; Shi et al., 2021).

In this article, we propose a novel deep learning-based multidomain packet representation model for identifying attacks in the network. The model is designed to learn hierarchical features, including time, frequency, and spatial domains, from raw packet data (Praseed and Thilagam et al., 2020; Fu et al., 2021). These learned features are then input into a fully connected neural network for classification (Jia et al., 2020; Hajimaghsoodi and Jalili, 2022). To evaluate our proposed model, we conducted experiments using real-world network datasets as well as samples from the application-layer DDoS dataset. We employed Q learning and deep convolution neural network (QLD CNN) (Li et al., 2021b; Guanyu et al., 2021). The results demonstrate that our suggested model performs better than cutting-edge methods in terms of accuracy, recall, precision, and time. Furthermore, our model achieves high efficiency in both training and testing times, making it suitable for real-time applications. We further analyse the effectiveness of our proposed model by comparing it with conventional feature-based models and deep learning-based models. The findings demonstrate that our model outperforms traditional approaches, highlighting the effectiveness of this multidomain approach in real-time scenarios. The proposed model can also be tested with other types of network data and integrated into existing FAMs to enhance their performance for various real-time use cases.

The paper outline is: in Section 1, we provide an introduction to network forensics and application-level DDoS attacks. Section 2 presents a comprehensive survey of recent literature on detecting patterns of application-level DDoS attacks using network forensics. The architecture of an effective VARMA LSTM-based model for detecting DDoS attacks through the analysis of application-level packets is explained in Section 3.

Section 4 elucidates and interprets the outcomes obtained from the proposed VARMA LSTM-based model. Lastly, Section 5 draws conclusions and summarises the findings of this study.

2 Related work

DDoS attacks represent a serious threat to the reliability of network infrastructure. These kinds of attacks are frequently carried out by flooding a target system with an excessive amount of traffic, rendering the system incapable of functioning normally. Analysis of data packets performed at the application layer is one of the general methods for identifying DDoS attacks (Guo et al., 2022). In an HTTP flood attack, the attacker can utilise rented or self-owned servers to launch HTTP GET or POST requests towards the target's virtual machine (VM). As a consequence, the victim experiences a significant increase in resource utilisation and monetary damages, and the intended host becomes overloaded with HTTP floods, jeopardising the entire computing cluster (CC). Detecting Web swarm attacks poses a challenge, as they employ legitimate HTTP requests to overburden VM resources (Beitollahi et al., 2022). A new and effective approach was proposed that utilises reinforced transformer learning to address the challenges posed by DDoS with very short intervals, i.e., VSI-DDoS attacks in edge clouds. This novel approach aims to mitigate issues such as tail latency and service availability, providing enhanced protection against VSI-DDoS attacks (Bin et al., 2022). Nevertheless, these attacks resulted in substantial resource depletion, including the energy level of sensory nodes and network lifespan mitigation, leading to the crippling of entire networks (Huang et al., 2020). In one of the research studies, an investigation was conducted on application-level packet analysis and the performance of different methods for detecting distributed denial of service attacks using application-level packet analysis (Doriguzzi-Corin et al., 2020; Bhayo et al., 2020).

The concept of threshold-based detection is one of the earliest methods developed for identifying DDoS attacks through application-level packet analysis (Harada et al., 2022). To address security concerns in SDN architecture, an in-depth examination of contemporary research and emerging trends utilising machine learning (ML) algorithms for recognising DDoS attacks at the control level was done. Comparative analysis of several well-known ML algorithms, including k-nearest neighbours (k-NN), support vector machine (SVM) learning, decision tree algorithms (DT), as well as neural network algorithms (ANN) is done. The efficacy of various feature selection techniques, including neighbourhood component analysis (NCA) as well as minimum redundancy maximum relevance (mRMR) in conjunction with these ML algorithms, was also examined (Ravi and Shalinie, 2020). A novel model and mitigation approach for identifying and preventing low-frequency attacks on services provided by clouds using containers is proposed by Li et al. (2019). The proposed technique involves segregating instances into two distinct parts. The first portion deals with traffic generated by a whitelist, which is considered appropriate, while the second part deals with unknown requests, which can be both harmful and helpful. This isolation mechanism enhances the security of container-based cloud services by efficiently detecting and blocking potential threats while allowing legitimate traffic to proceed without interruption. Specialised measures should be employed to mitigate DDoS flooding attacks at the application level (Yungaicela-Naula et al., 2021). In this work, a benchmark is established for a specific

measure (such as the number of messages per second). When the attack threshold crosses it, the system is labelled as being under attack. Shield recurrent neural networks (SRNN) are utilised in this approach (Alasmary et al., 2022).

Over the last decade, due to the widespread adoption of cloud services among clients, it has become crucial to acknowledge that attacks such as DDoS pose a serious danger to these services (Wahab et al., 2017). In this paper, a game-theoretic method is adopted to demonstrate the interaction between sensor-instrument-edge VM pairs and DDoS attackers. This approach involves investigating various constraints, including task duration and resource allotment (Liu et al., 2020a; Alamri et al., 2020). It improves reliability of resource utilisation.

However, this strategy can result in false positives when perfectly legitimate communication is mistakenly identified as an attack under real-time scenarios (Doshi et al., 2021). The compromised devices engage in continuous, uninterrupted transmission of a high volume of packets across the network, deceptively masquerading as legitimate traffic to the victim. Consequently, the host unknowingly interacts not only with various devices but also with diverse types of packets (Abubakar et al., 2020). In a study by Mohmand (2022), a novel hybrid model that combines random forest (RF) and XGBoost was proposed for predicting DDoS attack traffic. The benchmark data was pre-processed to remove irrelevant information, and relevant features were extracted using the available information and labelled accordingly. The collected features and tagged data were then used to train the hybrid model, resulting in a robust prediction framework for DDoS attack detection. In some other study, the attack can be observed from the attackers perspective. The study explores the ever-changing landscape of these attacks, with a specific focus on understanding the dynamics of the attacking force. The goal is to uncover any strategies employed by these malicious actors and shed light on the intricacies that occur behind the scenes (Wang et al., 2018). A novel framework called P4DDoS is introduced which aims to detect DDoS attacks in the data plane of P4 switches. The proposed framework leverages estimations of empirical entropy using CountMin, count sketch, and P4LogLog techniques with low relative error to accurately identify and mitigate DDoS attacks (Ding et al., 2021).

Utilising machine learning strategies is yet another method for identifying SDoS attacks through application-level traffic analysis (Biswas et al., 2020). The researchers have utilised the RBM technique for dimension reduction while employing a scalable deep CNN model in a flow-based network like SDN to effectively mitigate DDoS attacks (Haider et al., 2020; Cvitić et al., 2021). Here, they have introduced a novel and scalable approach named WisdomSDN, which serves as an efficient solution in the context of software-defined networking, effectively defending against the amplification of DNS threats (Abou El Houda et al., 2020; Zhou et al., 2021). Cybersecurity concerns are tackled through a sociotechnical approach, placing strong emphasis on the meticulous design of secure network elements that form the foundation of the i-voting platform's implementation. The system provided a conducive environment for conducting penetration testing aimed at uncovering any underlying security vulnerabilities within the i-voting network (Nwankwo et al., 2023).

Algorithms trained by machine learning can become familiar with the typical behaviour of the system and recognise when it deviates from its usual operations (Elsaeidy et al., 2021). The researchers (Maity et al., 2021) have introduced a novel approach for detecting attacks on DDoS in the context of SDN, or software-defined networks, using a probabilistic-based method. Their approach leveraged the central limit

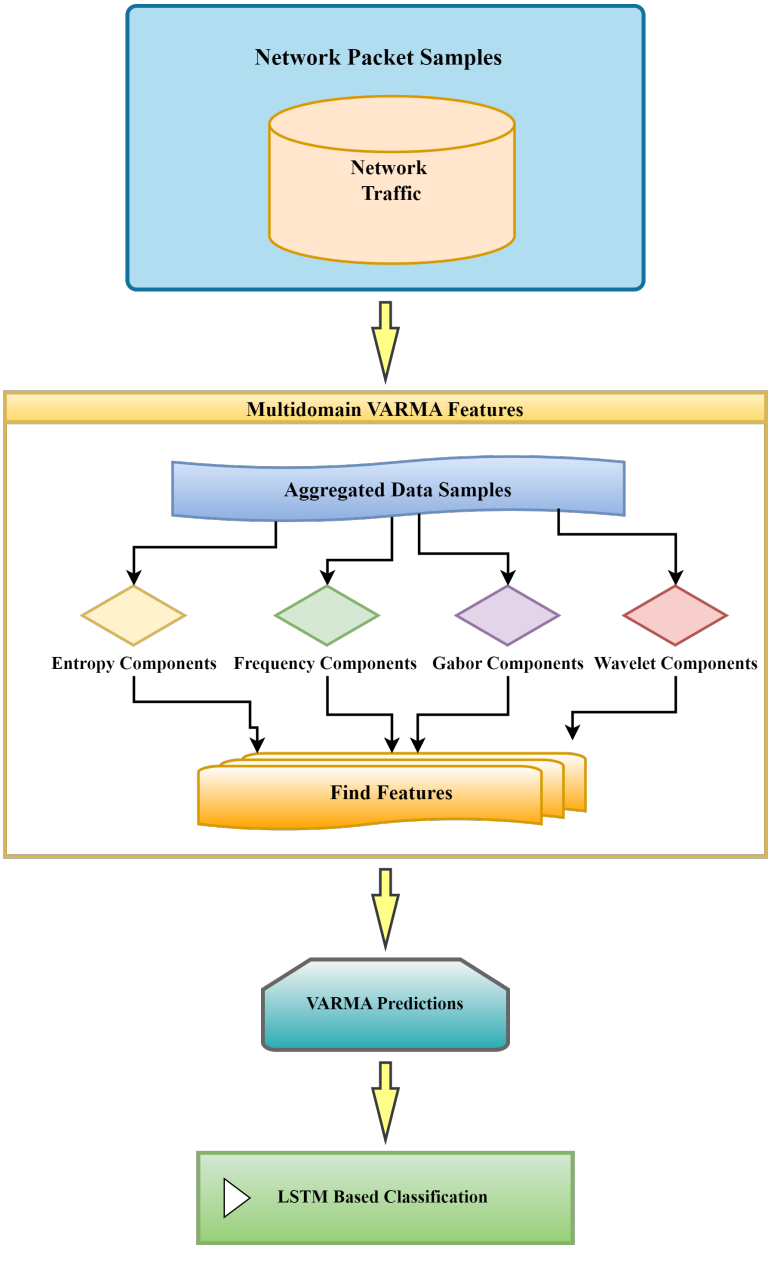
theorem and probability theory to analyse outcomes and identify DDoS attacks, with a particular focus on attacks due to resource depletion. The suggested technique used the transmission control protocol (TCP) preamble to distribute incoming packets for offline training and to improve detection accuracy. Chen et al. (2021) and Arturo et al. (2020) successfully employed a diverse range of machine learning methods to effectively detect and identify low-volume DDoS attacks, resulting in remarkable accuracy. In this research, they focused on novel application-layer DDoS attacks by examining distinctive attributes within incoming packets. These attributes encompassed dimensions such as HTTP frame packet dimensions, the volume of internet protocol (IP) addresses transmitted, steady port mappings, and the utilisation of proxy IP addresses. To gauge the efficacy of metrics-driven attack detection, a deep learning algorithm known as the multilayer perceptron (MLP) was employed (Ahmed et al., 2023).

These algorithms can be taught to recognise abnormalities in normal traffic by first being trained on a dataset consisting of normal traffic and then being used to analyse traffic in real-time. However, to train with this method, a significant quantity of data is necessary, and the quality of the data used for training can impact how accurately the algorithm performs (Derya and Anarim, 2020). They have investigated attacks against widely deployed internet of things (IoT) devices that exploit DDoS vulnerabilities in smart home environments. They also analyse the effects of these attacks on the power consumption of the affected devices. However, the report does not delve into the response of IoT sensors to such attacks (Tushir et al., 2020). The application of blockchain security features in IoT edge devices is noteworthy, as it involves segregating the control layer from the application layer. This separation facilitates the implementation of diverse features of the cellular network, including safeguarding data as well as authentication. Nevertheless, there are still hurdles to overcome, including the provision of energy-efficient resources and ensuring privacy (Yeh et al., 2020). Due to the mobility of vehicles within an inter-vehicle network, attackers can easily initiate an attack using DDoS, leading to a complete halt of all network services (Li et al., 2021b). The study presents a machine learning-based approach to identifying DDoS attacks in an SDN-WISE IoT controller. A detection module is integrated into the controller, utilising naive Bayes, decision tree, and support vector machine (SVM) algorithms to classify network packets. A controlled test environment is setup to simulate DDoS attack traffic, which is captured using a logging mechanism. The captured data is pre-processed to create a dataset for analysis. The study focuses on enhancing DDoS detection within SDN-IoT networks through effective machine learning techniques (Bhayo Jalal et al., 2023).

Utilising strategies for traffic categorisation is a third method for identifying DDoS attacks (Praseed and Thilagam et al., 2019; de Miranda Rios et al., 2021) through application-level packet analysis. Methods for classifying traffic can determine the nature of the traffic (e.g., HTTP, FTP, or SMTP) and identify any deviations from the typical structure of that traffic. However, this method can be very resource-intensive because it relies on comprehensive packet examination to categorise the traffic sets. This study delves into the concept of DDoS attacks, providing insights into the perspectives of the various studies conducted. It comprehensively explores the diverse array of potential DDoS attack types, accompanied by a range of machine learning approaches including naive Bayes, decision tree, SVM, random forest, and others. Furthermore, the discussion extends to encompass the multifaceted nature of DDoS attacks, covering

various manifestations, all of which are addressed within this article (Marwane et al., 2017).

Figure 1 Overall flow of the proposed model for identification of application-level DDoS attacks (see online version for colours)



There have been multiple attempts made by researchers using numerous detection methods, such as threshold-based detection, machine learning, traffic categorisation,

etc., to identify DDoS attacks through application-level packet analysis (Harada et al., 2022; Ravi and Shalinie, 2020; Li et al., 2019; Yungaicela-Naula et al., 2021; Alasmary et al., 2022; Doshi et al., 2021; Abubakar et al., 2020; Mohmand et al., 2022; Wang et al., 2018; Ding et al., 2021). These strategies have the potential to increase the precision of the monitoring system while simultaneously reducing the number of false positives. However, since they require the utilisation of a variety of different monitoring methods, they result in a significant investment of time and resources. Thus, application-level packet analysis is a potentially useful method for identifying DDoS attacks. Nevertheless, every strategy has its own set of benefits and drawbacks to consider. The choice of strategy will be determined by the specific needs of the system as well as the resources available in the given network deployment.

3 Proposed design of an efficient VARMA LSTM-based model for identification of DDoS attacks via application-level packet analysis

In the existing application-level DDoS attack detection models, it has been observed that either the developed system is very complex or it does not support multiple attack scenarios. To overcome these issues, we are proposing an efficient approach combining VARMA and LSTM-based model for the identification of DDoS attacks via application-level packet analysis. As shown in Figure 1, the proposed model originally uses an efficient VARMA model to learn hierarchical features from the raw packet data in multiple domains, including time, frequency, and spatial domains. The learned features are augmented via the LSTM model and then fed into a fully connected neural network for classification into multiple attacks.

The model initially collects application-level network parameters, including destination port, flow duration, total forwarded packets, total backward packets, total length of forwarded packets, total length of backward packets, forwarded packet length, maximum length of forwarded packet, minimum length of forwarded packet, standard deviation of forwarded packet length, minimum segmented size of forward packets, active mean, active standard deviation, active maximum, active minimum, idle mean, idle standard deviation, idle maximum, idle minimum, and the label of the packets. All these parameters are then converted into multidomain feature sets via frequency, entropy, spatial, approximate and detail components. These components assist in representing the packet parameters as feature vectors, which can be further processed through the hybrid VARMA LSTM process. To perform this task, frequency components are estimated using equation (1), where discrete Fourier transform (DFT) is employed for analysis as follows: the DFT is given by:

$$DFT_i = \sum_{j=1}^{N_f} x_j \left[\cos\left(\frac{2\pi ij}{N_f}\right) - \sqrt{-1}\sin\left(\frac{2\pi ij}{N_f}\right) \right] \tag{1}$$

where x and N_f represents value of the collected features, and total number of collected features.

Algorithm 1 Detection of application-level DDoS

Input: Network data samples
Output: Detection of application-level DDoS
Process:
for each input packet **do**
Find frequency, cosine, Gabor and wavelet features
Estimate VARMA coefficients as follows,
$y_t = c + A_1 y_{t-1} + A_2 y_{t-2} + ... + A_p y_{t-p} + B_1 e_{t-1} + B_2 e_{t-2} + ... + B_q e_{t-q} + e_t$
Estimate LSTM features as follows,
$h_t = f(W x_t + U h_{t-1} + b)$
$y'_t = g(V * h_t + c)$
end for
Apply GA for selection of features
for each iteration **do**
for each solution **do**
Identify stochastic solutions via selection of features
Find fitness as follows,
$f = \frac{1}{N} \sum_{i=1}^{N} \frac{t_{p_i} + t_{n_i}}{t_{p_i} + t_{n_i} + f_{p_i} + f_{n_i}}$
end for
end for
Use selected features for the classification process.

In a similar manner, entropy components are estimated via equation (2), where discrete cosine transform (DCT) is used, as follows: the DCT equation is given by:

$$\mathrm{DCT}_i = \frac{1}{\sqrt{2N_f}} x_i \sum_{j=1}^{N_f} x_j \cos\left[\frac{\sqrt{-1}(2i+1)\pi}{2N_f}\right] \tag{2}$$

where i and j are indices, N_f is a constant, x_i and x_j are variables, and cos denotes the cosine function.

To estimate spatial components, the VARMA model uses Gabor analysis, which is done as per equation (3),

The equation is given by:

$$G(x,y)_s = e^{-\frac{x'^2 + \partial^2 y'^2}{2\phi^2}} \cos\left(\frac{2\pi}{\lambda} x'\right) \tag{3}$$

where x, y are collected component indices and respective values, while ∂, $\varnothing$ and λ represents Gabor's angular and wavelength constants. For approximate and detailed analysis, the model uses Haar wavelet components which are estimated via equations (4) and (5) as follows,

The equation is given by:

$$W_a = \frac{x_i + x_{i+1}}{2} \tag{4}$$

$$W_d = \frac{x_i - x_{i+1}}{2} \tag{5}$$

where x_i and x_{i+1} are variables.

All these features are combined to form a VARMA DDoS feature vector (VFDV), which is processed by a fusion of VARMA and LSTM for identification of Application-level DDoS attacks.

VARMA is a statistical method commonly used for time-series analysis, including the detection of anomalies such as application-level DDoS attacks. The VARMA model is an extension of the autoregressive moving average (ARMA) model, which can capture dependencies and patterns of multiple variables simultaneously. The model can be represented by equation (6),

The equation is given by:

$$y_t = c + A_1 y_{t-1} + A_2 y_{t-2} + \ldots + A_p y_{t-p} + B_1 e_{t-1} + B_2 e_{t-2} + \ldots + B_q e_{t-q} + e_t \tag{6}$$

where y_t is a p-dimensional vector of observed VFDV variables at time t, c is a p-dimensional vector of constants, $A_1, A_2, \ldots, A_p$ are p × p matrices of autoregressive coefficients. e_t is a p-dimensional vector of error terms at time t, $B_1, B_2, \ldots, B_q$ are p × p matrices of moving average coefficients, q is the order of the moving average process.

To detect application-level DDoS attacks using VARMA, we initially modelled the normal traffic behaviour and identified deviations from it as potential attacks. The VARMA model was trained on the network traffic data during a period of normal operation, and then the model was used to predict the expected traffic behaviour. If the actual traffic deviates significantly from the expected behaviour, it may indicate the presence of a variation of application-level DDoS attacks.

We also used the residuals of the VARMA model as a measure of inconsistent behaviour sets. Residuals are the differences between the actual and predicted values, and their magnitude indicates the extent of deviation from the normal behaviour. If the residuals exceed a threshold, it may indicate the presence of an augmented set of application-level DDoS attacks.

LSTM and VARMA are two different models that can be used to analyse time-series data samples. This text combines these models to provide better performance for detecting application-level DDoS attacks in network traffic datasets. The combined model is called VARMA-LSTM, which utilises the strengths of both models to capture the complex temporal dependencies in the data samples. After estimating the VARMA coefficients, the LSTM coefficients are estimated via equations (7) and (8),

$$h_t = f(W x_t + U h_{t-1} + b) \tag{7}$$

$$y'_t = g(V h_t + c) \tag{8}$$

While, the combined coefficients are estimated via equation (9) as follows,

$$y_t = y'_t + e_t \tag{9}$$

where h_t is the hidden state of the LSTM model at timestamp t, f is the activation function of the LSTM model, such as the sigmoid or tanh function, W, U and V are the weight matrices of the LSTM model, b and c are the bias terms of the LSTM model

and the output layer, respectively, y'_t is the predicted output of the LSTM model at timestamp t, g is the activation function of the output layer, such as the softmax or linear functions.

Algorithm 2 Estimation of the value of k using a genetic algorithm

Result: Updated VARMA LSTM threshold for efficient identification of application-level DDoS attacks.
Input : NS: number of solutions to be generated
NE: total number of evaluation packets
NI: number of iterations to be performed
LR: learning rate for the genetic algorithm process
Output: k: the value of k that maximises fitness

Generate NS solutions by selecting stochastic value of k via equation (11);
for $i \leftarrow 1$ **to** NS **do**
  $k[i] \leftarrow$ stochastic_number_generation(0.1, 1);
end
for $i \leftarrow 1$ **to** NS **do**
  $fitness[i] \leftarrow 0$;
  for $j \leftarrow 1$ **to** NE **do**
    $tp[j], tn[j], fp[j], fn[j] \leftarrow$ test_VARMA_LSTM_model($k[i]$);
    $fitness[i] \leftarrow fitness[i] + (tp[j] + tn[j])/(tp[j] + tn[j] + fp[j] + fn[j])$;
  end
  $fitness[i] \leftarrow fitness[i]/NE$;
end
$f_{th} \leftarrow 0$;
for $i \leftarrow 1$ **to** NS **do**
  $f_{th} \leftarrow f_{th} + fitness[i] * LR$;
end
$f_{th} \leftarrow f_{th}/NS$;
for $iter \leftarrow 1$ **to** NI **do**
  for $i \leftarrow 1$ **to** NS **do**
    if $fitness[i] > f_{th}$ **then**
      Select another solution for crossover; crossover($k[i]$, $k[j]$);
    else
      Mutate $k[i]$ via equation (11);
    end
  end
end
$max\_fitness \leftarrow 0$;
for $i \leftarrow 1$ **to** NS **do**
  if $fitness[i] > max\_fitness$ **then**
    $max\_fitness \leftarrow fitness[i]$; $max_k \leftarrow k[i]$;
  end
end
update_VARMA_LSTM_threshold(max_k);

To detect application-level DDoS attacks using VARMA-LSTM, we trained the VARMA model on the network traffic data to capture temporal dependencies and predict expected

behaviours. Then, the residuals of the VARMA model were fed into the LSTM model as input sequences to further capture complex temporal patterns and detect inconsistencies. The LSTM model also learns the temporal patterns of the residual sequences and adjusts its predictions. The output of the LSTM model is combined with the predicted values from the VARMA model to obtain the final predictions. If the difference between the actual and predicted values exceeds a certain threshold, which is estimated via equation (10), it indicates the presence of an augmented set of application-level DDoS attacks.

$$\text{threshold} = \mu + k * \sigma \tag{10}$$

where μ is the mean of the residuals of the VARMA (p, q) model, σ is the standard deviation of the residuals, and k is a tuning parameter that controls the sensitivity of the threshold value sets. Threshold is the value above which the residuals are considered inconsistent. The value of k can be determined based on the desired false positive rate and false negative rates. A high value of k can lead to a high false positive rate, meaning that normal traffic may be incorrectly classified as an augmented set of attacks. A low value of k can lead to a high false negative rate, meaning that attacks may go undetected for real-time scenarios.

Thus, to estimate the value of k a genetic algorithm (GA) was used, which works as per the following operations.

Initially generate a set of NS solutions by selecting stochastic value of k via equation (11),

$$k = \text{STOCH}(0.1, 1) \tag{11}$$

where STOCH is a stochastic number generation process.

Based on this value, test the VARMA LSTM Model for different malicious and normal attack packets.

Estimate the fitness value of solution via equation (12),

$$f = \frac{1}{N} \sum_{i=1}^{N} \frac{t_{p_i} + t_{n_i}}{t_{p_i} + t_{n_i} + f_{p_i} + f_{n_i}} \tag{12}$$

where N represents total number of evaluation packets, while t_p, t_n, f_p and f_n represents the true positive, true negative, false positive and1 false negative rate for identification of normal and malicious packets.

This process is repeated for NS solutions, and a fitness threshold is estimated via equation (13),

$$f_{th} = \frac{1}{N_S} \sum_{i=1}^{N_S} f_i * LR \tag{13}$$

where LR is the learning rate for genetic algorithm process.

After generation of these solutions, if $f > f_{th}$, then current solution is cross over to the next iteration, otherwise it is mutated via equations (11) and (12), and then passed on the next set of iterations. This process is continued for N_i iterations, and new solutions are generated for each set of iterations. After completion of N_i iterations, solution with maximum fitness is selected, and its k value is used for updating VARMA

LSTM threshold for efficient identification of application-level DDoS attacks. Thus, the VARMA-LSTM model when combined with GA for threshold tuning provides better performance for detecting application-level DDoS attacks in network traffic data by combining the strengths of both models. Performance of this model was compared under different scenarios, and can be observed from the next section of this text.

4 Results and discussion

The proposed model employs an efficient VARMA model to learn hierarchical features from the raw packet data in time, frequency, and spatial domains. The learned features are augmented by the LSTM model and then combined to form a compact and informative representation of the packets. This representation is then input into a fully connected neural network for classification into multiple attacks. Experiments were conducted on real-world network datasets, including the application-layer DDoS dataset, which can be downloaded from Application Layer Dataset (https://www.kaggle.com/datasets/wardac/applicationlayer-ddos-dataset), were conducted to evaluate the proposed model under real-time scenarios. The accuracy of application-level DDoS classification (A), precision of classification (P), recall of classification (R), and approximation of the delay required for classification (d) operation sets were compared to verify the performance of this model. Equations (14), (15), (16) and (17) were used to determine these parameters, which were then compared to AE MLP (Wei et al., 2021), QLD CNN (Liu et al., 2020b), and SRNN (Alamri et al., 2020), which employ comparable projection techniques.

$$A = \frac{1}{N_c}\sum_{i=1}^{N_c}\frac{t_{p_i}+t_{n_i}}{t_{p_i}+t_{n_i}+f_{p_i}+f_{n_i}} \tag{14}$$

$$P = \frac{1}{N_c}\sum_{i=1}^{N_c}\frac{t_{p_i}}{t_{p_i}+f_{p_i}} \tag{15}$$

$$R = \frac{1}{N_c}\sum_{i=1}^{N_c}\frac{t_{p_i}}{t_{p_i}+t_{n_i}+f_{p_i}+f_{n_i}} \tag{16}$$

$$d = \frac{1}{N_c}\sum_{i=1}^{N_c}(t_{s_{\text{complete}_i}} - t_{s_{\text{start}_i}}) \tag{17}$$

where $t_{s_{\text{complete}_i}}$ and $t_{s_{\text{start}_i}}$ are the completion and starting timestamps for the classification process.

The dataset contains a total of 1.06 million records, consisting of different application-level DDoS classes. Out of the 1.06 million samples, nearly 650k samples were used for training, while 353k each were used for validation and testing operations. Based on this strategy, performance measures were evaluated, and the accuracy of application-level DDoS classification was tabulated with respect to different numbers of test samples (NTS) in Table 1.

Table 1 Average accuracy for estimation of application-level DDoS attacks

NTS	*Accuracy AE MLP*	*Accuracy QLD CNN*	*Accuracy SRNN*	*Accuracy VLMD ALP*
25k	77.02	83.23	82.22	90.95
42k	77.14	83.55	82.44	91.18
56k	77.24	83.86	82.64	91.4
70k	77.35	84.17	82.85	91.61
84k	77.46	84.48	83.06	91.83
100k	77.59	84.79	83.28	92.06
115k	77.73	85.1	83.51	92.29
130k	77.87	85.42	83.75	92.53
141k	78.02	85.73	83.98	92.77
155k	78.18	86.06	84.23	93.02
171k	78.33	86.4	84.48	93.27
185k	78.49	86.76	84.74	93.54
176k	78.66	87.14	85.01	93.82
211k	78.84	87.53	85.3	94.12
228k	79.03	87.94	85.59	94.43
242k	79.22	88.36	85.89	94.75
256k	79.42	88.78	86.2	95.07
270k	79.62	89.2	86.5	95.4
282k	79.82	89.63	86.81	95.73
298k	79.98	89.98	87.07	95.99
305k	80.13	90.32	87.31	96.25
329k	80.27	90.65	87.55	96.49
341k	80.4	90.97	87.78	96.73
353k	80.53	91.28	88.1	96.95

Table 2 Average precision for estimation of application-level DDoS attacks

NTS	*Precision AE MLP*	*Precision QLD CNN*	*Precision SRNN*	*Precision VLMD ALP*
25k	83.52	79.17	75.5	85.26
42k	83.74	79.77	75.9	85.68
56k	83.92	80.36	76.28	86.07
70k	84.1	80.95	76.68	86.46
84k	84.31	81.56	77.09	86.86
100k	84.56	82.18	77.53	87.29
115k	84.85	82.8	77.98	87.74
130k	85.13	83.42	78.45	88.21
141k	85.35	84.05	78.95	88.71
155k	85.46	84.68	79.49	89.24
171k	85.42	85.3	80.1	89.81
185k	85.23	85.92	80.76	90.42
176k	84.92	86.54	81.47	91.08
211k	84.54	87.15	82.21	91.75
228k	84.2	87.77	82.94	92.42
242k	83.97	88.39	83.63	93.07
256k	83.89	89.01	84.24	93.66
270k	83.96	89.63	84.79	94.2
282k	84.16	90.26	85.28	94.69
298k	84.37	90.88	85.74	95.15
305k	84.58	91.49	86.19	95.61
329k	84.74	92.1	86.66	96.07
341k	84.84	92.72	87.16	96.55
353k	84.9	93.33	87.68	97.05

Table 3 Average recall for estimation of application-level DDoS attacks

NTS	*Recall AE MLP*	*Recall QLD CNN*	*Recall SRNN*	*Recall VLMD ALP*
25k	70.08	74.32	80.93	85.54
42k	70.26	74.67	81.22	85.8
56k	70.41	75	81.5	86.05
70k	70.54	75.33	81.79	86.31
84k	70.67	75.66	82.08	86.58
100k	70.81	76	82.38	86.86
115k	70.97	76.35	82.69	87.14
130k	71.16	76.71	82.99	87.43
141k	71.38	77.09	83.29	87.73
155k	71.62	77.49	83.59	88.04
171k	71.87	77.92	83.9	88.37
185k	72.13	78.37	84.21	88.71
176k	72.4	78.83	84.54	89.07
211k	72.66	79.3	84.88	89.43
228k	72.9	79.76	85.22	89.79
242k	73.14	80.2	85.57	90.14
256k	73.38	80.63	85.92	90.48
270k	73.61	81.06	86.27	90.82
282k	73.85	81.48	86.61	91.15
298k	74.05	81.86	86.92	91.44
305k	74.25	82.24	87.22	91.74
329k	74.44	82.62	87.52	92.04
341k	74.64	83	87.82	92.33
353k	74.83	83.37	88.12	92.62

Table 4 Average delay for estimation of application-level DDoS attacks

NTS	*Delay AE MLP*	*Delay QLD CNN*	*Delay SRNN*	*Delay VLMD ALP*
25k	171.95	168.5	165.85	140.18
42k	172.59	170.03	166.86	141.08
56k	173.1	171.56	167.81	141.93
70k	173.56	173.11	168.77	142.78
84k	174.07	174.71	169.76	143.65
100k	174.66	176.34	170.81	144.54
115k	175.33	177.98	171.89	145.44
130k	176.07	179.58	172.97	146.28
141k	176.84	181.09	174.01	146.97
155k	177.64	182.63	175.07	147.72
171k	178.43	184.16	176.13	148.43
185k	179.21	185.67	177.16	149.11
176k	179.99	187.16	178.19	149.78
211k	180.77	188.68	179.24	150.49
228k	181.56	190.27	180.33	151.31
242k	182.34	191.81	181.38	152.05
256k	183.13	193.34	182.44	152.78
270k	183.91	194.88	183.49	153.51
282k	184.7	196.41	184.55	154.24
298k	185.48	197.95	185.6	154.98
305k	186.27	199.49	186.66	155.71
329k	187.05	201.02	187.71	156.44
341k	187.84	202.56	188.77	157.18
353k	188.62	204.09	189.82	157.91

The proposed model can accurately assess various application-level DDoS attacks due to its utilisation of multimodal feature extraction models along with the VARMA and LSTM processes. It was found that the proposed model was able to increase the attack detection accuracy by 15.16% when compared with AE MLP (Wei et al., 2021), 6.70% when compared with QLD CNN (Liu et al., 2020b), and 8.82% when compared with SRNN (Alamri et al., 2020) under different use cases. This accuracy was estimated with respect to various test samples as shown in Table 1. The use of GA-based threshold adjustment helps improve the categorisation performance even under smaller datasets and contributes to the enhancement of these accuracy levels. The precision for identifying these attacks was also calculated and demonstrated in Table 2 relative to the number of test samples (NTS).

It was found that our proposed model was able to increase attack recognition precision by 6.43% when compared to AE MLP (Wei et al., 2021), 4.73% when compared to QLD CNN (Liu et al., 2020b), and 9.59% when compared to SRNN (Alamri et al., 2020) under various use cases, as shown in Table 2.

By utilising multimodal feature extraction models in conjunction with the VARMA and LSTM processes, the proposed model can effectively assess various types of application-level DDoS attacks with a high recall rate. The proposed model was able to enhance the attack detection recall by 16.64% when compared to AE MLP (Wei et al., 2021), 10.26% when compared to QLD CNN (Liu et al., 2020b), and 4.51% when compared to SRNN (Alamri et al., 2020) under various use cases, as shown in Table 3. Similarly, the latency required for identification of these attacks was evaluated and contrasted in Table 4 relative to the type of attack, w.r.t. NTS.

As depicted in Table 4, the proposed system is able to increase attack recognition performance by 30.44% when compared to AE MLP (Wei et al., 2021), 37.02% when compared to QLD CNN (Liu et al., 2020b), and 28.36% when compared to SRNN (Alamri et al., 2020) under various use scenarios.

5 Conclusions

Our research focuses on devising a model for detecting application-level DDoS attacks with high accuracy, precision, recall, and speed. The model utilises a VARMA model for hierarchical feature learning from raw packet data in time, frequency, and spatial domains. The learned features are then augmented by an LSTM model and combined to form a compact and informative representation of the packets, which are classified into multiple application-level DDoS attacks using a fully connected neural network. The model also employs GA-based threshold adjustment to improve categorisation performance, especially with smaller data samples.

The integration of VARMA and LSTM techniques for detecting DDoS attacks through packet analysis presents potential drawbacks. These encompass concerns regarding data quality, computational complexity, interpretability, and the ability to generalise. To mitigate these limitations, it is imperative to employ strategies such as data augmentation and the incorporation of domain-specific features. These measures are pivotal in enhancing the overall performance of the model.

Future work includes validating the model's performance for a larger number of attacks and a larger dataset corpus, as well as exploring the use of Q-learning, transformer models, auto encoder-based models, generative adversarial networks

(GANs), and hybrid bio-inspired models to further improve the model's efficiency under heterogeneous attack scenarios and real-time situations.

References

Abou El Houda, Z., Khoukhi, L. and Hafid, A.S. (2020) 'Bringing intelligence to software defined networks: mitigating DDoS attacks', *IEEE Transactions on Network and Service Management*, Vol. 17, No. 4, pp.2523–2535.

Abubakar, R., Aldegheishem, A., Majeed, M.F., Mehmood, A., Maryam, H., Alrajeh, N.A., Maple, C. and Jawad, M. (2020) 'An effective mechanism to mitigate real-time DDoS attack', *IEEE Access*, Vol. 8, No. 1, pp.126215–126227.

Ahmed, S., Khan, Z.A., Mohsin, S.M., Latif, S., Aslam, S., Mujlid, H., Adil, M. and Najam, Z. (2023) 'Effective and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron', *Future Internet*, Vol. 15, No. 2, p.76.

Alamri, H.A. and Thayananthan, V. (2020) 'Bandwidth control mechanism and extreme gradient boosting algorithm for protecting software-defined networks against DDoS attacks', *IEEE Access*, Vol. 8, No. 1, pp.194269–194288.

Alasmary, F., Alraddadi, S., Al-Ahmadi, S. and Al-Muhtadi, J. (2022) 'ShieldRNN: a distributed flow-based DDoS detection solution for IoT using sequence majority voting', *IEEE Access*, Vol. 10, pp.88263–88275.

Almulhem, A. (2009) 'Network forensics: notions and challenges', *2009 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*, IEEE, pp.463–466.

Application Layer Dataset [online] https://www.kaggle.com/datasets/wardac/applicationlayer-ddos-dataset (accessed 9 October 2022)

Beitollahi, H., Sharif, D.M. and Fazeli, M. (2022) 'Application layer DDoS attack detection using cuckoo search algorithm-trained radial basis function', *IEEE Access*, Vol. 10, No. 1, pp.63844–63854.

Bhayo, J., Hameed, S. and Shah, S.A. (2020) 'An efficient counter-based DDoS attack detection framework leveraging software defined IoT (SD-IoT)', *IEEE Access*, Vol. 8, No. 1, pp.221612–221631.

Bhayo, J., Shah, S.A., Hameed, S., Ahmed, A., Nasir, J. and Draheim, D. (2023) 'Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks', *Engineering Applications of Artificial Intelligence*, Vol. 123, No. 1, p.106432.

Bhutto, A.B., Vu, X.S., Elmroth, E., Tay, W.P. and Bhuyan, M. (2022) 'Reinforced transformer learning for VSI-DDoS detection in edge clouds', *IEEE Access*, Vol. 10, No. 1, pp.94677–94690.

Biswas, R. and Wu, J. (2020) 'Optimal filter assignment policy against distributed denial-of-service attack', *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 1, pp.339–352.

Biswas, R., Kim, S. and Wu, J. (2021) 'Sampling rate distribution for flow monitoring and DDoS detection in datacenter', *IEEE Transactions on Information Forensics and Security*, Vol. 16, No. 1, pp.2524–2534.

Chen, X., Chen, Y., Feng, W., Xiao, L., Li, X., Zhang, J. and Ge, N. (2022) 'Real-time DDoS defense in 5G-enabled IoT: a multidomain collaboration perspective', *IEEE Internet of Things Journal*, Vol. 10, No. 5, pp.4490–4505.

Chen, X., Xiao, L., Feng, W., Ge, N. and Wang, X. (2021) 'DDoS defense for IoT: a Stackelberg game model-enabled collaborative framework', *IEEE Internet of Things Journal*, Vol. 9, No. 12, pp.9659–9674.

Cvitić, I., Perakovic, D., Gupta, B.B. and Choo, K.K.R. (2021) 'Boosting-based DDoS detection in internet of things systems', *IEEE Internet of Things Journal*, Vol. 9, No. 3, pp.2109–2123.

de Miranda Rios, V., Inácio, P.R., Magoni, D. and Freire, M.M. (2021) 'Detection of reduction-of-quality DDoS attacks using fuzzy logic and machine learning algorithms', *Computer Networks*, Vol. 186, No. 1, p.107792.

Ding, D., Savi, M. and Siracusa, D. (2021) 'Tracking normalized network traffic entropy to detect DDoS attacks in P4', *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 6, pp.4019–4031.

Ding, D., Savi, M., Pederzolli, F., Campanella, M. and Siracusa, D. (2021) 'In-network volumetric DDoS victim identification using programmable commodity switches', *IEEE Transactions on Network and Service Management*, Vol. 18, No. 2, pp.1191–1202.

Doriguzzi-Corin, R., Millar, S., Scott-Hayward, S., Martinez-del-Rincon, J. and Siracusa, D. (2020) 'LUCID: a practical, lightweight deep learning solution for DDoS attack detection', *IEEE Transactions on Network and Service Management*, Vol. 17, No. 2, pp.876–889.

Doshi, K., Yilmaz, Y. and Uludag, S. (2021) 'Timely detection and mitigation of stealthy DDoS attacks via IoT networks', *IEEE Transactions on Dependable and Secure Computing*, Vol. 18, No. 5, pp.2164–2176.

Elsaeidy, A.A., Jamalipour, A. and Munasinghe, K.S. (2021) 'A hybrid deep learning approach for replay and DDoS attack detection in a smart city', *IEEE Access*, Vol. 9, pp.154864–154875.

Erhan, D. and Anarim, E. (2020) 'Hybrid DDoS detection framework using matching pursuit algorithm', *IEEE Access*, Vol. 8, No. 1, pp.118912–118923.

Fu, Q.Y. and Wang, H.M. (2021) 'Detection of hijacking DDoS attack based on air interface traffic', *IEEE Wireless Communications Letters*, Vol. 10, No. 10, pp.2225–2229.

Guo, W., Xu, J., Pei, Y., Yin, L., Jiang, C. and Ge, N. (2022) 'A distributed collaborative entrance Defense framework against DDoS attacks on satellite internet', *IEEE Internet of Things Journal*, Vol. 9, No. 17, pp.15497–15510.

Haider, S., Akhunzada, A., Mustafa, I., Patel, T.B., Fernandez, A., Choo, K.K.R. and Iqbal, J. (2020) 'A deep CNN ensemble framework for efficient DDoS attack detection in software defined networks', *IEEE Access*, Vol. 8, No. 1, pp.53972–53983.

Hajimaghsoodi, M. and Jalili, R. (2022) 'RAD: a statistical mechanism based on behavioral analysis for DDoS attack countermeasure', *IEEE Transactions on Information Forensics and Security*, Vol. 17, No. 1, pp.2732–2745.

Harada, R., Shibata, N., Kaneko, S., Honda, K., Terada, J., Ishida, Y., Akashi, K. and Miyachi, T. (2022) 'Quick suppression of DDoS attacks by frame priority control in IoT backhaul with construction of Mirai-based attacks', *IEEE Access*, Vol. 10, No. 1, pp.22392–22399.

Huang, K., Yang, L.X., Yang, X., Xiang, Y. and Tang, Y.Y. (2020) 'A low-cost distributed denial-of-service attack architecture', *IEEE Access*, Vol. 8, No. 1, pp.42111–42119.

Hussain, B., Du, Q., Sun, B. and Han, Z. (2020) 'Deep learning-based DDoS-attack detection for cyber–physical system over 5G network', *IEEE Transactions on Industrial Informatics*, Vol. 17, No. 2, pp.860–870.

Jia, Y., Zhong, F., Alrawais, A., Gong, B. and Cheng, X. (2020) 'Flowguard: an intelligent edge defense mechanism against IoT DDoS attacks', *IEEE Internet of Things Journal*, Vol. 7, No. 10, pp.9552–9562.

Li, G., Zhang, M., Wang, S., Liu, C., Xu, M., Chen, A., Hu, H., Gu, G., Li, Q. and Wu, J. (2021) 'Enabling performant, flexible and cost-efficient DDoS defense with programmable switches', *IEEE/ACM Transactions on Networking*, Vol. 29, No. 4, pp.1509–1526.

Li, Y., Zhao, Y., Li, J., Yu, X., Zhao, Y. and Zhang, J. (2021a) 'DDoS attack mitigation based on traffic scheduling in edge computing-enabled TWDM-PON', *IEEE Access*, Vol. 9, No. 1, pp.166566–166578.

Li, Z., Kong, Y., Wang, C. and Jiang, C. (2021b) 'DDoS mitigation based on space-time flow regularities in IoV: a feature adaption reinforcement learning approach', *IEEE Transactions on Intelligent Transportation Systems*, Vol. 23, No. 3, pp.2262–2278.

Li, Z., Jin, H., Zou, D. and Yuan, B. (2019) 'Exploring new opportunities to defeat low-rate DDoS attack in container-based cloud environment', *IEEE Transactions on Parallel and Distributed Systems*, Vol. 31, No. 3, pp.695–706.

Liu, J., Wang, X., Shen, S., Yue, G., Yu, S. and Li, M. (2020) 'A Bayesian Q-learning game for dependable task offloading against DDoS attacks in sensor edge cloud', *IEEE Internet of Things Journal*, Vol. 8, No. 9, pp.7546–7561.

Liu, Z., Yin, X. and Hu, Y. (2020) 'CPSS LR-DDoS detection and defense in edge computing utilizing DCNN Q-learning', *IEEE Access*, Vol. 8, No. 1, pp.42120–42130.

Liu, Y., Tsang, K.F., Wu, C.K., Wei, Y., Wang, H. and Zhu, H. (2022) 'IEEE P2668-compliant multi-layer IoT-DDoS defense system using deep reinforcement learning', *IEEE Transactions on Consumer Electronics*, Vol. 69, No. 1, pp.49–64.

Maity, P., Saxena, S., Srivastava, S., Sahoo, K.S., Pradhan, A.K. and Kumar, N. (2021) 'An effective probabilistic technique for DDoS detection in OpenFlow controller', *IEEE Systems Journal*, Vol. 16, No. 1, pp.1345–1354.

Mohmand, M.I., Hussain, H., Khan, A.A., Ullah, U., Zakarya, M., Ahmed, A., Raza, M., Rahman, I.U. and Haleem, M. (2022) 'A machine learning-based classification and prediction technique for DDoS attacks', *IEEE Access*, Vol. 10, No. 1, pp.21443–21454.

Nwankwo, W., Chinedu, P.U., Masajuwa, F.U., Njoku, C.C. and Imoisi, S.E. (2023) 'Adoption of i-voting infrastructure: addressing network-level cybersecurity breaches', *Electronic Government, an International Journal*, Vol. 19, No. 3, pp.273–303.

Perez-Diaz, J.A., Valdovinos, I.A., Choo, K.K.R. and Zhu, D. (2020) 'A flexible SDN-based architecture for identifying and mitigating low-rate DDoS attacks using machine learning', *IEEE Access*, Vol. 8, No. 1, pp.155859–155872.

Praseed, A. and Thilagam, P.S. (2019) 'Multiplexed asymmetric attacks: next-generation DDoS on HTTP/2 servers', *IEEE Transactions on Information Forensics and Security*, Vol. 15, No. 1, pp.1790–1800.

Praseed, A. and Thilagam, P.S. (2020) 'Modelling behavioural dynamics for asymmetric application layer DDoS detection', *IEEE Transactions on Information Forensics and Security*, Vol. 16, No. 1, pp.617–626.

Praseed, A. and Thilagam, P.S. (2022) 'HTTP request pattern based signatures for early application layer DDoS detection: a firewall agnostic approach', *Journal of Information Security and Applications*, Vol. 65, No. 1, p.103090.

Ravi, N. and Shalinie, S.M. (2020) 'Learning-driven detection and mitigation of DDoS attack in IoT via SDN-cloud architecture', *IEEE Internet of Things Journal*, Vol. 7, No. 4, pp.3559–3570.

Shi, L., Li, J., Zhang, M. and Reiher, P. (2021) 'On capturing DDoS traffic footprints on the internet', *IEEE Transactions on Dependable and Secure Computing*, Vol. 19, No. 4, pp.2755–2770.

Tushir, B., Dalal, Y., Dezfouli, B. and Liu, Y. (2020) 'A quantitative study of DDoS and e-DDoS attacks on wifi smart home devices', *IEEE Internet of Things Journal*, Vol. 8, No. 8, pp.6282–6292.

Wahab, O.A., Bentahar, J., Otrok, H. and Mourad, A. (2017) 'Optimal load distribution for the detection of VM-based DDoS attacks in the cloud', *IEEE Transactions on Services Computing*, Vol. 13, No. 1, pp.114–129.

Wang, A., Chang, W., Chen, S. and Mohaisen, A. (2018) 'A data-driven study of DDoS attacks and their dynamics', *IEEE Transactions on Dependable and Secure Computing*, Vol. 17, No. 3, pp.648–661.

Wei, Y., Jang-Jaccard, J., Sabrina, F., Singh, A., Xu, W. and Camtepe, S. (2021) 'AE-MLP: a hybrid deep learning approach for DDoS detection and classification', *IEEE Access*, Vol. 9, No. 1, pp.146810–146821.

Yeh, L.Y., Lu, P.J., Huang, S.H. and Huang, J.L. (2020) 'SOChain: a privacy-preserving DDoS data exchange service over SOC consortium blockchain', *IEEE Transactions on Engineering Management*, Vol. 67, No. 4, pp.1487–1500.

Yungaicela-Naula, N.M., Vargas-Rosales, C. and Perez-Diaz, J.A. (2021) 'SDN-based architecture for transport and application layer DDoS attack detection by using machine and deep learning', *IEEE Access*, Vol. 9, No. 1, pp.108495–108512.

Zekri, M., El Kafhali, S., Aboutabit, N. and Saadi, Y. (2017) 'DDoS attack detection using machine learning techniques in cloud computing environments', *2017 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech)*, IEEE, pp.1–7.

Zhou, Y., Cheng, G. and Yu, S. (2021) 'An SDN-enabled proactive defense framework for DDoS mitigation in IoT networks', *IEEE Transactions on Information Forensics and Security*, Vol. 16, No. 1, pp.5366–5380.