ADVANCEMENTS IN MACHINE LEARNING ALGORITHMS WITH SELF-UPDATE PARAMETER CALIBRATION FOR DDOS INTRUSION DETECTION: A LITERATURE REVIEW

Ainebyoona Patrick and Adeleke Raheem Ajiboye

Department of Computer Science, Kampala
International University, Uganda

ABSTRACT

Distributed Denial of Service (DDoS) attacks have become some of the most common and damaging cyberthreats in our increasingly connected world. This literature review explores recent developments in using machine learning algorithms to detect DDoS intrusions, with a special emphasis on approaches that fine-tune self-updating parameters. By bringing together insights from multiple recent studies. This review examines a variety of machine learning methods such as Random Forest (RF), Support Vector Machine (SVM), and K-Nearest Neighbours (KNN). It looks at the strengths and weaknesses of each technique and discusses how best to integrate them with the existing security infrastructure. Particular attention is given to self-updating models that can quickly adapt to new and evolving attack patterns. The paper also reviews performance metrics, important considerations around datasets, and outlines future research directions in this fast-moving area. Overall, the findings indicate that adaptive, self-updating machine learning models outperform static ones in detecting complex DDoS attacks, with Random Forest approaches consistently delivering strong results across various studies.

KEYWORDS

DDoS detection, self-updating algorithms, Adaptive Parameter Calibration, Intrusion Detection Systems. Machine learning.

1. INTRODUCTION

Cybersecurity risks have become more sophisticated and widespread in today's digital environment, which is marked by the growth of Internet of Things (IoT) devices and increasingly intricate network infrastructures. Over 65% of all network attacks globally are Distributed Denial of Service (DDoS) attacks, making them stand out among these threats as being very disruptive. [1]. point out their vulnerability to zero-day attacks, calling for adaptive systems. This review bridges this gap by focusing on self-updating ML models that address concept drift.

The evolution of DDoS attacks has been phenomenal, progressing from the initial flooding methods to highly advanced, multi-vector attacks that possess the ability to adapt to defence systems in real time. As stated by Abirama sundari and Ramaswamy, "DDoS attacks have

 DOI:10.5121/ijci.2025.140502

become a critical issue in cyber security. This can result in temporary or even permanent loss of service to users" [2].

The impact extends beyond the interruption of services, typically resulting in massive financial loss, reputational damage, and loss of customer confidence.

Traditional intrusion detection systems (IDS) have struggled to keep pace with these evolving threats. Static rule-based systems, while effective at identifying known attack signatures, fail to identify new attack vectors or variations on old ones. This has led researchers and security practitioners to pursue more adaptive solutions, with machine learning emerging as a promising solution.

Machine learning algorithms offer several advantages for DDoS detection. They can identify patterns in network traffic that might be indistinguishable to human analysts, learn new attack signatures without being explicitly programmed, and operate at scale on large network infrastructures. However, their utility is highly a function of their design, implementation, and ability to update their parameters based on emerging attack patterns.

This literature review examines recent advancements in machine learning algorithms for DDoS intrusion detection, with a particular focus on self-update parameter calibration techniques. By synthesizing findings from multiple studies, this review aims to provide a comprehensive understanding of the current state of research in this field, identify promising approaches, and highlight areas for future investigation.

The review is structured as follows: Section 2 provides background information on DDoS attacks and their evolution; Section 3 examines various machine learning approaches for intrusion detection; Section 4 focuses specifically on self-update parameter calibration techniques; Section 5 discusses performance evaluation metrics; Section 6 presents a comparative analysis of different machine learning techniques; Section 7 explores future research directions; and Section 8 concludes the review with key insights and recommendations.

2. BACKGROUND ON DDOS ATTACKS

2.1. Definition and Types of DDoS Attacks

Distributed Denial of Service attacks refer to a form of cyberattack that target disrupting the regular functionality of a network, service, or website by overwhelming it with an excess of fake traffic. Unlike traditional Denial of Service (DoS) attacks that originate from a single source, DDoS attacks leverage a number of hijacked systems, usually referred to as a botnet, and create attack traffic from a variety of distributed sources [3].

The categorization of DDoS attacks has evolved over the years. The earlier attacks were largely volumetric in nature, i.e., UDP and ICMP flooding, that attempt to consume bandwidth by sending large volumes of packets to the victim. As defences improved, the attackers also grew sophisticated in their methodology, leveraging TCP SYN floods that drain connection resources, application-layer attacks that target specific weaknesses in web applications, and reflection/amplification attacks that exploit legitimate services to multiply attack traffic [4].

Researcher [1] indicates that "some of the rampant DDoS attacks are SYN flooding, UDP flooding, DNS-based flooding, ICMP directed broadcast, Ping flood attack, IP fragmentation, and

CGI attacks" [1]. All of these types of attacks represent their own respective detection and prevention challenges, and increasingly sophisticated defence techniques are required.

Hoque et al. [5] highlighted the changing trends of botnet-driven DDoS attacks, highlighting the need for adaptive detection mechanisms to counter constantly evolving threats.

Zargar et al. [6] provided a comprehensive review of DDoS mitigation methods, categorizing defence methods based on attack phases (prevention, detection, response).

2.2. Evolution and Impact of DDoS Attacks

The evolution of DDoS attacks has been driven by various factors including increased availability of vulnerable IoT devices, building of attack-for-hire platforms and increased complexity and sophistication of attack tools. This development has witnessed the emergence of attacks of unprecedented size and complexity.

Some of the most notable instances are the Dyn attack in 2016 that employed the Mirai botnet to bring down leading internet platforms in North America and Europe, as explained by Antonakakis et al. [7], the Mirai botnet revealed the devastating potential of IoT-powered DDoS attacks, employing vulnerable devices to generate record-breaking attacks. Also [1] states that, "hitting and taking down a DNS server puts millions of websites in the dark because users become unable to resolve domain names, as during the attack of Dyn in 2016" [1].

The Mirai botnet attack in 2016 [7] showed how IoT devices amplify DDoS scale, causing $2M+ damage per attack [5]. Currently, attackers evade detection using adversarial ML, e.g., perturbing traffic patterns to mislead static models [12].

The impact of DDoS attacks is not just the immediate service disruption. Organizations incur significant financial losses due to downtime, remediation costs, and potential regulatory penalties. In 2021, a report put the cost of a typical DDoS attack on businesses at approximately $2 million, and this continues to rise [8]. In addition, the attacks are typically employed as smokescreens for more advanced intrusions, diverting security resources while attackers target other objectives.

2.3. Challenges in DDoS Detection

Detection of DDoS attacks is extremely difficult for a number of reasons. First, the distributed nature of the attack makes it difficult to distinguish between legitimate traffic surge and the attack traffic. Second, attackers increasingly employ techniques to make their traffic appear legitimate by using proper TCP connections or mimicking normal user behavior. Third, high volume and high velocity of the network data make analysis in real-time extremely compute-intensive.

Kumari and Mrunalini emphasize that "DDoS attacks are the most difficult security problems to detect, mitigate, and trace today" due to "the limitations of conventional networking devices, the unpredictability of attack techniques, and the programmers' invisibility to host sites [9]. All these challenges are further compounded by the constant innovation of new attack techniques, to which the detection systems must adapt in turn.".

As noted by Aineyoona, "due to the uniformity and evolution of DDoS attack modes and the diverseness of attack traffic size, there has not been a detection method with desirable detection accuracy so far" [1]. This observation justifies the need for more adaptive and intelligent

detection techniques, particularly those that are founded on machine learning approaches with self-update capabilities.

3. MACHINE LEARNING APPROACHES FOR INTRUSION DETECTION

3.1. Supervised Learning Methods

Supervised learning algorithms have proven to be very promising for DDoS attack detection since they are able to learn from labelled examples of normal and attack traffic. The algorithms learn models that are able to predict new, unseen traffic patterns from features of the training data.

Table 1: Comparative Performance of ML Algorithms for DDoS

Algorithm	Accuracy (Dataset)	Strengths	Limitations	Key Study
Random Forest	98.9% (CICIDS2017)	Robust to overfitting	High memory usage	[2]
SVM	98.7% (CICIDS2018)	Works with small data	Sensitive to kernels	[2]
KNN	98.7% (CICDDoS2019)	No training phase	Slow for large data	[2]

3.2. Random Forest

Random Forest has been proven to be one of the most effective algorithms for DDoS detection in numerous researches. It is an ensemble learning method that creates a forest of several decision trees during training time and outputs the class corresponding to the mode of classes of individual trees. Its ability to operate on high-dimensional data, identify intricate patterns, and prevent overfitting renders it robust.

Abiramasundari and Ramaswamy proved that "RF achieves the highest accuracy of 98.9% on CICIDS2017" than other supervised learning techniques [2]. Similarly, Aineyoona's work showed that a Random Forest model trained using self-update parameter calibration achieved an accuracy of 96% in a real-time dataset [1]. These findings show that Random Forest has a strong foundation for DDoS detection systems, particularly when combined with adaptability.

3.3. Support Vector Machine (SVM)

Support Vector Machine algorithms distinguish data by finding the hyperplane with the highest margin between different classes in the feature space. In the context of DDoS detection, SVM has been extremely effective, particularly for use in binary classification for distinguishing between normal and attack traffic.

Abiramasundari and Ramaswamy have reported that "on the CICIDS2018 dataset, SVM achieves the best accuracy of 98.7%" [2]. But the performance of SVM may be feature selection dependent and parameter tuning dependent, so self-update calibration methods are promising.

3.4. K-Nearest Neighbors (KNN)

The K-Nearest Neighbors algorithm classifies new points into the most common class among their k nearest neighbors in feature space. It is a conceptually straightforward method but can be extremely effective at DDoS detection if the appropriate distance measures and feature representations are employed.

Research by Abiramasundari and Ramaswamy found that "in the CICDDoS2019 dataset, RF and KNN attain a higher accuracy of 98.7"[2], i.e., KNN can be as good as more advanced algorithms for certain datasets. However, KNN's computational requirements can increase exponentially with bigger datasets, which might limit its application for real-time detection in heavy-traffic networks.

3.5. Decision Tree

Decision Tree algorithms construct a model that predicts the value of a target variable by learning simple decision rules induced from the data features. Decision Tree algorithms are advantageous in terms of interpretability because the resulting models can be interpreted and visualized by human analysts.

While Decision Trees alone will not be optimal at best accuracy for DDoS detection, they are utilized to build stronger ensemble methods like Random Forest. Decision Trees are among those supervised models that can effectively "differentiate between attack and regular traffic" if used in combination with appropriate feature selection methods, as mentioned by Abiramasundari and Ramaswamy [2].

3.6. Logistic Regression and Naive Bayes

Logistic Regression and Naive Bayes are slightly more elementary machine learning techniques that have nevertheless been of use for DDoS filtering. Logistic Regression predicts the probability of a binary outcome relative to one or more predictor variables, while Naive Bayes applies Bayes' theorem with strong independence assumptions among features.

Kumari and Mrunalini also suggested a mathematical model for DDoS attacks with "Logistic Regression and Naive Bayes models. to detect DDoS attacks" [9]. Their work showed that these algorithms are capable of having decent detection accuracy without using much computational resources compared to other complicated methods, thus being ideal for resource-limited environments.

3.7. Deep Learning Approaches

Deep learning techniques, particularly those based on neural networks, have drawn interest in DDoS detection studies due to their ability to automatically learn hierarchical feature representations of raw data. Such techniques are capable of discovering subtle patterns in network traffic that might be missed by conventional machine learning techniques.

Various neural network architectures have been researched in recent work for DDoS detection, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and their combination. For instance, a piece of work Abiramasundari and Ramaswamy referred to constructed "a faster and easier-to-use deep learning algorithm for faster processing and better

results"[2]. Yin et al. [10] employed Recurrent Neural Networks (RNNs) for intrusion detection and demonstrated their capacity to learn temporal dependencies from network traffic.

Saied et al. [11] demonstrated that ANNs could recognize known and novel DDoS attacks by being trained with the complex traffic patterns, yet their 'black-box' nature is still a concern. Mirsky et al. [12] presented Kitsune, a set of autoencoders for real-time intrusion detection, emphasizing the strength of light-weight deep learning models in high-speed networks

While deep learning (e.g., RNNs [12]) can recognize fine patterns, its 'black-box' nature and susceptibility to adversarial attacks [9] restricts its use in security-critical applications. They tend to require more training data and computational resources than traditional machine learning algorithms. Additionally, the "black box" nature of the models might make it hard to interpret their decisions, which might prevent their use in security-critical applications where interpretability is preferred.

3.8. Feature Selection Techniques

Machine learning algorithm performance on DDoS detection is considerably dependent on feature extraction from traffic. Feature selection techniques attempt to identify the most effective features in reducing dimension, thereby improving performance and computational efficacy.

Principal Component Analysis (PCA) has also been an extremely effective technique of feature selection for application to DDoS detection. Abiramasundari and Ramaswamy proposed a "PCA-based Enhanced Distributed DDoS Attack Detection (EDAD) framework" which performed well on a variety of different data sets [2]. Thus, by reducing the number of features to be processed but without sacrificing the most important information from the data, PCA can improve the performance of many machine learning algorithms.

Kozik et al. [13] proposed a scalable distributed ML framework for edge computing attack detection that addressed the problems of real-time feature processing in decentralized environments.

Other feature selection approaches that have been considered in the literature include information gain, chi-squared testing, and correlation-based approaches. The optimal approach will be based on the specific characteristics of the network environment and the type of attacks being countered.

4. SELF-UPDATE PARAMETER CALIBRATION TECHNIQUES

4.1. Definition and Importance

Self-update parameter calibration is the ability of a machine learning model to learn to update its parameters automatically as a function of changing data patterns or environmental factors. In the case of DDoS detection, this proves particularly valuable in light of the dynamic nature of attack techniques and the dynamic nature of network traffic.

Aineyoona also emphasizes that "in order to counteract these attacks in the long term, self-updating models should be created" [1]. Such a statement is an expression of acceptance that static models, however they are originally trained on large data sets, over time will reduce their efficiency since attack methodologies change. Self-updating models are better because they

continuously improve their parameters based on new observations and hence maintain their detectability over time.

4.2. Implementation Approaches

There have been various suggestions for the use of self-update parameter calibration in DDoS detection mechanisms. All these are grouped into three categories: online learning techniques, reinforcement learning techniques, and hybrid techniques based on a mix of multiple adaptation techniques.

Online learning processes update model parameters incrementally as new data arrives, without having to redo the complete training process. This is particularly suited for detecting DDoS, where there can be steady amounts of network traffic data available to continually refine the model's understanding of normal and attack patterns.

Reinforcement learning approaches set the detection task as a sequence decision-making task, where the model learns to maximize a reward signal (such as successful attack detection) by exploring the environment. These approaches can be extremely powerful for learning how to change to adapt in adversarial settings in which the attackers actively adapt their behaviour in an attempt not to get discovered.

Hybrid methods pair various adaptation techniques to leverage their individual merits. For instance, Aineyoona's proposed method combines "two steps: Feature extraction and model detection" [1], whereby features are dynamically extracted based on discovered traffic behaviours and then used to update the detection model.

4.3. Advantages over Static Models

Self-learning models have several key advantages over static approaches for DDoS detection. Firstly, they are able to learn to handle concept drift, whereby the statistical properties of the target variable change over time. In DDoS attacks, this drift occurs because the attackers adapt their tactics in order to evade detection.

Second, self-updating models are updated using new knowledge independently of human interaction or complete retraining. This attribute is particularly valuable in operational environments where human intervention should be kept to a minimum for efficiency and scalability.

Third, these models are able to discover new attack patterns that did not exist in the original training data. Through constant updating of their knowledge of normal and abnormal traffic patterns, self-updating models can identify previously unknown attack vectors based on how far they deviate from known normalcy profiles.

Self-refreshing RF models are 96% accurate in live tests [1], reducing false negatives by 30% compared to static ones. Kozik et al. [13] also show these models cut computational latency by 50% in edge deployments.

Aineyoona's research demonstrated that a "Machine learning algorithm with self-update parameter calibration" achieved a 96% accuracy level on a live dataset [1], which bears witness to the usability of the approach. This result is particularly noteworthy in the context of the challenge of detecting DDoS attacks in real-world network conditions.

4.4. Real-time Adaptation Capabilities

The ability to adapt in real time is a prominent characteristic of real-time self-update parameter calibration for DDoS detection. Real-time adaptation enables detection systems to respond immediately to emerging attack trends, possibly mitigating their impact before causing serious harm.

Facilitating real-time adaptation requires careful consideration of computational efficiency, as the update process should not introduce unwarranted latency that would detract from the system's ability to process high-density network traffic. A number of mechanisms have been proposed to counteract this challenge, including incremental update algorithms, parallel processing architectures, and selective update strategies that focus computational attention on the most relevant model entities.

Aineyoona's research called for "a real time detection mechanism, that can deal with various types of attacks" [1]. It is an indicator that the timeframe for effective action when a DDoS attack is launched is typically short-lived, and swift detection and adaptability are necessary to limit damage.

5. PERFORMANCE EVALUATION METRICS

5.1. Accuracy, False Negative Rate, and False Positive Rate

The performance of DDoS detection systems is typically measured using a range of key performance indicators, but especially accuracy, false negative rate (FNR), and false positive rate (FPR) are important. Accuracy measures the general accuracy of the model's predictions, whereas FNR and FPR measure certain types of errors.

Low false negative rate is especially crucial for security applications because undetected attacks (false negatives) can result in successful service disruption. Low false positive rate is of concern for operational effectiveness because false alarms (false positives) can consume analyst time and could result in unnecessary defensive countermeasures that themselves cause disruption to service.

Aineyoona's paper validated their model "by three metrics (accuracy, false negative rate and false positive rate)" [1], which reflects the multi-dimensional nature of performance measurement for DDoS detection systems. This broad measurement approach provides a more accurate characterization of a model's capabilities and limitations than with one metric.

5.2. Comparative Analysis of Different Algorithms

Comparative analyses of different algorithms using standardized data and metrics provide valuable insights into their comparative advantages and disadvantages for detecting DDoS. Such analyses help researchers and practitioners select the most apt methodologies for specific operational contexts.

Abiramasundari and Ramaswamy performed a comparative analysis of some supervised learning algorithms in detail and concluded that "RF achieves the highest accuracy of 98.9% on CICIDS2017. RF and KNN have the highest accuracy of 98.7 in CICDDoS2019 dataset. SVM has the highest accuracy of 98.7% in CICIDS2018 dataset" [2]. These findings support the

dataset-dependent nature of algorithmic performance and suggest that the optimal method could very well be dependent on the idiosyncrasies of the network environment.

Similarly, Kumari and Mrunalini cross-compared Logistic Regression and Naive Bayes algorithms and studied "various performance measures of these algorithms" to "find the best algorithm that provides the best accuracy" [9]. All such comparative research contributes to the knowledge base regarding algorithm performance, which serves future research work and deployment.

5.3. Dataset Considerations

The data used for training and testing DDoS detection models significantly influence their performance and reliability. CICIDS2017, CICIDS2018, CICDDoS2019, and CAIDA 2007 are among the standardized datasets adopted as benchmarks.

These datasets vary in composition, including the kind of attack they represent, the mix of normal and attack traffic, and the network environments from which samples are drawn. As a consequence, results on one dataset will not necessarily translate to similar results in other operational contexts.

Abiramasundari and Ramaswamy validated their proposed framework on "CICIDS2018, CICIDS2017, and CICDDoS-2019 datasets" [2], while Kumari and Mrunalini used the "CAIDA 2007 Dataset" for experimentation [9]. This difference in test datasets provides a clearer picture of model performance across different scenarios.

However, it must be noted that even the most complete public datasets are not necessarily an ideal representation of the variety and intricacy of actual network environments. As Aineyoona's case, whose model "achieved accuracy of 96% over a real-time dataset" [1], illustrates, real-time data testing gives particularly valuable information about pragmatic efficacy.

5.4. Real-world Applicability

The real proof of the merit of a DDoS detection system is to see how well it performs under actual operating conditions. While experiments using standardized test sets in controlled laboratory environments provide useful insights, they cannot come even close to simulating practical deployment issues such as real-time handling of volume traffic, dynamically changing attack behaviors, and interoperation with deployable security infrastructures.

In practical implementations, distributed ML platforms like Kozik et al. [13] achieve 94% detection rates on edge devices, proving feasibility in low-resource IoT networks.

Aineyoona's research centered on real-world application by designing a model specifically for "intrusion detection of DDoS in communication networks" [1]. The focus on real-world application is a sign of the recognition that theoretical performance must ultimately translate to working effectiveness if a detection system is to provide genuine value.

Criteria that impact practical usability in real-world settings encompass computational efficiency, scalability to support increasing traffic volume, robustness to varying network conditions, and interpretability to support analysts' decision-making. Evaluation approaches addressing these criteria yield a more integrated view of the practical utility of a detection system.

6. COMPARATIVE ANALYSIS OF MACHINE LEARNING TECHNIQUES

6.1. Strengths and Limitations of Different Approaches

Each machine learning technique for DDoS detection also possesses its own strengths and weaknesses that influence its suitability in specific operational contexts. Knowledge of these is essential to select the most appropriate technique for a given context.

Random Forest models have uniformly high performance in many studies and datasets. They have the benefits of insensitivity to overfitting, ability to deal with high-dimensional data, and ability to model complex relationships between features. However, they may consume more computational resources than more basic methods and are less explainable than individual decision trees.

Support Vector Machines offer good theoretical guarantees and work well even when training data is scarce. However, their performance is sensitive to parameters as well as features, which can require more experience to apply efficiently.

K-Nearest Neighbors algorithms are cognitively simple and can learn complicated decision boundaries without training. Their computational requirement, however, increases with the size of the dataset, and they might not be applicable in high-volume network environments.

Deep learning methods can potentially learn hierarchical representations of features and possibly catch intricate patterns that non-deep-learning algorithms miss. They typically demand more training data, computational resources, and offer less interpretability.

6.2. Performance Across Different Attack Types

Effectiveness of machine learning techniques may vary greatly for different types of DDoS attacks. For instance, volumetric attacks, which attempt to deplete bandwidth with high-volume traffic, may pose different detection challenges from protocol attacks on specific network protocols or application-layer attacks on vulnerabilities of web applications.

Research by Aineyoona considered "Four categories that is; attack packets of UDP, TCP and ICMP flood and Http Slow" [1], recognizing the value in evaluating detection performance across a variety of attack vectors. This inclusive approach provides perspective on the robustness of detection mechanisms across the spectrum of DDoS attack techniques.

It is necessary to comprehend these performance disparities to develop detection systems that can most effectively deal with the full range of potential threats. In some cases, ensemble techniques that combine multiple detection techniques may provide the most comprehensive protection by exploiting the strengths of different algorithms for different kinds of attacks.

6.3. Computational Efficiency and Scalability

Computational complexity and scalability are critical aspects to take note of for DDoS detection systems, particularly those that require operation within high-traffic network environments. The computational burden of different machine learning approaches may vary significantly, which impacts the level of real-time detectability.

Less complicated algorithms like Logistic Regression and Naive Bayes typically require less processing power, so they may be better suited to systems with low processing capacity. More advanced techniques like Random Forest and deep learning models may offer higher detection accuracy but at the cost of increased computational needs.

Scalability issues extend beyond the initial training to include the computational requirements of model updating and inference. Self-updating models must balance the benefits of continuous adaptation against the computational expense of parameter updates, particularly in high-throughput applications where processing latency must be minimized.

6.4. Integration with Existing Security Infrastructure

The practical use of machine learning techniques for DDoS detection depends significantly on their ability to be integrated into existing security infrastructure. This integration consists of technical aspects, for example, joining machine learning with network monitoring systems, and operational aspects, for example, being compatible with existing security procedures.

Effective integration needs to consider issues such as data collection processes, alerting and prioritization, and coordination with other security measures. Machine learning models that generate excessive false positives or provide limited contextual information may struggle to be adopted within operational security teams, even with theoretical detection capability.

Aineyoona's research, developed to create a model "to improve intrusion detection of DDoS in communication networks" [1], tacitly confirms the importance of real-world incorporation by addressing one specific operational requirement within existing frameworks of network protection.

7. FUTURE DIRECTIONS

7.1. Emerging Trends in DDoS Detection

There are several emerging trends that are shaping the future of DDoS detection practice and research. These include the increasing application of deep learning techniques, the development of more sophisticated feature engineering techniques, and the exploration of unsupervised and semi-supervised learning techniques that can perform effectively with little labelled data.

Buczak and Guven [14] surveyed ML for cybersecurity and highlighted hybrid approaches that wedded supervised and unsupervised learning as one answer to data scarcity in new attack detection.

1. Explainable AI (XAI): Interpretable models are vital to gain analysts' trust, emphasize Buczak and Guven [14].
2. Federated Learning: Enables privacy-preserving collaboration across networks (e.g., healthcare IoT.
3. Edge-Deployed Models: Light-weight algorithms like Kitsune are critical for 5G and IoT scalability [12]

Abiramasundari and Ramaswamy noted a "growing focus towards shifting from unsupervised to supervised learning, with the use of both labelled and unlabelled datasets, for better detection" [2]. This trend illustrates the recognition that purely supervised approaches can be limited by the lack of fully labelled datasets, particularly for new attack vectors.

Another critical trend is increasing emphasis on explainable AI for security applications. As machine learning models continue to increase in complexity, there is a growing interest in techniques that are able to provide interpretable explanations of their decisions, to support analyst understanding and trust.

7.2. Integration with Other Security Systems

The extension of DDoS detection to integrated security systems is an interesting direction for enhancing overall defences. This integration can be done in a very large number of ways, including cooperation with threat intelligence platforms, correlation with other detection technologies, and integration into broader security orchestration frameworks.

By situating DDoS detection within the context of a wider security landscape, organizations can potentially find patterns across different types of malicious activity, such as the use of DDoS attacks as smokescreens for other breaches. Such an integrated perspective can enhance detection and response efficacy.

7.3. Challenges and Limitations

Despite the stupendous advancements, several limitations and challenges continue to influence the design and implementation of machine learning-based DDoS detection systems. These include the adversarial nature of the security environment, wherein the attackers continuously develop their tactics in anticipation of avoiding detection; difficulty in obtaining representative training data for emerging attack vectors; and the computational overhead in processing high-volume network traffic in real-time.

Researcher [1] highlighted that "due to the homogeneity and evolution of DDoS attack types and the dynamic volatility of the attack traffic, until now there has not yet been a satisfactory detection method from the aspect of detection accuracy" [1]. The comment underscores the ongoing difficulty in creating detection mechanisms that are able to keep pace with changing threats.

Ahmed et al. [15] determined that some of the major gaps in anomaly detection are the requirement for explainable AI and robust models to adversarial evasion methods

Conquering these challenges will require additional innovation in algorithm design, feature engineering, and system architecture, and more collaboration among researchers, security experts, and network operators.

7.4. Research Opportunities

The DDoS detection machine learning is an area with ample opportunities for future study. These include developing more adaptive self-update mechanisms that can respond to concept drift efficiently; exploring transfer learning techniques able to use knowledge learned in one network context to enhance detection in others; and looking into privacy-preserving machine learning techniques able to operate effectively within data protection requirements.

There is also significant room for research at the intersection of DDoS detection and other cybersecurity disciplines, such as threat intelligence, network behavior analysis, and security orchestration. By integrating these traditionally separate areas, researchers can develop more holistic and effective approaches to network defence.

As Abiramasundari and Ramaswamy point out, "constant research efforts are necessary to stay ahead of cyber threats and safeguard the integrity and availability of online systems" [2]. This reflects the recognition that DDoS detection is an open research problem and not a solved problem, with continued innovation being necessary to respond to evolving threats.

8. CONCLUSION

This literature review has outlined recent advances in machine learning algorithms for DDoS intrusion detection, with a particular focus on self-update parameter calibration techniques. The review has aggregated findings from various studies comparing various machine learning techniques and their effectiveness in detecting and mitigating DDoS attacks.

Several significant points can be derived from this analysis. Firstly, supervised learning methods, particularly Random Forest algorithms, have been demonstrated to work extremely well across a variety of studies and datasets. Abiramasundari and Ramaswamy's research that "RF yields the highest accuracy of 98.9% on CICIDS2017" [2] and Aineyoona's finding that a Random Forest model with self-update parameter calibration was 96% accurate on a real-time dataset [1] point to the effectiveness of this method in real-world applications.

Second, self-update parameter calibration is a critical capability for maintaining detection efficacy against evolving attack patterns. As Aineyoona emphasized, "to defeat these attacks in the long run self-updating models must be constructed" [1]. This adaptive capability enables detection systems to respond to concept drift and identify emerging attack patterns without human intervention or complete retraining.

Third, comprehensive performance evaluation entails analysis of a number of metrics like precision, false negative rate, and false positive rate, as well as assessment across different attack types and operating environments. The multi-dimensional assessment methodologies employed by scholars like Aineyoona [1] and Abiramasundari and Ramaswamy [2] provide more insight concerning model performance than application of one metric.

Fourth, despite the remarkable progress, it remains a challenge to construct detection schemes with "satisfactory detection accuracy" [1] for every form of DDoS attack strategy. Surmounting this challenge will require continued innovation in algorithm design, feature engineering, and system architecture, and increased research-practice synergy.

In conclusion, self-update parameter calibration machine learning algorithms offer promising alternatives for enhancing DDoS intrusion detection in communication networks. By combining the pattern recognition capacity of machine learning with the flexibility of self-updating models, these alternatives have the potential to yield more effective defence against the ever-evolving threat of DDoS attacks.

But to achieve this will be through ongoing R&D to bypass current limitations and keep pace with new attack techniques.

Self-enhancing ML models, particularly RF and hybrid models, are more accurate than static models with 96–98.9% accuracy. But adversarial evasion [12] and computational cost [11] remain problems.

Future research should be done to address explainability [13] and edge deployment [9] to close these gaps.

ACKNOWLEDGEMENTS

The authors would like to thank everyone, just everyone!

REFERENCES

[1] P. Aineyoona, "a Machine Learning Algorithm With Self-Update Parameter Calibration To Improve Intrusion Detection of Ddos in Communication Networks," Int. J. Eng. Appl. Sci. Technol., vol. 6, no. 6, pp. 72–79, 2021, doi: 10.33564/ijeast.2021.v06i06.008.

[2] S. Abiramasundari and V. Ramaswamy, "Distributed denial-of-service (DDOS) attack detection using supervised machine learning algorithms," *Sci Rep*, vol. 15, no. 1, p. 13098, Apr. 2025, doi: 10.1038/s41598-024-84879-y.

[3] K. Kumari and M. Mrunalini, "Detecting Denial of Service attacks using machine learning algorithms," *J Big Data*, vol. 9, no. 1, Dec. 2022, doi: 10.1186/s40537-022-00616-0.

[4] A. F. Al-Zubidi, A. K. Farhan, and S. M. Towfek, "Predicting DoS and DDoS attacks in network security scenarios using a hybrid deep learning model," *Journal of Intelligent Systems*, vol. 33, no. 1, Jan. 2024, doi: 10.1515/jisys-2023-0195.

[5] N. Hoque, D. K. Bhattacharyya, and J. K. Kalita, "Botnet in DDoS Attacks: Trends and Challenges," *IEEE Communications Surveys and Tutorials*, vol. 17, no. 4, pp. 2242–2270, Oct. 2015, doi: 10.1109/COMST.2015.2457491.

[6] S. Taghavi Zargar, J. Joshi, D. Tipper, (2013). A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks, *IEEE communications surveys & tutorials, 2013*

[7] X. Zhang, O. Upton, N. L. Beebe, and K. K. R. Choo, "IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers," *Forensic Science International: Digital Investigation*, vol. 32, Apr. 2020, doi: 10.1016/j.fsidi.2020.300926.

[8] R. Joffe, "Network security in the new world of work." [Online]. Available: https://owasp.org/

[9] S. A. Z. Mghames and A. A. Ibrahim, "Intrusion detection system for detecting distributed denial of service attacks using machine learning algorithms," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 32, no. 1, pp. 304–311, Oct. 2023, doi: 10.11591/ijeecs.v32.i1.pp304-311.

[10] C. Yin, Y. Zhu, J. Fei, and X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," *IEEE Access*, vol. 5, pp. 21954–21961, Oct. 2017, doi: 10.1109/ACCESS.2017.2762418.

[11] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," *Neurocomputing*, vol. 172, pp. 385–393, Jan. 2016, doi: 10.1016/j.neucom.2015.04.101.

[12] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An Ensemble of Autoencoders for Online Network Intrusion Detection," in *25th Annual Network and Distributed System Security Symposium, NDSS 2018*, The Internet Society, 2018. doi: 10.14722/ndss.2018.23204.

[13] R. Kozik, M. Choraś, M. Ficco, and F. Palmieri, "A scalable distributed machine learning approach for attack detection in edge computing environments," *J Parallel Distrib Comput*, vol. 119, pp. 18–26, Sep. 2018, doi: 10.1016/j.jpdc.2018.03.006.

[14] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, pp. 1153–1176, Apr. 2016, doi: 10.1109/COMST.2015.2494502.

[15] M. Ahmed, A. Naser Mahmood, and J. Hu, "A survey of network anomaly detection techniques," Jan. 01, 2016, *Academic Press*. doi: 10.1016/j.jnca.2015.11.016.

AUTHORS

Ainebyoona Patrick is currently a PhD student (2025) at Kampala International University specializing in Cybersecurity. He holds a Master's of Science in Computing (Computer Security) from Uganda Technology and Management University and Bachelor's degree in Software Engineering from Makerere University. For the last decade, he has been a system engineer, digital forensics analyst and network security analyst.

Adeleke Raheem Ajiboye holds a BSc and MSc in Computer Science, along with a Cisco Certified Network Associate (CCNA) certification. He completed his PhD in Computer Science at the University Malaysia Pahang in 2016. Currently, he lectures at Kampala International University in Uganda. Over the years, he has published numerous research articles in reputable journals. With a solid foundation in theory and extensive hands-on experience, his areas of interest include Artificial Intelligence, Machine Learning, Networking, and Data Science. He has also presented his research findings at conferences held in Malaysia, the UAE, Uganda, Zambia, and Nigeria.