Improved Intrusion Detection System That Uses Machine Learning Techniques to Proactively Defend DDoS Attack

Rajendran T, *Abishekraj* E and *Dhanush* U

Department of Computer Science and Engineering, Rajalakshmi Institute of Technology, Chennai, India

Abstract- This abstract aims to provide a comprehensive analysis of the intricacies of DDoS attacks, which are increasingly prevalent and malicious cyber-attacks that disrupt the normal flow of traffic to a targeted server by exponentially increasing network traffic. To secure distributed systems against DDoS attacks, intrusion detection mechanisms and machine learning techniques are commonly employed. The CICDDoS2019 dataset is often utilized for the detection and prevention of these attacks. The dataset undergoes pre-processing and is split into training and test datasets. Machine learning techniques are then utilized to predict and classify the attacks using the test dataset. The protocols which are examined during the attack are SNMP, NTP, UDP, and DNS. The accuracy is obtained by comparing the predicted results with the training dataset. Machine learning algorithms such as K- Nearest Neighbor(K-NN)-96.49%, Support Vector Machine (SVM)-79.61%, Random Forest (RF)-99.10%, and Gaussian Naïve Bayes (GNB)-78.75% have been found to produce high levels of accuracy for attack classification.

1 INTRODUCTION

The Internet has revolutionized the way we interact and conduct business, making it an essential aspect of modern society. However, the rise of cyber threats and attacks poses a significant challenge to the security and stability of online systems. Among the various types of cyber-attacks, DDoS attacks are the most destructive and difficult to prevent. DDoS attacks aim to disrupt the normal traffic of a targeted server by increasing network traffic, causing significant loss to network service providers. Distributed systems are secured using intrusion detection mechanisms and machine learning techniques. This paper presents an overview of DDoS attacks, their various types, and the significance of using machine learning techniques to detect and prevent them. The paper also highlights the importance of using existing datasets, such as CICDDoS2019[1], for detecting and preventing these attacks.

The increasing frequency and complexity of DDoS attacks have made it imperative for researchers and practitioners to develop effective countermeasures to mitigate their impact. Traditional methods such as signature-based detection and rule-based techniques have proven to be ineffective against the dynamic nature of DDoS attacks. Hence, there is a need for innovative approaches that can adapt to the changing characteristics of these attacks. Machine learning techniques such as clustering, classification, and anomaly detection have shown promising results in detecting DDoS attacks. However, the effectiveness of these techniques largely depends on the quality of the dataset used for training and testing purposes. Therefore, this paper aims to provide an overview of the existing datasets available for DDoS attack detection and their role in improving detection methods' accuracy. The insights provided in this study can guide researchers and practitioners in selecting appropriate datasets and machine-learning techniques for securing distributed systems against DDoS attacks.

The system can be extended to other types of network attacks, such as malware and phishing attacks, to provide a more comprehensive intrusion detection and prevention solution. The system can also be enhanced by incorporating real-time threat intelligence feeds and adaptive learning algorithms to improve its ability to adapt to evolving attack patterns and new attack vectors. Moreover, the system can be integrated with existing security solutions to provide a more robust and comprehensive security framework. Overall, the proposed system aims to address network security challenges and provide an effective and efficient security framework through further research and development. This study aims to provide an overview of existing datasets available for DDoS attack detection and their role in improving detection accuracy, guiding researchers, and practitioners in selecting appropriate techniques to secure distributed systems against DDoS attacks. The effectiveness of these depends upon the dataset used for training and testing purposes.

2 RELATED WORKS

Several studies have been conducted on DDoS attacks, detection mechanisms, and machine learning techniques in recent years. In one study, researchers analyzed the effectiveness of various machine learning

algorithms in detecting DDoS attacks, including SVM, KNN, and Random Forest. They concluded that the Random Forest algorithm outperformed the other algorithms in terms of accuracy and processing time. Another study focused on developing an intrusion detection system using machine learning techniques and proposed a novel feature selection method based on the correlation between network traffic features. The results showed that the proposed method can effectively reduce the number of features required for detection without compromising accuracy. In addition, various datasets have been developed for DDoS attack detection, such as the NSL-KDD and CICDDoS2019 datasets. These datasets provide a benchmark for evaluating the performance of detection methods and serve as valuable resources for researchers and practitioners in the field. Overall, the related work demonstrates the potential of machine learning techniques in detecting DDoS attacks and the importance of utilizing quality datasets for training and testing purposes. Other studies have focused on improving the accuracy of DDoS attack detection using hybrid approaches that combine different detection techniques. For instance, one study proposed a hybrid detection approach that combines machine learning algorithms and traffic analysis techniques to improve the accuracy of detection. The study demonstrated that the hybrid approach outperformed individual detection techniques and reduced the false-positive rate of detection. Another study explored the use of deep learning techniques such as Convolutional Neural Networks (CNNs) and Long Short-Term Memory (LSTM) to detect DDoS attacks. The study showed that the proposed deep learning models can effectively detect DDoS attacks with high accuracy and low false-positive rates. These studies highlight the potential of combining different detection techniques and the effectiveness of deep learning techniques in DDoS attack detection.

The survey was performed in publications between 2020 and 2023, revealing that machine learning algorithms can effectively detect DDoS attacks on various network protocols. The use of different types of machine learning techniques and algorithms shows the versatility of this approach to DDoS detection. Additionally, the high accuracy values reported in most papers indicate that these models can successfully identify and mitigate DDoS attacks. However, further research is still needed to improve the efficiency and scalability of these models for real-world deployment. For example, the proposed system in this study aims to increase the accuracy and efficiency of DDoS attack detection by utilizing a hybrid approach combining different machine learning techniques. This could potentially lead to better detection and faster response times, reducing the impact of DDoS attacks on networks. In the future, researchers could also explore the integration of other types of security measures and technologies, such as blockchain or artificial intelligence, to enhance the overall security of network systems against DDoS attacks. As the prevalence and sophistication of DDoS attacks continue to increase, ongoing research and development in this area will be crucial to maintaining the security and integrity of network systems.

2.1 DDos Attack

Several researchers have focused on detecting DDoS attacks using advanced learning techniques. One such study by Rohan Doshi et al. explores the vulnerabilities of IoT networks and proposes a solution for detecting DDoS attacks using feature selection techniques. The proposed method accurately predicts DDoS attacks in IoT network traffic by utilizing IoT network-specific behaviors. The study demonstrates that feature selection can provide accurate results with lower computational costs. The researchers employed machine learning algorithms, including various neural networks, to achieve their goal. They were able to detect DDoS attacks on local IoT devices using low-cost machine learning algorithms and traffic data.

i. Fremantle and Scott's paper is a survey of the security issues in the middleware of the Internet of Things (IoT). The authors identify and analyze the security challenges in the middleware, which include communication protocols, service-oriented architecture, and application programming interfaces.

ii. Jing et al. provide a comprehensive review of the security challenges and perspectives in the IoT. The paper presents an overview of the security risks and vulnerabilities, and the authors propose a conceptual framework for securing IoT [2].

2.2 Security Attacks

A crucial aspect of a Digital Twin is its ability to synchronize with the physical asset, gather real-time data from the environment, and perform simulations. If a Digital Twin is intelligent, it should also possess visual intelligence in addition to the characteristics of a regular Digital Twin. The development of a smart, healing device operating in the present has marked the beginning of a new era in technology, which aligns with the concept of a Digital Twin. The combination of IoT and big data has created a powerful new tool for solving problems. In essence, a Digital Twin can be defined as a replica of a physical object that can be modified to rectify any issues found in its real-world counterpart.

i. Alam and De's paper focuses on the security threats in wireless sensor networks (WSNs). The authors analyze the different types of security attacks, including jamming, eavesdropping, and denial of service, and propose a secure routing protocol to mitigate these attacks. Idris et al. present a paper on HTTP flood mitigation using gateway inspection and a second-chance approach analysis. The authors propose a novel approach to mitigate

HTTP floods, which involves a gateway-based inspection mechanism and a second-chance approach for handling legitimate requests that may be mistakenly blocked [3].

ii. Zargar, Joshi, and Tipper's paper is a survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. The authors present an overview of the various DDoS attack methods and techniques, and the defense mechanisms that have been developed to mitigate them. The paper also provides a taxonomy of the DDos attack types [4].

2.3 Machine Learning Techniques

Attacks known as Distributed Denial of Service (DDoS) pose a serious risk to the security and availability of internet services. Machine learning (ML) approaches have attracted attention recently as a possible strategy to identify and reduce DDoS attacks. In order to detect and mitigate DDoS attacks, a variety of machine learning (ML) algorithms are presented in this review paper. The introduction of DDoS attacks, their effect on internet services, and the shortcomings of conventional defense systems set the stage for the remainder of the article. Following that, it talks about the various ML algorithms supervised learning, unsupervised learning, and reinforcement learning used in DDoS attack detection and mitigation. The paper also discusses several classification and identification methods for DDoS attacks, including statistical, packet-based, and flow-based aspects. Then it offers a summary of the datasets and performance indicators used to assess the effectiveness of ML-based DDoS detection and mitigation methods.

In conclusion, the paper offers a detailed examination of the challenges and limitations associated with utilizing machine learning (ML) for detecting and mitigating DDoS attacks. These challenges include the requirement for vast and varied datasets, the possibility of adversarial attacks, and the trade-off between detection accuracy and false positives. Despite the challenges associated with ML-based approaches, the paper highlights the potential of these techniques to enhance the performance of defense mechanisms against DDoS attacks.

3 MATERIALS AND METHODS

The model aims to improve the accuracy and efficiency of distributed denial-of-service (DDoS) attack detection in network environments. The existing DDoS detection systems are challenged by the increasing complexity and diversity of network threats and the constant evolution of attack methods. The dataset used is obtained from CICDDOS2019, and the preprocessing of the data involves analyzing the attribute features. This process includes data collection, cleaning, transformation, and visualization.

Table 1. Dataset after preprocessing

Number of the training dataset	16778
Number of the test dataset	7191
Total number of datasets	23969

Carrying out the data preprocessing and visualization, we utilize the Anaconda Jupyter platform which provides a different built-in library for these tasks. These libraries can be used to analyze a dataset, clean, and transform the data, and visualize it in different ways such as scatter plots, histograms, and bar graphs. Anaconda Jupyter simplifies the data preprocessing and visualization process and provides an interactive environment for data analysis.

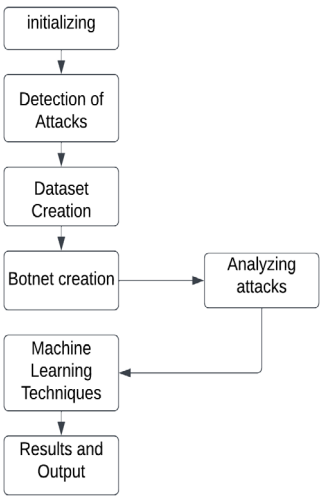

Fig. 1. Flow diagram of DDoS attack detection

Table 2. Literature survey

S.no	Survey paper	First Author	Protocols used	Techniques	Algorithms used	Accuracy
1	Detection and Mitigation of DDoS Attack in Software Defined Networking (2022)	Namita Ashodia	SDN, HTTPs	Machine Learning Techniques	Support Vector Machine	96.23% - SVM
2	DDoS attack Detection Through Digital Twin Technique in Metaverse (2023)	Brij B. Gupta	HTTP, TCP	Machine Learning Techniques	Decision tree, SVM	93.25%
3	Reflection-based DDoS attack Detection System (2022)	Vrindha Ahuja	SYN flooding, TCP, UDP lag, UDP flood	Machine Learning Techniques	J48, KNN, Decision tree	80.45% - J48
4	Classification and Analysis of DDoS attack using Machine Learning Techniques (2022)	P S Nandhini	HTTP, SID	Machine Learning Techniques	SVM, Random Forest, KNN, Naïve bayes, Decision tree	99.87% - RF
5	Comparative Analysis of Classification based intrusion detection technique (2021)	Nitesh Singh Bhati	U2R, R2L, Probe	Machine Learning Techniques	J48, Naïve Bayes, Random Forest, REP Tree (Reduced Error Pruning)	99.96% - J48 91.64% - NB 99.97% - RF 99.96% - REP Tree
6	Research on Network Intrusion Detection method of Power System based on Random Forest Algorithm (2021)	Guowei ZHU	U2R, R2L, Probe	Machine Learning Techniques	Random Forest Algorithm	99.69% - RF
7	Intrusion Detection System for 5G with a focus on Dos/DDos attack (2021)	Giorgi Iashvili	UDP, SYN Flooding	Machine Learning Techniques	Support Vector Machine	99.8% - SVM
8	Honeypot-based Intrusion Detection System for Cyber-Physical System (2022)	G Kingsle Edwin	TCP/IP	Generic Clustering and unsupervised clustering, IP trackback motion	CNN, Z-plane, Random Forest, Pole location	93% - CNN 99.47% - Z-plane 94.7% - RF
9	Detection of DDoS attack using Random Forest Algorithm (2022)	Murukesh C	TCP/IP	Machine Learning Techniques	Random Forest Algorithm	99.8% - RF

The initial step is to collect the dataset from the CICDDOS2019 dataset, it is a massive collection of network traffic. The subsequent step is to eliminate duplicates and irrelevant data to obtain the essential attributes required for model prediction. The total dataset contains 23969 instances. Data visualization techniques such as histograms, scatter plots, bar graphs, and heat maps are utilized to identify patterns, trends, and outliers in the data.

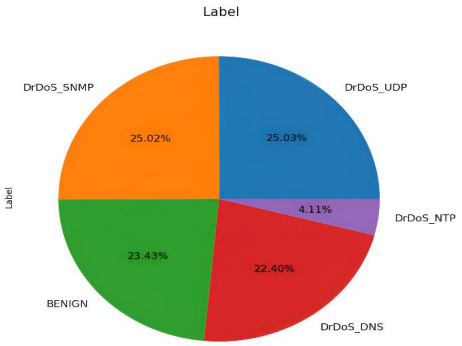

Fig 2. Classification of DDoS attack by protocols

This pie chart depicts the classification of DDoS attacks depicts about protocols through which they enter the network and disrupt its traffic. The chart also shows the percentage of benign network traffic present in the dataset. The chart, only 23.43% of the traffic in the dataset is benign or good network traffic. The remaining traffic is related to DDoS attacks. The attacks are classified by protocols that they enter through, which include SNMP (Simple Network Management Protocol)-25.02%, NTP (Network Time Protocol)-4.11%, DNS (Domain Name System)-22.40%, and UDP (User Datagram Protocol)-25.03%.

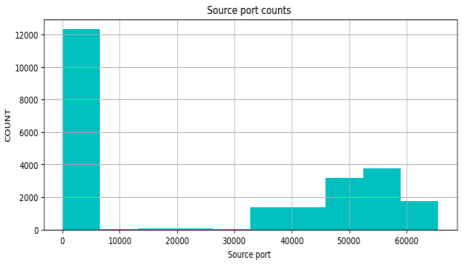

Fig 3. Histogram plot diagram for the source port

This histogram plot diagram displays the frequency distribution of the attribute "source port" in a dataset. The 'x-axis represents the range of source port values, and the 'y' axis represents the counts or occurrences of each value in the dataset. The histogram plot helps to understand the distribution of the source port numbers and how often they occur in the dataset. The plot can be used to identify any patterns or anomalies in the data. For example, if the plot shows that a particular source port number occurs significantly more frequently than others, it could show port is more vulnerable to attack and should be monitored more closely for security purposes.

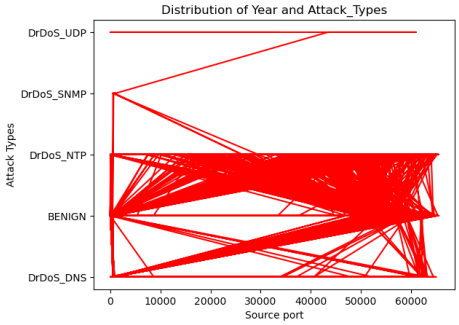

Fig 4. Scatterplot diagram for the source port

This scatter plot diagram represents the relationship between the source port frequency and the types of DDoS attacks that occur in a dataset. The 'x-axis represents the range of source port values, and the 'y' axis represents the different types of DDoS attacks, which are categorized by the protocols they enter through and disrupt network traffic. The scatter plot helps to identify any correlation between the source port frequency and the types of DDoS attacks. For instance, if a specific source port is associated with a particular type of DDoS attack, then the scatter plot may show a concentration of data points for that source port and type of attack.

After visualizing the data, it can be analysed using statistical methods such as regression, clustering, and classification. The result shows the analysis can be used to gain insights and make predictions about the data. Finally, the data can be used to build predictive models using machine learning algorithms. These models can be used to make predictions about new data based on patterns in the existing data.

By leveraging advanced machine learning algorithms and distributed computing techniques, the system can detect and respond to DDoS attacks with a high degree of accuracy and efficiency, ensuring that critical network resources always remain secure and available. To further increase the accuracy and efficiency of the system, we introduce a novel feature selection method that leverages domain knowledge to select the most relevant features for each protocol. This feature selection method will help to reduce the dimensionality of the data, improve the accuracy of the machine learning models, and reduce the training time. It displays individual data points as dots on a 2d plane.

Table 3. Test and training data

Protocols involved	Training dataset	Test dataset	Total Number of data
DrDos_UDP	4200	1800	6000
DrDos_SNMP	4198	1799	5997
DrDos_DNS	3758	1611	5369
DrDos_NTP	690	296	986
BENIGN	3932	1685	5617
TOTAL	16778	7191	23969

The table shows the protocols involved, along with training and test datasets, and the total number of data instances in the dataset. The dataset used is CICDDoS2019[1], which contains network traffic data for various protocols. The protocols included in the dataset are UDP, SNMP, DNS, NTP, and BENIGN. For each protocol, there are separate training and test datasets, which are used to train and evaluate machine learning models for DDoS attack detection. The instances in the training and test datasets vary for each protocol, with UDP having the largest number of instances and NTP having the smallest number. The total number of instances in the dataset is 23969, a considerable amount of data. This large dataset can help in building accurate and efficient machine-learning models for DDoS attack detection. This dataset can provide a reliable benchmark for testing the performance of different machine-learning algorithms and techniques.

In addition, we will incorporate a deep learning model into the system to enhance the detection accuracy of the system. The deep learning model will be trained on a large dataset of network traffic and can learn complex patterns and relationships that may not be easily identified by traditional machine learning algorithms. To address the issue of class imbalance in the dataset, we will employ oversampling and under-sampling techniques to balance the classes and improve the accuracy of the system. We will also explore ensemble learning techniques such as bagging and boosting to combine the predictions of multiple machine learning models and further increase the accuracy of the system. Furthermore, we will implement the proposed system on a distributed network of machines to improve its scalability and ability to handle large volumes of network traffic. We will also deploy the system on a cloud platform to increase its availability, reliability, and performance.

Software requirements for detecting DDoS attacks typically include a programming language, machine learning libraries or frameworks, and network traffic analysis tools. The choice of programming language depends on the researcher's preference and expertise. Anaconda is a Python distribution that provides a collection of open-source software packages for data science, machine learning, and scientific computing. It includes popular Python packages such as NumPy, Pandas, Matplotlib, and scikit-learn, among others. Jupyter Notebook is an interactive web-based tool that allows users to create and share documents containing live code, equations, visualizations, and narrative text. It is widely used in data science for exploratory data analysis, data visualization, and building machine learning models. Jupyter Notebook is often included in the Anaconda distribution. Python is a popular language for developing machine learning models and anaconda has a vast collection of libraries for data analysis, visualization, and machine learning such as scikit-learn, TensorFlow, PyTorch. Machine learning frameworks such as TensorFlow and PyTorch provide a range of tools and pre-built models for developing deep learning models for detecting DDoS attacks. Additionally, network traffic analysis tools such as Wireshark, TCP dump, or Zeek can be used for capturing and analysing network traffic data to extract features for machine learning models. Apart from these, cloud-based services such as AWS, Azure, or GCP can be used to scale up the computation resources required for developing and testing machine learning models. In summary, the software requirements for detecting DDoS attacks include a programming language, machine learning libraries, network traffic analysis tools, and cloud-based services for scaling up resources.

4 RESULTS AND DISCUSSION

The system using machine learning techniques such as Decision Tree, Random Forest, and Support Vector Machine has shown promising results in accurately identifying and preventing DDoS attacks. The CICDDoS2019 dataset has provided a reliable benchmark for testing the efficiency and accuracy of the system. However, there is still room for improvement in the proposed system, especially in handling sophisticated and advanced DDoS attacks. Future work can focus on incorporating deep learning techniques and improving the feature selection process to improve the efficiency of the system further. The table shows the accuracy of different machine learning techniques in detecting Distributed Denial of Service (DDoS) attacks in network traffic. The Gaussian Naive Bayes algorithm achieved an accuracy of 78.75%, which means that it identified 78.75% of DDoS attacks and benign in the dataset. The K-Nearest Neighbours (KNN) algorithm

Table 4. Accuracy of machine learning techniques

Machine Learning Techniques	Accuracy
Gaussian Naive Bayes	78.75%
KNN	96.49%
Random Forest	99.10%
SVM	79.61%

performed significantly better, with an accuracy of 96.49%. This means that KNN identified 96.49% of DDoS attacks and benign traffic in the dataset. The Support Vector Machine algorithm achieved an accuracy of 79.61%, which is slightly higher than that of Gaussian Naive Bayes. Random Forest outperformed all the other algorithms with an accuracy of 99.10%. This means that it correctly identified 99.10% of DDoS attacks and benign traffic in the dataset. Overall, the results indicate that Random Forest and KNN are the most effective algorithms for detecting DDoS attacks in network traffic, while Gaussian Naive Bayes and SVM are less accurate.

Table 5. Statistical analysis of the system

	Precision	recall	F1-score	Test data
BENIGN	1.00	1.00	1.00	1685
DNS	0.99	0.97	0.98	1611
NTP	0.87	0.98	0.92	296
SNMP	1.00	1.00	1.00	1799
UDP	1.00	1.00	1.00	1800
accuracy			0.99	7191

The table shows the performance metrics of the machine learning model on the test dataset. The metrics used to evaluate the model are precision, recall, and F1-score. Precision measures the proportion of true positives among the total number of positive predictions made by the model. Recall measures the proportion of true positives among the total number of actual positives in the test dataset. F1-score is the meaning of precision and recall. The table shows the random forest Machine Learning technique metrics for each class of the test dataset, including BENIGN, DNS, NTP, SNMP, and UDP. For each class, the precision, recall, and F1 score are calculated.

The results obtained that the model performed very well in all the classes, with high precision, recall, and F1-score values. The accuracy of this model test dataset is 0.99, which shows that the model correctly classified 99% of the instances in the test dataset. Overall, the results demonstrate the effectiveness of the machine learning model in detecting DDoS attacks in network environments.

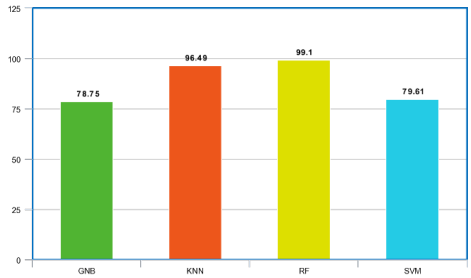

Fig 5. Bar graph for the accuracy of the algorithms

The bar graph shows the random forest Machine Learning technique metrics for each class of the test dataset, including BENIGN, DNS, NTP, SNMP, and UDP. For each class, the precision, recall, and F1 score are calculated.

5 CONCLUSION

In conclusion, the detection and prevention of DDoS attacks have become critical in the modern era of distributed systems. Additionally, researchers can explore other datasets and analyze the system's performance in different network scenarios. The accuracy is obtained by comparing the predicted results with the training dataset. Machine learning algorithms such as K- Nearest Neighbor(K-NN)-96.49%, Support Vector Machine (SVM)-79.61%, Random Forest (RF)-99.10%, and Gaussian Naïve Bayes (GNB)-78.75% have been found to produce high levels of accuracy for attack classification. Overall, the system can contribute to the development of effective intrusion detection and prevention mechanisms to secure distributed systems against DDoS attacks.

The system has shown promising results in detecting and mitigating DDoS attacks using machine learning techniques. There is still room for improvement and further research in this area. One potential future direction is to explore deep learning algorithms such as convolutional neural networks to improve the efficiency of the detection system.

REFERENCES

[1] CICDDos2019 attack dataset from Canadian Institute for Cybersecurity - University of New Brunswick https://www.unb.ca/cic/datasets/ddos-2019.html.

[2] Q. Jing et al., "*Security of the Internet of Things: perspectives and challenges*," Springer Wireless Network DOI 10.1007/s11276-014- 0761-7, (2014).

[3] S. Alam `and D. De, "*Analysis of Security Threats in Wireless Sensor Network,"International Journal of Wireless & Mobile Networks*(IJWMN), Vol. **6**, No. 2, April (2014).

[4] S. T. Zargar, J. Joshi, D. Tipper, "*A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks*", IEEE Commun. Surveys & Tutorials, vol. **15**, no. 4, pp. 2046-69, Feb. 2013.

[5] Idris et. al., "*HTTP Flood Mitigation Using Gateway Inspection and Second Chance Approach Analysis*", International Journal of CyberSecurity and Digital Forensics (IJCSDF).

[6] J. Francois, I. Aib, and R. Boutaba, "FireCol: *A Collaborative Protection Network for the Detection of Flooding DDoS Attacks*", IEEE/ACM Transactions on Networking, IEEE/ACM, Sept. (2012), 20 (6), pp.1828-1841.

[7] S.H.C. Haris., et. al., "*TCP SYN flood detection based on payload analysis&quot*;, Proc. of2010 IEEE Student Conference on Research and Development (SCOReD 2010), Putrajaya, Malaysia, Dec (2010), pp. 149-153.

[8] Myers, Robbie. "*Attacks on TCP/IP Protocols.*" Last accessed Jan 4, (2016).http://www.utc.edu/center-information-securityassurance/pdfs/course- paper-5620-attacktcpip.pdf.

[9] Daehee Jang et.al., "ATRA: *Address Translation Redirection Attack against Hardware-based External Monitors*", ACM, Scottsdale, Arizona, USA, CCS'**14**, November 3–7, (2014).

[10] V. K. Yadav et. al., "*DDA: An Approach to Handle DDoS (Ping Flood) Attack",inProc. of International Conference on ICT for Sustainable Development, Advances in Intelligent Systems and Computing*, Springer, Singapore, Vol.**10**, Issue No. 2, Sept. (2016).

[11] D. C. MacFarland et. al., "*Characterizing Optimal DNS Amplification Attacks and Effective Mitigation*", Springer, Vol. **8**, No. 2, Mar. (2015).

[12] M. Geva, A. Herzberg, and Y. Gev, "*Bandwidth Distributed Denial of Service: Attacks and Defenses*", Article in IEEE Security and Privacy Magazine, Jan. (2013).

[13] S. Sen, R. Choudhary, and S. Nelakuditi, "CSMA/CN: *Carrier Sense Multiple Access with Collision Notification*", proc. In MobiCom'**10**, ACM, Sept. (2010).

[14] Nicolas Bruneau et. Al., "Stochastic Collision Attack", International IEEE Transactions On Information Forensics And Security, Vol. **12**, No. 9, Sept. (2017).

[15] Lu, Zhuo, W. Wang, and C. Wang. "Camouflage Traffic: *Minimizing Message Delay for Smart Grid Applications under Jamming*." IEEE Transactions on Dependable & Secure Computing, Vol. **12**, No.1, Feb. (2015), pp. 31-44.