IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 5, May 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105120 |

# Detection and Prevention Mechanisms for DDoS Attack in BWSN

**Sinchana T L, Sneha K S, Sugnana Sagar B L, Yohan Swamy, Prof. Vidyashree K P**

UG Students, Dept. of ISE, VVCE, Visvesvaraya Technological University, Mysuru, India

Assistant Professor, Dept. of. IS, VVCE, Visvesvaraya Technological University, Mysuru, India

**ABSTRACT**: Attacks using bandwidth distributed denial-of-service (BW-DDoS) techniques, in which a large number of servers send out a high volume of packets to cause congestion and obstruct legitimate traffic, are a threat to the Internet. When introducing a defensive component against adversarial assaults, it is necessary to deploy many protection mechanisms in combination to obtain effective coverage of diverse attacks. BW-DDoS attacks have employed rather rudimentary, inefficient brute-force tactics; future assaults may be substantially more successful and damaging. More advanced defences are necessary to tackle the mounting risks. DDoS and other adverbial assaults pose a severe threat to the Internet. We address the Internet's susceptibility to Bandwidth Distributed Denial of Service (BW-DDoS) assaults, in which a large number of sites broadcast a significant amount of packets that exceed network capacity, creating congestion and losses and interrupting legitimate traffic. TCP and other protocols utilize congestion management strategies to respond to losses and delays by decreasing network use; as a result, their performance may suffer dramatically as a result of such attacks. Attackers may impair connectivity to servers, networks, autonomous systems, even entire nations or regions; such assaults have previously been carried out in a number of wars. We review BW-DDoS assaults and countermeasures in this study.

**KEYWORDS**: DDOS, Intrusion dection, BW-DDoS, Intrusion prevention system

## I. INTRODUCTION

Distributed Denial of Service (DDOS) attacks are a significant danger to the internet. We explore the Internet's vulnerability to Bandwidth Distributed Denial of Service (BWDDOS) attacks, in which a large number of sites transmit a large amount of packets that exceed network capacity, creating congestion and losses and interrupting legitimate traffic. TCP and other protocols have a congestion management system that responds to losses and delays by limiting network utilization, therefore their performance may suffer significantly as a result of such assaults. Attackers may impair connectivity to servers, networks, autonomous systems, even entire nations or regions; such assaults have previously been carried out in a number of wars. BWDDOS used a somewhat rudimentary, ineffective 'brute force' technique; subsequent assaults might be far more successful, and hence much more destructive. More modern defenses should be deployed to combat the growing dangers. This might include a previously proposed mechanism as well as fresh ones. BWDDOS used a somewhat rudimentary, ineffective 'brute force' technique; subsequent assaults might be far more successful, and hence much more destructive. To address the escalating threats, more advanced defenses should be put in place. This could include both new and previously suggested mechanisms. The most typical reason is to cause a machine learning model to malfunction. An adversarial attack might involve feeding a model false or misleading data while it is training, or adding deliberately prepared data to trick an already trained model. What exactly is an Adversarial Attack Machine learning methods take numeric vectors as inputs. An adversarial attack is when you design an input in a certain way to elicit the erroneous answer from the model.

## II. PROPOSED ALGORITHM

Toward generating a new intrusion detection dataset and intrusion traffic characterization With the exponential expansion in the size of computer networks and created applications, the enormous increase in the potential harm that may be produced by launching assaults is becoming clear, according to Iman Sharafaldin et al. Meanwhile, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are critical security weapons against complex and ever-increasing network threats.

The author of [1] they explain about the Anomaly-based techniques in intrusion detection systems suffer from inaccurate deployment, analysis, and assessment due to a lack of suitable dataset. There are a number of such datasets

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105120 |

available, including DARPA98, KDD99, ISC2012, and ADFA13, that researchers have used to test the efficacy of their proposed intrusion detection and intrusion prevention systems. According to our analysis of eleven publicly accessible datasets from 1998, several of them are out of date and unreliable for usage. Some of these datasets suffer from a lack of traffic diversity and volume, some do not cover a wide range of threats, while others anonymize packet information and payload, making it difficult to represent current trends, or they lack feature set and metadata.

The author of this paper[2] claim that the rising number of security risks on the Internet and computer networks necessitates extremely trustworthy security solutions. Meanwhile, intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) play critical roles in the design and maintenance of a resilient network architecture capable of defending computer networks by detecting and preventing a wide range of threats. Reliable benchmark datasets are essential for testing and evaluating a detection system's performance. There are several similar datasets, such as DARPA98, KDD99, ISC2012, and ADFA13, that researchers have used to evaluate the efficacy of various intrusion detection and prevention systems. However, not enough study has been conducted to evaluate and examine the datasets themselves. In this research, we give a detailed review of current datasets using our suggested criteria, as well as a methodology for evaluating IDS and IPS datasets. We investigated existing datasets for testing and evaluating intrusion detection systems (IDSs) and presented a new framework for evaluating datasets with the following characteristics: Attack Diversity, Anonymity, Available Protocols, Complete Capture, Complete Interaction, Complete Network Configuration, Complete Traffic, Feature Set, Heterogeneity, Labeled Dataset, and Metadata. The suggested framework takes into account organizational policy and conditions through the use of a coefficient, W, which may be established independently for each criterion. The author of this papper [3] have proposed this in their study. One of the most difficult tasks in today's security sector is traffic classification. It is a challenging work due to the ongoing growth and production of new apps and services, as well as the proliferation of encrypted communications. Virtual Private Networks (VPNs) are an example of an encrypted communication service that is gaining popularity as a technique of circumventing censorship and accessing geographically restricted services. In this research, we investigate the usefulness of flow-based time-related characteristics in detecting VPN traffic and classifying encrypted communication into distinct categories based on the kind of traffic, such as browsing, streaming, and so on. To assess the correctness of our features, we employ two well-known machine learning algorithms (C4.5 and KNN). Our results suggest that time- related characteristics are effective classifiers for encrypted traffic characterization, with high accuracy and performance. We investigated the effectiveness of time-related characteristics in addressing the difficult challenge of identifying encrypted communication and detecting VPN activity. As a classification strategy, we suggested a collection of time-related characteristics and two standard machine learning algorithms, C4.5 and KNN. The author of [4] have offered Over the last three decades, Network Intrusion Detection Systems (NIDSs), particularly Anomaly Detection Systems (ADSs), have been more important than Signature Detection Systems (SDSs) in identifying fresh assaults (SDSs). Evaluating NIDSs using KDD99 and NSLKDD benchmark data sets does not yield satisfying findings owing to three primary issues: (1) a lack of contemporary low footprint attack techniques, (2) a lack of modern typical traffic situations, and (3) a different distribution of training and testing sets. The UNSW-NB15 data set was recently created to address these difficulties. This data collection covers nine types of recent assaults designs and new patterns of normal traffic, as well as 49 attributes that compose the flow based between hosts and network packets inspection to distinguish between regular and aberrant observations. In this study, we show the UNSW-NB15 data set's complexity in three ways. The statistical analysis of the data and qualities is discussed first. Second, a look of feature correlations is presented. Finally, five existing classifiers are employed to assess the complexity in terms of accuracy and false alarm rates (FARs), and the results are compared to the KDD99 data set. The experimental results demonstrate that UNSW-NB15 is more complicated than KDD99 and may be used to evaluate NIDSs. The author of [5] explained that the lack of a comprehensive network-based data collection that can reflect current network traffic scenarios, large types of tiny footprint intrusions, and deep structured information about network traffic. KDD98, KDDCUP99, and NSLKDD benchmark data sets were created a decade ago to evaluate network intrusion detection systems research efforts. However, multiple recent studies have revealed that, in the present network security environment, traditional data sets do not comprehensively capture network traffic and new tiny footprint assaults. To address the issue of network benchmark data set scarcity, this research investigates the establishment of a UNSW-NB15 data set. This data collection is a combination of genuine modern normal and contemporary network traffic assault operations. The UNSWNB15 data set's features are generated using both existing and unique technologies. This data collection is accessible for research purposes and may be accessed via the link.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105120 |

## III. PROPOSED SYSTEM

The proposed system for detecting and preventing DDoS Nodes: A decentralize network of nodes in the system allows for real-time communication of information about active attacks. Each node is responsible for monitoring traffic to and from the server and is equipped to detect unusual traffic patterns that could indicate a DDoS attack. Consensus mechanism: The system employs a consensus procedure like proof of work or proof of stake to make sure that the information transferred between nodes is reliable and tamper-proof. This approach ensures that the nodes agree on the veracity of the information exchanged and prevents rogue nodes from tampering with the data. Smart contracts: Smart contracts are utilised by the system to generate a set of standards that must be followed to in order for client and server communication to occur. These rules could limit the amount of traffic that clients can transmit to the server at any one moment or require them to pass a challenge before they can access it.

Intrusion detection system: The system includes an intrusion detection system that can look at traffic patterns and identify suspicious activity. Machine learning techniques are used by the system to categorize traffic and spot potential DDoS attacks. The system can produce an alarm and take measures to stop the assault if it detects one. Overall, the suggested solution provides a trustworthy and safe way to use block-chain technology to spot and thwart DDoS attacks. The system can successfully reduce the risks posed by DDoS attacks by building a decentralized network of nodes that can exchange information in real-time and using smart contracts and a consensus method to assure data integrity.

A stronger defence against DDoS attacks is also made possible by the intrusion detection system's additional security layer and potential for quicker detection and response times.

## IV. USER MANAGEMENT

Nodes and servers frequently communicate across a computer network on different hardware, but both node and server may be on the same system. A server host is responsible for running one or more server applications that share resources with nodes. A node does not share any of its resources, but instead requests the content or service function of a server. As a result, nodes establish communication sessions with servers that await incoming requests. The server component offers a function or service to one or more nodes that begin service requests. A web server hosts web pages, whereas a file server hosts computer files. Any of the server computer's software and electrical components, from programmers and data to processors and storage devices, can be considered a shared resource

## V. SIGNATURE AND TOKEN ANALYSIS

Messages are sent between clients and servers in a request-response messaging pattern. The client submits a request, and the server responds. Inter-process communication is demonstrated by this message exchange. To communicate, the computers must speak the same language and follow the same rules, so that both the client and the server know what to anticipate. A communications protocol specifies the language and norms of communication. The blockchain mechanism and developed a modified SHA256 security protocol via smart contract to protect online transaction procedures that are especially based on the Blockchain Mechanism It focuses on the subject of changing security protocols especially tailored for practical blockchain applications, with a particular emphasis on privacy and trust Here, the server pulls a file from its database that matches the node request and sends it to the node.

## VI. CONCLUSION

When compared to standard detection techniques that merely use the distribution of the number of lost packets, utilizing the correlation between dropped packets enhances the accuracy in identifying malicious packet drops dramatically. This gain is notably noticeable when the number of intentionally discarded packets is equivalent to the number of packets dropped due to network failures. It is vital to obtain accurate packet-loss statistics from individual users in order to appropriately assess the correlation between lost packets. An auditing architecture was created to assure accurate packet-loss reporting by individual nodes.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 |

|| Volume 11, Issue 5, May 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1105120 |

## REFERENCES

1. Sharafaldin, A.Lashkari und A.Ghorbani, „Towards the generation of a new dataset for Intrusion Detection and Characterization of Intrusion Traffic“, 4th International Conference on Information Systems Security and Privacy (ICISSP), Purtogal, Türkei (2018 ).Gharib, I. Sharafaldin, A.
2. Lashkari und A. Ghorbani, "An Evaluation Framework for the Intrusion Detection Dataset." IEEE International Conference on Information Science and Security (ICISS), S. 1-6, 2016.(2016)
3. Gil, A.Lashkari, M.Mamun and A.Ghorbani, "Characterization of encrypted and VPN traffic based on time-related variables". pages.
4. 407-414 in Proceedings of the 2nd International Conference on Security and Privacy of Information Systems (2016). Moustafa and J. Slay, "Evaluation of the Network Anomaly Detection System: Statistical Analysis of the UNSW-NB15 Dataset and Comparison to the KDD99 Dataset." 25(1-3), pp. 18-31, Information Security Journal: A Global Perspective (2016).
5. Moustafa und J.Slay, „UNSW-NB15: Comprehensive Data Set for Network Intrusion Detection Systems“, UNSW-NB15: Comprehensive Data Collection for Network Intrusion Detection Systems (Data Set UNSW-NB15).1-6 , IEEE Military Konferenz zu Kommunikations- und Informations systemen (MilCIS) (2015).

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

# INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

## IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details