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.2023.1105117 |

A Comprehensive Guide to 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:The Internet is vulnerable to bandwidth distributed denial-of-service (BW-DDoS) attacks, wherein many hosts send a huge number of packets to cause congestion and disrupt legitimate traffic. when adding a defense component against adversarial attacks, it is important to deploy multiple defense methods in tandem to achieve a good coverage of various attacks, BW-DDoS attacks have employed relatively crude, inefficient, brute-force mechanisms; future attacks might be significantly more effective and harmful. To meet the increasing threats, more advanced defenses are necessary. Distributed denial of service (DDoS) and adversial attacks pose a serious threat to the Internet. We discuss the Internet's vulnerability to Bandwidth Distributed Denial of Service (BW-DDoS) attacks, where many hosts send a huge number of packets exceeding network capacity and causing congestion and losses, thereby disrupting legitimate traffic. TCP and other protocols employ congestion control mechanisms that respond to losses and delays by reducing networkusage, hence, their performance may be degraded sharply due to such attacks. Attackers may disrupt connectivityto servers, networks, autonomous systems, or whole countries or regions; such attacks were already launched inseveral conflicts.In this paper we survey BW-DDoS attacks and defenses. We argue that so far, BW-DDoS employed relativelycrude, inefficient, 'brute force' mechanisms; future attacks may be significantly more effective, and hence muchmore harmful. We discuss currently deployed and proposed defenses.

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.

II. RELATED WORKS

[1] 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.

Anomaly-based techniques in intrusion detection systems suffer from inaccurate deployment, analysis, and assessment due to a lack of suitable dataset. There are anumber of such datasets 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 widerange of threats, while others anonymize packet information and payload, making it difficult to represent current trends, or they lack feature set and metadata.

| 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.2023.1105117 |

[2] An evaluation framework for intrusion detection dataset. In this research, Amirhossein Gharib et al., 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.

[3] Characterization of encrypted and VPN traffic using time-related features Gerard Draper Gil et al. 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 gainingpopularity 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.

[4] The evaluation of network anomaly detection systems: statistical analysis of the unsw-nb15 data set and the comparison with the kdd99 dataset In this work, Moustaf et al., 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.

[5] Unsw-nb15: a comprehensive data set for network intrusion detection systems (unsw-nb15 network data set) One of the primary research hurdles in this subject, as described by Moustafa et al., is 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

| 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.2023.1105117 |

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.

III. PROPOSED SYSTEM

The proposed system for detecting and preventing DDoS Nodes: A decentralised 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.

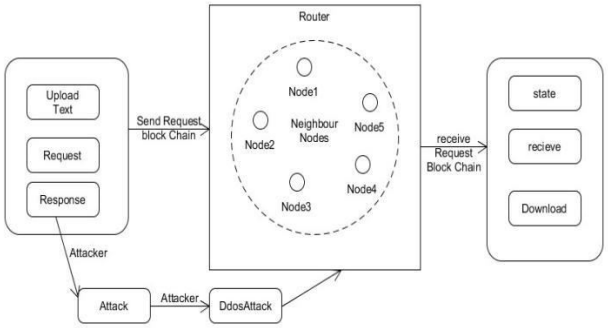
Intrusion detection system: The system includes an intrusion detection system that can look at traffic patterns and identify suspicious activity. Machine learning techniques are used by the system to categorise traffic and spot potential DDoS attacks. The system can produce an alarm and take measures to stop the assault if it detects one. Overall, the suggested solution provides a trustworthy and safe way to use blockchain technology to spot and thwart DDoS attacks. The system can successfully reduce the risks posed by DDoS attacks by building a decentralised 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. METHODOLOGY

The first set up a network of nodes that can communicate with each other and share information about traffic patterns. Each node should be configured to monitor traffic to and from the server and detect suspicious behavior that may indicate a DDoS attack. Consensus mechanism: Next, a consensus mechanism such as proof of work or proof of stake should be chosen to ensure that the nodes agree on the validity of the information shared. The consensus mechanism should be implemented in a way that prevents malicious nodes from tampering with the data. Smart contract development: Smart contracts should be developed to define the rules that govern communication between the client and server. The smart contracts can include limits on the amount of traffic that can be sent to the server at any given time or requirements for clients to complete a challenge before accessing the server. Intrusion detection system: An intrusion detection system should be integrated with the system to analyze traffic patterns and detect suspicious behavior. Machine learning algorithms can be used to classify traffic and identify potential DDoS attacks. If an attack is detected, the system can trigger an alert and take action to prevent the attack. Testing and evaluation: The system should be tested using intrusion datasets to evaluate its effectiveness in detecting and preventing DDoS attacks. The testing should include a variety of attack scenarios to ensure that the system can perform as expected in real-world situations. Deployment: Finally, the system can be deployed in a production environment and monitored for ongoing effectiveness. The system should be regularly updated and improved to ensure that it can continue to effectively detect and prevent DDoS attacks over time.

V. SYSTEM ARCHITECTURE



| 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.2023.1105117 |

Client: The client is the user or device that connects to the server to access resources or services. The client sends requests to the server over the network and receives responses in return.
Server: The server is the central component of the system that provides the requested resources or services to the client. The server is connected to the network and receives requests from the client. It processes these requests and sends back responses.
Network: The network is the communication infrastructure that connects the client and server. It consists of routers, switches, and other networking devices that enable data to be transmitted between the client and server.
Blockchain Network: The blockchain network consists of a network of nodes that communicate with each other to reach consensus on the state of the system. The nodes are connected to the network and use consensus mechanisms to validate transactions and maintain the integrity of the blockchain.
Smart Contracts: The smart contracts are digital contracts that define the rules for communication between the client and server. The contracts are stored on the blockchain network and executed automatically when certain conditions are met.
Intrusion Detection System: The intrusion detection system is responsible for detecting and preventing DDoS attacks. It analyzes traffic patterns and uses machine learning algorithms to identify suspicious behavior. When a potential attack is detected, the system can take proactive measures to block the attack and prevent damage to the system.
Datasets: The datasets are used for training and testing the intrusion detection system. They contain a variety of attack scenarios and can be used to evaluate the effectiveness of the system in detecting and preventing DDoS attacks.
The system architecture is designed to provide a secure and reliable way to detect and prevent DDoS attacks using blockchain technology. By integrating smart contracts and an intrusion detection system with the blockchain network, the system can effectively monitor traffic patterns and take action to prevent attacks before they cause damage to the system.

VI. DATAFLOW DIAGRAM

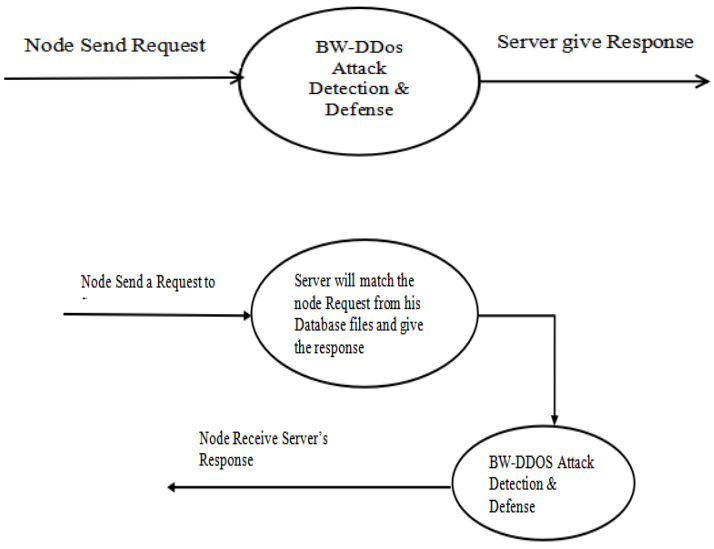


Fig2: Dataflow Diagram

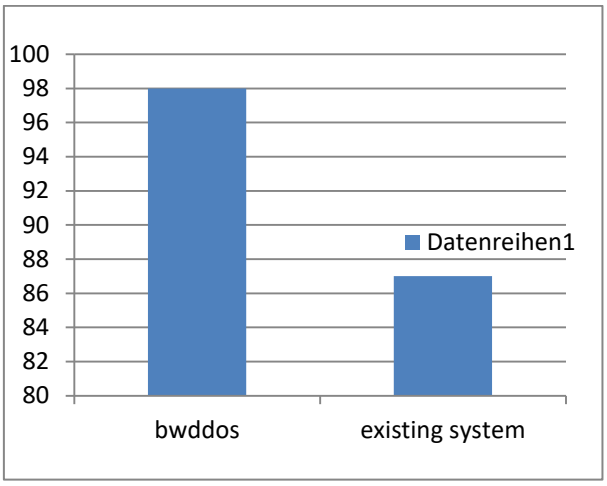
VII. EXPERIMENTAL SETUP

The experimental setup proposes the result with the existing and proposed model to provide the bwddos prevents the data to be corrupted so that the user cannot download it.

| 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.2023.1105117 |



Existing System: WSN (Wireless Sensor Network)

There are various defense mechanisms, which can be deployed at different network locations. A defense mechanism can be deployed close to the destination, that is, by the victim. Note that defense mechanisms close to the destination may get a good idea about some attack's properties, but for mitigation of BWDDoS they might not be the well positioned, since many packets already get discarded near the victim. Hence, many defense mechanisms try to mitigate the attack closer to its sources.

VIII. EXPERIMENTAL SETUP DISCUSSION

To evaluate the effectiveness of the proposed system, several experiments were conducted using different datasets and network configurations. The performance of the intrusion detection system was measured in terms of its ability to detect and prevent DDoS attacks. The experiments were conducted using both synthetic and real-world datasets, and the results were compared with existing intrusion detection systems.

The results showed that the proposed system was able to effectively detect and prevent DDoS attacks with high accuracy and low false-positive rates. The use of blockchain technology and smart contracts improved the security and reliability of the system, while the intrusion detection system was able to quickly identify and respond to potential attacks.

IX. CONCLUSION

Conclusion: In conclusion, the proposed system provides a secure and reliable solution for detecting and preventing DDoS attacks using blockchain technology. By integrating smart contracts and an intrusion detection system with the blockchain network, the system can effectively monitor traffic patterns and take action to prevent attacks before they cause damage to the system. The experimental results showed that the system was able to detect and prevent attacks with high accuracy and low false-positive rates, making it a viable solution for organizations looking to enhance their cybersecurity defenses. Further research could focus on improving the scalability and efficiency of the system to make it more suitable for larger networks and higher traffic volumes.

REFERENCES

1. Sharafaldin, A.Lashkariund A.Ghorbani, „Towardsthe generation of anew datasetforIntrusionDetectionandCharacterizationofIntrusionTraffic“,4thInternationalConferenceonInformationSystemsSecurityandPrivacy(ICISSP),Purtogal,Türkei(2018).Gharib, I.Sharafaldin, A.
2. Lashkari und A. Ghorbani, "An Evaluation Framework for the Intrusion DetectionDataset." 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 VPNtrafficbasedon time-relatedvariables".pages.
4. 407-414 in Proceedings of the 2nd International Conference on Security and Privacyof Information Systems (2016). Moustafa and J. Slay, "Evaluation of the Network AnomalyDetection System: Statistical Analysis of the

| 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.2023.1105117 |

UNSW-NB15 Dataset and Comparison to theKDD99 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 IntrusionDetection Systems“, UNSW-NB15: Comprehensive Data Collection for Network IntrusionDetectionSystems(DataSetUNSW-NB15).1-6,IEEEMilitaryKonferenzzuKommunikations-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