JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3412-3428
https://publishoa.com
ISSN: 1309-3452

A Systematic Review of DoS Attack Prevention Techniques on Delay Tolerant Network

Rajashri Chaudhari[1], Manoj Deshpande[2]

[1]Phd Research Scholar, ACPCE, Kharghar, Navi Mumbai.
[2]Professor and Dean,ACPCE, Kharghar, Navi Mumbai.
Email:rajashri.c93@gmail.com[1], mmdeshpande@acpce.ac.in[2]

Received: 2022 March 15; **Revised:** 2022 April 20; **Accepted:** 2022 May 10.

Abstract

The Delay Tolerant Network (DTN) was developed to solve technical problems in the end-to-end network. DTN is becoming more and more important because communication networks are ubiquitous today. It provides automotive communication solutions. DTN is a decentralized and self-managed system with unique network attributes and attributes; however, attributes such as high mobility nodes, network uplinks and downlinks, and separate routing can cause network vulnerabilities. These vulnerabilities include the host being compromised, which in turn will bring security risks, because the compromised host may destroy the routing protocol in the network. This article analyses the various types of attacks that we can use DTN to detect and prevent, such as DDoS attacks, flood attacks, and so on.

Keywords: Flooding attacks, security, DDoS attack, DTN

Introduction

As the Internet has become an indispensable part of human life, the security of data transmitted via the Internet has become more and more important. The Internet was originally designed to be open and extensible, without any security issues. Therefore, attackers use this weakness to achieve their goals. In recent years, the number of online threats has increased significantly. DDoS attacks and flood attacks are the main types of these threats [2]. The purpose of these attacks is to prevent legitimate users from accessing Internet services. Websites such as Yahoo, CNN, and Amazon.Com are all equipped with comprehensive security features and were reportedly attacked by DDoS in 2000.DDoS attacks act a serious threat to the availability of Internet services. This attack forces multiple agents to send a large number of data packets to the victim, which easily consumes the victim's resources [4]. A delay network is purposely designed to operate efficiently over extremely long distances (i.e. space communications). In these surroundings, a delay plays an important role for factor affecting network quality. The networks are constantly interconnected, and there is no dedicated network infrastructure for network management [6]. Combining this, DTN has faced some severe challenges, such as communication delay, broadcasting, and routing, but another major challenge is to protect network nodes from intruders. Existing mechanisms provide significant security but use different and costly methods. Time ultimately affects bandwidth; the battery life of mobile nodes is limited. Abbreviated as Delay Tolerant Network, is plotted to start a connection between two or more mobile nodes moved by people or vehicles [16]. Delay Tolerant Network supports communication in between unsteady and remote environments. In these environments, network nodes are often interrupted due to the lack of continuous communication & communication infrastructure.

When a node receives one or more data packets [18], DTN can transmit data through an automatic segmentation mechanism and store these data packets in its buffer space. The packets from buffer space can redirect data whenever they fall into another, when the packet is within the range of the node. To the destination in DTN, the connection between nodes is flexible, and the connection time can be shorter because the nodes are present in the mobile, the bandwidth available for transmission is also limited, and due to the mobility of the nodes, they can also have limited buffering [23]. If it is a malicious or selfish target, any number of nodes on the network can launch a flood attack. It can launch a flood attack to overload another network and improve its communication performance [22].

Need of review and contribution of the project

The contribution and focus of this article is the investigation of anonymous communication in the context of DTN (Delay Tolerant Network). Unfortunately, it is vulnerable to malicious nodes instead, our work proposes a new message forwarding algorithm that can transfer messages from source to target and try to achieve significant performance improvement in the terms of sensitivity, accuracy, precision as compared to the various existing attacks detection methods [24].

Literature Review

A literature review allows one to get an insight into the different aspects of the problem being studied. It explores innovative computational methods, shines a light on how to enhance data collecting performance, and proposes strategies to maximize data collection and understanding effectiveness. Therefore, reviewing the literature is an essential step in the development of the research project. Literature reports are secondary sources, which have no current or initial scientific research published.

Alodat I et al. [1] this paper examines message transmission from the attacker process within DTN.DTN is a new analysis field that can be developed in the networking.DTN network does not having established a complete trackconnecting end-to-end networks through direct channels and may have been in development for such a long time. As the improvement part, they compare the mapping of the Delay Tolerant Network routing protocol with the real area and then examine the possibility of detecting the existence of security holes that lead to protection. In a flood attack or black hole attack, need to control the size of the buffer when the host fills up the buffer.

Sumanth S [3]the system proposed a DDoS defence system, including detecting attacks in decision trees and tracking attackers using matching patterns. It is depend on the monitoring that network traffic is different from normal traffic during DDoS attacks, and uses decision trees and deep learning generation algorithms to build classification models to detect abnormal traffic.

Zhao Jingjing et al. [5] in this articlethe author examine the previous methods for network traffic classificationmethods from a new and overallviewby divide them into five categories based on representative classification features, i.e statistical classification and port-based classification, payload-based classification. We use the data set and traffic characteristics used to classify the traffic in the survey. Finally, we determined some unresolved issues and future directions in this research area.

J. Yang et al [7]proposed a new malicious SSL traffic detection method that can re-collect the SSL records of the captured IP packets and use deep learning to verify the properties of the SSL records. The proposed method extracts unencrypted content from the reorganized data set and generates a clear data stream from the sequential SSL data set for deep learning classification. These feature maps are sent to a neural network-based volume integration classifier to determine whether the SSL stream is malicious. The proposed method perfectly separates secure and malicious traffic flows through encrypted SSL channels.

Zulfiqar Ali Zardari et al [8] proposed a method for detecting jellyfish attacks in MANET. The proposed method combines the authentication and reliability of nodes and the KNN algorithm used to identify jellyfish attacks, where each node calculates the main trust scores and the main trust scores associated with the computing node. Secondary trust score through neighbour recommendation and trust index. The KNN algorithm separates the jellyfish node from other legal nodes based on the difference in behaviour. At the end the result shows the proposed technique could decrease delay and increase throughput of network by ignoring jellyfish nodes.

Zhaoyang Du et al [9] The Vehicle Delay Tolerant Network (DTN) can realize communication between mobile nodes when cellular base stations are unavailable and the connection between mobile nodes is intermittent. They proposed a new protocol for automotive DTN. The proposed protocol can more accurately evaluate the stability of the communication channel using drones in the VDTN environment. Through actual simulations, the proposed protocol is evaluated against the existing baseline.

Jiarui Man et al [10] proposed a residual learning model for network attack detection. Model converting the UNSW-

NB15 data set into an image uses the residual block to create a deeper neural convolution network to learn other important functions and calculated the loss to solve the class imbalance problem in the training set and identified minor attacks in the test set. Batch normalization and global average grouping were used to avoid overfitting and improve the model. From the experimental results, it is shown that the proposed model can improve the accuracy of attack detection.

N. Nishanth et al [11] In an SYN Flood DoS attack, the attacker sends a large number of forged SYN packets, which not only overflows the target buffer but also causes network congestion. Here Bayesian inference is used to detect SYN flood attacks.

M premkumar et al [12] proposed neural clustering algorithm for wired and wireless networks measures the load of the ISP server when necessary to better identify abnormal DDoS attacks during heavy traffic using NS2.

Vidal Attias et al [13] presents IoT devices which are mainly generate transactionsof data, distributed ledgers and micropayments that use fees to regulate network access are not the best choice. They checked the free architecture designed by IOTA and developed specifically for the Internet of Things. In this work, they have developed a denial of service prevention mechanism that can eliminate network diversity, computing power of limited nodes, & optimization of certain equipment.

S. Gao et al [14] recommended a device for the safety of network servers, routers, and customer hosts from turning into handlers, zombies, and sufferers of DDoS meals attacks. The IP primarily based public community is included via way of means of Net Shield devices on the internet. The device vulnerabilities are eliminated via way of means of preventive and deterrent management approaches. An adaption approach is carried out in this device to provoke the ambiguity detection approach for proper intrusion response. A low-charge DDoS (LDDoS) is green to cowl the community site visitors because of its similarity with regular site visitors.

Han Y et al [15] in recent years, as a brand new kind of community architecture, software-described networks have attracted fantastic interest from researchers. They are regularly being extensively implemented in diverse fields of the community. However, low-charge DDoS attacks in opposition to the statistics community make use of IoT networks to discover and save you DDoS attacks have now no longer but turn out to be studies hotspots, and associated studies outcomes also are less. This paper first researches a way to release such attacks and verifies the effectiveness of such attacks. Then, with the aid of extracting the 4 capabilities associated with the float rules, the characteristic statistics set for detecting such attacks is established.

Lunkad. D et al [17] A DDoS attack in a cloud computing environment is the application layer sending a request through a machine learning communication protocol, which is difficult to detect at the network layer because its pattern matches a legitimate request, making traditional countermeasures unusable. The goal of this paper is to demonstrate the process of detecting prototype DDoS attacks using a supervised learning model based on Support Vector Machines (SVM), which captures network traffic, filters HTTP headers, normalises the data based on operational variables such as rate of false positives, rate of false negatives, and rate of classification, and then sends the information to corresponding training and testing systems. Various machine learning models, such as Navies Bayes, SVM, and proposed methods based on Navies Bayes, are developed using the selected attributes for efficient detection of DDoS attacks.

ChinmayeeSahoo et al [19] proposed system uses several controlled DDoS detection algorithms. The proposed algorithm uses a kernel-based learning algorithm, chi-square test, and Mahalanobis distance. Statistically based on entropy and the four network traffic per minute are used as the discovery indicators. Then, they applied a kernel-based learning algorithm that uses entropy features to identify input vectors suspected of being DDoS attacks.

Sunita Swain et al [20].with the rapid development of the Internet, everyone uses the Internet for a specific purpose. Internet service providers (ISPs) are used to continuously respond to DoS attacks. The proposed system is designed to prevent DoS attacks that occur quickly anywhere. This article looks at 'Machine Learning' based on the discovery of the System. This system creates an interface depend on the signature database previously extracted from network traffic samples. In the Internet scenario, the device interacts with an application are running remotely on the network so that an attacker can control the device. Analysis of the distribution of this system shows that it is a normal network with very little traffic.

Uday Trivedi et al [21] provided a fully automated intellectual property verification system using machine learning methods to review and regularly update intellectual property signatures. Automatic traffic generation for mobile applications is achieved through open source tools such as GUITAR and Appium. Use AutoIT scripts to perform signature verification and search for undetected applications. The results show that our solution saves a lot of work time and recognizes signature updates in the blink of an eye.

P. Nagrath et al [25] this article examines the distinctive kinds of attacks. Experimental effects displaying the effect of numerous attacks like flooding attack, black hole attack& selfish attack on PRoPHET Protocol are provided within the paper. The effect of those attacks on community parameters like power consumed depend on messages delivered, and depend on dropped messages, overhead ratio, and message inactivity is analyzed.

Dr. D Bhavana et al [26] machine learning is rapidly turning into the commercial revolution that the existing global is so inclined to. The middle of this captivating era is to lay out structures that may learn to apply themselves for diverse scenarios, minimizing they want to guide human interventions as far as possible. It has been spreading its wings into many fields like Medicine, Networking, Agriculture, Image Processing etc.and converting them from the ground up.The goal of this paper is to use popular machine learning algorithms and train them on the UNSW-NB15 dataset to create a Network Intrusion Detection System (NIDS) based on the algorithm. This system has been trained and tested to detect nine different types of common cyber-attacks as defined in the dataset: fuzzers, analysis, backdoors, denial of service, exploits, generic, reconnaissance, shell code, and worms.

K. Hussain et al [27]proposed an adaptive detection mechanism that uses an artificial intelligence technology called SYN Flood Attack Detection Based on Bayesian Estimation (SFADBE) for mobile ad hoc networks (MANET). In SFADBE, each node collects current information from available channels and selects a safe and congested free channel (Best Path) for the traffic. The simulation results show that the proposed SFADBE algorithm is cheap and reliable.

W. Khalid et al [28] Delay tolerant network (DTN) is a special type of intermittent connection network (ICN), which is characterized by variable delays, frequent failures, asymmetric data rates, and high error rates. A new resource-efficient algorithm (distributed and based on an intrusion detection system) is proposed to mitigate flood attacks.

Bakker J. et al [29] shows how to use SDN to implement statistical classification to detect DDoS attacks. In a standalone environment, three classifiers were selected to integrate with nmeta2 and then rated on a test physical network that reproduced the DDoS attack scenario. SDN can classify traffic should be carefully considering the choice of the classifier to minimize packet processing overhead. However, there is no specific content in the DDoS attack scenario.

Khuphiran. P et al [30] Considering the application of machine learning algorithms in detecting DDoS attacks, and evaluating two algorithms, support vector machine (SVM) and deep feedforward (DFF), to prove the applicability of these algorithms. Compare the performance of these two algorithms. It is found that DFF can classify data more accurately. Therefore, deep learning is a useful way to classify DDoS attack packets based on accuracy. However, SVM is a suitable method.

K. Arai et al [31] proposed an ER reduction scheme based on theoretical contact probability to mitigate flood attacks on the network over time. If the node does not have enough time to receive conflicting input, increase the number of entries without conflicting entries on the network Possibility. By removing such entries, energy consumption can reduced while the effect of ER scheme is kept. As per the result shows, proposed scheme is successfully reduced energy consumption while the performance of ER.

T. Idezuka et al [32] in recent years, a variety of direct routing schemes have been proposed for distributed mobile ad hoc networks. These networks are the most representative in the network delay/disconnection environment. In this article, they focus on analyzing the behaviour of flooding attacks uses malicious nodes to generate unnecessary messages to exhaust network resources. Through the simulation result, they reveal, how flooding attacks are affecting the system performance.

J. Cho et al [33] this article shows DTNs are come across in the military environments, where network connectivity is not secure or guaranteed due to disconnection or delay of frequency level. They propose a trust framework based on provenance which is called PROVEST, they are worked to achieve the increase in the correct message delivery received by destination nodes with peer-to-peer trust networks. This work acquires a model-based technique to estimate the PROVEST performance.

QaisarAyub et al [34]By defining the ‘n' number of message transmission quotas, the delay tolerant network Spray and Wait routing protocol reduces resource consumption. A large-size message, on the other hand, consumes more buffer space, bandwidth, and energy with the same transmission quota. Similarly, existing buffer management policies consider message size, arrival time, and hop count but ignore the network congestion caused by a message. To address the above mentioned issues, we proposed a routing protocol for delay tolerant networks known as resource refrain quota based routing protocol. A 'N' number of message copies are assigned by the proposed protocol to transmit the energy quota. In addition, message was only passed to those nodes with high probability of meeting the destination of the message. We have also developed a mechanism to drop messages that cause the congestion.

Jichkar, B [35] this paper proposed a new Bayesian Network (BN) routing algorithm to create a predictive model designed to divine node movement patterns in real VDTN scenes. To increasemore accuracy of model prediction, a complete BN model is established, in which more node attributes are selected. The simulation results show that the proposed VDTN routing algorithm based on the BN model can increase delivery with a lower forwarding rate.

Yuan X. et al [36] this paper shows, Low-speed attacks are difficult to detect because they are similar to the victim's legitimate network traffic. At the same time, DDoS attacks on the victim's system must occur over time. The system proposed a deep learning based DDoS attack detection approach (DeepDefense). They have designed a RNN (recurrent neural network) to learn patterns from network traffic and track the network attack activities.

WooseokSeo et al [37] recent advancements in network technology and related services have resulted in a rapid increase in data traffic. Anomaly detection cannot be utilised for real-time traffic. This document provides signature-based variant attack detection. The system detects attacks on two levels. In order to execute accurate classification, the level 1 classifier performs real-time, medium-accuracy inbound traffic detection, while the level 2 classifier collects statistical characteristics of the traffic. Overcome the flaws in today's network security.

IndraneelSreeram et al [38] proposed a model that is a bio-inspired bat algorithm for rapid and early detection of App-DDOS using HTTP floods. These experiments were conducted using the CAIDA benchmark data set, and the results were to increase the relevance of the proposed model.

Karimazad and Faraahi et al [39] describes DDoS detection using attack packet attributes and RBF neural network methods. The RBF neural network uses seven feature activations in each window and classifies the information as normal or offensive. In the filtering module for future actions, if the data is normal, it is sent to its destination. They recommended using the statistical function of the RBF neural network to detect DDoS attacks, another method such as decision tree and gray correlation analysis.

Subbulakshmi T. et al [40] Due to widespread use of computer networks, the number of attackers continues to increased, so intrusion detection systems are very important as a protective measure, because firewalls cannot defend against attacks within the organization. We can use the dataset to train IDS effectively. In this paper, they use the latest DDoS data types to create DDoS data sets derived from various other DDoS attack parameters. A new type of SVM called EMCSVM is proposed that weights to the data set of the data set to detect different types of DDoS attacks.

J. F. Naves et al [41] this paper developed a buffer management machine that is used against the acknowledgment of forge attacks in DTNs (Disruption Tolerant Networks). The proposed machine is unable to immediately drop acknowledged messages but the machine can drop those messages first, when the buffer is full. The proposed system also does not depend upon any authentication method. The system providing higher delivery rates up to 142%.

P. T. Ngoc Diep et al [42]proposed FDER system to detect flooding attacks and even now allow simultaneously authorized burst traffic. They have design FP (Forwarding policy) to make sure fairness in the performance of delivery between normal traffic and burst traffic. The results show FDER can detect flooding attacks at a higher accuracy. Moreover, FP could reduce the smart flooding attack and still provide fair performance to support the scenario of bursty traffic.

T. N. D. Pham et al [43] Delay Tolerant Network (DTN) is designed to handle intermittent connections and long delays in wireless networks. To identify individual misbehaviours, we determined the forwarding rate that can distinguish the behaviour of the attacker from the normal host. Malicious hosts can evade detection by conspiring to manipulate their forwarding rate indicators. To permanently delete messages while increasing indicators, attackers usually need to create fake meeting minutes by sending a large number of fake messages. The proposed Statistical-based Detection of Blackhole and Greyhole attackers (SDBG) system is used to detect malicious attacks. SDBG can detect malicious colluding nodes, with a high detection rate, low false alarm rate, changes in the number of colluding nodes, high packet loss probability, and different routing protocols.

P. Asuquo et al [44]This article shows the analysis of the Delay Tolerant Network (DTN) in the communication area. DTN is used to the delivered message from the source to the destination node in the fact of imaginary infrastructure and network connectivity. However, the DTNs are also used for security threats in different attacks. This article focuses on the study of the impacts of black hole and packet flooding attacks in communication with the use of a DTN network.

W. Narongkhachavana et al [45] this paper presents a new routing protocol that is used to set limits to the message repetitions. This system's network node helps to spread the messages with a lower possibility in the case of messages are currently distributed in the local area. The system increases the chance for a node to spread messages to other network areas.

P. T. Ngoc Diep et al [46] proposed a scheme for detection of flooding attack that piggybacks to come across record based on another scheme of detecting black hole attack. Their simulation result shows that their system can detect flooding attacks at high accuracy and the system can detect multiple attacks in DTN with little overhead.

Gideon Rajan et al [47] this paper proposed a new secure key management framework for the security of DTN. The system using distribute cryptographic keys which securely represent the nodes. These distributed keys are used public-key cryptography to reduce during network attacks.

Aniekan Julius Bassey et al [48] Disruption Tolerant Networks (DTN) provide connectivity in complex network environments where traditional protocols fail due to extreme delays and disruptions. This document recommends using the Rivest Shamir Adleman (RSA) algorithm to improve security to identify the attacker, and remove the attacker's host. It provides rigorous probabilistic analysis and evaluates the effectiveness and efficiency of our system through extensive simulations.

Sarawagya Singh et al [49] this article shows an attack can attempt to destroy, filter, damage, leak, or gain unauthorized access. Attacks can damage the network and launch different types of attacks: black-hole attacks, gray attacks, and wormhole attacks. This document mainly focuses on node failures and DTN attacks. This work helps to understand the DTN network and information about misconduct and attacks on the DTN network.

D. S. Delphin Hepsiba [50] this paper shows Discontinuous communication between nodes used for data transmission is used by the Disruption Tolerant Network (DTNs), which is designed to operate in a distributed system. In addition, we can defend against a small number of attackers in each collision. The proposed algorithm is the training of an automata Feedback mechanism. It collects feedback from previous nodes, thereby reducing restrictions on subsequent nodes. The goal is to roughly identify the attacker and discard the flooded packets.

Mahalaxmi. R et al [51] The DTN use the mobility of nodes to achieve contact, and mobile nodes will move in some cases. It is recommended to check the transmission of the statement to prevent flood attacks; use homophonic encryption to protect the data. The P and T assertion scheme is used to verify the data. Proper buffer management can reduce the possibility of flood attacks in dynamic environments. It can withstand severe flood attacks.

Y. Cao et al [52] this article shows the survey of routing in DTN. The article shows the first review of the existing intended issue of DTNs because of its substantial research level. To examine their assumption author had performed research on the multicasting issues found in DTN.

Y. Guo et al [53], to control the pollution in the city author had proposed a system that uses the transportation system all over the city, Braunschweig. This system was designed based on the delay-tolerant networking principle. Since dependability and resilience are the crucial factors in such systems, they propose a Misbehaviour Detection System (MDS) to protect the Braunschweig network from the interference of faulty and hostile nodes. The proposed system estimates the technique between different routing protocols in DTNs (Delay Tolerant Network), this article tried to show that the proposed MDS system can protect the whole system at low cost.

Dhiraj Kr. Mishra et al [54]the delay-tolerant network has limited resources. A selfish node discards valid data packets from other nodes, resulting in poor message delivery and the loss of valuable network resources. Based on the mini-max theory, this scheme assigns credit to non-selfish nodes. It lowers the message discard rate, detects selfish nodes, and boosts network performance in terms of delay, message discard rate, and delivery rate.

G. Ansa et al [55]. The objective of this project is to make safety protocols resilient to DOS attacks, which are compulsory security services. They suggest a hierarchical design based on the usage of lightweight and difficult-to-forge cookies to achieve this. The DOS defence method can detect and delete assault packages in advance. Insider nodes that have compromised are discovered and isolated. As per result, the proposed system is adaptable and energy-saving. Because of the cookie's small weight, computation and verification are straightforward and quick. The DTN- cookie's composition and calculation mode make it difficult to fabricate and resistant to masquerade, replay, modification, and resource exhaustion attacks. The attacker's penetration of data packets can trigger a DOS flood attack. A security service that resists DOS attacks due to exhaustion of resources. To this end, they provide a hierarchical structure based on the use of easily forged cookies.

V. Natarajan et al [56] in this paper, refer to DoS attacks and selfish behaviours related to data generation as resource-based attacks. They are investigating two types of abuse attacks: Therefore, they have proposed different schemes to detect these attacks. Comprehensive and real-world evidence shows that their detection scheme has a lower average detection delay. In addition, the probability detection of deep attacks has a lower false-positive rate and a low false-positive rate.

F. C. Lee et al [57] this paper proposed to take advantage of and develop a very prospective factor to enclose and reduce flooding attacks by the queuing machine based on prospective factors. To illustrate the concept of the system they develop the module as a solution for Probabilistic Routing Protocol using History of Encounters and Transitivity (PRoPHET) which is the routing protocol in DTN.

S. H. C. Haris et al [58]the key issue in this document is how to identify TCP SYN flooding on the network. The payload and TCP SYN flooding attacks in this article are detected using anomaly detection based on unused spaces in the Hypertext Transfer Protocol (HTTP). Through the payload, the suggested detection method TCP SYN can identify flooding in the network.

K. Fall et al [59] this paper presents a review of the Delay Tolerant Network (DTN) architecture and point out some open issues. From the focus on the deep class of networks that may suffer from disturbance, affected on decisions spanning & addressing, message formatting, routing, congestion management, and security. The author expects the key management, congestion handling, the capability of multicasting on the research and development of active areas, and DTN may continue active research to try for the next few years.

Lloyd Wood et al [60].this article shows the study about bundle protocol. Bundle protocol is the layer over the different internet protocols on the different networks, many IP runs on many networking links already. They were implementing the customer support for the DTN bundle to meeting different layers directly on the links.

Conclusion

Delay tolerant networks are constructed networks. Security is the main concern of the Delay-Tolerant network. In particular, flood attacks can slow down the network speed and abuse network resources. We can work on DDoS attack detection as well as prevention Transit nodes monitor traffic and node behaviour to detect attacks. This method is centralized; our work will be mainly based on a distributed mechanism. Technological progress has brought many advantages to DTN, but it has also brought many challenges to DTN.

References

[1] Alodat, I. (2021). Monitor Potential Attack Locations in a Specific Area within DTN Network. Computer and Information Science, 14, 42.

[2] Liu, X., Ren, J., He, H., Zhang, B., Song, C., & Wang, Y. (2021). A fast all-packets-based DDoS attack detection approach based on a network graph and graph kernel. Journal of Network and Computer Applications, 103079.

[3] Sumathi, S., &Karthikeyan, N. (2021). Detection of distributed denial of service using deep learning neural network. Journal of Ambient Intelligence and Humanized Computing, 1-11.

[4] Selvavinayaki, K. (2021). An Effectual Data Transmission Approach to Prevent Black Hole Attack in Mobile Adhoc Networks.

[5] Jingjing Zhao, Xuyang Jing, Zheng Yan, WitoldPedrycz,Network traffic classification for data fusion: A survey,InformationFusion,Volume 72,2021,Pages 22-47, ISSN 1566-2535,https://doi.org/10.1016/j.inffus.2021.02.009.

[6] Ayub, Q., Rashid, S. Energy Efficient Inactive Node Detection Based Routing Protocol for Delay Tolerant Network. Wireless PersCommun 116, 227–248 (2021). https://doi.org/10.1007/s11277-020-07712-5.

[7] J. Yang and H. Lim, "Deep Learning Approach for Detecting Malicious Activities Over Encrypted Secure Channels," in IEEE Access, vol. 9, pp. 39229-39244, 2021, doi: 10.1109/ACCESS.2021.3064561.

[8] Zulfiqar Ali Zardari ,Jingsha He , Muhammad Salman Pathan , Sirajuddin Qureshi , Muhammad Iftikhar Hussain , Fahad Razaque , Peng He , and Nafei Zhu, "Detection and Prevention of Jellyfish Attacks Using kNN Algorithm and Trusted Routing Scheme in MANET",IEEE, Vol.23,pp[77-87],2021.

[9] Zhaoyang Du, Celimuge Wu, Tsutomu Yoshinaga, XianfuChen,"A Routing Protocol for UAV-Assisted Vehicular Delay Tolerant Networks," in IEEE Open Journal of the Computer Society, vol. 2, pp. 85-98, 2021, doi: 10.1109/OJCS.2021.3054759.

[10] Jiarui Man and GuoziSun,"A Residual Learning-Based Network Intrusion Detection System", Hindawi Security and Communication Networks Volume 2021.

[11] N. Nishanth and A. Mujeeb, "Modeling and Detection of Flooding-Based Denial-of-Service Attack in Wireless Ad Hoc Network Using Bayesian Inference," in IEEE Systems Journal, vol. 15, no. 1, pp. 17-26, March 2021, doi: 10.1109/JSYST.2020.2984797.

[12] M. Premkumar, T.V.P. Sundararajan, DLDM: Deep learning-based defense mechanism for denial of service attacks in wireless sensor networks, Microprocessors and Microsystems, Volume 79, 2020, 103278, ISSN 0141-9331, https://doi.org/10.1016/j.micpro.2020.103278.

[13] Attias, V., Vigneri, L., &Dimitrov, V. (2020). Preventing Denial of Service Attacks in IoT Networks through Verifiable Delay Functions. GLOBECOM 2020 - 2020 IEEE Global Communications Conference, 1-6.

[14] S. Gao, Z. Peng, B. Xiao, A. Hu, Y. Song and K. Ren, "Detection and Mitigation of DoS Attacks in Software Defined Networks," in IEEE/ACM Transactions on Networking, vol. 28, no. 3, pp. 1419-1433, June 2020, doi: 10.1109/TNET.2020.2983976.

[15] Han, Y., Lian, J., & Huang, X. (2020). Event-triggered H∞ control of networked switched systems subject to denial-of-service attacks. Nonlinear Analysis: Hybrid Systems, 38, 100930.

[16] Singh, N., Dumka, A., & Sharma, R. (2020). Comparative Analysis of Various Techniques of DDoS Attacks for Detection & Prevention and Their Impact in MANET.

[17] Lunkad, D. (2020). DDOS Attack Detection Using Machine Learning For Network Performance Improvement.

[18] Jalili, R., Imani-Mehr, F., Amini, M., &Shahriari, H. (2020). Detection of Distributed Denial of Service Attacks Using Statistical Pre-processor and Unsupervised Neural Networks. ISPEC.

[19] ChinmayeeSahoo. 'CLOUD COMPUTING AND ITS SECURITY MEASURES', International Journal of Electronics Engineering and Applications, Volume 8, Issue I, Jan-June 2020, pp 10-19, doi 10.30696/IJEEA.VIII.I.2020.10-19,

[20] Sunita Swain and Rajesh Kumar Tiwari, (2020), "Cloud Security Research- A Comprehensive Survey" Int. J. of Electronics Engineering and Applications, Vol. 8, No. 2, pp. 29-39, DOI- 10.30696/IJEEA.VIII.II.2020.29.39.

[21] Uday Trivedi, Munal Patel, "A Fully Automated Deep Packet InspectionVerification System With Machine Learning" 2020.

[22] Nadiammai, G.V., &Hemalatha, M. (2019). Effective approach toward Intrusion Detection System using data mining techniques. Egyptian Informatics Journal, 15, 37-50.

[23] Francisco Sales de Lima Filho, Frederico A. F. Silveira, Agostinho de Medeiros Brito Junior, Genoveva Vargas-Solar, Luiz F. Silveira, "Smart Detection: An Online Approach for DoS/DDoS Attack Detection Using Machine Learning", Security and Communication Networks, vol. 2019, Article ID 1574749, 15 pages, 2019. https://doi.org/10.1155/2019/1574749.

[24] Li Q., Meng L., Zhang Y., Yan J. (2019) DDoS Attacks Detection Using Machine Learning Algorithms. In: Zhai G., Zhou J., An P., Yang X. (eds) Digital TV and Multimedia Communication. IFTC 2018. Communications in Computer and Information Science, vol 1009.

Springer, Singapore. https://doi.org/10.1007/978-981-13-8138-6_17

[25] P. Nagrath, S. Aneja and G. N. Purohit, "Attacks in Delay Tolerant Networks: Classification and Analysis," 2019 11th International Conference on Communication Systems & Networks (COMSNETS), 2019, pp. 489-491, doi: 10.1109/COMSNETS.2019.8711072.

[26] Dr. D. Bhavana, Dr. K. Kishore Kumar, Vishnu Chilakala, Hemanth Gupta Chithirala, Tejesh Reddy Meka, "A Comparison Of Various Machine Learning Algorithms In Designing An Intrusion Detection System",IEEE, VOLUME 8,pp[2407-2413],2019.

[27] K. Hussain, S. J. Hussain, N. Jhanjhi and M. Humayun, "SYN Flood Attack Detection based on Bayes Estimator (SFADBE) For MANET," 2019 International Conference on Computer and Information Sciences (ICCIS), 2019, pp. 1-4, doi: 10.1109/ICCISci.2019.8716416.

[28] W. Khalid, N. Ahmed, M. Khalid, A. Ud Din, A. Khan and M. Arshad, "FRID: Flood Attack Mitigation Using Resources Efficient Intrusion Detection Techniques in Delay Tolerant Networks," in IEEE Access, vol. 7, pp. 83740-83760, 2019, doi: 10.1109/ACCESS.2019.2924587.

[29] J. N. Bakker, B. Ng and W. K. G. Seah, "Can Machine Learning Techniques Be Effectively Used in Real Networks against DDoS Attacks?," 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018, pp. 1-6, doi: 10.1109/ICCCN.2018.8487445.

[30] P. Khuphiran, P. Leelaprute, P. Uthayopas, K. Ichikawa and W. Watanakeesuntorn, "Performance Comparison of Machine Learning Models for DDoS Attacks Detection," 2018 22nd International Computer Science and Engineering Conference (ICSEC), 2018, pp. 1-4, doi: 10.1109/ICSEC.2018.8712757.

[31] K. Arai, S. Haruta, H. Asahina and I. Sasase, "Encounter Record Reduction Scheme based on Theoretical Contact Probability for Flooding Attack Mitigation in DTN," 2018 24th Asia-Pacific Conference on Communications (APCC), 2018, pp. 34-39, doi: 10.1109/APCC.2018.8633455.

[32] T. Idezuka, T. Kimura and M. Muraguchi, "Behavior Analysis of Flooding Attacks in Sparse Mobile Ad-Hoc Networks," 2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2018, pp. 1-2, doi: 10.1109/ICCE-China.2018.8448401.

[33] J. Cho and I. Chen, "PROVEST: Provenance-Based Trust Model for Delay Tolerant Networks," in IEEE Transactions on Dependable and Secure Computing, vol. 15, no. 1, pp. 151-165, 1 Jan.-Feb. 2018, doi: 10.1109/TDSC.2016.2530705.

[34] QaisarAyub and Sulma Rashid, "Resource refrain quota based routing protocol for delay tolerant network", Springer Science+Business Media, 2018.

[35] Jichkar, B., &Mehetre, D. (2017). Survey on Delay Attack Detection and Prevention in WSN Data Transport.

[36] X. Yuan, C. Li and X. Li, "DeepDefense: Identifying DDoS Attack via Deep Learning," 2017 IEEE International Conference on Smart Computing (SMARTCOMP), 2017, pp. 1-8, doi: 10.1109/SMARTCOMP.2017.7946998.

[37] WooseokSeo and Wooguil Pak," Real-Time Network Intrusion Prevention System Based on Hybrid Machine Learning", IEEE, VOLUME XX, 2017.

[38] IndraneelSreeram, Venkata Praveen Kumar Vuppala, "HTTP flood attack detection in application layer using machine learning metrics and bio inspired bat algorithm", Applied Computing and Informatics, Volume 15, Issue 1,2019, Pages 59-66,ISSN 2210-8327,https://doi.org/10.1016/j.aci.2017.10.003.

[39] Karimazad, R., &Faraahi, A. (2017). An Anomaly-Based Method for DDoS Attacks Detection using RBF Neural Networks.

[40] T. Subbulakshmi, K. BalaKrishnan, S. M. Shalinie, D. AnandKumar, V. GanapathiSubramanian and K. Kannathal, "Detection of DDoS attacks using Enhanced Support Vector Machines with real time generated dataset," 2011 Third International Conference on Advanced Computing, 2017, pp. 17-22, doi: 10.1109/ICoAC.2011.6165212.

[41] J. F. Naves and I. M. Moraes, "Mitigating the ACK counterfeiting attack in Delay and Disruption Tolerant Networks," 2017 IEEE Symposium on Computers and Communications (ISCC), 2017, pp. 1015-1020, doi: 10.1109/ISCC.2017.8024658.

[42] P. T. Ngoc Diep and C. K. Yeo, "Detecting flooding attack while accommodating burst traffic in delay tolerant networks," 2017 Wireless Telecommunications Symposium (WTS), 2017, pp. 1-7, doi: 10.1109/WTS.2017.7943536.

[43] T. N. D. Pham and C. K. Yeo, "Detecting Colluding Blackhole and Greyhole Attacks in Delay Tolerant Networks," in IEEE Transactions on Mobile Computing, vol. 15, no. 5, pp. 1116-1129, 1 May 2016, doi: 10.1109/TMC.2015.2456895.

[44] P. Asuquo, H. Cruickshank, Z. Sun and G. Chandrasekaran, "Analysis of DoS Attacks in Delay Tolerant Networks for Emergency Evacuation," 2015 9th International Conference on Next Generation Mobile Applications, Services and Technologies, 2015, pp. 228-233, doi: 10.1109/NGMAST.2015.65.

[45] W. Narongkhachavana, T. Choksatid and S. Prabhavat, "An efficient message flooding scheme in delay-tolerant networks," 2015 7th International Conference on Information Technology and Electrical Engineering (ICITEE), 2015, pp. 295-299, doi: 10.1109/ICITEED.2015.7408959.

[46] P. T. Ngoc Diep and C. K. Yeo, "Detecting Flooding Attack in Delay Tolerant Networks by Piggybacking Encounter Records," 2015 2nd International Conference on Information Science and Security (ICISS), 2015, pp. 1-4, doi: 10.1109/ICISSEC.2015.7370995.

[47] Gideon Rajan and Gihwan Cho, "Applying Security Architecture with Key Management Framework to the Delay/Disruption Tolerant Networks", IJSIA,Vol-9,pp [327-336], 2015.

[48] Aniekan Julius Bassey, C Fancy, "Mitigating Flooding Attacks in Disruption Tolerant Network", IEEE,Vol 3, pp[85-91],2015.

[49] Sarawagya Singh, Elayaraja.K," A SURVEY OF MISBEHAVIORS OF NODE AND ROUTING ATTACK IN DELAY TOLERANT NETWORK",IEEE,Vol 4,pp[310-315],2015.

[50] D. S. Delphin Hepsiba and S. Prabhu, "Enhanced techniques to strengthening DTN against flood attacks," International Conference on Information Communication and Embedded Systems (ICICES2014), 2014, pp. 1-4, doi: 10.1109/ICICES.2014.7033952.

[51] Mahalaxmi. R, Sambath. K, Sambath. K, "Addressing Flood Attacks In DTN: Prevent Malicious Invasion", IEEE, Vol.3, pp [455-459], 2014.

[52] Y. Cao and Z. Sun, "Routing in Delay/Disruption Tolerant Networks: A Taxonomy, Survey and Challenges," in IEEE Communications Surveys & Tutorials, vol. 15, no. 2, pp. 654-677, Second Quarter 2013, doi: 10.1109/SURV.2012.042512.00053.

[53] Y. Guo, S. Schildt, T. Pögel and L. Wolf, "Detecting malicious behavior in a vehicular DTN for public transportation," Global Information Infrastructure Symposium - GIIS 2013, 2013, pp. 1-8, doi: 10.1109/GIIS.2013.6684378.

[54] Dhiraj kr. Mishra, Dr. Meenu Chawla, "Minimax Theory Based Scheme to Detect Selfish Node and Reduce Latency in Delay Tolerant Network", Conference on Advances in Communication and Control Systems,pp[78-82],2013.

[55] G. Ansa, H. Criuckshank, Z. Sun and M. Al-Siyabi, "A DOS-resilient design for delay tolerant networks," 2011 7th International Wireless Communications and Mobile Computing Conference, 2011, pp. 424-429, doi: 10.1109/IWCMC.2011.5982571.

[56] V. Natarajan, Y. Yang and S. Zhu, "Resource-misuse attack detection in

delay-tolerant networks," 30th IEEE International Performance Computing and Communications Conference, 2011, pp. 1-8, doi: 10.1109/PCCC.2011.6108092.

[57] F. C. Lee, W. Goh and C. K. Yeo, "A Queuing Mechanism to Alleviate Flooding Attacks in Probabilistic Delay Tolerant Networks," 2010 Sixth Advanced International Conference on Telecommunications, 2010, pp. 329-334, doi: 10.1109/AICT.2010.78.

[58] S. H. C. Haris, R. B. Ahmad, M. A. H. A. Ghani and G. M. Waleed, "TCP SYN flood detection based on payload analysis," 2010 IEEE Student Conference on Research and Development (SCOReD), 2010, pp. 149-153, doi: 10.1109/SCORED.2010.5703991.

[59] K. Fall and S. Farrell, "DTN: an architectural retrospective," in IEEE Journal on Selected Areas in Communications, vol. 26, no. 5, pp. 828-836, June 2008, doi: 10.1109/JSAC.2008.080609.

[60] Lloyd Wood, "A Bundle of Problems", IEEE Aerospce conference Big Sky, Montana, March 2009.