Effective Prevention Techniques for Mitigating DOS/DDOS Attacks

Hafiz Muhammad Ashja Khan, Abdul Hafeez, Muhammad Ijlal Khan

Correspondence:

Muhammad Ijlal Khan: muhammad.ijlal.khan@huawei-partners.com

Article Link: https://journals.brainetwork.org/index.php/jcai/article/view/15

DOI: https://doi.org/10.69591/jcai.1.2.2

Citation: Khan, M. I., Khan, H. M. A., & Hafeez, A. (2023). Effective prevention techniques for mitigating DOS/DDOS attacks. *Journal of Computing and Artificial Intelligence, 1*(2), 11–28

Conflict of Interest: Authors declared no Conflict of Interest

Acknowledgment: No administrative and technical support was taken for this research

Article History

Submitted: Mar 11, 2023
Last Revised: Apr 20, 2023
Accepted: May 15, 2023

Volume 1, Issue 2, 2023

Funding
No

An official Publication of
Beyond Research Advancement & Innovation Network, Islamabad, Pakistan

Effective Prevention Techniques for Mitigating DOS/DDOS Attacks

Hafiz Muhammad Ashja Khan[1], Abdul Hafeez [1], Muhammad Ijlal Khan[2,*]

[1]Bahria University, Lahore, Pakistan

[2]Delivering Engineering Excellence, TurnoTech, Pakistan

Abstract

The technology is increasing day by day to a whole new concept, and surely there are more users which are willing to access the internet. Moreover, in increasing the tech there will be more threats that will be generated from time to time. Above all, DoS is the most frequently used attacked in networks to overload the traffic and to make device inaccessible. In our research we have focused on the DoS attack that what is it? Its types and categories etc. We will also be discussing its detection and prevention in different domains of networks like in VANET's or in digital health care etc.

Keyword: dos, ddoS, dos prevention, dos countermeasure, dos attack

Introduction

A Denial of Service (DoS) assault is an assault pointed toward closing down a PC or organization, delivering it blocked off to the planned clients. DoS assaults achieve this by flooding the objective with traffic or sending it data that sets off a block. In the two cases, the DoS assault ransacks genuine clients (i.e., workers, individuals, or record holders). Despite the fact that DoS assaults don't normally bring about burglary or loss of significant data or different resources. Their organization can cost the casualty a ton of time. Instances of objections can be email, internet banking, sites, or whatever other help that depends on an objective PC or organization.

* Corresponding Author: muhammad.ijlal.khan@huawei-partners.com

Categories of Dos Attack

Buffer Overflow

An assault type inside which a memory support flood will make a machine consume all suitable circle space, memory, or C.P.U. time. This sort of exploit regularly winds up in very surprising conduct like framework crashes, or different server ways of behaving, prompting disavowal of-administration.

Flood attacks

By flooding an objective server with a mind-boggling number of parcels, a malevolent entertainer can overpower the server's ability, bringing about a disavowal of administration. For most DoS flood assaults to find lasting success, the noxious entertainer should have more accessible data transmission than the objective.

Significant Dos Attacks

Historically, DoS assaults generally exploited protection vulnerabilities found in network, software program and hardware design. These assaults have grown to be much less common as DDoS assaults have an extra disruptive capability. In reality, maximum DoS assaults also can be changed into DDoS assaults. Common DoS assaults include:

Smurf Attack

A Smurf assault is a type of a disseminated forswearing of administration (DDoS) assault that renders PC networks inoperable. The Smurf program achieves this by taking advantage of weaknesses of the Internet Protocol (IP) and Internet Control Message Protocols (ICMP).

Ping of Death Attack

The ping of death is a type of disavowal of-administration (DoS) assault that happens when an assailant crashes, weakens, or freezes PCs or administrations by focusing on them with larger than usual information bundles. This type of DoS assault regularly targets and takes advantage of inheritance shortcomings that associations might have fixed.

How can we tell that system is experiencing a Dos attack?

While it can be difficult to separate an attack from other network connectivity errors or heavy bandwidth consumption, some characteristics may indicate an attack is underway.

Indicators of a DoS attack include:

1. A typically slow network performance such as long load times for files or websites
2. The inability to load a particular website
3. A sudden loss of connectivity across devices on the same network

Difference between Dos & DDos:

The distinctive contrast among DDoS and DoS is the wide assortment of associations applied withinside the attack. DoS utilizes a brought together association, while a DDoS attack utilizes numerous assets of attack traffic, routinely withinside the state of a botnet. As the server is overflowed with more prominent Transmission Control Protocol/User Datagram Protocol (TCP/UDP) parcels than it could process, it could crash, the data can likewise also develop to be defiled, and resources can be misled or perhaps depleted to the component of incapacitating the machine. The essential contrast among a DoS and a DDoS is that the past is a machine-on-machine attack, simultaneously as the last option incorporates various designs going after a solitary machine.

A. Literature Review on protection against Dos/DDos Attack:

While DoS attacks are less challenging to stop or prevent, but still these attacks can still present a serious threat. Before giving some protection/prevention against DOS attacks we decided to research about this attack in depth and later on we found that it is present in different categories. So at first we will list down the research topics on which we have researched and gathered data but remember they still needs to be explored for deciding that which prevention is better than all others.

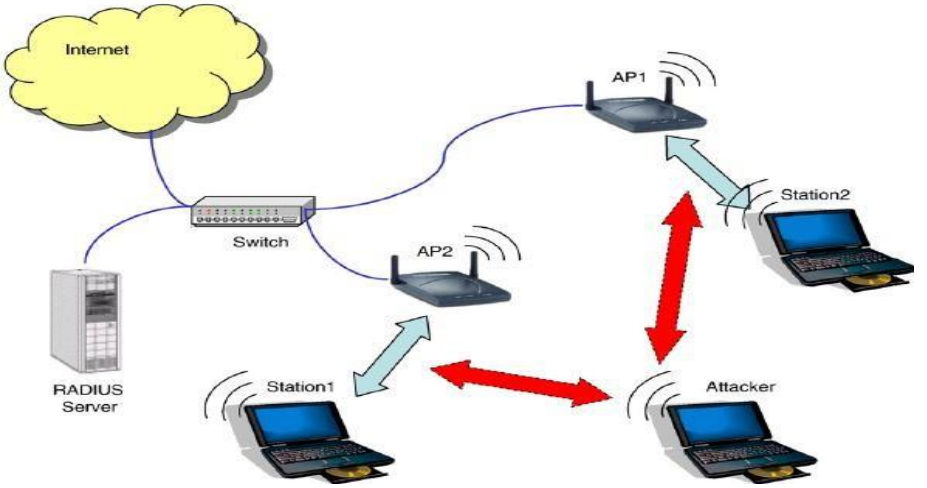
In an article named "Denial of Service Attacks and Countermeasures in IEEE802.11," writer Kemal Bicakci portrays how the accommodation and low worth of 802.11-based remote LANs have prompted their overall reception. We have increasingly more remote admittance to the Internet. It is known that because of the transmission idea of remote access, an excessive number of malevolent assaults and various security

improvements to 802.11 are possible and have proactively been proposed. [1] In any case, these augmentations primarily address weaknesses connected with unapproved access and breaks of privacy. Denial of Service (DoS) assaults are accessibility goes after that endeavour to keep approved clients from getting to the organization. Note that DoS assaults are particular from egotistical conduct roused by a possibly valuable outcome. Due to the transmission idea of remote organizations, DoS assaults are not difficult to perform, particularly in the remote space. Furthermore, there are many tentatively tried 802.11-explicit DoS weaknesses in the writing lately. Figure 1 shows a nonexclusive DoS assault situation on a delegate 802.11. In order to emphasize the importance of the problem, in this article the author would like to present a holistic view of DoS attacks on 802.11 wireless networks. The main goal of the author lies in two perspectives: [1]

1. Systematically overview, order and examine DoS weaknesses in 802.11 organizations. As a higher most extreme order, it is normal to bunch weaknesses in light of the organization layer they have a place with; however, a few assaults enter various layers.
2. The creator's order recognizes practical arrangements that are generally.

Figure 1

Explanation of DOS Working



3. simple to carry out and potential arrangements that require further expansions of the norm. The remainder of the paper is coordinated as

follows. In stage 2, the creator momentarily depicts the vital properties of the 802.11 standard that are generally pertinent tasks issues. In stage three, the creator gatherings and talks about DoS weaknesses and countermeasures at the actual layer of 802.11 organizations. In stage four, discussed DoS issues connected with the MAC layer. From that point onward, they talk about a few unexpected issues connected with DoS assaults and countermeasures.

In the article entitled Detecting and Preventing DoS and DDos in MHealth, writers Soumya Ray and Sandip Dutta portray how mHealth (otherwise called Mobile Health) is a vital piece of the medical care industry in this day and age. The total strategy for mhealthcare framework depends on a cloud framework. [2] Because of the administrations gave through the cloud stage, it has been observed that the organization instrumentation is probably going to be helpless against different sorts of assaults inside the framework. This could stop the organization administration right away and forestall admittance to delicate data. The assault can obliterate protection and data security by infusing malevolent information. This investigation paper makes sense of four MHealthcare configuration layers and furthermore makes sense of the particular purposes behind DDoS assaults inside the framework design. An exceptional DDoS identification recipe is anticipated the main location of the assault on the framework. Figure 2 shows a procedure for getting to secret wellbeing data. The entrance solicitation to delicate information can be produced at client level (through versatile, work area or other medical care association) and sent to cloud medical care framework. The full method of getting to secret data Strategies in mHealthcare are defenceless against weak DDoS assaults. This will essentially dial back persistent consideration as well as getting to secret data, documents, records and messages from the completely cloud-based system. The significant commitment of the creator towards this proposition is characterized beneath: [2]

1. The examination article centers around the critical effect of DDoS assaults on the medical care framework. The creators presented the mhealthcare design alongside the potential explanations for this weak assault on the cloud-based IoT framework
2. The creators gave an original DDoS discovery calculation to recognize the framework assault. The various sorts of DDoS assaults and their preventive methodologies are made sense of and broke down. At long

last, the huge impacts of various kinds of DDoS assaults and their protection instruments are capable and examined utilizing a cloud-based programming climate.

[3] Have defined a DDoS prevention scheme for protection in IoT-primarily based totally healthcare systems. The version facilitates to save you DDoS and replay assaults as all of the requests to the sensors are exceeded thru the e-Health Gateway clever device of the fog layer. [4] said that fitness statistics associated with a affected person is the maximum sensitive facts and cannot be disclosed publicly. Secure stop-to-stop conversation among the stop-customers and the m-fitness device is obligatory to include DDoS or every other inclined assaults. Their commentary suggests that the dispensed conversation among the m-health device is supplied through the e Health Gateway that is supported through Datagram Transport Layer Security protocol (DTLS). Here the author listed in table 1 some of the different DoS based attacks tools.

[5] Have proposed profound learning and device learning calculations to work on the security of IoT-based frameworks. Here the author listed in table 2 some of the different network attack in an IoT environment. Calculations are utilized with unique encryption techniques to keep a steady discussion between the individual and the mHealthcare gadget. Scrambled calculations with right ID verification assist with relieving DDoS assaults and assault recognition inside the gadget architecture. [6] They conveyed the particular weak assaults inside the IoT-based mHealthcare device.The objective of the examination is to make more prominent consciousness of the ongoing system update and keep up with methodologies for distinguishing and forestalling DDoS assaults. Classification, honesty and accessibility of information subject insights are the essential issues inside the IoT-based medical care gadget be outfitted with a hearty structure joined with the best security execution. [7] They have said that the gadgets included should be enacted inside the Health Device to confine the attacks. In a completely IoT based gadget, assaults can emerge out of the intra network gadget. In the building model of Figure 3, the creators have characterized the four-layer cell wellbeing structure gadget. The design upholds cooperative and distributive data control alongside 3 significant rules. In the first place, data trade and data recovery can be additionally upgraded for limited data. The immediate and dispersed data handling at each level of the medical care gadget gives low reaction time, and the

responsibility between various hubs can be reduced. [2] Minimum. Run of the mill connection points ought to be intended to effectively supplement client stories during enrolment and gadget access.

Figure 2

Technique to access Health Information

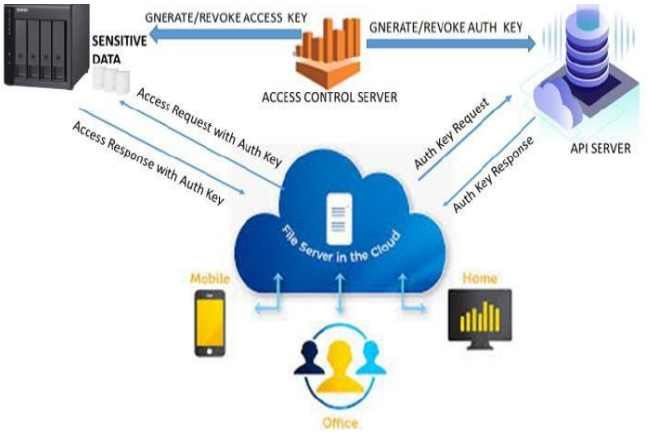


Figure 3

Technique to access Health info

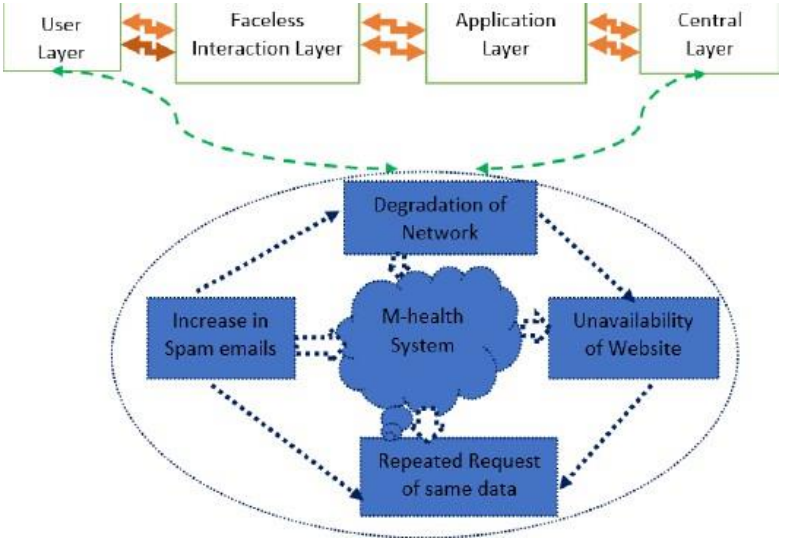


Table 1

Comparison of different Dos attack based tool

Sr.No	Tools	Availability	Language	Performance	App Model
1	Cloud Sim	Open-source	Java	Reliable	Data transfer, computation
2	Breaking Point	Proprietary	C#	Consistent	Data transfer, Execution time
3	HULK	Proprietary	Python	Real-time	DoS
4	DDoSSim	Proprietary	Java	Bulk Value	DoS
5	Golden Eye	Open-source	Pythn	Reliable	DoS
6	Cloud Analyst	Open-source	C++, Python	Reliable	Computation

Table 2

Different network attacks in a cloud environment

Sr.No	Attack type	Target Res	Detect type	Delay min
1	SQL Injection	SQL Server	Spread based	25
2	Port Scan	Server Resource	Signature based	60
3	UDP flood	Network Band	Volume based	120
4	TCP Syn flood	Server Resource	Volume based	2
5	DNS attack	Network Band	Volume based	30

Distributed denial of service is one an incredible premier featured and most critical assaults of the present cyber world. Anyway, extremely strong assault components, it acquaints a colossal danger with current web local area. During this article, Author depicted an extensive review of disseminated refusal of-administration assault, counteraction, and relief tech-niques [8]. Creator gives a logical investigation of dos goes after along with inspirations and development, examination of different goes after up until this point, security strategies and moderation methods, and likely restrictions and difficulties of existing examination [9]. At last, some significant examination bearings are printed that need a ton of

considerations in near future to ensure winning safeguard against disseminated forswearing of-administration assaults.

In this article, Author provides an up-to-date and progressive survey of DDoS attacks, interference techniques and migration techniques. Author present a scientific analysis of DDoS attacks that covers a taxonomy of DDoS attack sorts and their prevention and mitigation techniques. The contributions of this article include the following:

1. Creator gives representation of DDoS assault techniques that cover every one of the stages worried in DDoS assaults.
2. Creator present protection components against DDoS assaults that incorporate fundamental counteraction and relief procedures.
3. Creator incorporate the new assault types in much the same way as late examination on DDoS guard, introducing this cutting edge of DDoS research.
4. Creator moreover enrol a couple of requesting circumstances of the flow exploration. The creator's principal inspiration to go after these clients is to acquire monetary profit. Likewise, political associations and legislatures are additionally ideal objectives of DDoS assaults. Sites or trades can likewise be focuses of DDoS assaults, as displayed in Figure 4. This figure comes from a quarterly report by Kaspersky Research Laboratory and here we find that principally web-based business sites were the top focuses of DDoS assaults in Q2 2015. In this way, the clarifications or inspirations driving the DDoS assaults vary. [8] The creator makes sense of that the fundamental construction of a DDoS assault is displayed in Figure 5. It contains 3 totally various stages and 4 unique parts. [9] The parts are called assailants, different control experts or regulators, various slaves, specialists or zombies, and casualties or target machines.

Figure 3

Attacked cities breakdown

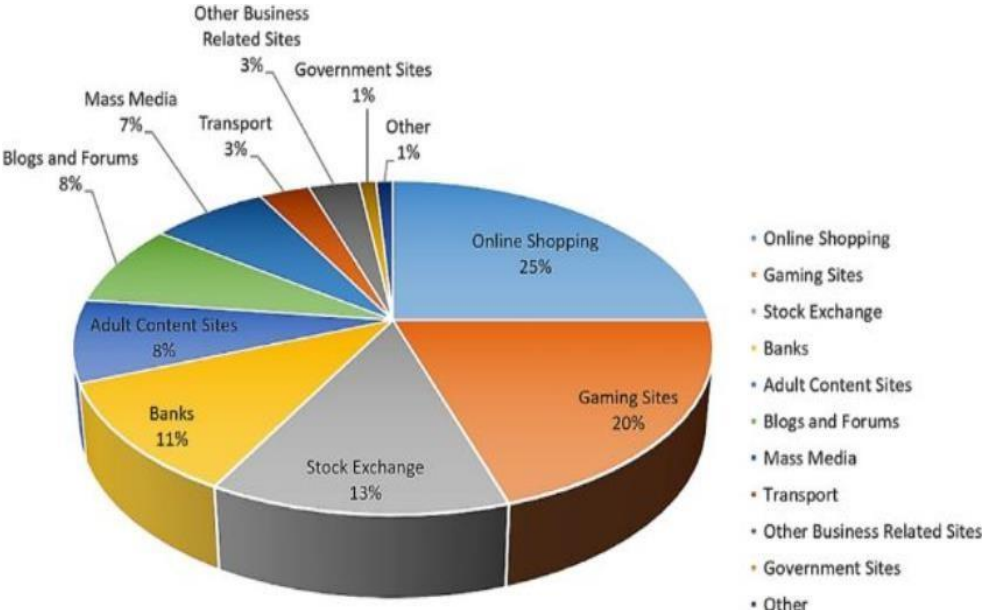


Figure 4

Structure of DDos Attack

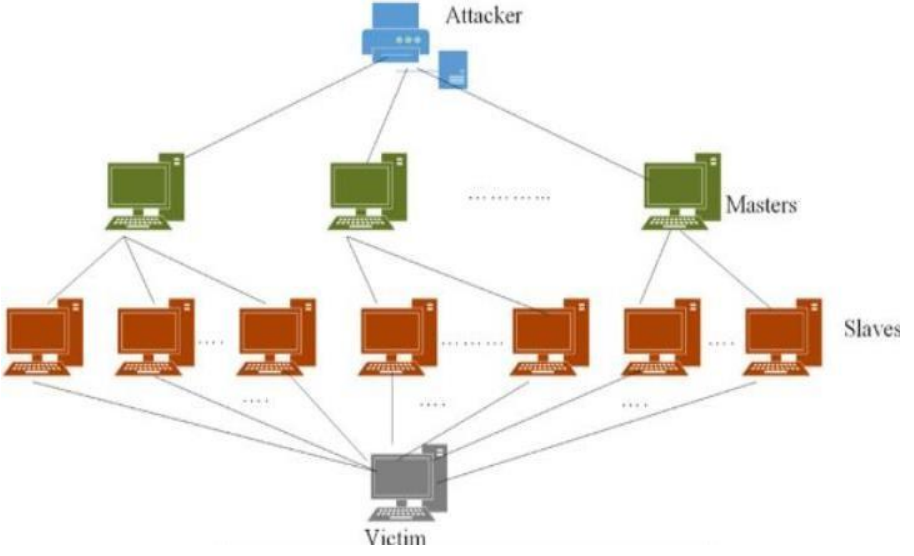
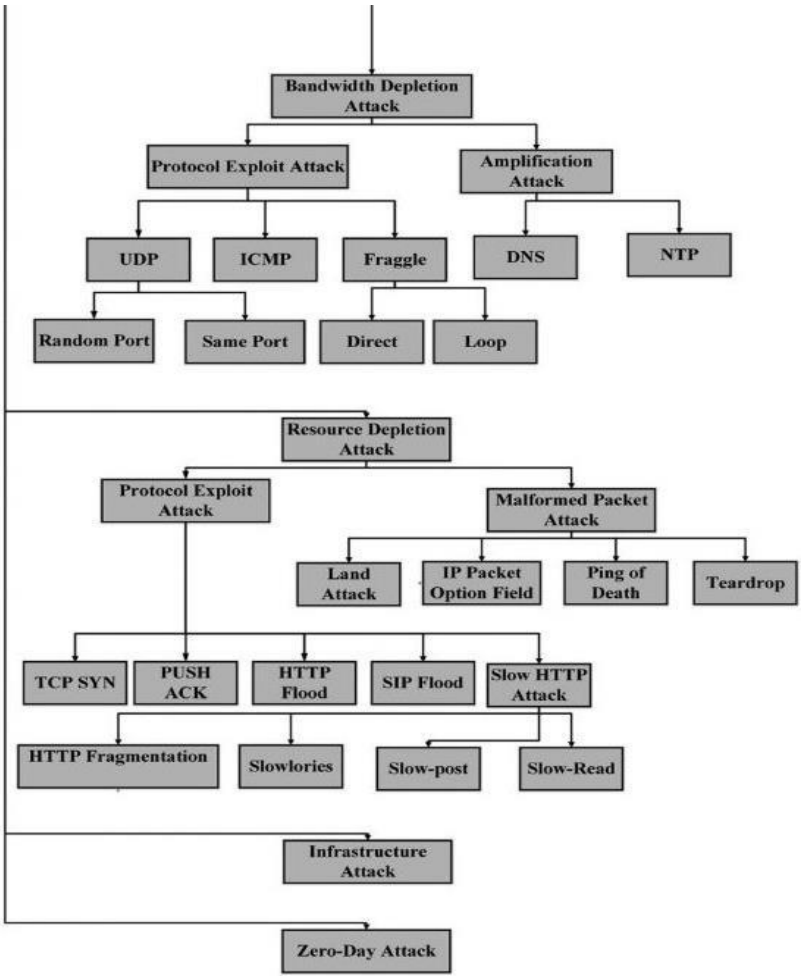


Figure 5

Different types of DDos Attacks



In the assault system stage, the author will probably look at this large number of assault scientific categorizations and present a completely covered and straightforward characterization component. Figure 6 shows our characterization instrument covering all parts of DDoS attacks. [10] This plan relies upon the impact of the attacks on the losses' associations or

resources. Overall, a web server or mediator server is the crucial overcomer of a DDoS attack and supervises confined resources for give its service. Therefore, our DDoS attack portrayal considers these two impacts and gatherings DDoS attacks into two general get-togethers: data exhaustion attacks and resource exhaustion attacks. Really, in any case, an attack can have any of the hits and have the best effects to the whole web. This type is known as an establishment attack. [2]

In this paper named as Early Detection of DoS in VANET usinf APD the creator RoselinMAry and Maheshwari portrays that the security of VANET (Vehicular specially appointed Networks) is urgent as their very presence connects with significant perilous circumstances. VANET could be a subtype of the MANET. During which the portable hubs are vehicles furnished with AN On-Board Unit (OBU) that transform them to send and to get messages to the contrary Nodes inside the organization. [11] Furthermore, to correspondence among the vehicles, VANET connect with correspondence focuses given by on street foundation. A few of the Researchers have previously confirmed in regards to the getting wellbeing messages [12]. What is more VANET face numerous security assaults. In existing VANET frameworks, a discovery calculation is utilized to notice assaults at the hour of examination during which defer over-burden has happened [13]. The different security dangers are hubs that act seriously and give bogus data, Sybil assaults, self-cantered regulator assaults, and so on. During this archive, the creator arranged an Attacked Packet Detection (APDA) decide that will be utilized to forestall DOS (Denial of Service) assaults before check time [14]. This limits the general handling delay and further develops security on VANET. The creator depicts the potential goes:

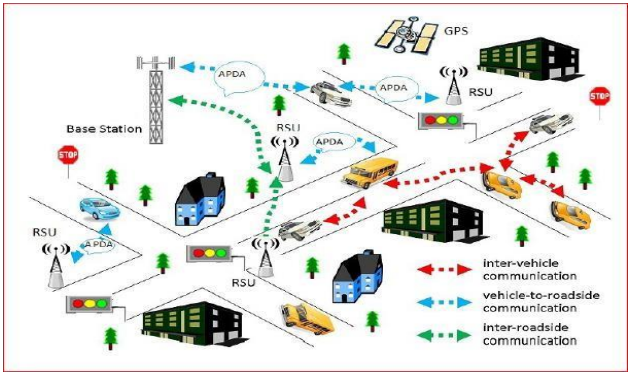
1. **Denial of Service Attacks:** DOS attacks are carried out by network insiders and outsiders [15] and provide a network inaccessible to real users by flooding the control channel with a loud blast of naturally generated messages and disrupting the network's connection [16].
2. **Broadcast Tampering:** A broadcast signal intrusion is the hijacking of broadcast signals, television channels, cable television channels, or satellite signals without authorization or license [17]. Local television and radio stations, as well as national and cable networks, were involved in kidnappings [18].
3. **Sybil Attack**: A Sybil assault [19] utilizes a solitary hub to work numerous dynamic phony personalities (or Sybil characters) all the while inside a shared organization. This kind of assault means to sabotage authority or

power in a genuine framework by acquiring the best impact on the organization [20].

4. **Message Suppression Attack:** Under the concealment assault, the malignant hub can multicast a progression of satire information messages inside a brief timeframe and hence, a higher addition rate is noticed. [21]

The creators present a proposed model for assault recognition utilizing parcel location calculation; Figure 7 shows the framework model of the proposed framework [22]. The system is incorporated with each RSU. Vehicles will send messages to the RSU through the APDA system. Recognizing an unmistakable place of vehicles with messages is planned. Put away inside the given RSU. Every vehicle has OBU gadget and TAMPER PROOF. [23] These gadgets store cautious data about the vehicles [24,25].

Figure 6



Conclusion

In this paper we have analyzed DoS attacked and its general key concepts. Also discussed the importance of DoS attack and different safety measures related to this attack. Like if we talk about the DoS attack best prevention techniques, I would rather say that all the techniques which were discussed above are impressive in their own way but if we want ot give opinion on the best technique then I'll mention the techniques mentioned for the DoS prevention in m-health system and in IEEE802.11. It is just

because in now a day we can see clearly the world is evolving day by day and the tech is improving day by day and all the tech is shifting from manual devices to digital ones. Like in the IEEE802.11 the safety measures like rapid frequency hopping is best in case the jammer station is equipped with transmitter in physical layer and as far as concern for mac layer the best suitable method described is cryptographic puzzle because if the server feels that there is DoS attack then it increased the complexity of the puzzle and then it will be harder to guess.

The attacked packed detection algorithm is used as the prevention in VANET because it can avoid overload time delay. It is also can be the best algorithm used to detect DoS attack as it can be used to send multiple fake requests from vehicle to detect early threats at the same time. The safety measures mentioned in the mobile-health are the basic safety measures but can be profitable as the world is now becoming digital with the passage of time so are the devices and for the digital devices, we need to have the basic security knowledge described in the mobile-health paper.

Acknowledgements

We would like to give my heartiest thanks to my subject teacher sir Usman Inayat who made this work possible for us. His guidance leads us to accomplish every stage of the project on time. Moreover, he supported us in every possible way he can and motivates us all the time.

We would also like to thanks my other colleagues those who stand by us in completing this project and helped us a lot in research work.

References

[1] A. Singh, A. Prasad, and Y. Talwar, “Compact and Secure S-Box Implementations of AES—A Review,” in *Smart Systems and IoT: Innovations in Computing*, vol. 141, A. K. Somani, R. S. Shekhawat, A. Mundra, S. Srivastava, and V. K. Verma, Eds., in Smart Innovation, Systems and Technologies, vol. 141. , Singapore: Springer Singapore, 2020, pp. 857–871. doi: 10.1007/978-981-13-8406-6_80.

[2] S. Ray, K. N. Mishra, and S. Dutta, “Detection and prevention of DDoS attacks on M-healthcare sensitive data: a novel approach,” *Int. J. Inf. Technol.*, vol. 14, no. 3, pp. 1333–1341, May 2022, doi: 10.1007/s41870-022-00869-1.

[3] A. Rajagopalan, M. Jagga, A. Kumari, and S. T. Ali, "A DDoS prevention scheme for session resumption SEA architecture in healthcare IoT," in *2017 3rd international conference on Computational Intelligence & Communication Technology (CICT)*, IEEE, 2017, pp. 1–5. https://ieeexplore.ieee.org/abstract/document/7977361/

[4] S. R. Moosavi *et al.*, "End-to-end security scheme for mobility enabled healthcare Internet of Things," *Future Gener. Comput. Syst.*, vol. 64, pp. 108–124, 2016.

[5] P. Kamble and A. Gawade, "Digitalization of healthcare with IoT and cryptographic encryption against DOS attacks," in *2019 international conference on contemporary computing and informatics (IC3I)*, IEEE, 2019, pp. 69–73. Available: https://ieeexplore.ieee.org/abstract/document/9055531/

[6] J. H. Ziegeldorf, O. G. Morchon, and K. Wehrle, "Privacy in the Internet of Things: threats and challenges," *Secur. Commun. Netw.*, vol. 7, no. 12, pp. 2728–2742, Dec. 2014, doi: 10.1002/sec.795.

[7] A.-M. Rahmani *et al.*, "Smart e-health gateway: Bringing intelligence to internet-of-things based ubiquitous healthcare systems," in *2015 12th annual IEEE consumer communications and networking conference (CCNC)*, IEEE, 2015, pp. 826–834. Available: https://ieeexplore.ieee.org/abstract/document/7158084/

[8] S. T. Zargar, J. Joshi, and D. Tipper, "A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks," *IEEE Commun. Surv. Tutor.*, vol. 15, no. 4, pp. 2046–2069, 2013.

[9] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Comput. Netw.*, vol. 44, no. 5, pp. 643–666, 2004.

[10] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 34, no. 2, pp. 39–53, Apr. 2004, doi: 10.1145/997150.997156.

[11] S. RoselinMary, M. Maheshwari, and M. Thamaraiselvan, "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm (APDA)," in *2013 international conference on information communication and embedded systems (ICICES)*, IEEE, 2013, pp. 237–240. Available: https://ieeexplore.ieee.org/abstract/document/6508250/

[12] S. Zeadally, R. Hunt, Y.-S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETS): status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, Aug. 2012, doi: 10.1007/s11235-010-9400-5.

[13] M. Rahbari and M. A. J. Jamali, "Efficient Detection of Sybil Attack Based on Cryptography in Vanet." arXiv, Dec. 10, 2011. Available: http://arxiv.org/abs/1112.2257

[14] M. Y. Gadkari and N. B. Sambre, "VANET: routing protocols, security issues and simulation tools," *IOSR J. Comput. Eng.*, vol. 3, no. 3, pp. 28–38, 2012.

[15] M. Mittal, K. Kumar, and S. Behal, "DDoS-AT-2022: a distributed denial of service attack dataset for evaluating DDoS defense system," *Proc. Indian Natl. Sci. Acad.*, vol. 89, no. 2, pp. 306–324, Jun. 2023, doi: 10.1007/s43538-023-00159-9.

[16] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "DDoS attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges," *J. Sens. Actuator Netw.*, vol. 12, no. 4, p. 51, 2023.

[17] R. Balamurugan, B. A. Princy, D. Kanchana, M. Murugesan, A. J. Selsia, and M. Dinesh, "Implementation of an Effective Methodology to Avoid DDoS Attacks using Cybersecurity Norms," in *2024 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE)*, IEEE, 2024, pp. 1–6. Available: https://ieeexplore.ieee.org/abstract/document/10467703/

[18] F. J. Abdullayeva, "Distributed denial of service attack detection in E-government cloud via data clustering," *Array*, vol. 15, p. 100229, Sep. 2022, doi: 10.1016/j.array.2022.100229.

[19] P. Kumari and A. K. Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," *Comput. Secur.*, vol. 127, p. 103096, 2023.

[20] T. Rajendran, E. Abishekraj, and U. Dhanush, "Improved intrusion detection system that uses machine learning techniques to proactively defend ddos attack," in *ITM Web of Conferences*, EDP Sciences, 2023, p. 05011. Available: https://www.itm-conferences.org/articles/itmconf/abs/2023/06/itmconf_icdsac2023_05011/itmconf_icdsac2023_05011.html

[21] S. Muzafar, N. Z. Jhanjhi, N. A. Khan, and F. Ashfaq, "Ddos attack detection approaches in on software defined network," in *2022 14th International conference on mathematics, actuarial science, computer science and statistics (MACS)*, IEEE, 2022, pp. 1–5. Available: https://ieeexplore.ieee.org/abstract/document/10022653/

[22] M. A. Setitra, M. Fan, I. Benkhaddra, and Z. E. A. Bensalem, "DoS/DDoS attacks in Software Defined Networks: Current situation, challenges and future directions," *Comput. Commun.*, 2024. Available: https://www.sciencedirect.com/science/article/pii/S0140366424001622

[23] G. S. Rao and P. K. Subbarao, "A Novel Framework for Detection of DoS/DDoS Attack Using Deep Learning Techniques, and An Approach to Mitigate the Impact of DoS/DDoS attack in Network Environment," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 1, pp. 450–466, 2024.

[24] S. Ahmed *et al.*, "Effective and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron," *Future Internet*, vol. 15, no. 2, p. 76, 2023.

[25] G. Nayak, A. Mishra, U. Samal, and B. K. Mishra, "Depth Analysis On DoS & DDoS Attacks," in *Wireless Communication Security*, 1st ed., M. Khari, M. Bharti, and M. Niranjanamurthy, Eds., Wiley, 2022, pp. 159–182. doi: 10.1002/9781119777465.ch9.