Distributed Denial of Service (DDoS)

Subjects: Others
Contributor: Sharyar Wani

Distributed Denial of Service (DDoS) attack is a major threat impeding service to legitimate requests on any network. Although the first DDoS attack was reported in 1996, the complexity and sophistication of these attacks has been ever increasing. A 2 TBps attack was reported in mid-August 2020 directed towards critical infrastructure, such as finance, amidst the COVID-19 pandemic. It is estimated that these attacks will double, reaching over 15 million, in the next 2 years. A number of mitigation schemes have been designed and developed since its inception but the increasing complexity demands advanced solutions based on emerging technologies. Blockchain has emerged as a promising and viable technology for DDoS mitigation. The inherent and fundamental characteristics of blockchain such as decentralization, internal and external trustless attitude, immutability, integrity, anonymity and verifiability have proven to be strong candidates, in tackling this deadly cyber threat. This survey discusses different approaches for DDoS mitigation using blockchain in varied domains to date. The paper aims at providing a comprehensive review, highlighting all necessary details, strengths, challenges and limitations of different approaches. It is intended to serve as a single platform to understand the mechanics of current approaches to enhance research and development in the DDoS mitigation domain.

distributed denial of service (DDoS) | DDoS attack | DDoS mitigation | DDoS defense | blockchain

1. Introduction

A distributed denial of service (DDoS) attack is a special type of denial of service attack that overwhelms the target or the related infrastructure with malicious traffic. This is achieved using bots, a network of malware compromised computers and other devices, under the remote control of an attacker (refer to illustration in Figure 1)[1]. It severely hampers the bandwidth and connectivity leading to disruption of all services on the network[2]. Cloud ecosystems suffer maximum loses due to complete service denial and service degradation[3].The primary target of DDoS attack is availability of resources for genuine users. The malicious flooding overloads the network, exceeding its bandwidth capabilities and disrupting the services[4]. The target range varies from financial institutions, health care providers and government agencies to low key public networks[2].

It is difficult to distinguish the attack traffic in a DDoS attack because of its similarity to the legitimate traffic[5]. They behave very closely to normal network packets, albeit in higher quantities and concentration towards the victim[6]. This is more prevalent during the early stages of attack, especially in low-rate and low-traffic attacks[5]. The attack is usually measured in volumetric parameters such as packets-per-second, bits-per-second and connections-per-second[6]. A malicious attack from a small number of nodes is easier to detect and mitigate. DDoS uses a significantly large number of nodes, and the collective behavior drastically severs any chance of serving non-malicious requests[7]. The compromised devices transfer a large volume of packets without any breaks over the network, tricking the victim into recognizing them as legitimate traffic. As a result, not only does the host communicate with different devices but with different types of packets as well [8]. DDoS attack has been proven as a resource battleground between the defenders and attackers; the more the resources, the higher the chance of success[9].

DDoS attacks can be classified as brute-force attacks, spoofing attacks and flooding attacks. Flooding attacks are the most common and severe among the three, thwarting the network bandwidth and blocking all legitimate requests. Survival approaches are focused on single target victims and require victims to detect and manage the attack themselves. However, a network wide flood requires mitigation approaches before it reaches the victims, making it suitable for multi-targeted attack. DDoS cannot be blocked or prevented altogether by installing software patches and deploying appliances. Therefore, Internet

service providers either use scrubbing services or over provision their networks. Both the methods are financially not feasible[10].

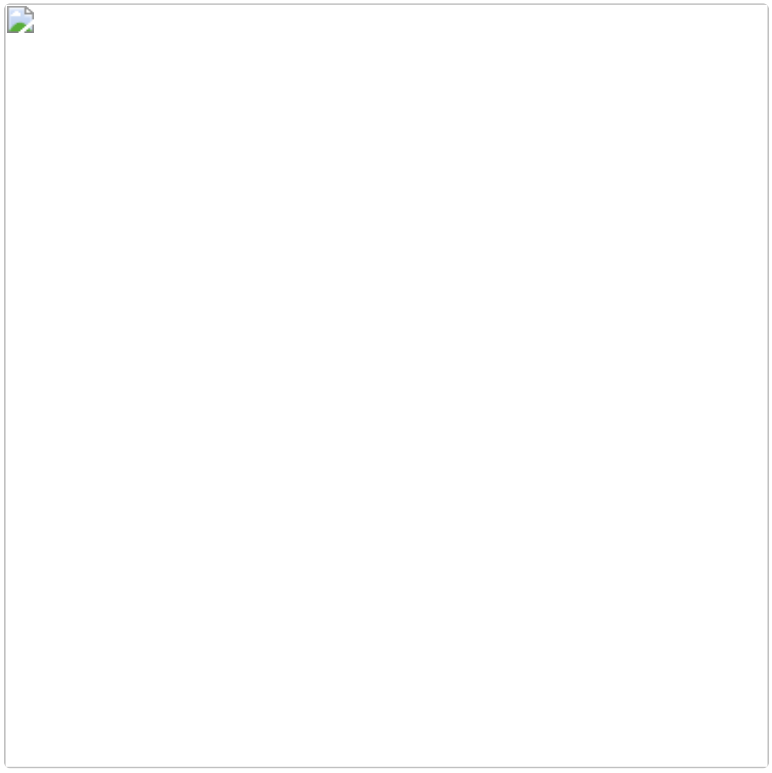

Figure 1. Distributed denial of service (DDoS) attack[6].

The DDoS architecture consists mainly of zombies based on handlers' models and Internet relay-chat. All communications between the handler and the attack are usually encrypted, making the attack invisible from detection. Attackers spoof MAC and IP addresses and are geographically well distributed, making detection a tedious effort.

DDoS attacks have rapidly evolved over time and have become very sophisticated. DDoS attacks severely affect an organization's computing, financial and infrastructural resources[11]. The number of DDoS attacks has increased exponentially over the years, not even sparing major cloud service providers such as Microsoft and Amazon EC2[5]. Around 79 countries were affected by DDoS attacks during the first quarter of 2018. The longest attack duration was about 297 h[12]. A 1.3 TBps attack was reported affecting GitHub. A 1.7 TBps attack was reported later following the attack on GitHub[13]. Some established banks were severely affected by a peak 160 Gbps and 32 million packets per second DDoS attack in April 2019[14]. Monetary losses of about $491 billion were reported in 2014 alone[11]. Amidst the COVID-19 pandemic (mid-August 2020), a world-wide DDoS extortion attack amounting to 2TBps, targeting finance and the travel industry, was reported by NetScout[15]. It is predicted that DDoS attacks will double from 7.9 million in 2018 to 15.4 million by 2023[16]. These numbers, attack traffic and timings clearly indicate the threat severity of DDoS attacks[14].

Different methods and technologies have been employed in previous years to tackle this severe resource drainer attack, such as machine learning[17][18][19], deep learning[20][21], reinforcement learning[22], SDN[23][24][25][26][27], protocol tuning[28][29], network traffic classifiers[30][31], network function virtualization[32][33][34], fog computing[35] and reputation scoring, among others. In addition to struggling with scalability, high computation and communication overhead, the aforementioned methods do not perform effectively in real world DDoS attacks. They not only suffer because of increased volume of botnet and amount of traffic involved[13][15] but also due to the ever-increasing sophistication and complexities of DDoS attacks[11].

2. Theoretical Background

2.1. DDoS Attack Types

DDoS attacks are aimed at denying service access to legitimate users targeting availability of network resources. The attack procedure relies heavily upon distributed access to devices exploiting known vulnerabilities[36]. Attacks are targeted at various layers of the network infrastructure, e.g., application layer, transport layer, etc.[37][38]. Based on the network architecture, DDoS attacks are classified as follows[39]:

1. Application layer attacks: This is a layer seven network architecture attack aimed at target resource exhaustion leading to denial of service[38]. The attacker leverages application or system vulnerabilities, causing network instability. These attacks are often mistaken as implementation errors because of the low rate traffic required to execute them successfully. Examples include HTTP flood, Slowloris and Zero-day attack. An HTTP flood is an attack whereby continuous access is requested from multiple devices, exhausting the capabilities of the targeted device. A typical setup for an HTTP flood is presented in Figure 2. Slowloris sends incomplete requests at predefined intervals, aiming at keeping the request channels engaged for an extended period of time, preventing legitimate access to the target devices[37][38][39][40][41].

2. Resource exhaustion attack: Network layer and transport layer vulnerabilities are exploited by this DDoS attack. These are also referred as state exhaustion attacks depleting computing resources such as computational power and primary and secondary memories. Since this attack exploits protocol vulnerabilities in addition to being voluminous, it forms a hybrid between specific messages and volume being sent to the victim. TCP SYN floods send SYN messages to the victim but provide no confirmation to the victim for establishment of a connection with spoofed source IP addresses. In this manner, the target resources are exhausted over time, since it responds to each hand shake but never receives any confirmation from the attacker[37][41]. Other examples include Ping of Death, which are ping packets greater than 65,535 bytes, making the victim inaccessible, and Smurf attack, which destabilizes the victim services by sending a large volume of ICMP packets[41]. As seen in Figure 3, the attacker creates a network packet attached to a false IP address (spoofing), transmitting an ICMP ping message. The network nodes are required to reply. The replies follow an infinite loop by being sent back to the network IPs.

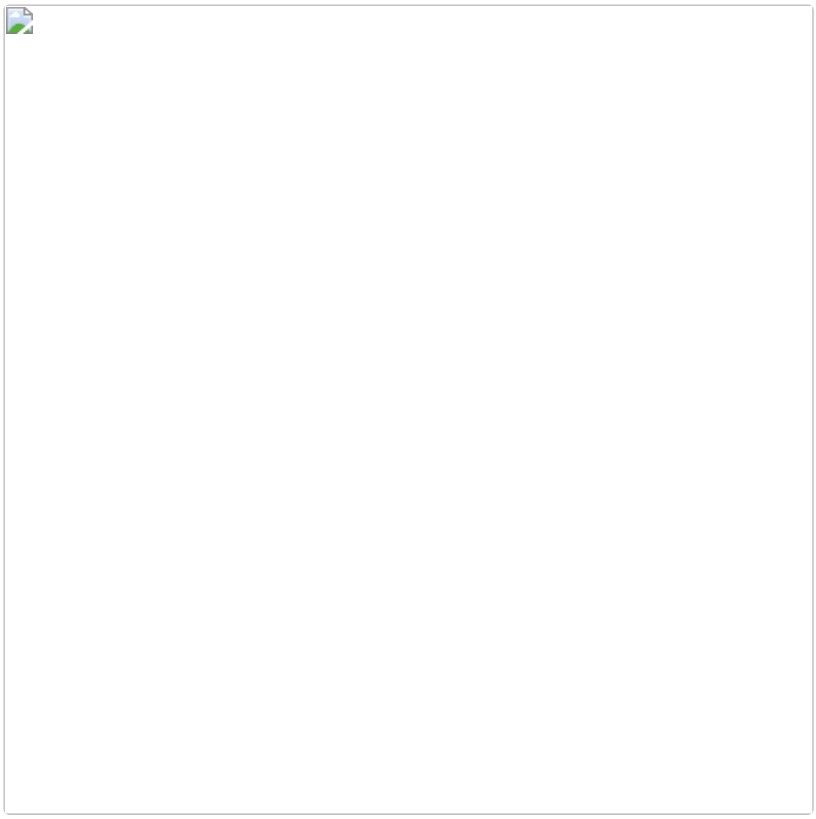

Figure 2. Application layer DDoS attack example[42].

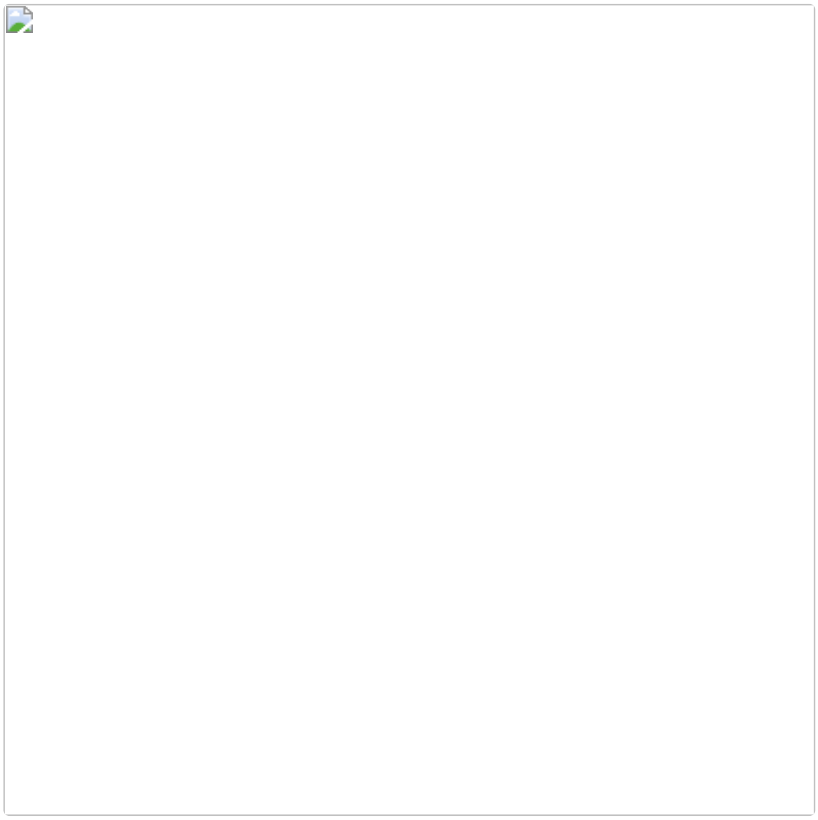

Figure 3. Smurf Attack—resource exhaustion attack example[43].

3. Volumetric attacks: Massive amounts of data are sent to the victim using botnets or other amplification methods, exhausting the bandwidth between the target and larger network/internet. UDP protocol is commonly used to exploit any excessive increase in packet size. DNS amplification attacks perform service requests to change the source address field with the victim's address, causing response amplification by the servers and exhausting the victim bandwidth, as demonstrated in Figure 4[37][40][41]. Similarly, ICMP floods send abnormal packets to target servers, making them inaccessible to legitimate requests[39][40][41].

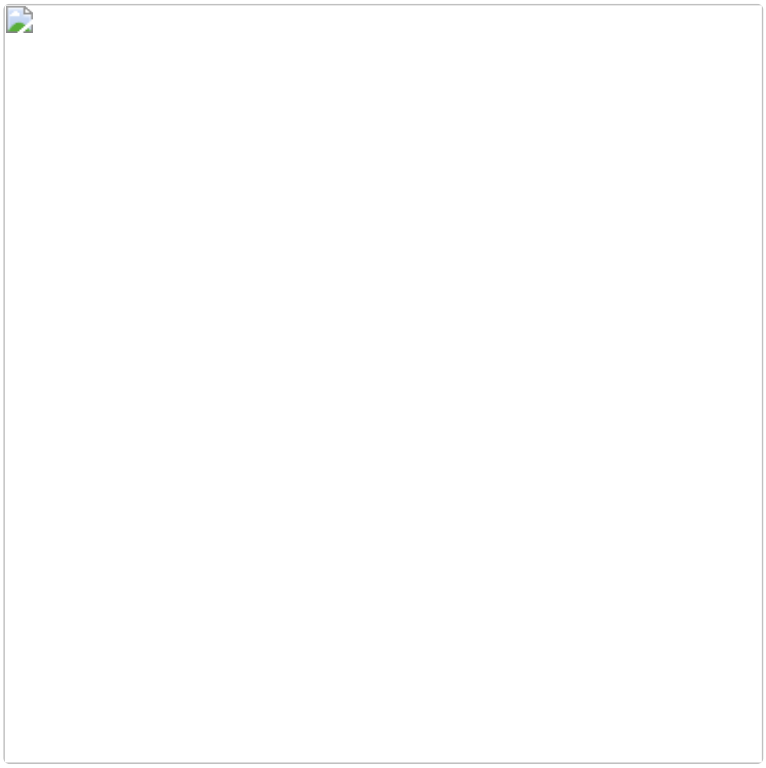

Figure 4. UDP Storm—volumetric attack example[43].

2.2. Blockchain

Blockchain aims at cryptographically secured list of records on globally available computing devices. These records are publicly certifiable, immutable and sequentially generated known as blocks. It is a distributed record keeping the ledger accessible to numerous nodes for record keeping. It is an interconnected chain of nodes starting with the genesis block with every next block, storing information about the previous node (see Figure 5). The nodes in this network possess the capability of accepting or rejecting data transactions by constantly observing the data blocks. Each record in these blocks is timestamped and added upon verification throughout the chain. Cryptographic hash functions map a random size input message to a fixed size output message given by $\{0,1\}^* - \{0,1\}^n$[44]. While it might not replace the traditional information sharing mechanisms completely, it represents a new paradigm in secure verifiable and immutable information sharing.

The blockchain is based on the following significant building blocks: database, block, hash, miner, transaction and consensus mechanism[45].

1. Database**:** This aspect covers blockchains' fundamental capability or buildup of storing the information in a non-traditional method and structure (rows and columns). It stores all transaction records of the participating users with high throughput, no central control and immutable records, among others.
2. Blocks: Blocks store data associated with different transactions among the participating users. They are chained together storing hash values of previous blocks, forming a loop of tightly interconnected data. Typically divided into two, the header contains information about the block in the chain, while the latter part is associated with storing the actual transactional data[45][46].
3. Hash: These are complex mathematical problems responsible for identification and verification. Miners must solve these problems in order to trace a block, while the hash function for two messages cannot be the same, allowing verification. A hash table is maintained for efficient indexing while the next blocks store hashes of previous blocks in the chain [45][47][48].
4. Miner: A network node that solves a computational problem locating a new block is referred as a block miner. New transactions are broadcasted across the chain, and participants efforts are rewarded based on proof-of-work. The

generated block is accepted into the chain when the miners start working on the next block, so that the previous hash is stored, ensuring continuity of the chain[45][47].

5. Transaction: This is the smallest amount of task information stored in a block once verified by majority participants in the chain. The records are accessible throughout while being immutable[45][48]. Figure 5 is a detailed infographic about transaction execution flow inside a blockchain.

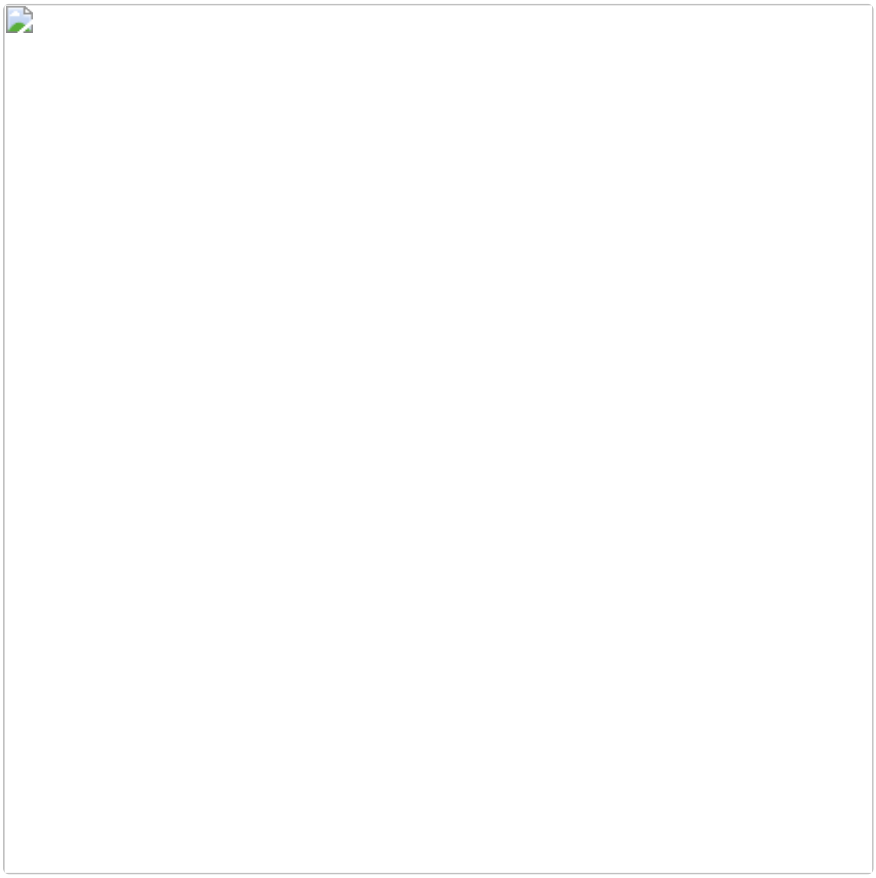

Figure 5. Transaction execution flow in a blockchain[49].

6. Consensus: Consensus over records is a key characteristic in blockchain achieved via various consensus mechanism. The famous ones are Proof of Work (PoW) and Proof of Stake (PoS); the former ones reward based on proof of the work for block generation while the latter distributes work based on a participant's virtual currency tokens [45][46].

References

1. Agrawal, N.; Tapaswi, S. Defense Mechanisms against DDoS Attacks in a Cloud Computing Environment: State-of-the-Art and Research Challenges. IEEE Commun. Surv. Tutorials 2019, 21, 3769–3795.
2. Banitalebi Dehkordi, A.; Soltanaghaei, M.R.; Boroujeni, F.Z. The DDoS attacks detection through machine learning and statistical methods in SDN. J. Supercomput. 2020, 1–33.
3. Fazeldehkordi, E.; Owe, O.; Ramezanifarkhani, T. A Language-Based Approach to Prevent DDoS Attacks in Distributed Financial Agent Systems. In Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics); Springer: Berlin/Heidelberg, Germany, 2020; Volume 11981, pp. 258–277.
4. Singh, K.; Dhindsa, K.S.; Nehra, D. T-CAD: A threshold based collaborative DDoS attack detection in multiple autonomous systems. J. Inf. Secur. Appl. 2020, 51, 102457.

5. Cheng, J.; Li, J.; Tang, X.; Sheng, V.S.; Zhang, C.; Li, M. A novel DDoS attack detection method using optimized generalized multiple kernel learning. Comput. Mater. Contin. 2020, 62, 1423–1443.
6. Mirchev, M.J.; Mirtchev, S.T. System for DDoS attack mitigation by discovering the attack vectors through statistical traffic analysis. Int. J. Inf. Comput. Secur. 2020, 13, 309–321.
7. Lotfalizadeh, H.; Kim, D.S. Investigating Real-Time Entropy Features of DDoS Attack Based on Categorized Partial-Flows. In Proceedings of the 2020 14th International Conference on Ubiquitous Information Management and Communication (IMCOM), Taichung, Taiwan, 3–5 January 2020.
8. Abubakar, R.; Aldegheishem, A.; Faran Majeed, M.; Mehmood, A.; Maryam, H.; Ali Alrajeh, N.; Maple, C.; Jawad, M. An Effective Mechanism to Mitigate Real-Time DDoS Attack. IEEE Access 2020, 8, 126215–126227.
9. Yuan, B.; Zhao, H.; Lin, C.; Zou, D.; Yang, L.T.; Jin, H.; He, L.; Yu, S. Minimizing Financial Cost of DDoS Attack Defense in Clouds with Fine-Grained Resource Management. IEEE Trans. Netw. Sci. Eng. 2020.
10. Khooi, X.Z.; Csikor, L.; Divakaran, D.M.; Kang, M.S. DIDA: Distributed in-Network Defense Architecture against Amplified Reflection DDoS Attacks. In Proceedings of the 2020 IEEE Conference on Network Softwarization: Bridging the Gap Between AI and Network Softwarization (NetSoft), Ghent, Belgium, 29 June–3 July 2020; pp. 277–281.
11. Wang, A.; Chang, W.; Chen, S.; Mohaisen, A. A Data-Driven Study of DDoS Attacks and Their Dynamics. IEEE Trans. Dependable Secur. Comput. 2020, 17, 648–661.
12. Saxena, U.; Sodhi, J.S.; Singh, Y. An Analysis of DDoS Attacks in a Smart Home Networks. In Proceedings of the Confluence 2020—10th International Conference on Cloud Computing, Data Science and Engineering, Noida, India, 29–31 January 2020; pp. 272–276.
13. Kotey, S.; Tchao, E.; Gadze, J. On Distributed Denial of Service Current Defense Schemes. Technologies 2019, 7, 19.
14. Choi, S.; An, Y.; Sasase, I. A Lightweight Detection Using Bloom Filter against Flooding DDoS Attack. IEICE Trans. Inf. Syst. 2020, 103, 2600–2610.
15. NETSCOUT. High-Profile DDoS Extortion Attacks—September 2020. Available online: https://www.netscout.com/blog/asert/high-profile-ddos-extortion-attacks-september-2020 (accessed on 14 January 2021).
16. Cisco Annual Internet Report—Cisco Annual Internet Report (2018–2023) White Paper—Cisco. Available online: https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html (accessed on 18 January 2021).
17. Ko, I.; Chambers, D.; Barrett, E. Unsupervised learning with hierarchical feature selection for DDoS mitigation within the ISP domain. ETRI J. 2019, 41, 574–584.
18. Mohammed, S.S.; Hussain, R.; Senko, O.; Bimaganbetov, B.; Lee, J.Y.; Hussain, F.; Kerrache, C.A.; Barka, E.; Alam Bhuiyan, M.Z. A New Machine Learning-based Collaborative DDoS Mitigation Mechanism in Software-Defined Network. In Proceedings of the International Conference on Wireless and Mobile Computing, Networking and Communications, Limassol, Cyprus, 15–17 October 2018.
19. Ko, I.; Chambers, D.; Barrett, E. Adaptable feature-selecting and threshold-moving complete autoencoder for DDoS flood attack mitigation. J. Inf. Secur. Appl. 2020, 55.
20. Essaid, M.; Kim, D.Y.; Maeng, S.H.; Park, S.; Ju, H.T. A Collaborative DDoS Mitigation Solution Based on Ethereum Smart Contract and RNN-LSTM. In Proceedings of the 2019 20th Asia-Pacific Network

Operations and Management Symposium: Management in a Cyber-Physical World (APNOMS 2019), Matsue, Japan, 18–20 September 2019.

21. Ko, I.; Chambers, D.; Barrett, E. Feature Dynamic Deep Learning Approach for DDoS Mitigation within the ISP Domain. In Proceedings of the International Journal of Information Securitym; Springer: Berlin/Heidelberg, Germany, 2020; Volume 19, pp. 53–70.
22. Simpson, K.A.; Rogers, S.; Pezaros, D.P. Per-Host DDoS Mitigation by Direct-Control Reinforcement Learning. IEEE Trans. Netw. Serv. Manag. 2020, 17, 103–117.
23. Hugues-Salas, E.; Ntavou, F.; Ou, Y.; Kennard, J.E.; White, C.; Gkounis, D.; Nikolovgenis, K.; Kanellos, G.; Erven, C.; Lord, A.; et al. Experimental demonstration of DDoS mitigation over a Quantum key distribution (QKD) network using Software Defined Networking (SDN). In Proceedings of the 2018 Optical Fiber Communications Conference and Exposition (OFC), San Diego, CA, USA, 11–15 March 2018; Available online: https://ieeexplore.ieee.org/document/8385709 (accessed on 28 January 2021).
24. Harikrishna, P.; Amuthan, A. SDN-based DDoS Attack Mitigation Scheme using Convolution Recursively Enhanced Self Organizing Maps. Sadhana Acad. Proc. Eng. Sci. 2020, 45.
25. Huong, T.T.; Thanh, N.H. Software defined networking-based One-packet DDoS mitigation architecture. In Proceedings of the 11th International Con-ference on Ubiquitous Information Management and Communication (IMCOM 2017), Beppu, Japan, 5–7 January 2017; Available online: https://dl.acm.org/doi/abs/10.1145/3022227.3022336 (accessed on 28 January 2021).
26. Hameed, S.; Khan, H.A. Leveraging SDN for Collaborative DDoS Mitigation. In Proceedings of the 2017 International Conference on Networked Systems (NetSys 2017), Gottingen, Germany, 13–16 March 2017.
27. Hameed, S.; Khan, H.A. SDN based collaborative scheme for mitigation of DDoS attacks. Futur. Internet 2018, 10, 23.
28. Somani, G.; Gaur, M.S.; Sanghi, D.; Conti, M.; Buyya, R. Service resizing for quick DDoS mitigation in cloud computing environment. Ann. Telecommun. Telecommun. 2017, 72, 237–252.
29. Kuka, M.; Vojanec, K.; Kucera, J.; Benacek, P. Accelerated DDoS Attacks Mitigation Using Programmable Data Plane. In Proceedings of the 2019 ACM/IEEE Symposium on Architectures for Networking and Communications Systems (ANCS 2019), Cambridge, UK, 24–25 September 2019.
30. Ko, I.; Chambers, D.; Barrett, E. Self-supervised network traffic management for DDoS mitigation within the ISP domain. Futur. Gener. Comput. Syst. 2020, 112, 524–533.
31. Ko, I.; Chambers, D.; Barrett, E. A Lightweight DDoS Attack Mitigation System within the ISP Domain Utilising Self-Organizing Map. In Proceedings of the Advances in Intelligent Systems and Computing; Springer: Berlin/Heidelberg, Germany, 2019; Volume 881, pp. 173–188.
32. Bulbul, N.S.; Fischer, M. SDN/NFV-Based DDoS Mitigation via Pushback. In Proceedings of the IEEE International Conference on Communications, Dublin, Ireland, 7–11 June 2020.
33. Beigi-Mohammadi, N.; Barna, C.; Shtern, M.; Khazaei, H.; Litoiu, M. CAAMP: Completely Automated DDoS Attack Mitigation Platform in Hybrid Clouds. In Proceedings of the 2016 12th International Conference on Network and Service Management (CNSM), Montreal, QC, Canada, 31 October–4 November 2016; pp. 136–143.
34. Fulber Garcia, V.; De Freitas Gaiardo, G.; Da Cruz Marcuzzo, L.; Ceretta Nunes, R.; Paula Dos Santos, C.R. DeMONS: A DDoS Mitigation NFV Solution. In Proceedings of the Proceedings—International Conference on Advanced Information Networking and Applications (AINA), Krakow, Poland, 16–18 May 2018; pp. 769–776.

35. Zhou, L.; Guo, H.; Deng, G. A fog computing based approach to DDoS mitigation in IIoT systems. Comput. Secur. 2019, 85, 51–62.
36. Lohachab, A.; Karambir, B. Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks. J. Commun. Inf. Netw. 2018, 3, 57–78.
37. Dantas Silva, F.S.; Silva, E.; Neto, E.P.; Lemos, M.; Venancio Neto, A.J.; Esposito, F. A Taxonomy of DDoS Attack Mitigation Approaches Featured by SDN Technologies in IoT Scenarios. Sensors 2020, 20, 3078.
38. Srinivasan, K.; Mubarakali, A.; Alqahtani, A.S.; Dinesh Kumar, A. A Survey on the Impact of DDoS Attacks in Cloud Computing: Prevention, Detection and Mitigation Techniques. In Lecture Notes on Data Engineering and Communications Technologies; Springer: Berlin/Heidelberg, Germany, 2020; Volume 33, pp. 252–270.
39. Adhikary, K.; Bhushan, S.; Kumar, S.; Dutta, K. Hybrid Algorithm to Detect DDoS Attacks in VANETs. Wirel. Pers. Commun. 2020, 114, 3613–3634.
40. Vishwakarma, R.; Jain, A.K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommun. Syst. 2020, 73, 3–25.
41. Azahari Mohd Yusof, M.; Hani Mohd Ali, F.; Yusof Darus, M. Detection and Defense Algorithms of Different Types of DDoS Attacks. Int. J. Eng. Technol. 2018, 9, 410–444.
42. Singh, K.; Singh, P.; Kumar, K. Application layer HTTP-GET flood DDoS attacks: Research landscape and challenges. Comput. Secur. 2017, 65, 344–372.
43. Gupta, B.B.; Badve, O.P. Taxonomy of DoS and DDoS attacks and desirable defense mechanism in a Cloud computing environment. Neural Comput. Appl. 2017, 28, 3655–3682.
44. Alkadi, O.; Moustafa, N.; Turnbull, B. A Review of Intrusion Detection and Blockchain Applications in the Cloud: Approaches, Challenges and Solutions. IEEE Access 2020, 8, 104893–104917.
45. Atlam, H.F.; Wills, G.B. Technical aspects of blockchain and IoT. In Advances in Computers; Academic Press: Amsterdam, The Netherlands, 2019; Volume 115, pp. 1–39. ISBN 9780128171899.
46. Khan, M.A.; Salah, K. IoT security: Review, blockchain solutions, and open challenges. Futur. Gener. Comput. Syst. 2018, 82, 395–411.
47. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction—Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder—Google Books. Available online: https://books.google.com.my/books?hl=en&lr=&id=LchFDAAAQBAJ&oi=fnd&pg=PP1&dq=Bitcoin+and+Cryptocurrency+Technologies&ots=AslEeY0InJ&sig=RO4XsMte7sftyGMYmbzU&redir_esc=y#v=onepage&q=BitcoinandCryptocurrencyTechnologies&f=false (accessed on 15 January 2021).
48. Peters, G.W.; Panayi, E. Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money. New Econ. Wind. 2016, 239–278.
49. Ismail, L.; Materwala, H. A Review of Blockchain Architecture and Consensus Protocols: Use Cases, Challenges, and Solutions. Symmetry 2019, 11, 1198.

Retrieved from https://encyclopedia.pub/entry/history/show/16773