Defensive Approach using Blockchain Technology against Distributed Denial of Service attacks

Anupama Mishra[1], B.B.Gupta[2], Dragan Peraković[3] and Zhili Zhou[4]

[1]Swami Rama Himalayan University, India

[2]National Institute of Technology, Kurukshetra, Haryana 136119, India & Asia University, Taichung 413, Taiwan & Staffordshire University, Stoke-on-Trent ST4 2DE, UK

[3]University of Zagreb, Croatia

[4]Nanjing university of information science and technology, NUIST, China

Abstract

To maintain our network's security and fight cybercrime, we must stay up to date with the latest technological initiatives. Nowadays, DDoS (Distributed Denial of Service) attacks include monetization and other risks and improvements in BGP (basic global protocol) routing have helped to combat these attacks. It is essential that we take all possible measures to maintain a safe space for online activities.The purpose of this work is to develop a botnet prevention system that leverages the advantages of Software Defined Networking (SDN) along with the Blockchain. Here, we develop a mechanism to detect and mitigate botnets using blockchain and SDN. The results and performance shows that the proposed approach works efficiently.

Keywords

Blockchain, Software Defined Network, Distributed Denial of Service Attack

1. Introduction

Botnets are malicious software-infected computer networks that are controlled as a group. They constitute a serious network danger [1, 2]. Botnets are active on more than 16-25 percent of internet-enabled devices, according to studies [21, 22]. Spam Messages, distributed denial of service attacks, unauthorized access, snooping, spoofing and other similar assaults are all possible on these networks [23, 24]. In the case of distributed denial of service attack, businesses and network resources can have severe results. Therefore, there are two basic approaches to DDoS prevention [30]. First and foremost, to protect your network from these types of attacks. Second, avoid turning your network resources into botforces or botnets that conduct attacks on other, mostly unnoticed, businesses. The growing number of devices throughout the world poses numerous issues in terms of connectivity, security, and management, not to mention the possibility of these devices being part of a notorious botnet force. An attacker's most essential weapon in botnet formation is a large number of devices. As a result, connected devices, smart transportation systems, smart health, energy, and IoT enabled vehicles represent the biggest potential for botnets. Some measures are proposed for preventing our device from

International Conference on Smart Systems and Advanced Computing (Syscom-2021), December 25–26, 2021

tiwari.anupama@gmail.com (A. Mishra); gupta.brij@gmail.com (B.B.Gupta); dperakovic@fpz.unizg.hr (D. Peraković); zhou1_zhili@163.com (Z. Zhou)

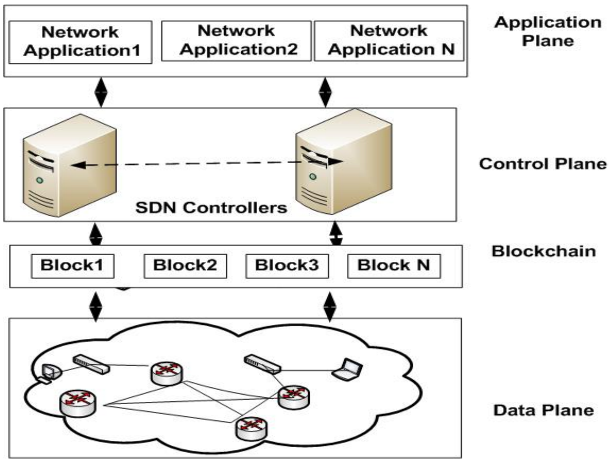

Figure 1: Architecture of SDN

becoming a DDoS attack launcher[31]. Approve and authenticated Devices that satisfy basic security standards, enforcing policies and the resources with which they communicate and also permitted devices that satisfy minimum requirements for security. As per authors in [25], advanced features of blockchain is used to address this requirement in architecture. The next criterion is to include scheduled scanning and remediation, which is a time-consuming activity that adds overhead. With this in mind, we have presented a technique for networks that takes advantage of SDN's programmability and management capabilities, as well as the blockchain's data security capabilities. The blockchain is essentially a distributed ledger which is constantly updated throughout the world wide networks. It may download flow rules from the SDN controller blockchain network (figure 1) and look for modifications, unusual behaviour, or traffic bound for a certain destination (innocent network), as well as detect DDoS botnets in the works. It is capable of detecting DDoS botnets as well as traffic directed at specific targets. It can detect changes to the system data plan, any changes to topological features, and the state of flow mode communication to identify malicious updates. The fundamental contribution of this research is summarised as follows: We have created a new blockchain based system that alerts the administrator if their network has been infected with botnet malware. This allows for quick botnet removal before the attack can cause any significant harm to your business/organization. The security elements of our work have been deployed, examined, and studied from numerous perspectives. The remainder of the paper is organised as follows. In section II, related work, and in section III, the core recommended architecture for botnet avoidance, Section IV is dedicated to implementation, and finally section V concluded the research work.

2. Related Work

There has been a lot of work done in the field of DDoS security [5, 12, 27]. In the reference paper [3], the authors introduce ZombieCoin, a means for botmasters to communicate bots via control information which is stored in bitcoin. The attackers use the bitcoin system to plan and send command and control (C&C) to bots. The authors in [4] enquiries the botnet's long-term survivability and problems like Spamming, phishing, identity theft, and different CC mechanisms were discussed along with their detection measures including internet relay protocol, Honeypots and other IDS/IPS. In paper [6], the researchers talked that the existence of botnets which facilitates majority of unlawful operations, including DDoS attacks, phishing, malicious code distribution, spam messages and mails for illicit content exchange. In paper [7], the authors discussed about an immutable ledger which performs similarly to blockchain to improve energy efficiency without mining which is used to secure devices but the results show that the technique has slow down the processing rate. The work in paper [9] is based on a smart contract. It was decided that the future coupling of blockchain with SDN will result in substantial changes in the business after researching the blockchain mechanism for facilitating services and resources between devices in a cryptographically verifiable manner. In reference paper [10], this work proposes a new approach for upgrading a flow rule table for the forwarding devices known as DiscblockNet that uses a blockchain technology to securely check a version of the flow rule table, validate the flow rule table, and download the latest flow rule table. Modeled Discblock Nets for the defence and prevention of threats like ARP spoofing and DDoS. In Reference paper [14], A secure distributed fog node architecture is proposed that leverages SDN and blockchain techniques and is then extended to the cloud to provide real-time processing security and high availability to reduce end-to-end data transmission delays. Furthermore, in order to support smart health-care applications and services that use smart sensors, this study provides a software-defined system architecture for raw data handling. Then, because all blocks are visible to the patient's doctor and other network members, blockchain is used to protect the patient's recorded processed data. Botnet C&C mechanism Associated work Agobot, SDBot, and SpyBot[15] are examples of first-generation botnets that communicate using the Internet Relay Chat network. Rustock, Asprox, and Zeus were examples of second-generation botnets that exploited HTTP-based C&C communication. Botmasters have also begun to use Domain Generation Algorithm (DGA) instead of web addresses and then move on to Domain Flux, in which botmasters use DNS records to bind multiple destination IP addresses to a domain name. P2P networks, which are employed by Conficker, Storm botnet, and Nugache [16], constitute the third key C&C framework. For extreme impacts, some use multiple solutions, such as Conficker, which exploits both HTTP and P2P networks. Darknets, cloud, and social media platforms are some of the esoteric C&C methods used by botnets. [17] The Flashback Trojan has a Twitter account. Whitewell Trojan makes use of Facebook [18]. Yahoo Mail is used by IcoScript[19]. Google Docs is used by Makadocs[20].

3. Proposed Approach

Every SDN controller is part of a distributed blockchain network. In this instance, all connected controllers can share authenticated information (flow rules) at any moment. By authenticating and verifying the version of the flow rule table, the controllers in blockchain will update it. It also gets most recent flow rule table for any devices connected to a switch. Those who have been approved and meet the security requirements have been triggered. Whenever authorised data was passed among controllers, any undesired data was generated by them, it was a symptom of a prospective DDoS attack on another network. With the help of Parser Flow Rules, the messages for incoming packet like PACKET IN, for statistics like STATS REPLY, foe flow mode like FLOW MOD, and for feature reply like FEATURES REPLY, can be monitored whether data is sent from our network to a supecious network. Also the topology builder identifies changes to the system at data plane layer and network topology due to security regulations which helps for detecting traffic that is headed to a potentially dangerous location. It's possible that the attacker is attacking any innocent network utilising network. In this way, if attackers intend to covert a normal devices into botnet to launch the DDoS attack, then the proposed work prevent our devices from becoming a botnet.

4. Implementation and Experiments

We tested the proposed architecture with various network topologies and traffic loads using the mininet [26] emulation tool. A python-based Ryu controller was used in our experiment. Four Ryu controller instances run on different Virtual Machines (VMs) and are connected via virtual connections to allow inter-VM connectivity. An instance of mininet emulator, is attached to each VM's controller. By building off-band channels using virtual linkages between Ryu instances, we were able to communicate information of blockchain for making synchronization in control plane. Fabric-SDK-Py, a python implementation of hyperledge [28] that is available on Github, is used by each Ryu controller instance to create blockchain information channels and unite them as peers. In contrast, in-band channels for communication are extended by Generic Routing Encapsulation (GRE) tunnels between networks switches running inside each mininet instance of each VM. To create traffic for a DDoS flooding assault, we employ the Stacheldraht [29] programme. Different assaults, such as TCP/SYN floods, UDP floods, and ICMP floods, are launched based on the quantity of flows. The LogMod and SecPoliMod modules accurately detect devices in botnets. Any switch can retrieve a set of device flow rules. Any device delivering data to an undesirable destination or as part of a botnet can benefit from the flow rules in each switch. To avoid becoming a botnet member, the controller implements flow rules on any switch where potentially undesired traffic may originate. From the figure 2, it can be seen that after implementing our scheme the rate of flow can be reduced since we have controlled the devices so that they can not be converted into bots. Also figure 3 depicts that the proposed scheme works better and give a good throughput after applying the scheme.

5. Conclusion

SDN and blockchain technology hold a lot of promise for solving security. Using these technologies, we proposed botnet prevention approaches in this paper. Using the amalgamation of SDN and blockchain strategies, it checks the flow rule and based on the matched rules , the flow table will be updated. An authorised flow table may be downloaded at any moment, and blockchain features prevent devices from becoming botnet slaves.

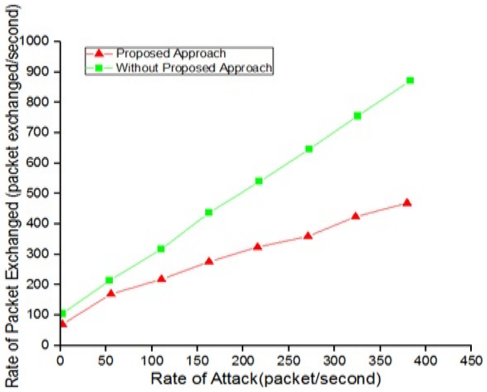

Figure 2: Rate of attack with proposed work

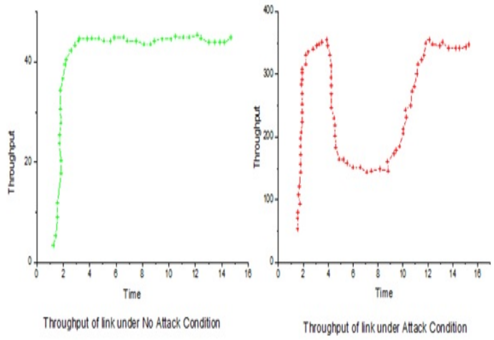

Figure 3: Throughput under attack period and non attack period

References

[1] Gupta, B. B., Joshi, R. C., Misra, M., Jain, A., Juyal, S., Prabhakar, R., & Singh, A. K. (2011, April). Predicting number of zombies in a DDoS attack using ANN based scheme. In International Conference on Advances in Information Technology and Mobile Communication (pp. 117-122). Springer, Berlin, Heidelberg.

[2] Gupta, B. B., & Quamara, M. (2021). A taxonomy of various attacks on smart card–based applications and countermeasures. Concurrency and Computation: Practice and Experience, 33(7), 1-1.

[3] Ali, Syed Taha, et al. "ZombieCoin: powering next-generation botnets with bitcoin." International Conference on Financial Cryptography and Data Security. Springer, Berlin, Heidelberg, 2015.

[4] Gupta, B. B., Joshi, R. C., & Misra, M. (2012). ANN Based Scheme to Predict Number of Zombies in a DDoS Attack. Int. J. Netw. Secur., 14(2), 61-70.

[5] Gupta, B. B., Misra, M., Joshi, R. C. (2012). An ISP level solution to combat DDoS attacks using combined statistical based approach. arXiv preprint arXiv:1203.2400.

[6] Srivastava, A., Gupta, B. B., Tyagi, A., Sharma, A., & Mishra, A. (2011, September). A recent survey on DDoS attacks and defense mechanisms. In International Conference on Parallel Distributed Computing Technologies and Applications (pp. 570-580). Springer, Berlin, Heidelberg.

[7] Dorri, Ali, Salil S. Kanhere, and Raja Jurdak. "Towards an optimized blockchain for IoT." Proceedings of the Second International Conference on Internet-of-Things Design and Implementation. ACM, 2017.

[8] Mishra, A., Gupta, N. & Gupta, B.B. Defense mechanisms against DDoS attack based on entropy in SDN-cloud using POX controller. Telecommun Syst 77, 47–62 (2021). https://doi.org/10.1007/s11235-020-00747-w.

[9] Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." IEEE Access 4 (2016): 2292-2303.

[10] Sharma, Pradip Kumar, et al. "DistBlockNet: A Distributed Blockchains-Based Secure SDN Architecture for IoT Networks." IEEE Communications Magazine 55.9 (2017): 78- 85.

[11] Kshetri, Nir. "Can Blockchain Strengthen the Internet of Things?." IT Professional 19.4 (2017): 68-72.

[12] Dhananjay Singh (2021) Captcha Improvement: Security from DDoS Attack, Insights2Techinfo, pp.1

[13] Sharma, Pradip Kumar, Mu-Yen Chen, and Jong Hyuk Park. "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT." IEEE Access 6 (2018): 115-124.

[14] AlZu'bi, S., Hawashin, B., Mujahed, M., Jararweh, Y., Gupta, B. B. (2019). An efficient employment of internet of multimedia things in smart and future agriculture. Multimedia Tools and Applications, 78(20), 29581-29605

[15] Barford, Paul, and Vinod Yegneswaran. "An inside look at botnets." Malware detection. Springer, Boston, MA, 2007. 171-191.

[16] Wang, Ping, Sherri Sparks, and Cliff C. Zou. "An advanced hybrid peer-to-peer botnet." IEEE Transactions on Dependable and Secure Computing 7.2 (2010): 113-127.

[17] Prince, B.: Flashback botnet updated to include twitter as C&C. SecurityWeek, 30 April 2012.

[18] Lelli, A.: Trojan.Whitewell: Whats your (bot) Facebook Status Today? Symantec Security Response Blog, October 2009. http://www.symantec.com/connect/blogs/trojanwhitewell-what-s-your-bot-facebook-status-today. Accessed on 20 November 2018.

[19] Kovacs, E.: RAT Abuses Yahoo Mail for C&C Communications. SecurityWeek, 4 August 2014. Accessed on 20 March 2018.

[20] Katsuki, T.: Malware Targeting Windows 8 Uses Google Docs. Symantec Official Blog, 16 November 2012. Accessed on 20 March 2018.

[21] Sturgeon, W. "Net pioneer predicts overwhelming botnet surge." ZDNet News, January 29 (2007).

[22] AsSadhan, Basil, et al. "Detecting botnets using command and control traffic." Network Computing and Applications, 2009. NCA 2009. Eighth IEEE International Symposium on.

IEEE, 2009.

[23] Ianelli, Nicholas, and Aaron Hackworth. "Botnets as a vehicle for online crime." FORENSIC COMPUTER SCIENCE IJoFCS19 (2005).

[24] Bacher, Paul, M.kotter. "Know your enemy: Tracking botnets(using honeynets to learn more about bots), Technical report , the Honeynet project, 2008.

[25] Rosenfeld, Meni. "Overview of colored coins." White paper, bitcoil. co. il (2012): 41.

[26] Lantz, Bob, Brandon Heller, and Nick McKeown. "A network in a laptop: rapid prototyping for software-defined networks." Proceedings of the 9th ACM SIGCOMM Workshop on Hot Topics in Networks. ACM, 2010.

[27] Tripathi, S., Gupta, B., Almomani, A., Mishra, A., Veluru, S. (2013). Hadoop based defense solution to handle distributed denial of service (ddos) attacks. Journal of Information Security. Vol. 4 No. 3 (2013) , Article ID: 34629 , 15 pages DOI:10.4236/jis.2013.43018

[28] Cachin, Christian. "Architecture of the Hyperledger blockchain fabric." Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016.

[29] The stacheldraht ddos attack tool," 2009. [Online] Available:http://staff.washington.edu/dittrich/misc/stacheldrah t.analysis.txt. Accessed on 10 December 2018.

[30] Chhabra, M., Gupta, B., & Almomani, A. (2013). A novel solution to handle DDOS attack in MANET. Journal of Information Security Vol. 4 No. 3 (2013) , Article ID: 34631 , 15 pages DOI:10.4236/jis.2013.43019

[31] A. Dahiya, B. B. Gupta (2021) How IoT is Making DDoS Attacks More Dangerous?, Insights2Techinfo, pp.1