DDoS Mitigation: Decentralized CDN Using Private Blockchain

Kyoungmin Kim
Department of Cyber Defense (CYDF)
Korea University
Seoul, Republic of Korea
richard2104@korea.ac.kr

Youngin You, Mookyu Park, Kyungho Lee
Institute of Cyber Security and Privacy(ICSP)
Korea University
Seoul, Republic of Korea
{crenius, ctupmk, kevinlee}@korea.ac.kr

***Abstract*—** Distributed Denial of Service (DDoS) attacks are intense and are targeted to major infrastructure, governments and military organizations in each country. There are a lot of mitigations about DDoS, and the concept of Content Delivery Network (CDN) has been able to avoid attacks on websites. However, since the existing CDN system is fundamentally centralized, it may be difficult to prevent DDoS. This paper describes the distributed CDN Schema using Private Blockchain which solves the problem of participation of existing transparent and unreliable nodes. This will explain DDoS mitigation that can be used by military and government agencies.

Keywords—Private Blockchain, DDoS mitigation, Content Delivery Network(CDN)

I. INTRODUCTION

There are many Distributed Denial of Service (DDoS) attacks around the world that degrade the availability of each system. This is not only against companies, but also against DDoS attacks against major government agencies, infrastructure sites and even national defense networks in each country. DDoS attacks on the media and political websites are taking place as a kind of hacktivism. [1] These attacks can have social and political impacts and have a large impact beyond general economic damage. Particularly in the case of Korea, there were 3/3, 6/25, 7/7 DDoS incidents. In these cases, DDoS was blown to various major infrastructure facilities such as the Blue House, broadcasting companies, and banks, thereby causing social confusion.

The type of DDoS is caused by overloaded traffic. To solve this problem, a content delivery network or a content distribution network (CDN) is used. [2] A system that stores and provides data to a network with multiple nodes to efficiently deliver content. Since the data is transmitted directly to an Internet Service Provider (ISP), there is an advantage that a content bottleneck can be avoided. Today, however, we rely on centralized CDNs to deliver high-speed Web site services. The CDN company has a worldwide network of proxy servers and data centers. CDN clients utilize these servers to deliver content over short distances, providing faster delivery times.

Nevertheless, current systems are vulnerable to DDoS because their operations are still centralized. Each company uses an ISP to borrow or install a CDN server, which limits the capability of the network on the basis of their capital. Also, DDoS attacks are evolving day by day, so if one does not solve this fundamental problem, the security patches that rise in the application layer become useless. By using a distributed platform, users can lease bandwidth and pool this bandwidth to handle a significant amount of data, which can greatly reduce this risk.

This paper describes a method of mitigating DDoS by using a blockchain that uses decentralized CDNs with trusted node participants authorized by the military or government agencies.

The composition is as follows. Chapter 2 explains the scale-free network to demonstrate the security and effectiveness of a blockchain network. Also, the concept of private blockchain has been written and the reasons for using it are explained. Chapter 3 describes mitigation solutions using traditional DDoS schemes and mitigations and borrowing from existing public blockchain schemes. The next section proposes a CDN solution that utilizes a private blockchain. The proof of concept is explained below. The final section describes the conclusion and limitations of the proposed method.

II. BACKGROUNDS

In this section, we describe the network structure using graph theory to demonstrate the degree of robustness to the DDoS, and introduce the overall background of the private blockchain.

A. Scale-Free Network

The scale-free network is a new concept because the existing network models do not fit well with the degree distribution.[3] Scale-free networks consist of a small number of high degree nodes and a lot of small degree nodes. A node with such a high degree is called a hub. In other words, a scale-free network means a network in which a hub exists.

A scale-free network is defined by a power-law degree distribution. The fraction P(k) of nodes in the network having k connections to other nodes goes for large values of k. It can be expressed as follows.

$$P(k) \sim k^{-\gamma} \quad (1)$$

Most scale-free networks have exponents between 2 and 3. This paper will see changes in the number of hub compared with the use of the proposed model instead of the existing centralized server operation.

B. Private Blockchain

Blockchain technology has been introduced for the first time as a bitcoin and has developed into various forms such as transaction anonymization, smart contract, and permissioned blockchain. The existing blockchain is transparent and open as a public blockchain, so unauthorized participants can access hackers with malicious intent. In this situation, all nodes in all parts of the world must share the same data while defending against malicious network participants' attacks. A public blockchain is basically a structure in which anyone creates and submits a block candidate, selects a block through a distributed agreement, and is recognized as a reliable block. [4] Therefore, when there is a time to share a block on the Internet and too many blocks are created at the same time, it is difficult to select one block.

In order to use Proof of Work (PoW) or Proof of Stake (PoS) as a decentralized algorithm that is adopted in the public blockchain, an internal currency is required. The goal of decentralized aggregation in a public blockchain is to select the nodes that will eventually be able to validate transaction details and create reliable blocks, and this will be a costly effort.

To solve this limitation, the concept of private blockchain occurred. Private blockchains are also called "Permissioned Ledgers". Participants should have permission to participate in the reading, writing and consensus process, and specific subjects may be added or removed as needed. It is also possible to design a private blockchain with different versions depending on the design purpose. Therefore, although everyone can view the data, the data recording can be applied in a variety of ways.

Most of the private blockchains do not allow network branching using the Byzantine Fault Tolerance family of distributed algorithm. These algorithms do not have hash competition, such as Federated Byzantine Agreement (FBA), Tendermint [5] and Practical Byzantine Fault Tolerance (PBFT) [6]

III. Related Works

This section introduces the existing mitigation method to prevent DDoS and introduces a method to prevent DDoS using blockchain recently. Also, this section explains about why we propose a new method.

A. Conventional DDoS Mitigation

There is a "Rate-Limiting" that blocks access to the website by identifying the IP address that requests the website excessively. Once the request threshold is reached, that IP is no longer accessible to the site. Similarly, there is a way to block future threats by grouping similar IP addresses that are related to each other through IP Address Matching. One can also detect geographic anomalies to prevent attacks. It verifies the information of the request as well as utilizing connection IP and geography to identify and filter out strange queries.

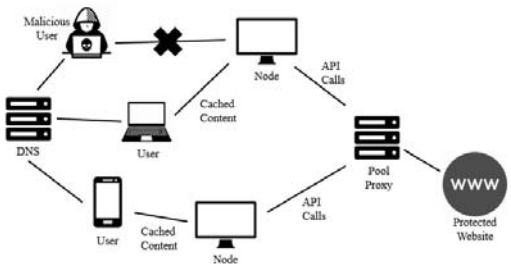

Fig. 1. Overview of Gladius to prevent DDoS

In addition, recent research suggests a method of using backup servers or multiple servers, or dynamic DDoS defense resource allocation through network visualization [7]. There is also a way to build the structure by load balancing based on the cluster for better network security.[8]

B. Using Blockchain to Prevent DDoS

A security company called Gladius uses Blockchain technology to enable computer users around the world to provide extra bandwidth to the websites they need. Small tokens, Gladius, are given to those who donate bandwidth. Gladius said that for companies using decentralized CDNs, this could provide effective protection against DDoS attacks as well as fast content delivery. Since the existing centralized CDN is too expensive, Decentralized CDN, which is a way to increase the bandwidth inexpensively, allows companies to implement more robust cyber security through fast content delivery.

The implementation schema is as follows. Similar to traditional CDN and DDoS protection techniques, it specifies a custom proxy between the server of the website and the open Internet. However, the layer located between the Web site and the Internet consists of a small number of clients, and traffic is checked and cached files / contents are divided into small parts and communicated with each other.

Web site owners can use the system to accelerate content delivery because computers around the world can effectively act as remote messengers of cached data.

There is also a node pool that groups people together to provide a faster network. These pools are viewable and accessible through a marketplace where one can view information about geographic locations, pool sizes, and reputation. Because a pool can consist of only one person or organization's resources, one can run an instance of the Gladius pool without having to approve the external node. The agreement allows anyone to distribute content and respond to DDoS attacks.

A key component of any DDoS protection system is that the final proxy keeps the IP address of the hidden server that the Gladius network performs by masking IP at the node of the pool. The network has a reputation system that prevents malicious pools. The pool also provides a secure environment with the ability to approve individual nodes entering the pool.

To create a full-featured CDN, each node must be able to cache its main content and deliver its content to its closest clients. Clients use a location-based DNS server to ensure that they are connected to the closest node and are always sent to the closest available node.

However, a solution that uses the public blockchain like Gladius have several problems. Untrusted anonymous nodes can participate in the network and it has transparent contract records. There is a limitation in that the information about which node provides the server is transparent, and anyone has to construct a pool that provides the power of the CDN and issue cryptocurrency to lead the participation of the nodes. Because governments of public authorities or government agencies are important to the servers of trusted entities, it is necessary to exclude the need to issue such cryptocurrency and utilize trusted nodes.

In addition, since the public blockchain technique is influenced by the block generation time and the block confirm time, it can occur the overhead problems that the contract might not be inserted to the right timing. This can lead to the problem that the ability of DDoS mitigation cannot be fully used due to the problem of public blockchain. It is important to make use of the special consensus of the private blockchain to avoid problems in availability. Private blockchain has the advantage that the acceptable transaction per second is higher than that of public blockchain.

In particular, since gladius is a smart contract implemented in the Ethereum blockchain, this mitigation cannot be used if an overload occurs in Ethereum blockchains [9].

IV. Proposed Method

As described above, the CDN scheme using the existing public blockchain requires an algorithm of agreement with untrusted nodes. Such a consensus algorithm cannot help but suffer from the problem that the transaction amount per second, which is the limit of the public blockchain, is significantly reduced. Also, as the token price fluctuates significantly, there may be a problem that the number of people providing the bandwidth decreases. In this section, we explain the CDN structure using private blockchain to solve these problems and prove its efficiency.

A. Block Structure

The block structure is as follows. The transaction inside the block stores the contract records. These contract records contain the bandwidth from which servers are borrowed. IP, location, and metadata are stored, and they are stored in the block after they have been authenticated through public key exchange. Each transaction that is stored through a separate authentication method adopts a method that can demonstrate integrity such as Merkle Root and stores it after hash digest.

B. Network Configuration

Participants in the proposed blockchain network are: Permissioned Node (Block Generator), Bandwidth Provider.

It is important to distinguish between the provider and the nodes that make up the blockchain. Permissioned nodes use the Byzantine Fault Tolerance family algorithm, which is a block confirm process consensus that does not cause branching. These nodes do not participate in database storage and are chosen by the administrator.

The Bandwidth Provider's role is similar to existing CDN or public blockchain. These methods can be a method of donating bandwidth to a pool proxy, or a method of borrowing bandwidth directly by developing a protocol. Transactions traded between them are stored in blocks. Each provider can provide bandwidth or set the permissions to be borrowed.

Basically, the reason for selecting the validators that confirm the block using the private blockchain is to minimize the possibility of modifying the block. To be used by companies or government agencies that are sensitive to data forgery. One can use vast bandwidth while ensuring the integrity of the contract record. This solves the scalability problem rather than the public blockchain and reduces the flaws in the blockchain network itself.

C. Motivation

It is easy to provide a compensation scheme when the integrity is verified and the contract record is saved. Information about people who have borrowed bandwidth is stored. Fixed-value coin can be used to compensate various people participating in the network. The token generated from the public blockchain, whose price fluctuates, cannot be consistently supplied by the bandwidth provider.

This approach can vary depending on the policy of operating the blockchain. The common point is that it should be provided by many people and those located in geographically remote areas should provide the bandwidth.

D. Proof of Concept

The assumptions about the network are as follows. An end node can be thought of as a web site or a user connecting to the system. We do not think end nodes are connected to each other. Each hub node is considered a CDN server providing cache information. The Proof of Concept proves that this hub node distribution evenly spreads. This is because an attacker will attack hub nodes to achieve maximum effectiveness at minimal cost, so hub nodes will be fewer and the degree of even distribution per node will not be vulnerable to DDoS.

It is assumed that the existing centralized CDN network follows a scale-free network. The reason is that the hub nodes provided by one CDN company are limited. This is because content is delivered through a small number of hub nodes. If a CDN company is large and has many hub nodes, it is likely to be decentralized, but there is a limitation because it is not a P2P scheme. The simulation is as follows. We have created a network that assumes the number of CDN data centers of existing companies. In the case of a network with a private blockchain, we generated a hub node with a suitably high degree in the new location.

According to the existing research, the more the user activity, the closer to the random network the blockchain

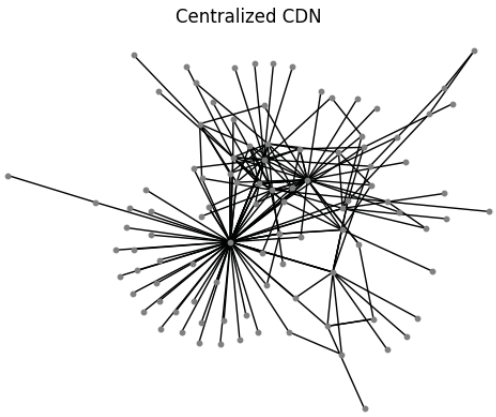

Fig. 2. Centralized CDN Network

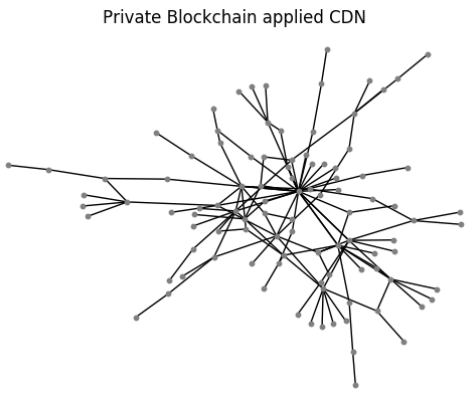

Fig. 3. CDN Network Using Private Blockchain

network is. [10] In other words, higher user activity in the network reduces global cliquishness in the graph.

The User Activity has the highest number of public blockchains with a large number of users and then the private blockchain. The public blockchain will provide the bandwidth with P2P, so it will be closest to the random network. The decentralized CDN is more likely that the trusted CDN server is more restrictive than the private blockchain and the users are connected. Therefore, the private blockchain is called a scale-free network and the parameters are compared. There are three parameters. The probability of adding a new node connected to an existing node arbitrarily selected according to the in-degree distribution and the possibility of adding a node connected to an existing node arbitrarily selected according to the probability and degree distribution to add an edge between two existing nodes. We set the variables for the nodes through the logic provided above and experimented several times. The following three illustrations are examples of one of them. Based on the Random Network, are the Perfect Decentralized Network, the traditional CDN, and the Private blockchain used CDN, respectively. The degree centrality generated through the graphs is also much more uniform than the conventional CDN.

V. Conclusion

This paper provides the scheme of the decentralized CDN using private blockchain and proof that it is more robust than conventional CDN network. We have created an example of a network model for the developed schema, applied it to a scale-free network, and compared the graph to the most decentralized network.

The advantage is that it is possible to participate in a larger amount of bandwidth than the existing limited CDN provision through private blockchain, and it can be used not only for the integrity of the blockchain but also for the block creation of reliable nodes. The number of hub nodes was increased compared to the conventional centralized CDN. In order to prove this, the most fundamental logic is that the bandwidth provider through the distributed platform simplifies the transaction authentication process and assurance process, thereby reducing the opportunity cost significantly. There are issues that tokens are not provided, but each institution can provide the incentive in various ways. For this reason, it is suitable for use in institutions where the reliability of nodes, such as government agencies and national defense networks, is very important.

Acknowledgment

This research was supported by the MSIT(Ministry of Science, ICT), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2018-2015-0-00403) supervised by the IITP(Institute for Information &communications Technology Promotion)

References

[1] Mansfield-Devine, Steve. "DDoS: threats and mitigation." Network Security 2011.12 (2011): 5-12.

[2] Saroiu, Stefan, et al. "An analysis of internet content delivery systems." ACM SIGOPS Operating Systems Review 36.SI (2002): 315-327.

[3] Li, Lun, et al. "Towards a theory of scale-free graphs: Definition, properties, and implications." Internet Mathematics 2.4 (2005): 431-523.

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

[5] Kwon, Jae. "Tendermint: Consensus without mining." Retrieved May 18 (2014): 2017.

[6] Castro, Miguel, and Barbara Liskov. "Practical Byzantine fault tolerance." OSDI. Vol. 99. 1999.

[7] Jakaria, A. H. M., et al. "Dynamic DDoS Defense Resource Allocation using Network Function Virtualization." Proceedings of the ACM International Workshop on Security in Software Defined Networks \& Network Function Virtualization. ACM, 2017.

[8] Frishman, Gal, Yaniv Ben-Itzhak, and Oded Margalit. "Cluster-based load balancing for better network security." Proceedings of the Workshop on Big Data Analytics and Machine Learning for Data Communication Networks. ACM, 2017.

[9] Wood, Gavin. "Ethereum: A secure decentralised generalised transaction ledger." Ethereum Project Yellow Paper 151 (2014): 1-32.

[10] Baumann, Annika, Benjamin Fabian, and Matthias Lischke. "Exploring the Bitcoin Network." WEBIST (1). 2014.