2018 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Ubiquitous Computing & Communications, Big Data & Cloud Computing, Social Computing & Networking, Sustainable Computing & Communications

A Blockchain based Online Trading System for DDoS Mitigation Services

Xue Yang
Huawei Technologies
Beijing, China
xueer.yangxue@huawei.com

Bingyang Liu
Huawei Technologies
Beijing, China
liubingyang@huawei.com

Fei Yang
Huawei Technologies
Beijing, China
yangfei15@huawei.com

Chuang Wang
Huawei Technologies
Beijing, China
wangchuang@huawei.com

***Abstract*—Existing DDoS mitigation services are often performed near the victim network, which have the drawbacks of wasting resources in the intermediate networks. This paper proposes a blockchain based online trading system for DDoS mitigation services, which enables a victim network to on-demand purchase DDoS mitigation services close to the attack sources. The blockchain provides a trust infrastructure for the victim network to find optimal remote service providers, and a sophisticated credit system to evaluate the credibility of players in the system.**

Keywords—DDoS mitigation, bockchain, credibility evaluation

I. INTRODUCTION

Distributed Denial of Service (DDoS) attacks combine multiple distributed attack sources to attack a single victim, thereby amplify the attack power and downgrade the services of the victim network. DDoS can exhaust not only the resources of victim networks but also of the uplinks. Mitigation near attack sources is better than near attack targets, because it prevents the attack traffic from consuming bandwidth resources of the intermediate networks. Besides, the burden of DDoS mitigation is shared, so the required service capacity of single provider will not be so challenging.

However, near-source DDoS mitigation requires a business model that the victim network to purchase mitigation services from multiple providers close to the multiple source networks, which can be any of the tens of thousands of autonomous systems (ASes). There are two challenges. First, the victim network has to set up business relationship with the remote providers, who may be unknown to the victim. Second, different attacks have different sources, and thus require setting up business relationship with different providers. Due to the challenges, existing mitigation services are typically provided closed to the victim networks.

In this paper, we use blockchain to build a trust infrastructure, which helps the victim network to set up trust relationship with the remote providers, and enables fast on-line trading between them to start DDoS mitigation as soon as possible. We present preliminary evaluation and show the feasibility of the system.

II. SYSTEM ARCHITECTURE

A. Find trusted DDoS mitigation service providers

Our system is built on top of a blockchain based Decentralized Internet resource trust Infrastructure (DII) [1]. DII runs a decentralized ledger based on blockchain. DII certifies IP prefix ownership and route origin authorization (ROA) which certifies prefix-to-ASN mapping. When the victim network (Client) detects a DDoS attack, it analyzes the characteristics of attack traffic and obtains the attack source IP addresses (in this paper we only deal with DDoS attacks without spoofed source addresses). The Client uses DII to obtain the AS number according to the attack source IP addresses.

Each DDoS mitigation provider (DMP) has an account on the blockchain. An AS owner in DII can write one or multiple DMPs (together with the DMPs' Server IP addresses) into the blockchain as the authorized DMPs for the AS. For security, we (and DII) use permissioned blockchain, instead of public blockchains like Bitcoin or Ethereum. Only the providers who are endorsed by authorities are permitted to the blockchain. The Client obtains the information of DMP(s) authorized by the source AS. If no DMP is found, the Client can look up the neighbor ASes on the path from the source AS to its network.

B. Evaluate credibility for DMP and Client

Before selling and purchasing services, the DMP and Client need to evaluate each other's credibility. Calculation of the credibility of DMP or Client is based on their historical transaction records, which are also recorded on the blockchain.

The credibility evaluation model is as follows. Let $I(c)$ denote the total number of transactions performed by c, $S(c, i)$ denote the feedback received from feedback node in its ith transaction, where $S(c, i) \in (0, 1)$. $Cr(c, i)$ is the credibility of the ith transaction and it is affected by the trust value of the feedback node and the trust factor of the transaction context. $N(c)$ denotes the trust factor of the number of transaction. The trust value of Client/DMP c denoted by $T(c)$ is defined in (1).

$$\boldsymbol{T(c) = N(c) \sum_{i=1}^{I(c)} (S(c,i) * Cr(c,i))} \quad (1)$$

When the number of transactions tends to infinity, the influence of the malicious node will be ignore and the trust factor is close to 1, $N(c)=e^{-1/I(c)}$. $Cr(c, i)$ is defined in (2). $p(c, i)$ denotes the feedback node of the ith transaction. $TF(c, i)$ denotes the trust factor of the ith transaction context. $TF(c,i) = 1 - n_i/24$, where n_i is the number of months since the ith transaction. n_i is 0 when the transactions is within one month, and so on. n_i is 23 when the transactions was over 23 months.

978-1-7281-1141-4/18/$31.00 ©2018 IEEE
DOI 10.1109/BDCloud.2018.00151

$$Cr(c,i) = \frac{T(p(c,i)) * TF(c,i)}{\sum_{j=1}^{I(c)} T(p(c,j)) * TF(c,j)} \quad (2)$$

The DMP/Client credibility evaluation model is based on PeerTrust [2]. After each transaction, Client and DMP will give feedback that reflects how well the evaluated node has fulfilled its part of the service agreement. Client and DMP may give false feedback to evaluated node due to malicious motives, so it needs to distinguish between honest and dishonest feedback to avoid being controlled by the malicious node. It considers the influence of transaction context, for example, the most recent transactions will better reflect the recent credibility of the evaluated node, and have a high weight. It effectively motivates nodes to maintain good credibility and prevents malicious nodes from deceiving after accumulating a certain amount of trust.

C. DMP and Client untrusted entity online trading

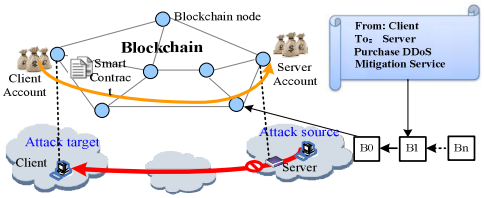

Fig. 1. Online DDoS mitigation service trading system based on blockchain

Online trading need to be performed quickly without the guarantee of a third-party centralization organization to reduce the time the Client is attacked. As shown in Fig.1, DDoS mitigation service online trading system uses the smart contract on blockchain to implement online trading for untrusted entities. The Client initiates a transaction to the DMP to request DDoS mitigation service. When the DMP receives the request transaction, it evaluates the Client's credibility, verifies that the Client has the ownership of the attacked IP address. If the DMP accept the service request, it initiates a transaction with the Client to agree to provide DDoS mitigation service. The Client can purchase the DDoS mitigation service from the DMP only when it receives the transaction from the DMP.

III. Peliminary Evaluation

This paper preliminary evaluates the feasibility of the system in the blockchain based on two aspects of transactions per second (TPS) and storage.

The max number of DDoS attacks is 1555 times per day according to the statistics of DDoS attacks in Q2 2018 from Kaspersky Lab [3]. The average number of DDoS attacks is 0.05 times per second, which is not a key factor affecting TPS. Currently, there are 238 countries in the world, and 80% of the DDoS attackers are distributed in 3 countries and 93.56% of the DDoS attackers are distributed in 10 countries [4]. Assume that a DMP in a country can mitigate DDoS attacks from all the ASes in the country. The number of attack sources is a key factor affecting TPS. As shown is Fig.2, if the attackers from all the countries in the world, the required TPS is 0.8K. The highest TPS in blockchain is exceed 3K (for example EOS), which can meet the requirements of TPS.

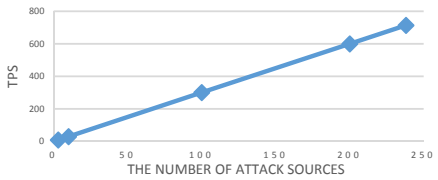

Fig. 2. TPS according to the number of attack sources

The IP address, ROA and the transactions are stored in the blockchain, and the number of records is increasing annually. The number of DDoS attacks per day is less than 0.6K [3], then total number of DDoS attacks in a year is 220K. The number of IP address allocated in 2017 is 15K. Assume the average number of ASs to which an IPv6 address belongs is 2. The storage size for one year is shown in table I.

TABLE I. IPv6, ROA and Transaction Storage Size

Data Type	Single Record Size(B)	Number(K)	Total Size (M)
IP	38	15	0.57
ROA	32	30	0.96
Transaction	800	220	176

In the next 10 years, the storage size will be 2G. The TPS and storage are not the issues of the system implemented based on blockchain.

IV. Discussion And Conclusion

DynaShield [4] is a cost-effective DDoS defense architecture. The similarity is that DynaShield and this paper use blockchain to mitigate DDoS attacks. The differences are as follows. First, DynaShield mitigates DDoS attack near attack targets, and we mitigate DDoS attack near attack sources. Second, DynaShield uses cryptocurrency mining as Proof-of-Work to help offset the cost of serverless functions, and we use blockchain to provide a trust infrastructure and online trading.

In this paper, we try to explore the potential of blockchain in facilitating network service trading between untrusted entities. We base our DDoS mitigation service trading system on DII for trusted IP and ASN ownership, and design a credibility system for trusted Client and DMP evaluation. We present preliminary evaluation results and show the feasibility of our system.

References

[1] Stefano Angieri, Alberto García-Martínez, Bingyang Liu, Zhiwei Yan, Chuang Wang, Marcelo Bagnulo. An experiment in distributed Internet address management using blockchains. arXiv.org. 2018, arXiv:1807.10528 [cs.NI]

[2] Li Xiong, Ling Liu. PeerTrust: Sopporting reputation-based trust for peer-to-peer electronic communities. IEEE Trans. on Knowledge and Data Engineering, 2004, 16 (7) : 843−857.

[3] DDoS attacks in Q2 2018. https://securelist.com/ddos-report-in-q2-2018/86537/

[4] Shengbao Zheng, Xiaowei Yang. DynaShield: A Cost-Effective DDoS Defense Architecture. In SIGCOMM Posters and Demos '18: ACM SIGCOMM 2018 Conference Posters and Demos, August 20-25, 2018, Budapest, Hungary, 3 pages. https://doi.org/10.1145/3234200.3234232