International Journal of Engineering & Technology, 7 (3.34) (2018) 551-553

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Analysis of Spam Transaction on the Blockchain

Tae Kyung Kim

Department of Internet Security Engineering as a Service, MyongJi College, 356-1 Hongeun3-dong, Seodaemun-gu, Seoul, 120-776 Korea

**Corresponding author E-mail: tkkim@mjc.ac.kr*

Abstract

Background/Objectives: The blockchain has been applied to many fields. Users are concerned about its security. The primary goal of this study is supporting the security service to protect DDoS attack.
Methods/Statistical analysis: To provide security service in the blockchain, the security model is suggested. This model can filter out illegitimate traffic and exchange information with other security switches to determine whether a connected node is a normal node or an abnormal node. Each procedure of the proposed model has been described. Also, two different attack types are used to show the operation process of suggested model.
Findings: Cyberattacks attempting to impact technology services availability continue to increase. Thus, DDoS is one of the most common type of attacks can also cause the most disruption to internet services. But blockchain has the characteristics of decentralization and peer to peer. This makes it harder to disrupt than conventional distributed application. Nevertheless, DDoS attacks remain a persistent threat. Therefore, a security model is suggested which can effectively block and respond to DDoS attacks.
Improvements/Applications: The suggested model makes it possible to protect the spam transaction attacks in blockchain network.

Keywords: *Blockchain, DDoS, Spam transaction, Eclipse attack, Abnormal node*

1. Introduction

A blockchain is a continuously growing list of records, called blocks, that are linked and protected using hash function. Each block generally contains a hash pointer as a link to a previous block, a timestamp and transaction data. A blockchain can serve as an open distributed ledger that can record transactions between two parties in an efficient, verifiable and permanent way[1]. The blockchain technology has been applied to many fields such as Internet of Things[2, 3], economics[4] and so on. The bitcoin network has suffered from multiple attacks over the past few months. But the bitcoin network was overloaded, and transactions were taking unusually longer to get processed. Because a large number of spam transactions occur in the network, resulting in denial of service. Therefore, it is required to study the countermeasure on the spam transaction of blockchain. These are not attacks against the technology, but rather individuals flooding the network with transactions. Spam attacks against the bitcoin network have become a major problem. Due to the nature of these actions, a few individuals can cause a major transaction backlog, as a result, the mempool fills up with unconfirmed transfers[5].
DDoS is one of the most common type of attacks, which can also cause the most disruption to internet services and hence blockchain enabled solutions. Given blockchains are distributed platforms, DDoS attacks on blockchains are not like regular attacks. They are costly as they attempt to overpower the network with large volumes of small transactions. The decentralization and peer-to-peer characteristics of the technology make it harder to disrupt than conventional distributed application architectures such as client-server, yet they are also subject to DDoS attacks, and as such adequate protection measures are still necessary, both at the network and application level.
Also, the eclipse attack is a useful basis for spam transaction attack[6]. The eclipse attack allows an attacker to monopolize all the connections of target's sending and receiving, which isolates the target from the other nodes in the network[7]. Then, the attacker can control the target's information of the blockchain, or let the target cost unnecessary computing power on the blockchain. Furthermore, the attacker is able to leverage the victim's computing power to conduct its own malicious acts. There are two types of eclipse attack on blockchain network[8], namely botnet attack and infrastructure attack. Different bots launch the botnet attack using various IP address. The infrastructure attacks are designed to destroy a system that includes critical data such as Internet Service Provider or company. The Bitcoin network might suffer from disruption and a victim's view of the blockchain will be filtered due to the eclipse attack. Using the eclipse attack, an attacker can manage the all the connection of target node. This attacker can manipulate the information about other parts of blockchain network. The process of eclipse attack is shown in Figure 1.

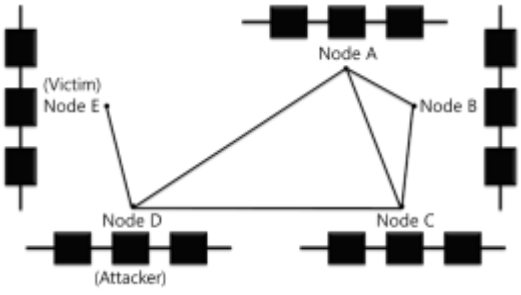

Figure 1: Eclipse Attack

The attacker node(node D) sends its information to the victim node(node E) so that the attacker's information is stored in the victim's table. Multiple requests are made to the victim node(node E) to fill the victim node(node E) table with only the attacker's information. In order to break the connection between the victim node(node E) and other nodes(node A, B, C), the attacker node(node D) must perform a DDoS attack to cause the victim node to restart. The victim node(node E) is restarted, reconnected to peer to peer network based on the information in the table and only connected to the attacker node(node D) because the table contains only the attacker's information. Eclipse attacks can be used as a pre-stage attack to perform spam transaction attacks. Although the block chain is a distributed ledger technology, DDoS attacks after eclipse attack can damage normal transactions of other nodes. The spam transaction process is suggested in Figure 2.

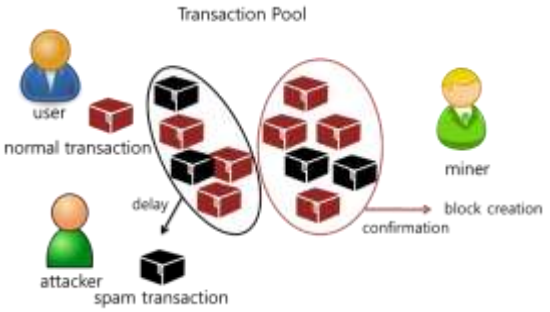

Figure 2: Spam Transaction Attack

The hacker continuously creates spam transactions to attack the normal bitcoin network. Then in the basic transaction pool, unauthorized transactions in the bitcoin are increased. Therefore, normal transactions are not approved and normal service is not provided. It also causes the increase in the confirmation time and fee of the bit coin network. This means that the instability of bitcoin network. This denial of service of bitcoin network is caused by the slow transaction processing.

The most common types of spam are like these[9]:

Sending many without sendmany: If sending payments to many people at around the same time, then it is not required do tons of individual transactions one after the other. Doing so is grossly wasteful of network resources because each transaction produces an extraneous change output. Instead, all the outgoing transactions should be bundled into one transaction. The bitcoin JSON-RPC command for doing this is sendmany.

Signalling and data transmission: Bitcoin is for storing and transferring value between people, and for limited hash-based timestamping. Transactions should never be used as a signal (such as a win/loss signal in a gambling game) or to send data directly.

Useless transactions: Attackers will sometimes waste network resources by sending BTC between their own addresses uselessly.

Very-low-fee flooding: A simplistic attack that people often try is to send tens of thousands of zero or very-low-fee transactions at once. This makes the "mempool" number shown by some websites go up massively.

Although resilient, decentralized blockchain solutions depend on high availability and DDoS attacks will remain a persistent threat.

2. Proposed Security Model for Blockchain

2.1. Overview

The primary goal of this study is supporting the security service to protect Distributed Denial of Service (DDoS) and unauthorized accesses. DDoS attacks cause resources to be exhausted, preventing normal users from using the services they want to use. Once a DDoS attack is successful, the nodes can not send or receive any information, including transactions or blocks. This is not significant in a public network of thousands of nodes, but in a consortium block chain network consisting of a small number of nodes, the attack affects the number of nodes participating in the consensus mechanism. Although this attack does not directly compromise the security of the data stored in the block chain, nodes that are under attack can not participate in the consensus mechanism and these nodes waste computing power by sending new blocks to the block-chain network. Access to an individual or consortium block chain is limited to a set of participating entities. Therefore, the network device must allow only the participating entities to access the nodes and should be able to block all other connection attempts as soon as possible[10].

To protect blockchain network against the DDoS and unauthorized access, the security model for blockchain is suggested. The architecture of security model is shown in Figure 3.

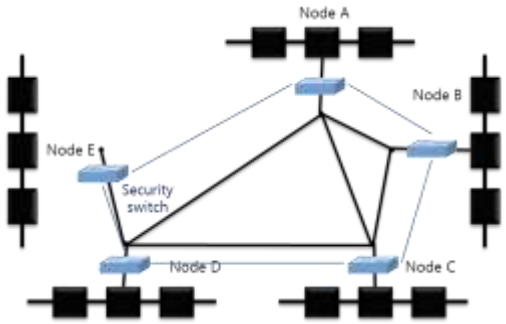

Figure 3: Architecture for Security model

To use the security model with multiple blockchain technologies, it is more useful not to rely on blockchain software modifications. Therefore, the security switch is placed in front of each blockchain node. In the proposed model, switches, which transmit all traffic to the node, and blockchain nodes and are required. The security switches filter out illegitimate traffic and exchange information with other security switch to determine whether a connected node is a normal node or an abnormal node.

Security switches consider three kinds of blockchain node such as legal, illegal and undefined node. Among the blockchain nodes, a normal node means nodes allowed to connect to a blockchain. The security switch only keeps track of the information of these nodes and does not interfere with the delivery of traffic to and from the nodes. And this list is forwarded to adjacent nodes. Undefined nodes are blockchain nodes that are not yet registered on the security switch. Security switch keeps track of these nodes and asks the other node for information about this node. Abnormal nodes are blockchain nodes that are not authorized to connect to a blockchain. The security switch keeps track of these nodes in response to packets being sent and received. To determine the type of blockchain node, security switch periodically interacts with other security switch. Also, each security switch decides which node is normal or abnormal using the thresholds of system resources such as buffer and bandwidth.

The Figure 4 shows the process of security switch when distributed denial of service attacks occur at a normal node[11].

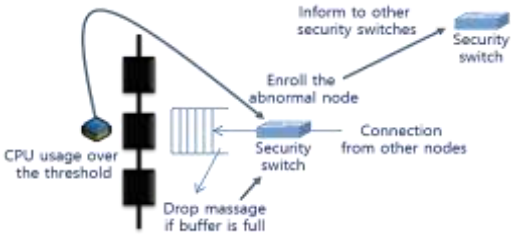

Figure 4: Process of Security switch

As shown in Figure 4, when the buffer of the node is full or if the CPU usage of the node exceeds the threshold, the node sends the security information to the security switch and security switch

enrolls the node to the abnormal node list. Also, security switch informs the abnormal node to other security switches.

2.2. Procedure

The procedure of the security model is divided into two parts. The first part is processing the security threat that occurs in the local node itself and the second part is the process of exchanging information with other security switches.

The first part is explained in Figure 4. Especially local security switch manages the three different kinds of blockchain node. New nodes connected to the local node are added to the initially undefined node list. Depending on the security switch's decision, the node is moved to the legal node list or the list of illegal nodes. If the node is allowed to connect to the blockchain, the node eventually becomes a peer of one of the connected nodes and the node enrolls to the legal node list. The node then remains in the legal node list until a new attack symptom is found or an illegal node list is contacted from another security switch. In addition, the security switch mitigates flooding attacks from multiple sources and detects the anomaly behavior. The detected information is also used to determine three types of node list.

The second part is an information exchange activity that occurs between security switches. Each node contains its own three types of node list and periodically exchange the node list with other security switches. The security switch contains table as shown in Table 1.

Table 1: List table of security switch

	legal node	undefined node	illegal node
node ID list			
information source node			
internal factors			
external factors			

In table 1, the list table of security switch has 4 fields such as node ID list, information source node, internal actors and external factors. The node ID list is a list of remote nodes belonging to legal, undefined, and illegal nodes. Information source node means that if the security switch receives the node list information from other external nodes, it indicates which node sent the information. When the security switch specifies an illegal node for a specific external node, if the cause is internal then the cause is explained in the internal factors field otherwise external factors field should explain the reason. The contents of this table information are periodically exchanged with other security switches.

3. Results and Discussion

To show the efficiency of suggested model, two types of attack were considered.

Firstly, flooding attack from a single source is considered. The malicious node generates a series of SYN packet and sends it to the target. Then the blockchain node can not process incoming packets from other blockchain nodes and cannot participate in the consensus mechanism. But in our model security switch detect the SYN flooding and block the massage from the malicious node. Then enroll the malicious node into the illegal list and sends the list and reason to other security switches. The attack will have a limited impact on the blockchain node.

Secondly, flooding attack from multiple sources is considered. This means that either an attack from many different sources or an attack in which the attackers spoof their IP address. In this case security switch enrolls the ID list to the undefined list and asks the information of these lists to other security switches. If other security switch has no information about these lists, the local security switch transfers the undefined ID list to legal list. But the resource such as buffer or CPU usage exceed the thresholds, the local security switch blocks the node until the node has room for resources. If the attack is conducted in the malicious node by spoofing IP address, the local security switch disconnects the connection with the malicious node and informs these information to the other security switches.

4. Conclusion

Blockchain is one of the core technology in FinTech and IoT industry, users are very concerned about its security. DDoS is one of the most common type of attacks, which can also cause the most disruption to internet services and hence blockchain enabled solutions. Also, the eclipse attack is a useful basis for spam transaction attack. To prevent these attacks in the blockchain, this study was conducted. Therefore, the primary goal of this study is supporting the security service to protect Distributed Denial of Service (DDoS) and unauthorized accesses. To provide security service in the blockchain, the security model is suggested. In the security model, the security switch is suggested which can filter out illegitimate traffic and exchange information with other security switches to determine whether a connected node is a normal node or an abnormal node. Each procedure of the proposed model has been described. As discussed, security model for spam transaction can detect the attack and block the spam transaction.

References

[1] Blockchain. (2018). Retrieved from https://en.wikipedia.org/wiki/Blockchain.

[2] Sun, J., Yan, J., & Zhang, K. Z. (2016). Blockchain-based sharing services: What blockchain technology can contribute to smart cities. Financial Innovation, 2(1), 26.

[3] Zhang, Y., & Wen, J. (2017). The IoT electric business model: Using blockchain technology for the internet of things. Peer-to-Peer Networking and Applications, 10(4), 983-994.

[4] Huckle, S., Bhattacharya, R., White, M., & Beloff, N. (2016). Internet of things, blockchain and shared economy applications. Procedia Computer Science, 98, 461-466.

[5] New spam attacks aim to slow down bitcoin network. (2017). JP BUNTINX. Retrieved from http://www.newsbtc.com/2017/03/04/new-spam-attacks-aim-slow-bitcoin-network/.

[6] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2017). A survey on the security of blockchain systems. Future Generation Computer Systems.

[7] Singh, A. (2006). Eclipse attacks on overlay networks: Threats and defenses. In IEEE INFOCOM.

[8] Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015, August). Eclipse Attacks on Bitcoin's Peer-to-Peer Network. In USENIX Security Symposium, 129-144.

[9] Spam transactions. (2018). Retrieved from https://en.bitcoin.it/wiki/Spam_transactions

[10] Steichen, M., Hommes, S., & State, R. (2017). ChainGuard—A firewall for blockchain applications using SDN with OpenFlow. In Principles, Systems and Applications of IP Telecommunications (IPTComm), 1-8.

[11] Guerin, R. (1992). A unified approach to bandwidth allocation and access control in fast packet-switched networks. In INFOCOM'92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, 1-12.