Revisiting Network-Level Attacks on Blockchain Network

Tong Cao, Jiangshan Yu, Jérémie Decouchant, Paulo Esteves-Verissimo
SnT, University of Luxembourg
Email: firstname.lastname@uni.lu

***Abstract*—Many attacks presented on Bitcoin are facilitated by its real world implementation, which is rather centralized. In addition, communications between Bitcoin nodes are not encrypted, which can be explored by an attacker to launch attacks. In this paper, we give a brief overview of possible routing attacks on Bitcoin. As future work, we will identify possible central points in the Bitcoin network, evaluate potential attacks on it, and propose solutions to mitigate the identified issues.**

I. Introduction

As originally proposed by Satoshi Nakamoto [1], Bitcoin places itself as a fully distributed cryptocurrency that removes the need for central authorities. However, despite the enormous success of Bitcoin, many attacks have been identified because of the conflict between the Bitcoin's envisioned distributed architecture and its real world implementation. Moreover, the Bitcoin architecture is, in practice, rather centralized due to the following reasons. First, the majority of the Bitcoin nodes are hosted by a small number of autonomous systems (AS) [2]. Second, the mining power [3] is shared among a small set of entities — several mining pools control the vast majority of the computing power in Bitcoin. For example, as of March 19th 2018, 14 top mining pools control 99.6% mining power in Bitcoin[1]. Third, some Bitcoin nodes are more stable, and new nodes prefer to establish connections with them for a better connectivity. Thus, a small set of these stable nodes maintains a majority of the connections among all Bitcoin nodes [4]. In fact, the centralization properties of implementing Bitcoin in real world lead to routing attacks possible. We show existing routing attack in Section II.

The Bitcoin network is a peer-to-peer network that relies on the Internet, where each node disseminates transactions and blocks in order to reach consensus. For instance, a node can receive, verify and forward transactions, and validated transactions are collected by nodes with mining power to blocks. Because of unencrypted messages exchanging among nodes, the attacker is able to gain some critical information by establishing connection to victim. This makes deanonymisation attack possible. We also show existing deanonymisation attack in Section II.

II. Existing attacks

Routing attack. Due to the highly centralized autonomous systems in the Bitcoin network, malicious messages can be injected into one autonomous system to announce incorrect IP prefixes, which leads to the network traffics going into wrong locations. It makes the Border Gateway Protocol (BGP) hijacking attack [2] possible in the Bitcoin network, where an attacker can delay the information propagation and partition the Bitcoin network in order to waste mining power, or spend one coin more than once. The eclipse attack was described in 2015 [7], where unsolicited incoming connections are used by an attacker to send bogus information to a victim to force it to restart. After that, the attacker can monopolize all 125 connections of victim and, with a high probability, control the endhost.

Deanonymisation attack. Fanti and Viswanath described Deanonymisation attacks [5], which aim at disclosing the IP address of nodes that generate transactions, even those located behind a Network Address Translation (NAT).

Since each client node has 8 entry nodes, and the generated transactions of the client are always first forwarded to its 8 entry nodes, it is possible to identify the entry nodes of a client node [5]. In addition, some approaches rely on the Bitcoin relay pattern, which can be used to identify the IP address of a transaction creator, i.e, the payer, based on the following observations [6]. First, a node that was the first forwarding a transaction is likely to be the payer. Second, a node is likely to be a payer if it re-transmits the transaction. Moreover, a node is likely to be a mining pool if the generated blocks from the pool were relayed frequently and firstly via that IP address during 10 days period [2].

III. Network-optimized routing attack

The hijacking attack [2] aims at isolating a set of nodes from the Bitcoin network at the AS-level. To make a successful hijacking, an attacker must block all connections of the isolated nodes. If a node cannot be full blocked, then they call this node a "leakage point". The authors then proposed their approach to detect the leakage points and remove them from the target set that is going to be isolated. However, no existing research has focused on how to select the target set of nodes to make the isolation more efficiently, and on how to improve the current situation. As previously explained, the eclipse attack [7] aims to control all the connections of a node in the Bitcoin network. However, the existing eclipse attack does not work for nodes that are behind of a NAT, as they do not have any incoming connections. In this case, we plan to study how a node select and maintain its entry nodes to evaluate the feasibility of this attack.

[1]https://blockchain.info/pools

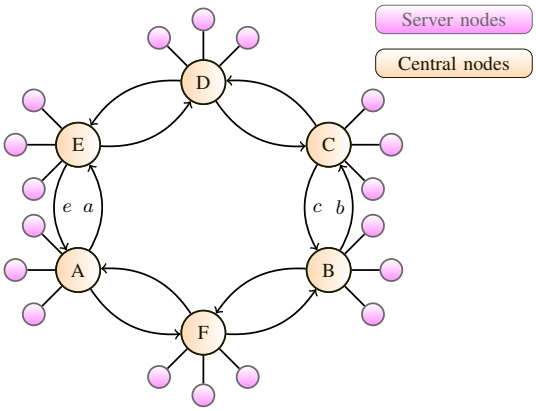

Fig. 1: Central nodes (A,B,C,D,E,F) in Bitcoin network, where a,b,c,e denotes an outgoing connection of node A,B,C,E respectively.

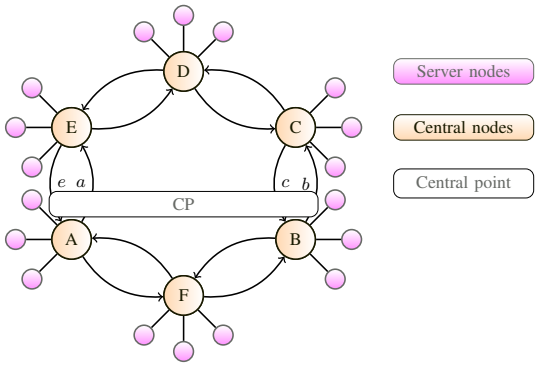

Fig. 2: Central point (CP) in Bitcoin network, where different outgoing connections a,b,c,e might share the same point somewhere in network. The point can be autonomous system or router, and we call them central points.

By default, each node can accept 117 incoming connections, and create 8 outgoing connections in Bitcoin network. Fanti and Viswanath pointed out two types of nodes: the server node that accepts incoming connection and client node that does not [5]. Due to the incoming and outgoing connections of each node being asymmetric, some nodes probably maintain more connections than others, and are frequently connected to other nodes as their outgoing nodes. Influential nodes [8] were defined and characterized by the fact that they connected server nodes with mining pools. To distinguish from influential nodes, we assume that there exist some central nodes in the network (Figure 1) beyond server nodes, which are frequently used to maintain the outgoing connections of server nodes. Furthermore, if we study the AS-level topology between those central nodes, then we might find some network points that frequently appear in the intersections of nodes' connections. We call the point "central point" (Figure 2).

As shown in Figure 2, if the adversary can identify the CP (central point) in the Bitcoin network, then it can disrupt the Bitcoin protocol by attacking CP. As a result, links (a,b,c,e) would subsequently be attacked, and the network partitioned into two parts, (A,B,F) and (C,D,E).

IV. Future work

To verify our observation, we will analyze the existing peer-to-peer network in the Bitcoin system. As a first step, we will monitor the Bitcoin network in order to infer the Bitcoin network's topology. Secondly, we will identify the central nodes and central points from the topology we gained. Lastly, we will evaluate the effectiveness of existing attacks based on our analysis.

Acknowledgment

This work is partially supported by the Fonds National de la Recherche Luxembourg (FNR) through PEARL grant FNR/P14/8149128.

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

[2] M. Apostolaki, A. Zohar, and L. Vanbever, "Hijacking bitcoin: Routing attacks on cryptocurrencies," in *2017 IEEE Symposium on Security and Privacy (SP)*, 2017, pp. 375–392.

[3] A. Gervais, G. O. Karame, V. Capkun, and S. Capkun, "Is bitcoin a decentralized currency?" *IEEE Security & Privacy*, vol. 12, no. 3, pp. 54–60, 2014.

[4] A. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, 2014.

[5] G. Fanti and P. Viswanath, "Deanonymization in the bitcoin p2p network," in *Advances in Neural Information Processing Systems 30*, I. Guyon, U. V. Luxburg, S. Bengio, H. Wallach, R. Fergus, S. Vishwanathan, and R. Garnett, Eds. Curran Associates, Inc., 2017, pp. 1364–1373. [Online]. Available: http://papers.nips.cc/paper/6735-deanonymization-in-the-bitcoin-p2p-network.pdf

[6] D. Koshy, *An Analysis of Anonymity in Bitcoin Using P2P Network Traffic*. Pennsylvania State University, 2013. [Online]. Available: https://books.google.lu/books?id=8WkUnQAACAAJ

[7] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network." in *USENIX Security Symposium*, J. Jung and T. Holz, Eds. USENIX Association, 2015, pp. 129–144.

[8] A. Miller, J. Litton, A. Pachulski, N. S. Gupta, D. Levin, N. Spring, and B. Bhattacharjee, "Discovering bitcoins public topology and influential nodes," 2015.