ComEX

IEICE Communications Express, Vol.10, No.8, 447–450

Special Cluster on Advanced Communication Technologies
in Conjunction with Main Topics of ICETC2020

Exploiting semi-structured overlay networks in blockchain systems

Ryohei Banno[1, 2, a)], **Yusuke Kitagawa**[1], **and Kazuyuki Shudo**[2]

[1] *Kogakuin University*

2665-1 Nakano-machi, Hachioji-shi, Tokyo 192-0015, Japan

[2] *Tokyo Institute of Technology*

2-12-1 Ookayama, Meguro-ku, Tokyo 152-8552, Japan

a) *banno@computer.org*

Abstract: Blockchain systems are built on top of overlay networks. While typical blockchains are based on unstructured overlays, some other blockchains utilizes structured overlays to improve the inefficiency of information propagation in unstructured overlays. However, using structured overlays have security risks such as Eclipse Attack. In this paper, we propose a method for blockchain systems to exploit a semi-structured overlay with Flexible Routing Tables (FRT), so that we can obtain both communication efficiency and safety.

Keywords: blockchain, structured overlay networks, peer-to-peer networks

Classification: Network System

References

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, accessed Feb. 12, 2021.

[2] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," https://ethereum.github.io/yellowpaper/paper.pdf, accessed Feb. 12, 2021.

[3] Y. Marcus, E. Heilman, and S. Goldberg, "Low-resource eclipse attacks on ethereum's peer-to-peer network," IACR ePrint Cryptology Report, vol. 2018, no. 236, pp. 1–15, 2018.

[4] H. Nagao and K. Shudo, "Flexible routing tables: Designing routing algorithms for overlays based on a total order on a routing table set," IEEE International Conference on Peer-to-Peer Computing, pp. 72–81, 2011. DOI: 10.1109/p2p.2011.6038664

[5] R. Banno, Y. Kitagawa, and K. Shudo, "A study of blockchain systems exploiting semi-structured overlay networks with frt," IEICE International Conference on Emerging Technologies for Communications (ICETC), N2–1, 2020.

[6] P. Maymounkov and D. Mazières, "Kademlia: A peer-to-peer information system based on the xor metric," *Peer-to-Peer Systems*, vol.2429, pp. 53–65, 2002. DOI: 10.1007/3-540-45748-8_5

[7] I. Stoica, R. Morris, D. Karger, M.F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *ACM SIGCOMM Computer Communication Review*, vol. 31, no. 4, pp. 149–160, 2001. DOI: 10.1145/964723.383071

DOI: 10.1587/comex.2021ETL0011
Received January 4, 2021
Accepted January 25, 2021
Publicized February 9, 2021
Copyedited August 1, 2021

1 Introduction

Recently blockchain systems have attracted much attention from industry and academic community. Typical blockchain systems including Bitcoin [1] are built on top of unstructured overlay networks. Since unstructured overlays are disadvantageous for the efficiency of information propagation, some other blockchain systems utilizes structured overlays e.g., Ethereum [2]. However, using structured overlays has risks; clearly defined rules to form the topology are possibly abused for controlling information propagation such as Eclipse Attack [3]. That is, there is a kind of conflict between safety by an unstructured topology and communication efficiency by a structured topology.

To address this issue, we propose a method to build a blockchain system exploiting a semi-structured overlay with Flexible Routing Tables (FRT) [4]. By exploiting the semi-structured overlay, we can obtain both information propagation efficiency and safety.

This letter is an extended version of [5] presented in IEICE ICETC 2020. The differences include detailed explanation and discussion of the proposed method and related works.

2 Related work

Bitcoin [1] is one of the cryptocurrencies based on peer-to-peer networks. Its network topology is unstructured; each node randomly selects its neighbors. Such unstructured overlay networks are robust to node churn. On the other hand, broadcasting with them causes large communication traffic or long latency since it generally exploits flooding or gossip-based protocols.

To obtain efficiency in communication among nodes, Ethereum [2] constructs its topology based on Kademlia [6][1] that is one of the algorithms of Structured Overlays. Although such structured overlay-style topology construction brings about fast information propagation without duplicate transmission, its clearly defined rules for finding neighbor nodes have a security risk. That is, an adversarial user can occupy neighbor-positions of a victim node by preparing sufficient number of nodes with arbitrary node IDs [3].

3 Proposed method

To obtain both communication efficiency and safety, we propose a method to exploit semi-structured overlays with FRT.

FRT is a methodology for maintaining routing tables flexibly in structured overlays. In contrast to general structured overlays, in which each node maintains its routing table by adding specific neighbor information according to a precise rule, FRT uses two steps of *entry learning* and *entry filtering* to construct a routing table. By widely collecting node information for the entry learning and abandoning comparatively useless information, FRT enables to form a routing table flexibly e.g., prioritizing the node information that belongs to the same autonomous system (AS).

In our proposed method, we introduce randomization into the entry filtering process. We assume that each node has an identifier calculated by hashing unique

[1]https://github.com/ethereum/devp2p/blob/master/discv4.md (accessed Dec. 30, 2020)

DOI: 10.1587/comex.2021ETL0011
Received January 4, 2021
Accepted January 25, 2021
Publicized February 9, 2021
Copyedited August 1, 2021

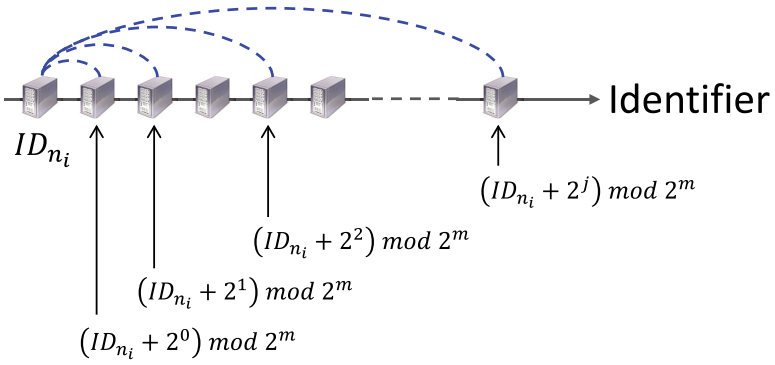

Fig. 1. Neighbor selection in Chord.

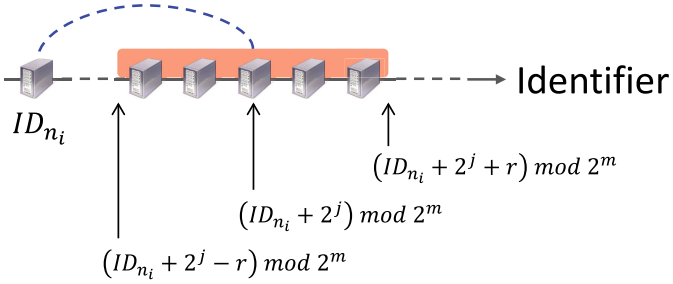

Fig. 2. Neighbor selection in proposed method.

information such as its IP address as with typical structured overlays like Chord [7]. Considering i-th node n_i with its identifier ID_{n_i}, node n_i firstly calculates target identifiers $T_{n_i,j}$ based on the algorithm of Chord, i.e.,

$$T_{n_i,j} = ID_{n_i} + 2^j \bmod 2^m \quad (j = 0, 1, ..., m-1) \tag{1}$$

where m is the bit length of the hash values. Figure 1 indicates neighbor selection of Chord[2]. In Chord, this scheme makes each node to have $O(logN)$ neighbors who have various distances from the node.

Then, in the proposed method, node n_i collects node information in the entry learning process and subsequently conducts the entry filtering process. In the entry filtering process, for each target identifier $T_{n_i,j}$ $(j = 0, 1, ..., m-1)$, node n_i randomly chooses a node from known nodes within the range $R_{n_i,j}$:

$$R_{n_i,j} = [(T_{n_i,j} - r) \bmod 2^m,\ \ (T_{n_i,j} + r) \bmod 2^m] \tag{2}$$

as shown in Fig. 2 where r is a predefined parameter. Node information that are not chosen are abandoned with priority.

3.1 Safety and communication efficiency

By the proposed method, the overlay network has a basically structured but partially randomized topology. Randomization could lower security risk; Setting r large makes adversarial users difficult to know exact neighbor IDs of a victim node.

Note that other countermeasures are possible to apply together with the proposed method. For example, Ethereum restricts the number of neighbor IP addresses from

[2]Note that in Chord the nearest successor node of the target identifier becomes the corresponding neighbor.

DOI: 10.1587/comex.2021ETL0011
Received January 4, 2021
Accepted January 25, 2021
Publicized February 9, 2021
Copyedited August 1, 2021

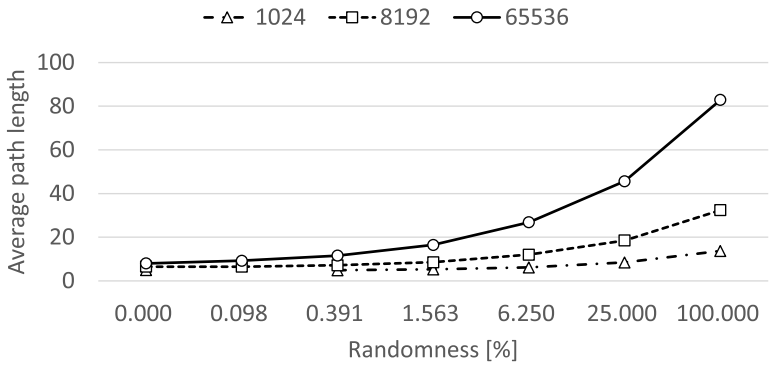

Fig. 3. Trade-off of path length and randomness.

the same subnet to increase the difficulty of Eclipse Attack. Such countermeasures could be introduced into the entry filtering process of the proposed method.

In addition, the semi-structured topology could partly keep the communication efficiency of structured overlays such as path length.

4 Evaluation

To confirm how the parameter r affects the trade-off between safety and efficiency, we conducted an experiment by using a Java-implemented simulator. It generates the given number of nodes and form an overlay network with specified randomness. Here, randomness is the ratio of the number of nodes within the range mentioned in Section 3 to the total number of nodes. It can be approximated by $2r/2^m$ which indicates the ratio of the range size to the identifier space size. The simulator then executes broadcast and calculates the average path length.

Figure 3 shows the result. We simulated three patterns of the number of nodes: 1024, 8192, and 65536.

From the result, high randomness causes longer average path length especially with a large number of nodes. Nevertheless, low randomness such as 1.563% or less does not enlarge the average path length significantly, i.e., the average path length is quite shorter than that of fully random network ($Randomness = 100\%$).

5 Conclusion

In this paper, we proposed a method to exploit semi-structured overlays by using FRT in blockchain systems. Future work includes designing a detailed algorithm and evaluating the security aspect quantitatively.

Acknowledgments

This work was supported in part by Kayamori Foundation of Informational Science Advancement, JSPS KAKENHI Grant Numbers 19K20253, and SECOM Science and Technology Foundation.

DOI: 10.1587/comex.2021ETL0011
Received January 4, 2021
Accepted January 25, 2021
Publicized February 9, 2021
Copyedited August 1, 2021