Evaluation of Security and Performance of Master Node Protocol in the Bitcoin Peer-to-Peer Network

Muntadher Sallal
Nottingham Trent University
School of Computing and Technology
E-mail: muntadher.sallal@ntu.ac.uk

Gareth Owenson
University of Portsmouth
School of Computing
E-mail: Gareth.Owenson@port.ac.uk

Mo Adda
University of Portsmouth
School of Computing
E-mail: Mo.Adda@port.ac.uk

***Abstract*—The mechanism of peers randomly choosing logical neighbors without any knowledge about underlying physical topology can cause a delay overhead in information propagation which makes the system vulnerable to double spend attacks. This paper introduces a proximity-aware extensions to the current Bitcoin protocol, named Master Node Based Clustering (MNBC). The ultimate purpose of the proposed protocol is to improve the information propagation delay in the Bitcoin network.**

***Keywords*—Bitcoin network, Propagation delay, Clustering**

1. Introduction

In the Bitcoin network, the sheer distance between the origin of a transaction or block and other nodes is deemed as the most significant problem in the Bitcoin network. As a result, transaction verification process is slower [1]. Hence, the potential of double spending attacks, that are more difficult to discover in a slow network, increases due to the conflict between nodes regarding the transactions history. Uncertainty regarding the validity of a given transaction causes the blockchain forks where a transaction can appear in two different branches of the blockchain [2]. Aiming at alleviating the propagation delay problem and thereby reduce the possibility of double spending attacks, this paper proposes, implements and evaluates a clustering protocol, named as Master Node Based Clustering (MNBC) with the aim of finding the optimal solution to such problems.

2. Master Node Based Clustering Protocol: Concept and Implementation

Master Node Based Clustering protocol (MNBC) extends the BCBSN protocol that was proposed in our previous work [3], with the aim of addressing security and performance limitations of BCBSN protocol. Specifically, the new protocol, named as Master Node Based Clustering(MNBC), relies on several nodes, known as master nodes, to achieve fully connected clusters based on the physical Internet proximity and random peers selection, where information can be exchanged between clusters via master nodes as well as normal nodes.

2.1. Master Node Selection

Master node role requires gaining a score which is calculated based on how much each node burns bitcoins and how long a node has been online. The main advantage of this approach is that, impersonation of a master node by a malicious node would be challenging. Therefore, this score helps in electing master nodes that are better suited for that role. To incentivises nodes to compete towards winning the master node's role, as it has proven in [4], a reward is given for a master node when it propagates a valid transaction and behaves honestly.

When a particular peer wants to occupy the role of master nodes, the peer invites other peers that connect to it by propagating two types of messages a $masterINV$ and an $AcceptINV$. Consider a node M decides to be a master node and a peer P receives a $masterINV$ from M. On receiving of the $masterINV$ message, the node P accepts $M's$ invitation if it finds the node M to be closer in the physical internet and has a bigger weight than the master node that P is connected to.

2.2. Cluster Maintenance

Let $R\{n_0,n_1,....,n_{i-1}\}$ be a set of peers in the Bitcoin network, where i is the number of total peers. Let $M\{mp_0, mp_1, ..., mp_{j-1}\}$ be a set of master nodes, where j is the number of master nodes and $M \subseteq R$, Let $mp_l\{mp_l, b_0, b_1, ..., b_{k-1}\}$, $(l = 0, 1, ..., j-1)$ and k is the number of peers in the cluster, mp_l be a set of peers in the lth cluster. Therefore, we have $mp_l \subseteq R$ and $R = mp_0 \cup mp_1 \cup ... \cup mp_{j-1}$. When a node z wants to join the Bitcoin network, it first learns about the available master nodes by contacting an arbitrary node T which already have been learnt from DNS service. The node T responds with a list of the master nodes it knows about in the network. The node z selects a master node mp_i such that $\forall mp_j \in M, distance(z, mp_i) \leq distance(z, mp_j)$.

As clusters are fully connected by their edge nodes and master nodes. Therefore, edge nodes will be selected between every pair of clusters. Specifically, let $S = s_1, s_2, ..., s_m$ and $R = r_1, r_2....., r_n$ represent two clusters, and let $[s_b, r_b]$ denote their border nodes, where $s_b \in S$ and

$r_b \in R$, then for all other pairs of clusters (such that $s_i \neq s_b$, $r_j \neq r_b$, $s_i \in S$, $r_j \in R$), $distance(s_i, r_j) \geqslant distance(s_b, r_b)$. Note that $distance(x, y)$ represents the physical internet distance between the two nodes x and y in the network.

3. Performance Evaluation

The information propagation delay will be considered as the main performance metric in the evaluation of the proposed protocol. we simulate our solution on an event based simulator that has been built in [3].

3.1. Experiments setup

The size of the network in each simulation matches the size of the real Bitcoin network which was measured following the same methodology proposed in our previous work [5]. Suppose the client c has proximity based connections (1,2,3,...., n), c propagates a transaction at time T, and it is received by its connected nodes at different times $(T_1, T_2, T_3, ..., T_n)$.

Where $T_n > T_{n-1} > , ..., T_2, T_1$. However, the latency is determined by an average of approximately 1000 runs in order to increase the accuracy of the collected latencies which might be affected by several factors such as data corruption and loss of connection. The time differences between the first transaction propagation and subsequent receptions of the transaction by connected nodes were calculated $(\Delta t_{c,1}, ..., \Delta t_{c,n})$ according to equation(1):

$$\Delta t_{c,n} = T_n - T_c \tag{1}$$

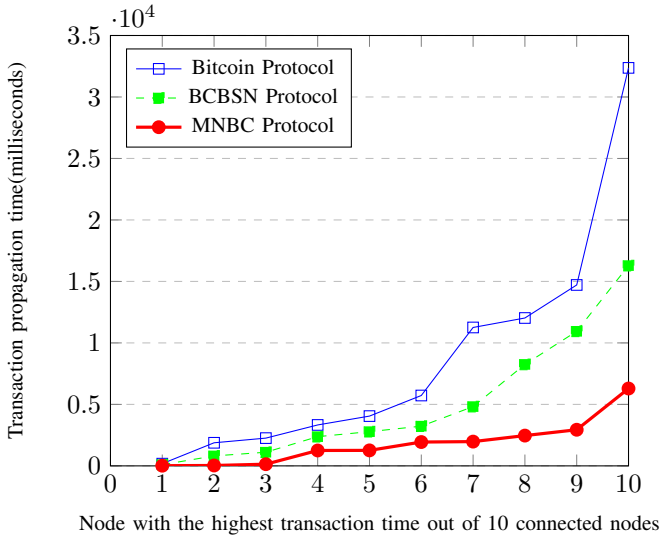

Figure 1: Comparison of the distribution of $\Delta t_{c,n}$ measured in the simulated Bitcoin protocol with MNBC protocol and BCBSN Protocol simulation results.(d_t in MNBC=25ms)

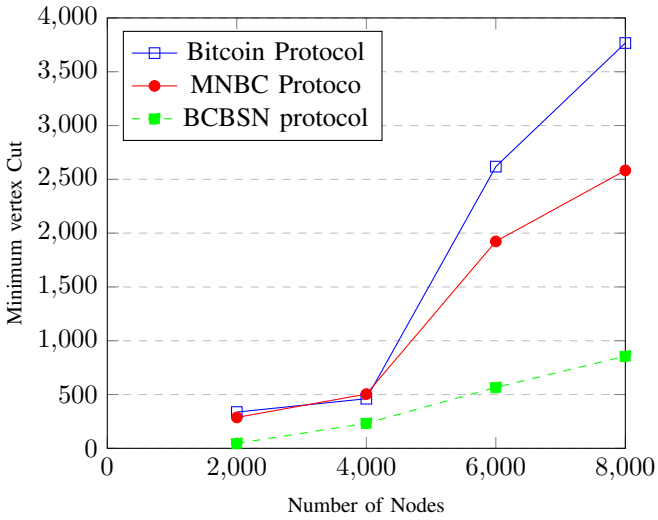

Figure 2: Number of honest peers on the minimum vertex cut

3.2. Results and discussions

Figure 1 compares the distributions of $\Delta t_{c,n}$ for the simulated Bitcoin protocol against the same distributions that have been measured in the simulated proposed protocol MNBC. The simulation results show that the proposed protocol offers an improvement in propagation delay compared to the Bitcoin protocol and BCBSN protocol. The reduction of the transaction propagation time variances in the proposed protocol has to do with the fact that the Bitcoin network layout in which nodes connect to other nodes without taking advantage of any proximity correlations results in a long communication link cost measured by the distance between nodes. The most likely cause of the higher variances of delays in the BCBSN protocol is the fact that the information flow between clusters in BCBSN protocol can only be maintained through supers peers.

4. Security Analysis

The potential of the partition attacks on the MNBC protocol as well as the Bitcoin network and BCBSN protocol [3] is evaluated in this section using the designed simulator. We based our partition attack evaluation on *minimum vertex cut* as a cost metric which is determined at regular intervals using *metis* graph partition toolkits [6]. Evaluation results are shown in Figure 2

5. Conclusion

MNBC evaluation results indicate an improvement in the transaction propagation delay over the Bitcoin network protocol. However, MNBC maintains lower variance of delays over the BCBSN protocol.

References

[1] Stathakopoulou, C.(2015).A faster Bitcoin network. Tech. rep., ETH, Zurich,. SemesterThesis, supervised by Decker.C and Wattenhofer.R.

[2] Sompolinsky, Y., & Zohar, A. (2013). Accelerating Bitcoin's Transaction Processing. Fast Money Grows on Trees, Not Chains. IACR Cryptology ePrint Archive, 2013, 881.

[3] Fadhil, M., Owenson, G., & Adda, M. (2016). A Bitcoin model for evaluation of clustering to improve the transaction propagation delay in Bitcoin network. *In 19th IEEE International Conference on Computational Science and Engineering*. Paris.

[4] Babaioff, M., Dobzinski, S., Oren, S., & Zohar, A. (2012, June). On bitcoin and red balloons. In Proceedings of the 13th ACM conference on electronic commerce (pp. 56-73). ACM.

[5] Fadhil, M., Owenson, G., & Adda, M. (2016). Bitcoin network measurements for simulation validation and parametrisation. *In International networking conference*. Frankfurt/ Germany.

[6] Karypis, G., & Kumar, V. (2016). Metis - Unstructured Graph Partitioning and Sparse Matrix Ordering System, Version 2.0. 1995.