APRP: An Anonymous Propagation Method in Bitcoin Network

Yuhang Yao, Xiao Zeng, Tianyue Cao, Luoyi Fu, Xinbing Wang
{yaoyuhang,ccnn20141227,vanessa_,yiluofu,xwang8}@sjtu.edu.cn
Department of Computer Science and Engineering
Shanghai Jiao Tong University
800 Dongchuan Road, Shanghai, China 200240

Abstract

Due to little attention given to anonymous protection against eavesdropping attacks in Bitcoin network, this paper initiatively proposes a solution to Bitcoin anonymization based on network structure. We first present a general adversarial network model for formulizing deanonymization attack, then present a novel propagation method APRP(Adaptive PageRank Propagation) that adopts PageRank as propagation delay factor and constantly adjusts PR-value of nodes to adapt to network dynamics. Experiments on both simulated and real Bitcoin networks confirm the superiority of APRP in terms of 20-50% performance enhancement under various deanonymization attacks.

Introduction

The anonymity implications of transaction broadcasting were largely ignored until recently, when researchers demonstrated practical deanonymization attacks on the P2P network. In 2015, the Bitcoin community changed its flooding protocol but it has also been proved insufficient (Fanti and Viswanath 2017) and can be deanonymized by maximum-likelihood estimator. To improve anonymity, we propose a novel propagation anonymous method, APRP(Adaptive PageRank Propagation). As far as we know, no previous work provides Bitcoin anonymization method based on network structure.

Our contributions are summarized as follows :

- We propose a general Bitcoin P2P adversarial network model for formulizing deanonymization attack problem in Bitcoin Network and providing optimized objective function.
- We initiatively present a novel propagation anonymous method APRP which detects high impact eavesdropping nodes, brings order to process of transaction message spreading and makes prohibitive cost for eavesdropper.
- We show that APRP has strong and robust performance, which largely reduces the probability of detection under deanonymization attacks on both simulated networks and real Bitcoin networks with different spreading protocols.

Network Model and Problem Formulation

General Adversarial Network Model

We derived a model shown in Figure 1. As the bases of the model, we first consider the P2P network of Bitcoin nodes as a graph $G(V, E)$. Graph G contains 2 types of nodes: eavesdropping nodes V_h and honest nodes V_e. Each server has an exclusive ID (IP address with port). Former work (Miller et al. 2015) shows theoretical analysis can model G_e and G_h as d-regular trees. The message should be initiated from source node $v^* \in V$ and be spread to the whole network.

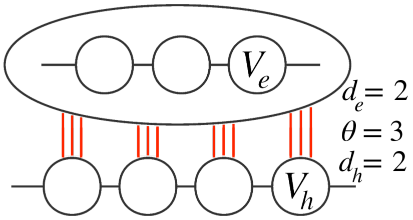

Figure 1: General Adversarial Network Model. Eavesdropping nodes establish θ connection (red edges) to each honest node. Eavesdropping nodes connect as a d_e-regular tree and honest nodes connect as a d_h-regular tree (black edges).

Objective Function

Let v_* denotes the source node of message and let τ_v denotes the timestamp at which attacker first receive message from node $v \in V$. Then we set $\boldsymbol{\tau} = \{\tau_v, \forall v \in V\}$.

The objective of attacker is: Given $\boldsymbol{\tau}$ and G, use deanonymous algorithm $A(\boldsymbol{\tau}, G)$ that maximize $P(A(\boldsymbol{\tau}, G) = v^*)$.

The objective of defender is: Given G, use anonymous algorithm $D(G)$ that minimize $P(A(\boldsymbol{\tau}, G) = v^*|D(G))$.

APRP: Adative PageRank Propagation Model

To break the bottleneck of anonymity, we present a novel method APRP (Adaptive PageRank Propagation) that

- Provides a transaction spreading protocol integrated in Trickle and Diffusion.
- Uses PageRank as propagation delay factor that determine the order of message spreading.

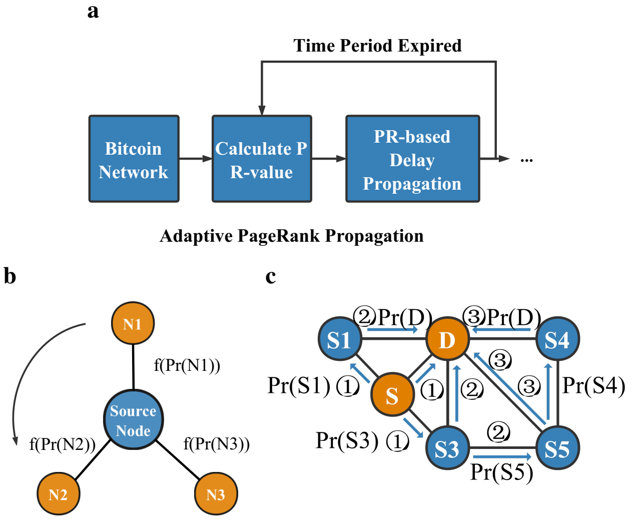

Figure 2: (a) Algorithm Flowchat. **(b)** APRP Algorithm. Pr(n) represents PageRank value of destination node. **(c)** APRP Spreading.

- Constantly adjusts PR-value of nodes to adapt to the changes in the network

The Adaptive PageRank Propagation algorithm, shown in Figure 2, detects high impact eavesdropping nodes and brings order to process of transaction message spreading, which spreads later to nodes with higher PageRank and make propagation paths unpredictable, to effectively makes confusion and prohibitive cost to eavesdroppers.

Experiments

We simulate the spreading experiments[1] on various networks and compare the APRP algorithms APRP(Trickle) and APRP(Diffusion) with baselines: original Trickle and Diffusion, under attack of deanonymous algorithms: FT (First Timestamp) and ML (Maximum Likelihood).

Dataset

We simulate our model in d-regular trees that are verified to be close to the real Bitcoin network that contains 4654 nodes and 18864 edges (Miller et al. 2015). According to the degree distribution shown in Figure 3a, the Bitcoin network is a scale-free network and follows the power law.

Performance Evaluation

We first consider the performance of algorithms on d-regular tree with different tree degree d shown in Figure 3b and Figure 3c. APRP greatly decrease the detection probability, make it approach to 0 and exceeding the best baseline by 20-40%. We then consider the performance with different eavesdropper connections θ over 4-regular trees shown in Figure 3d and Figure 3e. APRP is stable and keeps the detection probability lower than 0.1. Finally, Figure 3f shows estimation over real Bitcoin network. APRP demonstrates strong and robust anonymous performance under various deanonymization attacks.

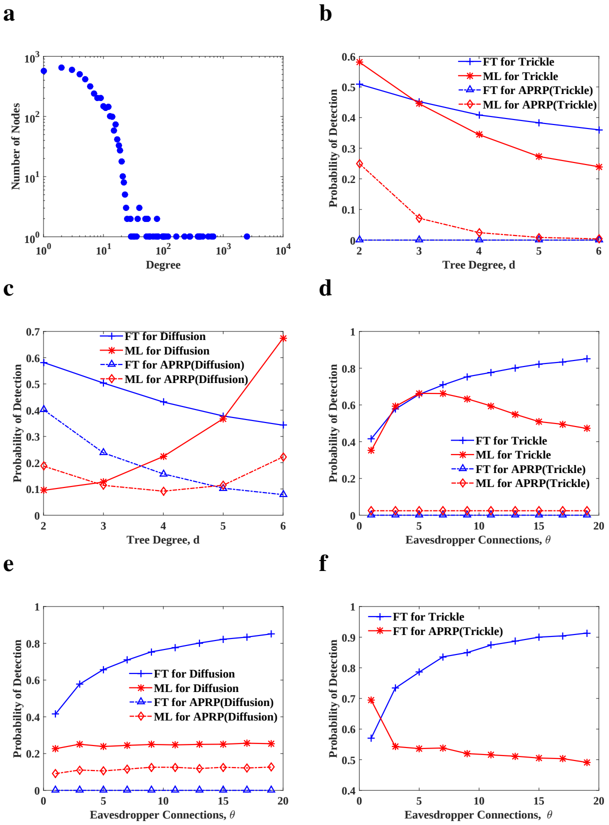

Figure 3: (a) Degree Distribution of real Bitcoin network. **(b)** Trickle vs. APRP(Trickle) estimation on d-regular trees. $\theta = 1$. **(c)** Diffusion vs. APRP(Diffusion) estimation on d-regular trees. $\theta = 1$. **(d)** Diffusion vs. APRP(Diffusion) estimation on 4-regular trees. **(e)** Diffusion vs. APRP(Diffusion) estimation on 4-regular trees. **(f)** Accuracy estimation over real Bitcoin network.

Acknowledgments

This work was supported by National Key R&D Program of China 2018YFB1004705, NSF China under Grant 61822206, Grant 61532012, Grant 61602303, Grant 61829201, CCFTencent RAGR 20180116, and Open Research Fund of Tianjin Key Laboratory of Advanced Networking (TANK).

References

Fanti, G., and Viswanath, P. 2017. Deanonymization in the bitcoin p2p network. In *Advances in Neural Information Processing Systems*, 1364–1373.

Miller, A.; Litton, J.; Pachulski, A.; Gupta, N.; Levin, D.; Spring, N.; and Bhattacharjee, B. 2015. Discovering bitcoin's public topology and influential nodes.(2015).

[1] Code available at https://github.com/APRPmaster/APRP-master