Wenbo ZHANG, Tao WANG, Chaoyang ZHANG, Jingyu FENG, 2024. Securing multi-chain consensus against diverse miner behavior attacks in blockchain networks. *Frontiers of Information Technology & Electronic Engineering*, 25(4):540-554. https://doi.org/10.1631/FITEE.2200505

Securing multi-chain consensus against diverse miner behavior attacks in blockchain networks

Key words: Blockchain; Cross-chain; Trust mechanism; Multi-chain consensus

Corresponding author: Jingyu FENG
E-mail: fengjy@xupt.edu.cn
ORCID: https://orcid.org/0000-0002-5353-3295

Motivation

1. Most consensus schemes are based on a single-chain mode and universal trust evaluation. This may provide opportunities for malicious users in a multi-chain consensus scheme. When there are multiple chains in a blockchain network, some miners may exist on all chains so that they can simultaneously process different businesses on different chains. Once these users are attacked or even hijacked, it is possible for malicious users to launch diverse miner behavior (DMB) attacks on different chains.

2. DMB attacks have a serious impact on the secure and stable operation of blockchain.

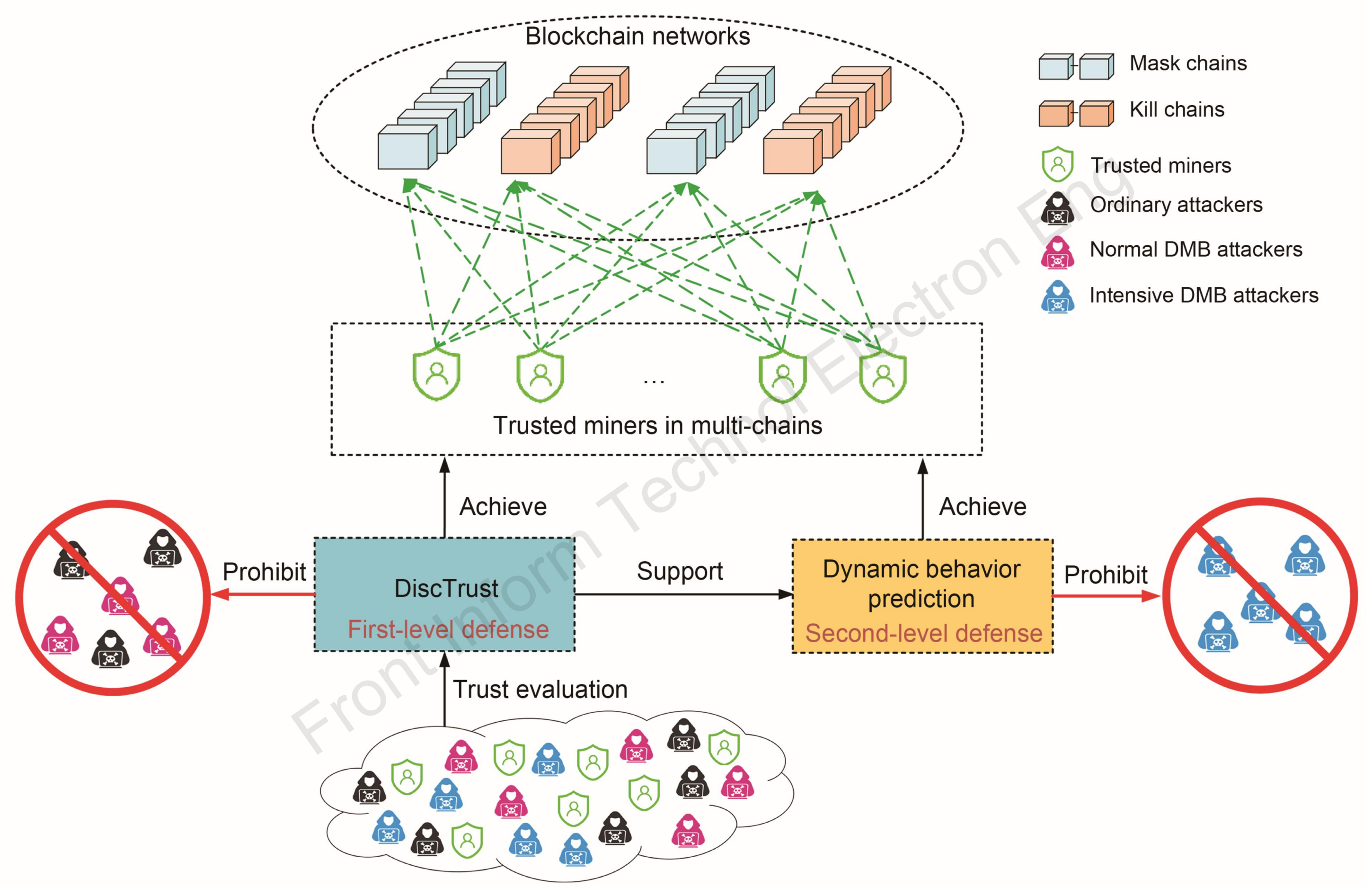
Main idea

1. According to the strategy of DMB attacks, the chains in the network can be divided into kill chains and mask chains. They can be friendly in the consensus process of mask chains to enhance their trust value and maintain honest miners, while in kill chains they engage in behaviors that undermine the consensus process.

2. An idea of distinctive trust (DiscTrust) is introduced to evaluate the trust value of each user across different chains. The trustworthiness of a user is split into local and global trust values. The evaluation of the local trust value for a user is bound to each chain. A multi-chain consensus scheme called Proof-of-DiscTrust (PoDT) is proposed to defend against DMB attacks.

3. A dynamic behavior prediction (DBP) scheme based on DiscTrust is proposed. Because support vector machine (SVM) is highly accurate and fast in dichotomy prediction, it is well suited to DBP to predict a user’s dynamic behavior on a kill chain.

Framework

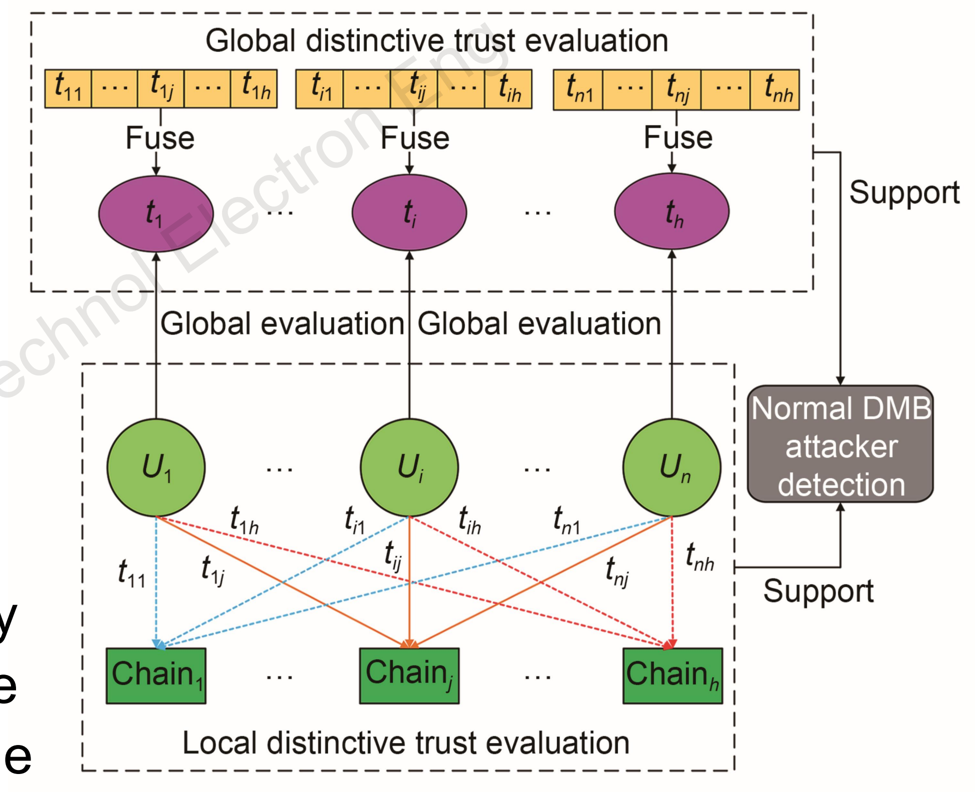


Overview of Proof-of-DiscTrust (PoDT), which includes two levels of defense: first-level defense, DiscTrust; second-level defense, dynamic behavior prediction

Method

In first-level defense, DiscTrust divides a user's trust value into a global trust value and local trust values. Although the global trust value of normal DMB attackers is higher than the threshold, their local trust values in kill chains will be lower than the threshold.

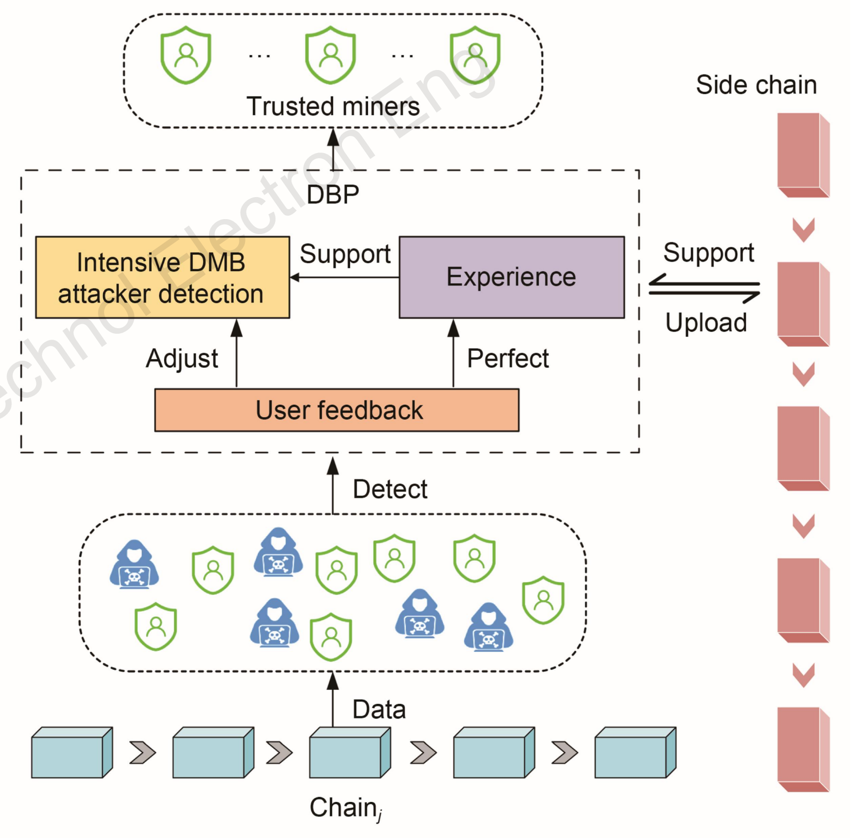
Therefore, DiscTrust can effectively detect normal DMB attackers. If the global trust value is smaller than the threshold, DiscTrust can also be used to detect ordinary attackers.


Global distinctive trust evaluation
t_{11} ⋯ t_{1j} ⋯ t_{1h}
t_{i1} ⋯ t_{ij} ⋯ t_{ih}
t_{n1} ⋯ t_{nj} ⋯ t_{nh}
Fuse
Fuse
Fuse
t_1 ⋯ t_i ⋯ t_h
Support
Global evaluation
Global evaluation
Normal DMB attacker detection
U_1 ⋯ U_i ⋯ U_n
t_{11}
t_{1j}
t_{1h}
t_{i1}
t_{ij}
t_{ih}
t_{n1}
t_{nj}
t_{nh}
Support
Chain_1 ⋯ Chain_j ⋯ Chain_h
Local distinctive trust evaluation

Functional modules in the DiscTrust scheme

Method

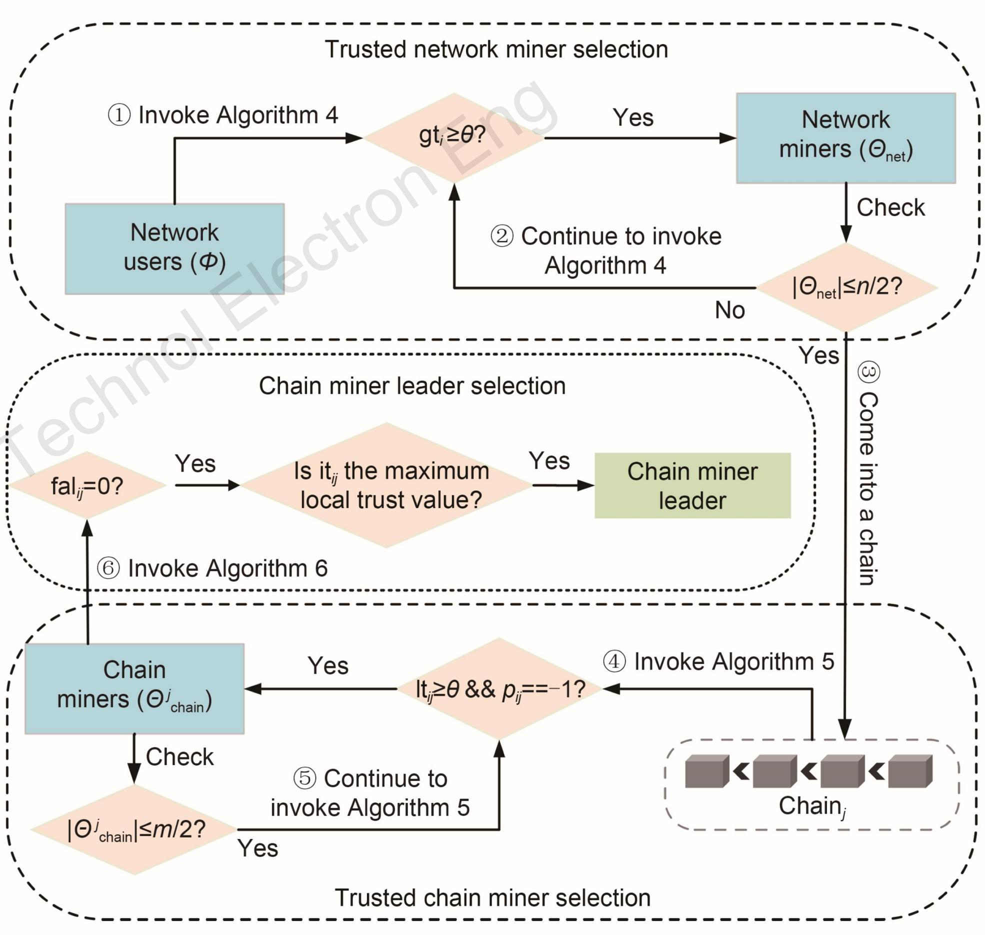
The second-level defense can collect the dynamic changes of the local and global trust values of users, and the proposed DBP scheme can be used to detect intensive DMB attackers and prevent kill chains from becoming their victims.



Architectural overview of DBP

Method

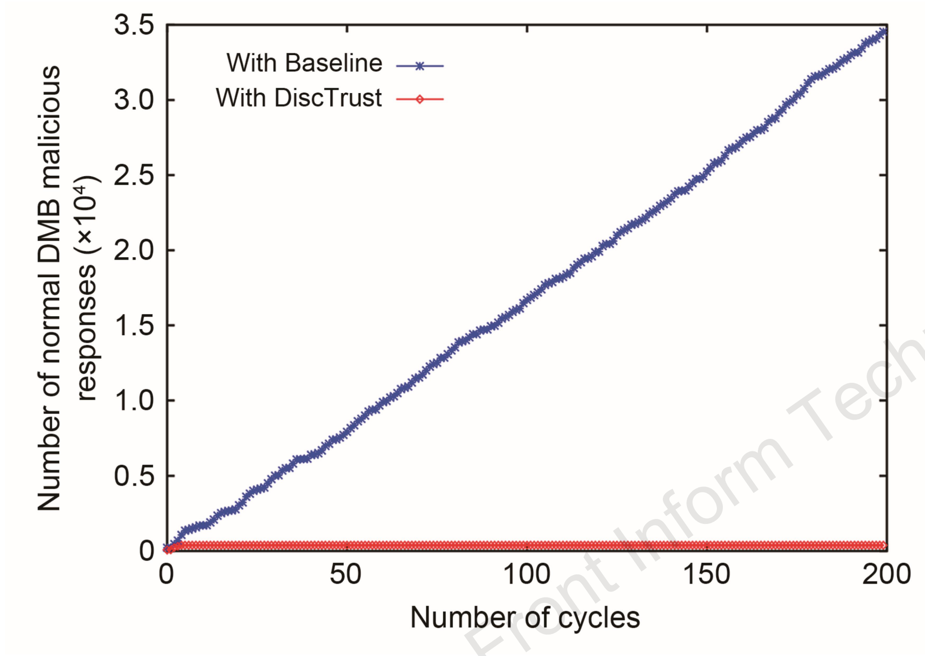
Three algorithms are designed to select trusted miners for a multi-chain environment. The global trust value is used to design the algorithm for the selection of trusted network miners. Only after a user has been selected as a network miner, will he/she be eligible for selection as a chain miner who has the authority to create blocks in the consensus scheme.

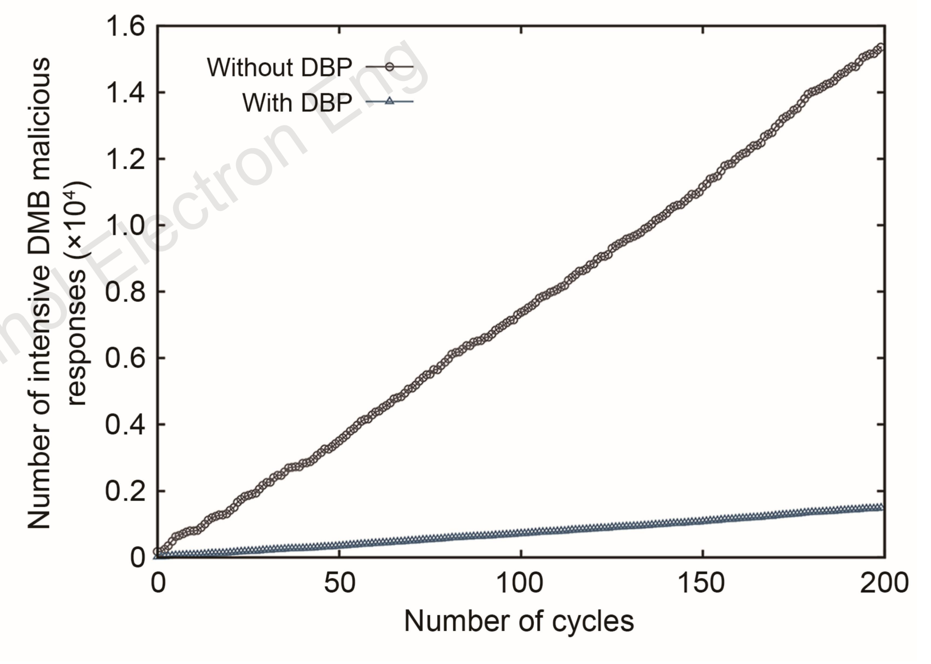


Trusted network miner selection
① Invoke Algorithm 4
$gt_i \geq \theta$?
Yes
Network miners (Θ_{net})
Network users (Φ)
Check
② Continue to invoke Algorithm 4
$|\Theta_{net}| \leq n/2$?
No
Yes
③ Come into a chain
Chain miner leader selection
$fal_{ij}=0$?
Yes
Is it_{ij} the maximum local trust value?
Yes
Chain miner leader
⑥ Invoke Algorithm 6
Chain miners (Θ^j_{chain})
Yes
$lt_{ij} \geq \theta$ && $p_{ij}==-1$?
④ Invoke Algorithm 5
Check
⑤ Continue to invoke Algorithm 5
$|\Theta^j_{chain}| \leq m/2$?
Yes
Chain_j
Trusted chain miner selection

Process of trusted miner selection

Major results

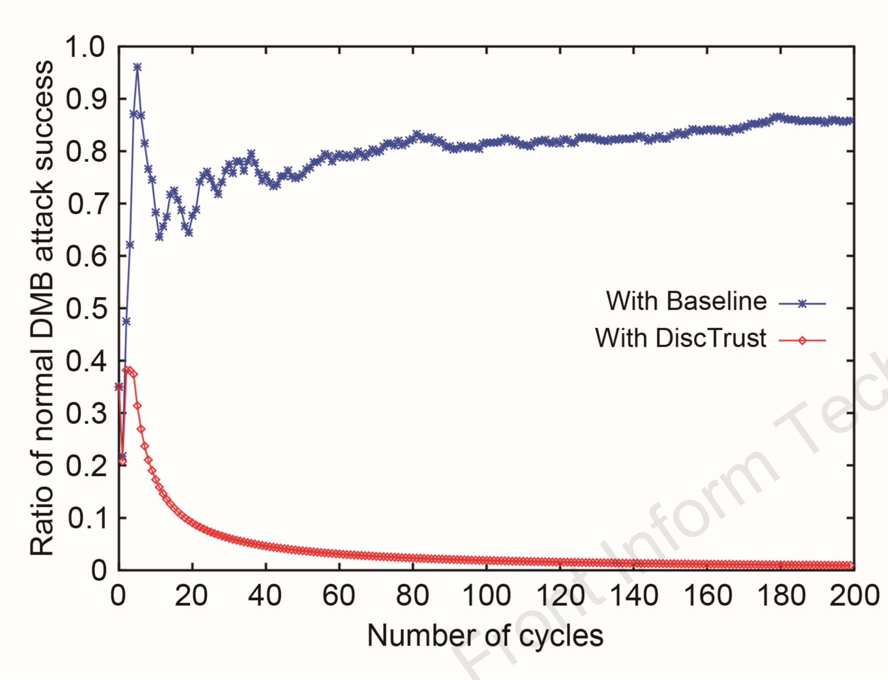




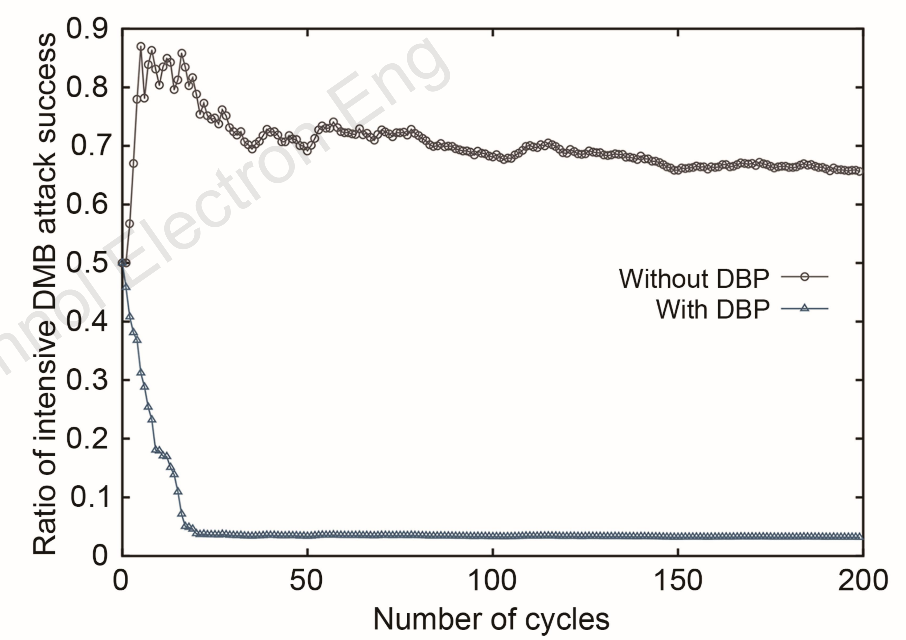
Suppressing normal diverse miner behavior (DMB) malicious responses

Suppressing intensive diverse miner behavior (DMB) malicious responses

Major results



Normal diverse miner behavior (DMB) attack success ratio



Intensive diverse miner behavior (DMB) attack success ratio

Conclusions

1. We proposed an advanced consensus scheme named PoDT for multiple chains to defend against DMB attacks in blockchain networks.

2. DiscTrust was introduced to detect normal DMB attackers with the help of local trust values. The DBP scheme can strengthen DiscTrust to detect intensive DMB attackers.

3. Experimental results showed that PoDT is secure against DMB attacks in multi-chain environments and more effective in terms of block creation.