Wang *et al. J Surveill Secur Saf* 2023;4:180-95
DOI: 10.20517/jsss.2023.34

Journal of Surveillance, Security and Safety

Original Article

Open Access

EFAW: a new mining attack model combining FAW attacks with the Eclipse attack

Jing Wang, Zihao Wang

School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin 541004, Guangxi, China.

Correspondence to: Prof.Jing Wang, School of Computer Science and Information Security, Guilin University of Electronic Technology, Jinji Road No.1, Qixing District, Guilin 541000, Guangxi, China. E-mail: wjing@guet.edu.cn

How to cite this article: Wang J, Wang Z. EFAW: a new mining attack model combining FAW attacks with the Eclipse attack. *J Surveill Secur Saf* 2023;4:180-95. http://dx.doi.org/10.20517/jsss.2023.34

Received: 26 Oct 2023 **First Decision:** 20 Nov 2023 **Revised:** 4 Dec 2023 **Accepted:** 8 Dec 2023 **Published:** 21 Dec 2023

Academic Editor: Leandros Maglaras **Copy Editor:** Dong-Li Li **Production Editor:** Dong-Li Li

Abstract

Aim: The Proof-of-Work consensus mechanism is the core mechanism of the blockchain, but the existing Fork After Withholding (FAW) attack can earn more rewards by launching attacks on the mining pools under the Proof-of-Work consensus mechanism. This paper proposes a new attack model based on the FAW attack, which further increases the attacker's reward to explore the impact of the attack method on the blockchain network and the losses caused by the attack, which is helpful for maintaining the blockchain.

Methods: This paper proposes a new mining attack model called the "Eclipse Fork After Withholding (EFAW) attack" by combining FAW attacks with the eclipse attack. In the EFAW attack, the attacker infiltrates the victim pool by dispatching infiltrator miners. At the same time, they isolate a portion of miners in the victim pool through eclipse attacks, intercepting the valid information transmitted by these isolated miners. The attacker selectively discards or strategically releases the information to gain extra rewards.

Results: In this paper, we launch an EFAW attack against a single mining pool and two mining pools, respectively, and evaluate the relative extra rewards of the attacker with theoretical analysis and Monte Carlo simulation experiments. Our experimental data indicate that this attack can earn more rewards than FAW attacks.

Conclusion: The experimental results demonstrate that the lower bound of earnings in the EFAW attack is higher than in FAW attacks, and it is directly proportional to the number of miners isolated by the attacker's eclipse attack in the victim pool. This indicates that the EFAW attack poses a greater threat compared to FAW attacks, representing

one of the major conclusions drawn from the study.

Keywords: Bitcoin, mining, Fork After Withholding attack, Eclipse attack

1. INTRODUCTION

As a cryptocurrency based on blockchain technology, the core of Bitcoin [1] is based on encryption and peer-to-peer (P2P) network technology, and it is constantly facing new challenges in terms of security [2,3]. By solving the undifferentiated hash of the problem by the participants (miners), the decentralized distributed ledger of the "bookkeeper" is determined by the computing power possessed by the miner. Unlike traditional centralized ledgers, all participants in the blockchain are synchronized and record the transactions of the entire system together, thus ensuring that the transactions in the system are difficult to tamper with. Because each miner has the same status, when multiple miners generate blocks at the same time, it causes a fork in the blockchain system [4]. To reach consensus among miners, a consensus mechanism called Proof-of-Work (PoW) is applied in Bitcoin [5,6]. Whenever a miner finds a PoW, they broadcast and add the blocks they find to the blockchain to earn a reward from the system. As the collective computing power of all miners in the Bitcoin system continues to increase, to reduce the variance of miners' earnings, miners cooperate to form mining pools [7]. Within these pools, participating miners search for proof-of-work for candidate blocks and earn rewards based on their mining contributions. Most mining pools today set a low-difficulty goal for the miners, usually more than 1,000 times less difficult than the Bitcoin network [8]. For results that meet the low difficulty requirements but do not meet the Bitcoin network, we call it Partial PoW (PPoW), and results that meet both are called Full PoW (FPoW). When someone in the pool successfully mines a piece, the pool earns a reward, and the pool manager distributes the reward based on each miner's contribution to the pool (PPoW and FPoW).

Since Bitcoin comes with a monetary value, it is naturally a target for attackers. Although it was designed with security in mind, various attack tactics against Bitcoin are gradually being proposed. We broadly divide them into two categories: attacks against the underlying network and attacks on Bitcoin's protocol. The Bitcoin system is based on the P2P network, and among the attacks against this network, DDoS attacks [9] and eclipse attacks are the two most typical attack strategies, destroying the system from the network communication layer, thereby causing a series of security problems. The DDoS attack [10] is carried out through computer networks connected to the Internet, which are infected with malware and thus controlled remotely by the attacker, constantly sending a large amount of meaningless information to the victim and disrupting the victim's communication with the outside world. The eclipse attack was proposed in 2015 by de Asís López-Fuentes *et al.* and utilizes the main principle that there is an upper limit on the number of connections per node in the Bitcoin network [11]. Although Zheng *et al.* [12], Alangot *et al.* [13], and other researchers have proposed some detection methods for eclipse attacks, attackers can use eclipse victim nodes to carry out some illegal activities in some scenarios [14], enabling them to reap benefits from these actions.

In addition, attacks on the Bitcoin protocol itself pose a greater threat to the Bitcoin system. Among them, the more classic ones are selfish mining, block withholding (BWH) attacks, and fork after withholding (FAW) attacks. Eyal *et al.* first proposed the concept of selfish mining, where attackers do not immediately broadcast a block in the Bitcoin network after mining [15]. Instead, they choose to continue mining secretly after discovering a block and selectively publish the found block according to a certain strategy, intentionally causing a fork in the Bitcoin system. The BWH attack was first proposed by Rosenfeld [16], and research at the time saw it as a form of attack that harmed others. Later, new BWH attack models were proposed [17–19], indicating that attackers can increase their rewards by launching block interception attacks. When two pools launch block interception attacks on each other, we are surprised to find that both pools are rewarded less than honest mining, which we call the "miner's dilemma" [20] problem. The FAW attack [21] then came up with the idea

of combining selfish mining with the BWH attack. In an FAW attack, the FPoW submitted by the infiltrated miner is retained by the attacker, and when an external honest miner (who is neither part of the attacker nor the target pool) finds a valid block, the attacker immediately announces the retained FPoW to fork. Compared with BWH attacks, FAW attacks can additionally gain the part of the attacker's rewards that is selected as the main chain, so FAW attacks will always gain additional rewards, and not less than the rewards of BWH attacks. Not only that, but the FAW attack also solved the "miner's dilemma"[22,23] problem. Since then, diverse attack methods, such as Stubborn mining[24], Selfholding attacks[25], GenSelfHolding attacks[26], and so on, have been proposed, which are all combinations of different types of attacks and can earn more rewards.

In this paper, based on the original FAW attack strategy, we introduce eclipse attacks against the network layer and propose a new attack model. We focus on the rewards when an attacker launches an Eclipse Fork After Withholding (EFAW) attack against a single honest pool and two honest pools, respectively. Our contributions are as follows:

- We propose a new combined attack model by combining FAW attacks against the Bitcoin protocol with the eclipse attack at the blockchain network layer;
- Through theoretical analysis, we give the expected reward expression of the attacker in the scenario of the EFAW attack against a single mining pool and two mining pools and prove that the attacker's actual reward is consistent with the theoretical value through simulation experiments;
- We compare the rewards of the EFAW attack with FAW attacks, proving that attackers always earn more rewards by launching EFAW attacks, and the lower limit is FAW attacks.

The remainder of this paper is structured as follows. Section 2 provides an overview of related work. In Section 3, we describe the attack overview and assumptions of the EFAW attack model in detail. In Sections 4 and 5, we analyze the impact of launching EFAW attacks against a single mining pool and two mining pools, respectively, and provide the expected rewards and simulation experiment results. In Section 6, we discuss the feasibility, cost, and future scope of the EFAW attack. Finally, we summarized the full text in Section 7.

2. RELATED WORK

In this section, we review the most classic mining attacks, including selfish mining, BWH attacks, FAW attacks, and network-level eclipse attacks.

Selfish mining: In a selfish mining attack, the attacker gains extra rewards by delaying the broadcast of found blocks and maintaining a hidden private branch to create forks in the system. When the attacker discovers a new block, they do not broadcast it immediately but continue mining on top of that block. When other honest miners find the new block and broadcast it, the attacker can selectively reveal multiple blocks from their private chain, causing a fork. If the attacker's private chain becomes the main chain chosen by the system, blocks mined by other miners become orphan blocks, and their efforts are discarded, while the attacker earns extra rewards[27] for successfully causing a fork. After Eyal *et al.* introduced the concept of selfish mining[15], many researchers conducted further studies and optimizations to maximize the rewards of selfish mining[28,29].

BWH attacks: In this attack, the attacker divides their computational power into two parts: one part is used as infiltrating power to join a victim pool, while the other part continues to operate as honest mining power to earn rewards. The infiltrating power in the victim pool does not submit the PPoWs and FPoWs to the pool manager in the same manner as ordinary honest mining power. Instead, it only submits PPoWs to earn rewards while discarding any found FPoWs. The BWH attack "wastes" the attacker's computational power, preventing the victim pool from receiving the expected rewards corresponding to their computational power. Additionally, the reward of honest miners in the pool is also diminished as the attacker claims a portion of their rewards, thus reducing the actual earnings of honest miners.

FAW attacks: At the beginning of the attack, as with the BWH attack, an attacker divides his computational power between honest mining and infiltration mining. When an infiltration miner finds an FPoW in the victim pool, the attacker retains the FPoW instead of committing it immediately. When other honest miners discover a new block, the attacker will submit the previously reserved FPoW to the manager to let the pool broadcast a new block at the same time, deliberately causing the blockchain to fork. Therefore, the rewards of an FAW attack are greater than or equal to the reward of BWH attacks (when the attacker's branch fails to be selected as the main chain, the reward of an FAW attack is the same as the reward of BWH attacks). Then, the researchers propose a new attack strategy[30] to further increase the rewards of the attackers.

Eclipse attacks: Nodes in the blockchain system have two link tables, tried and new. The attacker fills the node addresses he controls into the tried table of the victim node and continuously fills invalid address information into the new table. Eventually, all 117 inbound nodes and eight outbound nodes of the victim node will be replaced by nodes controlled by the attacker, thereby controlling all incoming and outgoing information of the victim node, effectively isolating it from the blockchain system. This type of attack can be successfully applied to mainstream blockchain networks such as Bitcoin and Ethereum[31]. Despite the various vulnerability patches implemented in blockchain systems to mitigate early eclipse attacks, the impact on Bitcoin nodes by network attacks utilizing a large number of network address resources remains feasible.

3. ATTACK OVERVIEW AND ASSUMPTIONS

3.1. Attack overview

We combine FAW attacks with the eclipse attack to propose a new attack model called EFAW attacks. The attacker dispatches his computational power into two parts: honest mining and infiltration mining. The attack behaviors of these two parts of computational power are the same as in FAW attacks. At the same time, the attacker launches an eclipse attack on the nodes within the victim pool to gain control over the information of these affected nodes (including both incoming and outgoing data). The purpose of the attack is to control the PoWs submitted by these affected nodes. For a PPoW, the attacker has the option to choose not to include it in the consensus process. This means that the workload submitted by that node will not be accepted and confirmed by other nodes, thereby increasing the attacker's share of rewards from the infiltration computational power within the victim pool. For an FPoW, the pool manager retains it and strategically releases it to create a branch in the system for additional rewards. This paper proposes an EFAW attack model for a single pool and two pools, provides an expression of the expected reward, and compares it with the original FAW reward. Next, we will provide a detailed description of this attack tactic.

3.2. Attack overview

To simplify our analysis, we made some reasonable assumptions about the variables in the experiment.

- We have normalized the total computational power in the entire blockchain system to 1, and the computational power of any participant is necessarily less than 1;
- The computing power of any miner or pool in the system must be less than 0.5 to avoid the possibility of a "51% attack" in the network;
- There is only one attacker in the system, and there is no hybrid model of multiple attacks or any other form of attack other than EFAW attacks;
- We have standardized the actual reward for each valid block to 1 instead of using the current system's actual reward of 12.5 Bitcoins, and we represent it in terms of expected probabilities;
- In this system, unintentional forks do not exist. Moreover, the probability that a miner will find a valid block is equal to its normalized computing power;
- The pool manager broadcasts the block generated by the miner in the network, and if a block is successfully added to the main chain and confirmed, then the pool will earn a reward for the response. Finally, the manager will distribute the rewards based on the number of shares (FPoWs and PPoWs) submitted by each

Table 1. List of notations

Notation	Descriptions
α	The total computational power of the attack pool A
β	Computational power of the victim pool B
τ	The proportion of the attacker's infiltration mining computational power ($\tau\alpha$ as part of α)
q	Computational power of eclipsed miners as a proportion of β
c	The probability that FPoW submitted by an infiltration miner or eclipsed miner will be chosen as the main chain (two-branch case)

FPoW: Full Proof-of-Work.

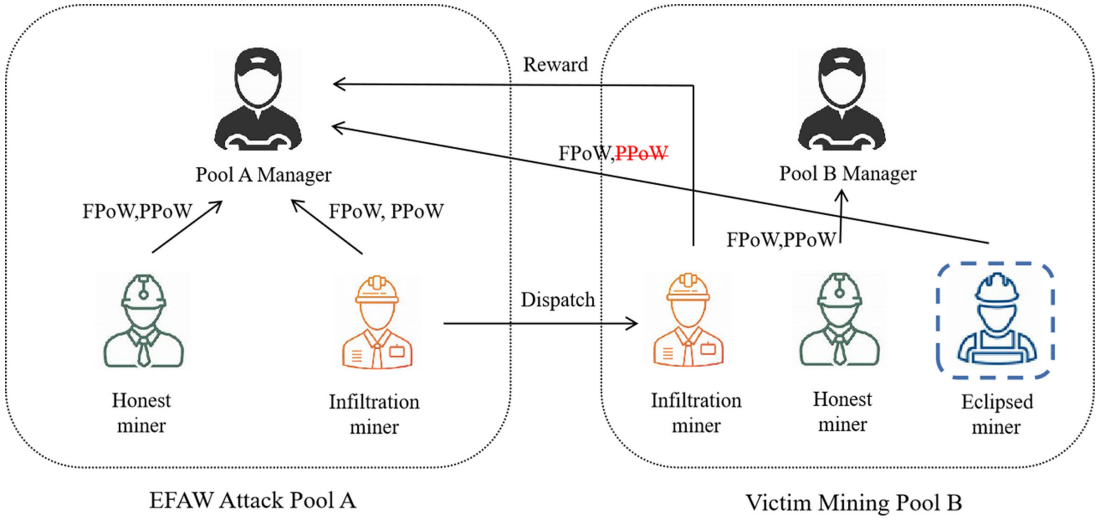

Figure 1. EFAW attacks against a single mining pool. The left is the EFAW attack pool A, and the right is the victim mining pool B. EFAW: Eclipse Fork After Withholding; FPoW: Full Proof-of-Work; PPoW: Partial Proof-of-Work.

miner in this round.

4. THE EFAW ATTACK AGAINST ONE POOL

In this section, we will introduce the EFAW attack model against a single victim pool and detail how to combine these two attack methods in a specific model. Finally, we have theoretically and quantitatively analyzed the optimal behavior and maximum rewards of launching an EFAW attack against a single mining pool.

4.1. Theoretical Analysis

The model for the attacker launching an EFAW attack against an honest mining pool is depicted in Figure 1. The model includes two mining pools: pool A is the attack pool, and pool B is the victim pool. The manager of pool A divides their computational power into two parts: one part is used for honest mining, and the other part is dispatched as infiltrating miners in pool B. At the same time, pool A launches the eclipse attack on pool B; those miners who are controlled by pool A are called eclipsed miners. Note that honest miners and infiltrator miners in pool A submit FPoWs and PPoWs to pool A's manager. However, the FPoWs and PPoWs submitted by the eclipsed miners are also controlled by the pool A manager. The manager immediately publishes the FPoW submitted by honest miners, discards the PPoWs submitted by eclipsed miners, and retains the FPoWs submitted by infiltrator miners and eclipsed miners. The specific strategies will be detailed in this section, with the relevant parameters listed in Table 1.

In this case, the attacker allocates $1 - \tau\alpha$ computational power for honest mining in their mining pool and $\tau\alpha$ computational power for infiltrating mining in the victim pool. The computational power of the victim

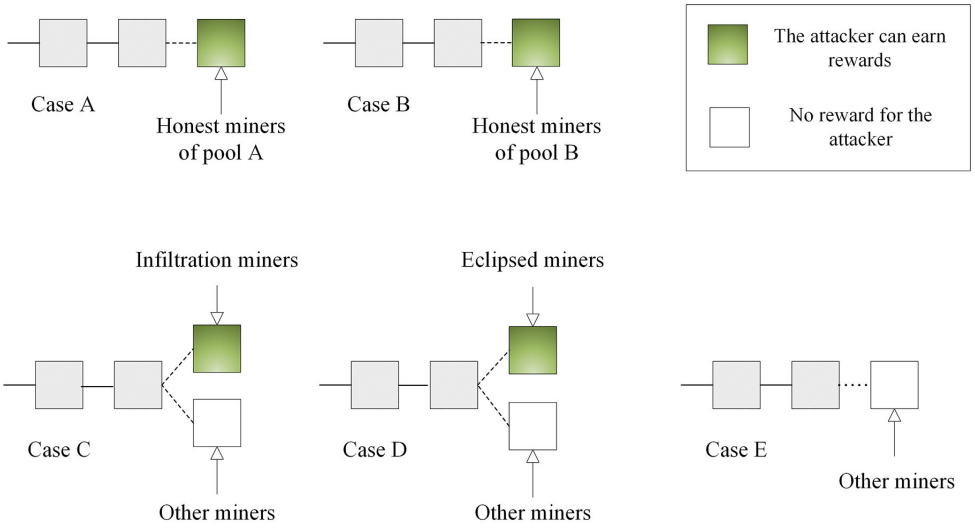

Figure 2. The possible consequences of an EFAW attack against a single mining pool. The green blocks represent the attacker can earn rewards, so he can earn rewards in four cases: Cases A-D. EFAW: Eclipse Fork After Withholding.

pool is denoted as β (excluding the infiltrating computational power), including the computational power of the eclipsed miners, denoted as $q\beta$. The parameter c is closely related to the network capabilities of both the attacker and the Bitcoin network's topology[32]. It is a coefficient that accounts for the relationship between the attacker's network capabilities and the topology of the Bitcoin network.

Firstly, we analyze the attack pool A, where neither the infiltration miners nor the eclipsed miners find an FPoW. At this point, when an honest miner finds an FPoW, the manager immediately submits the FPoW. Three cases will occur when the infiltration miner or the eclipsed miner finds an FPoW: (1) If the honest miner from pool A finds an FPoW, the pool A manager will discard the FPoW found by the infiltration miner or the eclipsed miner; (2) If the honest miner from pool B finds an FPoW, the manager will also discard the FPoW found by the infiltration miner or the eclipsed miner; (3) If another honest miner submits a valid block, the manager immediately submits the retained FPoW, resulting in a fork in the Bitcoin network. This action is part of the EFAW attack strategy to disrupt the consensus and potentially gain extra advantages or rewards for pool A.

In conclusion, when an attack launches the EFAW attack against a victim pool, there can be five possible cases in the Bitcoin network, and the total probability of these five cases sums up to 1 [Figure 2]. Next, we analyze the reward for the EFAW attack strategy and give the expected reward expression for pool A.

Theorem 4.1. The rewards that the attack pool A can earn by launching an EFAW attack against pool B:

$$R_A = \frac{(1-\tau)\alpha}{1-\tau\alpha-q\beta} + \left(\frac{(1-q)\beta}{1-\tau\alpha-q\beta} + c(\tau\alpha+q\beta)\cdot\frac{1-\alpha-\beta}{1-\tau\alpha-q\beta}\right)\cdot\frac{\tau\alpha}{(1-q)\beta+\tau\alpha} \tag{1}$$

Proof: Firstly, the attack pool A can earn block rewards through honest mining and infiltration mining. As shown in Figure 2, when an honest miner in pool A submits a valid block, they earn the full reward, and the probability is $\frac{1-\tau\alpha}{1-\tau\alpha-q\beta}$ (Case A in Figure 2). The PPoWs submitted by the eclipsed miners are discarded by the attacker; this part of the computational power cannot earn a reward. Therefore, the reward ratio that the attack pool A can earn when the victim pool B submits a valid block is $\frac{\tau\alpha}{1-q\beta+\tau\alpha}$. Three cases can happen, as shown in Cases B-D: The reward that the attacker can earn is $\frac{(1-q)\beta}{1-\tau\alpha-q\beta}\cdot\frac{\tau\alpha}{1-q\beta+\tau\alpha}$ (Case B in Figure 2). The

attacker submits that the FPoW found by an infiltration miner generates a fork in the system, and the FPoW the attacker submitted is selected as the main chain. At this point, the reward is $c\tau\beta \cdot \frac{1-\alpha-\beta}{1-\tau\alpha-q\beta} \cdot \frac{\tau\alpha}{1-q\beta+\tau\alpha}$ (Case C in Figure 2). The attacker submits the FPoW found by the eclipsed miner to generate a fork, and the FPoW is selected as the main chain. The reward is $cq\beta \cdot \frac{1-\alpha-\beta}{1-\tau\alpha-q\beta} \cdot \frac{\tau\alpha}{1-q\beta+\tau\alpha}$ (Case D in Figure 2). Therefore, the attacker's rewards can be expressed in Equation (1).

To maximize the reward, the attacker will reasonably allocate her computational power to infiltration miners and honest miners. We set the ratio of computing power for R_A maximization to $\overline{\tau}$, and we can obtain the optimal $\overline{\tau}$ by solving this equation $\frac{\partial R_A}{\partial \tau} = 0$.

Theorem 4.2. The reward of the EFAW attack is greater than or equal to FAW attacks, and when the eclipse attack does not isolate the victim pool's miner nodes, the EFAW attack will degrade into an FAW attack.

Proof: Compared to the FAW attack, the key feature of the EFAW attack is the combination of eclipse attacks. Control the network view of some nodes and use the computing power of these nodes to illegally mine for more rewards. Firstly, since the PPoWs submitted by the eclipsed nodes are discarded by the pool A manager, the reward for miners in pool A who participate in infiltration mining increases. Secondly, the attacker will strategically release the FPoW submitted by the eclipsed miner to create forks in the blockchain. If the block wins in the competition, the infiltration miners earn more rewards in pool B. Therefore, the reward for launching an EFAW attack is higher than for an FAW attack. However, when the attacker has not controlled miner nodes by the eclipse attack, the reward for the EFAW attack is equal to the reward for the FAW attack.

As described in Theorem 4.2, the attacker can earn more rewards by combining FAW attacks with the eclipse attack, and this extra reward comes from the victim pool B. Next, we analyze the loss of rewards from the victim pool B and give the expected reward expression.

Theorem 4.3. The rewards that the victim pool B can earn under the EFAW attack strategy:

$$R_B = \left(\frac{(1-q)\beta}{1-\tau\alpha-q\beta} + c(\tau\alpha+q\beta) \cdot \frac{1-\alpha-\beta}{1-\tau\alpha-q\beta}\right) \cdot \frac{(1-q)\beta}{(1-q)\beta+\tau\alpha} \tag{2}$$

Proof: The victim pool B can be rewarded in the following three cases. In the first case, an honest miner in pool B finds a valid block with a probability of $\frac{(1-q)\beta}{1-\tau\alpha-q\beta}$. In the second case, the valid block submitted by an infiltration miner wins the competition with a probability of $c\tau\alpha \cdot \frac{1-\alpha-\beta}{1-\tau\alpha-q\beta}$. In the third case, the block submitted by an eclipsed miner is chosen as the main chain with a probability of $cq\beta \cdot \frac{1-\alpha-\beta}{1-\tau\alpha-q\beta}$. Since the PPoWs submitted by the eclipse victim miners are discarded by the manager of pool A, the proportion of rewards that pool B can earn is $\frac{(1-q)\beta}{(1-q)\beta+\tau\alpha}$. Thus, the expected reward of pool B is shown in Equation (2).

4.2. Quantitative analysis and simulation

To analyze the reward of the attack pools A and B, we introduce a relative extra reward (RER) under the EFAW attack model on a single mining pool, defined as the ratio of extra reward to honest mining reward. Pool A can be represented by Equation (3) and pool B by Equation (4). RER_h represents the reward earned by the pool for honest mining. It is worth noting that when RER is negative, it means that the pool's reward is lower than that of honest mining under this attack model.

$$RER_A^{'} = \frac{RER_A - RER_{\mathrm{h}}}{RER_{\mathrm{h}}} \tag{3}$$

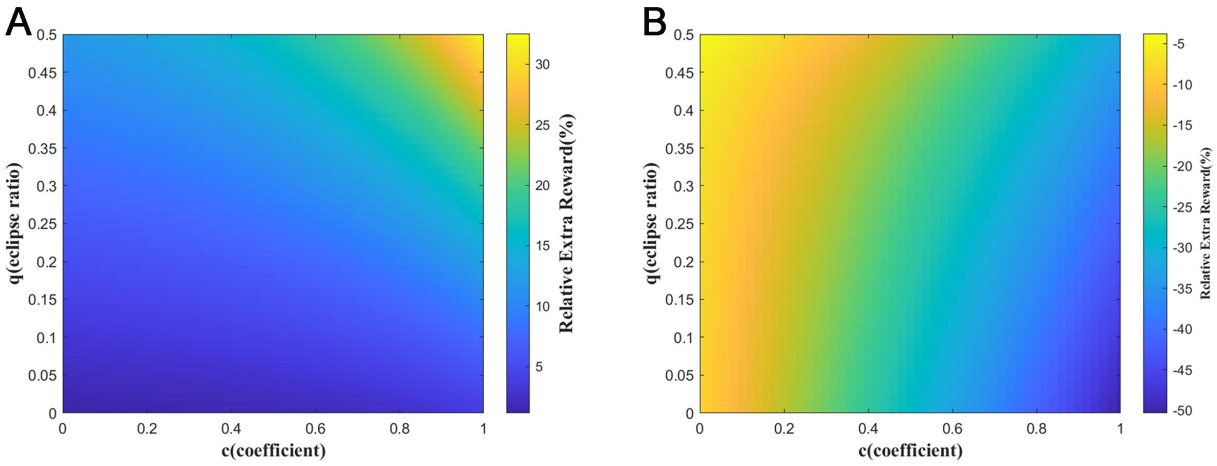

Figure 3. The changes in RERs when an attacker launches an EFAW attack against a single mining pool. (A) Changes in the attacker's relative additional rewards when launching an EFAW attack against a single mining pool; (B) Changes in the victim pool's relative additional rewards when launching an EFAW attack against a single mining pool. A negative number in the victim pool on the right represents a loss of rewards. EFAW: Eclipse Fork After Withholding; RERs: relative extra rewards.

$$RER_B^{'} = \frac{RER_B - RER_{\mathrm{h}}}{RER_{\mathrm{h}}} \tag{4}$$

Firstly, we consider a specific situation: the computational power of the attack pool A and the computational power of the victim pool B are both 0.2, the proportion of the eclipsed miners is not more than 0.5 ($0 \leq q \leq 0.5$), and the probability of the FPoW submitted by the infiltration miner or the eclipsed miner being selected as the main chain is not greater than 1 ($0 \leq c \leq 1$). At this point, we observe the changes in the RERs $RER_A^{'}$ and $RER_B^{'}$ of pools A and B [Figure 3].

Following Figure 3A, the EFAW attack has a greater increase in RERs than FAW attacks. We observe that the $RER_A^{'}$ is an increasing function of q. Because the more victim pool miners the attacker intercepts, the greater the proportion of the penetration computational power that the attacker puts into the victim pool according to the optimal penetration ratio to the total computational power of the victim pool, the more rewards the attacker earns. When q reaches the threshold of 0.5, the attack pool can gain up to a maximum of 32.54% RERs. However, when $q = 0$, the EFAW attack reverts to FAW attacks.

Additionally, Figure 3B indicates that in the presence of an EFAW attack, the victim pool always incurs losses, and the reward for loss increases with the increase of the proportion of the eclipsed miners. This is because the PPoWs are discarded by the attacker, leading to no rewards for them. As c increases, the loss of the victim pool gradually decreases since it can also gain rewards from the block selected as the main chain.

Similarly, we give a comparison of the RERs between an EFAW attack and an FAW attack. Considering the consumption of resources required to launch an eclipse attack, we set q as 0.05 in the experiment, which is a reasonable value. Assume pool A's computational power is 0.2. We show the expected RER of the attack pool to launch the EFAW attack against the victim pool with 0.1, 0.2, and 0.3 computational power, respectively, corresponding to Cases 1-3 in Figure 4 . It indicates that when we combine an FAW attack with an eclipse attack to form an EFAW attack, we can earn more rewards. Even if c is 0, the EFAW attack is still better than FAW attacks.

4.3. Simulation experiments

To further validate the accuracy of our quantitative analysis results, we used the following system setup: Intel® Core™ i5 – 93000H CPU @ 2.40 GHz, 16 GB RAM, and 64-bit processor on Windows 10. We use this setup to

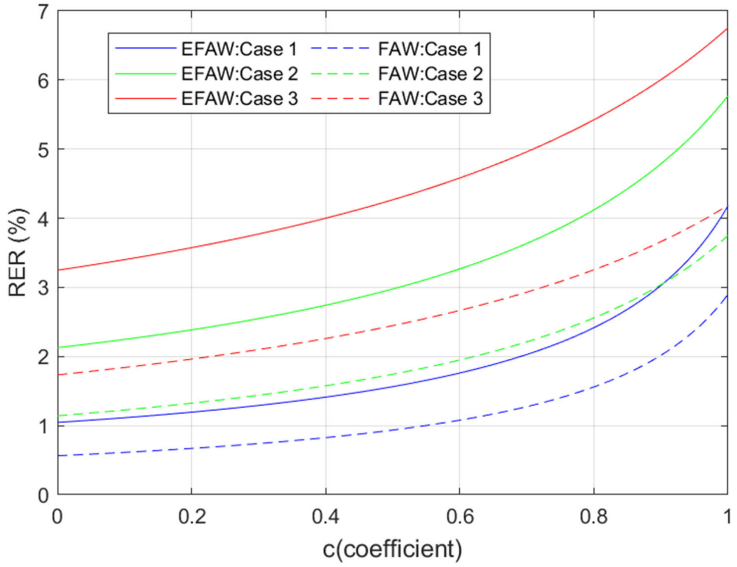

Figure 4. Comparison of RERs (%) that launch the EFAW attack and an FAW attack against a single mining pool. The solid line represents the EFAW attack, and the dashed line represents the FAW attack. EFAW: Eclipse Fork After Withholding; FAW: Fork After Withholding; RERs: relative extra rewards.

Table 2. The RER (%) of an attacker when the computational power is 0.2 and the proportion of eclipsed miners in the victim pool is 0.05. The value a (b) gives RERs based on theoretical analysis and simulation, respectively

β	c = 0	c = 0.25	c = 0.5	c = 0.7	c = 1
0.1	1.05 (1.05)	1.24 (1.24)	1.56 (1.56)	2.20 (2.20)	4.18 (4.18)
0.2	2.13 (2.13)	2.46 (2.46)	2.98 (2.97)	3.86 (3.86)	5.77 (5.78)
0.3	3.25 (3.26)	3.67 (3.67)	4.27 (4.27)	5.18 (5.18)	6.76 (6.76)

RER: Relative extra reward.

implement a Monte Carlo simulator to verify our theoretical analysis. We follow the basic steps of the Monte Carlo method, simulate the process of generating blocks and the fork competition process, and combine it with matlat implementation to conduct simulation analysis.

Firstly, simulate the block generation process. New blocks may be discovered by five subjects: honest miners in the attacking pool, honest miners in the victim pool, infiltration miners, eclipsed miners, and other miners. Among them, the probability of discovery by each subject is proportional to its computing power. In this paper, we simulate a scenario involving competition among five subjects by generating a random number r [r = rand ()] of the average price distribution between (0,1) and determine whether the r value falls within a specific range; that is: (1) r $\in [0, (1-\tau)\alpha]$, it is considered that the attacker's honest miner discovers a new block; (2) r $\in ((1-\tau)\alpha, (1-\tau)\alpha + (1-q)\beta)$, it is considered that the victim pool's honest miner discovers a new block; (3) r $\in ((1-\tau)\alpha + (1-q)\beta, \alpha + (1-q)\beta)$, it is considered that the infiltration miner discovers a new block; (4) r $\in [\alpha + (1-q)\beta, \alpha + \beta]$, it is considered that the eclipsed miner discovers a new block; (5) r $\in (\alpha + \beta, 1)$, it is considered that another miner discovers a new block. If a new block is discovered by an infiltrator or an eclipsed miner, a random number simulation is performed in this case, and the simulated time fork competition is the case. Set the reward to R, $R = R + 1$ when the block submitted by the honest miner of the attack pool is selected as the main chain, and $R = R + \frac{(1-q)\beta}{1-\tau\alpha-q\beta} \cdot \frac{\tau\alpha}{1-q\beta+\tau\alpha}$ when the block submitted by the victim pool's honest miner, the infiltration miner, or the eclipsed miner is selected as the main chain; When the block submitted by another miner is selected as the main chain, then $R = R$. For the three cases in Figure 4, we run the simulator for 10^9 rounds. The results are shown in Table 2, and the RER (%) of the attacker who launched the EFAW attack is almost the same as expected, confirming the calculation results.

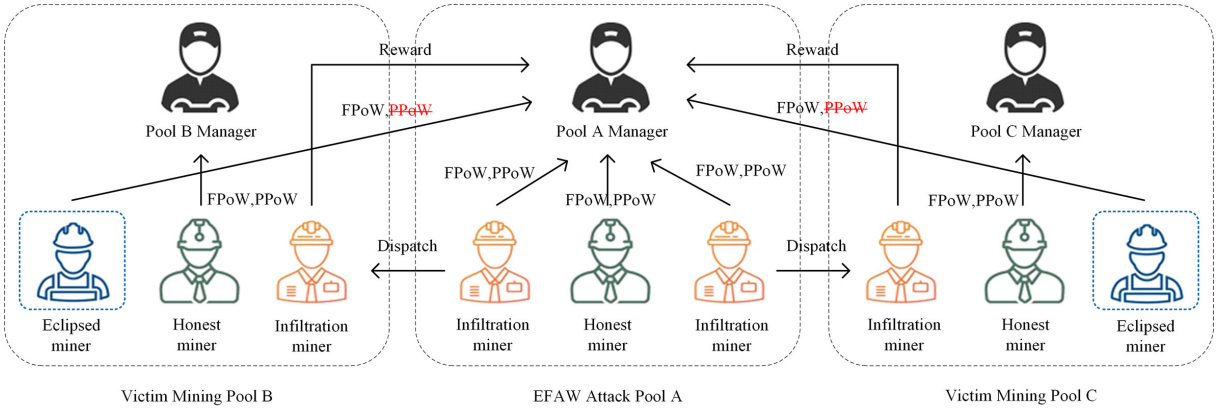

Figure 5. EFAW attacks against two victim mining pools. The one in the middle is EFAW attack pool A, the left is victim mining pool B, and the right is victim mining pool C. EFAW: Eclipse Fork After Withholding; FPoW: Full Proof-of-Work; PPoW: Partial Proof-of-Work.

5. THE EFAW ATTACK AGAINST TWO POOLS

In the previous section, we only consider the case of launching an EFAW attack against a single mining pool. In reality, however, an attacker can launch an attack against multiple mining pools at the same time. In this section, we assume that there is one EFAW attack pool and two honest mining pools in Bitcoin, and the attacker maximizes her rewards by launching EFAW attacks on these two victim pools. We establish an attack model when an attacker attacks two honest mining pools at the same time and analyze this attack scenario theoretically and quantitatively.

5.1. Theoretical analysis

Firstly, we introduce a model in which an attacker attacks two honest mining pools [Figure 5]. In this model, there are two honest mining pools labeled B and C, respectively. The EFAW attack pool is represented by A. Similarly, the pool A manager divides the computational power into two parts; one part is for honest mining, and the other part is dispatched to victim pools B and C as infiltration miners to do infiltration mining. The attacker simultaneously launches the eclipse attack on pool B and pool C to control all peer connections of some victim nodes. As in Section 4, the attacker discards the PPoWs submitted by the eclipsed nodes, keeps its FPoW submitted by the infiltration miner, and strategically releases it at the opportune time.

Let the computational power of the attack pool A be α, and the computational power of the victim pool B and pool C be β_1 and β_2, respectively. The pool A manager dispatches τ_1 and τ_2 the proportion of computational power to infiltration mining in pool B and pool C, respectively, while the remaining $(1-\tau_1-\tau_2)\alpha$ proportion of computational power is used for honest mining. At the same time, the attack pool A launches the eclipse attack on pool B and pool C to control their q_1 and q_2 proportion computational power, respectively. $c_i^{'}$ and $c_i^{''}$ indicate the probability that pool B and pool C will be chosen as the main chain in the case of two or three branches. Table 3 lists the parameters.

In our model, when an attacker launches the EFAW attack against two mining pools, the Bitcoin network may generate a fork of two branches or a fork of three branches [Figure 6]. If the FPoW submitted by an infiltration miner or eclipse victim miner in pool B or pool C is retained by the pool A manager, when other honest miners submit blocks, the manager will immediately submit the FPoW to generate a fork. Next, we analyze

Table 3. List of notations

Notation	Descriptions
α	The total computational power of the attack pool A
β_1	Computational power of the victim pool B
β_2	Computational power of the victim pool C
τ_1	The proportion of the attacker's infiltration mining computational power to pool B ($\tau_1\alpha$ as part of α)
τ_2	The proportion of the attacker's infiltration mining computational power to pool C ($\tau_2\alpha$ as part of α)
q_1	Computational power of eclipsed miners as a proportion of β_1
q_2	Computational power of eclipsed miners as a proportion of β_2
$c_i^{'}$	The probability that the FPoW submitted by an infiltration miner or eclipsed miner will be chosen as the main chain (two-branch case)
$c_i^{''}$	The probability that the FPoW submitted by an infiltration miner or eclipsed miner will be chosen as the main chain (three-branch case)

FPoW: Full Proof-of-Work.

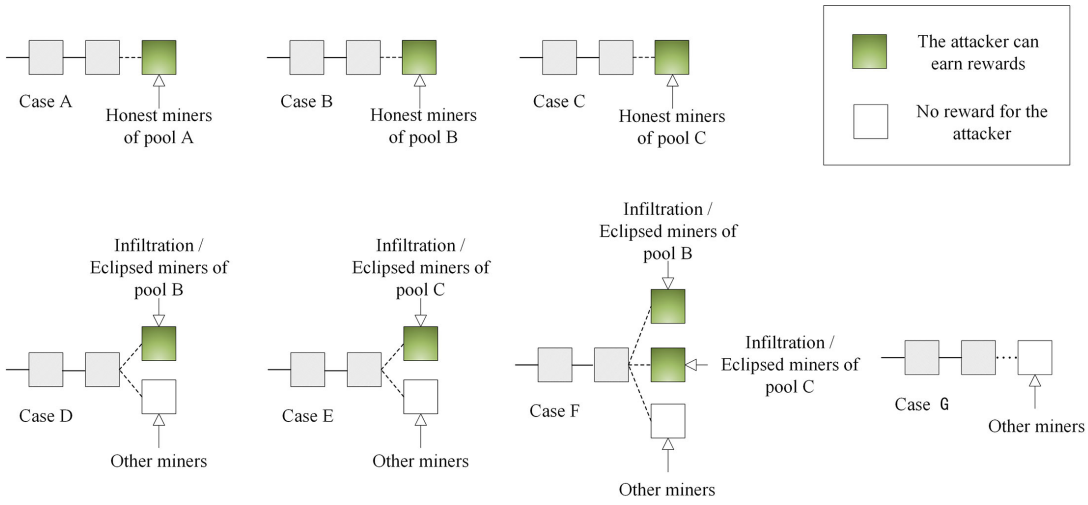

Figure 6. The possible consequences of an EFAW attack against two victim mining pools. The green blocks represent the attacker can earn rewards, so he can earn rewards in six cases: Cases A-F. EFAW: Eclipse Fork After Withholding.

the rewards earned by the attack pool A in this model. The rewards are as follows:

$$R_A = \frac{(1-\tau_1-\tau_2)\alpha}{1-(\tau_1+\tau_2)\alpha-q_1\beta_1-q_2\beta_2} + \sum_{i=1,2}\{\frac{\tau_i\alpha}{\tau_i\alpha+(1-q_i)\beta_i}\cdot(\frac{(1-q_i)\beta_i}{1-(\tau_1+\tau_2)\alpha-q_1\beta_1-q_2\beta_2} + c_i^{'}(\tau_i\alpha+q_i\beta_i)\cdot\frac{1-\alpha-\beta_1-\beta_2}{1-\tau_i\alpha-q_i\beta_i} + c_i^{''}\sum_{j=1,2}\{(\tau_j\alpha+q_j\beta_j)\cdot\frac{\tau_{\neg j}\alpha+q_{\neg j}\beta_{\neg j}}{1-\tau_j\alpha-q_j\beta_j}\}\cdot\frac{1-\alpha-\beta_1-\beta_2}{1-(\tau_1+\tau_2)\alpha-q_1\beta_1-q_2\beta_2})\} \quad (5)$$

Proof: Pool A can earn block rewards through two parts: honest mining and infiltration mining. This is shown in Figure 6: If an honest miner of pool A submits a valid block, the pool earns the full block reward: $\frac{(1-\tau_1-\tau_2)\alpha}{1-(\tau_1+\tau_2)\alpha-q_1\beta_1-q_2\beta_2}$ (Case A in Figure 6). When an honest miner finds an FPoW in the victim pool B, the reward is $\frac{(1-q_1)\beta_1}{1-(\tau_1+\tau_2)\alpha-q_1\beta_1-q_2\beta_2}\cdot\frac{\tau_1\alpha}{(1-q_1)\beta_1+\tau_1\alpha}$ (Case B in Figure 6). When an honest miner in pool C finds an FPoW, the reward is $\frac{(1-q_2)\beta_2}{1-(\tau_1+\tau_2)\alpha-q_1\beta_1-q_2\beta_2}\cdot\frac{\tau_2\alpha}{(1-q_2)\beta_2+\tau_2\alpha}$ (Case C in Figure 6). If the FPoW found by the infiltration miner or eclipse victim miner in pool B is submitted by the attacker manager and wins the competition. At this point, the reward is $c_1^{'}(\tau_1\alpha+q_1\beta_1)\cdot\frac{1-\alpha-\beta_1-\beta_2}{1-\tau_1\alpha-q_1\beta_1}\cdot\frac{\tau_1\alpha}{(1-q_1)\beta_1+\tau_1\alpha}$ (Case D in Figure 6). Similarly, the pool A manager submits an FPoW found by an infiltration miner or eclipse victim miner in pool C to earn the reward, which is $c_2^{'}(\tau_2\alpha+q_2\beta_2)\cdot\frac{1-\alpha-\beta_1-\beta_2}{1-\tau_2\alpha-q_2\beta_2}\cdot\frac{\tau_2\alpha}{(1-q_2)\beta_2+\tau_2\alpha}$ (Case E in Figure 6). Next, we discuss the case where three forks arise in the system (Case F in Figure 6). If an infiltration miner or the eclipsed miner in pool B wins in the fork competition, the attack pool A can earn the following rewards:$c_1^{''}(\tau_1\alpha+q_1\beta_1)\cdot\frac{\tau_2\alpha+q_2\beta_2}{1-\tau_1\alpha-q_1\beta_1}\cdot\frac{1-\alpha-\beta_1-\beta_2}{1-(\tau_1+\tau_2)\alpha-q_1\beta_1-q_2\beta_2}\cdot\frac{\tau_1\alpha}{(1-q_1)\beta_1+\tau_1\alpha}$,

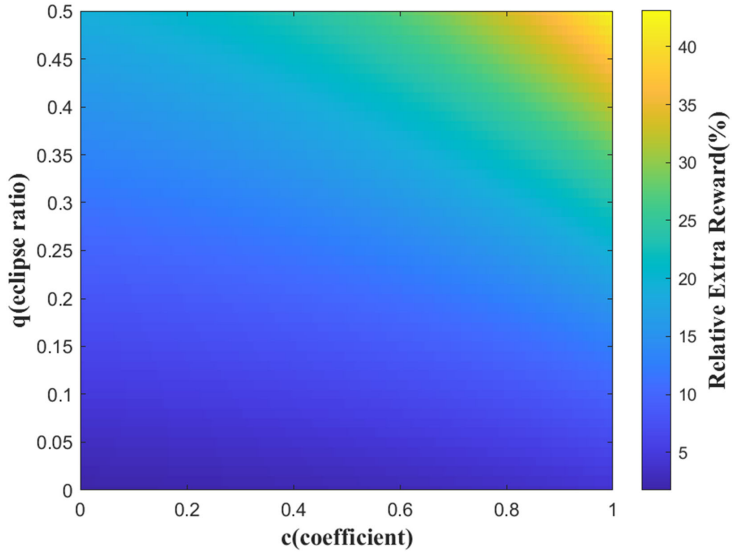

Figure 7. The changes in RERs when an attacker launches an EFAW attack against two victim mining pools. The rewards earned by the attacker gradually increase from dark blue to light yellow. EFAW: Eclipse Fork After Withholding; RERs: relative extra rewards.

and if an infiltration miner or eclipse victim miner in pool C wins, the rewards that pool A can earn is $c_2^{''}(\tau_2\alpha + q_2\beta_2) \cdot \frac{\tau_1\alpha+q_1\beta_1}{1-\tau_2\alpha-q_2\beta_2} \cdot \frac{1-\alpha-\beta_1-\beta_2}{1-(\tau_1+\tau_2)\alpha-q_1\beta_1-q_2\beta_2} \cdot \frac{\tau_2\alpha}{(1-q_2)\beta_2+\tau_2\alpha}$. Thus, the total rewards for pool A can be represented by Equation (5).

To earn more rewards, the attackers should choose the appropriate τ_1 and τ_2 to maximize their rewards. τ_1 and τ_2 can be obtained by solving the optimization equation: $\underset{\tau_1,\tau_2}{\arg\max} R_A$. Among them, it can be deduced that the values of τ_1 and τ_2 are related to q_1, q_2, β_1, and β_2, and the relationship between them can be expressed as $\frac{\tau_1\alpha+q_1\beta_1}{\beta_1} = \frac{\tau_2\alpha+q_2\beta_2}{\beta_2}$.

5.2. Quantitative analysis

Next, we use a specific case to show the RER(%) that an attacker can earn by launching an EFAW attack against two mining pools. For ease of calculation, we set the computational power α of the attack pool A to 0.2. The computational powers of the victim pools B and C are 0.1 and 0.2, respectively. c represents the ratio of the probability of winning the competition to the number of branches of valid blocks intercepted and submitted by the pool A manager ($0 \le c \le 1$). At the same time, we assume that both pools have the same proportion of mining power by eclipsed miners, expressed by q($0 \le q_1 = q_2 \le 0.5$).

Figure 7 shows that it is always profitable for an attacker to launch an EFAW attack against two mining pools and earn a higher reward than an FAW attack. Similarly, the RER for launching an EFAW attack against two mining pools is proportional to q, and the maximum rewards can even reach 43.16% when $q = 0.5$ and $c = 1$.

Secondly, we compare the RERs for launching an EFAW attack against two mining pools with an FAW attack. We also assume that the computational power of the attack pool A α is 0.2 and launch attacks on the victim pools B and C in the following three cases, respectively. Cases 1-3 represent two victim pools with computational power (β_1, β_2) equal to (0.1, 0.1), (0.1, 0.2), and (0.2, 0.2), respectively. We set $q_1 = q_2 = 0.05$ and change the probability c of a malicious fork submitted by an attacker being chosen as the main chain. At this point, the RER of pool A is shown in Figure 8 . It is clear that same as attacking a single mining pool when an eclipse attack controls and exploits a subset of the victim nodes, the attacker can always earn a higher reward by launching the EFAW attack than an FAW attack, and the larger of c, the higher the RER.

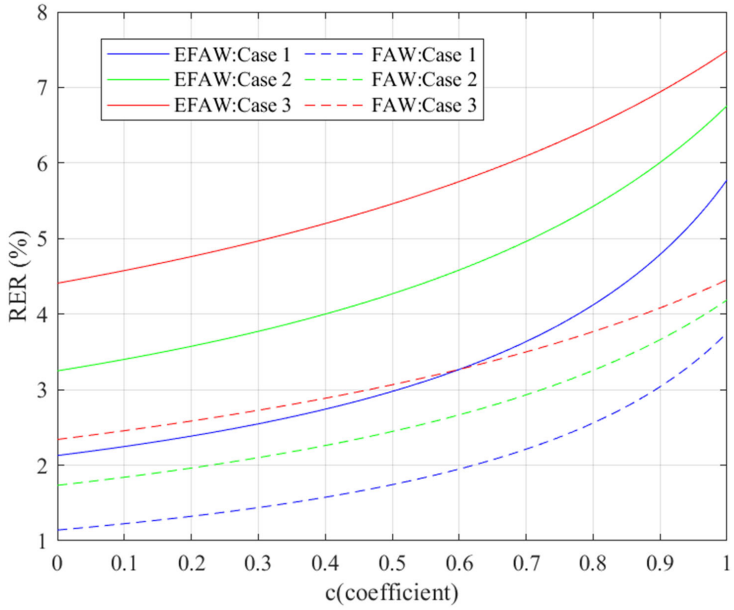

Figure 8. The changes in RERs when an attacker launches an EFAW attack against two victim mining pools. The solid line represents the EFAW attack, and the dashed line represents the FAW attack. EFAW: Eclipse Fork After Withholding; FAW: Fork After Withholding; RERs: relative extra rewards.

Table 4. The RER (%) of an attacker when the computational power is 0.2 and the proportion of eclipsed miners in the victim pool is 0.05. The value a (b) gives RERs based on theoretical analysis and simulation, respectively

(β_1,β_2)	c = 0	c = 0.25	c = 0.5	c = 0.75	c = 1
(0.1,0.1)	2.13 (2.13)	2.46 (2.47)	2.98 (2.98)	3.86 (3.86)	5.78 (5.78)
(0.1,0.2)	3.25 (3.25)	3.67 (3.68)	4.27 (4.27)	5.18 (5.18)	6.76 (6.75)
(0.2,0.2)	4.40 (4.40)	4.86 (4.87)	5.46 (5.46)	6.28 (6.27)	7.48 (7.48)

RER: Relative extra reward.

5.3. Simulation experiments

Similarly, we validate our theoretical analysis through Monte Carlo simulators. As with the previous experiment, the difference is that this experiment has eight subjects: honest miners in the attacking pool, honest miners in the victim pool B, honest miners in the victim pool C, infiltration miners in the victim pool B, infiltration miners in the victim pool C, eclipsed miners in the victim pool B, eclipsed miners in the victim pool C, and other miners. We run 10^9 rounds of simulation for the three cases in Figure 8, and the results are shown in Table 4. The RER of the attacker who launched the EFAW attack was almost the same as expected, confirming the calculations.

6. DISCUSSION

A mining pool called "Eligiu"[33] suffered a BWH attack in 2014 that caused the pool to lose 300 Bitcoins (about $3.5 million). The EFAW attack proposed in this paper combines the FAW attack and the eclipse attack; although there is no large-scale outbreak of the FAW attack at present, the paper[21] finally mentions that the malicious mining attack (FAW attack) of digital currency under the PoW mechanism may break out on a large scale. Eclipse attacks, on the other hand, have actually occurred, so EFAW attacks are also likely to erupt on a large scale in practice. The occurrence of this attack requires the attacker to have certain network technology and resources, enabling them to isolate some nodes of the target mining pool. At the same time, the attacker needs to have a certain amount of computing power to launch an FAW attack and subsequently execute an eclipse attack on the basis of the FAW attack to control and use some nodes of the target mining pool to earn more block rewards.

Through theoretical analysis and simulation experiments, we have proved that the reward of the EFAW attack is greatly improved compared with an FAW attack. The cost of the EFAW attack is mainly due to the resources consumed by launching an eclipse attack to isolate some nodes. The eclipse attack typically does not rely directly on large amounts of computing power but rather focuses more on technology and resources on the network side. Meanwhile, the attacker, as a mining pool, usually has quite high network resources on its own, as it consists of a large number of miner nodes that are connected to the mining pool server through the network. The attacker would only need to isolate or manipulate a small number of nodes in the target pool rather than the entire network and only consider the eclipse ratio of 0.05 in the experimental part of this paper. The infiltration miner nodes are dispatched to the target mining pool; the information about the network topology around the nodes can be grasped by the attacker in detail, which is more convenient for launching eclipse attacks. Therefore, the resources required by the EFAW attack are very limited compared to the rewards obtained by the attack, so we will not consider the resource consumption in this part of this article but focus on the reward increase brought by the EFAW attack.

In the future, we can pay more attention to attacks on the blockchain network layer and protocol layer, and the effective combination of different types of attacks may achieve surprising results. However, the purpose of our theoretical research is to maintain the homeostasis of the blockchain and give researchers more ideas to formulate defensive countermeasures to prevent the blockchain system from being attacked.

7. CONCLUSION

FAW attacks cause serious harm to PoW consensus, and the research on FAW attacks has become an important topic in the field of blockchain security. In this paper, we combine FAW attacks with the eclipse attack targeting the network layer of P2P systems to propose a new mining attack model, in which the attacker further increases the rewards for FAW attacks by launching an eclipse attack against the victim mining pool. In addition, we verify our model in two specific scenarios, proving that the attacker can always earn more rewards than FAW attacks by launching the EFAW attack. This part of the rewards is related to the computing power ratio of the mining pool occupied by the miners controlled by the eclipse attack, and the lower limit is FAW attacks. Therefore, The EFAW attack is more harmful than FAW attacks, and research on its security is of great significance.

DECLARATIONS

Acknowledgments

We have received quite a bit of support and help throughout the writing of this article. First of all, we would like to thank Wu Senkai and Xiao Zihan for their valuable suggestions on the ideas and arguments of this article. Their insightful feedback has facilitated the improvement of our thought process and improved the quality of my work. In addition, we would like to thank Wenjie He and Xuesheng Zhang for their suggestions on the format of the paper.

Authors' contributions

Made substantial contributions to the conception and design of the study, reviewed this paper, and provided administrative, financial, and technical support: Wang J

Significantly contributed to the idea of this paper, conducted experimental data collection, and wrote this paper: Wang Z

Availability of data and materials

The data that support the findings of this study are available upon reasonable request from the corresponding author, Wang J.

Financial support and sponsorship

None.

Conflicts of interest

All authors declared that there are no conflicts of interest.

Ethical approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

REFERENCES

1. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system. Available from: https://bitcoin.org/bitcoin.pdf. [Last accessed on 15 Dec 2023]
2. Nasir MH, Arshad J, Khan MM, Fatima M, Salah K, Jayaraman R. Scalable blockchains - a systematic review. *Future Gener Comput Syst* 2022;126:136-62. DOI
3. Qasse IA, Abu Talib M, Nasir Q. Inter blockchain communication: a survey. In: Proceedings of the ArabWIC 6th Annual International Conference Research Track. New York: Association for Computing Machinery; 2019. p.1-6. DOI
4. Mišić VB, Mišić J, Chang X. On forks and fork characteristics in a Bitcoin-like distribution network. In: 2019 IEEE International Conference on Blockchain (Blockchain); 2019 Jul 14-17; Atlanta, USA. IEEE; 2019. pp. 212-9. DOI
5. Saad M, Spaulding J, Njilla L, et al. Exploring the attack surface of blockchain: a comprehensive survey. *IEEE Commun Surv Tutor* 2020;22:1977-2008. DOI
6. Ghimire S,Selvaraj H. A survey on Bitcoin cryptocurrency and its mining. In: 2018 26th International Conference on Systems Engineering (ICSEng); 2018 Dec 18-20l; Sydney, Australia. IEEE; 2018. pp. 1-6. DOI
7. Tovanich N, Soulié N, Heulot N, et al. The evolution of mining pools and miners' behaviors in the Bitcoin blockchain. *IEEE Trans Netw Service Manag* 2022;19:3633-44. DOI
8. Fullmer D, Morse A S. Analysis of difficulty control in Bitcoin and proof-of-work blockchains. In: 2018 IEEE conference on decision and control (CDC); 2018 Dec 17-19; Miami, USA. IEEE; 2018. pp. 5988-992. DOI
9. Tapsell J, Akram RN, Markantonakis K. An evaluation of the security of the Bitcoin peer-to-peer network. In: 2018 IEEE international conference on internet of things (IThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData); 2018 Jul 30 - Aug 3; Halifax, Canada. IEEE; 2018. pp. 1057-62. DOI
10. Kumari P, Jain AK. A comprehensive study of DDoS attacks over IoT network and their countermeasures. *Comput Secur* 2023;127:103096. DOI
11. de Asís López-Fuentes F, Eugui-De-Alba I, Ortíz-Ruiz OM. Evaluating P2P networks against eclipse attacks. *Proc Technol* 2012;3:61-8. DOI
12. Zheng H, Tran T, Arden O. Total Eclipse of the enclave: detecting Eclipse attacks from inside TEEs. In: 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC); 2021 May 3-6; Sydney, Australia. IEEE, 2021. pp. 1-5. DOI
13. Alangot B, Reijsbergen D, Venugopalan S, Szalachowski P, Yeo KS. Decentralized and lightweight approach to detect eclipse attacks on proof of work blockchains. *IEEE Trans Netw Service Manag* 2021;18:1659-72. DOI
14. Ch R, Kumari DJ, Gadekallu TR, Iwendi C. Distributed-ledger-based blockchain technology for reliable electronic voting system with statistical analysis. *Electronics* 2022;11:3308. DOI
15. Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. *Commun ACM* 2018;61:95-102. DOI
16. Rosenfeld M. Analysis of Bitcoin pooled mining reward systems. arXiv. [Preprint.] Dec 21, 2011. [accessed 2023 Dec 14]. Available from: https://api.semanticscholar.org/CorpusID:15548076.
17. Courtois N, Bahack L. On subversive miner strategies and block withholding attack in Bitcoin digital currency. arXiv. [Preprint.] Jan 28, 2014. [accessed 2023 Dec 14]. Available from: https://api.semanticscholar.org/CorpusID:16387130. [Last accessed on 15 Dec 2023]
18. Luu L, Saha R, Parameshwaran I, Saxena P, Hobor A. On power splitting games in distributed computation: the case of Bitcoin pooled mining. In: 2015 IEEE 28th Computer Security Foundations Symposium; 2015 Jul 13-17; Verona, Italy. IEEE; 2015. pp. 397-411. DOI

19. Bag S, Ruj S, Sakurai K. Bitcoin block withholding attack: analysis and mitigation. *IEEE Trans Inf Forensics Secur* 2016;12:1967-78. DOI
20. Eyal I. The miner's dilemma. In: IEEE symposium on security and privacy; 2015 May 17-21; San Jose, USA. IEEE; 2015. pp. 89-103. DOI
21. Kwon Y, Kim D, Son Y, Vasserman EY, Kim Y. Be selfish and avoid dilemmas: fork after withholding (faw) attacks on Bitcoin. In: Proceedings of the 2017 ACM SIGSAC conference on computer and communications security. Association for Computing Machinery; 2017. pp. 195-209. DOI
22. Li W, Cao M, Wang Y, Tang C, Lin F. Mining pool game model and nash equilibrium analysis for pow-based blockchain networks. *IEEE Access* 2020;8:101049-60. DOI
23. Toda K, Kuze N, Ushio T. Game-theoretic approach to a decision-making problem for blockchain mining. *IEEE Control Syst Lett* 2020;5:1783-8. DOI
24. Nayak K, Kumar S, Miller A, Shi E. Stubborn mining: generalizing selfish mining and combining with an eclipse attack. In: 2016 IEEE European Symposium on Security and Privacy (EuroS&P); 2016 Mar 21-24; Saarbruecken, Germany. IEEE; 2016. pp. 305-20. DOI
25. Dong X, Wu F, Faree A, Guo D, Shen Y, Ma J. Selfholding: a combined attack model using selfish mining with block withholding attack. *Comput Secur* 2019;87:101584. DOI
26. Dong X, Gao S. GenSelfHolding: fusing selfish mining and block withholding attacks on Bitcoin revisited. *J Netw Netw Appl* 2022;2:23-35. DOI
27. Feng Y, Torlak E, Bodik R. Precise attack synthesis for smart contracts. arXiv. [Preprint.] Feb 16, 2019 [accessed 2023 Dec 18]. Available from: https://arxiv.org/abs/1902.06067.
28. Sapirshtein A, Sompolinsky Y, Zohar A. Optimal selfish mining strategies in Bitcoin. In: Grossklags J, Preneel B, editors. Financial Cryptography and Data Security: FC 2016. Lecture Notes in Computer Science. Berlin, Springer; 2017. pp. 515-32. DOI
29. Motlagh SG, Mišić J, Mišić VB. The impact of selfish mining on Bitcoin network performance. *IEEE Trans Netw Sci Eng* 2021;8:724-35. DOI
30. Gao S, Li Z, Peng Z, et al. Power adjusting and bribery racing: novel mining attacks in the Bitcoin system. In: Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security. Association for Computing Machinery; 2019. pp. 833-50. DOI
31. Buterin V. A next-generation smart contract and decentralized application platform. Available from: https://api.semanticscholar.org/CorpusID:19568665. [Last accessed on 15 Dec 2023]
32. Miller AK, Litton J, Pachulski A, et al. Discovering Bitcoin's public topology and influential nodes. Available from: https://api.semanticscholar.org/CorpusID:15600193. [Last accessed on 15 Dec 2023]
33. Eligius: 0% fee BTC, 105% PPS NMC, no registration, CPPSRB. Available from: https://bitcointalk.org/?topic=441465.msg7282674. [Last accessed on 15 Dec 2023]