CS765 HW2 Report

Submitted by
Nishant (24M0743)
Harsh Kumar (24M0804)
Dipanshu Garg (24M0755)

March 2025

Contents

1 Experiments

1.1 Experiment 1

For this experiment, we use the following parameters:

Total Number of Nodes:	100
Mean Block Inter-arrival Time:	50 seconds
Mean Transaction Inter-arrival Time:	1000 second
Simulation Time:	5000 seconds
Timeout Timer:	25 (< Mean Block Interarrival Time)

1.1.1 Comparison of the fraction of ringmaster-mined blocks included in the main chain (relative to total blocks in the longest chain)

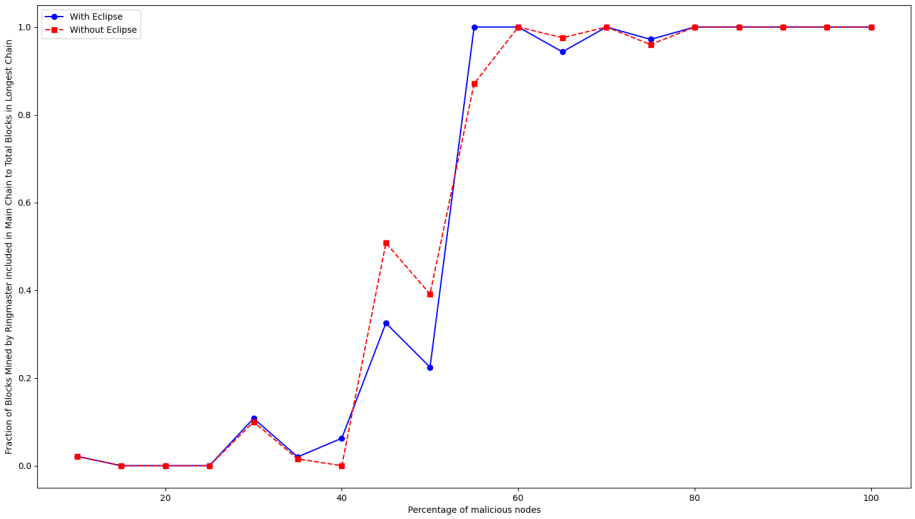

Figure 1.1.1: Ringmaster Block inclusion in longest chain

1.1.2 Comparison of the fraction of ringmaster-mined blocks included in the main chain (relative to total ringmaster-mined blocks)

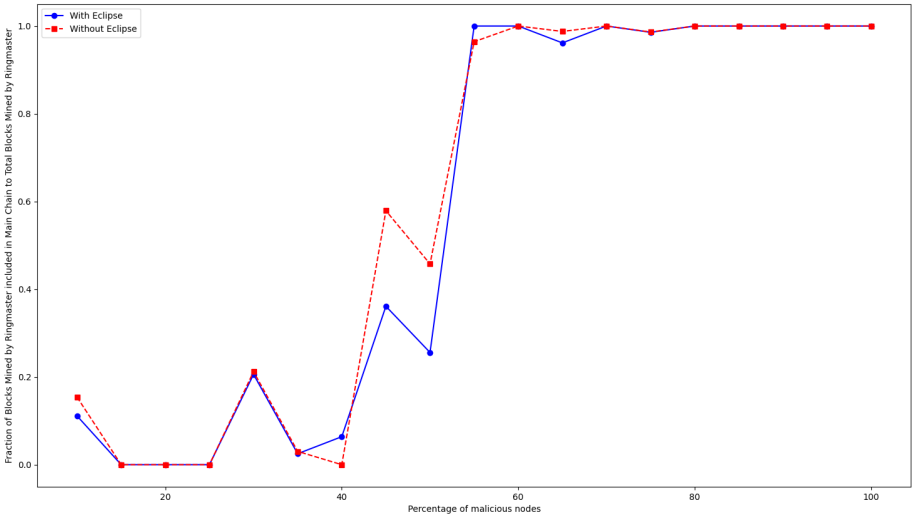

Figure 1.1.2: Ringmaster Block Inclusion Ratio

1.2 Experiment 2

For this experiment, we use the following parameters:

Total Number of Nodes:	100
Mean Block Inter-arrival Time:	50 seconds
Mean Transaction Inter-arrival Time:	1000 second
Simulation Time:	5000 seconds
Timeout Timer:	50 (= Mean Block Interarrival Time)

1.2.1 Comparison of the fraction of ringmaster-mined blocks included in the main chain (relative to total blocks in the longest chain)

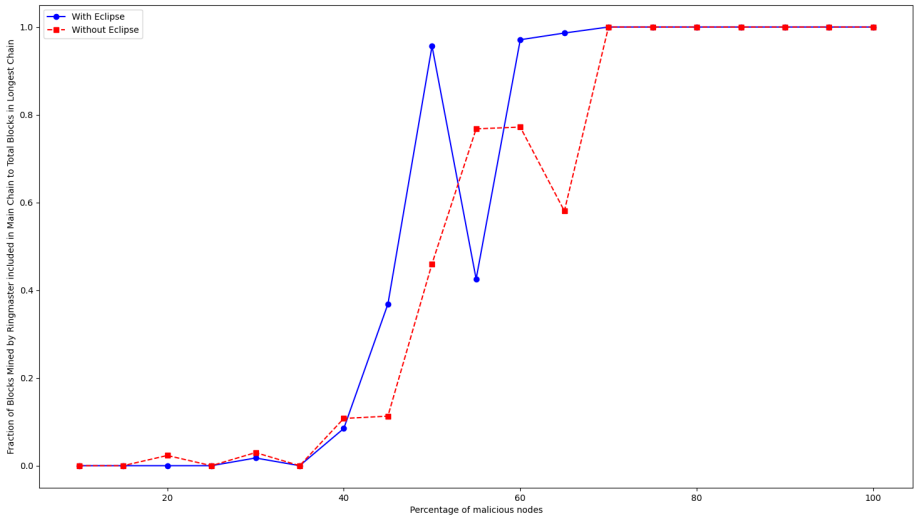

Figure 1.2.1: Ringmaster Block inclusion in longest chain

1.2.2 Comparison of the fraction of ringmaster-mined blocks included in the main chain (relative to total ringmaster-mined blocks)

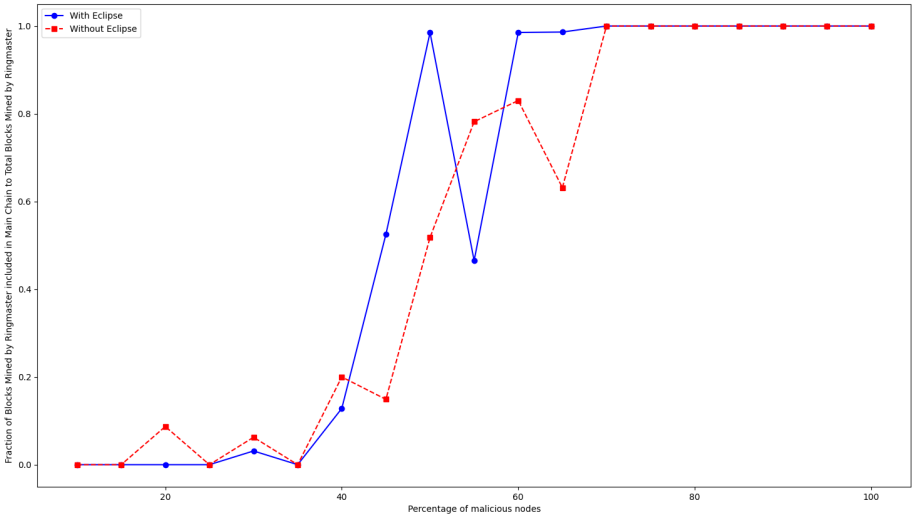

Figure 1.2.2: Ringmaster Block Inclusion Ratio

1.3 Experiment 3

For this experiment, we use the following parameters:

Total Number of Nodes:	100
Mean Block Inter-arrival Time:	50 seconds
Mean Transaction Inter-arrival Time:	1000 second
Simulation Time:	5000 seconds
Timeout Timer:	75 (> Mean Block Interarrival Time)

1.3.1 Comparison of the fraction of ringmaster-mined blocks included in the main chain (relative to total blocks in the longest chain)

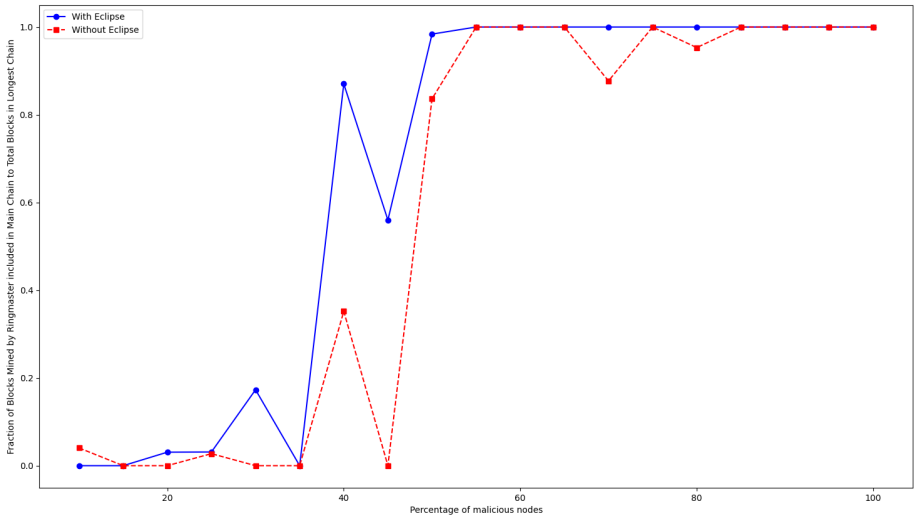

Figure 1.3.1: Ringmaster Block inclusion in longest chain

1.3.2 Comparison of the fraction of ringmaster-mined blocks included in the main chain (relative to total ringmaster-mined blocks)

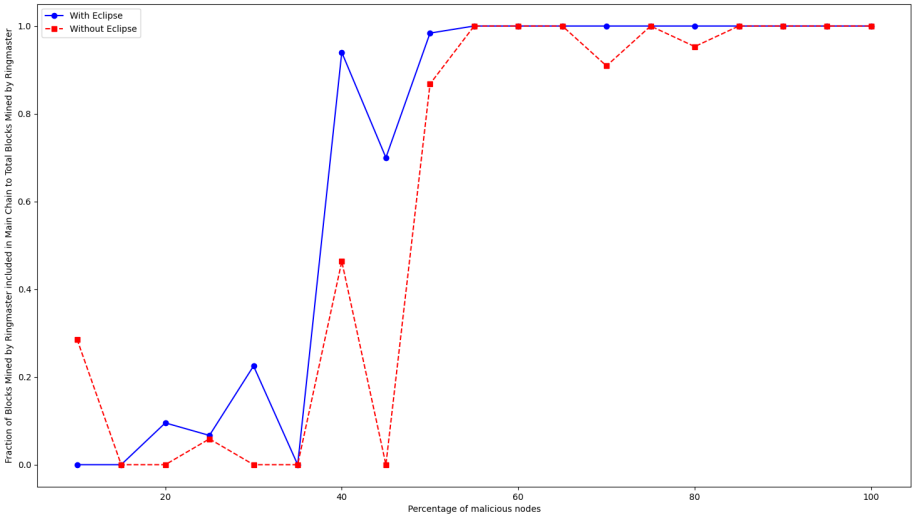

Figure 1.3.2: Ringmaster Block Inclusion Ratio

2 Observations

2.1 When malicious nodes' percentage is in between 0% to 30%

- **Minimal Impact on Main Chain:** Minimal difference in the number of ringmaster blocks in the main chain when comparing selfish mining with and without eclipse attack.
- **Lower Hashing Power:** Malicious nodes, being a small fraction of the network, have significantly lower hashing power than honest nodes, limiting their ability to extract and remove blocks.
- **Chain Extension Favoring Honest Nodes:** With honest nodes in the majority, the chance of receiving a block hash from a malicious node is low, so most honest nodes continue to extend the honest chain.
- **Difficulty in Competing:** Due to limited hash power and block retentionability, malicious nodes struggle to maintain a competing chain, resulting in the longest chain being predominantly honest.

2.2 When malicious nodes' percentage is in between 30% to 55%

- **Increased Impact:** With 30%–55% malicious nodes, the effects of selfish mining and eclipse attack become more pronounced.
- **Higher Control:** The chance of receiving a block hash from a malicious node increases, giving them more control over chain growth.
- **Increased Malicious Contribution:** More blocks in the longest chain come from malicious nodes when the eclipse attack is active.

2.3 When malicious nodes' percentage is in between 55% to 100%

- **Majority Behavior:** With 55%–100% malicious nodes, behavior is similar regardless of the eclipse attack.
- **Effective Selfish Mining:** Dominant hashing power enables malicious nodes to mine and propagate their blocks, ensuring nearly all ringmaster blocks enter the main chain.
- **Overwhelming Chain Composition:** The longest chain is mostly composed of ringmaster blocks, leaving little room for honest blocks.

3 Some Questions

3.1 How does increasing the timeout time (Tt) affect block propagation in the presence of an eclipse attack?

- **Effect of Timeout Timer:**
  - **Timeout < Mean Block Interarrival Time:** Honest nodes quickly request missing blocks, reducing malicious influence.
  - **Timeout ≥ Mean Block Interarrival Time:** Malicious nodes can extend their chain, increasing their share in the longest chain.
- **No Timeout Impact (No Eclipse):** Without the eclipse attack, the timeout timer minimally affects selfish mining as honest nodes receive blocks on time.(refer to Fig. 3.1.1)

Figure 3.1.1: W = 100, M=25% without eclipse attack

Note: In selfish mining with eclipse attack, the longer the timeout timer, the more forks and the shorter the chain.

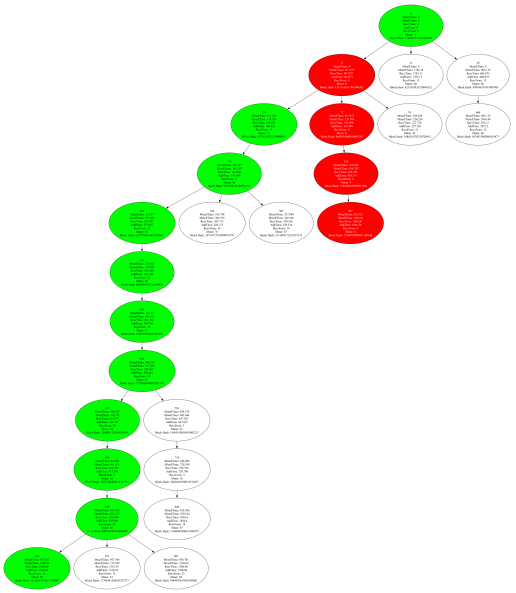

Figure 3.1.2: W = 100, M=25% with eclipse attack

3.2 Suggest countermeasures to mitigate or weaken the above-described attack.

- **Reduce Timeout Duration:** By setting the timeout duration significantly lower than the average time between blocks, honest nodes don't wait too long for missing blocks. Instead, they promptly request these blocks from multiple peers, reducing reliance on any single node. This rapid, multi-source block retrieval helps maintain consistency across the blockchain, as nodes are less likely to be left with outdated or incomplete chain data.

  Experiment Comparison

  - **Experiment 1 (Timeout Timer: 25 seconds, $<$ Mean Block Interarrival Time):** With a timeout of 25 seconds—significantly shorter than the 50-second mean block interarrival time—honest nodes quickly request missing blocks from multiple peers. This rapid response minimizes the window for malicious nodes to exploit the network, effectively reducing the impact of both selfish mining and the eclipse attack.
  - **Experiment 2 (Timeout Timer: 50 seconds, $=$ Mean Block Interarrival Time):** When the timeout equals the block interarrival time, honest nodes' responses are slower, giving malicious nodes more time to extend their chain.
  - **Experiment 3 (Timeout Timer: 75 seconds, $>$ Mean Block Interarrival Time):** A longer timeout of 75 seconds allows malicious nodes ample time to withhold blocks and extend their chain further, increasing their share in the longest chain and amplifying the attack's impact.

  Conclusion: The experiments demonstrate that reducing the timeout duration below the mean block interarrival time forces honest nodes to quickly retrieve missing blocks from multiple peers. This significantly minimizes the window for malicious exploitation, effectively mitigating the combined effects of selfish mining and eclipse attacks.

- **Implement Checkpointing:** Introduce periodic checkpoints in the blockchain to designate certain blocks as final and immutable. This countermeasure works by:

  - **Finalizing Blocks:** Once a block is checkpointed, all nodes treat it as confirmed, and any fork or alternate chain attempting to replace these blocks is automatically rejected.
  - **Preventing Reorganizations:** This finalization prevents attackers from rewriting or reordering blocks—a common tactic in both selfish mining and eclipse attacks—by locking in the blockchain history.

  - **Mitigating Isolation Effects:** In an eclipse attack, even if a node is isolated and fed alternate data, it will eventually synchronize with the checkpointed blocks, ensuring consistency with the honest network.

- **Penalize Nodes:** Introduce a penalty mechanism that reduces rewards or reputation for nodes that consistently withhold blocks. This discourages selfish mining by:
  - **Economic Disincentives:** Nodes that engage in block withholding receive lower mining rewards or transaction fees, making the selfish mining strategy less profitable.
  - **Reputation Damage:** Penalized nodes are marked as less reliable, causing honest nodes to reduce or cut off their connections with them, thereby limiting the malicious nodes' influence on the network.
  - **Increased Operational Costs:** It means that if a node is penalized, the network closely watches it and quickly adjusts any changes it makes. This makes it much harder and costlier for an attacker to manipulate the blockchain, so attackers are less likely to try exploiting the system.

- **Network Activity Monitoring:** Continuously track key network metrics, such as block propagation times and node behavior. When these metrics stray from their normal ranges, alerts are triggered for immediate investigation. This early warning system helps quickly identify anomalies that may signal an eclipse or selfish mining attack, allowing for rapid mitigation before significant damage occurs.