International Journal of Advanced Engineering Application
Volume No.1 Issue No 6 Oct 2024
ISSN NO:3048-6807

Dependability Analysis of Bitcoin at the System Level under Eclipse and 51% Attacks

[1]Tannu Priya, [2] Sohamkar, [3] *Abhinandan*
[1,2,3]*Department of Computer Science Engineering.*
[1,2,3]*Sai Vidya Institute of Technology, Karnataka, India*

Abstract

Bitcoin, a digital cryptocurrency rooted in Blockchain technology, has surged in popularity due to its decentralized nature. However, it is susceptible to certain cyberattacks, such as the 51% attack, where malicious actors can gain control over more than half of the network's computing power, thus having the ability to modify the blockchain. To execute this, attackers may initially perform an Eclipse attack, monopolizing communication channels to and from a Bitcoin node. In this paper, we analyze the reliability of the Bitcoin network when subjected to Eclipse and 51% attacks. We propose a hierarchical model using a continuous-time Markov chain (CTMC) for node-level dependability analysis and a multi-valued decision diagram (MDD) for system-level dependability assessment. The model is evaluated through case studies of Bitcoin systems with both homogeneous and heterogeneous nodes, analysing the influence of critical parameters on network dependability.

Keywords: Bitcoin, Dependability, Eclipse attack, Hierarchical modelling, 51% attack.

1. Introduction

Bitcoin, a decentralized cryptocurrency built upon blockchain technology, allows users to conduct peer-to-peer transactions without the need for intermediaries (Ferrag et al., 2018; Kang et al., 2018; Frizzo-Barker et al., 2020; Xing, 2020). Despite its benefits, Bitcoin is vulnerable to various cyber threats. For example, an attacker may exploit the open nature of Bitcoin's network to track transaction addresses and compromise user privacy (Reid and Harrigan, 2013). Similarly, attackers can attempt to tamper with the consensus mechanism of the blockchain, as seen in the case of selfish mining (Eyal and Sirer, 2014), Sybil attacks (Zhang and Lee, 2019), and 51% attacks (Bastiaan, 2015; Novoa et al., 2021). An Eclipse attack (Heilman et al., 2015; Zhou et al., 2021a) allows attackers to monopolize a victim node's connections, facilitating further attacks like the 51% attack.

Various mitigation strategies have been proposed in response to these attacks. For instance, Eyal and Sirer (2014) recommended altering the Bitcoin protocol to counter selfish mining, while Gervais et al. (2015) suggested methods such as dynamic timeouts and penalizing unresponsive nodes to improve Bitcoin's security. Additionally, Monaco (2015) proposed a decentralized anonymous payment system to protect user privacy.

Recent research has focused on quantitatively analyzing Bitcoin's dependability. Zhou et al. (2021a) developed a continuous-time Markov chain (CTMC) model to examine the impact of Eclipse attacks on individual Bitcoin nodes. In contrast, Zhou et al. (2021b) explored a semi-Markov process to assess the steady-state dependability of nodes. The selfish mining behavior and its effects on system-level dependability were studied by Zhou et al. (2022). While these efforts provide insights into node-level vulnerabilities, they primarily consider individual attacks in isolation. The reality, however, is that Bitcoin systems may simultaneously face multiple attacks, such as Eclipse and 51% attacks.

In this paper, we aim to fill this gap by modeling and analyzing Bitcoin's system-level dependability under the combined threat of Eclipse and 51% attacks. We propose a hierarchical model that integrates a CTMC approach for node-level behavior and a multi-valued decision diagram (MDD) for system-level dependability analysis. We evaluate the proposed model through case studies of Bitcoin networks with homogeneous and heterogeneous nodes, investigating the influence of key parameters on network dependability.

The remainder of this paper is organized as follows: Section 2 explains the mechanisms behind the Eclipse and 51% attacks. Section 3 presents our hierarchical modeling approach for analyzing system-level dependability. Section 4 presents case studies and examines the impact of critical parameters on node- and system-level dependability. Finally, Section 5 summarizes the results and outlines future research directions.

2. Attack Models

This section focuses on two distinct types of attacks: the Eclipse attack (Heilman et al., 2015) and the 51% attack (Novoa et al., 2021).

An Eclipse attack occurs when an attacker successfully monopolizes the flow of information to and from a victim node (VN), cutting off the VN's access to legitimate network nodes. To initiate an Eclipse attack, the attacker fills the routing table of the VN with malicious addresses before a restart. After the VN restarts, it connects to these malicious nodes, losing contact with legitimate peers. At this point, the attacker controls all information flowing to and from the VN (Heilman et al., 2015).

A 51% attack is launched when malicious miners or a group of them gain control over more than 50% of the network's computing power. This allows the attackers to disrupt network operations, such as halting payments, preventing transaction confirmations, and reversing transactions to enable double-spending by altering the blockchain. Successful Eclipse attacks on multiple nodes can lead to a 51% attack, which we use to define system-level dependability in this study.

3. Proposed Hierarchical Modeling Approach

Our proposed hierarchical modeling approach integrates two components: the CTMC-based node-level dependability analysis for Eclipse attacks, and the MDD-based system-level dependability assessment for 51% attacks.

3.1 Node-Level Modeling

For node-level dependability, we utilize the CTMC-based method from Zhou et al. (2021a) to model the behavior of a Bitcoin node under an Eclipse attack. The Bitcoin node transitions through five distinct states: original (0), table hacked (1), restart (2), connected (3), and monopolized (4). The state transitions, illustrated in Figure 1, show how a victim node gradually becomes monopolized by the attacker.

- The transition from state 0 to state 1 occurs when the attacker starts filling the victim node's routing table with malicious IP addresses (transition rate λ01).
- The transition from state 1 to state 2 occurs when the victim node restarts (transition rate λ12), and from state 1 back to state 0 if the victim deletes the malicious addresses (rate μ10).

Once the node reaches state 4, the Eclipse attack is considered successful, as the attacker monopolizes the node's connections. The dependability of the node is calculated as Dnode(t) = P0(t) + P1(t) + P2(t), representing the probability of the node being in a dependable state.

3.2 System-Level Modeling

The Bitcoin system as a whole can exist in one of three states: stable (S0), exposed (S1), and dominated/failed (S2). The dominated state occurs when more than 50% of the network's nodes are controlled by an attacker, which corresponds to a successful 51% attack. For a Bitcoin network with nnn nodes, the dominated state is reached when at least ω\omegaω nodes are monopolized, where:

$$\omega = \{2n + 12n + 1 if\ n\ is\ even, if\ n\ is\ odd.$$

The system is considered to be in a stable state (S0) when at least ω\omegaω nodes are in their original state (state 0). Any state other than the stable or dominated states is defined as the exposed state (S1). The system's dependability is determined as the probability that the system is in a non-dominated state:

$$Dsystem(t) = PS0(t) + PS1(t) = 1 - PS2(t).$$

3.2.2 Heterogeneous Nodes

In networks with heterogeneous nodes, where each node may have different state probabilities, a multi-valued decision diagram (MDD) is applied to represent the system-level behavior. Each node is modeled as a five-state component, where each edge of the MDD represents the probability of the node being in a specific state.

Consider a Bitcoin network with n=4n = 4n=4 nodes (N1, N2, N3, N4). Nodes N1 and N2 share the same parameter set (normal-level protection), node N3 has an above-average level, and node N4 has a strong protection level. Using MDD modeling, the system dependability is calculated by evaluating paths from the root node to the sink nodes that represent either the stable or dominated state.

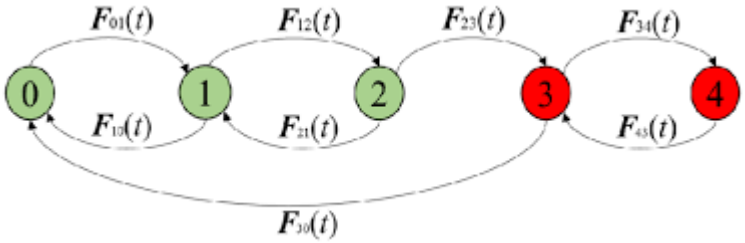

Figure 1. The state transition diagram of the Bitcoin node under the Eclipse attack.

For the dominated state, the probability is given by:

$$PS2(t) = PN1,4 \times PN2,4 \times PN3,4 + PN1,4 \times PN2,4 \times (1 - PN3,4) \times PN4,4 + \cdots$$

Similarly, for the stable state, the calculation follows the structure of the MDD model.

4. Numerical Results and Analysis

We conducted several case studies to explore the effects of various user behavior parameters on the dependability of both homogeneous and heterogeneous Bitcoin networks.

4.1 Node-Level Dependability Analysis

The dependability of individual Bitcoin nodes under different protection levels and restart habits is summarized in Table 2. It is evident that nodes with higher protection awareness tend to remain in a dependable state for longer periods. Conversely, nodes with frequent restarts are more prone to being monopolized due to the Eclipse attack's dependency on system reboots.

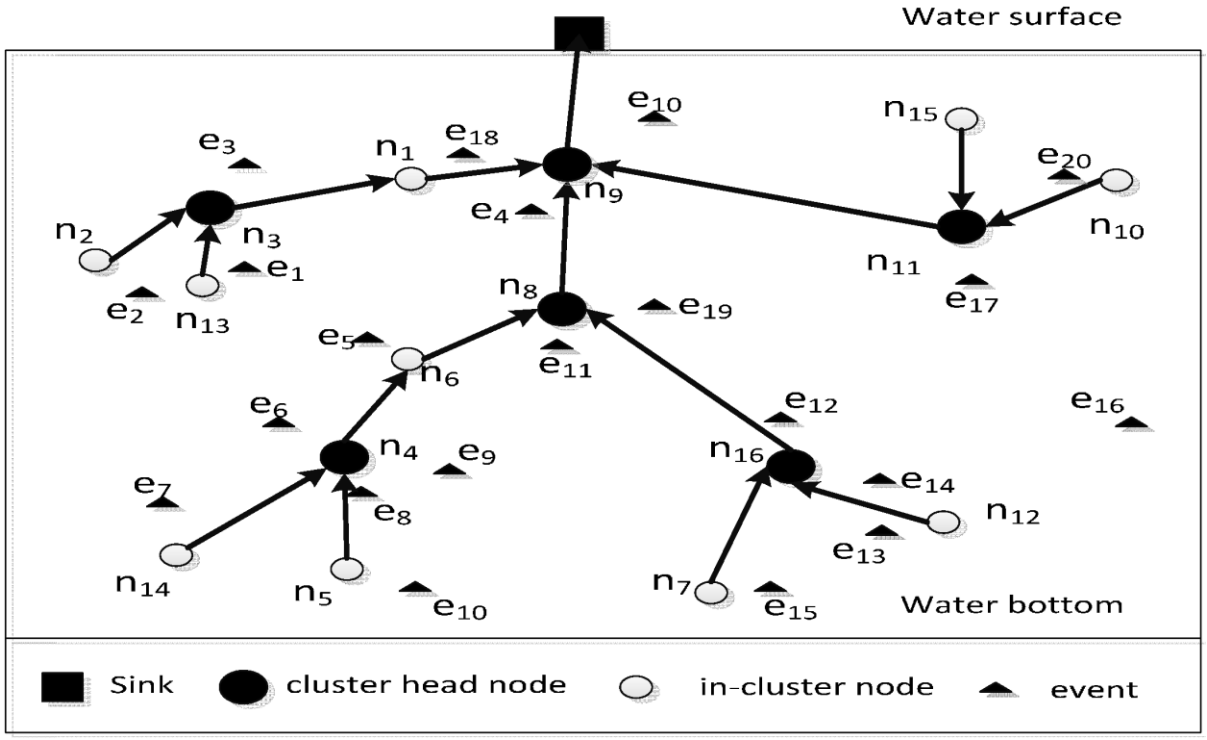

Figure 2. An MDD non-sink node modeling Bitcoin node m.

4.2 System-Level Dependability Analysis

We further explore system-level dependability under different network sizes and configurations, including homogeneous and heterogeneous nodes. Table 4 shows that larger networks exhibit higher resilience to 51% attacks, as seen in Bitcoin networks with 10, 20, and 30 nodes. Additionally, networks with miners who restart less frequently are more dependable, as shown in Figure 7.

5. Conclusions and Future Research Plan

This study proposed a hierarchical model for evaluating the dependability of Bitcoin systems under Eclipse and 51% attacks. We found that the Bitcoin system's dependability improves with increased user protection awareness and reduced

restart frequencies. In future work, we plan to extend this model to examine other attack types, such as block withholding and jumping mining attacks.

Reference

1. Bag, S., Ruj, S., & Sakurai, K. (2016). Bitcoin block withholding attack: Analysis and mitigation. *IEEE Transactions on Information Forensics and Security*, 12(8), 1967-1978.
2. Bastiaan, M. (2015). Preventing the 51%-attack: A stochastic analysis of two phase proof of work in Bitcoin. https://fmt.ewi.utwente.nl/media/175.pdf, Accessed in June 2023.
3. Eyal, I., & Sirer, E.G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In *International Conference on Financial Cryptography and Data Security* (pp. 436-454). Springer, Berlin, Heidelberg.
4. Ferrag, M.A., Derdour, M., Mukherjee, M., Derhab, A., Maglaras, L., & Janicke, H. (2018). Blockchain technologies for the Internet of Things: Research issues and challenges. *IEEE Internet of Things Journal*, 6(2), 2188-2204.
5. Frizzo-Barker, J., Chow-White, P.A., Adams, P.R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, 51, 102029. https://doi.org/10.1016/j.ijinfomgt.2019.10.014
6. Gervais, A., Ritzdorf, H., Karame, G.O., & Capkun, S. (2015). Tampering with the delivery of blocks and transactions in Bitcoin. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security* (pp. 692-705). Denver, United States.
7. Göbel, J., Keeler, H.P., Krzesinski, A.E., & Taylor, P.G. (2016). Bitcoin blockchain dynamics: the selfish-mine strategy in the presence of propagation delay. *Performance Evaluation*, 104, 23-41.
8. Heilman, E., Kendler, A., Zohar, A., & Goldberg, S. (2015). Eclipse attacks on Bitcoin's peer-to-peer network. In *24th USENIX Security Symposium* (pp. 129-144). Washington D.C., United States.
9. Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., & Zhang, Y. (2018). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet of Things Journal*, 6(3), 4660-4670.
10. Monaco, J.V. (2015). Identifying Bitcoin users by transaction behavior. In *Biometric and Surveillance Technology for Human and Activity Identification XII* (Vol. 9457, pp. 945704). International Society for Optics and Photonics. Baltimore, United States. https://doi.org/10.1117/12.2177039.
11. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Consulted*, 1(2012), 28, https://bitcoin.org/bitcoin.pdf.
12. Novoa, F., Orozco, A., Polanco, R., & Wightman, A. (2021). The 51% attack on blockchains: A mining behavior study. *IEEE Access*, 9, 140549-140564. https://doi.org/10.1109/ACCESS.2021.3119291.
13. Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the Bitcoin system. In *Security and Privacy in Social Networks* (pp. 197-223). Springer, New York, United States.
14. Sapirshtein, A., Sompolinsky, Y., & Zohar, A. (2016). Optimal selfish mining strategies in Bitcoin. In *International Conference on Financial Cryptography and Data Security* (pp. 515-532). Springer, Berlin, Heidelberg.
15. Xing, L. (2020). Reliability in internet of things: Current status and future perspectives. *IEEE Internet of Things Journal*, 7(8), 6704-6721. https://doi.org/10.1109/JIOT.2020.2993216.
16. Xing, L., & Amari, S.V. (2015). *Binary decision diagrams and extensions for system reliability analysis*. Scrivener Publishing LLC, Beverly, MA. https://doi.org/10.1002/9781119178026.
17. Xing, L., & Dai, Y. (2009). A new decision-diagram-based method for efficient analysis on multistate systems. *IEEE Transactions on Dependable and Secure Computing*, 6(3), 161-174.
18. Zhang, S., & Lee, J.H. (2019). Double-spending with a sybil attack in the Bitcoin decentralized network. *IEEE Transactions on Industrial Informatics*, 15(10), 5715-5722.
19. Zhou, C., Xing, L., & Liu, Q. (2021a). Dependability analysis of Bitcoin subject to eclipse attacks. *International Journal of Mathematical, Engineering and Management Sciences*, 6(2), 469-479.
20. Zhou, C., Xing, L., Guo, J., & Liu, Q. (2022). Bitcoin selfish mining modeling and dependability analysis. *International Journal of Mathematical, Engineering and Management Sciences*, 7(1), 16-27.
21. Zhou, C., Xing, L., Liu, Q., & Wang, H. (2021b). Semi-Markov based dependability modeling of Bitcoin nodes under eclipse attacks and state-dependent mitigation. *International Journal of Mathematical, Engineering and Management Sciences*, 6(2), 480-492.
22. Zhou, C., Xing, L., Liu, Q., & Wang, H. (2023). Effective selfish mining defense strategies to improve Bitcoin dependability. *Applied Sciences*, 13(1), 422. https://doi.org/10.3390/app13010422.