On the Routing-Aware Peering against Network-Eclipse Attacks in Bitcoin

Introduction:

In this paper, the authors address the problem of eclipse attacks in blockchain systems. An eclipse attack occurs when an attacker gains control of a majority of nodes in a peer-to-peer (P2P) network, which in turn allows them to control the flow of information and manipulate the network. The authors focus on the vulnerability of Bitcoin to eclipse attacks and explore possible countermeasures to prevent these attacks.

One such countermeasure is routing-aware peering (RAP), which aims to increase the resilience of P2P networks by considering the routing information of network connections. However, the authors evaluate the effectiveness of RAP and find that it is not effective enough to prevent eclipse attacks in Bitcoin.

The authors carry out a critical evaluation of the existing countermeasures for eclipse attacks in Bitcoin and provide recommendations for optimizing and customizing these countermeasures for each node. The authors also compare the results of their work to previous studies on routing awareness in Tor, a related network system.

The goal of this paper is to help improve the reliability of P2P networking protocols in blockchain systems and to take a step towards more secure and robust blockchain networks.

Methods:

The authors conducted a critical evaluation of routing-aware peering (RAP), a highly promising countermeasure for eclipse attacks on Bitcoin. The evaluation was based on simulations using a network topology model derived from actual Bitcoin network data and a set of metrics designed to measure the performance of RAP against eclipse attacks. The authors also compared the results of RAP with those of other available countermeasures and discussed their limitations and potential for optimization and customization.

The simulations were conducted using the ns-3 network simulator, which allows for the modeling and evaluation of various network scenarios. The authors used a network topology model derived from actual Bitcoin network data, which includes information about node connectivity, node capacities, and node behavior. The authors also used a set of metrics designed to measure the performance of RAP against eclipse attacks, including attack success rate, average latency, and average attack cost.

The data collected from the simulations was analyzed using statistical methods, including t-tests, chi-square tests, and regression analysis. The results of the analysis were used to compare the performance of RAP with that of other available countermeasures, including black-holing, which involves cutting off all incoming traffic from the attacker, and white-holing, which involves allowing only trusted nodes to participate in the network.

Overall, the authors' methods provide a thorough evaluation of the effectiveness of RAP against eclipse attacks on Bitcoin, while also highlighting its limitations and the potential for further optimization and customization.

Results:

The results of the study found that routing-aware peering (RAP), a highly promising countermeasure for eclipse attacks, had disappointing defense performance due to its weakness. The study also confirmed that Bitcoin can be protected from most Erebus attacks when these available countermeasures are carefully optimized and customized for each node.

The authors evaluated the idea of routing awareness in blockchain systems through a critical evaluation of RAP. The study compared the results of RAP with those of other inter-domain route inference algorithms used in Tor and found that there was an overall 80% difference between the inferred AS paths of the Tor connections and the data-plane paths.

The authors also noted that the routing-aware mechanisms developed for Tor cannot be directly used for Bitcoin due to the fundamental differences between the semi-permissionless nature of Tor network and the permissionless nature of Bitcoin.

Discussion/conclusion:

The authors provide an overall answer to the research question of finding an effective countermeasure against eclipse attacks in the Bitcoin network. They found that while routing-aware peering (RAP) is a highly promising countermeasure, its performance in defense against eclipse attacks was disappointing due to its weaknesses. However, the authors confirmed that Bitcoin can be protected from most Erebus attacks when available countermeasures are carefully optimized and customized for each node. The authors also highlight the importance of considering the overall reliability of blockchain P2P networking protocols in the future.

The authors explain their results by pointing out the weaknesses of RAP and the importance of considering the optimization and customization of countermeasures for each node. They also discuss the need for continued research in this field in order to achieve more highly reliable blockchain P2P networking protocols.

The implications of the results are that more work needs to be done in order to achieve reliable defense against eclipse attacks in blockchain systems, particularly in the Bitcoin network. The authors recommend that future research focus on optimizing and customizing countermeasures for each node in the network, as well as continuing to investigate new and innovative ways to improve the overall reliability of blockchain P2P networking protocols.

The limitations of the study include the fact that the results are specific to the Bitcoin network and may not be applicable to other blockchain systems. Additionally, the results of the study may change over time as new countermeasures are developed and existing ones are improved.