블록체인 환경에서의 Sybil 공격 방어를 위한 보안기법 분석

장현호, 황주영, 서정민, 정종문*
연세대학교 전기전자공학과, 연세대학교 전기전자공학과, 연세대학교 전기전자공학과,
*연세대학교 전기전자공학과

jhh0112@yonsei.ac.kr, wndud85v@yonsei.ac.kr, sjm1335@yonsei.ac.kr, *jmc@yonsei.ac.kr

Analysis of Sybil Attack Defense Methods for Blockchain Environments

Hyunho Jang, Juyeong Hwang, Jungmin Seo, Jong-Moon Chung*
Yonsei Univ Electrical and Electronic Engineering, Yonsei Univ Electrical and Electronic Engineering, Yonsei Univ Electrical and Electronic Engineering, *Yonsei Univ Electrical and Electronic Engineering

요 약

최근 혁신적인 기술로서 IoT 네트워크에서 활용도가 증대하는 블록체인 환경에서는 보안침해를 목적으로 발생하는 여러 사이버 공격이 증가하고 있다. 다양하게 변화하고 예상치 못한 방식으로 발생하는 공격에 대응하는 것은 작게는 개인정보보호부터 크게는 네트워크의 안전을 위해 매우 중요하다. 본 논문에서는 블록체인 환경에서 일어나는 대표적인 사이버공격으로 공격자가 다수의 위조된 신원을 생성하여 보안위협을 가하는 Sybil 공격을 방어하기 위한 여러 보안기법에 대해 분석하였다.

Ⅰ. 서 론

블록체인 기술은 중앙화된 기관이나 제 3 자의 개입 없이 분산화된 네트워크에 참여한 노드들이 공동으로 거래 정보가 기록된 원장을 관리하는 분산 원장 기술(Distributed Ledger Technology)을 적용하기 때문에 데이터의 무결성과 보안 성능이 입증되어 최근 크게 이슈가 되는 개인정보 보호 차원에서도 강점을 지니고 있다. 이로 인해, 금융 분야를 넘어 헬스 케어, 물류, 부동산 등 사회 전반의 다양한 분야에서 활용되고 있다. 특히 스마트 시티, 스마트 팩토리 등 사물 인터넷(IoT) 기기 수요와 사용이 기하급수적으로 증가하며 우리 삶에 편리함을 가져다 주는 IoT 네트워크에도 블록체인 기술 활용이 점차 증가하고 있다. 하지만 사이버공격으로 인해 개인정보 유출, 금융자산 도난 등 심각한 피해가 발생할 수 있다. 따라서 보안위협에 대비하기 위해 블록체인 기술에 기반한 여러 연구가 진행되고 있다. 본 논문에서는 여러 공격기법 중에서도 악의적인 행위자가 여러 신원을 생성하여 다수의 공격자가 공격하는 것처럼 공격하는 Sybil 공격이 블록체인 환경에 끼친 영향을 피해 사례를 통해 살펴보았다. 그리고 Sybil 공격을 방어하기 위한 여러 보안기법에 대해 각각 적용된 합의 알고리즘과 Sybil 저항성의 관점에서 분석하였다.

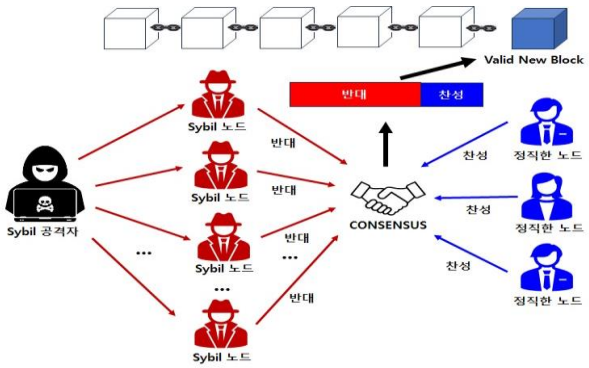
Ⅱ. 본 론

1.블록체인

블록체인 기술은 기존의 전통적인 중앙집중식 방식과는 다르게 네트워크에 참여한 노드들이 서로 데이터를 검증하고 합의를 통해 신뢰성을 유지하는 분산 네트워크 기술로서 투명성, 불변성, 분산화 등의 여러 특성을 지니고 있다. 이 때, 참여 노드들이 합의에 도달하기 위해 사용되는 다양한 유형의 핵심 프로토콜이 합의알고리즘이다. 이러한 합의알고리즘은 각각의 블록체인 환경이 요구하는 에너지 효율, 보안, 거래를 처리하는 성능 등에 따라 설계되고 계속 진화하고 있다. 대표적으로 비트코인에 사용되는 작업증명(PoW, Proof-of-Work), 이더리움 2.0 에 사용되는 지분증명(PoS, Proof-of-Stake), 비잔틴장애허용(BFT)의 개선 알고리즘인 PBFT(Practical-BFT) 등이 있다.

2.Sybil 공격

Sybil 공격은 P2P(Peer-to-Peer) 네트워크에서 공격자 노드가 다수의 가짜 신원을 생성하여 마치 다수의 노드가 공격을 수행하는 것처럼 공격 목적을 달성하는 기법이다. 그림 1 에서 보듯이 Sybil 공격자는 새로운 블록의 chaining 을 위한 합의 과정에서 다수의 Sybil 노드들로 하여금 합의에 반대하게 하여 Valid 한 새 블록의 chaining 을 방해할 수도 있으며, 이와 반대로 Invalid 한 블록을 자신들이 원하는 대로 chaining 할 수도 있다. 블록체인 환경에서의 Sybil 공격은 주로 누구나 네트워크에 접근하고 참여할 수 있도록 공개된 비허가형(Permissionless) 블록체인, 즉 공개형(Public) 블록체인에서 발생하기 쉽다 [1]. Sybil 공격은 블록체인 환경에서 다수의 가짜 노드로 블록 수신을 거부하거나 다른 노드를 네트워크에서 차단하는 등 51% 공격, 노드 평판 변조 등에 활용되며, 샤드 기반 블록체인 환경에서는 합의를 파괴하는 BCP 공격(Break-Consensus-Protocol) 또는 가짜 Transaction 을 생성하는 GFT 공격(Generate-Fake-Transaction)에 활용되기도 한다. 그 외에도 Sybil 기반 Linking 공격, DoS 공격 등 그 유형과 수법이 끊임없이 진화하고 있다.



(그림 1) Sybil 공격 동작 예시

3. 블록체인 환경에서의 Sybil 공격 사례

경제적 맥락에서 현재 Sybil 공격은 주로 암호화폐 시스템에서 빈번하게 발생하는 것으로 확인된다. 다양한 암호화폐 시스템들은 Sybil 공격으로 인한 피해와 위협에 대비하기 위해 여러 보안 메커니즘을 적용하고 있으나 최근까지도 Sybil 공격으로 인한 빈번한 피해가 발생하고 있다. 표 2 를 통해 Sybil 공격에 의한 암호화폐 시스템의 피해 현황을 살펴볼 수 있다. 가장 최근 발생한 피해로는 22 년 9 월 FTX 에서 실시한 유로스테이블코인 충전 이벤트에서 전체 Wallet 의 약 67%에 해당하는 442 개의 Wallet 을 소유한 Sybil 공격자를 통해 111,260 EUROC 가 공격자에게 획득된 것으로 추정된다. [2]

(표 1) Sybil 공격에 의한 암호화폐 피해 사례

암호화폐	Sybil 공격 피해	시기
Ethereum Classic	Sybil 공격에 의해 $5.6 million 가치의 ETC 코인이 도난당함	2020
Bitcoin SV	51% 공격에 의한 이중지불로 BSV 코인 가치를 하락시킴	2021
Euro Coin	EUROC 충전 이벤트에서 전체 71%의 Wallet 을 소유한 Sybil 공격자가 획득함	2022
Arbitrum	Arbitrum 이 발행한 ARB 토큰 전체 21%를 에어드랍받은 주소가 Sybil 공격 주소였음	2023

4. Sybil 공격 방어 기법

Sybil 공격이 발생할 수 있는 블록체인 환경의 여러 취약점에 대해 Sybil 저항성을 갖는 보안성을 보장하는 여러 방어 기법들에 대한 연구가 다양하게 진행되고 있다. 먼저, Sybil 공격을 방어하기 위해 PBFT 합의 알고리즘에 각 노드가 얼마나 정직하게 행동하는지를 주변 노드들의 평판을 기반으로 도출하는 평판 기법을 적용해 Sybil 저항성을 갖는 연구가 있었다 [3]. 다음으로 블록체인 환경의 변조방지와 데이터 구조 확장성을 통해 PoW 를 대체할 수 있는 평판 기반 분산 신뢰를 생성하는 TrustChain 을 사용하여 Sybil 저항 알고리즘인 NetFlow 를 제안한 연구도 진행되었다 [4]. 해당 연구에서는 Sybil 공격을 완화하는 게 아닌, 공격받는 동안 도출된 노드 신뢰도를 기반으로 공격자의 이익을 줄이는 부분 저항성을 갖는다. 또한, 기존의 PoW 알고리즘이 갖는 한계를 극복하고 IoT 환경에 적용하기 위해 매 Epoch 마다 신뢰값을 업데이트하고 HW 정보를 확인하여 공격자의 신원 위조나 합의 참여를 어렵게 하는 LightPoW 알고리즘을 제안한 연구도 있었다 [5]. 다음으로, PoW 의 네트워크 확장성 한계 극복을 위해 제안된 Sharding 기반의 블록체인 환경에서 Sybil 공격이 수행될 경우 치명적인 Single shard takeover attack 의 발생 확률을 확률적으로 분석하는 PGFA(Probabilistic Generating Function Approach)를 제안한 연구도 진행되었다 [6]. 해당 연구에서는 선형적

(표 2) Sybil 공격 방어 기법 (○ : 방어, △ : 피해 완화)

구분	핵심 메커니즘	방어 중점
[3]	PBFT 에 평판기법 적용	○
[4]	PoW 에 평판기법 적용	△
[5]	PoW 에 신뢰값, HW 정보 확인 적용	○
[6]	Sharding 에 PGFA 적용	○
[7]	Ethereum 환경에서의 SRM 모델 제시	○

계산 복잡성을 기반으로 실패 확률과 실패 평균 횟수를 계산해 Sybil 저항성을 확보하였다. 마지막으로 이더리움 플랫폼 기반 헬스케어 DApps 인 Medrec 을 예시로 SRM 모델(Security-Risk-Management)을 통해 Sybil 공격이 발생할 수 있는 여러 Version 을 Diagram 을 통해 제시하고 각 Version 별로 대응하는 대책을 수립한 연구가 진행되었다 [7]. 그 외에도 네트워크에 생성된 ID 를 중앙기관이 검증하거나 생성된 ID 마다 수수료를 지불하게 하는 방식 등을 통해 공격자의 Sybil 공격을 방어하는 방법도 있다.

Ⅲ. 결 론

본 논문에서는 블록체인 환경에서 발생할 수 있는 Sybil 공격의 위험을 최근 피해사례와 이를 방어할 수 있는 여러 방어기법에 대해 분석하였다. Sybil 저항성을 확보하기 위해 네트워크를 확장하여 검증노드를 늘리면 취약점을 보완할 수 있지만 보안, 확장성 측면에서 성능이 떨어지는 문제가 발생한다. 따라서 성능 트릴레마(Trilemma)를 고려하여 지속적으로 고도화되고 지능화되는 다양한 Sybil 공격에 대응하기 위해 여러 시나리오를 고려하여 기존 취약점을 개선하고 보안 성능 향상을 목표로 하는 연구가 필요할 것으로 보인다.

참 고 문 헌

[1] A. S. Rajasekaran, M. Azees, and F.Al-Turjaman, “A comprehensive survey on blockchain technology,” *Sustain. Energy Technol. Assessments*, Vol.52, Aug. 2022, Art. No.102039

[2] https://crypto.news/ftx-exchanges-traumatic-side-of-the-sybil-attack-and-losses-story-the-analysis/

[3] Alex Biryukov, Daniel Feher. “Recon: Sybil-resistant consensus from reputation,” *Pervasive and Mobile Computing*, Vol.61, 101109

[4] P.Otte, M.de Vos, and J.Pouwelse, “TrustChain: A Sybil-resistant scalable blockchain,” *Future Gener. Comput. Syst.*, Vol. 107, Jun.2020.

[5] Ahmed, Mohiuddin, et al. “A dependable and secure consensus algorithm for blockchain assisted microservice architecture,” *Computers and Electrical Engineering* 109 (2023) : 108762

[6] A. Hafid, and M. Samih “A tractable probabilistic approach to analyze sybil attacks in sharding-based blockchain protocols,” *IEEE Trans. Emerg. Topics Comput. Early Access*, Jun. 7,2022

[7] Mubashar Iqbal, Raimundas M. “Exploring Sybil and Double-Spending Risks in Blockchain Systems”, *IEEE Access*, Vol 9, May 28, 2021