블록 보류 공격 방지 기법 동향

김원웅[1], 강예준[1], 김현지[1], 임세진[1], 서화정[1]
[1]한성대학교 IT융합공학과

dnjsdndeee@gmail.com, etus1211@gmail.com, khj1594012@gmail.com,
dlatpwls834@gmail.com, hwajeong84@gmail.com

Trends of Block Withholding Attack Countermeasure

Won-Woong Kim[1], Yea-Jun Kang[1], Hyun-Ji Kim[1], Se-Jin Lim[1], Hwa-Jeong Seo[1]
[1]Dept. of IT Convergence Engineering, Han-Sung University

요 약

비트코인은 현재 가장 많이 사용하는 전자 화폐 거래 시스템으로, Proof-of-Work를 합의 알고리즘으로 사용한다. 이때 비트코인에 대한 다양한 공격기법들이 연구되었으며 대표적으로 Selfish Mining과 블록 보류 공격이 존재한다. 본 논문에서는 블록 보류 공격에 대한 방지 기법의 동향에 대해서 조사하였으며, 대표적으로 딥러닝, 평판 기반 블록체인, 게임 전략을 통한 방지 기법이 존재하였다.

1. 서론

비트코인은 P2P 시스템으로 되어있는 현재 가장 많이 사용하는 전자 화폐 거래 시스템이다. 비트코인 내에서는 블록에 대한 검증을 위해 PoW(Proof-of-Work)라고 하는 합의 알고리즘을 사용한다. 이에 따라 비트코인에 대한 다양한 공격 기법들이 연구되었으며, 이를 방지하기 위한 공격 대응 기법 또한 활발히 연구되고 있다. 공격 기법에는 대표적으로 Selfish Mining, 블록 보류 공격(Block WithHolding)기법이 있다. 이러한 기법은 채굴자들이 본인의 이익을 위하여 다른 채굴자들의 해시파워를 떨어트리며 부당한 이익을 취하는 형태이다. Selfish Mining 기법은 블록체인 네트워크 내의 더 긴 블록체인이 메인 블록체인으로 선택되고, 높은 해시 파워를 갖는 채굴자가 채굴한 블록에 대해서 브로드캐스팅하지 않고 다음 블록을 채굴해나가는 과정을 악용하여 이득을 취하는 공격 기법이다. 블록 보류 공격 기법은 마이닝 풀 내에서 기여를 하지 않고 참가 보상만을 얻으며 마이닝 풀의 연산을 낮추는 문제를 발생시킨다. 본 논문에서는 블록 보류 공격에 대한 방지 기법의 동향에 대하여 조사하였다.

2. 관련연구

2.1 PoW

PoW는 비트코인 네트워크에서 블록을 검증하기 위한 합의 알고리즘으로, 블록에 랜덤 값을 추가한 형태를 입력 값으로 하여 특정한 길이의 해시 값을 찾는 것을 목표로 한다. 이때 PoW는 목표 해시값의 길이를 조절하여 블록 채굴 난이도를 조절하며, 이는 약 10분 정도를 목표로 조절된다. 해시 값을 출력하는 단순 작업을 반복하여 목표하는 길이를 가진 블록 해시 값을 찾을 경우 해당 해시 값을 브로드캐스팅한다. 그 후 해시 값이 정직하다고 판단되었을 경우 블록체인에 해당 블록을 추가하며 블록 내의 트랜잭션들에 대한 수수료를 보상으로 얻게 된다. 이때 블록을 동시에 채굴하여 블록체인 네트워크에 fork가 발생하였을 때, 최종적으로 더 긴 블록체인을 갖는 네트워크를 메인 네트워크로 판단하게 된다.

2.2 블록 보류 공격[1-4]

블록 보류 공격은 공격자가 마이닝 풀에 참여하여 마이닝 풀에 참가한 보상만 취하고 실제 마이닝에는 기여하지 않는 공격 기법이다. 또한 보상만을 취하고 기여하지 않는 채굴자에 대해 탐지하는 것에 어려움이 존재한다. 이러한 공격은 FPoW(Full Proof-of-Work)의 경우에는 일어나지 않으며,

PPoW(Partial Proof of Work)의 경우에만 일어난다.

2.2 Selfish Mining Attack[5-6]

Selfish Mining Attack은 블록체인 네트워크 내에 fork가 일어났을 경우 더 긴 블록체인을 메인 네트워크로 선택한다는 점을 악용한 공격 기법이다. 공격자는 자신이 채굴한 블록을 브로드캐스팅 하지 않고 보류해놓으며 다음 블록을 계속해서 채굴해나간다. 그 후 블록이 충분히 쌓였을 경우 한 번에 브로드캐스팅 하여 자신의 블록체인을 메인 블록체인 네트워크로 만들어 다른 정직한 채굴자들의 네트워크를 무력화시켜 채굴 파워를 낭비하게 만들고 부당한 보상을 받게 된다. 이러한 Selfish Mining Attack의 발전 형태인 Stalker Attack과 같은 공격기법도 존재한다[7].

2.4 강화학습(Reinforcement Learning)

강화학습은 기계 학습의 일종으로, 상태 S에서 행동 A를 통해 얻게 되는 보상을 반복 측정하여 보상이 최대화될 수 있는 방향으로의 행동 또는 행동 순서를 선택하는 것을 목표로 한다.

3. 블록 보류 공격 방지 기법

P Pourtahmasbi et al.[1]은 게임 이론을 기반으로 한 평판 기반 채굴 방식을 통해 블록 보류 공격을 방지하였으며 신뢰 구간 테스트를 통해 블록 보류 공격을 효과적으로 탐지하였다. 평판은 특정 기간 동안 정직한 채굴에 대한 채굴자의 약속을 기반으로 특정 시간 간격마다 업데이트 된다. 이때 마이닝 풀 관리자는 채굴자들의 평판에 따라 마이닝 풀 초대장을 보내게 된다. 평판이 좋은 채굴자는 평판이 좋지 않은 채굴자들에 비해 높은 확률로 초대장을 받게 된다. 또한 여러 번 초대를 받은 채굴자는 자신이 원하는 마이닝 풀에 참여할 수 있는 옵션이 존재하지만, 초대를 받지 못한 채굴자는 참여할 수 없게 된다. 해당 논문에서는 실제 환경에서의 데이터를 통해 분석하기 위하여 시뮬레이션 하였으며 평판, 비평판, 공격 없음의 세 가지 경우로 나누어 시나리오를 진행하였다. 시뮬레이션은 총 해시파워, 암호화폐의 가격 등과 같은 다양한 변수를 고려하여 각 개인별로 고유한 특성을 갖도록 설계하였으며, 이 때 평판 기반의 채굴의 경우 블록 보류 공격의 수를 감소시키고 결과적으로 각 마이너들의 실제 수익이 이론상 예상 수익과 가까워지는 것을 알 수 있었다. 또한 신뢰 구간 테스트를 통해 블록 보류 공격을 효과적으로 탐지하였지만, 약간의 위양성 사례가 발견되었다.

Fujita et al.[2]은 강화학습을 통해 지능적인 마이닝 풀 선택 기능을 적용하였다. 또한 강화학습 모델 중 QL(Q-Learning), DQN(Deep Q Network), A2C(Advanced Actor-Critic)의 세 가지 모델을 채택하였다. 그 후 실제 환경에서의 보상을 측정하기 위하여 이벤트 시뮬레이터를 사용하여 성능을 측정하였다. 최종적으로 세 가지의 모델 모두 최적의 마이닝 풀을 선택하는 행동을 학습하는 데에 효과적이지만, A2C가 DQN에 비해 보상 및 수렴 성능 측면에서 DQN보다 뛰어난 것으로 나타났다.

Ren et al.[3]은 마이닝 풀 간의 블록 보류 공격에 의한 마이닝 딜레마에 중점을 두었다. 마이닝 딜레마는 하나의 마이닝 풀만이 블록 보류 공격을 수행하였을 경우 정직하게 채굴을 시도하였을 때 보다 높은 수익을 얻을 수 있게 되지만, 두 개의 마이닝 풀이 서로를 공격하게 될 경우 정직하게 채굴하는 것보다 적은 수익을 얻게 되어 모두가 손해보는 현상을 의미한다. 따라서 매 채굴 라운드마다 공격자는 블록 보류 공격을 수행할 지에 대하여 선택하여야 하며, 결과적으로 전체 네트워크 성능에 안 좋은 영향을 끼치게 된다[8]. 따라서 이러한 문제를 해결하여 시스템의 총 수익을 늘리기 위하여 마이닝 풀 선택을 최적화하는 방법으로써 zero-determinant 전략을 사용하였다. 또한 실제 수익 변동을 측정하기 위하여 30세트의 게임 전략을 시뮬레이션 한다. 최종적으로 세 가지의 zero-determinant 전략이 마이닝 풀 보상의 수렴율을 효과적으로 개선하고 블록 보류 공격이 줄어들며 시스템의 총 수익이 최대화될 수 있음을 보여주었다.

4. 결론

본 논문에서는 비트코인의 마이닝 풀에 관한 공격인 블록 보류 공격 기법에 대한 대응 방안에 대하여 조사하였다. 대표적으로 게임 전략, 평판 기반 블록체인, 딥러닝 기법이 사용되었으며, 세 방법 모두 효과적인 블록 보류 공격에 대한 대응 기법으로 사용될 수 있음을 보여주었다.

5. Acknowledgement

This work was supported by Institute of Information & communications Technology Planning & Evaluation (IITP) grant funded by the

Korea government(MSIT) (No.2022-0-00627, Development of Lightweight BIoT technology for Highly Constrained Devices).

참고문헌

[1] Pourtahmasbi, Pouya, and Mehrdad Nojoumian. "Analysis of reputation-based mining paradigm under dishonest mining attacks." *Blockchain: Research and Applications* 3.2 (2022): 100065.

[2] Fujita, Kentaro, et al. "Intelligent Mining Pool Selection in the Case of Unobservable Block Withholding Attack." *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*. IEEE, 2021.

[3] Ren, Min, Hongfeng Guo, and Zhihao Wang. "Mitigation of block withholding attack based on zero-determinant strategy." *PeerJ Computer Science* 8 (2022): e997.

[4] Chen, Zhihuai, et al. "Discouraging pool block withholding attacks in Bitcoin." *Journal of Combinatorial Optimization* 43.2 (2022): 444-459.

[5] Fayaz, Muhammad, et al. "Counteracting selfish nodes using reputation based system in mobile Ad Hoc networks." *Electronics* 11.2 (2022): 185.

[6] Schwarz-Schilling, Caspar, Sheng-Nan Li, and Claudio J. Tessone. "Stochastic Modelling of Selfish Mining in Proof-of-Work Protocols." *Journal of Cybersecurity and Privacy* 2.2 (2022): 292-310.

[7] Jesus, Emanuel Ferreira, et al. "A survey of how to use blockchain to secure internet of things and the stalker attack." *Security and Communication Networks* 2018 (2018).

[8] Ren, Min, Hongfeng Guo, and Zhihao Wang. "Mitigation of block withholding attack based on zero-determinant strategy." *PeerJ Computer Science* 8 (2022): e997.