비트코인 네트워크 공격 기법 및 대응 방안 분석*

나윤석*, 김석현**, 조영섭**, 김수형**
*과학기술연합대학원대학교 한국전자통신연구원 캠퍼스
**한국전자통신연구원
e-mail:neil123@etri.re.kr

Analysis of bitcoin network attack methods and countermeasures

YunSeok Na*, SeokHyun Kim**, YoungSeob Cho**, Soo-Hyung Kim**
*UST-ETRI
**ETRI

요 약

사토시 나카모토는 비트코인 논문을 통해서 P2P 네트워크에 기반을 둔 전자화폐인 비트코인을 제안하였다. 비트코인은 블록체인과 합의 알고리즘을 이용해 금융기관이 필요 없는 전자화폐 기술이며 이에 대한 관심이 높아지면서 비트코인에 관련된 다양한 보안 문제들이 발견되었다. 본 논문에서는 비트코인에서 발생할 수 있는 네트워크 관련 취약점을 기술하고 이에 대한 대응 방안을 분석한다.

1. 서론

2008년 사토시 나카모토는 P2P 네트워크에 기반을 둔 전자화폐인 비트코인을 제안하였다[1]. 비트코인은 두 가지 개념을 사용해서 탈중앙화된 전자화폐를 구현하였다. 첫 번째는 블록체인 데이터 구조이다. 블록체인은 디지털 서명, 머클 트리, 해시 포인터, 타임 스탬프 등을 활용하여 거래내역의 무결성을 보장한다[2]. 두 번째는 SHA256 해시 연산의 특성인 역상 저항성(preimage resistance)과 충돌 저항성(collision resistance)[3]을 활용한 합의 알고리즘이다. 비트코인 거래자들은 트랜잭션을 멤풀(mempool)에 업로드하고 채굴자는 트랜잭션을 모아서 채굴을 수행하여 블록을 생성한다. 채굴자는 거래 수수료와 새로 발행 된 비트코인을 받게 된다[1].

비트코인에 대한 관심이 높아짐에 따라 비트코인의 취약점이 발견되고 이에 따른 대응책도 발전되고 있다.

비트코인의 취약점을 이용하는 공격 기법은 여러 가지 분류로 나누어진다. 먼저, 채굴 효율성을 높이고 다른 마이닝풀의 채굴을 방해하기 위한 공격들이 있다. 이런 공격들은 마이닝풀 프로토콜의 취약점과 게임이론을 활용한다. 대표적인 공격법은 BWH(Block Withholding)[4]와 FAW(Fork After Withholding)[5] 등이 있다. 두 번째로, 검열을 활용한 공격들이 있다. 이는 비트코인에서 공격 대상의 비트코인 거래 자체를 막는 공격을 뜻한다. 대표적인 공격법은 Naive Censorship, Punitive Forking, Feather Forking 등이 있다[6]. 세 번째로, 이중 지불 공격이 있으며 이것은 같은 코인을 두 번 사용할 수 있도록 하는 것이다. 대표적인 공격법으로는 Race Attack과 Goldfinger Attack이 있다[6]. 네 번째로, 네트워크 관련 공격이 있다. 네트워크 프로토콜의 취약점을 이용하여 비트코인을 공격하는 방식이다. 대표적으로 Eclipse Attack[7]과 Hijacking Bitcoin[8]이 있다. 이외에도 많은 취약점이 있지만 대부분의 공격은 이 4가지 분류에 속한다.

이 4가지 분류 중 효율성 문제로 비트코인 네트워크 공격 기법이 최근 주목받고 있다. 대부분의 비트코인 공격 기법은 최소한 한 블록의 채굴을 성공해야 하며 높은 계산 능력을 필요로 한다. 하지만 네트워크 관련 공격은 채굴 없이 공격을 실행할 수 있어[7] 효율적이며 성공 확률도 높다. 본 논문에서는 네트워크 관련 공격 방법인 Hijacking Bitcoin과 Eclipse Attack의 개념과 대응 방식에 대해서 분석한다.

본 논문의 구성은 다음과 같다. 2장에서는 BGP와 비트코인 클라이언트의 Peer Table 구조를 살펴본다. 3장에서는 BGP와 Peer Table의 취약점을 활용한 네트워크 공격 기법에 대해서 기술한다. 4장에서 공격에 대한 대응 방법을 기술하고 분석하고 5장에서 결론을 맺는다.

2. 배경지식

본 장에서는 비트코인에 대한 네트워크 관련 공격 기법의 이해를 위해 필요한 BGP 라우팅의 개념과 프로토콜의

* 이 논문은 2018년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임(No.2016-0-00097, 비대면 본인확인을 위한 바이오 공개키 기반 구조 기술 개발)

취약성을 먼저 기술한다. 이후 비트코인 클라이언트의 취약점을 발생시키는 Peer Table의 동작 방식을 기술한다.

1) BGP(Border Gateway Protocol)

인터넷에서 패킷을 전송하는 길을 찾는 것을 라우팅이라고 한다[9]. 동일한 라우팅 정책을 가지고 있는 네트워크를 AS(Autonomous System)라고 한다. 같은 AS에서 라우팅 할 때는 RIP(Routing Information Protocol)와 OSPF(Open Shortest Path First) 등을 사용하고 다른 AS와 라우팅이 필요할 때는 주로 BGP를 사용하게 된다[9]. BGP는 가장 많이 사용되는 표준과 같은 프로토콜이지만 3가지 보안 취약점이 있다[10]. 첫 번째로 BGP 메시지는 무결성을 검증할 수 없다. 두 번째는, NLRI(Network Layer Reachability Information) 정보를 전송하는 AS의 권한 증명이 불가능하다. 세 번째는, BGP 메시지에 담겨 있는 전송 경로를 신뢰하기 어렵다. 이와 같은 문제점 때문에 BGP 하이재킹 공격이 가능하다. 공격자는 BGP 메시지를 조작하여 잘못된 라우팅 정보를 다른 AS에게 전송한다. BGP 하이재킹이 성공하면 특정 AS로 가는 모든 패킷은 공격자에게 전송된다.

2) Peer Table[7]

비트코인 노드에서 P2P 네트워크에 접속하기 위해 사용하는 IP 주소의 목록이 저장되어있는 테이블을 Peer Table이라고 한다. Peer Table은 접속이 가능하다고 알려진 주소의 목록인 New Table과 과거에 접속했었던 주소의 목록인 Tried Table로 나누어져 있다. IP 주소는 해당 IP 주소를 마지막으로 사용했던 시간이 기록된 타임스탬프와 함께 저장된다. New Table은 256개의 buckets으로 이루어져 있고 Tried Table은 64개의 buckets으로 이루어져 있다. Peer Tables에서 IP 주소를 선택하는 방법은 다음과 같다. 먼저 New Table에서 선택할지 Tried Table에서 선택할지 결정한다. 그 다음 IP 주소를 랜덤으로 선택하는데 타임스탬프가 최근일수록 선택될 확률이 증가한다. IP 주소가 저장되는 bucket의 번호는 난수, IP 주소 등을 연산하여 결정한다. <표 1>에서는 테이블의 차이와 취약점을 정리하였다.

<표 1> Peer Table 개요

	New Table	Tried Table
Buckets 숫자	256	64
과거 접속 기록	X	O
취약점	새로 갱신 또는 추가 되는 IP가 있을 경우 기존 IP주소를 버리기 때문에 공격자는 지속적으로 공격자의 IP로 접속을 시도해 테이블을 공격자 IP로 채워지도록 갱신한다.	

3 네트워크 취약점 공격 기법

3.1 Eclipse Attack

Eclipse Attack은 peer tables의 취약점을 이용하는 공격 기법이다[7]. 이 공격의 목표는 타겟이 되는 노드의 모든 통신이 공격자에게 전달되게 하는 것이다. 이 공격은 수신을 허용하는 비트코인 노드에만 사용 가능한 공격법이다.

공격은 다음과 같은 방식을 통해서 이루어진다. 먼저, 공격 대상의 Tried Table과 New Table에 공격자의 IP로 채우는 작업을 수행한다. 공격자는 공격 대상에 연결을 시도하고 연결이 완료되면 공격 대상의 Tried Table에 공격자 IP 한 개를 추가할 수 있다. 이후 공격 대상은 1,000개의 IP가 포함된 ADDR 메시지를 수락한다. 이 메시지에 포함된 IP는 New Table에 추가된다. 만약 bucket이 가득 차 있다면 오래된 IP 주소를 버리고 새로운 IP 주소를 채워 넣게 된다. 이를 통해 기존 IP 리스트를 ADDR에 포함시킨 악의적 IP 리스트로 변경할 수 있다. 또한 비트코인 노드는 DNS나 피어에게 네트워크 관련 정보를 요청하지 않는 경향이 있어 공격자는 쉽게 Table을 갱신할 수 있다. 다음으로 공격 대상의 테이블이 공격자의 IP로 가득차면, 공격 대상의 노드가 재부팅 또는 재시작 되기를 기다린다. 통계에 의하면 25%의 노드들이 10시간 안에 재시작하게 된다[7]. 재시작을 하게 되면 공격 대상은 Peer Table에 있는 공격자 IP 또는 무의미한 IP로 접속하게 된다.

공격의 효과는 다음과 같다. 먼저, 동시에 여러 개의 블록이 채굴되어 경쟁하는 블록 레이스 상황에서 블록체인에 추가될 블록을 더 높을 확률로 결정할 수 있다. 두 번째로, 채굴 능력을 분산시킬 수 있으며 세 번째로, 이기적 채굴의 확률을 높일 수 있다. 마지막으로, 이중 지불 공격이 가능하게 된다.

3.2 Hijacking Bitcoin

Hijacking Bitcoin은 BGP의 라우팅 취약점을 활용해 비트코인 네트워크를 공격하는 방법으로 Partitioning attacks과 Delay attacks 두 가지 공격 기법이 있다[8].

두 공격 모두 BGP 하이재킹을 먼저 실행하여야 한다. BGP 하이재킹은 다음과 같이 이루어진다. 먼저, 공격자는 공격 대상 노드의 IP 주소와 IP 프리픽스를 얻는다. 그리고 공격자는 IP 프리픽스가 공격 대상 노드의 IP 프리픽스 보다 더 길고, AS 라우팅 경로가 공격자의 AS로 지정된 BGP 메시지를 다른 AS에게 전송한다. 예를 들어 공격 대상 노드의 IP 주소와 IP 프리픽스가 200.0.0.0/16이고 AS2에 속해있다고 가정하자. AS2는 200.0.0.0/16 - AS2 BGP 메시지를 주변 AS에게 전송한다. 공격자는 이 BGP

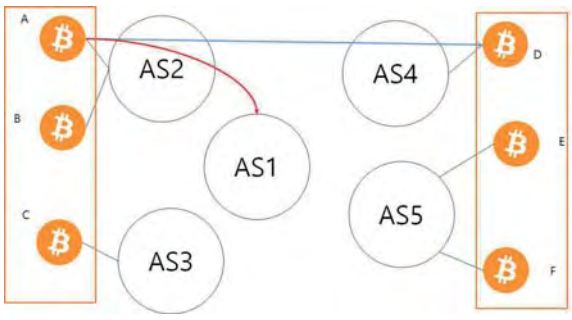
메시지를 보고 공격 대상의 IP 프리픽스 보다 더 길고 AS 라우팅 경로가 공격자의 AS 주소인 AS1으로 지정한 200.0.0.0/24 - AS1 BGP 메시지를 주변 AS에게 전송한다. BGP는 IP 프리픽스가 더 긴 주소를 우선시하기 때문에 AS2로 전달돼야 하는 트래픽이 AS1로 전송되게 된다[11]. 다음 <표 2>는 BGP를 하이재킹하기 위한 메시지의 내용을 보인다.

<표 2> BGP 하이재킹을 위한 메시지

	공격 대상의 BGP 메시지	공격자의 BGP 메시지
IP	x	x(공격 대상과 같은 IP주소)
IP Prefix	y	y+1 이상의 값
AS	공격 대상이 속해 있는 AS번호	공격자가 속해 있는 AS번호

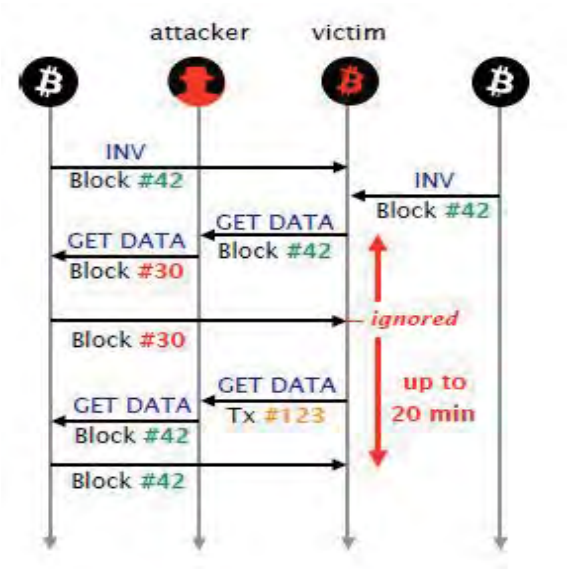
1) Partitioning attacks: 이 공격의 목표는 비트코인 네트워크 전체를 두 개의 그룹으로 나누고 이 두 그룹간의 통신을 불가능하게 하는 것이다. 즉, 고립시키고 싶은 노드들의 집합을 먼저 정의하고 이들을 전체 네트워크에서 격리시키는 것이다. (그림 1)에서 A, B, C 노드와 D, E, F 노드는 BGP 하이재킹 공격을 받아 서로 격리되어 있다. A에서 D로 블록이나 트랜잭션을 전송하고 싶어도 AS1이 AS4로 가는 패킷을 하이재킹한 후 전송을 차단한다.

공격자는 partitioning attacks을 통해서 다음과 같은 효과를 얻을 수 있다. 첫 번째로 DoS(Denial of Service) 공격이 가능하다. 네트워크에서 고립된 비트코인 클라이언트는 트랜잭션과 블록을 전송할 수 없다. AS1에 속한 공격자는 AS2, AS3에서 전송되는 모든 패킷을 차단할 수 있다. 두 번째로 피해자 그룹의 채굴 능력이 공격자보다 낮다면 피해자 그룹이 채굴한 블록을 무효화시킬 수 있다. 채굴 능력이 피해자보다 더 크기 때문이다. 채굴 능력이 더 강하면 피해자가 만들어낸 체인보다 더 긴 체인을 만들 수 있다. 이를 이용해 이중 지불 공격을 수행할 수 있다.



(그림 1) AS1에 위치하는 공격자의 공격으로 A, B, C 노드와 D, E, F 노드가 분리된 네트워크

2) Delay attacks: 이 공격의 목표는 비트코인 노드에 최신 블록 정보를 최대한 늦게 전송하는 것이다. 피해자가 GETDATA를 P2P 네트워크에 전송할 때 이 메시지를 변조하거나 GETDATA의 응답으로 돌아오는 메시지인 BLOCK을 변조하는 방식으로 공격이 이루어진다. 비트코인의 프로토콜에 의해서 유효하지 않은 데이터를 전송받은 피해자는 20분간 다른 결과를 기다리게 된다[12]. 20분은 두 번의 confirmation[2]이 일어나는 비트코인에서는 긴 시간이므로 공격자는 이를 활용한 이득을 취할 수 있다. 이를 통해 공격자가 얻을 수 있는 이득은 다음과 같다. 노드를 공격하게 되면 공격 대상은 0-confirmation 이중 지불, DoS 공격에 취약해진다. 만약 마이닝풀을 공격하게 되면 마이닝풀에 채굴능력을 낭비하게 된다. 네트워크 전체를 공격하게 되면 포크 확률을 증가시킨다.



(그림 2) GETDATA를 위조하는 Delay attack[8]

4. 대응 방법

4.1 Eclipse Attack

E. Heilman 등은 Eclipse Attack에 다음과 같은 대응 방법을 제시하였다[7].

1) 비트코인 P2P 프로토콜의 변경: 기존에는 새로운 IP가 Peer table에 추가되면 접속한 지 오래된 IP가 지워질 확률이 높았는데 이를 균등분포로 변경한다. 그리고 현재 비트코인 클라이언트는 같은 IP 주소가 다른 bucket에 들어갈 수 있는데 항상 같은 버킷에 추가되도록 변경하면 같은 IP로 여러 번 공격을 시행해도 효과가 없다.

2) 유효성 검증: Tried Table에서 새로운 IP를 추가하기 위해 접속한 지 오래된 IP 주소를 지우기 전에 접속을 시도해 정상적인 IP 주소면 삭제하지 않는다. 그리고 New Table에 있는 IP가 유효한 IP인지 지속적으로 검증한다. 마지막으로, 노드 재시작 후에 기존에 연결되어 있는 IP에 먼저 접속한다[13].

3) 연결의 다양성: Peer Table의 용량과 최대 연결 가

능 수를 늘린다. 이는 악의적 IP나 무의미한 IP와 접속될 확률을 줄여준다.

4.2 Hijacking Bitcoin

M. Apostolaki 등은 Hijacking Bitcoin에 대해 다음과 같은 대응 방법을 제시하였다[8].

1) 연결의 다양성: Eclipse Attack과 비슷한 맥락이다. 다른 AS에 있는 게이트웨이를 사용하거나 블록을 여러 개의 피어에서 수신한다. 이는 악의적 IP나 무의미한 IP와 접속될 확률을 줄여준다.

2) 네트워크 통계의 관찰: 왕복시간(RTT), UDP Heartbeat 등을 지속적으로 관찰한다.

3) BGP에 취약하지 않은 네트워크와 통신: 같은 AS에 있는 피어와 통신하거나 IP프리픽스가 24 이상인 노드와 통신한다.

4) 통신의 암호화: 블록이나 트랜잭션의 메시지가 변조되지 않게 통신을 암호화한다.

5) 제어에 사용되는 연결과 데이터 전송에 사용되는 연결을 분리한다.

5. 결론

본 논문에서는 여러 연구결과를 분석하여 비트코인 네트워크 취약점을 이용하는 공격 기법과 대응 방법을 살펴보았다. 네트워크 공격 기법은 채굴 능력 없이도 공격이 가능하기 때문에 최근 많은 주목을 받고 있다. 대표적인 네트워크 공격 기법으로는 Eclipse Attack과 Hijacking Bitcoin이 있다. Eclipse Attack은 Peer Table 프로토콜의 취약점을 이용하여 P2P 네트워크 연결을 공격자와만 수립하도록 하는 공격이다. Hijacking Bitcoin은 BGP 하이재킹을 이용해서 비트코인 네트워크를 분리시키거나 최신 블록 정보를 늦게 받도록 하는 공격이다.

Eclipse Attack과 Hijacking Bitcoin의 취약점 대응 방안의 공통점은 다음과 같다. 먼저, 형성하는 연결의 개수와 다양성을 늘리는 것이다. 이는 공격자 외에 정상적인 노드와의 연결될 가능성을 높여준다. 두 번째는, 연결을 허용하거나 차단하기 전에 연결의 유효성을 테스트하는 것이다. 유효한 연결인데 연결을 종료할 경우 공격자 IP와 연결될 확률이 높아지게 된다. 세 번째는, 네트워크 통계를 지속적으로 확인하는 것이다. 예를 들어 급격히 연결 시도가 늘어나거나 반응속도가 크게 변하면 네트워크 공격의 징후라고 판단할 수 있다.

현재 비트코인 외에도 다른 암호화폐들이 많이 활성화되어 있는 상태이다. 암호화폐 네트워크 공격 기법 관련 연구는 이더리움(Ethereum)과 모네로(Monero) 외에는 부족한 상황이다. 향후에는 다른 암호화폐들이 Eclipse Attack과 Hijacking Bitcoin에 취약한지 분석하는 연구를 수행할 필요가 있다.

참고문헌

[1] Nakamoto, Satoshi. “Bitcoin: A peer-to-peer electronic cash system.” (2008).

[2] Narayanan, Arvind, et al. Bitcoin and cryptocurrency technologies: a comprehensive introduction. Princeton University Press, 2016.

[3] Lindell, Yehuda, and Jonathan Katz. Introduction to modern cryptography. Chapman and Hall/CRC, 2014.

[4] Luu, Loi, et al. "On power splitting games in distributed computation: The case of bitcoin pooled mining." Computer Security Foundations Symposium (CSF), 2015 IEEE 28th. IEEE, 2015.

[5] Kwon, Yujin, et al. “Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin.” Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. ACM, 2017.

[6] Bonneau, Joseph, et al. “Sok: Research perspectives and challenges for bitcoin and cryptocurrencies.” Security and Privacy (SP), 2015 IEEE Symposium on. IEEE, 2015.

[7] Heilman, Ethan, et al. “Eclipse Attacks on Bitcoin's Peer-to-Peer Network.” USENIX Security Symposium. 2015.

[8] Apostolaki, Maria, Aviv Zohar, and Laurent Vanbever. “Hijacking bitcoin: Routing attacks on cryptocurrencies.” Security and Privacy (SP), 2017 IEEE Symposium on. IEEE, 2017.

[9] Kurose, James F. Computer networking: A top-down approach featuring the internet, 3/E. Pearson Education India, 2005.

[10] Murphy, Sandra. BGP security vulnerabilities analysis. No. RFC 4272. 2005.

[11] Ballani, Hitesh, Paul Francis, and Xinyang Zhang. “A study of prefix hijacking and interception in the Internet.” ACM SIGCOMM Computer Communication Review. Vol. 37. No. 4. ACM, 2007.

[12] Gervais, Arthur, et al. “Tampering with the delivery of blocks and transactions in bitcoin.” Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. ACM, 2015.

[13] Dingledine, Roger, et al. “One fast guard for life (or 9 months).” 7th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2014). 2014.