Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.28, NO.4, Aug. 2018 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2018.28.4.1009

Bitcoin Lightning Network의 강건성에 대한 연구*

이 승 진,† 김 형 식‡
성균관대학교

A Study on the Robustness of the Bitcoin Lightning Network*

Seung-jin Lee,† Hyoung-shick Kim‡
Sungkyunkwan University

요 약

Bitcoin은 블록체인을 활용한 최초의 어플리케이션으로 새로운 지불 수단으로 각광받고 있지만, 확장성에 있어서 한계점을 갖는다. Lightning Network의 개념은 최근 Bitcoin의 확장성 문제를 다루기 위해 소개되었다. 본 논문에서는 실제 Bitcoin Lightning Network가 scale-free 특성을 갖는다는 것을 밝혔다. 따라서 임의 노드 실패에 강건한 반면, 네트워크의 특정 노드를 목표로 하는 공격에 대해 취약할 수 있다. 네트워크 공격 모델의 시뮬레이션을 통해 Bitcoin Lightning Network의 강건성을 실험적으로 분석했으며, 시뮬레이션 결과는 실제로 Lightning Network가 높은 차수를 갖는 소수의 노드를 파괴하는 공격에 취약하다는 것을 보여 준다.

ABSTRACT

Bitcoin is the first application utilizing the blockchain, but it has limitations in terms of scalability. The concept of Lightning Network was recently introduced to address the scalability problem of Bitcoin. In this paper, we found that the real-world Bitcoin Lightning Network shows the scale-free property. Therefore, the Bitcoin Lightning Network can be vulnerable to the intentional attacks targeting some specific nodes in the network while it is still robust to the random node failures. We experimentally analyze the robustness of the Bitcoin's Lightning Network via the simulation of network attack model. Our simulation results demonstrate that the real-world Lightning Network is vulnerable to target attacks that destroy a few nodes with high degree.

Keywords: Lightning Network, Network robustness, Network attack, Network failure

I. 서 론

최근 블록체인(blockchain)이 새로운 지불 시스템을 위한 기술로 각광받고 있다. 블록체인은 분산화(decentralization), 투명성(transparency), 익명성(anonymity)과 같은 특징 때문에 이미 산업계에 지대한 영향을 미치고 있으며, 블록체인을 활용한 서비스와 어플리케이션도 급속도로 개발되고 있다. Bitcoin[14]은 블록체인을 활용한 최초의 어플리케이션이며, 세계의 어느 곳에서라도 누구나 즉시

Received(07. 13. 2018), Modified(08. 10. 2018), Accepted(08. 10. 2018)
* 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (No.2016-0-00078, 맞춤형 보안서비스 제공을 위한 클라우드 기반 지능형 보안 기술 개발)
* 본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학지원사업의 연구결과로 수행되었음(2015-0-00914)
† 주저자, jine33@skku.edu
‡ 교신저자, hyoung@skku.edu (Corresponding author)

결제를 할 수 있도록 설계된 분산 전자 화폐 중 하나이다. 하지만, Bitcoin은 메인 블록체인에서의 블록크기와 블록 생성 시간 때문에 확장성(scalability) 에 있어서 한계점을 갖는다. Bitcoin의 이러한 한계점을 극복하기 위해 Bitcoin 프로토콜을 수행하는 노드와 그 노드들 간의 지불 채널로 구성된 Lightning Network[13]이 개발되었다. Lightning Network는 노드의 차수(degree)가 멱함수 분포(power-law distribution)를 따르는 scale-free 특성을 갖는데, scale-free 특성을 갖는 네트워크는 노드의 차수가 갖는 분포에 의해 임의 노드에서 발생하는 오류나 공격에는 강건하지만, 소수의 차수가 높은 노드를 통해 전체 네트워크의 연결성(connectivity)을 유지하기 때문에 이러한 노드를 목표로 하는 공격에 취약할 수 있다[1][2]. 실제로 2018년 3월, Lightning Network의 일부 노드들에 대해 DDoS (Distributed Denial of Service)공격이 발생했으며, 당시 Lightning Network의 1050개의 노드 중 약 200개의 노드가 공격으로 인해 오프라인 상태가 되었다[15]. 이 공격은 단순히 특정 노드에 막대한 양의 새로운 지불 채널 생성 요청을 보냄으로써 이루어졌으며, 이 때 공격을 받은 노드는 실제 트랜젝션(transaction)에 사용되어야할 새로운 채널을 생성하지 못한다. 이러한 DDoS 공격이 허브 노드들을 잘 선별해 발생한다면 Lightning Network의 연결성에 큰 피해를 입을 수 있을 것이다.

본 논문에서는 네트워크에서의 반복적인 공격과 방어 행위를 모델링한 프레임워크[8]를 활용해 Lightning Network에서의 네트워크 실패(network failure) 모델을 시뮬레이션하고 Lightning Network의 강건성을 분석했다. 활용된 프레임워크에서는 네트워크의 노드를 불능 상태가 되도록 공격할 수 있는 공격자와 추가적인 자원을 활용해 노드를 추가할 수 있는 방어자간의 유동적 상호작용을 모델링했다. 공격자가 노드를 제거하고 방어자가 노드를 추가하는 방법에는 그 효율성을 극대화하기 위한 다양한 전략이 있을 수 있는데, 시뮬레이션을 통해 네트워크의 연결성 측면에서 각 전략의 효율성을 분석했다. 시뮬레이션 결과는 Lightning Network가 scale-free 특성을 가지며 실제로 높은 차수를 갖는 소수의 허브 노드를 파괴하는 공격에 취약하다는 것을 보여준다.

II. 배경 지식

2.1 Bitcoin Lightning Network

Lightning Network[13]은 Bitcoin의 블록체인 상에서 동작하는 오버레이(overlay) 네트워크 형태의 지불 프로토콜이며, Bitcoin의 확장성 문제를 해결하기 위해 개발되었다. Lightning Network의 핵심은 메인 블록체인에서 벗어난 오프체인(off-chain) 형태의 지불 채널에 있다. 즉, Lightning Network의 참여자들은 자신이 채널을 통해 사용할 자금을 포함하는 펀딩 트랜젝션(funding transaction)을 메인 블록체인에 브로드캐스팅 함으로써 서로 간의 양방향 지불 채널을 생성할 수 있다. 채널이 생성된 이후에는 그 채널의 두 참가자들 간의 모든 거래는 메인 블록체인에 브로드캐스팅 되지 않고 채널을 통해 이루어지며, 거래를 통해 채널을 수립할 때 메인 블록체인에 기록한 자금에 발생한 변동사항은 채널에 기록된다. 참여자 간의 거래가 종료된 후 채널이 닫힐 때에만 채널의 잔여 자금을 분배하기 위해 최종 결과에 대한 트랜젝션이 메인 블록체인에 전달된다. 이러한 지불 채널이 모여서 Lightning Network를 구성하며, 네트워크의 여러 채널을 연결한 경로를 통해 직접적인 채널을 수립하지 않고도 다른 참여자와 거래를 할 수도 있다. 메인 블록체인에 매번 트랜젝션이 브로드캐스팅 되지 않기 때문에 confirmation을 기다리지 않아도 되며 트랜젝션 수수료를 절약할 수 있다는 점에서 빈번하게 트랜젝션이 발생하는 생산자와 소비자 간의 지불 채널에서 이점을 갖는다. 하지만, 일반적으로 생산자는 Lightning Network에서 다른 많은 노드들과 연결된 일종의 허브 노드의 역할을 할 수 있으며, 이러한 경우 네트워크는 이러한 허브 노드를 목표로 하는 악의적인 공격에 취약하게 된다. 본 논문에서는 네트워크 실패 모델의 시뮬레이션을 통해 Bitcoin의 두 네트워크인 메인넷(mainnet)과 테스트넷(testnet)의 강건성을 분석한다.

2.2 커뮤니티 구조

웹, 소셜 네트워크, 모바일 네트워크 등의 크고 복잡한 네트워크에 관한 연구에서 일반적인 접근법 중 하나는 커뮤니티 구조를 추출하고 시각화하는 것이다[4]. 커뮤니티 추출 알고리즘과 관련하여 좋은

파티션을 빠르게 찾기 위한 많은 연구들이 있지만 [4]-[7], 본 논문에서는 커뮤니티 추출 알고리즘으로 Modularity 최적화 접근법을 기반으로 한 Louvain method[5]를 사용했다. Louvain method는 다른 커뮤니티 추출 알고리즘보다 시간 복잡도 측면에서 우위를 갖기 때문에 네트워크 노드 및 에지(edge) 수가 많은 경우에도 효율적으로 커뮤니티 구조를 찾을 수 있는 장점을 가진다. 알고리즘은 여러 번 단계(pass)적으로 반복하여 수행되며, 매 단계에서 Modularity Optimization, Community Aggregation의 두 과정의 절차를 순서대로 수행한다. Modularity Optimization 과정에서는 각 커뮤니티 내부 노드 사이의 거리는 짧게, 커뮤니티 간 노드 사이의 거리는 길도록, Modularity의 값이 최대가 되도록 네트워크의 각 노드에 대해 해당 노드의 이웃 노드가 속한 커뮤니티로 그 노드를 옮기는 과정을 수행한다. 가중치 그래프에 대해서 커뮤니티의 Modularity는 아래의 식 (1)과 같이 정의된다.

$$Q=\frac{1}{2m}\sum_{ij}\left[A_{ij}-\frac{k_i k_j}{2m}\right]\delta(c_i,c_j) \quad (1)$$

여기서 A_{ij}는 노드 i와 노드 j사이의 에지 가중치이며, k_i는 노드 i에 연결된 에지의 가중치 합이다. $2m$은 그래프의 모든 에지 가중치의 합이며, c_i는 노드 i의 커뮤니티, δ는 *Kronecker* 델타 함수이다. Community Aggregation 과정에서는 이렇게 추출한 커뮤니티들을 하나의 노드로 구성해 새로운 네트워크를 만드는 작업을 수행한다. 알고리즘은 더 이상 Modularity값이 향상되지 않을 때까지 반복해서 이 두 과정을 반복한다.

III. 시뮬레이션 모델

본 논문의 시뮬레이션 모델은 종래 연구[8]에서 제안된 네트워크 실패 모델을 시뮬레이션하기 위한 프레임워크를 기반으로 구현되었으며, 시뮬레이션의 타겟 네트워크는 실제 Lightning Network에 대한 정보 수집을 통해 구성했다. 시뮬레이션 프레임워크는 특정 기간 동안 그래프 G에서 반복적으로 발생하는 공격과 방어 과정으로 구성된다. 이 때, 공격자의 목표는 DDoS와 같이 노드를 파괴하는 공격을 통해 네트워크의 연결성이나 효율성이 감소되도록 피해를 최대화하는 것이며, 반대로 방어자의 목표는 새로운 자원을 활용함으로써 공격으로 인한 피해를 최소화하는 것이다. 공격 과정에서 공격자는 공격 전략에 따라 그래프 G에서 k_a개의 노드를 선택해 제거한다. 노드가 제거될 때에는 연결된 모든 에지도 함께 제거된다. 방어 과정에서 방어자는 방어 전략에 따라 그래프 G에 k_d개의 노드를 추가하고 그래프 G의 노드 중 m개의 다른 노드들과 연결한다. 직관적으로 바로 직전의 그래프 상태를 복원하는 것이 최고의 방어 전략이므로 방어자는 공격 과정에서 어떤 노드가 제거되었는지 알 수 없다고 가정한다. 방어 과정에서 추가되는 에지의 수 m은 식(2)와 같이 정의된다.

$$m = Round(w^* d(G)) \quad (2)$$

이 때, w는 방어자의 에지 생성 능력(edge construction weight), $d(G)$는 그래프 G의 평균 차수를 나타낸다. 각 변수들이 네트워크의 강건성에 미치는 영향을 알아보기 위해 k_a, k_d, w와 공격·방어 전략을 바꿔가며 시뮬레이션을 진행한다. 네트워크 강건성의 측도로는 평균 차수(average degree)와 LCC(Largest Connected Component)의 크기를 사용했다.

3.1 공격 전략과 방어 전략

시뮬레이션에서 공격자는 k_a라는 한정된 공격 능력으로 피해를 최대화하기 위해서 네트워크의 연결성을 유지하는 소수의 노드를 잘 찾을 수 있는 전략이 필요한 반면, 방어자는 k_d라는 한정된 방어 자원으로 피해를 최소화하기 위해서 네트워크의 연결성을 최대한 복원할 수 있는 전략이 필요하다. 본 논문에서는 몇 가지 전략을 고려해 시뮬레이션 함으로써 Lightning Network의 연결성에 가장 큰 영향을 줄 수 있는 공격 전략과 방어 전략을 살펴본다.

3.1.1 임의(random) 전략

임의 전략에서는 공격자가 제거할 노드와 방어자가 새로운 노드를 추가한 뒤 그래프 G에서 새로운 노드와 연결할 노드를 임의로 선택한다. 즉, 공격 과

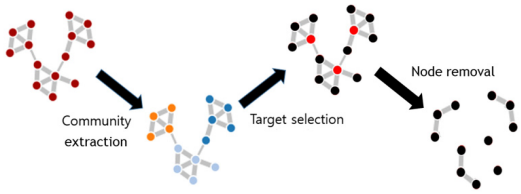


Fig. 1. Process of community-based attack strategy, where k_a = 3.

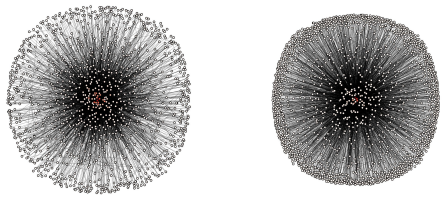
정에서 공격자는 임의로 k_a개의 노드를 선택해 제거하며, 방어 과정에서 방어자는 k_d개의 노드를 그래프 G에 추가하고 새로 추가된 각 노드가 연결될 m개의 서로 다른 노드를 임의로 선택해 에지를 생성한다. 이 전략은 공격자와 방어자가 네트워크의 토폴로지에 대한 지식이 없다고 가정하며, 다른 전략들의 효과를 비교하기 위한 기준으로 사용된다. 임의 공격(random removal)과 임의 방어(random replenishment)는 각각 A^{random}과 D^{random}으로 표기한다.

3.1.2 차수 기반(degree-based) 전략

차수 기반 전략에서는 공격자가 제거할 노드와 방어자가 새로운 노드를 추가한 뒤 그래프 G에서 새로운 노드와 연결할 노드를 노드의 차수에 따라 선택한다. 즉, 공격 과정에서 공격자는 가장 높은 차수를 갖는 k_a개의 노드를 선택해 제거하며, 방어 과정에서 방어자는 k_d개의 노드를 그래프 G에 추가하고 새로 추가된 각 노드가 연결될 m개의 서로 다른 노드를 높은 차수 순으로 선택해 에지를 생성한다. 차수 우선 공격(high-degree removal)과 차수 우선 방어(preferential replenishment)는 각각 A^{degree}와 D^{prefer}로 표기한다.

3.1.3 중심성 기반(centrality-based) 전략

중심성 기반 전략에서는 공격자가 제거할 노드와 방어자가 새로운 노드를 추가한 뒤 그래프 G에서



(a) Mainnet (b) Testnet

Fig. 2. Visualization of the Bitcoin Lightning Network

새로운 노드와 연결할 노드를 노드의 매개 중심성(betweenness centrality)에 따라 선택한다. 즉, 공격 과정에서 공격자는 가장 높은 매개 중심성을 갖는 k_a개의 노드를 선택해 제거한다. 반대로 방어 과정에서 방어자는 k_d개의 노드를 그래프 G에 추가하고 새로 추가된 각 노드가 연결될 m개의 서로 다른 노드를 낮은 매개 중심성 순으로 선택해 에지를 생성한다. 중심성은 노드의 중요도를 나타내는 측도 중 하나이며, 본 논문에서는 차수 중심성(degree centrality), 고유 벡터 중심성(eigenvector centrality), 근접 중심성(closeness centrality) 등의 다양한 중심성 중 네트워크의 연결성과 가장 밀접한 관련이 있다고 알려진 매개 중심성을 사용했다. 중심성 우선 공격(high-centrality removal)과 중심성 균형 방어(balanced replenishment)는 각각 $A^{central}$와 $D^{balanced}$로 표기한다.

3.1.4 커뮤니티 기반(community-based) 공격 전략

본 논문에서는 종래 연구[8]에서 수행한 공격 및 방어 전략에 더해 추가적으로 커뮤니티 기반 공격 전략도 고려한다. 다른 전략과 다르게 이 전략에서 공격자는 그래프 G에서 커뮤니티 구조를 먼저 추출하고 큰 커뮤니티 순으로 커뮤니티 내에서 가장 높은 차수를 갖는 노드를 선택해 총 k_a개의 노드를 제거한다. 커뮤니티 기반 공격은 $A^{community}$로 표기한다. Fig.1. 은 k_a가 3일 때 $A^{community}$의 과정을

Table 1. Properties of the Lightning Network

	$\|V\|$	$\|E\|$	Diameter	Density	$d(G)$	LCC size	$s(G)$
Mainnet	1211	5277	8	0.007	8.715	1194	1.039
Testnet	1898	4289	8	0.002	4.520	1865	1.097

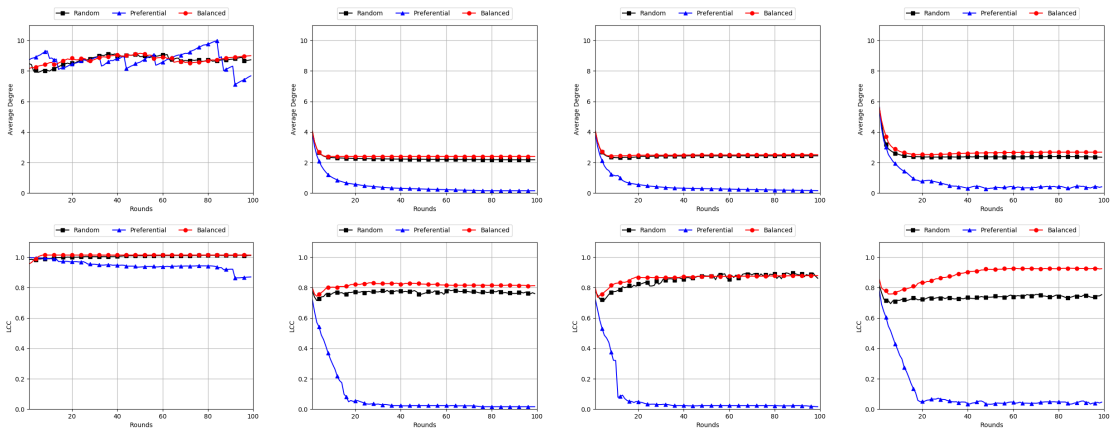


Fig. 3. Changes in the average degree and the size of largest connected component of Mainnet over the rounds. (a) A^{random}, (b) $A^{\deg ree}$, (c) $A^{central}$, (d) $A^{community}$

나타낸다. Fig.1. 의 첫 번째 그래프에서 평균 차수는 2.714, LCC의 크기는 14이다. 공격자는 먼저 Louvain method를 사용해 총 세 개의 커뮤니티 구조를 추출한 뒤, 각 커뮤니티에서 순서대로 제거할 3개의 노드를 노드의 차수에 따라 선택한다. 공격 과정이 끝난 뒤, 그래프는 부분적으로 분열되어 평균 차수는 1.091, LCC의 크기는 3이 되었다.

3.2 네트워크 구성

본 논문에서 고려하는 공격 전략과 방어 전략 실제 Lightning Network에 미치는 영향을 시뮬레이션하기 위해 먼저 Bitcoin의 메인넷과 테스트넷에서 실제로 동작하고 있는 Lightning Network의 네트워크 토폴로지를 동일하게 구성한다. Lightning Network에 대한 정보는 Lightning Network explorer[16][17]를 크롤링(crawling)해 수집했다. Fig.2. 는 수집된 정보를 통해 구성된 Lightning Network의 토폴로지이며, Fig.2. 의 (a)와 (b)는 각각 메인넷과 테스트넷의 그래프를 나타낸다. 시각화된 그래프에서 노드의 색이 짙어질수록 차수가 높은 노드임을 의미하는데 소수의 노드만 색을 가지고 있는 것을 볼 수 있다. Table 1. 은 메인넷과 테스트넷이 가지는 특성들을 나타낸다. Table 1. 에서 지름(diameter)은 그래프에서 노드 간의 최대 거리를 의미하며[9], 밀도(density)는 정규화된 평균 이웃(neighbor)의 수로 그래프에서 모든 노드들 간의 전반적인 상호작용 수준을 나타낸다[10]. $d(G)$와 $s(G)$는 각각 그래프 G의 평균 차수와 평균 최단 경로 길이를 의미한다.

IV. 시뮬레이션 결과

본 논문에서의 목표는 Lightning Network의 강건성을 경험적으로 분석하고 최적의 공격 및 방어 전략을 찾는 것이다. 이 장에서는 Lightning Network의 메인넷에 대한 시뮬레이션 결과를 서술하며, 테스트넷에 대한 시뮬레이션 결과는 부록에 제시한다(Fig.6. , Fig.7. , Fig.8. 참조).

4.1 시간 경과에 따른 연결성 변화

공격과 방어 과정이 진행됨에 따라 평균 차수와 LCC의 크기가 어떻게 변화하는지 확인하기 위해 먼저 k_a, k_d, m을 고정하고 시뮬레이션을 진행했다. Fig.3. 은 $k_a = k_d = 10$, $w = 1.0$ 일 때, 반복된 공격 및 방어 과정을 포함하는 라운드의 진행에 따른 연결성 측도의 변화를 나타낸다. LCC의 크기는 시뮬레이션을 진행하기 전 그래프의 LCC 크기로 나눔으로써 정규화된 값을 나타낸다. A^{random}(Fig.3. (a) 참조)에 대해서 D^{random}과 $D^{balanced}$가 사용되었을 때, 평균 차수와 LCC의 크기에 큰 변화가 없었다. D^{prefer}의 경우에도 약간의 변동이 있었지만 기존 그래프의 연결성을 대부분 유지했다. 즉, 모든 방어 전략은 임의 공격이나 임의 노드 실패에 대해 효

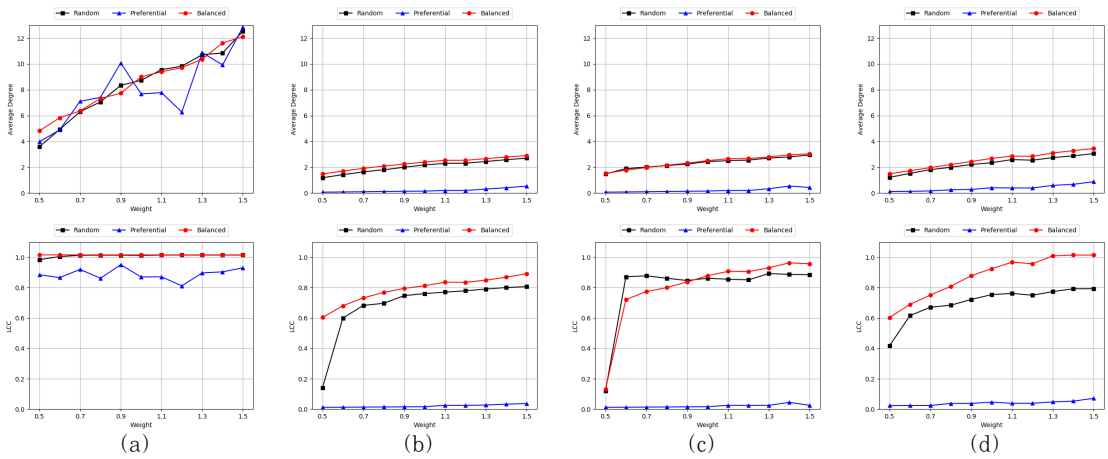


Fig. 4. Changes in the average degree and the size of largest connected component of Mainnet with varying w. (a) A^{random}, (b) A^{degree}, (c) $A^{central}$, (d) $A^{community}$

과적으로 대응할 수 있다는 것을 의미하며, 이는 scale-free 특성을 갖는 네트워크가 임의 공격과 임의 노드 실패에 대해 강건하다는 사실과 부합한다.

임의 공격 시나리오와는 다르게 다른 공격 전략들(Fig.3. 의 (b), (c), (d) 참조)에 대해서는 그래프의 평균 차수가 급격히 감소하는 모습을 보였다. 특히 D^{prefer}가 방어 전략으로 사용되었을 때, 40 라운드 만에 그래프의 평균 차수뿐만 아니라 LCC의 크기도 0에 가까워지는 결과를 보였다. D^{random}과 $D^{balanced}$의 경우에도 평균 차수가 급격히 떨어졌지만 2 이하로 감소하진 않았으며, LCC의 크기도 원래 그래프의 약 80%정도로 유지되었다. 흥미로운 점은 종래 연구[8]에서 논의되었던 평균 차수와 LCC 크기의 관계와 유사하게 평균 차수가 2 이하로 감소된 D^{prefer}가 사용되었을 경우에만 LCC의 크기가 0에 가깝게 급락했다는 것이다. 평균 차수가 2 이하로 떨어지지 않은 다른 방어 전략에 대해서는 LCC의 크기에도 약간의 감소만 있었다.

4.2 w의 변화에 따른 연결성 변화

그래프의 연결성은 방어 과정에서 방어자의 방어 능력에 따라 달라질 수 있기 때문에 방어자가 새롭게 추가하는 노드의 수와 새로운 노드에 연결될 에지의 수에 따른 그래프의 연결성 변화를 분석한다. 본 시뮬레이션을 통해 원래 그래프의 연결성을 유지하기 위해 필요한 방어 비용을 실험적으로 알 수 있다. 먼저 w의 영향을 관찰하기 위해 $k_a = k_d = 10$으로 고정하고 w가 0.5부터 1.5까지 변화할 때, 100 라운드 이후의 연결성 측도를 분석한다.

Fig.4. 에서 볼 수 있듯이 모든 공격에 대해 w가 증가함에 따라 그래프의 평균 차수가 증가하는 경향을 띈다. A^{random}(Fig.4. (a) 참조)의 경우에 어떤 방어 전략이 사용되더라도 라운드가 거듭될수록 그래프의 평균 차수는 원래 그래프의 평균 차수 이상으로 증가했으며, D^{prefer}를 제외하고는 LCC의 크기도 그대로 유지되었다. 하지만 A^{random}을 제외한 나머지 공격 전략(Fig.4. (b), (c), (d) 참조)에서는 모든 방어 전략이 w의 증가에도 불구하고 원래 그래프의 평균 차수를 회복하지 못했다. 즉, 공격자에 의해 특정 노드에서 의도적으로 발생한 공격에 대해서는 어떤 방어 전략도 평균 차수 측면에서의 연결성을 효과적으로 유지하지 못했다. 특히 D^{prefer}의 경우에는 $w = 1.5$일 때조차 평균 차수와 LCC의 크기가 0 근처에 머물렀으며, 이는 거의 모든 노드의 연결이 끊어졌다는 것을 의미한다.

다른 두 방어 전략 D^{random}, $D^{balanced}$에서는 A^{random}외의 모든 공격 전략에 대해 $w = 0.6$ 이상에서 LCC의 크기가 급증하는 모습을 보였다. 또한, $A^{community}$(Fig.4. (d) 참조)에 대해 $D^{balanced}$가 사용되고 $w = 1.5$일 때, 원래 그래프의 LCC 크기를 완전히 회복하는 모습을 보였다. 하지만, A^{degree}와 $A^{central}$에 대해서는 모든 방어 전략이 $w = 1.5$일

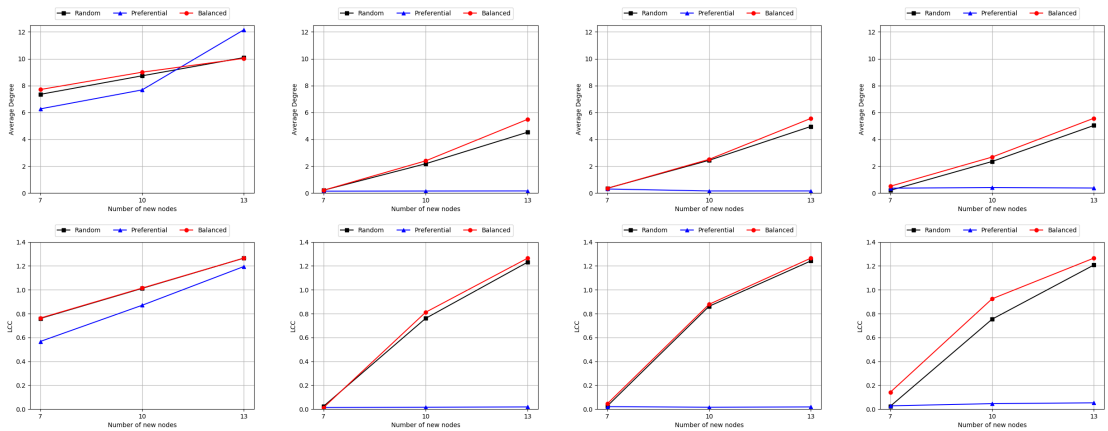


Fig. 5. Changes in the average degree and the size of largest connected component of Mainnet with varying k_d. (a) A^{random}, (b) A^{degree}, (c) $A^{central}$, (d) $A^{community}$

때에도 평균 차수와 LCC의 크기를 완전히 회복하지 못했으며, 이는 $w=1.0$일 때 방어자의 방어 능력이 공격자의 공격 능력과 동일하다는 것을 감안했을 때, 원래 그래프의 연결성을 유지하기 위해서는 방어자의 방어 능력이나 방어 비용이 공격자의 공격 능력이나 공격 비용보다 1.5배 이상 커야한다는 것을 의미한다.

4.3 k_d의 변화에 따른 연결성 변화

다음으로 방어 과정에서 새롭게 추가되는 노드의 수인 k_d의 영향을 분석한다. Fig.5. 는 $k_a=10$, $w=1.0$이고 k_d가 각각 7, 10, 13일 때, 100 라운드 후 그래프의 연결성 변화를 나타낸다. Fig.5. 에서 볼 수 있듯이 k_d가 증가함에 따라 평균 차수와 LCC의 크기 모두 증가하는 모습을 보였으나, 특정 노드를 목표로 하는 공격에 대해서는 모든 방어 전략이 $k_a=13$일 때조차 원래 그래프의 평균 차수를 회복하지 못했다. 특히, D^{prefer}의 경우에는 평균 차수와 LCC의 크기 모두 0 근처에 머물었으며, 이는 새롭게 추가되는 노드의 수를 증가시키는 것이 D^{prefer}의 효율성에 도움이 되지 못한다는 것을 의미한다.

V. 관련 연구

네트워크 강건성은 네트워크가 실패하거나 공격의 대상이 되었을 때에도 잘 동작할 수 있는 능력을 의미한다. 네트워크가 강건한지의 여부를 결정하기 위해 네트워크의 강건성을 정량적으로 측정할 수 있는 기법이 요구된다. Nagaraja 등[12]은 특정 기간 동안 반복적으로 발생하는 공격과 방어 전략의 동적 상호작용을 분석하기 위해 게임 이론을 기반으로 한 프레임워크를 제안했다. 제안 프레임워크는 네트워크의 연결성이나 효율성이 감소하도록 피해를 최대화하는 것이 목적인 공격자와 새로운 자원을 활용하여 네트워크의 피해를 최소화하려는 방어자로 구성되어 있다. 공격자와 방어자가 각자의 전략에 따라 제거할 노드와 새로운 노드를 연결할 다른 노드를 선택하는 과정이 여러 라운드동안 반복된다.

이 프레임워크에서는 방어자가 새롭게 생성할 노드의 수가 고정되어서 노드를 생성할 때의 비용을 현실적으로 모델링하지 못했기 때문에 Kim 등[8]이 더 일반화된 프레임워크로 확장했다. 따라서 확장된 프레임워크에서는 새롭게 생성할 노드의 수와 새로운 노드와 연결될 에지의 수를 변화시켰으며, 실제 네트워크를 포함하는 다양한 네트워크에서 공격 및 방어 전략의 효율성을 분석했다. 하지만 이 프레임워크에서 사용된 전략은 노드의 차수, 노드의 중심성과 같은 개별 노드의 특성만을 활용했기 때문에 본 논문에서는 종래 연구의 전략에 더해 Lightning Network을 구조적으로 분석해 커뮤니티 구조를 추출하는 새로운 공격 전략을 추가했다.

VI. 결 론

본 논문에서는 종래 연구[8]에서 사용한 네트워크 실패 및 공격 모델에 대한 프레임워크를 사용해 Lightning Network의 강건성을 경험적으로 분석했다. 시뮬레이션 결과는 Lightning Network이 scale-free 특성을 가지며, 따라서 임의 노드 실패에 강건하지만 특정 노드를 목표로 하는 공격에 의해 네트워크의 연결성이 극심하게 저하될 수 있음을 보여준다. 특히, 높은 차수를 갖는 노드를 목표로 하는 A^{degree}가 가장 효과적인 공격 전략이었으며, 방어 비용을 최대화할 수 있었다. 네트워크에서 중심성이 낮은 노드를 새로운 노드와 연결하는 $D^{balanced}$가 가장 효과적인 방어 전략이었으며, 방어자의 방어 비용을 $w=1.5$ 이상으로 늘릴 수 있다면 A^{degree}에 대해서 사용되었을 때 LCC의 크기 측면에서의 연결성을 원래 그래프의 80% 이상으로 유지할 수 있었다. D^{prefer}의 경우에는 모든 공격 전략에 대해서 최악의 성능을 보였는데, 많은 실제 네트워크는 소셜 그래프 특성을 가지며 소셜 그래프에서 새로운 노드가 네트워크에 추가되는 패턴은 우선적 연결성(preferential connectivity)을 나타내기 때문에 [11] 지속적으로 네트워크에 노드가 추가되더라도 특정 노드를 목표로 하는 공격에 의해 네트워크의 연결성에 막대한 피해를 입을 수 있다.

향후 연구로는 최고의 공격 전략인 A^{degree}를 효과적으로 방어할 수 있는 새로운 방어 전략을 개발할 것이며, 그래프 상에서의 분석이 아닌 실제 Lightning Network 상에서 노드를 제거하거나 추가하는 방법에 대해 고려할 것이다.

References

[1] Estrada, E, "Network Robustness to Targeted Attacks", The European Physical Journal B - Condensed Matter and Complex System, vol. 52, no. 4, pp. 563-574, Aug. 2006.

[2] Albert, R., Jeong, H. and Barabasi, A. -L., "Error and Attack Tolerance of Complex Networks", Nature, vol. 406, no. 6794, pp. 378-382, Jul. 2000.

[3] Iuon-Chang Lin and Tzu-Chun Liao, "A Survey of Blockchain Security Issues and Challenges", International Journal of Network Security, vol. 19, no. 5, pp. 653-659, Sep. 2017.

[4] Girvan, M. and Newman, M. E. J., "Community Structure in Social and Biological Networks", National Academy of Sciences, vol. 99, no. 12, pp. 7821-7826, Jun. 2002.

[5] Blondel, V. D., Guillaume, J. L., Lambiotte, R. and Lefebvre, E., "Fast Unfolding of Communities in Large Networks", Journal of Statistical Mechanics Theory and Experiment, vol. 2008, no. 2008, pp. P10008, Jul. 2008.

[6] Porter, M. A., Onnela, J. -P. and Mucha, P. J. "Communities in Networks", Notices of the American Mathematical Society, vol. 56, no. 9, pp. 1082 - 1166, Sep. 2009.

[7] Fortunato, S. and Castellano, C., "Community Structure in Graphs", Physics Report, vol. 486, no. 3-5, pp. 490 - 512, Feb. 2010.

[8] Kim, H. and Anderson, R. "An Experimental Evaluation of Robustness of Networks", IEEE System Journal, vol. 7, no. 2, pp. 179 - 188, Jun. 2013.

[9] Hage, P. and Harary, "Eccentricity and centrality in networks", Social Networks, vol. 17, no. 1, pp. 57 - 63, Jan. 1995.

[10] Dong, J. and Horvath, S., "Understanding network concepts in modules", BMC Systems Biology, vol. 1, no. 1, pp. 24 - 43, Jun. 2007.

[11] Barabasi, A. -L. and Albert, R. "Emergence of scaling in random networks", Science, vol. 286, no. 5439, pp. 509-512, Oct. 1999.

[12] Nagaraja, S. and Anderson, R., "The topology of covert conflict", Proceedings of the 5th Workshop on The

Economics of Information Security, pp. 250-263, Jun, 2006.
〔13〕 Poon, J. and Dryja, T., "The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments", http://lightning.network/lightning-network-paper.pdf, 2015.
〔14〕 Bitcoin Wiki, "Bitcoin", http://en.bitcoin.it/wiki, Last accessed 10 August 2018.
〔15〕 Lightning Network DDoS Sends 20% of Nodes Down, Trustnodes, https://www.trustnodes.com/2018/03/21/lightning-network-ddos-sends-20-nodes, Last accessed 10 August 2018.
〔16〕 Lightning Network Explorer, "Lightning Network Explorer", https://lnmainnet.gaben.win,Last accessed 10 August 2018.
〔17〕 Lightning Network Explorer 〔TESTNET〕, "Lightning Network Explorer", https://explorer.acinq.co, Last accessed 10 August 2018.

VII. 부 록

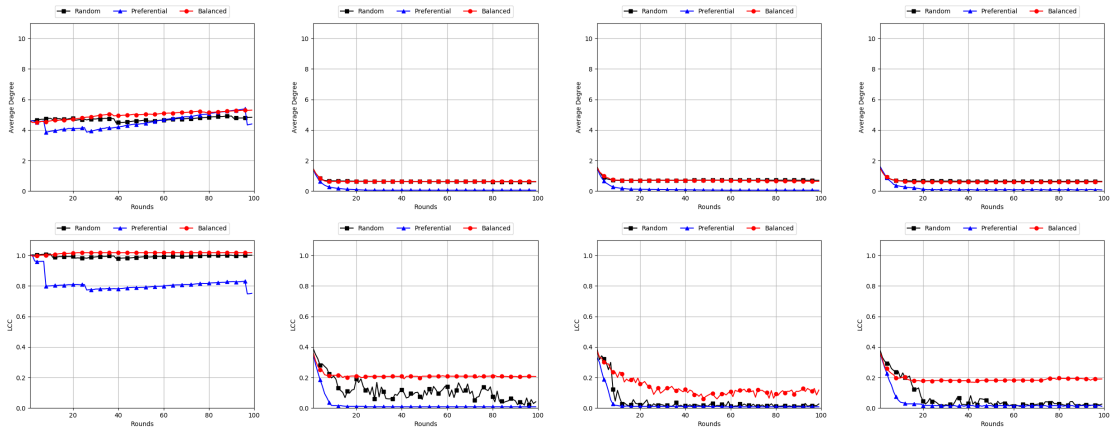


Fig. 6. Changes in the average degree and the size of largest connected component of Testnet over the rounds. (a) A^{random}, (b) A^{degree}, (c) $A^{central}$, (d) $A^{community}$

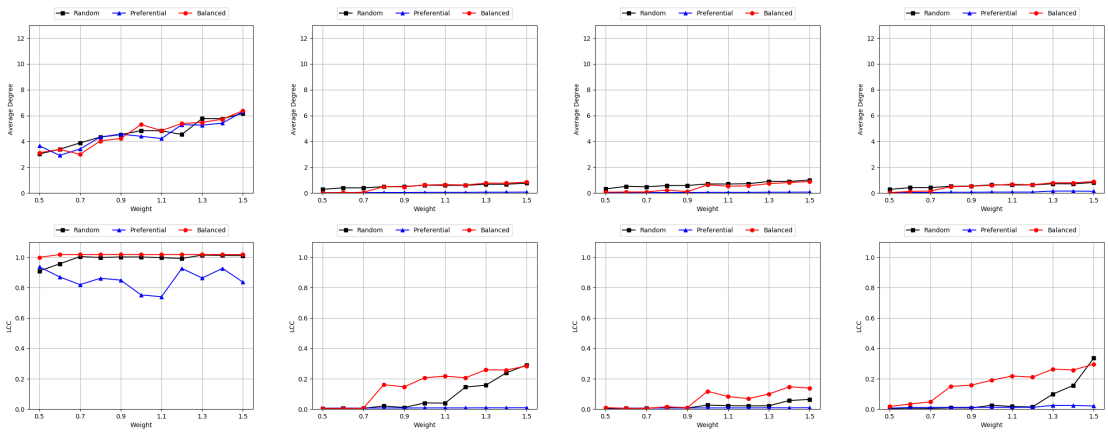


Fig.7. Changes in the average degree and the size of largest connected component of Testnet with varying w. (a) A^{random}, (b) A^{degree}, (c) $A^{central}$, (d) $A^{community}$

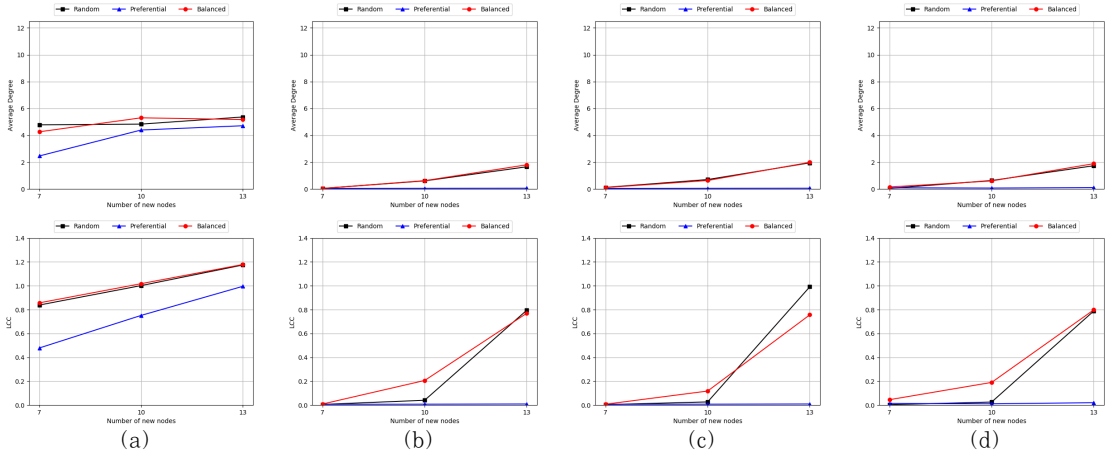
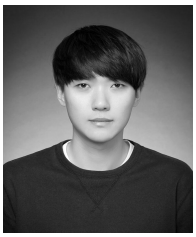


Fig.8. Changes in the average degree and the size of largest connected component of Testnet with varying k_d. (a) A^{random}, (b) A^{degree}, (c) $A^{central}$, (d) $A^{community}$

〈저자소개〉



이 승 진 (Seung-jin Lee) 학생회원
2017년 2월: 성균관대학교 컴퓨터공학과 학사
2017년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 석사과정
〈관심분야〉 정보보호, 네트워크 보안

김 형 식 (Hyoung-shick Kim) 종신회원
1999년 2월: 성균관대학교 정보공학부 학사
2001년 2월: KAIST 컴퓨터 과학과 석사
2012년 2월: University of Cambridge 컴퓨터공학과 박사
2013년 3월~현재: 성균관대학교 전자전기컴퓨터공학과 조교수
〈관심분야〉 보안공학, 소셜 컴퓨팅