(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2019-0075495
(43) 공개일자 2019년07월01일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01)
(52) CPC특허분류
H04L 63/1458 (2013.01)
(21) 출원번호 10-2017-0177121
(22) 출원일자 2017년12월21일
심사청구일자 2017년12월21일

(71) 출원인
서강대학교산학협력단
서울특별시 마포구 백범로 35 (신수동, 서강대학교)
(72) 발명자
박수용
서울특별시 마포구 독막로 18길 5 상수 두산 위브 아파트 101동 1001호
정원우
서울특별시 노원구 상계1동 미주동방 아파트 103동 1303호
이상록
서울특별시 마포구 마포대로 115-8 101동 203호
(74) 대리인
이지연

전체 청구항 수 : 총 10 항

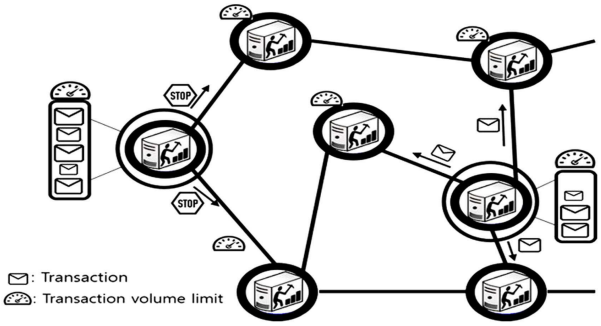
(54) 발명의 명칭 **블록체인상에서 발생하는 디도스 공격 방지 방법 및 디도스 공격 방지 가능한 블록체인 시스템**

(57) 요 약

본 발명은 블록체인상에서 발생하는 디도스 공격 방지 방법 및 블록체인 시스템에 관한 것이다. 상기 블록체인 네트워크를 구성하는 노드들에서의 디도스 공격 방지 방법은, (a) 현재 주기(n)에 대하여 실제 측정된 현재 거래 생성 크기(x_n) 및 예측된 현재 거래 생성 예측 크기($\hat{x}_n$)를 이용하여, Least mean square 방식을 적용하여 다음 주기(n+1)에 대한 미래 거래 생성 크기 ($\hat{x}_{n+1}$)를 예측하는 단계; (b) 상기 예측한 미래 거래 생성 크기($\hat{x}_{n+1}$)를 이용하여 최대 거래 생성 제한 크기 (TLV_{n+1})를 구하는 단계;를 구비한다.

본 발명은 블록체인 네트워크 시스템을 구성하는 각 노드들의 최대 거래 생성 크기를 Least Mean Square를 적용하여 동적으로 제한함으로써, 디도스 공격과 같은 Overflood attack을 방지할 수 있도록 한다.

대 표 도



이 발명을 지원한 국가연구개발사업
과제고유번호 1711055377
부처명 과학기술정보통신부
연구관리전문기관 정보통신기술진흥센터
연구사업명 SW중심대학 지원사업
연구과제명 SW중심대학(서강대학교)
기 여 율 1/1
주관기관 서강대학교 산학협력단
연구기간 2017.03.01 ~ 2017.12.31

명 세 서

청구범위

청구항 1

블록체인 네트워크를 구성하는 노드들에서의 디도스 공격 방지 방법에 있어서,

(a) 현재 주기(n)에 대하여 실제 측정된 현재 거래 생성 크기(x_n) 및 예측된 현재 거래 생성 예측 크기 ($\hat{x}_n$)를 이용하여, Least mean square 방식을 적용하여 다음 주기(n+1)에 대한 미래 거래 생성 크기 ($\hat{x}_{n+1}$)를 예측하는 단계;

(b) 상기 예측한 미래 거래 생성 크기($\hat{x}_{n+1}$)를 이용하여 최대 거래 생성 제한 크기 (TLV_{n+1})를 구하는 단계;

를 구비하여, 블록체인 네트워크를 구성하는 모든 노드들이 일정 주기동안 만들어 낼 수 있는 최대 거래 생성 크기를 동적으로 제한하여 Overflood attack을 방지하는 것을 특징으로 하는 블록체인 네트워크에서의 디도스 공격 방지 방법.

청구항 2

제1항에 있어서, 상기 (a) 단계에서 다음 주기(n+1)에 대한 미래 거래 생성 크기 ($\hat{x}_{n+1}$)는 아래의 수학식에 의해 결정되며,

$$\hat{x}_{n+1} = \max(W_n * x_n , W_n * \hat{x}_n) , 0 \leq x_n \leq TLV_n$$

여기서, Wn은 증감 가중치로서, n+1 번째 주기의 예측 거래 생성 크기를 결정하는 상수값인 것을 특징으로 하는 블록체인 네트워크에서의 디도스 공격 방지 방법.

청구항 3

제2항에 있어서, Wn+1은 아래의 수학식에 의해 결정되며,

$$W_{n+1} = W_n + \mu * (x_n - \hat{x}_n) * x_n$$

여기서, μ는 증감 가중치가 증감하는 정도를 조절하는 최적 결절 점 거리(step size) 인 것을 특징으로 하는 블록체인 네트워크에서의 디도스 공격 방지 방법.

청구항 4

제3항에 있어서, μ는 아래의 수학식에 의해 결정되며,

$$\mu = \frac{1}{x_n * TVL_n} * \frac{T_l}{T_B} * \frac{1}{I * sur_I}$$

여기서, T_I은 제한 주기로서 n번째 주기에서 n+1번째 주기가 되는데 까지 걸리는 시간이며, T_B 는 블록 주기로서 하나의 블록이 생성된 후 그 다음 블록이 생성될 때 까지 걸리는 시간이며, I 는 중요도 가중치로서 주위 노드 중요도가 얼마나 중요한지를 결정하는 무게 상수값이며, sur_I 는 주위 노드 중요도이며, TLVn은 최대 거래 생성 제한 크기로서 n번째 주기동안 최대로 생성 가능한 총 거래 크기를 나타내는 것을 특징으로 하는 블록체인 네트워크에서의 디도스 공격 방지 방법.

청구항 5

제1항에 있어서, 상기 (b) 단계에서 최대 거래 생성 제한 크기 (TLV_{n+1})는 아래의 수학식에 의해 구해지며

$$TLV_{n+1} = \frac{\hat{x}_{n+1}}{c}$$

여기서 c 는 최대 생성 비율로서, 예측 거래 생성 크기에서 허용할 수 있는 최대 거래 생성 제한 크기 비율인 것을 특징으로 하는 블록체인 네트워크에서의 디도스 공격 방지 방법.

청구항 6

디도스 공격 방지가 가능한 블록체인 네트워크 시스템에 있어서, 상기 블록체인 네트워크 시스템을 구성하는 각 노드들은,

현재 주기(n)에 대하여 실제 측정된 현재 거래 생성 크기(x_n) 및 예측된 현재 거래 생성 예측 크기($\hat{x}_n$)를 이용하여, Least mean square 방식을 적용하여 다음 주기(n+1)에 대한 미래 거래 생성 크기 ($\hat{x}_{n+1}$)를 예측하고,

상기 예측한 미래 거래 생성 크기($\hat{x}_{n+1}$)를 이용하여 최대 거래 생성 제한 크기 (TLV_{n+1})를 구하고,

상기 최대 거래 생성 제한 크기에 따라 거래 크기를 제함함으로써, 각 노드에서의 Overflood attack을 방지하는 것을 특징으로 하는 블록체인 네트워크 시스템.

청구항 7

제6에 있어서, 다음 주기(n+1)에 대한 미래 거래 생성 크기 ($\hat{x}_{n+1}$)는 아래의 수학식에 의해 결정되며,

$$\hat{x}_{n+1} = \max(W_n * x_n , W_n * \hat{x}_n) , 0 \leq x_n \leq TLV_n$$

여기서, Wn은 증감 가중치로서, n+1 번째 주기의 예측 거래 생성 크기를 결정하는 상수값인 것을 특징으로 하는 블록체인 네트워크 시스템.

청구항 8

제7항에 있어서, 증감 가중치 Wn+1은 아래의 수학식에 의해 결정되며,

$$W_{n+1} = W_n + \mu * (x_n - \hat{x}_n) * x_n$$

여기서, μ는 증감 가중치가 증감하는 정도를 조절하는 최적 결절 점 거리(step size) 인 것을 특징으로 하는

블록체인 네트워크 시스템.

청구항 9

제8에 있어서, μ는 아래의 수학식에 의해 결정되며,

$$\mu = \frac{1}{x_n * TVL_n} * \frac{T_l}{T_B} * \frac{1}{I * sur_I}$$

여기서, T_l은 제한 주기로서 n번째 주기에서 n+1번째 주기가 되는데 까지 걸리는 시간이며, T_B 는 블록 주기로서 하나의 블록이 생성된 후 그 다음 블록이 생성될 때 까지 걸리는 시간이며, I 는 중요도 가중치로서 주위 노드 중요도가 얼마나 중요한지를 결정하는 무게 상수값이며, sur_I 는 주위 노드 중요도이며, TLVn은 최대 거래 생성 제한 크기로서 n번째 주기동안 최대로 생성 가능한 총 거래 크기를 나타내는 것을 특징으로 하는 블록체인 네트워크 시스템.

청구항 10

제6항에 있어서, 최대 거래 생성 제한 크기 (TLV_{n+1})는 아래의 수학식에 의해 구해지며

$$TLV_{n+1} = \frac{\hat{x}_{n+1}}{C}$$

여기서 c 는 최대 생성 비율로서, 예측 거래 생성 크기에서 허용할 수 있는 최대 거래 생성 제한 크기 비율인 것을 특징으로 하는 블록체인 네트워크 시스템.

발명의 설명

기 술 분 야

[0001] 본 발명은 블록체인상에서 발생하는 디도스 공격 방지 방법 및 블록체인 시스템에 관한 것으로서, 더욱 구체적으로는 블록체인 네트워크 시스템을 구성하는 각 노드들의 최대 거래 생성 크기를 Least Mean Square를 적용하여 동적으로 제한함으로써, 디도스 공격과 같은 Overflood attack을 방지할 수 있도록 하는 디도스 공격 방지 방법 및 이러한 방법들이 적용된 블록체인 네트워크 시스템에 관한 것이다.

배 경 기 술

[0002] 블록체인은 p2p 기반의 신뢰 제공 기술로, 중앙 관리 시스템이 없이 p2p로 네트워크에 참여한 노드들이 서로 신뢰를 갖고 데이터를 공유할 수 있다. 블록체인 네트워크에 참여한 모든 노드들이 같은 데이터를 동일한 절차를 거쳐 블록체인을 통해 공유하고 있기 때문에, 블록체인에 저장된 데이터에 대한 무결성을 보장해 준다.

[0003] 비트코인과 이더리움은 전술한 블록체인 기술을 기반으로 하는 전자 화폐 거래 플랫폼으로, 수년간 많은 사람들이 전자화폐를 신뢰를 갖고 직접 거래를 할 수 있도록 하는 결정적인 기술로 블록체인이 사용되었다. 초기에는 전자 화폐 거래로만 사용하던 블록체인 기술이 최근들어 데이터의 신뢰와 무결성이 필요한 다양한 분야에서 사용되고 있다. 블록체인 안에서 생성된 거래와 블록은 모두 'Flooding'이라는 p2p에서 사용하는 데이터 전달 방식을 통해 블록체인 네트워크 전체에 전달된다. 이러한 데이터 전달 방식에서 발생할 수 있는 불필요한 전달을 방지하기 위하여, 블록체인 네트워크을 구성하는 각 노드들은 각 노드에 저장되는 '메모리 풀'을 확인한다. '메모리 풀'에 거래가 많이 남아 있을수록 블록체인 네트워크는 좋지 않은 영향을 받게 된다.

[0004] 한편, 블록체인 네트워크 시스템은 중앙 서버가 없기 때문에, 블록체인 네트워크를 구성하는 노드의 거래 생성 속도에 대한 제한이 없다. 각 노드의 거래 생성 속도에 대한 제한이 없기 때문에, DDoS 공격자들은 거래 생성을 이용하여 블록체인을 쉽게 공격할 수 있다.

[0005] 블록체인 네트워크에 참여한 모든 노드들은 같은 데이터를 공유하고 있다. 블록체인에서 하나의 데이터가 생성되어 네트워크 전체에 전송되어 공유되도록 하기 위해 'Flooding'이라는 p2p 시스템에서의 데이터 전송 방법을 사용하고 있다.

[0006] 도 1은 블록체인 네트워크에서 데이터 전송 방식으로 사용되는 Flooding 전달 방식을 설명하기 위하여 도시한 모식도이다. 도 1을 참조하면, 'Flooding'은 p2p 시스템에서 전송하고자 하는 데이터가 직접 연결되어 있는 노드에게 전송되고, 데이터를 전송받은 노드들은 해당 데이터를 자신과 연결되어 있는 노드들에게 다시 전송하는 방법이다. 블록체인에서 전송하는 데이터는 거래(transaction)와 블록(block)이다. 블록체인 네트워크의 모든 노드들은 'Flooding'방식을 통해 전송 받은 거래와 블록을 단순히 다시 전송하는 것이 아니라, '데이터 검증'과 '메모리풀 관리'를 통해 불필요한 전송을 방지한다. '데이터 검증'은 전송을 받은 거래와 블록이 올바른가를 검증하는 과정이다.

[0007] 블록체인 시스템에 있어서, 모든 노드들은 원활한 블록체인 네트워크를 유지하기 위하여 '메모리풀 관리'를 수행한다. '메모리풀' 이란, 블록체인 네트워크에서 발생한 거래들 중 '데이터 검증'을 통과한 올바른 거래들이 블록에 들어가기 전에 저장되어 있는 공간으로, 블록체인 네트워크를 구성하는 모든 노드들이 각각 갖고 있다. 각 노드들은 '메모리풀 관리'를 올바른 거래와 블록들이 들어왔을 때 진행한다. 우선, 거래가 들어왔을 때, 메모리풀에 저장되어 있는 거래들과 비교하여, 새로운 거래인 경우 메모리풀에 저장한 후 연결된 노드들에게 전송하고 이미 받은 거래인 경우 무시한다.

[0008] 다음, 블록이 들어왔을 때, 블록에 들어 있는 거래들을 메모리풀과 비교하여 같은 거래가 있다면 해당 거래를 메모리풀에서 제거한 후 다른 노드들로 전송한다. 또한, 메모리풀에 들어 있는 거래들 중 일정 시간동안 계속 블록에 들어가지 못한 거래들은 메모리풀에서 자동적으로 제거된다. 이처럼 블록체인 네트워크의 모든 노드의 메모리풀은 거래의 저장과 제거가 지속적으로 진행된다. 블록체인에서 하나의 블록에는 정해진 크기만큼의 거래들이 들어 갈 수 있기 때문에, 메모리풀에는 블록에 들어가길 기다리는 거래들이 항상 존재할 수 있다.

[0009] 전술한 블록체인 시스템에서 발생할 수 있는 DDoS 공격이 존재한다. 올바르게 생성된 새로운 거래들은 항상 메모리풀에 저장되고 정해진 크기만큼의 거래들만하나의 블록안에 들어 갈 수 있다. 블록체인 시스템에서 DDoS 공격 노드는 짧은 시간 동안 무수히 많은 새로운 거래를 생성하여 DDoS 공격 노드와 연결된 희생 노드들에게 전송하는 방법을 사용한다.

[0010] DDos 공격에 의한 피해는 다음과 같다. (1) 희생 노드들의 메모리풀은 공격자로부터 받은 거래들로 점차적으로 가득 차게 되고 더 이상 거래들을 저장할 수 없게 된다. 이로 인해 메모리풀 관리를 진행 한 후 다른 연결된 노드들에게 전달을 하는 시간이 늘어 나게 되고 심각하게는 더 이상 거래를 전달할 수 없게 되며 블록체인 노드로서의 역할을 할 수 없게 된다. 또한 (2) 블록체인의 모든 노드들의 메모리풀에 공격 노드가 만들어낸 거래들이 무수히 많게 되고, 이로 인해 한정적인 크기를 갖는 하나의 블록에 일반 노드들의 거래가 들어가는 데 까지 걸리는 시간이 늘어나게 되고, 심각하게는 거래가 들어가지 못하는 블록체인 노드들의 메모리풀에서 해당 거래가 삭제될 수 있다. 본 발명에서는 블록체인상에서 위와 같은 피해를 주는 DDoS 공격을 'overflood attack' 이라고 정의한다.

[0011] 도 2는 블록체인 네트워크 시스템에 발생되는 overflood attack 을 설명하기 위하여 도시한 모식도이다. 도 2와 같이, 블록체인 시스템에 있어서, 공격 노드가 주위 노드들에게 'overflood attack'은 하는 경우, 직접 공격자에게 공격을 받은 노드들은 더 이상 데이터를 다른 노드들에게 전달할 수 없게 된다.

[0012] 현재 블록체인 네트워크 시스템에서는, 각 노드가 거래를 생성하고 싶을 때, 언제든지 짧은 시간동안 거래를 무한으로 생성하여 블록체인 네트워크에 전파할 수 있다. 전자 화폐 및 실제 돈과 관계있는 블록체인 네트워크 시스템에서는 수수료가 존재하므로, 'Overflood attack'을 하고자 하는 공격 노드는 무한정으로 거래를 생성하는 것에 한계가 있기는 하나 공격의 목적을 달성할 수는 있다. 다양한 데이터의 무결성과 신뢰성 제공을 목적으로 연구되고 있는 다양한 블록체인에서는 무한으로 거래를 생성할 수 있다. 그렇기 때문에, 공격 노드는 'Overflood attack'을 시도하여 노드들의 메모리풀의 크기를 기하급수적으로 증가시켜, 피해를 발생시킬 수 있다.

[0013] 따라서, 네트워크 시스템과 P2P 시스템에서 'Overflood attack"의 형태를 이용한 DDoS 공격을 방지하기 위한 다양한 연구가 진행되고 있다. 이러한 연구들 중, 네트워크 시스템 차원 DDoS 공격을 탐지하여 시스템에서 행동을 취하는 방법인 'Detection and Filtering' 과 분산된 P2P 환경에서 P2P 시스템 노드들의 평가를 통해 공격자에게 시스템에서 행동을 취하는 방법인 'Reputation and Filtering'이 있다. 이하, 이들 각각에 대하여 설명하며,

'Detection and Filtering '에서 DDoS 공격을 탐지하기 위해 사용하는 다양한 수식 및 알고리즘들 중 하나인 "Least Mean Square(LMS)"에 대하여도 설명한다.

[0014] LMS은 'Detection and Filtering'에서 현재까지의 실제 측정값과 현재 예측값을 이용하여 미래의 값을 예측할 때 널리 사용하고 있다. LMS은 시간이 지남에 따라 n번째에서 (n+1)번째로 지나간다. LMS의 가장 큰 목적은 (n+1)번째의 예측값 $\hat{x}_{n+1}$ 과 실제 측정값 x_{n+1} 의 오차를 최소화 시키는 것이다. 이를 위해 (n+1)번째의 예측값 $\hat{x}_{n+1}$ 은 기울기 하강(gradient descent) 방법을 사용한다. (n+1)번째 예측값은 수학식 1을 통해서 구한다. Wn 은 n번째 증감 가중치이고 x_n 은 n번째까지의 측정값들이다. Wn 은 수학식 2를 통해서 구한다. 수학식 2의 μ 은 최적 결절 점 거리(step size)로 이 값에 따라 LMS의 목적인 오차를 최소화 시키는 과정의 특성이 정해진다. μ 값이 클수록 수학식 1의 결과가 발산할 확률이 올라간다. LMS를 이용하고자 하는 특성에 따라 μ 값을 최적으로 결정짓는 연구들도 존재한다. 수학식 1과 수학식 2를 시간이 지남에 따라 반복적으로 연산하여 실제 측정값 x_{n+1} 과 예측값 $\hat{x}_{n+1}$ 의 오차가 최소화된다.

수학식 1

[0015] $$\hat{x}_{n+1} = W_n^T * X_n$$

수학식 2

[0016] $$W_{n+1} = W_n + \mu * (x_n - \hat{x}_n) * X_n$$

[0017] 'Detection and Filtering'은 주로 네트워크 전체에서 발생하는 트래픽 흐름을 지속적으로 모니터링 및 분석하여 공격이 들어옴을 판단하고 대처한다. 공격이 발생하지 않았을 때의 트래픽 흐름 패턴을 기준으로 정하고 트래픽 분석을 통해 사전에 정의한 기준에 따라 공격 여부를 판단한다. 위에서 설명한 Least Mean Square은 공격이 발생하지 않은 일반적인 상태의 트래픽 흐름 패턴을 생성하기 위해 사용하는 방법 중 하나이다.

[0018] 'Flooding Attacks Detection in Traffic of Backbone Networks'은 'Detection and Filtering' 의 한 종류이다. Overflood attack과 같은 공격은 발생하였을 때, 트래픽이 수치적으로 변화하게 된다. 따라서, 비정상 트래픽을 탐지할 수 있다. 이 연구에서 비정상 트래픽을 탐지하기 위한 기준이 되는 정상 트래픽을 만들 때 사용한 방법이 Least Mean Square 이다. Least Mean Square을 이용하여 현재 측정값과 예측값을 토대로 미래의 예측값을 예상하여 정상 트래픽 기준을 생성 한다. Chi-square divergence을 이용하여 예측값과 실제 측정값의 차이를 계산한다. 이렇게 계산된 값으로 공격이 발생하였을 때를 탐지하게 된다.

[0019] 이 연구가 블록체인의 overflood attack을 방지하기 위해 적용을 하였을 때의 한계점으로는 부정 오류가 생기는 확률과 탐지 시간이 반비례한다는 것이다. 전술한 방법에서는, 공격 탐지의 정확도를 올리기 위해서는 트래픽을 판단하는 탐지 시간을 길게 해야 한다. 그렇기 때문에, 공격을 탐지하기까지 걸리는 시간이 너무 길다면, 블록체인에서 발생하는 overflood attack이 충분히 일어나 블록체인 노드에 피해를 주고 난 뒤에서야 공격 탐지를 할 수 있게 되는 것이다. 공격을 탐지하기 위해서는 언제나 네트워크 전체에서 실행이 되고 있어야 한다. 그에 따라 모든 노드가 항상 소비해야 하는 컴퓨팅 파워와 메모리 공간이 크다. 또한 공격이라 판단을 하는 기준 값(threshold)에 따라 올바른 탐지의 확률이 영향을 많이 받게 된다. 판단 기준값을 낮춘 다면, 모든 overflood attack을 항상 탐지할 수 있지만, 그에 따라 정상적인 트래픽 역시 공격으로 판단할 수 있다. 항상 긍정 오류와 부정 오류가 존재하고 탐지를 위해 소비되는 리소스가 많기 때문에, 분산 환경인 블록체인에 적용하여

overflood attack을 방지 하는데에 사용하기에는 한계점이 많다.

[0020] 'Reputation and Filtering' 은 시스템에서 발생하는 DDoS 공격을 시스템에 참여하고 있는 노드들의 평가를 통해 공격을 시도하는 노드들을 시스템 자체적으로 차단 혹은 불이익 등을 통해 방지하고자 하는 연구이다.

[0021] 'Credit Model and Message Rate Control'은 P2P 시스템에서 노드들을 평가하고 평가된 등급에 따라 노드들이 생성할 수 있는 메시지 양을 다르게 주는 것을 통해 DDoS공격을 방지한다. 하나의 노드에서 모든 노드들을 평가하기에는 시스템 적으로 너무 무거울 수 있기 때문에, 이 연구에서는 노드들의 역할을 Credit Model Node(CMN), Message Rate Controlling Model Node(MRCMN)과 General Node(GN)으로 나누었다. CMN은 평가를 하는 노드로 시스템을 구성하는 모든 노드들의 정보를 수집하여 등급 평가를 하여 MRCMN에게 전달을 한다. MRCMN은 전달받은 등급을 기준으로 모든 노드들의 메시지 생성양을 조절한다.

[0022] 이 연구의 내용을 블록체인 네트워크 시스템에 대한 overflood attack을 방지하기 위해 적용하는 경우, 몇몇 노드들에게만 평가와 조절을 할 수 있는 권한을 주는 한계점이 발생한다. 즉, 모든 노드들이 동일한 역할을 수행하지 않게 되는 것이다. 평가를 위해 수집하는 데이터의 양이 많을수록 더 정확한 평가 결과를 얻을 수 있기 때문에 많은 저장 공간을 요구하게 된다. Overflood attack을 시도한 노드는 등급이 낮아지게 되어 메시지 생성양의 제한이 걸리게 되지만 그 등급의 부정 오류 확률과 평가를 위해 수집하는 데이터의 시간이 반비례하는 한계점이 존재한다. 짧은 시간동안의 데이터를 이용하여 평가한다면, overflood attack을 하는 노드를 항상 막을 수 있게 된다. 그러나 공격을 하지 않은 일반 노드까지도 overflood attack을 하는 노드와 같이 평가 등급이 낮아질 수 있게 된다. 또한 긴 시간동안의 데이터를 이용하여 평가한다면, overflood attack이 충분하게 시도된 후에서야 해당 노드의 등급이 낮아지게 된다. 항상 평가를 위해 방지 방안이 시스템에 작용을 하고 있어야 함으로 이는 블록체인 자체 성능에 영향을 주게 되는 문제점이 있다.

[0023] 블록체인 네트워크에서 발생하는 overflood attack을 방지하기 위해 위에서 설명한 방지 방안들을 적용하였을 때, 아래와 같은 한계점이 발생하게 된다. 첫째, 방지 방안을 블록체인에 적용하기 위해 사전에 필요한 데이터 정보군이 필요하다. 둘째, 공격을 탐지하기 위해 블록체인 네트워크 상에서 항상 작동하고 있어야 하기 때문에 시스템 자체가 무거워질 수 있으며, 공격자의 능력에 따라 방지 방안이 무용지물이 될 수 있다. 마지막으로, 셋째, 'Overflood attack'을 하는 공격자들은 빈번히 ‘좀비 피시’ 를 이용하고 공격자는 뒤에 숨어 있기 때문에 공격에 이용당한 노드들이 피해를 보게 된다.

[0024] 한편, 블록체인에 적용하였을 때에의 가장 큰 문제점은 완전하게 공격과 공격이 아닌 것에 대한 분리를 확실하게 할 수 없다는 것이다. 위와 같은 방지 방안들은 언제나 부정 오류 확률이 존재한다. 이는 현재까지도 많은 연구에서 말하는 한계점이다. DDoS공격 혹은 공격자로 판단하기까지 걸리는 시간과 판단의 기준 값(threshold)에 따라 공격 방지 성공률이 확연하게 차이가 난다. 판단 시간과 판단의 기준값에 대한 확실한 정의가 어렵다.

선행기술문헌

특허문헌

[0025] (특허문헌 0001) 한국공개특허공보 제 10-2012-0006250호

(특허문헌 0002) 미국공개특허공보 US 2017/0324757

발명의 내용

해결하려는 과제

[0026] 전술한 문제점을 해결하기 위한 본 발명의 목적은 'Least Mean Square(LMS)'을 응용하여 블록체인 노드들의 개별적 거래 생성 크기를 고려하려 최대 거래 생성 크기를 제한함으로서, 블록체인 네트워크를 구성하는 노드들에서의 디도스 공격 방지 방법을 제공하는 것이다.

[0027] 본 발명의 다른 목적은 각 노드들의 최대 거래 생성 크기를 동적으로 제한함으로서, Overflood attack과 같은 디도스 공격을 방지할 수 있도록 한 블록체인 네트워크 시스템을 제공하는 것이다.

과제의 해결 수단

[0028] 전술한 기술적 과제를 달성하기 위한 본 발명의 제1 특징에 따른 블록체인 네트워크를 구성하는 노드들에서의 디도스 공격 방지 방법은, (a) 현재 주기(n)에 대하여 실제 측정된 현재 거래 생성 크기(x_n) 및 예측된 현재 거래 생성 예측 크기($\hat{x}_n$)를 이용하여, Least mean square 방식을 적용하여 다음 주기(n+1)에 대한 미래 거래 생성 크기 ($\hat{x}_{n+1}$)를 예측하는 단계; (b) 상기 예측한 미래 거래 생성 크기($\hat{x}_{n+1}$)를 이용하여 최대 거래 생성 제한 크기 (TLV_{n+1})를 구하는 단계;를 구비하여, 블록체인 네트워크를 구성하는 모든 노드들이 일정 주기동안 만들어 낼 수 있는 최대 거래 생성 크기를 제한하여 Overflood attack을 방지한다.

[0029] 전술한 제1 특징에 따른 블록체인 네트워크를 구성하는 노드들에서의 디도스 공격 방지 방법에 있어서, 상기 (a) 단계에서 다음 주기(n+1)에 대한 미래 거래 생성 크기 ($\hat{x}_{n+1}$)는 아래의 수학식에 의해 결정되며,

$$\hat{x}_{n+1} = \max(W_n * x_n , W_n * \hat{x}_n) , 0 \leq x_n \leq TLV_n$$

[0030]

[0031] 여기서, Wn은 증감 가중치로서, n+1 번째 주기의 예측 거래 생성 크기를 결정하는 상수값이다.

[0032] 전술한 제1 특징에 따른 블록체인 네트워크를 구성하는 노드들에서의 디도스 공격 방지 방법에 있어서, Wn+1은 아래의 수학식에 의해 결정되며,

$$W_{n+1} = W_n + \mu * (x_n - \hat{x}_n) * x_n$$

[0033]

[0034] 여기서, μ는 증감 가중치가 증감하는 정도를 조절하는 최적 결절 점 거리(step size) 이다.

[0035] 전술한 제1 특징에 따른 블록체인 네트워크를 구성하는 노드들에서의 디도스 공격 방지 방법에 있어서, μ는 아래의 수학식에 의해 결정되며,

$$\mu = \frac{1}{x_n * TVL_n} * \frac{T_l}{T_B} * \frac{1}{I * sur_I}$$

[0036]

[0037] 여기서, Tl은 제한 주기로서 n번째 주기에서 n+1번째 주기가 되는데 까지 걸리는 시간이며, TB 는 블록 주기로서 하나의 블록이 생성된 후 그 다음 블록이 생성될 때 까지 걸리는 시간이며, I 는 중요도 가중치로서 주위 노드 중요도가 얼마나 중요한지를 결정하는 무게 상수값이며, surI 는 주위 노드 중요도이며, TLVn은 최대 거래 생성 제한 크기로서 n번째 주기동안 최대로 생성 가능한 총 거래 크기를 나타낸다.

[0038] 전술한 제1 특징에 따른 블록체인 네트워크를 구성하는 노드들에서의 디도스 공격 방지 방법에 있어서, 상기 (b) 단계에서 최대 거래 생성 제한 크기 (TLV_{n+1})는 아래의 수학식에 의해 구해지며

$$TLV_{n+1} = \frac{\hat{x}_{n+1}}{C}$$

[0039]

[0040] 여기서 c 는 최대 생성 비율로서, 예측 거래 생성 크기에서 허용할 수 있는 최대 거래 생성 제한 크기 비율이다.

[0041] 본 발명의 제2 특징에 따른 디도스 공격 방지 가능한 블록체인 네트워크 시스템에 있어서, 상기 블록체인 네트워크 시스템을 구성하는 각 노드들은,

[0042] 현재 주기(n)에 대하여 실제 측정된 현재 거래 생성 크기(x_n) 및 예측된 현재 거래 생성 예측 크기($\hat{x}_n$)를 이용하여, Least mean square 방식을 적용하여 다음 주기(n+1)에 대한 미래 거래 생성 크기 ($\hat{x}_{n+1}$)를 예측하고, 상기 예측한 미래 거래 생성 크기($\hat{x}_{n+1}$)를 이용하여 최대 거래 생성 제한 크기 (TLV_{n+1})를 구하고, 상기 최대 거래 생성 제한 크기에 따라 거래 크기를 제함함으로써, 각 노드에서의 Overflood attack을 방지한다.

발명의 효과

[0043] 본 발명에 따른 블록체인 네트워크에서의 DDoS 공격 방지 방법은 'Least Mean Square'을 응용하여 블록체인 노드들의 거래 사용성을 고려하여 동적 최대 거래 생성 크기를 제한함으로써, 공격자의 overflood attack을 성공시킬 수 없도록 한 것을 특징으로 한다.

[0044] 도 3은 본 발명에 따른 DDoS 공격 방지 방법과 종래의 연구 방법들을 정량적으로 평가한 결과들을 도시한 도표이다. 도 3에서 본 발명에 따른 DDoS 공격 방지 방법은 "동적 거래 크기 제한"으로 표시된다.

[0045] 도 3을 참조하면, 본 발명에 따른 '동적 거래 크기 제한' 에서는 종래의 다른 연구들의 가장 큰 문제점이었던 부정 오류의 확률이 없음을 알 수 있다. 이용당한 노드의 피해를 살펴 보면, DDoS 공격에서 대부분의 실제 공격자들은 일반 노드 뒤에서 일반 노드를 이용하기 때문에, 이용당한 노드의 피해가 생기는 것은 블록체인에 적용하였을 때 문제가 발생하게 된다.

[0046] 한편, 본 발명에 따른 '동적 거래 크기 제한'은 거래 생성을 제한시키기 때문에, 거래 생성의 자유를 '보통'으로 평가하였다. 하지만, 본 발명에 따른 '동적 거래 크기 제한'은 Least mean square을 통해 실제 거래 생성양을 고려하여 매 주기마다 동적으로 제한 크기가 정해지기 때문에, 거래를 꾸준히 생성하는 노드들은 실제 거래 생성이 방해되지 않게 된다.

[0047] 한편, 공격을 막는 시점은 공적 이전과 공격 도중으로 나눌 수 있는데, 관련 연구들은 공격을 막는 시점, 부정 오류 확률과 공격 방어 능력이 서로 많은 영향을 주게 되어 가장 최적인 지점을 결정하기가 어렵다. 하지만, 본 발명에 따른 '동적 거래 크기 제한'은 공격을 막는 시점이 공격 이전이므로, 공격을 보다 효율적으로 막을 수 있게 된다.

[0048] 또한, 도 3을 통해, 종래의 관련 연구들을 블록체인 네트워크를 구성하는 모든 노드들에게 적용하여 실행하기에서는 상시 수행되어야 할 부하와 리소스 소비가 본 발명에 따른 '동적 거래 크기 제한'보다 훨씬 높음을 알 수 있다.

도면의 간단한 설명

[0049] 도 1은 블록체인 네워크에서 데이터 전송 방식으로 사용되는 Flooding 전달 방식을 설명하기 위하여 도시한 모식도이다.

도 2는 블록체인 네트워크 시스템에 발생되는 overflood attack 을 설명하기 위하여 도시한 모식도이다.

도 3은 본 발명에 따른 DDoS 공격 방지 방법과 종래의 연구 방법들을 정량적으로 평가한 결과들을 도시한 도표이다.

도 4는 본 발명에 따라 디도스 공격 방지를 위한 '동적 거래 크기 제한'을 적용한 블록체인 네트워크 시스템을 개념적으로 도시한 모식도이다.

도 5는 본 발명에 따른 디도스 공격 방지 방법에 의해 각 노드들에 대한 동적 거래 크기 제한에 사용되는 변수들을 정의한 도표이다.

도 6은 시나리오 1에 따라 공격이 없을 때 초당 2개의 거래가 지속적으로 생성될 때의 메모리 풀의 크기를 도시한 그래프이다.

도 7은 시나리오 2에 따라, 블록체인에 'overflood attack'이 발생하였을 때의 메모리 풀의 크기를 도시한 그래

프이다.

도 8은 본 발명에 따른 방법, 즉 시나리오 3이 적용된 후의 'overflood attack'이 발생하였을 때의 메모리 풀의 크기를 도시한 그래프이다.

도 9는 시나리오 1의 시간에 따른 완전 전달 시간을 측정한 결과를 도시한 그래프이다.

도 10은 시나리오 2의 시간에 따른 완전 전달 시간을 측정한 결과를 도시한 그래프이다.

도 11은 시나리오 3의 시간에 따른 완전 전달 시간을 측정한 결과를 도시한 그래프이다.

도 12는 서로 다른 최대 생성 비율(C)에 따라 최대 거래 생성 제한 크기(TVL_n)의 크기를 도시한 그래프이다.

발명을 실시하기 위한 구체적인 내용

[0050] 이하, 첨부된 도면을 참조하여, 본 발명에 따른 블록체인 네트워크에서의 디도스 공격 방지 방법 및 디도스 공격 방지 가능한 블록체인 네트워크에 대하여 구체적으로 설명한다.

[0051] 먼저, 'Overflood attack'과 같은 디도스 공격 방지를 위하여, 블랙체인 네트워크를 구성하는 각 노드들은 최대 거래 생성 크기를 제한함으로써, 공격을 방지하고, 또한 최대 거래 생성 크기는 노드들의 거래 생성 크기를 최대한 고려하여 LMS 를 기반으로 하여 설정한다.

[0052] 도 4는 본 발명에 따라 디도스 공격 방지를 위한 '동적 거래 크기 제한'을 적용한 블록체인 네트워크 시스템을 개념적으로 도시한 모식도이다. 도 4를 참조하면, 각 노드들은 최대 거래 생성 제한 크기(Transaction volume limit)에 따른 거래(Transaction)을 전송하게 된다.

[0053] 도 5는 본 발명에 따른 디도스 공격 방지 방법에 의해 각 노드들에 대한 동적 거래 크기 제한에 사용되는 변수들을 정의한 도표이다.

[0054] 종래의 LMS는 다음 주기 동안의 예측값($\hat{x}_{n+1}$)은 현재 주기까지의 모든 측정값 x_1, x_2, x_3,..., x_n 을 이용하였으나, 본 발명에서는 바로 이전 주기의 측정값(x_n)만을 이용하는 것을 특징으로 한다. 이에 따라, 증감 가중치(Wn)은 증감 가중치 1개의 값이 된다.

[0055] 본 발명에 따른 디도스 공격 방지 방법에 있어서, 각 노드의 최대 거래 생성 제한 크기(TVL_n)는 수학식 3으로 구할 수 있다.

수학식 3

[0056]
$$TLV_{n+1} = \frac{\hat{x}_{n+1}}{C}$$

[0057] 수학식 3에 따른 최대 거래 생성 제한 크기는 다음 주기(n+1)에 대한 예측 거래 생성 크기($\hat{x}_{n+1}$)를 기준으로 최대 생성 비율(C)에 따라 상계값(upper bound)으로 결정된다. C 는 0 ~ 100 % 로 표현될 수 있으며, C = 100% 에 가까워질 수록 상계값(TVL_n)은 $\hat{x}_{n+1}$ 과 가까워지게 되며, 실제 거래 생성 크기(x_{n+1})는 항상 TVL_n 보다 작거나 같다.

[0058] 예측 거래 생성 크기($\hat{x}_{n+1}$)는 반복적으로 수학식 4에 의해 구해진다.

수학식 4

$$\hat{x}_{n+1} = \max(W_n * x_n , W_n * \hat{x}_n) , 0 \leq x_n \leq TLV_n$$

[0059]

[0060] 종래의 LMS에서는 증감 가중치 Wn 과 실제 측정값 (x_n)을 이용하여 다음 주기에 대한 예측값($\hat{x}_{n+1}$)을 구하였으며, 수학식 3을 통해 x_n 의 상계값(TVL_n)은 계산될 수 있지만, 하계값에 대하여는 고려하지 않았다. 만약 한 주기동안 실제 생성한 거래 크기(x_n)가 0이 된다면 $\hat{x}_{n+1}$ 및 TVL_n 이 모두 항상 0이 되는 문제가 발생할 수 있다. 이러한 문제를 해결하기 위하여, 본 발명에서는 LMS 에 대한 수학식 1을 수정하여 수학식 4로 표현하였다. 수학식 4에서와 같이, max() 함수를 사용함으로써, 현재 주기(n)에 대한 실제 거래 생성 크기(x_n)가 예측 거래 생성 크기($\hat{x}_n$)보다 작아졌을 때, 다음 주기(n+1)의 예측값($\hat{x}_{n+1}$)이 현재 주기(n)에 대한 예측값($\hat{x}_n$)보다 작아지는 감소율을 줄일 수 있게 된다.

[0061] 기존의 LMS 에서는 증감 가중치 Wn를 계산함에 있어서 현재 주기까지의 모든 측정값 x_1, x_2, x_3,..., x_n 을 이용하였으나, 본 발명에서는 바로 이전 주기의 실제 측정값인 x_n 만을 사용하여 수학식 2를 수정하여 수학식 5로 표현하였다.

수학식 5

$$W_{n+1} = W_n + \mu * (x_n - \hat{x}_n) * x_n$$

[0062]

[0063] μ 값에 따라 실제 거래 생성 크기와 예측 거래 생성 크기의 오차를 얼마나 빨리 줄여주는가를 결정하게 된다. 따라서, μ 값에 따라 수학식 4에 사용하는 증감 가중치 Wn의 증감하는 정도를 조절할 수 있게 된다. 실제 거래 생성 크기(x_n)와 예측 거래 생성 크기($\hat{x}_n$)의 오차를 매 제한 주기마다 계산을 통해 점차적으로 줄여주게 된다.

[0064] 수학식 5의 증감 가중치 Wn 의 변화 정도를 결정하는 μ 값은 수학식 6을 통해 얻을 수 있다.

수학식 6

$$\mu = \frac{1}{x_n * TVL_n} * \frac{T_l}{T_B} * \frac{1}{I * sur_I}$$

[0065]

[0066] x_n과 $\hat{x}_n$의 차이값은 $\frac{1}{x_n * TVL_n}$을 이용하여 $(x_n - \hat{x}_n) * x_n$에서 x_n을 제거해 주고, 실제 거래 생성 크기와 예측 거래 생성 크기의 오차인 $x_n - \hat{x}_n$와 $\frac{1}{TVL_n}$의 곱을 통해 오차의 값을 1보다 작은 값으로 표준화시켰다. $\frac{T_l}{T_B}$은 제한 주기 T_l와 블록주기 T_B로 $\frac{T_L}{T_B} = N$이다. N 값이 커질수록 제한 주기 동안 생성되는 블록 개수가 많아진다. 블록 하나가 만들어질 때 블록에 들어간 거래들은 '메모리 풀'에서 삭제된다. 그러므로, $\frac{T_l}{T_B}$을 계산하는 μ값을 추가하였다.

[0067] 수학식 6에 있는 주위 노드 중요도(sur_I)를 통해 블록체인 네트워크를 구성하는 노드들이 같은 거래 생성 크기를 하여도 서로 다른 주위 노드 중요도값에 따라 다음 주기 동안의 예측 거래 생성 크기($\hat{x}_{n+1}$)에 영향을 주게 된다. 주위 노드 중요도의 값이 크다는 것은 본인 노드와 연결된 노드들이 많은 노드들과 연결되어 있다는 것을 의미한다. 이는 많은 노드들과 연결되어 있는 노드들은 많은 노드들로부터 거래가 직접적으로 들어 온다는 것을 의미하게 된다. $\frac{1}{I*sur_I}$을 통해 많은 노드들과 연결되어 있는 노드들을 "Overflood attack'으로부터 더 강하게 보호해 주게 된다. 블록체인 네트워크를 구성하는 노드의 수가 증가되면, 노드들의 sur_I의 차이가 작아지게 된다. 따라서, 중요도 가중치(I)의 값을 증가시켜 μ의 변화비율을 조절할 수 있게 된다.

[0068] 본 발명에 따른 각 노드들에 대한 최대 거래 생성 크기를 동적으로 제한함으로서, 블록체인 네트워크에서 발생하는 'overflood attack' 방지가 얼마나 효율적인지 여부를 확인하기 위하여 실제 시뮬레이션을 이용한 실험을 진행하였다. 시뮬레이션에 사용될 블록체인은 '메모리풀' 관리를 거치는 자체적으로 개발된 블록체인이며 2가지의 실험을 3가지의 시나리오로 시뮬레이션하였다.

[0069] 2가지의 실험들은 공통적으로 블록이 생성되어 '메모리 풀'에서 거래를 삭제하는 과정이 일어나는 도중에는 거래를 생성하지 않았다. 이는 원활한 측정을 위해 블록 생성이 끝난 후, 다시 거래를 생성했다.

[0070] 첫번째 실험을 통해 'Overflood attack'을 막는지를 실험할 것이다. 이를 실험하기 위해 하나의 거래가 이번 연구에서 구성한 블록체인 시스템 전체에 전달이 되는 시간을 측정하는 것이다. 이렇게 측정된 값을 이번 연구에서는 '완전 전달 시간(RTT)' 라고 정의한다. 또한 블록체인 노드의 '메모리 풀 크기'를 측정 할 것이다. 총 세 가지의 시나리오에서 '완전 전달 시간'과 '메모리 풀 크기'를 측정을 할 것이다. 세가지의 시나리오는 다음과 같다.

[0071] (1) 시나리오1 : 공격이 없을 때. 블록 크기 만큼 거래가 생성되었을 때.

[0072] (2) 시나리오2 : 적용 전, 'Overflood attack'이 발생했을 때.

[0073] (3) 시나리오3 : 적용 후, 'Overflood attack'이 발생했을 때.

[0074] 공격이 없을 때 실험을 위해 하나의 노드에서 초당 2개의 거래를 지속적으로 생성시켰다. 'Overflood attack'을 발생시키기 위해 하나의 노드에서 초당 100개의 거래를 지속적으로 생성시켰다.

[0075] 두번째 실험을 통해 최대 거래 생성 제한 크기(TLV_{n+1})의 실제 거래 생성 크기(x_n)에 따른 변화를 측정할 것이다. 동일한 실제 거래 생성 크기(x_n)에서 서로 다른 최대 생성 비율(C) 에 따른 TLV_{n+1}의

값을 측정하여 그래프로 보여주도록 한다. 본 실험을 위해 첫번째 실험의 시나리오 3과 동일한 조건에서 측정하였다.

[0076] (1) 초당 100개의 거래 생성을 시도, 최대 생성 비율 c = 75%

[0077] (2) 초당 100개의 거래 생성을 시도, 최대 생성 비율 c = 50%

[0078] 전술한 실험 계획을 통해 계획한 두 가지의 실험을 그래프로 표현하여 보여 주도록 한다. 실험을 통해 측정하고자 하는 '완전 전달 시간', '메모리 풀 크기'의 측정시간을 기준으로 보여준다. 블록 주기(T_B)에 따라 생성되는 블록의 개수를 가로축에 표시하였다. 블록 개수는 블록체인에서 시간 기준으로 많이 사용한다. '최대 거래 생성 제한 크기'은 시간에 따라 TLV_1, TLV_2, TLV_3, ..., TLV_{10}의 크기를 보여준다.

[0079] 실험1에서 측정을 위해 블록이 40개 만들어지는 동안 세가지 시나리오의 '완전 전달 시간' 과 '메모리 풀 크기'을 측정하였다. 블록이 10개 생기는 동안 블록에 들어가지 못한 거래들은 '메모리 풀'에서 자동으로 삭제가 되도록 하였다. 이는 기존 블록체인에서도 있는 남아 있는 거래들에 대한 자동 삭제를 동일하게 적용 시킨 것이다. '완전 전달 시간'은 측정할 때, 네트워크의 상황에 따라 시간이 변칙적으로 바뀌어 동일 조건에서의 반복적인 실험을 통해 평균 시간으로 계산하였다.

[0080] 이번 연구에서 제안하는 방지 방안을 적용하는 시나리오 3의 $\frac{T_L}{T_B} = N$ (N=2), 최대 생성 비율 C = 75% 로 설정하여 실험을 진행하였다. 시나리오 1은 초당 2개의 거래를 지속적으로 생성 시켜서 실험을 진행 하였다. 시나리오 2와 시나리오 3은 초당 100개의 거래를 지속적으로 생성 시간에 따른 '완전 전달 시간'과 '메모리 풀 크기'을 측정하여 그래프로 표현하였다.

[0081] 도 6은 시나리오 1에 따라 공격이 없을 때 초당 2개의 거래가 지속적으로 생성될 때의 메모리 풀의 크기를 도시한 그래프이다. 이번 실험에서 하나의 블록에는 100kb 만큼의 거래가 들어간다. 도 6을 통해, 블록 주기 동안 생성된 거래의 총 크기가 하나의 블록 크기보다 작으면 언제나 블록이 생성된 직후 메모리 풀의 크기가 0이 되는 것을 확인할 수 있다.

[0082] 도 7은 시나리오 2에 따라, 블록체인에 'overflood attack'이 발생하였을 때의 메모리 풀의 크기를 도시한 그래프이다. 공격을 위해 하나의 노드에서 초당 100개의 거래를 지속적으로 생성시켰다. 도 6 및 도 7을 참조하면, 시나리오 1의 결과와 비교를 해보았을 때, 총 20개의 블록이 생성될 때까지 시나리오 1의 결과인 도 6에서는 메모리 풀 크기는 0~100kb 사이에서 반복적인 패턴이 보여진다. 그러나, 도 7의 시나리오 2의 결과를 보았을 때, 메모리 풀의 크기가 기하급수적으로 증가하고 있는 것을 볼 수 있다. 이는 이번 연구에서 말한 'overflood attack'에 의한 메모리 풀의 증가이다.

[0083] 도 8은 본 발명에 따른 방법, 즉 시나리오 3이 적용된 후의 'overflood attack'이 발생하였을 때의 메모리 풀의 크기를 도시한 그래프이다. 시나리오 3의 실험을 위해, 제한 주기는 블록 주기의 2배로 설정했다. 또한 최대 생성 비율인 C 값은 75%로 설정하였다. 초당 100개의 거래를 생성시켜 시나리오 2와 같은 'overflood attack'을 발생시켰다. 도 8을 참조하면, 매 제한 주기가 지남에 따라 메모리 풀의 크기가 늘어나는 것을 확인할 수 있다. 시나리오 2의 결과인 도 7과 비교해 보았을 때, 'overflood attack'은 블록이 10개 생성되는 시간 동안 메모리 풀의 크기가 40000kb를 넘겼다. 시나리오 3에서 메모리 풀의 크기가 40000kb를 넘기는 것을 불가능하다. 또한 시나리오 1의 결과인 도 6과 비교해 보면, 메모리 풀의 크기가 0~200kb 정도에서 유지되는 것을 알 수 있다.

[0084] 이하, '메모리 풀 크기(Memory pool size)'와 동시에 측정한 '완전 전달 시간(RTT)'에 대한 실험 결과들에 대해 설명한다.

[0085] 도 9는 시나리오 1의 시간에 따른 완전 전달 시간을 측정한 결과를 도시한 그래프이다. 완전 전달 시간은 하나의 거래가 모든 노드에게 전달될 때 까지 걸리는 시간을 의미한다. 도 9를 참조하면, 시나리오 1에 대한 메모리 풀 크기의 결과와 유사하게 반복적인 패턴임을 확인할 수 있다. 이로서 '메모리풀 크기'가 '완전 전달 시간'에 영향을 주는 것을 확인할 수 있다. 시나리오 1의 완전 전달 시간은 2~14ms에서 반복 적적인 패턴을 보여준다.

[0086] 도 10은 시나리오 2의 시간에 따른 완전 전달 시간을 측정한 결과를 도시한 그래프이다. 도 10을 참조하면, 시나리오 2의 '완전 전달 시간'은 도 9의 시나리오 1에 대한 반복적인 패턴과는 확연한 차이를 보여 주고 있다. 도 10을 참조하면, 블록이 10개가 만들어 지기 전에 이미 4000ms을 넘어서는 것을 확인할 수 있다. 도 7의 시나리오 2의 메모리풀 크기와 마찬가지로 'overflood attack'이 발생하였을 때, '완전 전달 시간'이 기하 급수적으

로 증가하는 것을 볼 수 있다. 시나리오 2의 실험을 진행하면서 시간이 지날수록 하나의 거래가 생성되어 전체 노드들에게 전달 될 때 까지의 시간이 확연하게 길어지고 있음을 실험을 통해 확인 할 수 있었다.

[0087] 도 11은 시나리오 3의 시간에 따른 완전 전달 시간을 측정한 결과를 도시한 그래프이다. 도 11을 참조하면, 시나리오 3의 완전 전달 시간을 측정한 값으로 시나리오 2와 동일하게 'overflood attack'을 시도하는 초당 100개의 거래를 생성하였다. 시나리오 2의 결과인 도 10과 비교하면, 시나리오 3은 'overflood attack'이 성공하지 못하였음을 확인할 수 있다. 블록에 20개 만들어지는 동안 도 10의 시나리오 2에서는 '완전 전달 시간'이 5000ms이 넘는 것을 확인할 수 있지만, 도 11의 시나리오 3에서는 불과 2~15ms 사이에서 유지되고 있음을 볼 수 있다. 이와 같은 결과는 세가지 시나리오에 따른 '메모리 풀 크기'를 비교 하였을 때와 같은 결과이다.

[0088] 하나의 노드에 블록에 들어가길 기다리는 거래가 증가할수록 '완전 전달 시간'에 영향을 주고 있음을 확인할 수 있다. 세가지의 시나리오에 따른 '메모리 풀 크기'와 '완전 전달 시간(RTT)'의 결과를 통해 본 발명에 따른 '동적 거래 크기 제한'이 'overflood attack'을 방지하고 있음을 알 수 있다.

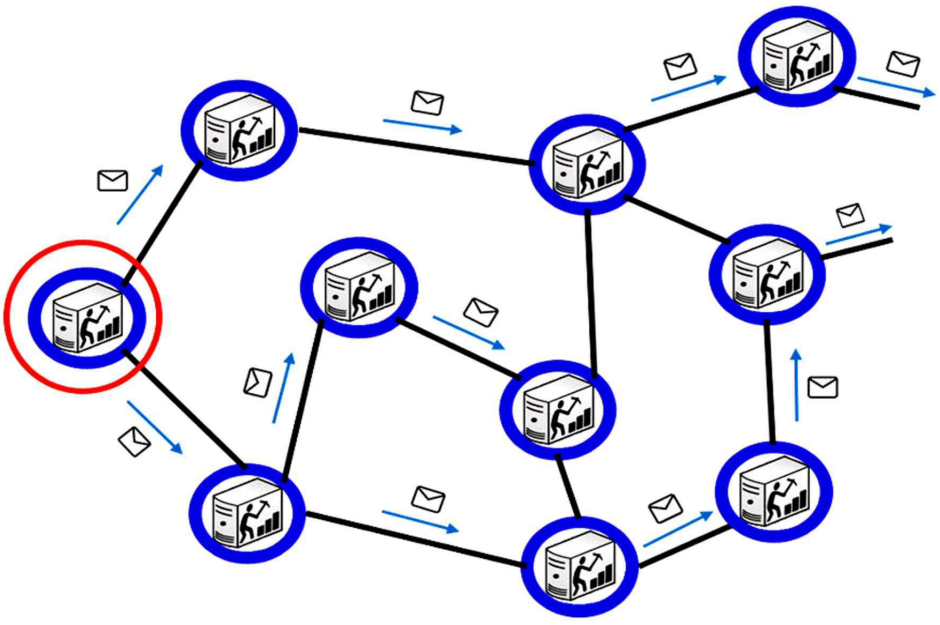
[0089] 도 12는 서로 다른 최대 생성 비율(C)에 따라 최대 거래 생성 제한 크기(TVL_n)의 크기를 도시한 그래프이다. 도 12를 참조하면, 초당 100개의 거래를 지속적으로 생성하였을 때, 서로 다른 최대 생성 비율 C를 갖는 두 개의 시나리오에서 초기에는 비슷한 최대 거래 생성 제한 크기 값을 갖고 있지만 점차적으로 최대 생성 비율 C가 50%인 시나리오의 최대 거래 생성 제한 크기가 75%보다 더 많이 증가하고 있음을 알 수 있다.

[0090] 따라서, 본 발명에 따른 '동적 거래 크기 제한'은 다양한 블록체인에 따라 서로 다르게 적용하여 'overflood attack'을 방지할 수 있음을 확인할 수 있다. 최대 생성 비율 C는 최대 0~100%까지 설정이 가능한 변수이다. 그렇기 때문에 '동적 거래 크기 제한'을 이용하여 완전하게 노드당 생성할 수 있는 거래의 양을 고정적으로 설정할 수 있고 블록체인의 다양한 분야의 활용에 따라 적절하게 조절될 수 있음을 알 수 있다.

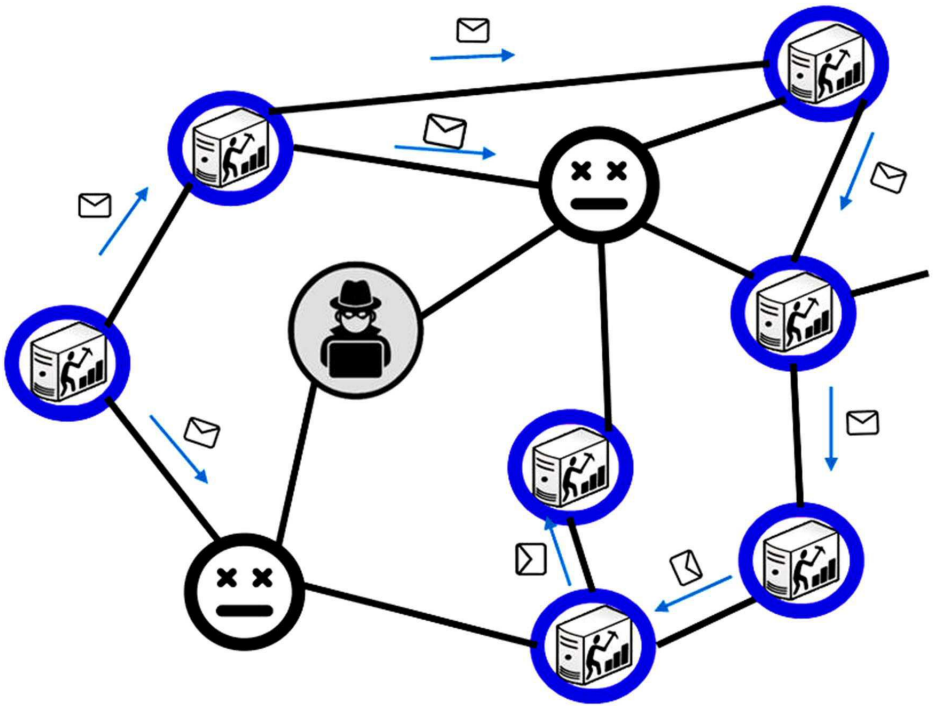
[0091] 이상에서 본 발명에 대하여 그 바람직한 실시예를 중심으로 설명하였으나, 이는 단지 예시일 뿐 본 발명을 한정하는 것이 아니며, 본 발명이 속하는 분야의 통상의 지식을 가진 자라면 본 발명의 본질적인 특성을 벗어나지 않는 범위에서 이상에 예시되지 않은 여러 가지의 변형과 응용이 가능함을 알 수 있을 것이다. 그리고, 이러한 변형과 응용에 관계된 차이점들은 첨부된 청구 범위에서 규정하는 본 발명의 범위에 포함되는 것으로 해석되어야 할 것이다.

도면

도면1



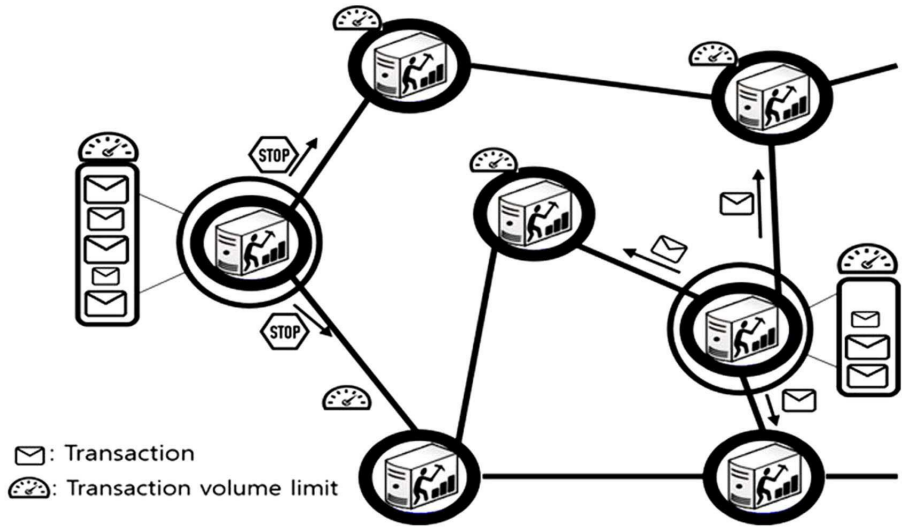
도면2



도면3

		동적 거래 크기 제한	Detection and Filtering	Reputation and Filtering
결과(Service 품질)	부정오류 확률	없음	높음	높음
	공격 방어 능력	높음	보통	보통
	이용 당한 노드의 피해 (좀비 노드 사용)	없음	높음	높음
	사용성 (거래 생성의 자유)	보통	높음	높음
고유(Design 특성)	공격을 막는 시점	공격 이전	공격 도중	공격 도중
	중앙 집중도	낮음	보통	높음
	상시 수행 되어야 할 부하	낮음	높음	높음
	리소스 소비	낮음	높음	높음

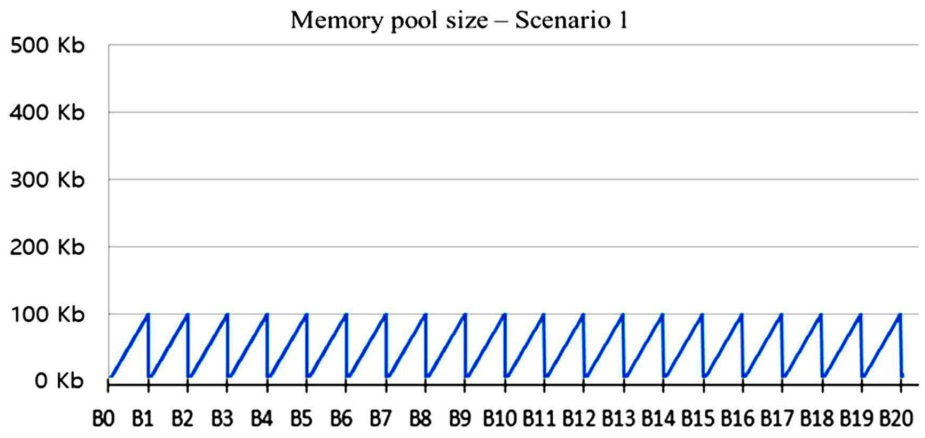
도면4



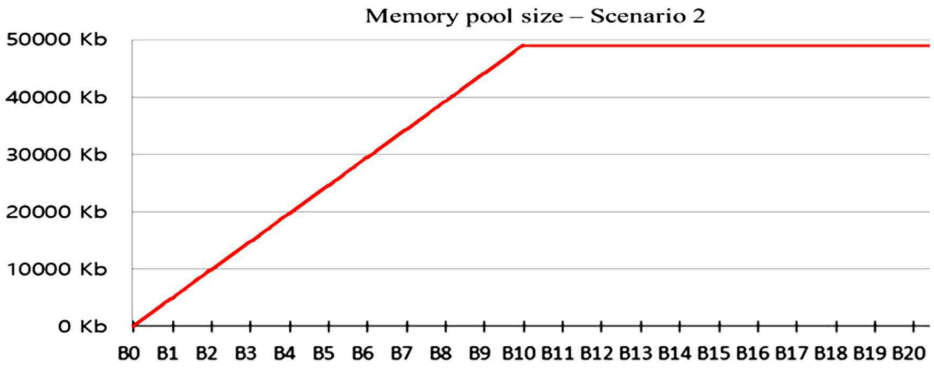
도면5

이름	단위	기호	설명
블록 주기	초	T_B	하나의 블록이 생성된 후 그 다음 블록이 생성 될때 까지 걸리는 시간
제한 주기	초	T_L	n 번째 주기에서 n+1 번째 주기가 되는데 까지 걸리는 시간, $\frac{T_L}{T_B}$ = N, N 은 자연수
블록 크기	Kb	S_{B_tx}	하나의 블록에 최대로 들어 갈 수 있는 거래의 총 크기
최대 거래 생성 제한 크기	Kb	TLV_n	n 번째 주기 동안 최대로 생성 가능한 총 거래 크기
예측 거래 생성 크기	Kb	$\hat{x}_n$	n 번째 주기 동안 생성 할 것으로 예측한 총 거래 크기
실제 거래 생성 크기	Kb	x_n	n 번째 주기 동안 실제로 생성한 총 거래 크기
최대 생성 비율	%	C	예측 거래 생성 크기에서 허용 할 수 있는 최대 거래 생성 제한 크기 비율, 0~100
증감 가중치	상수	W_n	n+1 번째 주기의 예측 거래 생성 크기를 결정하는 상수 값
주위 노드 중요도	상수	sur_i	본인 노드와 연결된 노드들이 연결 하고 있는 평균 노드 수
중요도 가중치	상수	I	주위 노드 중요도가 얼마나 중요한지를 결정하는 무게 상수 값

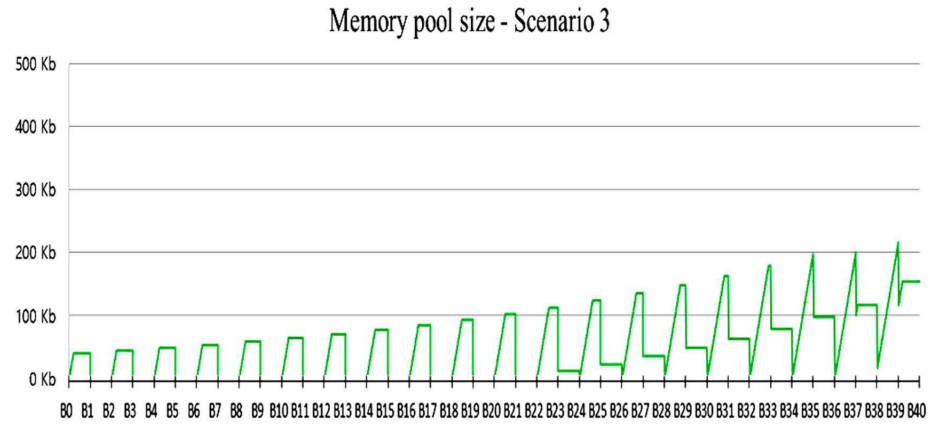
도면6



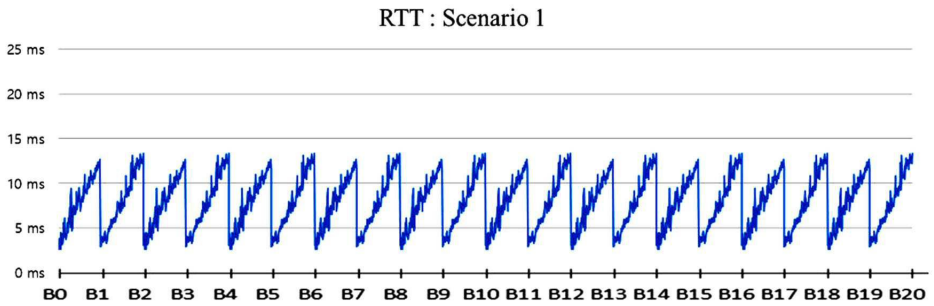
도면7


Memory pool size – Scenario 2
50000 Kb
40000 Kb
30000 Kb
20000 Kb
10000 Kb
0 Kb
B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 B12 B13 B14 B15 B16 B17 B18 B19 B20

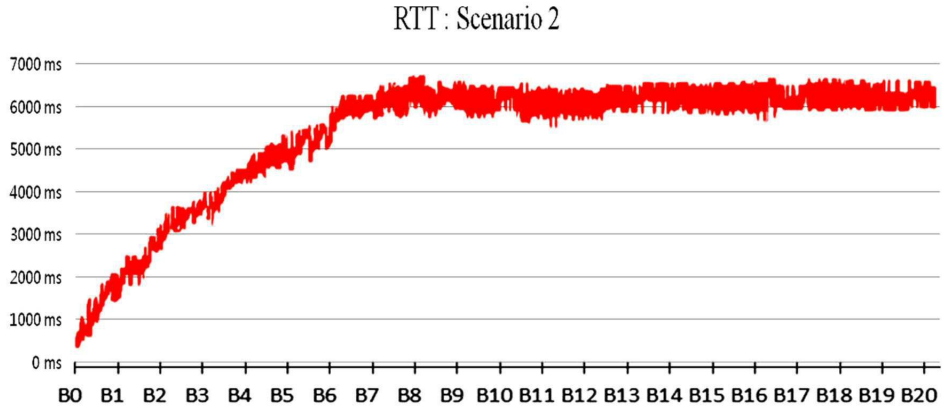
도면8


Memory pool size - Scenario 3
500 Kb
400 Kb
300 Kb
200 Kb
100 Kb
0 Kb
B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 B12 B13 B14 B15 B16 B17 B18 B19 B20 B21 B22 B23 B24 B25 B26 B27 B28 B29 B30 B31 B32 B33 B34 B35 B36 B37 B38 B39 B40

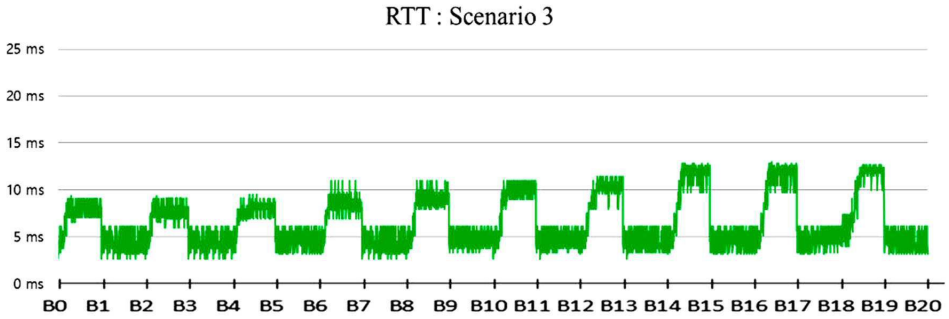
도면9


RTT : Scenario 1
25 ms
20 ms
15 ms
10 ms
5 ms
0 ms
B0 B1 B2 B3 B4 B5 B6 B7 B8 B9 B10 B11 B12 B13 B14 B15 B16 B17 B18 B19 B20

도면10



도면11



도면12