(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2008-0079791
(43) 공개일자 2008년09월02일

(51) Int. Cl.
H04B 7/26 (2006.01)
(21) 출원번호 10-2007-0020218
(22) 출원일자 2007년02월28일
심사청구일자 2007년02월28일

(71) 출원인
재단법인서울대학교산학협력재단
서울특별시 관악구 봉천7동 산4의 2번지
(72) 발명자
김이용
서울 관악구 봉천7동 1620-14 504호
김황남
서울 성북구 하월곡동 레미안월곡아파트 126동 403호
박근수
서울 동작구 사당2동 극동아파트 110동 704호
(74) 대리인
특허법인명문

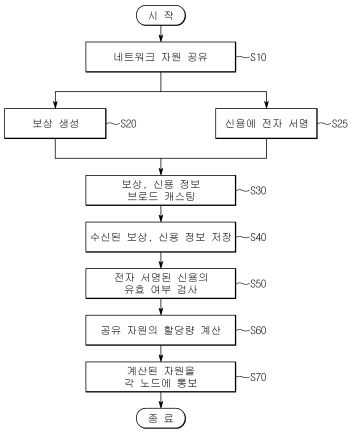
전체 청구항 수 : 총 15 항

(54) 무선 네트워크 시스템 및 그의 자원공유방법

(57) 요 약

본 발명은 자원공유 프로토콜을 제시하여 효율적으로 네트워크 자원을 활용할 수 있도록 하는 무선 네트워크 시스템 및 그의 자원공유방법에 관한 것으로서, 인접한 노드에 자원을 제공하면 제공한 자원의 양적 정보를 나타내는 신용(credit)을 생성하여 네트워크 상에 브로드캐스팅(broadcasting)하는 제 1노드; 및 상기 제 1노드로부터 받은 자원에 대한 정보를 나타내는 보상(reward)을 생성하여 네트워크 상에 브로드캐스팅하는 제 2노드를 포함하여 상기 보상 데이터를 통해 상기 제 1노드의 신용정보가 유효한지 검증하고, 그에 따라 사용가능한 네트워크 자원을 상기 제 1노드에 할당하는 것을 특징으로 하여 각 노드가 중계하는 중계정보의 유효성과 안전성을 보장함으로써 이기적인 노드들에게는 자원 할당을 적게 주고, 협력적인 노드들에게는 자원 할당을 많이 줌으로써 노드들이 전체 네트워크의 연결성에 협력하여 네트워크 자원을 효율적으로 활용할 수 있으며 연결의 안정성을 높일 수 있는 효과가 있다

대표도 - 도4



특허청구의 범위

청구항 1

다수의 노드를 포함하여 네트워크를 형성하는 무선 네트워크 시스템에 있어서,

인접한 노드에 자원을 제공하면 제공한 자원의 양적 정보를 나타내는 신용(credit)을 생성하여 네트워크 상에 브로드캐스팅(broadcasting)하는 제 1노드; 및

상기 제 1노드로부터 받은 자원에 대한 정보를 나타내는 보상(reward)을 생성하여 네트워크 상에 브로드캐스팅하는 제 2노드

를 포함하여 상기 보상 데이터를 통해 상기 제 1노드의 신용정보가 유효한지 검증하고, 그에 따라 사용가능한 네트워크 자원을 상기 제 1노드에 할당하는 것을 특징으로 하는 무선 네트워크 시스템.

청구항 2

제 1 항에 있어서,

상기 보상(reward)은 발급자(issuer), 신용(credit), 대상자(recipient), 및 기타정보를 포함하는 튜플(tuple)로 구성되는 것을 특징으로 하는 무선 네트워크 시스템.

청구항 3

제 2 항에 있어서,

상기 제 1노드는 제공한 자원에 따라 쌓은 신용(credit)을 자신의 개인키(private key)로 전자서명하여 일정 주기로 네트워크 상에 브로드캐스팅하는 것을 특징으로 하는 무선 네트워크 시스템.

청구항 4

제 2 항에 있어서,

상기 제 2노드는 제공받은 자원에 따라 보상(reward)를 생성하고, 자신의 개인키로 전자서명하여 일정주기로 네트워크 상에 브로드캐스팅하는 것을 특징으로 하는 무선 네트워크 시스템.

청구항 5

제 4 항에 있어서,

상기 제 2노드는 상기 튜플 내 저장된 신용정보를 제 1노드의 공개키로 보호하는 것을 특징으로 하는 무선 네트워크 시스템.

청구항 6

제 2 항에 있어서,

상기 시스템은 각 노드로부터 자원공유에 대한 신용(credit) 또는 보상(reward) 데이터를 수신하여, 수신된 신용정보가 상기 보상정보에 포함된 신용정보와 일치하는지 판단하고, 일치하는 경우 그에 해당하는 만큼의 네트워크 자원을 비례하여 해당 노드에 할당하는 신용기관을 더 포함하여 구성되는 것을 특징으로 하는 무선 네트워크 시스템.

청구항 7

자원을 제공하여 인접한 노드의 네트워크 트래픽을 중계하거나 인접한 노드로부터 자원을 제공받은 경우, 제공된 자원의 양에 대응하는 신용(credit)정보를 생성하거나 제공받은 자원에 대응하는 보상(reward)정보를 생성하는 단계;

일정시간 간격으로 생성된 신용정보 또는 보상정보를 전자서명하여 브로드캐스팅하는(broadcasting)하는 단계;

인접한 다른 노드로부터 전자서명된 신용정보 및 보상정보를 수신하여 상기 신용정보가 유효한지 판단하는 단계; 및

유효한 경우 상기 신용정보만큼의 네트워크 자원을 산출하는 단계

를 포함하여 이루어지는 것을 특징으로 하는 무선 네트워크 시스템의 자원공유방법.

청구항 8

제 7 항에 있어서,

상기 자원 산출단계 후,

산출된 각 네트워크 자원을 해당 노드에 할당하여 각 노드에 통보하는 단계를 더 포함하여 이루어지는 것을 특징으로 하는 무선 네트워크 시스템의 자원공유방법.

청구항 9

제 7 항에 있어서,

난수를 생성하여 상기 보상정보를 생성하고, 다음 시간간격에서 이전 생성된 난수를 이용하여 상기 신용정보를 전자서명하는 것을 특징으로 하는 무선 네트워크 시스템의 자원공유방법.

청구항 10

제 7 항에 있어서,

상기 자원공유방법은 상기 신용 및 보상을 보호하기 위한 자원공유 프로토콜을 포함하여 이루어지는 것을 특징으로 하는 무선 네트워크 시스템의 자원공유방법.

청구항 11

제 10 항에 있어서,

상기 자원공유 프로토콜은 SIG 알고리즘을 포함하여 이루어지며,

상기 SIG 알고리즘은 시스템 공개키 P, 아이덴터티 id_A, 신용 c, 및 비밀키를 입력받아 전자서명을 출력하는 것을 특징으로 하는 무선 네트워크 시스템의 자원공유방법.

청구항 12

제 10 항에 있어서,

상기 자원공유 프로토콜은 RWD 및 TEST 알고리즘을 포함하여 이루어지는 것을 특징으로 하는 무선 네트워크 시스템의 자원공유방법.

청구항 13

제 12 항에 있어서,

상기 RWD 알고리즘은 시스템 공개키 P, 신용, 자원을 제공받는 노드의 개인키 및 상기 난수를 사용하여 보상(reward)를 생성하는 것을 특징으로 하는 무선 네트워크 시스템의 자원공유방법.

청구항 14

제 12항에 있어서,

상기 TEST 알고리즘은 시스템 공개키 P, 보상, 전자서명을 사용하여 상기 전자서명에 포함된 신용정보가 유효한지 여부를 판단하는 것을 특징으로 하는 무선 네트워크 시스템의 자원공유방법.

청구항 15

네트워크 시스템에 있어서 제 1노드가 제 2노드의 트래픽을 일정 양만큼 중계한 경우,

제 2노드가 RWD 알고리즘을 통해 일정시간 동안의 보상정보를 생성하고, 생성된 보상정보를 브로드캐스팅하는 단계;

제 1노드가 이전 시간 동안의 신용정보를 SIG 알고리즘을 통해 전자서명하고, 서명된 신용정보를 브로드캐스팅하는 단계;

브로드캐스팅에 의해 수신된 전자서명을 VER 알고리즘을 통해 유효한지 판단하고, 유효한 경우 이전 저장된 보상정보를 상기 전자서명 및 TEST 알고리즘을 통해 검증하는 단계; 및

검증된 경우 상기 보상정보에 해당하는 만큼의 네트워크 자원을 할당하는 단계

를 포함하여 이루어지는 것을 특징으로 하는 무선 네트워크 시스템의 자원공유방법.

명 세 서

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

<9> 본 발명은 무선 네트워크 시스템 및 그의 자원공유방법에 관한 것으로서, 특히 자원공유 프로토콜을 제시하여 효율적으로 네트워크 자원을 활용할 수 있도록 하는 무선 네트워크 시스템 및 그의 자원공유방법에 관한 것이다.

<10> 최근 급속도로 발전하고 있는 인터넷 분야에서 제안된 IEEE 802.11 기반 무선 네트워킹 기술은 무선 ad-hoc 네트워크를 거쳐 무선 메쉬(mesh) 네트워크 형태로 발전해 가면서 인접한 노드들 사이에 임의로 연결설정을 할 수 있게 되었다. 이러한 특성은 IEEE 802.11 기반 기술이 가지는 통신 주파수 영역에 대한 비면허 특성과 함께 P2P(Peer-to-peer) 서비스 망과 같이 노드들 사이에 자원공유가 가능하도록 한다.

<11> 도 1은 일반적인 무선 네트워크 시스템에 있어서, 자원공유 흐름이 간략하게 도시된 개요도이다.

<12> 즉, 도 1에 도시된 바와 같이 네트워크 내에 있는 각 노드들은 직접적인 인터넷과 접속이 불가능한 경우라도 접속 가능한 다른 노드의 중계 서비스를 통해 간접적으로 인터넷 접속이 가능하게 된다.

<13> 이러한 중계서비스를 위해서는 각 중계 노드들은 자신의 네트워크 대역폭(bandwidth)나 메모리 등의 자원을 제공해야 한다. 이와 같이 자원 공유가 가능한 무선 네트워크는 노드 장애(node failure)나 링크 장애(link failure)가 발생시 다른 경로를 찾아 접속을 유지할 수 있어 장애에 능동적으로 대처할 수 있다. 또한 인접한 노드들의 자원을 사용할 수 있기 때문에 각 노드 자체의 자원 환경에 제한되지 않는 네트워크 서비스를 제공할 수 있다.

<14> 이러한 자원공유서비스는 P2P파일 공유 서비스에서 이미 구현되고 있다. 그러나, 구현된 기존 P2P 형태의 서비스는 자원 공유를 약속했던 각 노드들이 자원공유에 지속적으로 참여하고 있는지 또는 네트워크 운영을 위해 자원을 많이 제공하는 노드들에 대한 보상이 제대로 제공되고 있는지에 대한 구체적인 방법이 존재하지 않았다. 따라서 자기의 자원은 제공하지 않으면서 노드들 간 자원 공유를 통해 이루어지는 서비스는 사용하는 free-riding 문제가 발생하게 되었다.

<15> 특히 ad-hoc으로 메쉬 형태의 네트워크 토폴로지(topology)를 구성하는 무선 네트워크 환경에서는 기존 P2P 서비스에서처럼 자원공유에 대한 보상을 보장하는 방안이 없는 경우 free-riding 등을 야기하는 이기적인 노드(selfish node)들이 생기게 된다. 이들은 자신을 위해서는 네트워크 전체의 자원을 사용하지만 다른 노드들을 위해 자신의 자원을 제공하지는 않는다. 따라서 이기적인 노드들은 무선망 전체에 존재하는 네트워크 트래픽을 자원공유에 협력적인 노드들에게 집중되게 하거나 이에 따라 네트워크 연결을 단절시키게 된다.

<16> 따라서, 노드들 사이에 자원공유를 권장하고 자원공유에 대한 보상을 보호할 수 있도록 하는 방안이 요구되며, 이러한 사항이 충족되어야 자원 공유를 통한 무선 네트워크를 충분히 활용할 수 있게 되는 것이다.

발명이 이루고자 하는 기술적 과제

<17> 본 발명은 상기한 종래 기술의 문제점을 해결하기 위한 것으로서, 자원공유 프로토콜을 사용하여 네트워크 트래픽에 기여한 정도에 따라 각 노드에게 네트워크 자원을 비례하여 할당함으로써 자원공유가 원활하게 이루어질 수 있도록 하고, 이에 따라 무선 네트워크 내에 연결성을 보장하여 보다 다양한 서비스를 제공할 수 있도록 하

는 무선 네트워크 시스템 및 그의 자원공유방법을 제공하는 데 그 목적이 있다.

발명의 구성 및 작용

<18> 본 발명에 따른 무선 네트워크 시스템은 다수의 노드를 포함하여 네트워크를 형성하는 무선 네트워크 시스템에 있어서, 인접한 노드에 자원을 제공하면 제공한 자원의 양적 정보를 나타내는 신용(credit)을 생성하여 네트워크 상에 브로드캐스팅(broadcasting)하는 제 1노드; 및 상기 제 1노드로부터 받은 자원에 대한 정보를 나타내는 보상(reward)을 생성하여 네트워크 상에 브로드캐스팅하는 제 2노드를 포함하여 상기 보상 데이터를 통해 상기 제 1노드의 신용정보가 유효한지 검증하고, 그에 따라 사용가능한 네트워크 자원을 상기 제 1노드에 할당하는 것을 특징으로 한다.

<19> 또한, 본 발명에 따른 무선 네트워크 시스템의 자원공유방법은 자원을 제공하여 인접한 노드의 네트워크 트래픽을 중계하거나 인접한 노드로부터 자원을 제공받은 경우, 제공된 자원의 양에 대응하는 신용(credit)정보를 생성하거나 제공받은 자원에 대응하는 보상(reward)정보를 생성하는 단계; 일정시간 간격으로 생성된 신용정보 또는 보상정보를 전자서명하여 브로드캐스팅하는(broadcasting)하는 단계; 인접한 다른 노드로부터 전자서명된 신용정보 및 보상정보를 수신하여 상기 신용정보가 유효한지 판단하는 단계; 및 유효한 경우 상기 신용정보만큼의 네트워크 자원을 해당 노드에 할당하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

<20> 또한, 네트워크 시스템에 있어서 제 1노드가 제 2노드의 트래픽을 일정 양만큼 중계한 경우, 제 2노드가 RWD 알고리즘을 통해 일정시간 동안의 보상정보를 생성하고, 생성된 보상정보를 브로드캐스팅하는 단계; 제 1노드가 이전 시간 동안의 신용정보를 SIG 알고리즘을 통해 전자서명하고, 서명된 신용정보를 브로드캐스팅하는 단계; 브로드캐스팅에 의해 수신된 전자서명을 VER 알고리즘을 통해 유효한지 판단하고, 유효한 경우 이전 저장된 보상정보를 상기 전자서명 및 TEST 알고리즘을 통해 검증하는 단계; 검증된 경우 상기 보상정보에 해당하는 만큼의 네트워크 자원을 할당하는 단계를 포함하여 이루어지는 것을 특징으로 한다.

<21> 이하, 첨부된 도면을 참조로 하여 본 발명의 실시예를 설명한다. 우선, 본 명세서에서는 ad-hoc 무선 네트워크 시스템을 예로 하여 설명하나 자원공유 서비스를 제공하는 네트워크라면 모두 그 적용이 가능함으로 명시한다.

<22> 한편, 본 발명에서 사용되는 용어를 정의하면 다음과 같다.

<23> (1) 신용(credit)은 한 노드가 다른 노드의 네트워크 트래픽을 위해 제공하는 자원의 양 또는 그에 준하는 정량적 정보를 뜻한다.

<24> (2) 보상(reward)는 발급자(issuer), 신용(credit), 대상자(recipient), 기타 정보로 구성된 튜플로 이루어져, 발급자의 신용만큼의 자원이 대상자에 의해 사용되었다는 사실이나 그에 준하는 정보를 의미한다.

<25> 도 2는 본 발명에 따른 무선 네트워크 시스템에 있어서, 신용기관이 존재하는 경우 자원공유 구조가 도시된 도이다.

<26> 본 발명에 따른 무선 네트워크 시스템은 도 2에 도시된 바와 같이 인터넷망에 연결된 적어도 하나 이상의 게이트웨이와 상기 각 게이트웨이와 연결된 다수의 노드를 포함하여 구성된다.

<27> 상기 게이트웨이는 상기 각 노드가 정상적으로 인터넷망을 사용할 수 있도록 가상의 주소를 할당하고 그에 따른 데이터 송수신을 제어한다.

<28> 상기 노드는 상기 게이트웨이 및/또는 인접한 노드와 연결되어 정보처리 및 통신기능을 수행하며, 구체적으로는 컴퓨터, 원격처리장치 또는 단말기 등으로 구현될 수 있다.

<29> 이러한 상기 각 노드는 자신에게 할당된 네트워크 대역폭 또는 물리적인 메모리, CPU등의 자원을 갖게 되는데, 자신이 현재 사용하지 않는 자원을 다른 인접한 노드에 제공함으로써 네트워크의 효율성을 더욱 높일 수 있다.

<30> 이때, 자원을 제공한 노드에 대해 보다 많은 네트워크 자원을 공유할 수 있도록 하기 위해 상기 각 노드는 자신이 제공한 자원에 대한 신용정보를 생성하여 지속적으로 갱신하게 된다.

<31> 또한, 이러한 신용정보는 일정한 시간간격으로 특정의 기관인 신용기관(R으로 전송된다.

<32> 각 노드들은 자신의 트래픽을 중계해주는 인접한 노드들에 대해 보상을 발급하게 되는데, 발급한 보상을 일정시간마다 상기 신용기관(R)에 보고한다.

<33> 따라서, 상기 신용기관(R)은 각 노드에서 전송되어 온 신용정보가 적합한지 여부를 보상을 사용하여 판단하고

신용정보가 정당하다면 그에 해당하는 네트워크 자원을 비례하여 할당하게 된다. 판단하여 그에 따른 네트워크 자원을 비례하여 할당하게 된다.

<34> 이때, 상기 신용기관(R)은 소정의 정보처리를 수행할 수 있는 별도의 기기일 수 있으나, 상기 게이트웨이 또는 상기 네트워크를 중앙 제어하는 상위계층 장치에 포함되는 형태로 구현될 수 있다.

<35> 한편, 임의성을 갖는 ad-hoc 무선 네트워크의 특성에 따라 모든 네트워크 망이 신용기관을 포함하지는 않는다. 도 3은 본 발명에 따른 무선 네트워크 시스템에 있어서, 신용기관이 존재하지 않는 경우 자원공유 구조가 도시된 도이다.

<36> 즉, 도 3에 도시된 바와 같이 각 노드에서 생성된 신용정보를 수집하는 별도의 신용기관을 구비하지 않은 경우, 각 노드는 인접한 다른 노드들의 트래픽을 중계할 때 자신의 신용을 스스로 갱신하며, 일정시간마다 자신의 신용정보를 네트워크 상에 브로드캐스팅(broadcasting)한다.

<37> 이와 동시에 각 노드는 자원을 제공하여 자신의 트래픽을 중계해주는 인접한 노드들에 대해 보상(c_0 내지c_5)을 발급하고, 일정시간마다 자신이 발급한 보상 및 다른 노드에서 발급한 보상을 네트워크 상에 브로드캐스팅한다.

<38> 결국 각 노드들은 다른 노드들의 신용과 보상을 수집하며, 신용이 유효한 지 보상을 가지고 검사한다. 이때 각 신용정보가 유효하다면 모든 노드들에게 신용만큼의 네트워크 자원을 할당하게 된다.

<39> 도 4는 상기와 같이 구성되는 본 발명에 따른 무선 네트워크 시스템에 있어서, 자원공유방법이 도시된 순서도이다.

<40> 우선, 각 노드간 연결이 성사되어 네트워크를 형성하고, 이에 따라 인터넷망과 접속하여 데이터를 송수신하게 된다.

<41> 이때, 단계 S10에서, 한 노드에 네트워크 트래픽이 과도하게 걸리면 인접한 주변의 노드에서 자원을 제공한다.

<42> 단계 S20에서, 자원을 제공받은 노드는 자원을 제공한 노드 및 상기 노드로부터 제공받은 자원의 양에 대한 보상정보를 생성한다. 이와 동시에, 단계 S25에서, 자원을 제공하는 노드는 자신이 제공한 자원의 양에 대한 신용주장정보를 생성하여 자신의 개인키로 전자서명한다.

<43> 다음, 단계 30에서 상기 각 노드는 자신의 신용주장정보 또는 보상정보를 네트워크 상에 브로드캐스팅한다.

<44> 단계 40에서는 브로드캐스팅된 정보에 따라 각 노드의 신용주장정보 및 보상정보는 신용기관 또는 모든 노드에 전부 전송되며, 상기 신용기관 또는 각 노드는 수신된 신용주장정보 및 보상정보를 모두 저장하게 된다.

<45> 다음, 단계 50에서 신용주장정보 및 보상정보를 모두 저장하게 된 신용기관 또는 각 노드는 전자서명된 상기 신용주장정보가 유효한 정보인지 판단한다. 이때 신용은 네트워크 자원 제공자의 개인키(private key)로 전자서명되며, 보상은 발급자, 신용, 대상자, 기타정보의 튜플로서 신용이 대상자의 공개키에 의해서 숨겨지고 발급자의 개인키에 의해서 전자서명되는 형태이다. 신용이 유효한지 테스트를 수행하는 노드는 보상정보로부터 신용을 알아낼 수 없지만, 보상이 숨기고 있는 신용이 대상자가 주장하는 신용과 같은지를 판단한다. 이러한 테스트는 신용 기관이 네트워크 내에 존재할 때에는 신용 기관이 수행하고, 그렇지 않을 때에는 해당 테스트를 각 노드들이 각각 수행한다.

<46> 단계 50에서 판단결과, 서로 일치하면 단계 60에서는 신용정보에 해당하는 만큼의 네트워크 자원이 해당 노드에 제공될 수 있도록 할당하여 계산한다.

<47> 신용기관이 존재하는 경우, 단계 70에서는 계산된 할당정보를 각 노드에 통보하여 자원을 제공하도록 제어하며, 신용기관이 존재하지 않는 경우 산출된 할당정보에 맞게 해당 노드에서 자체적으로 네트워크 자원을 활용한다.

<48> 한편, 본 발명에 따른 무선 네트워크 시스템에 있어서, 자원공유 프로토콜은 다음과 같은 공격들에 대해 안전해야 한다.

<49> 1. 신용에 대한 공격: 노드 자신의 신용을 위조하거나 다른 노드의 신용을 조작하는 공격이다. 다른 노드들의 트래픽을 중계하지 않고 자신에 대한 거짓 신용을 만들어서 자원 할당을 더 받으려는 공격과, 다른 노드들의 신용을 중계할 때 그것을 감소시킴으로써 자신이 원래 받을 자원 할당보다 더 많은 할당을 받으려는 공격으로 나눌 수 있다.

<50> 2. 보상에 대한 공격: 다른 노드들의 보상을 변경하거나 제거하여 그들의 신용주장 유효 테스트가 실패하도록

만들고 따라서 자신이 더 많은 자원할당을 받으려는 공격이다.

<51> 3. 재시도 공격: 이전에 발급된 보상을 이후 계속 사용하는 공격이다. 공격자는 다른 노드들의 트래픽을 중계하지 않고 한 번 받은 보상을 계속 사용하게 되므로 자원 할당을 일정한 만큼 받을 수 있다.

<52> 선행기술을 보면, 기존의 접근 방법들은 대부분 현실적으로 존재하지 않는 하드웨어에 의존하거나(Nuglet), 작동 중에 중앙의 신용기관과의 대화가 필요하거나(Sprite), 통계적인 방법(Catch)에 의존하여 이기적인 노드들을 찾아내고 고립시키는 방법을 이용한다. 그러나 본 발명에서는 증명가능한 안전한 암호 스킴에 의존하여 작동 중 중앙의 신용기관과의 존재에 상관없이 결정적인(deterministic) 방법으로 이기적인 노드들을 찾아낸다. 그리고 발견한 이기적인 노드들에게는 자원 할당을 적게 주는 방식으로 불이익을 줌으로써 노드들이 전체 네트워크의 연결성에 협력하도록 권장한다.

<53> 따라서, 본 발명에 따른 무선 네트워크 시스템에 있어서 자원공유 프로토콜은 보상 비밀성, 보상 익명성, 보상 위조불가성, 서명 위조불가성 등의 성질을 만족하여야 한다.

<54> 보상 비밀성(Reward Privacy)은 보상이 숨기고 있는 신용의 정보를 노출시켜서는 안된다는 것이고, 보상 익명성(Reward Anonymity)은 보상의 발급자와 대상자에 대한 정보를 노출시켜서는 안 된다는 것이며, 보상 위조불가성(Reward Unforgeability)은 발급자의 개인키가 없으면 그 발급자에 대한 보상을 위조할 수 없어야 한다는 것이고, 서명 위조불가성(Signature Unforgeability)은 대상자의 개인키가 없으면 신용에 대한 전자서명을 위조할 수 없어야 한다는 것이다.

<55> 이를 만족하는 본 발명에 따른 자원공유 프로토콜은 SETUP, KG, RWD, SIG, VER, 그리고 TEST여섯 개의 알고리즘을 이용하여 작동한다. 프로토콜에서 필요한 난수를 생성할 때는 one-way체인을 이용한다. 유사 난수 함수(pseudo-random function) f를 이용하여 one-way 함수 F를 만든다.

수학식 1

<56> $F: F(k) = f_k(0)$

<57> 이 함수 F를 이용하여 체인은 다음과 같이 계산된다.

수학식 2

<58> $r_i = F(r_{i+1}) \quad (i \geq 0)$

<59> 무선 네트워크 시스템에 연결되어 있는 모든 노드들은 시간 간격, 시작 시간, 간격 인덱스 i를 공유한다. 또한, 시간 간격 i에 모든 노드들은 간격 i에 해당하는 신용주장과 보상을 퍼뜨린다. 그리고 간격 i-1의 신용주장을 간격 i-1의 보상으로 검증한다.

<60> 이를 예를 들어 설명하면 다음과 같다.

<61> 도 5는 본 발명의 실시예에 따른 자원공유 데이터의 흐름이 도시된 흐름도로서, 별도의 신용기관이 존재하지 않는 경우 노드 B가 노드 A의 트래픽을 c_i만큼 중계한 경우를 예로 하여 도시한 것이다. 이때, 신용기관이 존재하는 경우 신용기관은 노드 T의 동작을 그대로 수행한다.

<62> 도 5에 도시된 바와 같이, 노드 A는 난수 r_{i+1}을 선택하고, RWD 알고리즘을 돌려서 익명 보상 $R_A^B(c_i; r_{i+1})$을 생성한다. 노드 A는 $R_A^B(c_i; r_{i+1})$을 이웃 노드들에게 브로드캐스팅하고 이전에 저장했던 r_i를 노드 B에게 보내고, r_{i+1}은 디스크에 저장한다.

<63> 또한, 노드 B는 현재 신용 정보 (id_A, c_i)를 디스크에 저장하고 이전에 저장했던 (id_a, c_{i-1})을 읽어온다. 난수 r_i를 노드 A로부터 받은 다음 SIG 알고리즘을 돌려서 전자서명 $S_B^A(c_{i-1}; r_i)$를 생성한다. 노드 B는 현재 신용정보 (id_A, c_i)를 전자서명 $S_B^A(c_{i-1}; r_i)$과 함께 이웃 노드들에게 브로드캐스팅한다.

<64> 점차적으로, 노드 T는 보상 $R_A^B(c_i; r_{i+1})$와 신용주장 (id_A, c_i), $S_B^A(c_{i-1}; r_i)$를 받게 된다. 노드 T는 $R_A^B(c_i; r_{i+}$

$_1$)와 (id_A, c_i)를 디스크에 저장한다. 노드 T는 받은 서명 $S_B^A(c_{i-1}; r_i)$를 이전에 저장했던 (id_A, c_{i-1}) 와 노드 B의 아이덴티티와 함께 VER 알고리즘을 돌려서 검증한다. 만약 서명이 유효하다면, 노드 T는 이전에 저장했던 보상들을 서명 $S_B^A(c_{i-1}; r_i)$와 노드 A의 아이덴티티와 함께 TEST 알고리즘을 돌려서 검사한다.

<65> 노드 T는 현재 시간간격의 신용 c_i를 검증하지 않고 이전 간격의 신용 c_{i-1}을 검증한다. 만약 노드 T가 신용 c_{i-1}이 노드 B가 거짓으로 주장한 것임을 발견한다면, 다음 시간간격 i+1에서 자원 공유를 계산할 때 노드 B에게 할당되는 자원을 감소시킴으로써 불이익을 주게 된다.

<66> 한편, 상기와 같은 본 발명의 자원공유 프로토콜에서 동작하는 SETUP, KG, RWD, SIG, VER, 그리고 TEST 의 여섯 개의 알고리즘은 다음과 같이 동작한다.

<67> 안전도 파라미터 k를 입력으로 받아서 k-bit 소수 q, 오더가 q인 두 그룹 G1, G2, 그리고 효율적으로 계산 가능한 겹선형 페어링 함수 $\mathbf{e}$: $G_1 \times G_1 \rightarrow G_2$를 출력한다. 이 페어링 함수는 겹선형성 및 정상성의 성질을 갖고 있어 보상의 내용을 외부에 노출시키지 않고 암호화할 수 있다.

<68> 페어링 파라미터 생성함수를 이용하여 (q, G_1, G_2, $\mathbf{e}$)의 튜플을 생성한다. 세 개의 암호학적인 해쉬 함수 H_1 : $\{0, 1\}^*$ -> G_1, H_2 : $\{0, 1\}^*$ -> Z_q^*, H_3 : G_2 -> Z_q^* 를 선택한다.

<69> (1) SETUP 알고리즘: 보안 파라미터 k를 입력으로 받는다.

<70> 랜덤 생성자 $g \in G_1^*$ 와 난수 $s \in Zq^*$ 를 선택한 후 $g^s \in G_1$을 계산한다. 다음, 시스템 공개키인 P <- (g, g^s)와 시스템 마스터키인 K <- s를 출력한다.

<71> (2) KG 알고리즘: 시스템 마스터키 K와 아이덴터티 $id \in \{0, 1\}^*$를 입력받는다.

<72> 공개키 pk_{id} <- $H_1(id) \in G_1$ 을 계산하고, 비밀키 sk_{id} <- $pk_{id}^s \in G_1$을 계산하여 출력한다.

<73> (3) RWD 알고리즘: 시스템 공개키 P, 신용 $c \in \{0, 1\}^*$, 아이덴터티 $id_B \in \{0, 1\}^*$, 비밀키 $sk_A \in G_1$ 및 난수 $r \in Zq^*$를 입력으로 받는다.

<74> x <- g^r, pk_B <- $H_1(id_B)$, h2 <- $H_2(id_A, c, x)$, 및 w <- $\mathbf{e}((g^s)^r, pk_B^{h2}) \in G_2$ 를 계산한다.

<75> h3 <- $H_3(w)$, y <- $sk_A^{h3} \in G_1$ 을 계산한 후, 익명 보상(anonymous reward) $R_A^B(c)$ <- (x, y) 를 출력한다.

<76> (4) SIG 알고리즘: 시스템 공개키 P, 아이덴터티 $id_A \in \{0, 1\}^*$, 신용 $c \in \{0, 1\}^*$, 비밀키 $sk_B \in G_1$, 그리고 난수 $r' \in Zq^*$ 를 입력으로 받는다.

<77> u <- $g^{r'}$, h2 <- $H_2(id_A, c, u)$, 및 v <- $sk_B^{h2} \in G_1$을 계산하고, 전자서명 $S_B^A(c)$ <- (u, v) 를 출력한다.

<78> (5) VER 알고리즘: 시스템 공개키 P, 전자서명 $S_B^A(c)$, 아이덴터티 $id_A \in \{0, 1\}^*$, 신용 $c \in \{0, 1\}^*$, 및 아이덴터티 $id_B \in \{0, 1\}^*$를 입력으로 받는다.

<79> pk_B <- $H_1(id_B)$, h2 <- $H_2(id_A, c, u)$를 계산한다.

<80> $\mathbf{e}(g, v) = e(g^s, pk_B^{h2})$ 이면 전자서명이 일치한다는 메시지를 출력하고 아니면, 일치하지 않는다는 메시지를 출력한다.

<81> (6) TEST 알고리즘: 시스템 공개키 P, 보상 $R_A^B(c)$, 전자서명 $S_B^A(c)$, 그리고 아이덴터티 $id_A \in \{0, 1\}^*$를 입력으로 받는다.

<82> pk_A <- $H_1(id_A)$, w <- **e**(x, v), 및 h3 <- H_3(w)를 계산한다.

<83> **e**(g, y) = **e**(g^s, pk_A^{h3}) 이면 신용주장이 유효하다는 메시지를 출력하고, 아니면 유효하지 않다는 메시지를 출력한다.

<84> 한편, 위와 같이 동작하는 자원공유 프로토콜에 있어서 신용기관이 존재하지 않는 경우, 각 노드에서 TEST 알고리즘을 수행해야 한다. 이때 트래픽을 중계한 노드가 자신에게 발급된 보상과 다른 노드에서 발급된 보상을 구분하여 변경 또는 제거와 같은 방법으로 다른 노드들에게 손해를 끼칠 수가 있다. 따라서, 중계 노드가 자신에게 발급된 보상과 다른 노드에게 발급된 보상을 구분할 수 없도록 하기 위해서 one-way 체인을 이용하여 난수를 생성한다. 또한 생성된 난수를 사용하여 상술한 알고리즘이 동작됨으로써 보상에 대한 어떠한 정보도 직접적으로 외부에 노출되지 않게 된다.

<85> 도 6은 본 발명의 실시예에 따른 Test 알고리즘이 수행되는 데이터 흐름이 도시된 흐름도로서, 노드 B가 노드 A의 트래픽을 중계하는 것을 예로 하여 설명한다.

<86> 노드 A는 one-way 체인의 길이를 결정한다. 이 길이는 새로운 one-way 체인이 생성되기까지의 시간간격의 최대값을 제한하게 되는데, 상기한 수학식 2를 사용하여 난수를 생성한다.

<87> 시간간격 i에 노드 A는 R_{ci}^{ri+1}을 생성하고 이것을 이웃 노드들에게 익명으로 퍼뜨린다. 노드 A는 난수 r_i를 노드 B에게 공개한다.

<88> 난수 r_i를 받은 다음 노드 B는 $F(r_i) = r_{i-1}$임을 검사한다. r_i가 유효하다면 노드 B는 서명 S_{ci-1}^{ri}를 생성한 후 이웃 노드들에게 퍼뜨린다.

<89> 점차적으로 네트워크에 있는 모든 노드들이 보상 R_{ci}^{ri+1}과 서명 S_{ci-1}^{ri}를 공유하게 된다. 노드 T는 보상 R_{ci}^{ri+1}을 디스크에 저장한다. 그리고 노드 T는 서명 S_{ci-1}^{ri}를 i-1에 저장되었던 보상들과 검사한다. 보상 중에 R_{ci-1}^{ri}가 존재하면 유효ㅎ한 것으로 판단하여 그에 따른 메시지가 출력된다.

<90> 이상과 같이 본 발명에 따른 무선 네트워크 시스템 및 그의 자원공유방법을 예시된 도면을 참조로 하여 설명하였으나 본 발명은 본 명세서에 개시된 실시예와 도면에 의해 한정되지 않으며, 다수의 알고리즘을 사용하여 안전하게 신용 및 보상정보의 유효성을 판단하여 네트워크 자원의 효율성을 향상하는 본 발명의 기술사상은 보호되는 범위 이내에서 당업자에 의해 용이하게 응용될 수 있다.

발명의 효과

<91> 상기와 같이 구성 및 동작하는 무선 네트워크 시스템 및 그의 자원공유방법은 제안된 자원공유 프로토콜을 통해 각 노드가 중계하는 중계정보의 유효성과 안전성을 보장함으로써 이기적인 노드들에게는 자원 할당을 적게 주고, 협력적인 노드들에게는 자원 할당을 많이 줌으로써 노드들이 전체 네트워크의 연결성에 협력하여 네트워크 자원을 효율적으로 활용할 수 있으며 연결의 안정성을 높일 수 있는 효과가 있다.

<92> 또한, ad-hoc무선 네트워크 뿐만 아니라 인접한 노드간에 자원 공유가 필요한 모든 네트워크에서 적용이 가능하므로 인접한 노드들 간에 다양한 자원(메모리, 스크린, 디스크, 키보드 등 주변장치나, 파일 등 데이터)의 공유가 필요하거나 그러한 공유를 이용하는 서비스 등에 폭 넓게 사용될 수 있다.

도면의 간단한 설명

<1> 도 1 은 일반적인 무선 네트워크 시스템에 있어서, 자원공유 흐름이 간략하게 도시된 개요도,

<2> 도 2 는 본 발명에 따른 무선 네트워크 시스템에 있어서, 신용기관이 존재하는 경우 자원공유 구조가 도시된 도,

<3> 도 3 은 본 발명에 따른 무선 네트워크 시스템에 있어서, 신용기관이 존재하지 않는 경우 자원공유 구조가 도시된 도,

<4> 도 4 는 본 발명에 따른 무선 네트워크 시스템에 있어서, 자원공유 방법이 도시된 순서도,

<5> 도 5 는 본 발명의 실시예에 따른 자원공유 데이터의 흐름이 도시된 흐름도, 및

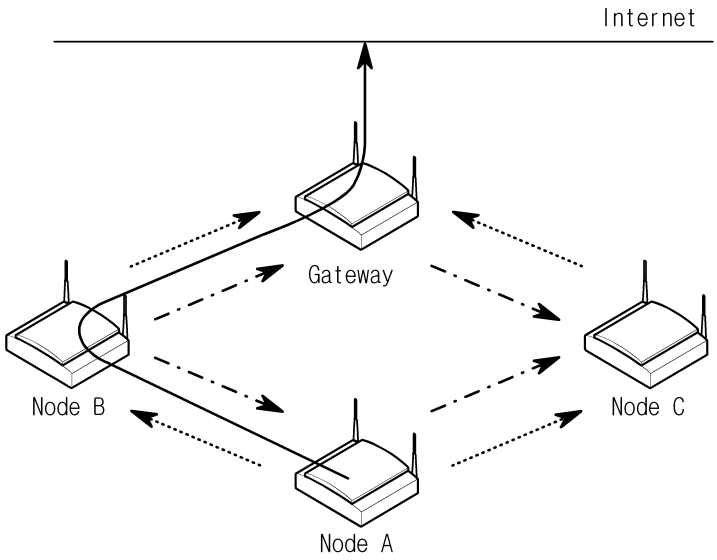
<6> 도 6 은 본 발명의 실시예에 따른 Test 알고리즘이 수행되는 데이터 흐름이 도시된 흐름도이다.

<7> <도면의 주요부분에 관한 설명>

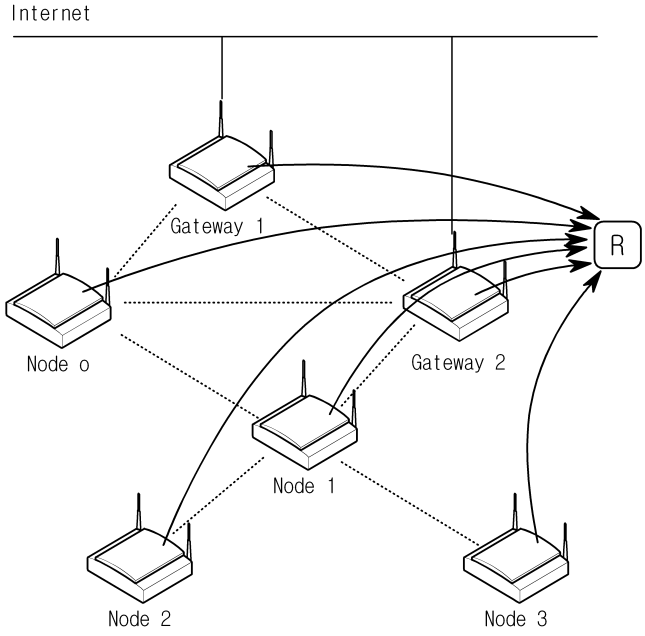
<8> R: 신용기관

도면

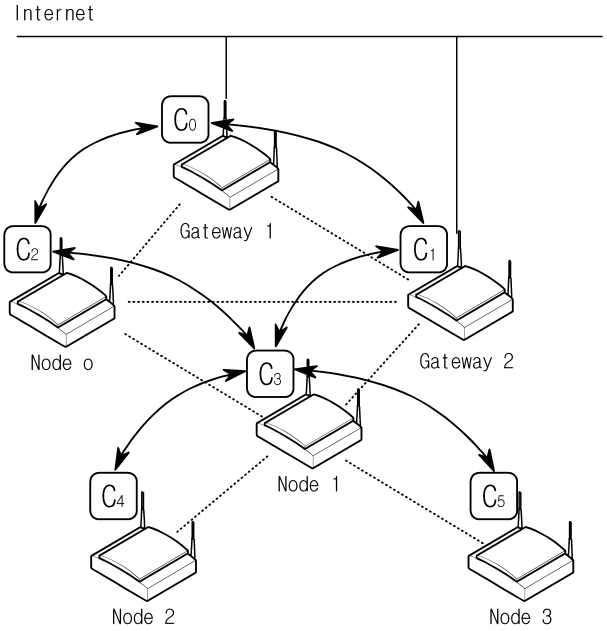
도면1



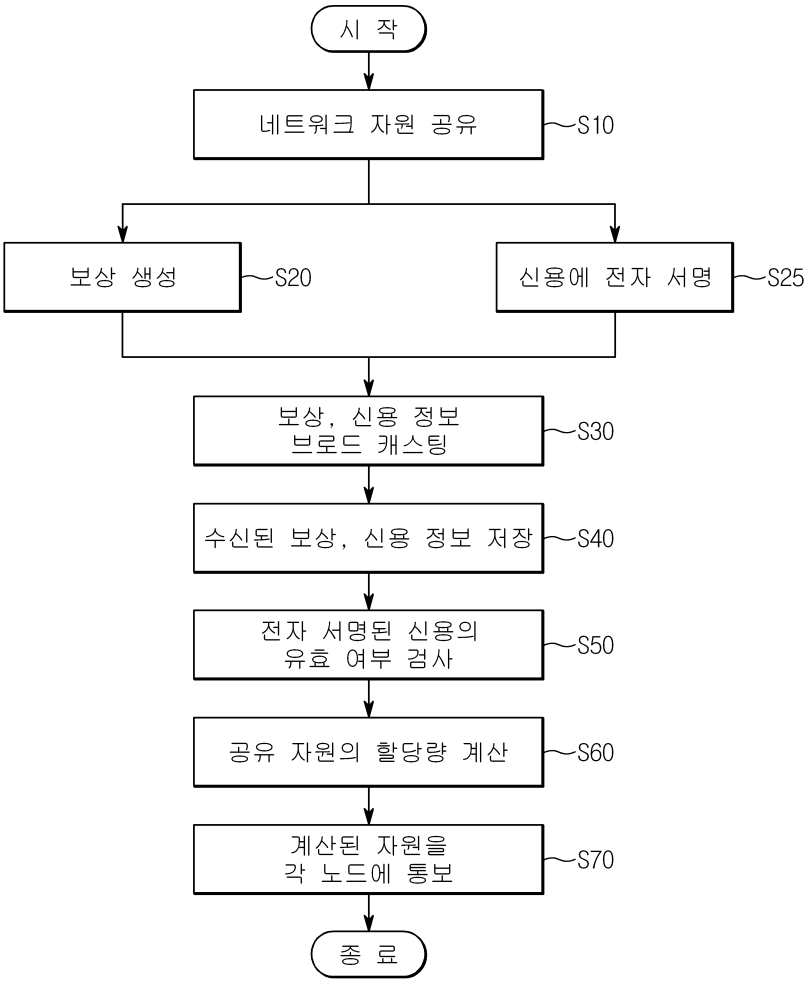
도면2



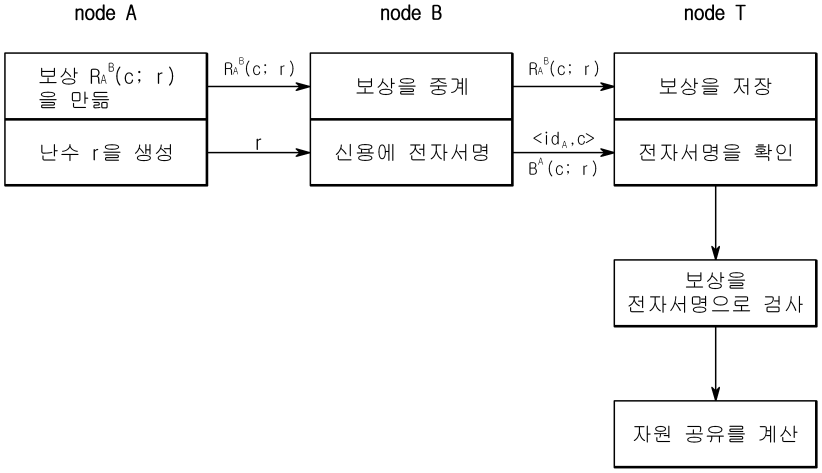
도면3


Internet
C0
Gateway 1
C2
C1
Node o
Gateway 2
C3
Node 1
C4
C5
Node 2
Node 3

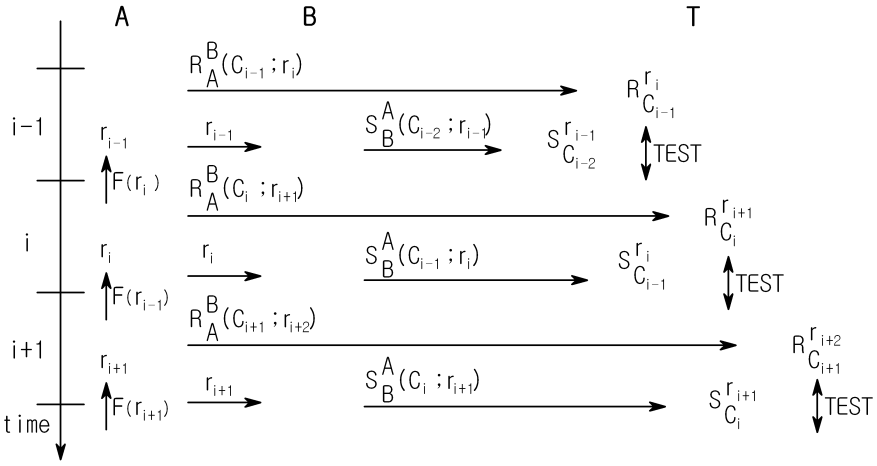
도면4


시 작
네트워크 자원 공유
S10
보상 생성
S20
신용에 전자 서명
S25
보상, 신용 정보
브로드 캐스팅
S30
수신된 보상, 신용 정보 저장
S40
전자 서명된 신용의
유효 여부 검사
S50
공유 자원의 할당량 계산
S60
계산된 자원을
각 노드에 통보
S70
종 료

도면5


node A
node B
node T
보상 $R_A^B(c; r)$ 을 만듦
난수 r을 생성
$R_A^B(c; r)$
r
보상을 중계
신용에 전자서명
$R_A^B(c; r)$
$<id_A, c>$
$B^A(c; r)$
보상을 저장
전자서명을 확인
보상을 전자서명으로 검사
자원 공유를 계산

도면6


A
B
T
i-1
i
i+1
time
$R_A^B(C_{i-1}; r_i)$
r_{i-1}
$F(r_i)$
$S_B^A(C_{i-2}; r_{i-1})$
$S_{C_{i-2}}^{r_{i-1}}$
$R_{C_{i-1}}^{r_i}$
TEST
$R_A^B(C_i; r_{i+1})$
r_i
$F(r_{i-1})$
$S_B^A(C_{i-1}; r_i)$
$S_{C_{i-1}}^{r_i}$
$R_{C_i}^{r_{i+1}}$
TEST
$R_A^B(C_{i+1}; r_{i+2})$
r_{i+1}
$F(r_{i+1})$
$S_B^A(C_i; r_{i+1})$
$S_{C_i}^{r_{i+1}}$
$R_{C_{i+1}}^{r_{i+2}}$
TEST