



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2020-0012375
(43) 공개일자 2020년02월05일

(51) 국제특허분류(Int. Cl.)
H04L 29/06 (2006.01) H04L 29/08 (2006.01)
(52) CPC특허분류
H04L 63/12 (2013.01)
H04L 67/1097 (2013.01)
(21) 출원번호 10-2018-0087609
(22) 출원일자 2018년07월27일
심사청구일자 2018년07월27일

(71) 출원인
이화여자대학교 산학협력단
서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)
(72) 발명자
유서희
서울특별시 중구 서소문로6길 34, 505호(중림동, 성요셉아파트)
도인실
인천광역시 연수구 센트럴로 194, 201동 2705호 (더샵센트럴파크2단지아파트)
채기준
서울특별시 강남구 강남대로136길 34, 402호 (논현동, 월드노블레스빌)
(74) 대리인
윤귀상

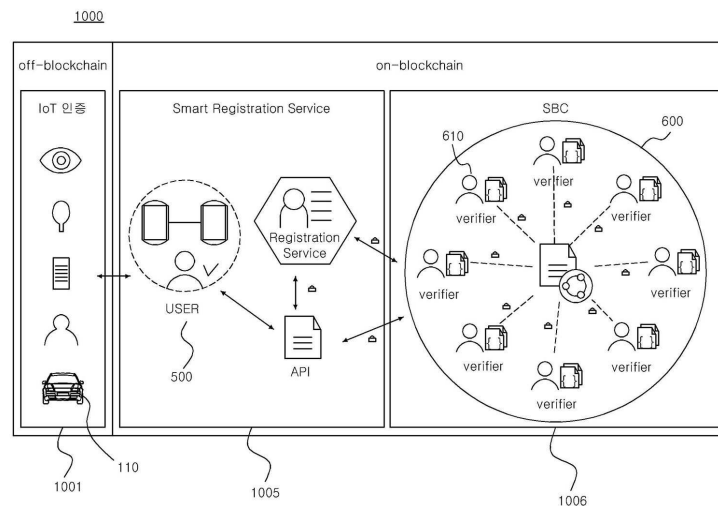
전체 청구항 수 : 총 15 항

(54) 발명의 명칭 D2D 통신 환경 하에서의 블록체인 시스템 및 이의 구축 방법

(57) 요약

D2D 통신 환경 하에서의 블록체인 시스템 및 이의 구축 방법이 개시된다. D2D 통신 환경 하에서의 블록체인 시스템은 블록체인에 저장할 사용자 데이터를 수집하고, 상기 블록체인의 예비 참여 노드의 D2D(Device-to-Device) 통신 리소스 값에 기초하여 상기 예비 참여 노드를 상기 블록체인의 참여 노드로의 등록 여부를 결정하는 스마트 등록 서비스 모듈 및 상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 사용자 데이터 저장에 대한 합의 알고리즘을 진행할 검증 노드를 선출하고, 상기 검증 노드에 의한 상기 합의 알고리즘을 진행하여 상기 사용자 데이터를 상기 블록체인에 저장하는 블록체인 합의 모듈을 포함한다.

대표도 - 도1



(52) CPC특허분류

H04L 67/12 (2013.01)

이 발명을 지원한 국가연구개발사업

과제고유번호 2016R1A2B4015899

부처명 과학기술정보통신부

연구관리전문기관 한국연구재단

연구사업명 기초연구사업(학술진흥)(2016)-중견연구자지원사업(총연구비1.5억초과~3억이하)

연구과제명 CPS 환경에서의 신뢰성있는 서비스 제공을 위한 보안기법 및 공격 대응 방안

기 여 율 1/1

주관기관 이화여자대학교 산학협력단

연구기간 2018.04.01 ~ 2019.02.28

명세서

청구범위

청구항 1

블록체인에 저장할 사용자 데이터를 수집하고, 상기 블록체인의 예비 참여 노드의 D2D(Device-to-Device) 통신 리소스 값에 기초하여 상기 예비 참여 노드를 상기 블록체인의 참여 노드로의 등록 여부를 결정하는 스마트 등록 서비스 모듈; 및

상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 사용자 데이터 저장에 대한 합의 알고리즘을 진행할 검증 노드를 선출하고, 상기 검증 노드에 의한 상기 합의 알고리즘을 진행하여 상기 사용자 데이터를 상기 블록체인에 저장하는 블록체인 합의 모듈을 포함하는 D2D 통신 환경 하에서의 블록체인 시스템.

청구항 2

제1항에 있어서,

상기 사용자 데이터를 수집하는 IoT(Internet of Things) 기기 및 상기 사용자 데이터를 상기 블록체인에 전송하는 모바일 기기 간의 인증을 진행하는 IoT 인증 모듈을 더 포함하는 D2D 통신 환경 하에서의 블록체인 시스템.

청구항 3

제1항에 있어서,

상기 스마트 등록 서비스 모듈은,

상기 블록체인 참여 노드 리스트인 스마트 등록 서비스 리스트; 및

상기 예비 참여 노드의 D2D 통신 리소스 값에 기초하여 상기 예비 참여 노드의 데이터 수신 가능성을 나타내는 보안 전송률을 계산하고, 상기 보안 전송률에 따라 상기 예비 참여 노드를 상기 스마트 등록 서비스 리스트에 등록하는 스마트 등록 서비스 리스트 관리부를 포함하는 D2D 통신 환경 하에서의 블록체인 시스템.

청구항 4

제3항에 있어서,

상기 스마트 등록 서비스 리스트 관리부는,

상기 예비 참여 노드의 RSSI(Received Signal Strength Indicator) 값을 이용하여 상기 보안 전송률을 계산하는 D2D 통신 환경 하에서의 블록체인 시스템.

청구항 5

제3항에 있어서,

상기 스마트 등록 서비스 리스트 관리부는,

노이즈 신호를 포함하는 D2D 통신 환경 하에서 상기 예비 참여 노드의 RSSI 값에 따른 보안 용량에서 상기 D2D 통신 환경 하에서 허가되지 않은 제 3자의 RSSI 값에 따른 보안 용량을 제외한 값을 상기 보안 전송률로 계산하는 D2D 통신 환경 하에서의 블록체인 시스템.

청구항 6

제1항에 있어서,

상기 블록체인 합의 모듈은,

상기 참여 노드에 의해 구축되는 블록체인; 및

상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 참여 노드의 무임승차(Free-riding) 여부를 판단할 수 있는 수치를 나타내는 참여도를 계산하고, 상기 참여도에 따라 상기 참여 노드를 상기 검증 노드로 선출하여 상기 합의 알고리즘을 진행하는 검증 노드 선출부를 포함하는 D2D 통신 환경 하에서의 블록체인 시스템.

청구항 7

제6항에 있어서,

상기 검증 노드 선출부는,

상기 참여 노드의 CPU 점유량 및 메모리 사용량에 따른 자원 사용량을 소정의 기준에 따라 정량화하여 레벨을 부여하고, 상기 참여 노드의 신호 세기 값을 소정의 기준에 따라 정량화하여 레벨을 부여하며, 상기 자원 사용량 레벨 값 및 상기 신호 세기 레벨 값을 이용하여 상기 참여 노드를 상기 검증 노드로 선출하는 D2D 통신 환경 하에서의 블록체인 시스템.

청구항 8

제7항에 있어서,

상기 검증 노드 선출부는,

상기 참여 노드의 자원 사용량 레벨 값이 1 이하가 되게 하는 참여도를 임계값으로 설정하고, 상기 참여 노드의 참여도가 임계값을 초과하는 경우 해당 참여 노드를 상기 검증 노드로 선출하는 D2D 통신 환경 하에서의 블록체인 시스템.

청구항 9

블록체인에 전송할 사용자 데이터를 수집하는 단계;

상기 블록체인의 예비 참여 노드의 D2D(Device-to-Device) 통신 리소스 값에 기초하여 상기 예비 참여 노드를 상기 블록체인의 참여 노드로의 등록 여부를 결정하는 단계;

상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 사용자 데이터 저장에 대한 합의 알고리즘을 진행할 검증 노드를 선출하는 단계; 및

상기 검증 노드에 의한 상기 합의 알고리즘을 진행하여 상기 사용자 데이터를 상기 블록체인에 저장하는 단계를 포함하는 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법.

청구항 10

제9항에 있어서,

상기 블록체인에 전송할 사용자 데이터를 수집하는 단계는,

상기 사용자 데이터를 수집하는 IoT(Internet of Things) 기기 및 상기 사용자 데이터를 상기 블록체인에 전송하는 모바일 기기 간의 인증을 진행하는 단계를 포함하는 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법.

청구항 11

제9항에 있어서,

상기 블록체인의 예비 참여 노드의 D2D(Device-to-Device) 통신 리소스 값에 기초하여 상기 예비 참여 노드를 상기 블록체인의 참여 노드로의 등록 여부를 결정하는 단계는,

상기 예비 참여 노드의 D2D 통신 리소스 값에 기초하여 상기 예비 참여 노드의 데이터 수신 가능성을 나타내는 보안 전송률을 계산하는 단계; 및

상기 보안 전송률에 따라 상기 예비 참여 노드를 스마트 등록 서비스 리스트에 등록하는 단계를 포함하는 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법.

청구항 12

제11항에 있어서,

상기 예비 참여 노드의 D2D 통신 리소스 값에 기초하여 상기 예비 참여 노드의 데이터 수신 가능성을 나타내는 보안 전송률을 계산하는 단계는,

노이즈 신호를 포함하는 D2D 통신 환경 하에서 상기 예비 참여 노드의 RSSI 값에 따른 보안 용량에서 상기 D2D 통신 환경 하에서 허가되지 않은 제 3자의 RSSI 값에 따른 보안 용량을 제외한 값을 상기 보안 전송률로 계산하는 단계인 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법.

청구항 13

제9항에 있어서,

상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 사용자 데이터 저장에 대한 합의 알고리즘을 진행할 검증 노드를 선출하는 단계는,

상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 참여 노드의 무임승차(Free-riding) 여부를 판단할 수 있는 수치를 나타내는 참여도를 계산하는 단계; 및

상기 참여도에 따라 상기 참여 노드를 상기 검증 노드로 선출하는 단계를 포함하는 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법.

청구항 14

제13항에 있어서,

상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 참여 노드의 무임승차 여부를 판단할 수 있는 수치를 나타내는 참여도를 계산하는 단계는,

상기 참여 노드의 CPU 점유량 및 메모리 사용량에 따른 자원 사용량을 소정의 기준에 따라 정량화하여 레벨을 부여하고, 상기 참여 노드의 신호 세기 값을 소정의 기준에 따라 정량화하여 레벨을 부여하는 단계;

상기 참여 노드의 자원 사용량 레벨 값이 1 이하가 되게 하는 참여도를 임계값으로 설정하는 단계; 및

상기 자원 사용량 레벨 값 및 상기 신호 세기 레벨 값을 이용하여 상기 참여 노드를 상기 검증 노드로 선출하되, 상기 참여 노드의 참여도가 임계값을 초과하는 경우 해당 참여 노드를 상기 검증 노드로 선출하는 단계를 포함하는 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법.

청구항 15

제9항에 있어서,

상기 검증 노드에 의한 상기 합의 알고리즘을 진행하여 상기 사용자 데이터를 상기 블록체인에 저장하는 단계는,

비잔틴 오류(Byzantine Fault) 합의 알고리즘에 따른 상기 합의 알고리즘을 진행하여 상기 사용자 데이터를 상기 블록체인에 저장하는 단계인 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법.

발명의 설명

기술 분야

[0001] 본 발명은 D2D 통신 환경 하에서의 블록체인 시스템 및 이의 구축 방법에 관한 것으로서, 더욱 상세하게는 D2D 통신 환경 하에서 사용자 데이터 전송 시, 사용자 데이터의 무결성을 입증하기 위한 블록체인 시스템 및 이의 구축 방법에 관한 것이다.

배경 기술

[0002] IoT 네트워크 환경의 발전에 힘입어 D2D(Device-to-Device) 통신 또한 각광받고 있다. 셀룰러 네트워크 통신 방식은 AP(Access Point)와 같이 데이터 전달을 관리하는 중앙 시설이 필수이나, D2D 통신은 디바이스 간에 직접 데이터를 교환할 수 있다. 따라서, D2D 통신은 셀룰러 네트워크 확장, 처리율 향상, 에너지 효율 향상 등의 장점이 있다.

- [0003] 한편, D2D 통신의 보안 취약성을 해결하기 위한 방법으로 블록체인 기술이 각광받고 있다. 블록체인은 피어-투-피어 통신을 기반으로 분산화 네트워크 환경을 구축하며, 거래내역을 체인 형식으로 형성함으로써 데이터의 안정성을 보장하는 기술이다.
- [0004] 그러나, D2D 통신 환경 하에서 블록체인 시스템이 적용되는 경우, 블록체인 시스템에 사용되는 다수의 디바이스가 네트워크를 공유하게 된다. 이에, 비인증 기기에 의한 프라이버시 침해 문제가 발생할 수 있다.
- [0005] 또한, D2D 통신 환경 하에서는 간접현상으로 인해 안전한 수신자가 아닌 인증되지 않은 악의적인 수신자가 비밀 메시지를 전송 받는 도청 가능성이 존재한다.
- [0006] 또한, 블록체인 시스템은 모든 참여자가 검증에 참여하기 때문에 참여자가 늘어날수록 성능이 떨어지는 문제점이 발생한다. 이는 메모리 용량이 한정되는 D2D 통신 환경에 적합하지 않다. 아울러, D2D 통신 환경에 참여하는 일부 이기적 노드는 에너지 절약을 위해 다른 노드의 데이터를 수신하면서 이를 전달하지는 않는 무임승차(Free-riding) 문제점이 있다. 이러한 이기적 노드에 의해 블록체인 시스템의 처리 속도를 현저히 저하시킬 수 있다.

발명의 내용

해결하려는 과제

- [0007] 본 발명의 일측면은 D2D 통신 기기의 보안성을 검증하여 블록체인에 참여시키고, D2D 통신 기기의 참여도 레벨을 검증하여 블록체인 합의 알고리즘의 검증자를 선출하는 D2D 통신 환경 하에서의 블록체인 시스템 및 이의 구축 방법을 제공한다.
- [0008] 본 발명의 다른 측면은 블록체인 합의가 진행되기 전의 오프-블록체인 영역에서 블록체인에 저장할 사용자 데이터를 수집하는 기기를 인증하여 검증된 사용자 데이터를 블록체인에 전송하는 블록체인 시스템 및 이의 구축 방법을 제공한다.

과제의 해결 수단

- [0009] 상기 과제를 해결하기 위한 본 발명의 D2D 통신 환경 하에서의 블록체인 시스템은 블록체인에 저장할 사용자 데이터를 수집하고, 상기 블록체인의 예비 참여 노드의 D2D(Device-to-Device) 통신 리소스 값에 기초하여 상기 예비 참여 노드를 상기 블록체인의 참여 노드로의 등록 여부를 결정하는 스마트 등록 서비스 모듈 및 상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 사용자 데이터 저장에 대한 합의 알고리즘을 진행할 검증 노드를 선출하고, 상기 검증 노드에 의한 상기 합의 알고리즘을 진행하여 상기 사용자 데이터를 상기 블록체인에 저장하는 블록체인 합의 모듈을 포함한다.
- [0010] 한편, 상기 사용자 데이터를 수집하는 IoT(Internet of Things) 기기 및 상기 사용자 데이터를 상기 블록체인에 전송하는 모바일 기기 간의 인증을 진행하는 IoT 인증 모듈을 더 포함할 수 있다.
- [0011] 또한, 상기 스마트 등록 서비스 모듈은, 상기 블록체인 참여 노드 리스트인 스마트 등록 서비스 리스트 및 상기 예비 참여 노드의 D2D 통신 리소스 값에 기초하여 상기 예비 참여 노드의 데이터 수신 가능성을 나타내는 보안 전송률을 계산하고, 상기 보안 전송률에 따라 상기 예비 참여 노드를 상기 스마트 등록 서비스 리스트에 등록하는 스마트 등록 서비스 리스트 관리부를 포함할 수 있다.
- [0012] 또한, 상기 스마트 등록 서비스 리스트 관리부는, 상기 예비 참여 노드의 RSSI(Received Signal Strength Indicator) 값을 이용하여 상기 보안 전송률을 계산할 수 있다.
- [0013] 또한, 상기 스마트 등록 서비스 리스트 관리부는, 노이즈 신호를 포함하는 D2D 통신 환경 하에서 상기 예비 참여 노드의 RSSI 값에 따른 보안 용량에서 상기 D2D 통신 환경 하에서 허가되지 않은 제 3자의 RSSI 값에 따른 보안 용량을 제외한 값을 상기 보안 전송률로 계산할 수 있다.
- [0014] 또한, 상기 블록체인 합의 모듈은, 상기 참여 노드에 의해 구축되는 블록체인 및 상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 참여 노드의 무임승차(Free-riding) 여부를 판단할 수 있는 수치를 나타내는 참여도를 계산하고, 상기 참여도에 따라 상기 참여 노드를 상기 검증 노드로 선출하여 상기 합의 알고리즘을 진행하는 검증 노드 선출부를 포함할 수 있다.
- [0015] 또한, 상기 검증 노드 선출부는, 상기 참여 노드의 CPU 점유량 및 메모리 사용량에 따른 자원 사용량을 소정의

기준에 따라 정량화하여 레벨을 부여하고, 상기 참여 노드의 신호 세기 값을 소정의 기준에 따라 정량화하여 레벨을 부여하며, 상기 자원 사용량 레벨 값 및 상기 신호 세기 레벨 값을 이용하여 상기 참여 노드를 상기 검증 노드로 선출할 수 있다.

[0016] 또한, 상기 검증 노드 선출부는, 상기 참여 노드의 자원 사용량 레벨 값이 1 이하가 되게 하는 참여도를 임계값으로 설정하고, 상기 참여 노드의 참여도가 임계값을 초과하는 경우 해당 참여 노드를 상기 검증 노드로 선출할 수 있다.

[0017] 또한, 상기 과제를 해결하기 위한 본 발명의 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법은 블록체인에 전송할 사용자 데이터를 수집하는 단계, 상기 블록체인의 예비 참여 노드의 D2D(Device-to-Device) 통신 리소스 값에 기초하여 상기 예비 참여 노드를 상기 블록체인의 참여 노드로의 등록 여부를 결정하는 단계, 상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 사용자 데이터 저장에 대한 합의 알고리즘을 진행할 검증 노드를 선출하는 단계 및 상기 검증 노드에 의한 상기 합의 알고리즘을 진행하여 상기 사용자 데이터를 상기 블록체인에 저장하는 단계를 포함한다.

[0018] 한편, 상기 블록체인에 전송할 사용자 데이터를 수집하는 단계는, 상기 사용자 데이터를 수집하는 IoT(Internet of Things) 기기 및 상기 사용자 데이터를 상기 블록체인에 전송하는 모바일 기기 간의 인증을 진행하는 단계를 포함할 수 있다.

[0019] 또한, 상기 블록체인의 예비 참여 노드의 D2D(Device-to-Device) 통신 리소스 값에 기초하여 상기 예비 참여 노드를 상기 블록체인의 참여 노드로의 등록 여부를 결정하는 단계는, 상기 예비 참여 노드의 D2D 통신 리소스 값에 기초하여 상기 예비 참여 노드의 데이터 수신 가능성을 나타내는 보안 전송률을 계산하는 단계 및 상기 보안 전송률에 따라 상기 예비 참여 노드를 스마트 등록 서비스 리스트에 등록하는 단계를 포함할 수 있다.

[0020] 또한, 상기 예비 참여 노드의 D2D 통신 리소스 값에 기초하여 상기 예비 참여 노드의 데이터 수신 가능성을 나타내는 보안 전송률을 계산하는 단계는, 노이즈 신호를 포함하는 D2D 통신 환경 하에서 상기 예비 참여 노드의 RSSI 값에 따른 보안 용량에서 상기 D2D 통신 환경 하에서 허가되지 않은 제 3자의 RSSI 값에 따른 보안 용량을 제외한 값을 상기 보안 전송률로 계산하는 단계일 수 있다.

[0021] 또한, 상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 사용자 데이터 저장에 대한 합의 알고리즘을 진행할 검증 노드를 선출하는 단계는, 상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 참여 노드의 무임승차(Free-riding) 여부를 판단할 수 있는 수치를 나타내는 참여도를 계산하는 단계 및 상기 참여도에 따라 상기 참여 노드를 상기 검증 노드로 선출하는 단계를 포함할 수 있다.

[0022] 또한, 상기 참여 노드의 자원 사용량 및 통신 세기 값에 기초하여 상기 참여 노드의 무임승차 여부를 판단할 수 있는 수치를 나타내는 참여도를 계산하는 단계는, 상기 참여 노드의 CPU 점유량 및 메모리 사용량에 따른 자원 사용량을 소정의 기준에 따라 정량화하여 레벨을 부여하고, 상기 참여 노드의 신호 세기 값을 소정의 기준에 따라 정량화하여 레벨을 부여하는 단계, 상기 참여 노드의 자원 사용량 레벨 값이 1 이하가 되게 하는 참여도를 임계값으로 설정하는 단계 및 상기 자원 사용량 레벨 값 및 상기 신호 세기 레벨 값을 이용하여 상기 참여 노드를 상기 검증 노드로 선출하되, 상기 참여 노드의 참여도가 임계값을 초과하는 경우 해당 참여 노드를 상기 검증 노드로 선출하는 단계를 포함할 수 있다.

[0023] 또한, 상기 검증 노드에 의한 상기 합의 알고리즘을 진행하여 상기 사용자 데이터를 상기 블록체인에 저장하는 단계는, 비잔틴 오류(Byzantine Fault) 합의 알고리즘에 따른 상기 합의 알고리즘을 진행하여 상기 사용자 데이터를 상기 블록체인에 저장하는 단계일 수 있다.

발명의 효과

[0024] 본 발명에 따르면, 온-블록체인 영역에서 보안성이 검증된 모바일 기기만을 블록체인에 참여시킴으로써, D2D 통신에서 발생 가능한 도청의 위험성을 방지하고 기밀성을 보장할 수 있다.

[0025] 또한, 온-블록체인 영역에서 참여도가 검증된 모바일 기기를 블록체인 합의 알고리즘의 검증자로 선출함으로써, 무임승차(Free-riding)를 방지하고, 전체 실행 시간 향상으로 가용성 저하를 막을 수 있다.

[0026] 또한, 오프-블록체인 영역에서 사용자 데이터를 수집하는 IoT 기기를 검증함으로써, 사용자 데이터 위변조로 인한 사고를 방지하고, 안정성을 보장할 수 있다.

도면의 간단한 설명

- [0027] 도 1은 본 발명의 일 실시예에 따른 D2D 통신 환경 하에서의 블록체인 시스템의 개념도이다.
- 도 2는 도 1에 도시된 블록체인 시스템에서의 데이터 흐름을 나타낸 흐름도이다.
- 도 3은 도 1에 도시된 오프-블록체인 영역에서의 데이터 흐름을 나타낸 흐름도이다.
- 도 4는 D2D 통신 환경에서 발생하는 노이즈 신호의 일 예를 도시한 그래프이다.
- 도 5는 D2D 통신 환경에서 RSSI 값에 따른 보안 전송률의 일 예를 도시한 그래프이다.
- 도 7은 본 발명의 일 실시예에 따른 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법의 순서도이다.

발명을 실시하기 위한 구체적인 내용

- [0028] 후술하는 본 발명에 대한 상세한 설명은, 본 발명이 실시될 수 있는 특정 실시예를 예시로서 도시하는 첨부 도면을 참조한다. 이들 실시예는 당업자가 본 발명을 실시할 수 있기에 충분하도록 상세히 설명된다. 본 발명의 다양한 실시예는 서로 다르지만 상호 배타적일 필요는 없음이 이해되어야 한다. 예를 들어, 여기에 기재되어 있는 특정 형상, 구조 및 특성은 일 실시예와 관련하여 본 발명의 정신 및 범위를 벗어나지 않으면서 다른 실시예로 구현될 수 있다. 또한, 각각의 개시된 실시예 내의 개별 구성요소의 위치 또는 배치는 본 발명의 정신 및 범위를 벗어나지 않으면서 변경될 수 있음이 이해되어야 한다. 따라서, 후술하는 상세한 설명은 한정적인 의미로서 취하려는 것이 아니며, 본 발명의 범위는, 적절하게 설명된다면, 그 청구항들이 주장하는 것과 균등한 모든 범위와 더불어 첨부된 청구항에 의해서만 한정된다. 도면에서 유사한 참조부호는 여러 측면에 걸쳐서 동일하거나 유사한 기능을 지칭한다.
- [0029] 이하, 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.
- [0030] 도 1은 본 발명의 일 실시예에 따른 D2D 통신 환경 하에서의 블록체인 시스템의 개념도이다.
- [0031] 도 1을 참조하면, 본 발명의 일 실시예에 따른 D2D(Device-to-Device) 통신 환경 하에서의 블록체인 시스템(이하, 블록체인 시스템)(1000)은 D2D 통신 환경 하에서 사용자 데이터 전송 시, 블록체인 기술을 적용하여 사용자 데이터의 무결성을 입증할 수 있다.
- [0032] D2D 통신은 기기 간 직접 통신으로 기지국이나 중간 인프라 없이 기기 간 유연한 데이터 교환이 가능하다. 예를 들면, D2D 통신은 NFC, ZigBee, Bluetooth, Wi-Fi 등을 포함할 수 있다. D2D 통신은 기기 간 직접 통신으로 네트워크 트래픽을 줄이고 통신 지연과 전력을 줄일 수 있으며, 재난, 전쟁 등으로 인해 기지국 가동이 멈춘 후에도 지속적인 통신이 가능하다는 장점을 갖는다. 이에 D2D 통신은 의료 분야, 금융 분야, IoT(Internet of Things) 서비스 등에 적용될 수 있으며, 특히 IoT 서비스에 있어서 저전력 기기가 지닌 통신 거리의 한계를 보완할 수 있어 각광받고 있다. 본 실시예에서는 IoT 서비스에 적용된 D2D 통신 환경을 예로 들어 설명하기로 한다.
- [0033] 본 발명의 일 실시예에 따른 블록체인 시스템(1000)은 오프-블록체인 영역 및 온-블록체인 영역으로 나뉘어질 수 있다. 오프-블록체인 영역에서는 사용자 데이터를 수집할 수 있다. 온-블록체인 영역에서는 D2D 통신을 수행하는 기기(500)의 보안성 및 가용성을 검증하여 블록체인(600)에 참여시키고, 이러한 블록체인(600)에 사용자 데이터를 저장할 수 있다.
- [0034] 본 발명의 일 실시예에 따른 블록체인 시스템(1000)은 오프-블록체인 영역에 IoT 인증 모듈(1001)을 포함하여, 사용자 데이터를 수집하는 IoT 기기(110)를 검증할 수 있다.
- [0035] IoT 기기(110)는 사용자 데이터를 수집하고, 수집한 데이터를 모바일 기기(500)를 매개체로 하여 블록체인(600)에 전송할 수 있다. IoT 기기(110)에서 수집하는 사용자 데이터는 사용자의 민감한 정보에 해당하며, 이러한 데이터를 다루는 어플리케이션의 경우 해킹 위험이 높다.
- [0036] 본 발명의 일 실시예에 따른 블록체인 시스템(1000)은 오프-블록체인 영역에 IoT 인증 모듈(1001)을 포함하여, 검증된 IoT 기기(110)로부터 사용자 데이터를 수집할 수 있다. 이와 관련하여 구체적인 설명은 도 3을 참조하여 후술하기로 한다.
- [0037] 본 발명의 일 실시예에 따른 블록체인 시스템(1000)은 온-블록체인 영역에 스마트 등록 서비스 모듈(1005) 및

블록체인 합의 모듈(1006)을 포함할 수 있다.

- [0038] 스마트 등록 서비스 모듈(1005)은 D2D 통신을 수행하는 모바일 기기(500)의 보안성을 검증하여 블록체인(600) 참여 허용 여부를 결정할 수 있다. 스마트 등록 서비스 모듈(1005)은 모바일 기기(500)의 RSSI(Received Signal Strength Indicator) 등을 포함하는 D2D 통신 리소스 값에 기초하여 모바일 기기(500)의 보안 전송률을 계산할 수 있다. 스마트 등록 서비스 모듈(1005)은 모바일 기기(500)의 보안 전송률에 따라 모바일 기기(500)를 블록체인(600)의 참여 노드인 거래 허용 참가자로 등록할 수 있다. 이와 관련하여 구체적인 설명은 도 4 및 도 5를 참조하여 후술하기로 한다.
- [0039] 본 발명의 일 실시예에 따른 블록체인 시스템(1000)은 온-블록체인 영역에 스마트 등록 서비스 모듈(1005)을 포함하여 보안성이 검증된 모바일 기기(500)만을 블록체인(600)에 참여시킴으로써, D2D 통신에서 발생 가능한 도청의 위험성을 방지하고 기밀성을 보장할 수 있다.
- [0040] 블록체인 합의 모듈(1006)은 블록체인(600)의 거래 허용 참가자로 등록된 모바일 기기(500)의 참여도를 검증하여 합의 알고리즘에 참여할 검증자(610)를 선출할 수 있다. 블록체인 합의 모듈(1006)은 블록체인(600)의 거래 허용 참가자로 등록된 모바일 기기(500)의 자원 사용량 및 통신 세기 값에 따라 합의 알고리즘에 참여하는 검증 노드인 검증자(610)를 선출할 수 있다. 검증자(610)로 선출된 모바일 기기는 비잔틴 오류(Byzantine Fault) 합의 알고리즘을 진행하여, 사용자 데이터를 블록체인(600)에 저장할 수 있다. 이와 관련하여 구체적인 설명은 도 6을 참조하여 후술하기로 한다.
- [0041] 본 발명의 일 실시예에 따른 블록체인 시스템(1000)은 온-블록체인 영역에 블록체인 합의 모듈(1006)을 포함하여 참여도가 검증된 모바일 기기(500)를 블록체인 합의 알고리즘의 검증자(610)로 선출함으로써, 무임승차(Free-riding)를 방지하고, 전체 실행 시간 향상으로 가용성 저하를 막을 수 있다.
- [0043] 도 2는 도 1에 도시된 블록체인 시스템에서의 데이터 흐름을 나타낸 흐름도이다.
- [0044] 도 2를 참조하면, 사용자 데이터를 수집하는 IoT 기기(110)와 사용자 데이터를 블록체인(600)에 전송하는 모바일 기기(500) 간의 인증이 진행될 수 있다(①). 이는 도 1에 도시된 오프-블록체인 영역에서 진행될 수 있다.
- [0045] IoT 기기(110)는 사용자 데이터를 수집하는 저전력 지능형 센서일 수 있다.
- [0046] 모바일 기기(500)는 D2D 통신이 가능하고 정보의 입출력이 가능한 장치로, 예를 들면, PC, 스마트폰, 태블릿 등으로 구현될 수 있다. 모바일 기기(500)는 Window, Linux, Android, iOS 등과 같은 운영 체제가 탑재될 수 있다. 본 실시예에서는 모바일 기기(500)는 Android가 탑재된 것을 예로 들어 설명하기로 한다.
- [0047] IoT 기기(110)는 특정 서버로부터 내려 받은 어플리케이션에 의해 실행될 수 있으며, 모바일 기기(500)는 특정 서버에서 인증한 기기일 수 있다. IoT 기기(110)는 특정 서버로부터 어플리케이션을 내려 받을 때 SEED 키(K_{seed})를 함께 내려 받을 수 있다. IoT 기기(110) 및 모바일 기기(500)는 이러한 SEED 키(K_{seed})를 이용하여 인증을 진행할 수 있다.
- [0048] 모바일 기기(500)는 IoT 기기(110)와의 인증이 완료되면, IoT 기기(110)에서 수집한 사용자 데이터를 D2D 통신 방식에 따라 도 1에 도시된 온-블록체인 영역으로 전달할 수 있다(②).
- [0049] 또한, 도 1에 도시된 온-블록체인 영역에서는 블록체인(600)을 구성하는 노드(501)를 검증하여 블록체인(600) 참여 허용 여부를 결정할 수 있다.
- [0050] 블록체인(600)은 사실 블록체인 플랫폼인 하이퍼레저일 수 있다.
- [0051] 노드(501)는 D2D 통신이 가능한 기기일 수 있으며, D2D 통신 환경 하에서 블록체인(600)을 구성할 수 있다.
- [0052] 도 2를 참조하면, 노드(501)의 보안 전송률 및 자원 사용량에 따라 참여도(P_{pi})가 계산될 수 있으며(③), 이러한 참여도(P_{pi})가 소정의 조건을 만족하는 경우, 해당 노드(501)는 스마트 등록 서비스 모듈(1005)로부터 블록체인(600)의 참여 노드(501)로 등록될 수 있다(④).
- [0053] 예를 들면, 스마트 등록 서비스 모듈(1005)에 등록된 노드(501)는 사용자 데이터에 대한 블록 및 스마트 컨트랙트를 작성할 수 있으며, 이를 다른 노드(501)로 브로드캐스트할 수 있다.
- [0054] 스마트 등록 서비스 모듈(1005)에 등록된 노드(501) 중, 참여도(P_{pi})가 소정의 조건을 만족하는 노드(501)는 블

록에 대한 합의 알고리즘을 진행하는 노드(501)로 선출될 수 있으며, 합의 알고리즘을 실행하고 그 결과를 다른 노드(501)로 브로드캐스트할 수 있다(⑤).

- [0056] 이하, 도 3을 참조하여 도 1에 도시된 오프-블록체인 영역에서의 데이터 흐름에 대해 구체적으로 설명한다.
- [0057] 도 3은 도 1에 도시된 오프-블록체인 영역에서의 데이터 흐름을 나타낸 흐름도이다.
- [0058] 도 3을 참조하면, 사용자 데이터를 수집하는 IoT 기기(110)에 대한 인증이 진행될 수 있다. 이는 도 1에 도시된 오프-블록체인 영역에 포함되는 IoT 인증 모듈(1001)에서 진행될 수 있다.
- [0059] IoT 인증 모듈(1001)은 사용자(111), IoT 기기(110), TrustZone 어플리케이션(500) 및 IoT 인증 서버(120)를 포함할 수 있다.
- [0060] 도 3에 도시된 TrustZone 어플리케이션(500)은 도 2의 모바일 기기(500)에 해당할 수 있다. 일반적으로 Android 운영체제가 탑재된 기기의 경우, TrustZone의 TEE(Trusted-Execution Environment) 보안 플랫폼이 탑재될 수 있다. TEE 보안 플랫폼은 운영체제의 접근 가능/불가능 영역을 분리하여 고립된 환경을 제공하는 플랫폼으로, 내부에 로드된 코드 및 데이터의 기밀성과 무결성을 보장할 수 있다. 본 실시예에서는 모바일 기기(500)에 탑재된 TrustZone 어플리케이션(500)을 이용하여 IoT 기기(110) 및 모바일 기기(500)의 무결성을 검증할 수 있다.
- [0061] 구체적으로는, IoT 기기(110)는 사용자(111)의 제어에 의해 IoT 인증 서버(120)로부터 내려 받는 어플리케이션에 의해 실행될 수 있다. IoT 기기(110)는 IoT 인증 서버(120)로부터 어플리케이션을 내려 받는 경우 SEED 키(K_{seed})를 함께 내려 받을 수 있다.
- [0062] IoT 기기(110)는 사용자(111)에 의해 실행되면, SEED 키(K_{seed}) 및 앱 ID(A_{ID})를 TrustZone 어플리케이션(500)으로 전송할 수 있다.
- [0063] TrustZone 어플리케이션(500)은 IoT 기기(110)로부터 수신한 SEED 키(K_{seed})를 검증하고, 그 결과, SEED 키(K_{seed})가 "true"로 검증되는 경우, 앱 ID(A_{ID})를 IoT 인증 서버(120)로 전달할 수 있다.
- [0064] SEED 키(K_{seed})가 "true"로 검증되는 경우, IoT 기기(110) 및 IoT 인증 서버(120)는 각각 IoT 기기(110)의 고유 번호(D_{ID}) 및 앱 ID(A_{ID})를 해싱한 후, 오늘 날짜(date)로 해싱하여 해시 값($H(1)$, $H(2)$)을 생성할 수 있다.
- [0065] IoT 인증 서버(120)는 두 해시 값($H(1)$, $H(2)$)을 비교하고, 그 결과 두 해시 값($H(1)$, $H(2)$)이 동일하면 IoT 기기(110)가 정상적인 기기인 것으로 판단할 수 있다.
- [0066] IoT 인증 서버(120)는 IoT 기기(110)가 정상적인 기기로 판단하면, 랜덤 키(K_{random})를 생성하여 IoT 기기(110)로 전달할 수 있다. 랜덤 키(K_{random})는 자동 로그인, 비정상 종료 후 남아있는 쿠키, 세션 값을 이용하여 악의적으로 데이터를 변형하거나, 암호화 키를 가로채는 것 등을 방지하기 위한 임시키로 사용될 수 있으며, 또는, 사용자 인증에 사용될 수 있다.
- [0067] 본 발명의 일 실시예에 따른 블록체인 시스템(1000)은 이와 같은 방식으로 사용자 데이터를 수집하는 IoT 기기(110) 및 이를 블록체인에 전달하는 모바일 디바이스(500) 간의 인증을 진행함으로써, 사용자 데이터의 위, 변조를 방지할 수 있으며, 사용자 데이터가 유출될 가능성을 예방할 수 있다.
- [0069] 이하, 도 1에 도시된 온-블록체인 영역에서의 데이터 흐름에 대해 구체적으로 설명한다.
- [0070] 도 1에 도시된 온-블록체인 영역에 포함되는 스마트 등록 서비스 모듈(1005)은 D2D 통신을 수행하는 모바일 기기(500)의 보안성을 검증하여 블록체인(600) 참여 허용 여부를 결정할 수 있다.
- [0071] 이하에서는, 설명의 편의를 위해 모바일 기기(500)를 블록체인(600)을 구성하는 노드로 칭하여 설명하기로 한다. 또한, 스마트 등록 서비스 모듈(1005)에 의해 보안성이 검증되기 전의 노드를 예비 참여 노드로 정의하고, 스마트 등록 서비스 모듈(1005)에 의해 블록체인(600) 참여가 허용된 노드를 참여 노드로 정의한다.
- [0072] 스마트 등록 서비스 모듈(1005)은 스마트 등록 서비스 리스트 및 이를 관리하는 스마트 등록 서비스 리스트 관리부를 포함할 수 있다. 스마트 등록 서비스 리스트는 블록체인(600) 참여가 허용된 노드 리스트일 수 있다. 스

마트 등록 서비스 리스트 관리부는 예비 참여 노드의 보안성을 검증하여 스마트 등록 서비스 리스트에 등록할 수 있다.

[0073] 구체적으로는, 스마트 등록 서비스 리스트 관리부는 예비 참여 노드의 D2D 통신 리소스 값에 기초하여 예비 참여 노드의 보안 전송률을 계산할 수 있다.

[0074] D2D 통신 리소스 값은 D2D 통신에서 발생하는 값을 의미하며 수신 신호 세기인 RSSI 값이 포함될 수 있다.

[0075] 보안 전송률은 D2D 통신에서 예비 참여 노드가 데이터를 수신할 가능성을 나타낼 수 있으며, 실제 D2D 통신 환경에서 잡음 Noise 및 Fading을 발생시킨 후, 허가된 수신자의 보안 용량에서 제 3자인 악의적인 도청자의 보안 용량을 제외한 값으로 정의될 수 있다. D2D 통신 환경 하에서 허가되지 않은 제 3자가 허가된 수신 대상과 근접하여 위치하는 경우, 허가되지 않은 제 3자가 데이터를 도청할 가능성이 높다. 따라서, D2D 통신 환경에서 송신자가 수신자에게 데이터 전송 시, 도청자가 해독할 수 없는 전송률을 이용하여 전송하는 경우 데이터를 수신자에게 안전하게 전달할 수 있을 것이다.

[0076] 이에, 본 실시예에서는 보안 전송률을 상술한 바와 같이 정의할 수 있으며, 보안 전송률이 높을수록 보안성이 높은 안전한 노드로 판단할 수 있다.

[0077] 스마트 등록 서비스 리스트 관리부는 아래 수학적 식 1에 따라 예비 참여 노드의 보안 전송률을 계산할 수 있다.

수학적 식 1

$$C_s = \left\{ W \log_2 \left(\frac{RSSI_m P}{\sigma_m^2} \right) - W \log_2 \left(\frac{RSSI_w P}{\sigma_w^2} \right) \right\}$$

$$if, \frac{RSSI_m P}{\sigma_m^2} > \frac{RSSI_w P}{\sigma_w^2}$$

[0078]

[0079] 수학적 식 1에서 P는 송신 전력, RSSI는 수신 신호 세기, σ_m^2 은 수신자를 방해하는 신호, σ_w^2 은 도청자를 방해하는 신호, W는 통신 대역폭을 의미하며 일예로, W=1일 수 있다.

[0080] 스마트 등록 서비스 리스트 관리부는 예비 참여 노드의 RSSI 값을 수학적 식 1에 대입할 수 있다. 스마트 등록 서비스 리스트 관리부는 매트랩을 이용하여 획득할 수 있는 Gaussian Noise 값을 수학적 식 1의 σ_m^2 및 σ_w^2 에 대입할 수 있다.

[0081] 도 4는 D2D 통신 환경에서 발생하는 노이즈 신호의 일 예를 도시한 그래프이다.

[0082] 도 4를 참조하면, Gaussian Noise 가 적용된 시그널 값과 평균 시그널 값을 확인할 수 있다. 스마트 등록 서비스 리스트 관리부는 예비 참여 노드의 RSSI 에서 노이즈가 적용된 시그널 값을 수학적 식 1에 적용하여 예비 참여 노드의 보안 전송률을 계산할 수 있다.

[0083] 도 5은 D2D 통신 환경에서 RSSI 값에 따른 보안 전송률의 일 예를 도시한 그래프이다.

[0084] 도 5를 참조하면, 도청자의 수신 방해 값이 작을수록 예비 참여 노드의 보안 전송률이 높아짐을 확인할 수 있다. 즉, 도청자의 수신 방해 값이 작을수록 예비 참여 노드가 안전하게 데이터를 수신할 가능성이 상승됨을 확인할 수 있다.

[0085] 스마트 등록 서비스 모듈(1005)은 이와 같은 예비 참여 노드의 보안 전송률을 계산하고, 예비 참여 노드의 보안 전송률이 높을수록 안전한 모바일 기기인 것으로 판단하고 관리할 수 있다.

[0086] 예를 들면, 스마트 등록 서비스 모듈(1005)은 예비 참여 노드의 보안 전송률이 1 이상으로 계산되는 경우, 해당 예비 참여 노드를 스마트 등록 서비스 리스트에 블록체인의 참여 노드로 등록할 수 있다. 이에 따라, 스마트 등록 서비스 모듈(1005)은 D2D 통신에서 발생할 수 있는 도청의 위험성을 방지하고, 인가된 기기를 구별함으로써

기밀성을 보장할 수 있다.

- [0088] 한편, 도 1에 도시된 온-블록체인 영역에 포함되는 블록체인 합의 모듈(1006)은 스마트 등록 서비스 리스트에 등록된 참여 노드 중 블록체인 합의 알고리즘에 참여할 노드를 선출하여 합의 알고리즘을 진행할 수 있다.
- [0089] 이하에서는, 설명의 편의를 위해 스마트 등록 서비스 리스트에 등록된 참여 노드 중, 합의 알고리즘에 참여할 노드로 선출된 노드를 검증 노드로 정의한다.
- [0090] 블록체인 합의 모듈(1006)은 블록체인 및 검증 노드 선출부를 포함할 수 있다. 블록체인은 사실 블록체인 플랫폼인 하이퍼레저로, 참여 노드에 의해 구축된 블록체인 네트워크일 수 있으며, 검증 노드 선출부는 참여 노드 중 블록체인에 사용자 데이터 저장에 대한 합의 알고리즘을 진행할 검증 노드를 선출할 수 있다.
- [0091] 구체적으로는, 검증 노드 선출부는 참여 노드의 CPU 점유량 및 메모리 사용량에 따른 자원 사용량을 소정의 기준에 따라 정량화하여 레벨을 부여할 수 있다. 또한, 검증 노드 선출부는 참여 노드의 신호 세기 값을 소정의 기준에 따라 정량화하여 레벨을 부여할 수 있다. 검증 노드 선출부는 참여 노드의 자원 사용량 레벨 값 및 신호 세기 레벨 값에 따라 검증 노드를 선출할 수 있다.

표 1

Level	Secrecy Capacity (Based on RSSI)
1	Fail
2	Weak < -70 dBm
3	Fair -60 to -70 dBm
4	Good -50 to -60 dBm
5	Excellent >-50 dBm

[0092]

표 2

Level	Resource Utilization (%) (Based on CPU & Memory)
1	CPU 0 & memory $\leq$ 0.06
2	CPU 0 & $0.06 <$ memory $\leq$ 0.08
3	$0.01 \leq$ CPU $<$ 0.03 & $0.08 <$ memory
4	$0.03 \leq$ CPU $<$ 0.05 & $0.08 <$ memory
5	$0.05 \leq$ CPU & $0.08 <$ memory

[0093]

[0094]

표 1은 신호 세기에 따라 나뉘지는 신호 세기 레벨 값의 일 예이고, 표 2는 CPU 점유량 및 메모리 사용량에 따라 나뉘지는 자원 사용량 레벨 값의 일 예이다.

[0095]

표 1 및 표 2와 같은 각 레벨 값을 구분하는 기준은 하이퍼레저 블록체인 플랫폼에서 각 노드를 도커(Docker) 가상 머신으로 구현한 경우, UCP(universal Control Plane)을 활용하여 설정될 수 있다.

[0096]

도 6은 도 1에 도시된 블록체인 합의 모듈에 의해 선출된 검증 노드의 일 예를 도시한 도면이다.

[0097]

도 6을 참조하면, 검증 노드 선출부는 참여 노드(620)의 자원 사용량 레벨 값(RC) 및 신호 세기 레벨 값(SC)에 따라 검증 노드(610)를 선출할 수 있다. 검증 노드 선출부는 자원 사용량 레벨 값(RC) 및 신호 세기 레벨 값(SC)이 높은 참여 노드(620)를 검증 노드(610)로 선출할 수 있다.

[0098]

예를 들면, 검증 노드 선출부는 참여 노드(620)의 자원 사용량 레벨 값(RC)이 3 이상인 경우 해당 참여 노드(620)를 검증 노드(610)로 선출할 수 있다. 또는, 검증 노드 선출부는 참여 노드(620)의 자원 사용량 레벨 값(RC)이 1 이하인 경우 해당 참여 노드(620)를 검증 노드(610)에서 제외할 수 있다.

[0099]

검증 노드 선출부는 이와 같이 참여 노드(620)의 자원 사용량 레벨 값(RC) 및 신호 세기 레벨 값(SC)에 따라 검증 노드(610)를 선출할 수 있도록 아래 수학적식 2에 따라 참여 노드(620)의 참여도를 계산할 수 있다.

수학적식 2

$$P_{pi} = W \left\{ \frac{SC_{pi} \times RU_{pi}}{\sum_{i=0}^n RU_{pi}} \right\}, RU_{pi} = (C_{pi} + M_{pi})$$

[0100]

[0101]

수학적식 2에서 SC_{pi} 는 참여 노드의 보안 전송률, RU_{pi} 는 참여 노드의 자원 사용량, C_{pi} 는 참여 노드의 CPU 사용량, M_{pi} 는 참여 노드의 메모리 사용량, W 는 통신 대역폭을 의미하며 일례로, $W=1$ 일 수 있다.

[0102]

검증 노드 선출부는 참여 노드(620)의 참여도에 따라 검증 노드(610)를 선별할 수 있다. 참여도는 참여 노드(620)의 무임승차 여부를 판단할 수 있는 수치를 나타낼 수 있으며, 참여도가 낮을수록 무임승차 가능성이 높은 것으로 판단할 수 있다. 예를 들면, 검증 노드 선출부는 참여 노드(620)의 자원 사용량 레벨 값(RC)이 1 이하가 되는 참여도를 임계값으로 설정하고, 참여 노드(620)의 참여도가 임계값을 초과하는 경우 해당 참여 노드(620)

를 검증 노드(610)로 선출할 수 있다.

- [0103] 사실 블록체인 플랫폼에 적용되는 합의 알고리즘은 PBFT(Practical Byzantine Fault Tolerance) 알고리즘으로, 다수결로 합의를 도출하는 방식이다. 따라서, 참여 노드의 수가 늘어날수록 전체 속도 저하 문제가 발생할 수 있으며, 일부 참여 노드가 악의적으로 담합하여 합의하는 경우 잘못된 검증이 진행될 수 있다. 이에, 본 실시예에서는 스마트 등록 서비스 리스트에 등록된 참여 노드를 대상으로 합의를 진행하되, 참여 노드의 참여도에 따라 검증 노드를 선별함으로써 참여 노드의 무임승차를 방지하여 전체 실행 시간을 향상시킬 수 있다.
- [0105] 이하에서는, 본 발명의 일 실시예에 따른 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법에 대하여 설명한다.
- [0106] 본 발명의 일 실시예에 따른 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법은 도 1에 도시된 블록체인 시스템(1000)과 실질적으로 동일한 구성에서 진행될 수 있다. 따라서, 도 1에 도시된 블록체인 시스템(1000)과 동일한 구성요소는 동일한 도면부호를 부여하고, 반복되는 설명은 생략하기로 한다.
- [0107] 도 7은 본 발명의 일 실시예에 따른 D2D 통신 환경 하에서의 블록체인 시스템 구축 방법의 순서도이다.
- [0108] 도 7을 참조하면, 오프-블록체인 영역에서는 인증된 IoT 기기(110)로부터 사용자 데이터를 수집할 수 있다(S10).
- [0109] IoT 인증 모듈(1001)은 사용자 데이터를 수집하는 IoT 기기(110)와 사용자 데이터를 블록체인(600)에 전송하는 모바일 기기(500) 간의 인증을 진행할 수 있다.
- [0110] IoT 기기(110)는 특정 서버로부터 내려 받은 어플리케이션에 의해 실행될 수 있으며, 모바일 기기(500)는 특정 서버에서 인증한 기기일 수 있다. IoT 기기(110)는 특정 서버로부터 어플리케이션을 내려 받을 때 SEED 키(K_{seed})를 함께 내려 받을 수 있다. IoT 인증 모듈(1001)은 이러한 SEED 키(K_{seed})를 이용하여 IoT 기기(110) 및 모바일 기기(500) 간의 인증을 진행할 수 있다.
- [0111] 온-블록체인 영역에서는 블록체인(600)의 예비 참여 노드의 보안 전송률을 계산하고(S20), 보안 전송률에 따라 예비 참여 노드의 참여 노드로의 등록을 결정할 수 있다(S30).
- [0112] 스마트 등록 서비스 모듈(1005)은 예비 참여 노드의 D2D 통신 리소스 값에 기초하여 예비 참여 노드의 보안 전송률을 계산할 수 있다.
- [0113] D2D 통신 리소스 값은 D2D 통신에서 발생하는 값을 의미하며 수신 신호 세기인 RSSI 값이 포함될 수 있다.
- [0114] 보안 전송률은 D2D 통신에서 예비 참여 노드가 데이터를 수신할 가능성을 나타낼 수 있으며, 실제 D2D 통신 환경에서 잡음 Noise 및 Fading을 발생시킨 후, 허가된 수신자의 보안 용량에서 제 3자인 악의적인 도청자의 보안 용량을 제외한 값으로 정의될 수 있다.
- [0115] 스마트 등록 서비스 모듈(1005)은 상술한 수학적 식 1에 따라 예비 참여 노드의 보안 전송률을 계산하고, 예비 참여 노드의 보안 전송률이 높을수록 안전한 모바일 기기인 것으로 판단하고 관리할 수 있다.
- [0116] 예를 들면, 스마트 등록 서비스 모듈(1005)은 예비 참여 노드의 보안 전송률이 1 이상으로 계산되는 경우, 해당 예비 참여 노드를 스마트 등록 서비스 리스트에 블록체인의 참여 노드로 등록할 수 있다.
- [0117] 온-블록체인 영역에서는 사용자 데이터에 대한 블록 및 스마트 컨트랙트를 작성하여 블록체인(600) 참여 노드로 브로드캐스트할 수 있다(S40).
- [0118] 그리고, 온-블록체인 영역에서는 참여 노드의 참여도를 계산하고(S50), 참여도에 따라 참여 노드를 검증 노드로 선출할 수 있다(S60).
- [0119] 블록체인 합의 모듈(1006)은 참여 노드 중 블록체인에 사용자 데이터 저장에 대한 합의 알고리즘을 진행할 검증 노드를 선출할 수 있다.
- [0120] 블록체인 합의 모듈(1006)은 상술한 수학적 식 2에 따라 참여 노드(620)의 참여도를 계산할 수 있다. 참여도는 참여 노드의 무임승차 여부를 판단할 수 있는 수치를 나타낼 수 있으며, 참여도가 낮을수록 무임승차 가능성이 높은 것으로 판단할 수 있다.
- [0121] 블록체인 합의 모듈(1006)은 참여도를 이용하여 자원 사용량 레벨 값(RC) 및 신호 세기 레벨 값(SC)이 높은 참

여 노드를 검증 노드로 선출할 수 있다.

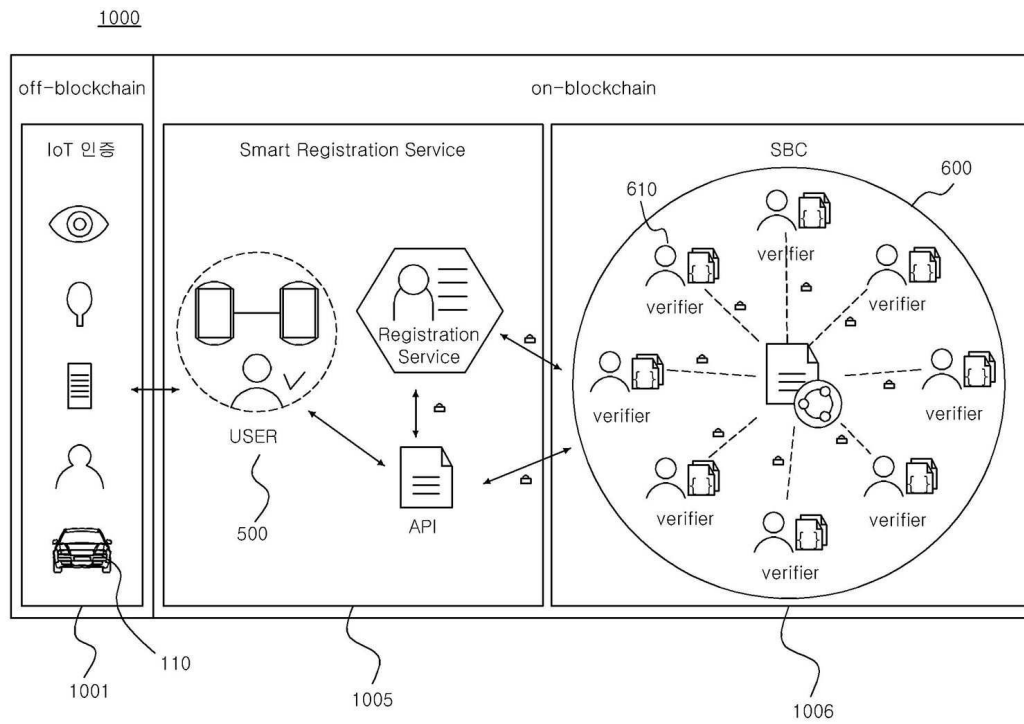
- [0122] 자원 사용량 레벨 값(RC)은 참여 노드의 CPU 점유량 및 메모리 사용량에 따른 자원 사용량을 소정의 기준에 따라 정량화하여 레벨을 부여한 값일 수 있다. 또한, 신호 세기 레벨 값(SC)은 참여 노드의 신호 세기 값을 소정의 기준에 따라 정량화하여 레벨을 부여한 값일 수 있다.
- [0123] 블록체인 합의 모듈(1006)은 참여 노드의 자원 사용량 레벨 값(RC)이 1 이하가 되는 참여도를 임계값으로 설정하고, 참여 노드의 참여도가 임계값을 초과하는 경우 해당 참여 노드를 검증 노드로 선출할 수 있다.
- [0124] 온-블록체인 영역에서는 검증 노드가 선출되면, 검증 노드에 의한 합의 알고리즘이 실행될 수 있으며(S70), 합의 알고리즘 결과에 따라 블록체인(600)에 블록이 저장될 수 있다(S80).
- [0125] 본 실시예에서 합의 알고리즘은 비잔틴 오류(Byzantine Fault) 합의 알고리즘을 따를 수 있다. 또한, 합의 알고리즘 실행 결과, 스마트 컨트랙트에 대한 검증이 완료되면, 블록을 체인에 연결하고 그 결과를 참여 노드로 브로드캐스트할 수 있다.
- [0127] 이와 같은, D2D 통신 환경 하에서의 블록체인 시스템 구축 방법은 애플리케이션으로 구현되거나 다양한 컴퓨터 구성요소를 통하여 수행될 수 있는 프로그램 명령어의 형태로 구현되어 컴퓨터 판독 가능한 기록 매체에 기록될 수 있다. 상기 컴퓨터 판독 가능한 기록 매체는 프로그램 명령어, 데이터 파일, 데이터 구조 등을 단독으로 또는 조합하여 포함할 수 있다.
- [0128] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.
- [0129] 컴퓨터 판독 가능한 기록 매체의 예에는, 하드 디스크, 플로피 디스크 및 자기 테이프와 같은 자기 매체, CD-ROM, DVD 와 같은 광기록 매체, 플롭티컬 디스크(floptical disk)와 같은 자기-광 매체(magneto-optical media), 및 ROM, RAM, 플래시 메모리 등과 같은 프로그램 명령어를 저장하고 수행하도록 특별히 구성된 하드웨어 장치가 포함된다.
- [0130] 프로그램 명령어의 예에는, 컴파일러에 의해 만들어지는 것과 같은 기계어 코드뿐만 아니라 인터프리터 등을 사용해서 컴퓨터에 의해서 실행될 수 있는 고급 언어 코드도 포함된다. 상기 하드웨어 장치는 본 발명에 따른 처리를 수행하기 위해 하나 이상의 소프트웨어 모듈로서 작동하도록 구성될 수 있으며, 그 역도 마찬가지이다.
- [0131] 이상에서는 실시예들을 참조하여 설명하였지만, 해당 기술 분야의 숙련된 당업자는 하기의 특허 청구범위에 기재된 본 발명의 사상 및 영역으로부터 벗어나지 않는 범위 내에서 본 발명을 다양하게 수정 및 변경시킬 수 있음을 이해할 수 있을 것이다.

부호의 설명

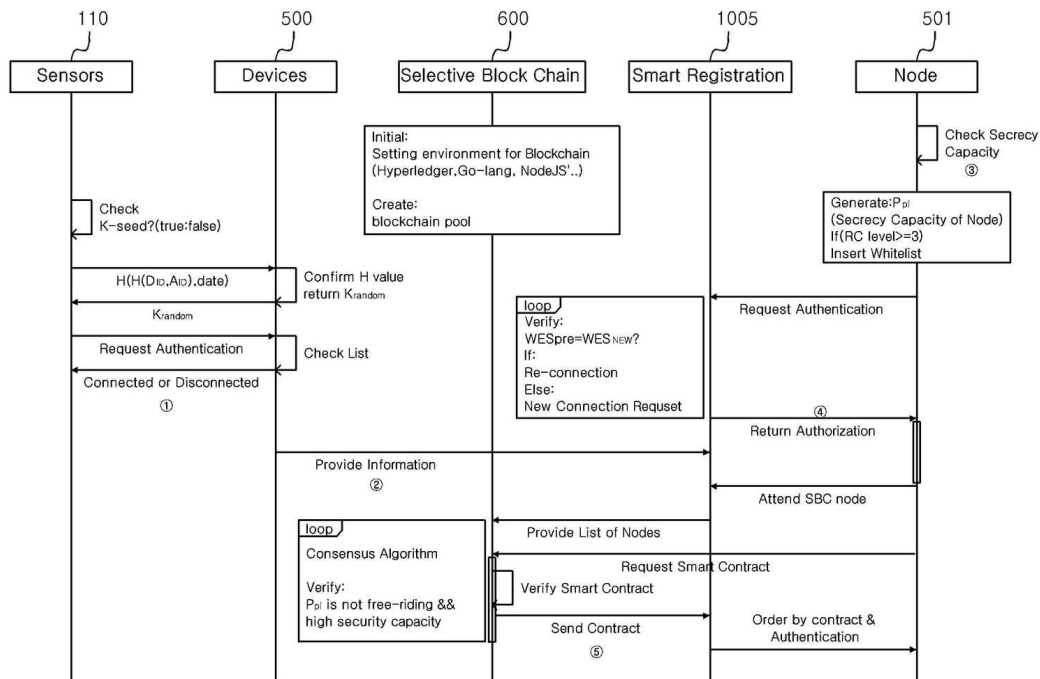
- [0132] 1000: D2D 통신 환경 하에서의 블록체인 시스템
- 1001: IoT 인증 모듈
- 1005: 스마트 등록 서비스 모듈
- 1006: 블록체인 합의 모듈
- 110: IoT 기기
- 500: 모바일 기기
- 600: 블록체인
- 610: 검증자

도면

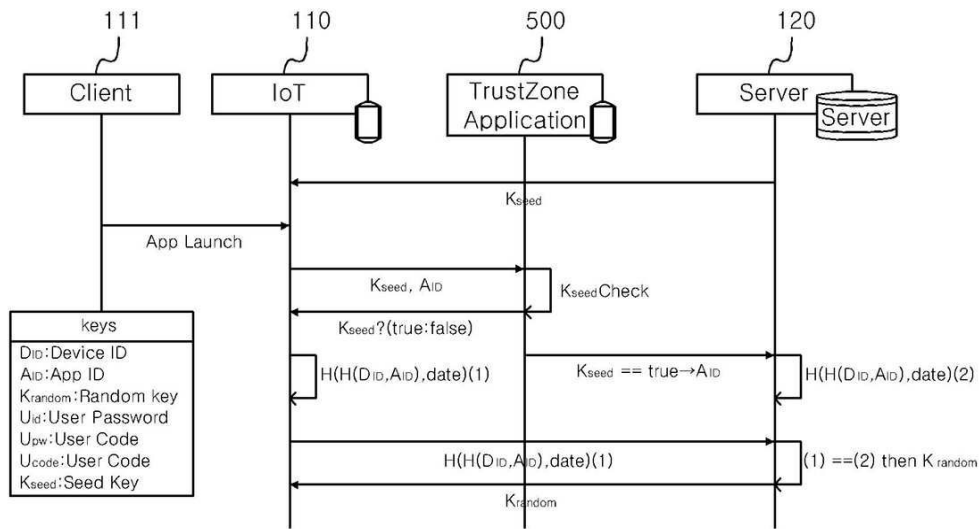
도면1



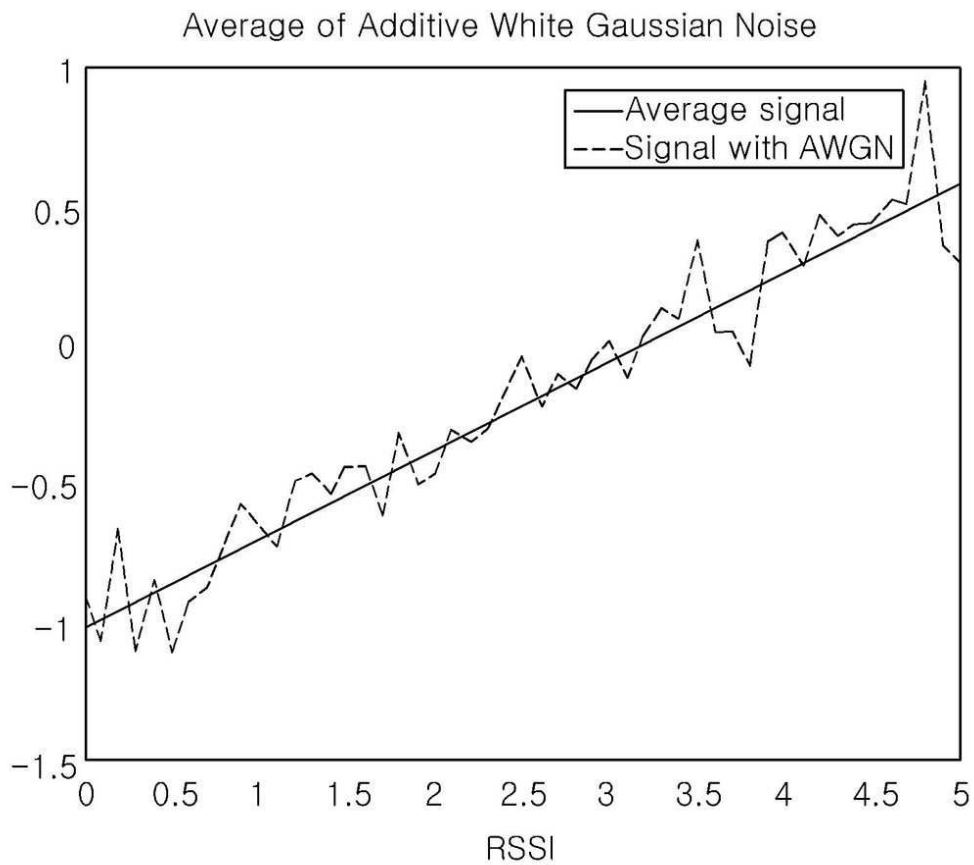
도면2



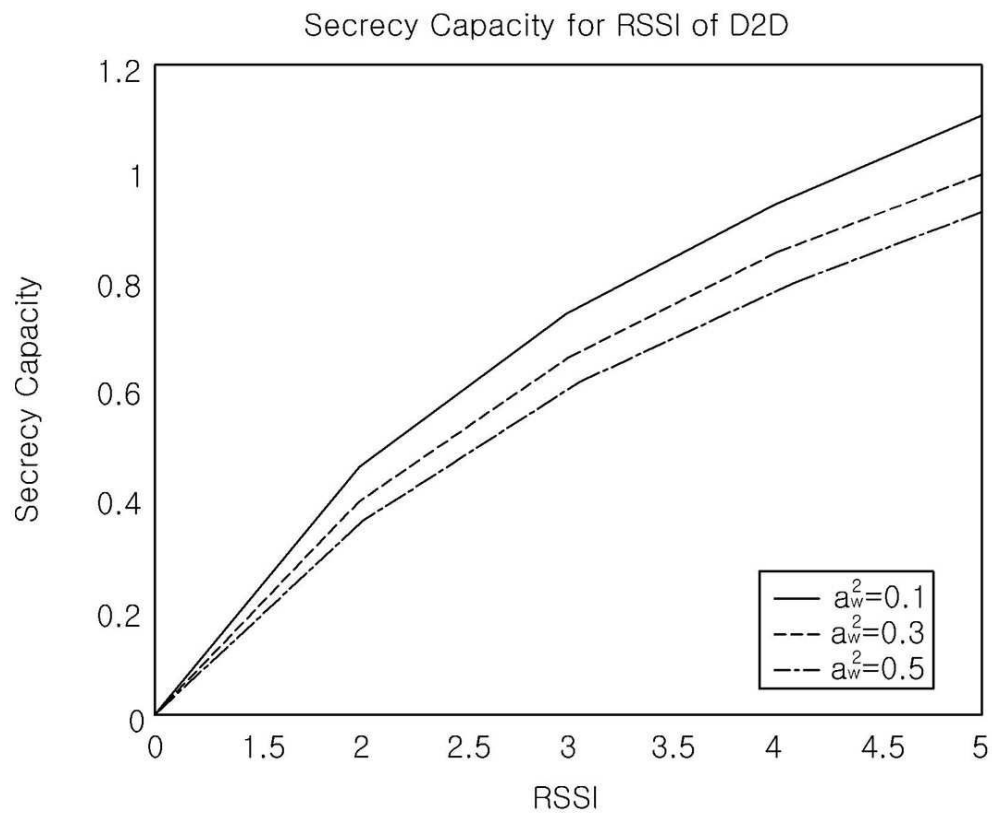
도면3



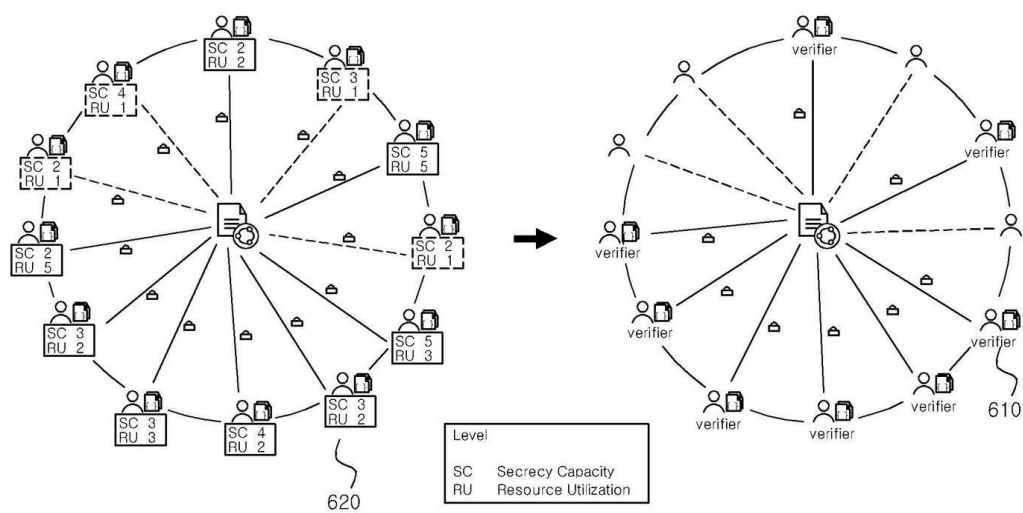
도면4



도면5



도면6



도면7

