



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0160031
(43) 공개일자 2023년11월23일

(51) 국제특허분류(Int. Cl.)

H04L 9/08 (2006.01) G16Y 10/35 (2020.01)
G16Y 20/10 (2020.01) H04L 67/1097 (2022.01)
H04L 9/00 (2022.01) H04W 4/02 (2018.01)
H04W 4/70 (2018.01) H04W 84/06 (2019.01)

(52) CPC특허분류

H04L 9/0833 (2013.01)
G16Y 10/35 (2020.01)

(21) 출원번호 10-2022-0059562

(22) 출원일자 2022년05월16일

심사청구일자 2022년05월16일

(71) 출원인

이화여자대학교 산학협력단

서울특별시 서대문구 이화여대길 52 (대현동, 이화여자대학교)

(72) 발명자

도인실

인천광역시 연수구 센트럴로 194, 201동 1703호
(더샵센트럴파크2단지아파트)

허가빈

경상남도 창원시 의창구 하남천서길21번길 8-14,
1동 1107호 (도계동, 강남훼미리아파트)

(74) 대리인

윤귀상

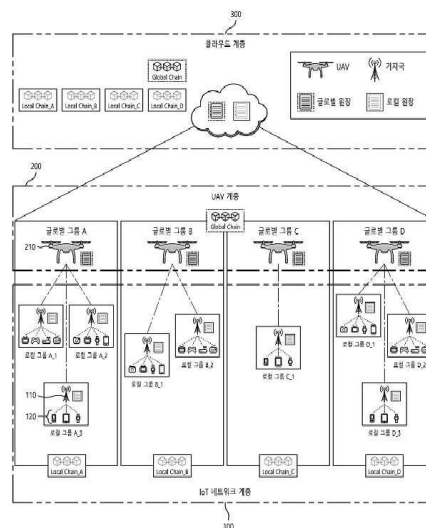
전체 청구항 수 : 총 18 항

(54) 발명의 명칭 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 시스템 및 방법

(57) 요약

본 발명은 도시 컴퓨팅 환경에서의 계층적 블록체인에 기반한 데이터 그룹 관리 시스템에 관한 것으로, 하나의 기지국과 복수의 IoT 기기들이 포함되는 로컬 그룹을 복수개 포함하는 엔드 노드; 상기 복수의 로컬 그룹을 설정 영역으로 그룹핑하고 상기 로컬 그룹과 통신하는 게이트웨이로서 데이터 전송을 수행하는 UAV를 복수개 포함하는 엣지 노드; 및 상기 엔드 노드와 상기 엣지 노드의 모든 데이터를 전달받아 데이터의 흐름을 추적하는 클라우드를 포함한다. 이에 의해 블록체인과 UAV를 이용하여 IoT 기기의 이동성과 데이터 밀집도를 판단하고 밀집 구역의 통신이 원활해지도록 할 수 있고, IoT의 데이터 보안을 위해 계층마다 다른 블록체인으로 구성하고, 같은 계층마다 원장을 공유하여 IoT 기기의 이동성과 밀집도를 판단할 수 있다.

대표도 - 도1



(52) CPC특허분류

G16Y 20/10 (2020.01)
H04L 67/1097 (2022.05)
H04L 9/0891 (2013.01)
H04L 9/50 (2022.05)
H04W 4/02 (2020.05)
H04W 4/70 (2018.02)
H04W 84/06 (2019.01)

이 발명을 지원한 국가연구개발사업

과제고유번호	1711154280
과제번호	2020R1A2C1006497
부처명	과학기술정보통신부
과제관리(전문)기관명	한국연구재단
연구사업명	개인기초연구(과기정통부)
연구과제명	UAV를 활용한 모바일 IoT 환경에서 효율적이고 안전한 노드 및 데이터 프라이버시
보장 기법	
기 여 율	1/1
과제수행기관명	이화여자대학교
연구기간	2022.03.01 ~ 2023.02.28

명세서

청구범위

청구항 1

도시 컴퓨팅 환경에서의 계층적 블록체인에 기반한 데이터 그룹 관리 시스템에 있어서,
 최하위에서 IoT 네트워크 계층을 형성하고, 하나의 기지국과 복수의 IoT 기기들이 포함되는 로컬 그룹을 복수개 포함하는 엔드 노드;
 상기 복수의 로컬 그룹을 설정 영역으로 그룹핑하고 상기 로컬 그룹과 통신하는 게이트웨이로서 데이터 전송을 수행하는 UAV를 복수개 포함하여 UAV(Unmanned Aerial Vehicle, 무인항공기) 계층을 형성하는 엣지 노드; 및
 최상위에서 클라우드 계층을 형성하고, 상기 엔드 노드와 상기 엣지 노드의 모든 데이터를 전달받아 저장하고, 데이터의 흐름을 추적하는 클라우드를 포함하고,
 상기 엣지 노드는,
 그룹핑된 각 로컬 그룹 간의 IoT 기기 이동성 및 상기 설정 영역의 IoT 기기 밀집도 중 적어도 하나를 판단하고, 판단한 결과에 기초하여 상기 로컬 그룹을 통합하거나 상기 UAV를 이동하도록 제어하는 것을 특징으로 하는 데이터 그룹 관리 시스템.

청구항 2

제1항에 있어서,
 상기 IoT 네트워크 계층은,
 동일한 UAV를 기준으로 그룹핑된 로컬 그룹의 기지국들끼리 블록체인 네트워크로 구성되어 상기 기지국들끼리 그룹 통신을 통해 각 기지국에서 생성된 데이터를 저장한 로컬 원장(Local Ledger)을 공유하고,
 상기 UAV 계층은,
 복수의 UAV들끼리 블록체인 네트워크로 구성되어 상기 UAV들끼리 각 UAV에서 생성된 데이터를 저장한 글로벌 원장(Global Ledger)을 공유하는 데이터 그룹 관리 시스템.

청구항 3

제2항에 있어서,
 상기 기지국은,
 상기 로컬 그룹 내 IoT 기기 정보가 변할 때마다 트랜잭션(Transaction, TX)을 발생시키고, 트랜잭션을 상기 로컬 원장에 저장하고, 상기 그룹 통신에 사용되는 그룹키를 변경하여 변경된 그룹키 정보를 상기 엣지 노드를 통해 해당 UAV에 전송하고,
 상기 UAV는,
 상기 엔드 노드를 통해 자신의 설정 영역 내 기지국에서 변경한 그룹키 정보를 전달받고, 전달받은 그룹키 정보를 이용하여 트랜잭션을 발생시키고, 트랜잭션을 상기 글로벌 원장에 저장하는 것을 특징으로 하는 데이터 그룹 관리 시스템.

청구항 4

제3항에 있어서,
 상기 IoT 네트워크 계층에서는,
 IoT 기기의 이동에 따라 IoT 기기가 소속된 로컬 그룹이 변경되면, 현재 로컬 그룹 내 기지국이 상기 IoT 기기의 이동 경로에 대한 정보를 상기 현재 로컬 그룹을 그룹핑한 UAV에 전송하는 것을 특징으로 하는 데이터 그룹

관리 시스템.

청구항 5

제4항에 있어서,

상기 엣지 노드는,

동일한 UAV에서 기설정된 시간 동안 발생한 트랜잭션들에서 두 개의 특정 기지국 아이디가 설정 횟수 이상 포함되면, 상기 특정 기지국 아이디 각각에 대응되는 특정 로컬 그룹들끼리 IoT 기기의 이동성이 높은 것으로 판단하는 것을 특징으로 하는 데이터 그룹 관리 시스템.

청구항 6

제5항에 있어서,

상기 엣지 노드는,

상기 이동성이 높은 것으로 판단한 경우, 상기 특정 로컬 그룹들이 기설정된 시간 동안 하나의 그룹키를 공유하도록 하는 것을 특징으로 하는 데이터 그룹 관리 시스템.

청구항 7

제4항에 있어서,

상기 엣지 노드는,

동일한 UAV에 상기 변경된 그룹키 정보가 설정 시간 내 설정 횟수 이상 전달되는 경우, 해당 설정 영역의 IoT 기기 밀집도가 높은 것으로 판단하는 것을 특징으로 하는 데이터 그룹 관리 시스템.

청구항 8

제5항에 있어서,

상기 엣지 노드는,

상기 밀집도가 높은 것으로 판단한 경우, 상기 글로벌 원장을 공유하여 가장 적은 트랜잭션을 발생시키는 UAV가 상기 IoT 기기가 밀집된 영역으로 이동하도록 제어하고,

상기 이동한 UAV의 엣지 노드는,

보조 게이트웨이 역할을 수행하여 상기 엣지 노드와 함께 상기 밀집된 영역의 트래픽을 완화시키는 것을 특징으로 하는 데이터 그룹 관리 시스템.

청구항 9

제8항에 있어서,

상기 UAV가 상기 밀집된 영역으로 이동하면, 상기 이동한 UAV의 이전 위치와 가장 인접한 위치의 UAV가 상기 이동한 UAV의 트랜잭션을 더 처리하는 것을 특징으로 하는 데이터 그룹 관리 시스템.

청구항 10

도시 컴퓨팅 환경에서의 계층적 블록체인에 기반한 데이터 그룹 관리 시스템에서 수행되는 데이터 그룹 관리 방법에 있어서,

하나의 기지국과 복수의 IoT 기기들이 포함되는 로컬 그룹을 복수개 포함하는 엔드 노드가 IoT 기기의 데이터를 전달하는 단계;

상기 복수의 로컬 그룹을 설정 영역으로 그룹핑하고 상기 로컬 그룹과 통신하는 UAV(Unmanned Aerial Vehicle, 무인항공기)를 복수개 포함하는 엣지 노드가 상기 전달받은 데이터를 처리하고 전달하는 단계; 및

최상위에서 클라우드 계층을 형성하는 클라우드가 상기 엔드 노드와 상기 엣지 노드의 모든 데이터를 전달받아 저장하고, 데이터의 흐름을 추적하는 단계를 포함하고,

상기 데이터를 처리하고 전달하는 단계에서는,

상기 엷지 노드가 그룹핑된 각 로컬 그룹 간의 IoT 기기 이동성 및 상기 설정 영역의 IoT 기기 밀집도 중 적어도 하나를 판단하고, 판단한 결과에 기초하여 상기 로컬 그룹을 통합하거나 상기 UAV를 이동하도록 제어하는 것을 특징으로 하는 데이터 그룹 관리 방법.

청구항 11

제10항에 있어서,

상기 엔드 노드는 최하위에서 IoT 네트워크 계층을 형성하고,

상기 IoT 네트워크 계층은,

동일한 UAV를 기준으로 그룹핑된 로컬 그룹의 기지국들끼리 블록체인 네트워크로 구성되고, 상기 기지국들끼리 그룹 통신을 통해 각 기지국에서 생성된 데이터를 저장한 로컬 원장 (Local Ledger)을 공유하고,

상기 엷지 노드는 UAV 계층을 형성하고, 상기 로컬 그룹과 통신하는 게이트웨이로서 데이터 전송을 수행하며,

상기 UAV 계층은,

복수의 UAV들끼리 블록체인 네트워크로 구성되어 상기 UAV들끼리 각 UAV에서 생성된 데이터를 저장한 글로벌 원장(Global Ledger)을 공유하는 데이터 그룹 관리 방법.

청구항 12

제11항에 있어서,

상기 데이터를 전달하는 단계에서는,

상기 기지국이 상기 로컬 그룹 내 IoT 기기 정보가 변할 때마다 트랜잭션(Transaction, TX)을 발생시키고, 트랜잭션을 상기 로컬 원장에 저장하고, 상기 그룹 통신에 사용되는 그룹키를 변경하여 변경된 그룹키 정보를 상기 엷지 노드를 통해 해당 UAV에 전송하고,

상기 데이터를 처리하고 전달하는 단계에서는,

상기 UAV가 상기 엔드 노드를 통해 자신의 설정 영역 내 기지국에서 변경한 그룹키 정보를 전달받고, 전달받은 그룹키 정보를 이용하여 발생시키고, 트랜잭션을 상기 글로벌 원장에 저장하는 것을 특징으로 하는 데이터 그룹 관리 방법.

청구항 13

제12항에 있어서,

상기 데이터를 전달하는 단계에서는,

IoT 기기의 이동에 따라 IoT 기기가 소속된 로컬 그룹이 변경되면, 현재 로컬 그룹 내 기지국이 상기 IoT 기기의 이동 경로에 대한 정보를 상기 현재 로컬 그룹을 그룹핑한 UAV에 전송하는 것을 특징으로 하는 데이터 그룹 관리 방법.

청구항 14

제13항에 있어서,

상기 데이터를 처리하고 전달하는 단계에서는,

동일한 UAV에서 기설정된 시간 동안 발생한 트랜잭션들에서 두 개의 특정 기지국 아이디가 설정 횟수 이상 포함되면, 상기 특정 기지국 아이디 각각에 대응되는 특정 로컬 그룹들끼리 IoT 기기의 이동성이 높은 것으로 판단하는 것을 특징으로 하는 데이터 그룹 관리 방법.

청구항 15

제14항에 있어서,

상기 데이터를 처리하고 전달하는 단계에서는,

상기 이동성이 높은 것으로 판단한 경우, 상기 특정 로컬 그룹들이 기설정된 시간 동안 하나의 그룹키를 공유하도록 하는 것을 특징으로 하는 데이터 그룹 관리 방법.

청구항 16

제13항에 있어서,

상기 데이터를 처리하고 전달하는 단계에서는,

동일한 UAV에 상기 변경된 그룹키 정보가 설정 시간 내 설정 횟수 이상 전달되는 경우, 해당 설정 영역의 IoT 기기 밀집도가 높은 것으로 판단하는 것을 특징으로 하는 데이터 그룹 관리 방법.

청구항 17

제16항에 있어서,

상기 데이터를 처리하고 전달하는 단계에서는,

상기 엣지 노드가 상기 밀집도가 높은 것으로 판단한 경우, 상기 글로벌 원장을 공유하여 가장 적은 트랜잭션을 발생시키는 UAV가 상기 IoT 기기가 밀집된 영역으로 이동하도록 제어하고,

상기 이동한 UAV 엣지 노드가 보조 게이트웨이 역할을 수행하여 상기 엣지 노드와 함께 상기 밀집된 영역의 트래픽을 완화시키는 것을 특징으로 하는 데이터 그룹 관리 방법.

청구항 18

제17항에 있어서,

상기 데이터를 처리하고 전달하는 단계에서는,

상기 UAV가 상기 밀집된 영역으로 이동하면, 상기 이동한 UAV의 이전 위치와 가장 인접한 위치의 UAV가 상기 이동한 UAV의 트랜잭션을 더 처리하는 것을 특징으로 하는 데이터 그룹 관리 방법.

발명의 설명

기술 분야

[0001] 본 발명은 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 시스템 및 방법에 관한 것으로, 보다 상세하게는 도시 컴퓨팅 환경에서 노드의 이동성과 밀집도를 판단하고, 블록체인과 UAV(Unmanned Aerial Vehicle, 무인항공기)를 이용하여 데이터 그룹을 관리할 수 있는 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 시스템 및 방법에 관한 것이다.

배경 기술

[0002] 사람과 사물을 포함하여 모든 것이 네트워크로 연결되어 정보를 공유하는 환경인 IoE(Internet of Everything) 시대로 발전하면서 모든 데이터는 중요한 자원이 되었다.

[0003] 최근 스마트 도시를 이루는 도시 컴퓨팅 환경에서는 통신 기술의 발달을 기반으로 사물인터넷(Internet of Things, 이하 IoT) 기기의 수가 증가하며 매일 방대하고 다양한 종류의 데이터가 생성되고 있다. 여기서 IoT는 다양한 사물에 부착된 센서를 통해 실시간으로 데이터를 주고받을 수 있는 기술이나 환경을 의미할 수 있다.

[0004] 이러한 IoT 환경은 다양한 IoT 기기로 구성되어 있어 많은 데이터를 생성하며, IoT 기기에서 수집된 데이터가 다른 IoT 기기의 학습 데이터로 사용되는 순환 구조로 이루어져 있다. 따라서 해당 환경에서 데이터는 공유되는 자원이며 매우 중요한 요소이다.

[0005] 하지만 모든 IoT 기기가 데이터를 발생시키는 환경에서 기기의 밀집도가 높을 경우, 데이터 손실 또는 전송 지연의 문제가 발생하게 된다.

[0006] 또한 모든 IoT 기기의 효율적인 통신을 위해 그룹 통신을 수행하는데 이동성이 높은 IoT 기기의 경우 이동에 따라 필수적으로 그룹키를 업데이트해야 하지만, 이러한 그룹키 업데이트에 대한 빈도가 높아지면 결국 시스템 성

능 저하로 이어진다는 문제가 있다.

[0007] 따라서 도시 컴퓨팅 환경에서의 데이터 그룹을 효율적으로 관리하기 위한 기술의 개발이 필요한 실정이다.

선행기술문헌

특허문헌

[0008] (특허문헌 0001) 대한민국 등록특허공보 제10-2154347호

발명의 내용

해결하려는 과제

[0009] 본 발명은 상기와 같은 문제를 해결하기 위해 안출된 것으로, 본 발명의 목적은 블록체인과 UAV를 이용하여 IoT 기기의 이동성과 데이터 밀집도를 판단하고 밀집 구역의 통신이 원활해지도록 하는 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 시스템 및 방법을 제공하는 것이다.

[0010] 또한 본 발명의 다른 목적은 IoT의 데이터 보안을 위해 계층마다 다른 블록체인으로 구성하고, 같은 계층마다 원장을 공유하여 IoT 기기의 이동성과 밀집도를 판단할 수 있는 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 시스템 및 방법을 제공하는 것이다.

[0011] 그리고 본 발명의 또 다른 목적은 IoT 기기의 이동성이 높은 그룹은 통신 그룹에 필요한 그룹키를 공유하도록 하여 그룹키 업데이트 오버헤드가 감소되도록 하고, 밀집 구역 발생시 같은 계층의 UAV를 활용하여 IoT 기기 밀집 구역의 트래픽이 완화되도록 하는 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 시스템 및 방법을 제공하는 것이다.

과제의 해결 수단

[0012] 상기 목적을 달성하기 위한 본 발명의 일 실시예에 따른 도시 컴퓨팅 환경에서의 계층적 블록체인에 기반한 데이터 그룹 관리 시스템은, 최하위에서 IoT 네트워크 계층을 형성하고, 하나의 기지국과 복수의 IoT 기기들이 포함되는 로컬 그룹을 복수개 포함하는 엔드 노드; 상기 복수의 로컬 그룹을 설정 영역으로 그룹핑하고 상기 로컬 그룹과 통신하는 게이트웨이로서 데이터 전송을 수행하는 UAV를 복수개 포함하여 UAV(Unmanned Aerial Vehicle, 무인항공기) 계층을 형성하는 엡지 노드; 및 최상위에서 클라우드 계층을 형성하고, 상기 엔드 노드와 상기 엡지 노드의 모든 데이터를 전달받아 저장하고, 데이터의 흐름을 추적하는 클라우드를 포함하고, 상기 엡지 노드는, 그룹핑된 각 로컬 그룹 간의 IoT 기기 이동성 및 상기 설정 영역의 IoT 기기 밀집도 중 적어도 하나를 판단하고, 판단한 결과에 기초하여 상기 로컬 그룹을 통합하거나 상기 UAV를 이동하도록 제어한다.

[0013] 그리고 상기 IoT 네트워크 계층은, 동일한 UAV를 기준으로 그룹핑된 로컬 그룹의 기지국들끼리 블록체인 네트워크로 구성되어 상기 기지국들끼리 그룹 통신을 통해 각 기지국에서 생성된 데이터를 저장한 로컬 원장(Local Ledger)을 공유하고, 상기 UAV 계층은, 복수의 UAV들끼리 블록체인 네트워크로 구성되어 상기 UAV들끼리 각 UAV에서 생성된 데이터를 저장한 글로벌 원장(Global Ledger)을 공유할 수 있다.

[0014] 또한 상기 기지국은, 상기 로컬 그룹 내 IoT 기기 정보가 변할 때마다 트랜잭션(Transaction, TX)을 발생시키고, 트랜잭션을 상기 로컬 원장에 저장하고, 상기 그룹 통신에 사용되는 그룹키를 변경하여 변경된 그룹키 정보를 상기 엡지 노드를 통해 해당 UAV에 전송하고, 상기 UAV는, 상기 엔드 노드를 통해 자신의 설정 영역 내 기지국에서 변경한 그룹키 정보를 전달받고, 전달받은 그룹키 정보를 이용하여 트랜잭션을 발생시키고, 트랜잭션을 상기 글로벌 원장에 저장할 수 있다.

[0015] 그리고 상기 IoT 네트워크 계층에서는, IoT 기기의 이동에 따라 IoT 기기가 소속된 로컬 그룹이 변경되면, 현재 로컬 그룹 내 기지국이 상기 IoT 기기의 이동 경로에 대한 정보를 상기 현재 로컬 그룹을 그룹핑한 UAV에 전송할 수 있다.

[0016] 또한 상기 엡지 노드는, 동일한 UAV에서 기설정된 시간 동안 발생한 트랜잭션들에서 두 개의 특정 기지국 아이디가 설정 횟수 이상 포함되면, 상기 특정 기지국 아이디 각각에 대응되는 특정 로컬 그룹들끼리 IoT 기기의 이동성이 높은 것으로 판단할 수 있다.

- [0017] 그리고 상기 엡지 노드는, 상기 이동성이 높은 것으로 판단한 경우, 상기 특정 로컬 그룹들이 기설정된 시간 동안 하나의 그룹키를 공유하도록 할 수 있다.
- [0018] 또한 상기 엡지 노드는, 동일한 UAV에 상기 변경된 그룹키 정보가 설정 시간 내 설정 횟수 이상 전달되는 경우, 해당 설정 영역의 IoT 기기 밀집도가 높은 것으로 판단할 수 있다.
- [0019] 그리고 상기 엡지 노드는, 상기 밀집도가 높은 것으로 판단한 경우, 상기 글로벌 원장을 공유하여 가장 적은 트랜잭션을 발생시키는 UAV가 상기 IoT 기기가 밀집된 영역으로 이동하도록 제어하고, 상기 이동한 UAV의 엡지 노드는, 보조 게이트웨이 역할을 수행하여 상기 엡지 노드와 함께 상기 밀집된 영역의 트래픽을 완화시킬 수 있다.
- [0020] 또한 상기 UAV가 상기 밀집된 영역으로 이동하면, 상기 이동한 UAV의 이전 위치와 가장 인접한 위치의 UAV가 상기 이동한 UAV의 트랜잭션을 더 처리할 수 있다.
- [0021] 한편 상기 다른 목적을 달성하기 위한 본 발명의 일 실시예에 따른 도시 컴퓨팅 환경에서의 계층적 블록체인에 기반한 데이터 그룹 관리 시스템에서 수행되는 데이터 그룹 관리 방법은, 하나의 기지국과 복수의 IoT 기기들이 포함되는 로컬 그룹을 복수개 포함하는 엔드 노드가 IoT 기기의 데이터를 전달하는 단계; 상기 복수의 로컬 그룹을 설정 영역으로 그룹핑하고 상기 로컬 그룹과 통신하는 UAV(Unmanned Aerial Vehicle, 무인항공기)를 복수개 포함하는 엡지 노드가 상기 전달받은 데이터를 처리하고 전달하는 단계; 및 최상위에서 클라우드 계층을 형성하는 클라우드가 상기 엔드 노드와 상기 엡지 노드의 모든 데이터를 전달받아 저장하고, 데이터의 흐름을 추적하는 단계를 포함하고, 상기 데이터를 처리하고 전달하는 단계에서는, 상기 엡지 노드가 그룹핑된 각 로컬 그룹 간의 IoT 기기 이동성 및 상기 설정 영역의 IoT 기기 밀집도 중 적어도 하나를 판단하고, 판단한 결과에 기초하여 상기 로컬 그룹을 통합하거나 상기 UAV를 이동하도록 제어할 수 있다.
- [0022] 그리고 상기 엔드 노드는 최하위에서 IoT 네트워크 계층을 형성하고, 상기 IoT 네트워크 계층은, 동일한 UAV를 기준으로 그룹핑된 로컬 그룹의 기지국들끼리 블록체인 네트워크로 구성되고, 상기 기지국들끼리 그룹 통신을 통해 각 기지국에서 생성된 데이터를 저장한 로컬 원장 (Local Ledger)을 공유하고, 상기 엡지 노드는 UAV 계층을 형성하고, 상기 로컬 그룹과 통신하는 게이트웨이로서 데이터 전송을 수행하며, 상기 UAV 계층은, 복수의 UAV들끼리 블록체인 네트워크로 구성되어 상기 UAV들끼리 각 UAV에서 생성된 데이터를 저장한 글로벌 원장 (Global Ledger)을 공유할 수 있다.
- [0023] 또한 상기 데이터를 전달하는 단계에서는, 상기 기지국이 상기 로컬 그룹 내 IoT 기기 정보가 변할 때마다 트랜잭션(Transaction, TX)을 발생시키고, 트랜잭션을 상기 로컬 원장에 저장하고, 상기 그룹 통신에 사용되는 그룹키를 변경하여 변경된 그룹키 정보를 상기 엡지 노드를 통해 해당 UAV에 전송하고, 상기 데이터를 처리하고 전달하는 단계에서는, 상기 UAV가 상기 엔드 노드를 통해 자신의 설정 영역 내 기지국에서 변경한 그룹키 정보를 전달받고, 전달받은 그룹키 정보를 이용하여 발생시키고, 트랜잭션을 상기 글로벌 원장에 저장할 수 있다.
- [0024] 그리고 상기 데이터를 전달하는 단계에서는, IoT 기기의 이동에 따라 IoT 기기가 소속된 로컬 그룹이 변경되면, 현재 로컬 그룹 내 기지국이 상기 IoT 기기의 이동 경로에 대한 정보를 상기 현재 로컬 그룹을 그룹핑한 UAV에 전송할 수 있다.
- [0025] 또한 상기 데이터를 처리하고 전달하는 단계에서는, 동일한 UAV에서 기설정된 시간 동안 발생한 트랜잭션들에서 두 개의 특정 기지국 아이디가 설정 횟수 이상 포함되면, 상기 특정 기지국 아이디 각각에 대응되는 특정 로컬 그룹들끼리 IoT 기기의 이동성이 높은 것으로 판단할 수 있다.
- [0026] 그리고 상기 데이터를 처리하고 전달하는 단계에서는, 상기 이동성이 높은 것으로 판단한 경우, 상기 특정 로컬 그룹들이 기설정된 시간 동안 하나의 그룹키를 공유하도록 할 수 있다.
- [0027] 또한 상기 데이터를 처리하고 전달하는 단계에서는, 동일한 UAV에 상기 변경된 그룹키 정보가 설정 시간 내 설정 횟수 이상 전달되는 경우, 해당 설정 영역의 IoT 기기 밀집도가 높은 것으로 판단할 수 있다.
- [0028] 그리고 상기 데이터를 처리하고 전달하는 단계에서는, 상기 엡지 노드가 상기 밀집도가 높은 것으로 판단한 경우, 상기 글로벌 원장을 공유하여 가장 적은 트랜잭션을 발생시키는 UAV가 상기 IoT 기기가 밀집된 영역으로 이동하도록 제어하고, 상기 이동한 UAV 엡지 노드가 보조 게이트웨이 역할을 수행하여 상기 엡지 노드와 함께 상기 밀집된 영역의 트래픽을 완화시킬 수 있다.
- [0029] 또한 상기 데이터를 처리하고 전달하는 단계에서는, 상기 UAV가 상기 밀집된 영역으로 이동하면, 상기 이동한

UAV의 이전 위치와 가장 인접한 위치의 UAV가 상기 이동한 UAV의 트랜잭션을 더 처리할 수 있다.

발명의 효과

- [0030] 상술한 본 발명의 일측면에 따르면, 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 시스템, 방법 및 이를 수행하기 위한 기록 매체를 제공함으로써, 블록체인과 UAV를 이용하여 IoT 기기의 이동성과 데이터 밀집도를 판단하고 밀집 구역의 통신이 원활해지도록 할 수 있고, IoT의 데이터 보안을 위해 계층마다 다른 블록체인으로 구성하고, 같은 계층마다 원장을 공유하여 IoT 기기의 이동성과 밀집도를 판단할 수 있다.
- [0031] 또한 본 발명에 따르면 IoT 기기의 이동성이 높은 그룹은 통신 그룹에 필요한 그룹키를 공유하도록 하여 그룹키 업데이트 오버헤드가 감소되도록 하고, 밀집 구역 발생시 같은 계층의 UAV를 활용하여 IoT 기기 밀집 구역의 트래픽이 완화되도록 할 수 있다.

도면의 간단한 설명

- [0032] 도 1은 본 발명의 실시예에 따른 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 시스템을 나타낸 구성도,
- 도 2는 도 1의 시스템에서 글로벌 원장과 로컬 원장의 트랜잭션 구성 요소를 예시적으로 도시한 도면,
- 도 3은 도 1의 시스템에서 두 로컬 그룹 간의 이동성이 높아 두 로컬 그룹이 통합된 경우를 설명하기 위한 도면,
- 도 4는 도 1의 시스템에서 밀집 구역 발생 시 UAV 이동을 설명하기 위한 도면,
- 도 5 내지 도 10은 본 발명의 실시예에 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 방법을 설명하기 위한 흐름도, 그리고,
- 도 11 내지 도 18은 도 1의 시스템의 효과를 설명하기 위한 실험 결과를 도시한 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0033] 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.
- [0034] 또한 본 발명에 따른 구성요소들은 물리적인 구분이 아니라 기능적인 구분에 의해서 정의되는 구성요소들로써 각각이 수행하는 기능들에 의해서 정의될 수 있다. 각각의 구성요소들은 하드웨어 또는 각각의 기능을 수행하는 프로그램 코드 및 프로세싱 유닛으로 구현될 수 있을 것이며, 두 개 이상의 구성요소의 기능이 하나의 구성요소에 포함되어 구현될 수도 있을 것이다. 따라서 이하의 실시예에서 구성요소에 부여되는 명칭은 각각의 구성요소를 물리적으로 구분하기 위한 것이 아니라 각각의 구성요소가 수행되는 대표적인 기능을 암시하기 위해서 부여된 것이며, 구성요소의 명칭에 의해서 본 발명의 기술적 사상이 한정되지 않는 것임에 유의하여야 한다.
- [0035] 본 발명에 따른 실시 예를 설명하기에 앞서, 본 발명은 도시 컴퓨팅 환경에서의 계층적 블록체인에 기반하며, 이때 블록체인은 ICT(Information & Communication Technology)의 핵심 기술 중 하나로, 차세대 네트워크 기술로 주목받고 있다. 블록체인이란 분산 데이터베이스의 일종으로 중앙 서버가 없으므로 모든 노드가 동등하다는 특징을 가진다.
- [0036] 이러한 블록체인은 누구나 자유롭게 네트워크에 참여할 수 있는 퍼블릭 블록체인과 허가 받은 사람만 네트워크에 참여할 수 있는 프라이빗 블록체인으로 나누어지며, 블록체인의 특징에 따라 PoW(Proof of Work), PoS(Proof of Stake), 또는 PBFT(Practical Byzantine Fault Tolerance) 등 다양한 합의 알고리즘을 사용하여 블록을 생성한다.

- [0037] 블록체인에서 데이터는 "블록"으로 불리며, 각 블록은 해시값을 통해 체인 형태로 연결되어 저장된다. 블록체인 참여자들은 모든 거래 내용을 검증하고 보관하기 때문에, 만약 악의적인 사용자가 거래 내용을 수정한다고 하더라도 하나의 거래를 수정하기 위해 모든 참여자의 원장을 수정해야 한다.
- [0038] 이에 블록체인은 제3자가 아닌 참여자들의 합의를 통해 데이터가 검증되므로 데이터의 신뢰성이 보장되며, 모두가 같은 정보를 가지고 있으므로 무결성이 보장된다는 특징을 가지고 있다.
- [0040] 이하에서는 도면들을 참조하여 본 발명의 바람직한 실시예들을 보다 상세하게 설명하기로 한다.
- [0041] 도 1은 본 발명의 실시예에 따른 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 시스템을 나타낸 구성도이다.
- [0042] 도 1에서와 같이 본 발명의 실시예에 따른 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 시스템(이하 시스템)은, IoT 네트워크 계층(100), UAV 계층(200) 및 클라우드 계층(300)을 포함한다.
- [0043] 먼저, IoT 네트워크 계층(100)은 최하위 계층으로서, IoT 기기(120)의 실제 데이터를 가지고 있는 복수의 엔드 노드로 형성된다.
- [0044] 자세히는, IoT 네트워크 계층(100)은 하나의 기지국(110)과 복수의 IoT 기기(120)들이 포함되는 로컬 그룹(Local Group)을 복수개 포함하고, 각각의 로컬 그룹에 포함되는 복수의 엔드 노드로 형성된다.
- [0045] 이때, IoT 네트워크 계층(100)은 실제 IoT 어플리케이션을 이용하는 사용자들의 계층이다.
- [0046] 따라서, 엔드 노드는 실제 트래픽 데이터를 가지고 있는 노드이며, 하나의 엣지 노드에 복수의 엔드 노드가 연결될 수 있다. 엔드 노드의 예로는 사용자의 태블릿, 스마트폰, 스마트 워치, 노트북 등일 수 있으며, 디바이스(device), 기구(apparatus), 단말(terminal), UE(user equipment), MS(mobile station), 무선기기(wireless device), 휴대기기(handheld device) 등 다른 용어로 불릴 수도 있다. 본 발명의 실시 예에서는 이와 같은 기기들을 통합하여 IoT 기기(120)로 지칭하기로 한다.
- [0047] IoT는 사물과 그에 부착된 센서를 통해 실시간으로 데이터를 주고받고 이용할 수 있는 기술이나 환경을 말한다. IoT 환경에 기반한 IoT 서비스는 인간의 조작이 필요하지 않고, 사물 간의 인터넷 통신과 정보 교환이 가능하다는 특징이 있다.
- [0048] 또한, IoT 네트워크 계층(100)은, 동일한 UAV(210)에 그룹핑된 로컬 그룹(L)의 기지국(110)들끼리 블록체인 네트워크로 구성되고, 기지국(110)들끼리 그룹 통신을 통해 각 기지국(110)에서 생성된 데이터를 저장한 로컬 원장(Local Ledger)을 공유한다.
- [0049] 이때, 기지국(110)의 통신 영역에 따라 로컬 그룹(L) 내 포함된 IoT 기기(120)들은 그룹 통신을 진행한다. 즉, 도 1에 나타난 '로컬 그룹 A_1' 영역처럼 각 IoT 기기(120)들은 기지국(110)을 기준으로 그룹 통신을 진행하며, 로컬 그룹들(A_1, A_2, A_3)은 지리적으로 그룹핑되어 '글로벌 그룹 A' 영역과 같이 UAV(210)가 관리하는 글로벌 그룹(A)을 이루게 된다.
- [0050] 또한, 기지국(110)은 로컬 그룹 내 IoT 기기(120) 정보가 변할 때마다 트랜잭션(Transaction, TX)을 발생시키고 트랜잭션을 로컬 원장에 저장하고, 그룹 통신에 사용되는 그룹키를 업데이트, 즉 변경하여 변경된 그룹키 정보를 엣지 노드를 통해 해당 UAV(210)에 전송한다.
- [0051] 로컬 원장의 트랜잭션은 트랜잭션 발생시간, 로컬 그룹 아이디, IoT 기기(120) 리스트 및 IoT 기기(120)의 이동 경로 중 적어도 하나 이상을 포함할 수 있다.
- [0052] 그리고 IoT 네트워크 계층(100)은 IoT 기기(120)의 이동에 따라 IoT 기기(120)가 소속된 로컬 그룹이 변경되면, 현재 로컬 그룹 내 기지국(110)이 이전 로컬 그룹 내 기지국 아이디를 현재 로컬 그룹을 그룹핑한 UAV에 전송할 수 있다.
- [0053] 그리고 UAV 계층(200)은 실제 환경에 효율적으로 적용하기 위한 복수의 UAV(Unmanned Aerial Vehicle, 무인항공기)(210)가 구성하는 복수의 엣지 노드로 형성된다.
- [0054] 자세히는, UAV 계층(200)은 복수의 로컬 그룹을 설정 영역으로 그룹핑하여 통신하는 게이트웨이로서 데이터 전송을 수행하는 UAV(210)가 복수로 구성되어 각각의 UAV(210)가 구성하는 복수의 엣지 노드로 형성된다. UAV 계

층(200)은 이에 하나의 UAV(210)에 복수의 로컬 그룹을 그룹핑한 글로벌 그룹을 포함할 수 있다.

- [0055] 이때, 각각의 엣지 노드들은 그룹핑된 각 로컬 그룹 간의 IoT 기기(120) 이동성 및 설정 영역의 IoT 기기(120) 밀집도 중 적어도 하나를 판단하고, 판단한 결과에 기초하여 로컬 그룹을 통합하거나 UAV(210)가 이동하도록 제어할 수 있다.
- [0056] 그리고 엣지 노드들은 IoT 기기(120)의 밀집도가 높은 영역에서 보조 게이트웨이 역할을 함으로써 효율적으로 데이터 전송을 수행하는 역할을 한다.
- [0057] 또한, UAV 계층(200)은 복수의 UAV(210)들끼리 블록체인 네트워크로 구성되어 UAV(210)들끼리 각 UAV(210)에서 생성된 데이터를 저장한 글로벌 원장(Global Ledger)을 공유한다.
- [0058] 따라서 본 실시예에 따른 시스템에서 블록체인은 UAV(210)들끼리 공유하는 글로벌 체인과 하나의 글로벌 그룹으로 그룹핑된 로컬 그룹에 포함되는 기지국(110)들끼리 공유하는 로컬 체인으로 구분될 수 있다.
- [0059] 여기서 동일한 글로벌 그룹에 속하는 기지국(110)의 로컬 체인은 IoT 기기(120)의 비정상 동작 여부를 확인하는 보안 장치 인증을 위한 블록체인이다.
- [0060] 그리고 UAV(210)는 엔드 노드를 통해 자신의 설정 영역 내 기지국(110)에서 변경한 그룹키 정보를 전달받고, 전달받은 그룹키 정보를 이용하여 발생시키고 트랜잭션을 글로벌 원장에 저장한다. 그리고 UAV(210)는 엔드 노드를 통해 자신의 설정 영역인 글로벌 그룹 내의 로컬 그룹에서 그룹키가 업데이트될 때 마다 트랜잭션을 생성할 수 있다.
- [0061] 글로벌 원장의 트랜잭션은 트랜잭션 발생시간, 트랜잭션을 발행한 UAV 아이디, 로컬 그룹을 그룹핑한 글로벌 그룹 아이디, IoT 그룹키 정보를 전달한 기지국(110)의 아이디, IoT 기기(120)의 이동 전 로컬 그룹의 기지국 아이디 및 변경된 그룹키 정보 중 적어도 하나 이상을 포함할 수 있다.
- [0062] 이때 IoT 기기(120)가 소속된 로컬 그룹이 변경되면, UAV(210)는 이동 전 로컬 그룹의 기지국(110)이 아닌 현재 로컬 그룹의 기지국(110)으로부터 이전 로컬 그룹의 기지국 아이디를 전달받을 수 있다.
- [0063] 이를 통해 엣지 노드는 동일한 UAV(210)에 변경된 그룹키 정보에 기초하여 해당 로컬 그룹들 간의 IoT 기기(120)의 이동성, 그리고 글로벌 그룹 내의 IoT 기기(120) 밀집도 중 적어도 하나를 판단할 수 있다.
- [0064] 그리고 엣지 노드는 이동성 및 밀집도 중 적어도 하나를 판단한 결과에 기초하여 로컬 그룹을 통합하거나 밀집도가 지역으로 UAV(210)가 이동하도록 제어할 수 있다.
- [0065] 이를 위해 엣지 노드는 동일한 UAV(210)에서 기설정된 시간 동안 발생한 트랜잭션들에 두 개의 특정 기지국 아이디가 설정 횟수 이상 포함되면, 특정 기지국 아이디 각각에 대응되는 특정 로컬 그룹들끼리 IoT 기기의 이동성이 높은 것으로 판단할 수 있다.
- [0066] 그리고 엣지 노드는, 두 개의 특정 로컬 그룹들 간에 이동성이 높은 것으로 판단되면, 특정 로컬 그룹들이 기설정된 시간 동안 하나의 그룹키를 공유하도록 할 수 있다. 여기서 기설정된 시간은 설정 시간 내에 두 로컬 그룹 간에 발생하는 IoT 기기(120)의 이동 횟수가 일정 횟수 이하로 떨어질 때까지의 시간을 의미할 수 있다.
- [0067] 또한 엣지 노드는 하나의 그룹키를 공유하는 두 개의 특정 로컬 그룹들에서 IoT 이동 비율이 설정된 비율 이하로 낮아지면 통합된 두 개의 특정 로컬 그룹들을 다시 분리하여 각각의 그룹키를 사용하도록 할 수 있다.
- [0068] 그리고 엣지 노드는 동일한 UAV에 변경된 그룹키 정보가 설정 시간 내 설정 횟수 이상 전달되는 경우, 해당 설정 영역의 IoT 기기 밀집도가 높은 것으로 판단할 수 있다.
- [0069] 엣지 노드는 IoT 기기(120)가 밀집되어 있는 것으로 판단한 경우, UAV 계층(200)의 UAV(210)들과 글로벌 원장을 공유하여 가장 적은 트랜잭션을 발생시키는 UAV(210)가 IoT 기기(120)가 밀집된 밀집 영역으로 이동하도록 제어할 수 있다.
- [0070] 그리고 IoT 기기(120)가 밀집된 영역으로 이동한 UAV(210)의 엣지 노드는 보조 게이트웨이 역할을 수행하여 해당 영역의 엣지 노드와 함께 데이터가 밀집된 영역의 트래픽을 완화시킨다.
- [0071] 또한, UAV(210)가 밀집 영역으로 이동하면, 이동한 UAV의 이전 위치와 가장 인접한 위치의 UAV(210)가 이동한 UAV(210)의 트랜잭션을 더 처리하게 된다.
- [0072] 이후 엣지 노드는 UAV(210)가 이동한 영역의 밀집도가 일정 수치 이하로 유지되면 이동한 UAV(210)가 초기의 설

정 영역으로 이동하도록 제어할 수 있다.

- [0073] 한편 클라우드 계층(300)은 최상위 계층으로서, 엔드 노드와 엣지 노드의 모든 데이터를 전달받아 저장하는 클라우드로 구성되며, 로컬 원장과 글로벌 원장을 이용하여 데이터의 흐름을 추적한다.
- [0075] 도 2는 도 1의 시스템에서 글로벌 원장과 로컬 원장의 트랜잭션 구성 요소를 예시적으로 도시한 도면,
- [0076] 도 2에 도시된 바와 같이, 글로벌 원장(Global ledger)의 트랜잭션(Transaction, Tx)은 트랜잭션 발생시간(TIME(Tx)), 트랜잭션을 생성한 UAV 아이디(UAV_{ID}), 트랜잭션을 생성한 UAV가 소속된 글로벌 그룹의 아이디(G_{ID} (상위그룹)), IoT 기기(120)의 이동 경로 상에서 이동 전 기지국 아이디(BS_{Source}) 및 목적지 기지국 아이디(BS_{ID(Destination)}), 그리고 로컬 그룹에서 업데이트되어 변경된 그룹키 정보(KEY_{Up_Info}) 중 적어도 하나 이상을 포함하여 발생된다.
- [0077] 한편 로컬 원장(Local ledger)의 트랜잭션(Transaction, Tx)은 트랜잭션 발생시간(TIME(Tx)), IoT 기기(120)의 이동 경로 상에서 목적지에 대응되는 기지국이면서 트랜잭션을 생성한 기지국 아이디(BS_{Destination}), 트랜잭션을 생성한 기지국이 소속된 로컬 그룹 아이디(G_{ID}(하위그룹)), 비정상적으로 동작한 IoT 기기의 아이디(Abnormal_IoT_{ID}), 로컬 그룹을 구성하는 IoT 기기 리스트(IoT_{List}), 그리고 IoT 기기(120)의 이동 경로 상에서의 이동 전 기지국 아이디(BS_{Source}) 중 적어도 하나 이상을 포함하여 발생된다.
- [0078] 따라서 엣지 노드는 IoT 기기(120)가 어디에서 어디로 이동하였는지에 대한 이동 경로(BS_{Destination} → BS_{Source})를 확인할 수 있다.
- [0079] 그리고 기지국(210)은 로컬 그룹 내의 IoT 기기(120)가 비정상적으로 동작하면 해당 IoT 기기(120)의 아이디가 포함되도록 트랜잭션을 생성하게 되므로, 이후 해당 비정상 IoT 기기(120)가 다른 로컬 그룹으로 이동하면 이동한 로컬 그룹에서 해당 IoT 기기(120)를 승인하지 않을 수 있게 된다.
- [0080] 본 발명의 실시 예에서는 계층 별로 블록체인 네트워크로 구성되기 때문에 같은 계층끼리는 원장을 공유하며, 본 발명의 시스템에서 UAV는 글로벌 체인에 그룹키가 업데이트되어 변경된 그룹키 정보만을 기록할 수 있으므로 상위 계층인 UAV 계층(200)에서는 하위 계층인 IoT 네트워크 계층(100)에 속해 있는 IoT 기기(120)의 정보를 알 수 없게 된다.
- [0081] 따라서 IoT 데이터 보안을 보장할 수 있고, 로컬 그룹의 그룹키가 노출되지 않으므로 키 도난에 대한 보안을 보장할 수 있는 것은 물론, UAV(210)는 이동성이 높고 하이재킹(Hijacking)에 취약하다는 점에서 야기될 수 있는 문제들을 해결할 수 있게 된다.
- [0082] 또한, IoT 네트워크 계층(100)에 구성된 로컬 그룹은 각 그룹 내 통신을 진행하기 때문에, 그룹 통신을 위한 그룹키를 공유하고 사용한다.
- [0083] 만약 로컬 그룹 내 IoT 기기(120)에 변화가 있을 경우, 보안을 위해 그룹키를 변경한다. 그룹키가 변경될 때마다 해당 기지국(110)은 그룹키가 변경되었다는 정보를 UAV(210)에게 전송한다.
- [0084] 이때, 글로벌 원장에는 변경된 그룹키 정보(KEY_{Up_Info})가 저장되므로 특정 로컬 그룹에서 그룹키 정보의 변경이 빈번할 경우, 그룹 내의 IoT 기기(120)의 이동성이 높은 것으로 판단할 수 있다. 또한, 로컬 원장에서 트랜잭션을 생성하는 주체는 IoT 기기(120)가 속한 로컬 그룹의 기지국(110)이기 때문에, 어느 하나의 기지국(110)에서 많은 트랜잭션이 발생한다면 해당 지역에 IoT 기기(120)가 밀집된 것으로 판단할 수 있다.
- [0086] 도 3은 도 1의 시스템에서 두 로컬 그룹 간의 이동성이 높아 두 로컬 그룹이 통합된 경우를 설명하기 위한 도면이다.
- [0087] 도 1에 나타난 바와 같이, 본 발명의 실시예에서는 각 계층의 원장을 확인하여 IoT 기기(120)의 이동성을 판단할 수 있다.
- [0088] 도 3을 예로 들어 설명하자면, 도 1에서와 같이 글로벌 그룹 A에 그룹핑된 복수의 로컬 그룹(A₁, A₂, A₃) 중에서 로컬 그룹 A₁과 A₂ 간에 IoT 기기(120)의 이동성이 높은 경우, 그룹키 업데이트에 대한 오버헤드가 증가

할 수밖에 없다.

- [0089] 이에 글로벌 그룹 A를 담당하는 UAV(210)의 엣지 노드는 로컬 그룹 A_1와 A_2를 물리적으로 통합하는 것이 아닌, 일시적으로 동일한 그룹키를 공유하도록 두 로컬 그룹(A_1, A_2)를 병합하여 그룹키 재입력 오버헤드를 감소시키도록 할 수 있다.
- [0091] 한편 도 4는 도 1의 시스템에서 밀집 구역 발생 시 UAV 이동을 설명하기 위한 도면이다.
- [0092] 본 발명의 실시예에서는 각 계층의 원장을 확인하여 IoT 기기(120)의 밀집도를 판단할 수 있다.
- [0093] 도 1 및 도 4를 예로 들어 설명하면, 만약 글로벌 그룹 D에 데이터가 밀집되어 있는 경우, 글로벌 그룹 D를 담당하는 UAV(210)의 엣지 노드는 공유되는 글로벌 원장을 통해 가장 적은 트랜잭션을 발생시키는 UAV(210, 글로벌 그룹 A의 UAV라 가정함)를 판단한다.
- [0094] 판단 결과에 따라 글로벌 그룹 D를 담당하는 UAV(210)는 Group A를 담당하는 UAV(210)에 요청 신호를 전달하여 글로벌 그룹 A를 담당하는 UAV(210)가 밀집 구역의 통신 완화를 위해 글로벌 그룹 D 영역으로 이동하도록 한다. 그리고 글로벌 그룹 D가 담당하는 로컬 그룹(D_1 내지 D_3)에서 발생하는 트랜잭션을 글로벌 그룹 A를 담당하는 UAV(210)의 엣지 노드와 글로벌 그룹 D를 담당하는 UAV(210)의 엣지 노드가 분담하여 처리한다.
- [0095] 또한, 글로벌 그룹 A가 담당하는 로컬 그룹(A_1 내지 A_3)에서 발생하는 트랜잭션은 글로벌 그룹 A를 담당하는 UAV(210)와 지리적으로 가장 가까운 위치를 담당하는 UAV(210, 글로벌 그룹 B의 UAV라 가정함)가 자신이 담당하는 로컬 그룹(B_1 내지 B_2)의 트랜잭션과 함께 이동된 UAV(210, 글로벌 그룹 A)가 복귀하기 전까지 일시적으로 트랜잭션을 처리한다.
- [0096] 즉, 데이터 밀집 구역이 발생했을 경우, 상대적으로 적은 트랜잭션이 발생하는 영역의 UAV(210)가 데이터 밀집 구역이 발생한 위치로 이동하여 보조 게이트웨이 역할을 수행하여 트래픽을 완화시킨다. 이때 이동된 UAV(210)이 원래 담당하던 그룹은 지리적으로 가까운 그룹을 담당하는 UAV(210)가 자신이 담당하던 그룹과 함께 이동된 UAV(210)가 복귀하기 전까지 일시적으로 트랜잭션을 처리한다.
- [0097] 또한 본 발명의 시스템에서는 이동성 및 밀집도 모두가 높은 것으로 판단되면, 로컬 그룹의 통합 및 UAV(210)의 이동이 함께 수행되도록 할 수도 있다.
- [0099] 한편, 도 5 내지 도 10은 본 발명의 실시예에 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 방법을 설명하기 위한 흐름도이다.
- [0100] 먼저 도 5는 본 발명의 실시예에 따른 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 방법의 동작 흐름을 도시한 순서도이고, 이를 참조하여 본 발명의 특정 로컬 그룹 간의 IoT 기기 이동성이 높은 경우의 구체적인 동작을 설명한다.
- [0101] 먼저 엣지 노드가 IoT 기기(120)의 데이터를 엣지 노드에 전달한다(S10).
- [0102] 이때 엣지 노드는 하나의 기지국(110)과 복수의 IoT 기기(120)들이 포함되는 로컬 그룹으로 구성하며, 복수의 로컬 그룹에 대응하도록 복수로 구성될 수 있다.
- [0103] 복수의 엣지 노드는 최하위에서 IoT 네트워크 계층(100)을 형성하고, IoT 네트워크 계층(100)은 동일한 UAV(210)에 그룹핑된 로컬 그룹의 기지국(110)들끼리 블록체인 네트워크로 구성되고, 각 기지국(110)들끼리 그룹 통신을 통해 각 기지국(110)에서 생성된 데이터를 저장한 로컬 원장을 공유한다.
- [0104] 데이터를 전달하는 단계(S10)에서 기지국(110)은 로컬 그룹 내 IoT 기기(120) 정보가 변할 때마다 트랜잭션(Transaction, TX)을 발생시키고 트랜잭션을 로컬 원장에 저장하고, 그룹 통신에 사용되는 그룹키를 변경하여 변경된 그룹키 정보를 엣지 노드를 통해 해당 UAV(210)에 전송할 수 있다.
- [0105] 그리고 본 발명의 데이터를 전달하는 단계(S10)에서는, IoT 기기(120)의 이동에 따라 IoT 기기(120)가 소속된 로컬 그룹이 변경되면, 이전 로컬 그룹 내 기지국(110) 및 현재 로컬 그룹 내 기지국(110) 중에서 현재 로컬 그룹 내 기지국(100)이 IoT 기기(120)의 이동 경로에 대한 정보를 현재 로컬 그룹을 그룹핑한 UAV(210)에 전송할 수 있다.

- [0106] 이는 트랜잭션의 중복을 방지하고, 하나의 트랜잭션에 IoT 기기(120)의 이동 경로를 기록하기 위함이다.
- [0107] 이후 UAV(210)가 구성하는 엣지 노드가 S10 단계에서 전달받은 데이터를 처리할 수 있다(S20).
- [0108] 이때, 엣지 노드는 복수의 로컬 그룹을 설정 영역으로 그룹핑하여 통신하는 UAV(210)가 구성하며, 복수의 UAV(210)에 대응하도록 복수로 구성된다.
- [0109] 복수의 엣지 노드는 UAV 계층(200)을 형성하고, 게이트웨이로서 데이터 전송을 수행하며, UAV 계층(200)은 복수의 UAV(210)들끼리 블록체인 네트워크로 구성되어 UAV(210)들끼리 각 UAV(210)에서 생성된 데이터를 저장한 글로벌 원장을 공유한다.
- [0110] 그리고 데이터를 처리하고 전달하는 단계(S20)에서 UAV(210)는 엔드 노드를 통해 자신의 설정 영역 내 기지국(110)에서 변경한 그룹키 정보를 전달받고, 전달받은 그룹키 정보를 이용하여 트랜잭션을 발생시키며, 트랜잭션을 글로벌 원장에 저장한다.
- [0111] 이러한 데이터를 처리하고 전달하는 단계(S20)는 엣지 노드가 그룹핑된 각 로컬 그룹 간의 IoT 기기 이동성 및 상기 설정 영역의 IoT 기기 밀집도 중 적어도 하나를 판단하고, 판단한 결과에 기초하여 상기 로컬 그룹을 통합하거나 UAV가 이동하도록 제어하는 단계를 포함할 수 있다. 이하에서는 이동성을 판단하는 경우를 기준으로 설명하기로 하며, 밀집도를 판단하는 경우에 대해서는 후술할 도 9에서 자세히 설명하기로 한다.
- [0112] 엣지 노드가 트랜잭션에 포함된 IoT 기기(120)의 이동 경로를 통해 IoT 기기(120)의 이동성을 판단한다(S30).
- [0113] 자세히는, 동일한 UAV(210)에서 기설정된 시간 동안 발생한 트랜잭션들에서 두 개의 특정 기지국 아이디가 설정 횟수 이상 포함되면, 특정 기지국 아이디 각각에 대응되는 특정 로컬 그룹들끼리 IoT 기기(120)의 이동성이 높은 것으로 판단할 수 있다.
- [0114] 그리고 특정 로컬 그룹들끼리 IoT 기기(120)의 이동성이 높은 것으로 판단되면, 특정 로컬 그룹들이 기설정된 시간 동안 하나의 그룹키를 공유하도록 할 수 있다(S40).
- [0115] 마지막으로 클라우드가 엔드 노드와 엣지 노드의 모든 데이터를 전달받아 저장하고, 데이터의 흐름을 추적한다(S80).
- [0116] 이때 클라우드는 최상위에서 클라우드 계층(30)을 형성한다.
- [0117] 즉, 클라우드 계층(30)은 로컬 원장과 글로벌 원장을 모두 가지고 있어 데이터의 흐름 추적이 필수인 모바일 IoT 환경에서 원활한 데이터 추적이 이루어지도록 하여 데이터 무결성을 보장할 수 있다.
- [0119] 한편 도 6은 본 발명의 시스템에서 그룹키를 관리하기 위한 그룹키 관리 메커니즘을 설명하기 위한 도면이고, 도 7 내지 도 8은 본 발명의 시스템에서 그룹키를 관리하는 동작을 설명하기 위한 도면이다. 구체적으로 도 7은 IoT 기기(120)가 로컬 그룹을 떠나는 경우에 그룹키를 변경하는 흐름도이고, 도 8은 IoT 기기(120)가 유입된 경우에 그룹키를 변경하는 흐름도이다.
- [0120] 본 발명에서 그룹키를 관리하는 그룹키 관리 메커니즘을 먼저 설명하기로 한다. 본 발명에서 사용하는 LKH(Logical Key Hierarchy) 구조는 트리 구조에 leaf node에 사용자가 위치하고, root node에 위치한 그룹키를 공유하는 방식이다. 그리고 그룹키인 GK(Group Key)를 효율적으로 업데이트하기 위해 키 암호화 키인 KEK(Key Encryption Key)를 사용할 수 있다. 그리고 각 노드는 $\log_2 n$ 개의 키를 저장하여 통신 오버 헤드를 낮출 수 있다.
- [0121] 구체적으로 도 6 (a)에 도시된 바와 같이 초기에 기지국(110)과 통신하는 IoT 기기(120)인 3개의 노드(N1, N2, N3)가 존재하는 상태에서 이후 도 6(b)처럼 새로운 노드인 N4가 추가되면, 기지국(110)은 새 노드 N4의 공유 비밀 키인 SSK(Shared Secret Key)를 얻고, 새 노드 N4의 루트로의 경로를 따라 그룹키인 GK(Group Key)와 키 암호화 키인 KEK(Key Encryption Key)를 업데이트하게 된다. 그리고 기지국(110)은 새 노드 N4의 SSK를 이용해 KEK를 암호화하여 새 노드 N4에게 전송할 수 있다. 이후 업데이트된 GK'는 KEK34로 암호화되어 새 노드 N4로 전송될 수 있고, 기존의 IoT 기기(120)인 노드 N1 내지 N3은 기지국(110)으로부터 GK'를 전달받지 않고, 해시 함수를 통해 그룹키를 업데이트하여 통신 및 계산 비용을 절감할 수 있게 된다.
- [0122] 한편 도 6의 (c)는 새 노드 N4를 추가한 후 N2가 로컬 그룹을 떠나는 경우로, N2가 로컬 그룹을 떠날 때 해시를 통해 그룹키를 변경하면 로컬 그룹을 떠난 N2도 변경된 그룹키를 알게 된다. 따라서 이 경우에는 그룹키는 해시

을 통해 그룹키를 업데이트하지 않고, 기지국이 GK"를 생성하여 KEK로 암호화한 후 기존의 IoT 기기(120)인 노드 N1, N2, N3에게 전송할 수 있다.

- [0124] 이상의 그룹키 관리 메커니즘에 기초하여 도 7을 참조하여 글로벌 그룹 A의 로컬 그룹(A₁)에 위치하던 IoT 기기(120)가 해당 로컬 그룹 A₁을 떠나는 경우를 설명하기로 한다.
- [0125] 먼저 기지국_{A-1}(110-A-1)은 현재 로컬 그룹 A₁에 위치하는 기존 IoT 기기_{A-1}(120-A-1)들에게 이동한 IoT 기기(120)의 정보를 전송한다(S110).
- [0126] 이후 기지국_{A-1}(110-A-1)은 KEK를 업데이트하여 KEK'를 생성한다(S120).
- [0127] 그리고나서 기지국_{A-1}(110-A-1)은 각 기존 IoT 기기_{A-1}(120-A-1)들의 SSK로 암호화된 KEK'를 현재 로컬 그룹 A-1에 위치하는 기존 IoT 기기_{A-1}(120-A-1)들에게 전송한다(S130).
- [0128] 이후 기지국_{A-1}(110-A-1)은 GK를 업데이트하여 GK'를 생성한다(S140).
- [0129] 그리고나서 기지국_{A-1}(110-A-1)은 KEK'로 암호화된 GK'를 현재 로컬 그룹 A-1에 위치하는 기존 IoT 기기_{A-1}(120-A-1)들에게 전송한다(S150).
- [0130] 이후 기지국_{A-1}(110-A-1)은 로컬 그룹(A₁)의 구성원 변경에 대한 트랜잭션을 생성하여 로컬 원장에 저장한다(S160).
- [0131] 그리고 기지국_{A-1}(110-A-1)은 변경된 그룹키 정보를 해당 UAV_A(210-A)로 전송한다(S170).
- [0132] 이후 해당 UAV_A(210-A)는 전달받은 변경된 그룹키 정보에 기초하여 트랜잭션을 생성하고 글로벌 원장에 저장한다(S180).
- [0134] 한편 도 8을 참조하여 본 발명의 실시예에서 글로벌 그룹 A의 로컬 그룹(A-1)에 신규 IoT 기기i(120-i)가 유입되는 경우를 가정하여 그룹키를 관리하는 흐름을 설명하기로 한다.
- [0135] 로컬 그룹(A-1)에 신규 IoT 기기i(120-i)가 유입되면, 먼저 신규 IoT 기기i(120-i)는 기지국_{A-1}(110-A-1)으로 본인 ID와 이동 전에 소속된 로컬 그룹의 아이디인 이전 로컬 그룹 ID를 전송한다(S210).
- [0136] 그러면 기지국_{A-1}(110-A-1)은 블록체인을 쿼리하여 신규 IoT 기기i(120-i)에 대한 정보를 확인한다(S215). 구체적으로 신규 IoT 기기i(120-i)의 아이디(IoT_{ID})와 이전 로컬 그룹 ID(preG_{ID})가 일치하는지를 확인할 수 있다.
- [0137] 이후 신규 IoT 기기i(120-i)가 이전 로컬 그룹에서 이동한 것으로 확인되면, 기지국_{A-1}(110-A-1)은 승인 메시지 및 SSK를 신규 IoT 기기i(120-i)로 전송한다(S220).
- [0138] 그리고 기지국_{A-1}(110-A-1)은 로컬 그룹 A-1에 현재 소속된 기존 IoT 기기_{A-1}(120-A-1)들에게 그룹키 변경 요청 메시지를 전송한다(S225).
- [0139] 이후 기지국_{A-1}(110-A-1)과 기존 IoT 기기_{A-1}(120-A-1)들은 해시 함수를 통해 그룹키인 GK를 업데이트하여 GK'를 생성한다(S230, S235).
- [0140] 그리고나서 기지국_{A-1}(110-A-1)은 그룹 통신에 필요한 그룹키로써 KEK로 암호화된 GK'를 신규 IoT 기기i(120-i)로 전송한다(S240).
- [0141] 또한 기지국_{A-1}(110-A-1)은 신규 IoT 기기i(120-i)의 SSK로 암호화된 KEK'를 신규 IoT 기기i(120-i)로 전송한다(S245).
- [0142] 이후 기지국_{A-1}(110-A-1)은 기존 IoT 기기_{A-1}(120-A-1)의 SSK로 암호화된 KEK' 또는 공유된 KEK로 암호화된 KDK'를 기존 IoT 기기(120-A-1)들에게 전송한다(S250).

- [0143] 이후 기지국_{A_1}(110-A-1)은 로컬 그룹(A₁)의 구성원 변경에 대한 트랜잭션을 생성하여 로컬 원장에 저장한다(S255).
- [0144] 그리고 기지국_{A_1}(110-A-1)은 변경된 그룹키 정보를 해당 UAV_A(210-A)로 전송한다(S260).
- [0145] 이후 해당 UAV_A(210-A)는 전달받은 변경된 그룹키 정보에 기초하여 트랜잭션을 생성하고 글로벌 원장에 저장한다(S265).
- [0146] 상술한 도 7 및 8을 통해 알 수 있듯이 본 발명에 따른 데이터 그룹 관리 방법에서는 IoT 기기(120)의 이동경로에 대한 정보는 이동한 IoT 기기(120)가 유입된 기지국(120)에서 UAV(210)로 전달함을 알 수 있다. 이를 통해 트랜잭션의 중복을 방지하고, 하나의 트랜잭션에 IoT 기기(120)의 이동 경로를 기록할 수 있다.
- [0148] 한편 도 9는 도 5에서 이동성이 높은 것으로 판단되어 특정된 두개의 로컬 그룹이 통합되는 경우에 그룹키를 변경하는 과정의 흐름도로써, 구체적으로 도 9를 참조하여 글로벌 그룹 A에 속한 로컬 그룹 중 A₁ 및 A₂ 간의 IoT 기기의 이동성이 높은 것으로 판단된 경우를 예시적 사항으로 설명하기로 한다.
- [0149] UAV_A(210-A)는 글로벌 원장을 통해 두 로컬 그룹(A₁ 및 A₂) 간의 IoT 기기(120)의 잦은 이동성을 확인하면, 그룹키가 자주 변경되는 두 로컬 그룹(A₁ 및 A₂)을 지정한다(S310).
- [0150] 이후 UAV_A(210-A)는 각각의 로컬 그룹 기지국인 기지국_{A_1}(110-A-1) 및 기지국_{A_2}(110-A-2)로 로컬 그룹 통합을 요청한다(S315).
- [0151] 그러면 통합 요청을 받은 두 로컬 그룹의 기지국(110-A-1, 110-A-2)은 각 로컬 그룹을 구성하는 IoT 기기(120)들에게 로컬 그룹 통합 요청을 공지한다(S325).
- [0152] 이후 UAV_A(210-A)가 두 로컬 그룹의 기지국(110-A-1, 110-A-2) 각각으로부터 통합을 수락하는 메시지를 수신한다(S330, S335).
- [0153] 이때 로컬 그룹에서 사고와 같은 이벤트가 발생하여 두 로컬 그룹의 기지국(110-A-1, 110-A-2) 모두로부터 사전에 설정된 시간 내에 통합을 수락하는 메시지를 수신하지 못하면 UAV_A(210-A)는 두 로컬 그룹(A₁, A₂)의 통합을 수행하지 않을 수 있다.
- [0154] 두 로컬 그룹의 기지국(110-A-1, 110-A-2) 각각으로부터 통합을 수락하는 메시지를 수신하면, UAV_A(210-A)는 동일한 그룹키 생성을 위한 시드 값(seed(x))과 그룹키 변경 요청을 두 로컬 그룹의 기지국(110-A-1, 110-A-2)으로 전달할 수 있다(S340). 구체적으로 seed(x)에서 x는 GK를 생성하기 위한 랜덤 시드값을 의미할 수 있다.
- [0155] 그리고나서 두 로컬 그룹의 기지국(110-A-1, 110-A-2)은 임시로 결합되어 시드 값(seed(x))을 통해 GK'를 생성하고 GK'를 업데이트할 수 있게 된다(S345).
- [0156] 이후 두 로컬 그룹의 기지국(110-A-1, 2)은 GK 변경에 기초하여 트랜잭션을 생성하여 로컬 원장에 저장할 수 있다(S355, S360).
- [0157] 그리고나서 해당 UAV_A(210-A)는 두 로컬 그룹(A-1, A-2)의 통합에 기초하여 트랜잭션을 생성하고 글로벌 원장에 저장할 수 있다(S365).
- [0158] 이후 도면에는 미도시되었으나, 두 로컬 그룹의 각 기지국(110-A-1, 110-A-2)은 일정 기간 동안 자신과 통신하는 IoT 기기 목록을 포함하는 트랜잭션을 생성하여 해당 UAV_A(210-A)로 전송할 수 있다.
- [0159] 그리고 두 로컬 그룹이 통합된 이후에 해당 UAV_A(210-A)는 통합된 두 로컬 그룹의 기지국(110-A-1, 110-A-2)이 통신하는 IoT 기기 목록에 기초하여 일정 변화율을 유지하면 두 로컬 그룹(A₁, A₂)이 분할되도록 할 수 있다.
- [0160] 두 로컬 그룹(A₁, A₂)이 분할되고 나면 각 기지국(110-A-1, 110-A-2)은 임의의 시드값을 생성하고 이를 기초로 GK를 재생성하게 된다.
- [0162] 한편 도 10은 본 발명의 실시예에 따른 도시 컴퓨팅 환경에서 계층적 블록체인에 기반한 데이터 그룹 관리 방법

의 동작 흐름을 도시한 순서도로써 보다 구체적으로는 IoT 기기 밀집도가 높은 영역이 발생한 경우에 수행되는 흐름도이다.

- [0163] 본 발명의 실시 예에 따르면, 먼저 엔드 노드가 IoT 기기(120)의 데이터를 엷지 노드에 전달한다(S10).
- [0164] 그 다음, UAV(210)가 구성하는 엷지 노드가 S10 단계에서 전달받은 데이터를 처리한다(S20).
- [0165] 그 다음, 엷지 노드가 설정 영역의 IoT 기기(120)의 밀집도를 판단한다(S50).
- [0166] 구체적으로 동일한 UAV에 로컬 원장의 트랜잭션을 발생시키는 기지국(110)으로부터 변경된 그룹키 정보가 설정 시간 내 설정 횟수 이상 전달되는 경우, 엷지 노드는 해당 로컬 그룹 내 IoT 기기(120)의 밀집도가 높은 것으로 판단하고(S50-예), 글로벌 원장을 공유하여 가장 적은 트랜잭션을 발생시키는 UAV(210)가 데이터가 IoT 기기(120)가 밀집한 밀집 지역으로 이동하도록 제어한다(S60).
- [0167] 그 다음, S60 단계의 제어에 따라 이동한 UAV(210)의 엷지 노드는 보조 게이트웨이 역할을 수행하여 해당 UAV(210)의 엷지 노드와 함께 밀집 지역의 트래픽을 완화시킨다(S50).
- [0168] 이때, UAV(210)가 밀집된 영역으로 이동하면 가장 인접한 위치의 UAV(210)가 이동한 UAV(210)의 트랜잭션을 더 처리할 수도 있다.
- [0169] 마지막으로 클라우드가 엔드 노드와 엷지 노드의 모든 데이터를 전달받아 저장하고, 데이터의 흐름을 추적한다(S80).

- [0171] 한편 도 11 내지 도 18은 도 1의 시스템의 효과를 설명하기 위한 실험 결과를 도시한 도면이다.
- [0172] 먼저 본 발명에 따른 시스템의 효과를 설명하기 위한 실험에서는 Ubuntu 20.04.2 LTS에서 Intel Core i7-10700 64비트 CPU@2.90GHz, 24GB RAM 및 200GB 하드 드라이브 공간이 장착된 가상 머신을 사용하였다. 그리고 도시 컴퓨팅에서의 그룹 관리 시뮬레이션을 위해 ns-3 버전 3.32를 사용하였다. 또한 그룹키 메커니즘의 계산 오버헤드를 평가하고 블록체인 시스템의 성능을 측정하기 위해 각각 Miracl 코어 라이브러리와 Hyperledger caliper 0.3의 오픈 소스 버전을 사용하였다.
- [0173] 이때 Miracl 코어는 암호화 및 해시 함수를 지원하며 아키텍처와 무관한 다국어 암호화 라이브러리고, Hyperledger caliper는 블록체인을 벤치마킹하여 성능을 측정하고 보고서 형식으로 결과를 제공할 수 있다.
- [0174] 본 발명에 따른 그룹 및 그룹키 관리의 효율성을 분석하기 위해 다음과 같은 시뮬레이터를 채택하였다. 먼저 그룹 관리의 효율성을 분석하기 위해 ns-3를 사용하여 통신 환경을 구축하였으며, 구체적인 환경 구성은 하기의 표와 같다.

- [0175] [표]

Simulation area	1000m x 1000m
Mobility model	Random waypoint
Loss model	Two ray ground propagation loss
Routing protocol	AODV
Number of nodes	10 ~ 200

- [0176]
- [0177] 그리고 노드 수를 늘려 시뮬레이션을 수행한 다음, miracl 코어 라이브러리를 사용하여 암호화 작업을 시뮬레이션하여 그룹키 계산 오버헤드를 분석하였다.
- [0178] 그 결과 64바이트 블록의 AES-256은 133.6 μ s, SHA-256은 103.8 μ s가 소요된 것을 확인하였다. 또한 Hyperledger Caliper를 사용하여 트랜잭션 생성 및 원장 조회 시간을 측정한 결과, 100개의 노드를 기준으로 트랜잭션 생성 시간은 13,000 μ s, 쿼리 시간은 200 μ s가 소요된 것을 확인하였다.
- [0179] AES-256을 사용하여 대칭 키 암호화를 수행하고 SHA-256을 사용하여 해시 함수를 수행하였다. 이러한 결과를 기반으로 그룹키를 변경하기 위한 계산 오버헤드를 계산하였다.
- [0180] 그리고 IoT 기기(120)인 노드의 이동성과 그룹의 밀집도를 고려하고, 이에 따라 그룹을 통합하거나 보조 게이트웨이를 추가하는 본 발명의 시스템을, 그룹으로만 통신하고 IoT 기기인 노드 이동성 또는 그룹 밀집도를 고려하

지 않는 종래의 기술과 비교하였다.

- [0181] 그리고 그룹 관리의 효율성을 분석하기 위해 그룹 밀집도에 대한 임계값을 설정하였다.
- [0182] 먼저 도 11은 각 글로벌 그룹의 밀집도에 따른 처리량(throughput)과 패킷 손실률을 나타낸 그래프이다.
- [0183] 도시된 바와 같이 글로벌 그룹의 밀집도가 높을수록 패킷 손실이 커지며, 최대 처리량은 글로벌 그룹 밀집도가 80일 때 발생하며 그 이후에는 처리량이 감소함을 알 수 있다. 이를 통해 글로벌 그룹의 노드 수가 증가할수록 더 많은 데이터가 생성되고 데이터를 처리할 리소스가 부족해짐을 알 수 있으며, 이에 기초하여 시뮬레이션에서 밀집도의 임계값을 80으로 설정하였다.
- [0184] 한편 도 12는 글로벌 그룹 내 노드 밀집도에 따른 패킷 손실을 나타낸 그래프이다.
- [0185] 그래프에 도시된 바와 같이 회색으로 표현된 종래 기술에서는 노드 밀집도가 80보다 높아짐에 따라 패킷 손실률이 급격히 증가하는 것을 알 수 있으나, 본 발명에 따른 시스템에서는 80의 밀집도를 기준으로 다른 글로벌 그룹의 UAV를 보조 게이트웨이로 배치하기 때문에 보조 게이트웨이가 더 많이 처리할수록 패킷 손실 비율이 감소하는 것을 알 수 있다.
- [0186] 그리고 도 13은 그룹의 밀집도에 따른 처리량을 나타낸 그래프로, 패킷 손실과 마찬가지로 처리량은 밀집도 90에서 감소하지만, 본 발명에서와 같이 다른 글로벌 그룹의 UAV를 보조 게이트웨이로 배치하여 보조 게이트웨이가 처리를 시작하면 처리량이 증가하는 것을 알 수 있다.
- [0187] 한편 도 14는 평균 E2E(End-to-End) 지연을 보여주는 그래프이다. E2E 지연은 패킷이 소스에서 목적지까지 네트워크를 통해 전송되는 시간입니다. 본 발명의 시스템은 밀집도가 높아지면 보조 게이트웨이를 통한 트래픽을 완화시키므로 E2E 지연도 감소하는 것을 알 수 있다.
- [0188] 그림 15는 E2E 지연의 지터(jitter)를 보여주는 그래프이다. 지터는 패킷이 네트워크를 통해 이동하는 지연의 급격한 변화를 나타내는 것이다. 구체적으로 패킷이 목적지에 도착할 때까지 지연이 얼마나 일정한지를 나타내는 편차를 보여줄 수 있는 것으로, E2E 지연이 짧더라도 변동이 심할 경우 시스템 성능 저하가 발생할 수 있다.
- [0189] 시뮬레이션 결과 종래 방식에서는 지터 값이 점차 증가하는 반면, 본 발명의 시스템에서는 다른 글로벌 그룹의 UAV를 보조 게이트웨이로 배치한 후 지터 값이 감소하는 것을 알 수 있다.
- [0191] 한편 도 16은 UTR(Useful Traffic Rate)을 보여주는 그래프이다.
- [0192] UTR은 네트워크 계층의 패킷 중 의미 있는 트래픽을 나타내는 성능 지표로써, 소스의 트래픽 간에 전송되는 데이터의 양을 나타내고, 값이 높을수록 성능이 좋음을 의미한다.
- [0193] 종래 방식에서는 그룹 밀집도가 증가함에 따라 유용한 트래픽 비율이 감소하는 반면, 본 발명의 시스템에서는 UTR이 감소했다가 UAV 이동에 따른 보조 게이트웨이 배치로 인해 손실 없이 더 많은 데이터를 처리함에 따라 다시 증가하는 것을 알 수 있다.
- [0195] 한편 도 17 및 도 18은 본 발명의 시스템에서 그룹키 업데이트 오버헤드를 줄이기 위해 이동성이 높은 IoT 기기(120)를 갖는 두 로컬 그룹을 일시적으로 결합한 경우의 효과를 설명하기 위한 도면이다.
- [0196] 시뮬레이션을 위해 두 개의 인접한 로컬 그룹 A_1 및 A_2와 각 로컬 그룹에 100개의 IoT 기기 즉 노드가 있다고 가정한다.
- [0197] 이때 해당 시뮬레이션에서는, IoT 기기(120)의 로컬 그룹 A_1 및 A_2 간의 이동만을 고려하였다. 즉 회원 탈퇴(membership withdrawal)는 고려하지 않았으며, 각각의 로컬 그룹 A_1 및 A_2와 로컬 그룹 A_1 및 A_2가 통합된 그룹에 대한 통신 및 계산 오버헤드를 비교하였다.
- [0198] 여러 KEK를 각 노드에 연결하여 통신 비용을 줄이는 그룹키 재입력에 LKH 구조를 사용하였으며, KEK에 대한 업데이트 통신에는 n 노드에 대한 $\log(n)$ 멀티캐스트가 필요하다.
- [0199] 도 17은 로컬 그룹 구성원 변경에 따른 통신 오버헤드를 나타낸 그래프이다.
- [0200] 도시된 바와 같이 로컬 그룹 구성원 변경이 증가함에 따라 개별 로컬 그룹에서는 많은 키 재입력 메시지가 발생

하게 되며, 로컬 그룹 A₂(분홍색 점선)가 로컬 그룹 A₁(검정색 점선)보다 오버헤드가 높은 이유는 이동 가정 때문이다.

- [0201] 이 가정에서 노드인 IoT 기기(120)는 로컬 그룹 A₂에서 로컬 그룹 A₁로 이동한다. 즉, IoT 기기(120)인 노드는 로컬 그룹 A₂를 떠나 로컬 그룹 A₁에 유입된다.
- [0202] 따라서 노드가 유입되는 로컬 그룹 A₁의 기지국(110)은 GK 재생성(rekeying) 메시지를 기존 구성원에게 브로드캐스트(broadcast)하고 키 정보를 유입된 노드에 유니 캐스트(unicast)한다.
- [0203] 한편 노드가 떠난 로컬 그룹 A₂의 기지국(110)은 KEK 재생성(rekeying)을 위해 기존 구성원에게 GK 재생성 메시지와 $\log(n)$ 을 기존 구성원에게 멀티 캐스트(multicast)한다.
- [0204] 따라서 로컬 그룹 A₂의 통신 오버헤드가 더 높게 된다. 하지만 두 로컬 그룹의 평균 오버헤드(파란색 실선)는 로컬 그룹 A₁의 오버헤드(검정색 점선)에 더 가깝다. 이는 노드가 많은 로컬 그룹 A₁은 키 재입력 메시지가 더 적기 때문이다.
- [0205] 로컬 그룹 통합(빨간색 실선)의 경우 UAV 간의 추가 통신이 필요하지만 추가적인 UAV 통신 오버헤드에도 불구하고 로컬 그룹을 통합하는 본 발명의 시스템은 그룹 멤버십 변경이 빈번한 경우 낮은 오버헤드를 갖는다.
- [0206] 연산 오버헤드를 위해 노드가 인접한 두 로컬 그룹 사이를 이동한 후에도 각 로컬 그룹의 평균 노드 수가 유지된다고 가정하였다. 이 가정은 각 로컬 그룹의 노드 수가 계산 오버헤드에 영향을 미치기 때문에 중요하다.
- [0207] 순방향 비밀성을 위한 그룹키 재입력은 역방향 비밀성을 위한 키 재입력이 계산을 줄이기 위해 해시 함수를 사용하기 때문에 역방향 비밀성을 위한 것보다 오버헤드가 더 높다.
- [0208] 또한 노드가 로컬 그룹에 가입할 때 블록체인 쿼리는 노드의 권한을 확인해야 한다.
- [0209] 마지막으로 그룹 통합에 대한 로컬 원장은 통합 트랜잭션을 저장해야 한다. 따라서 블록체인 쿼리 시간과 트랜잭션 생성 시간을 고려하였다.
- [0210] 도 18은 로컬 그룹 통합에 따른 계산 오버헤드를 보여주는 그래프이다.
- [0211] 도면에서와 같이 로컬 그룹 A₂(분홍색 점선)는 시뮬레이션에서 로컬 그룹 A₂ 노드 유입이 노드 유출보다 먼저 이루어지기 때문에 로컬 그룹 A₁(검정색 점선)보다 계산 오버헤드가 더 높다.
- [0212] 인접한 두 로컬 그룹(A-1, A-2)이 통합되면 새 그룹키가 생성되고 블록체인은 이 트랜잭션을 저장하게 된다. 통신 오버헤드와 유사하게 로컬 그룹의 구성원이 자주 변경될 때 계산 오버헤드가 훨씬 낮다.
- [0213] 시뮬레이션에서 통신 및 연산 오버헤드를 고려할 때 로컬 그룹 구성원 변경 수가 30개 이상일 때 로컬 그룹 통합이 효율적인 것을 알 수 있다.
- [0214] 따라서 로컬 그룹 통합 후 노드 이동 비율이 일정 시간 감소하면 더 나은 성능을 위해 로컬 그룹을 다시 분리해야 한다. 이에 본 발명의 시스템은 그룹 구성원 이동에 따른 적절한 그룹 결합 및 분리를 수행할 수 있다.
- [0215] 이와 같은 본 발명의 데이터 그룹 관리 방법은 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.
- [0216] 상기 컴퓨터 판독 가능한 기록 매체에 기록되는 프로그램 명령어는 본 발명을 위하여 특별히 설계되고 구성된 것들이거나와 컴퓨터 소프트웨어 분야의 당업자에게 공지되어 사용 가능한 것일 수도 있다.
- [0217] 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.
- [0218] 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.

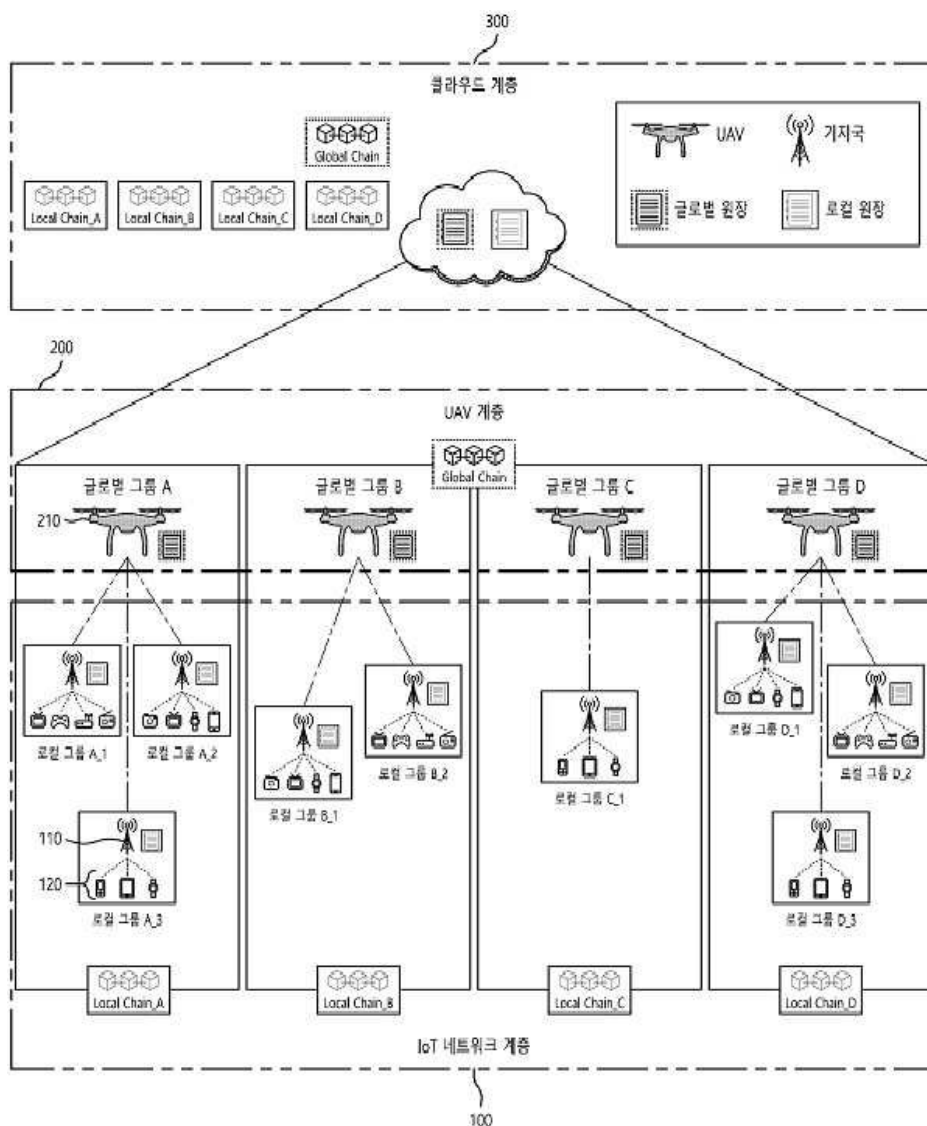
[0220] 이상에서는 본 발명의 다양한 실시예에 대하여 도시하고 설명하였지만, 본 발명은 상술한 특징의 실시예에 한정되지 아니하며, 청구범위에서 청구하는 본 발명의 요지를 벗어남이 없이 당해 발명이 속하는 기술분야에서 통상의 지식을 가진 자에 의해 다양한 변형실시가 가능한 것은 물론이고, 이러한 변형실시들은 본 발명의 기술적 사상이나 전망으로부터 개별적으로 이해되어져서는 안 될 것이다.

부호의 설명

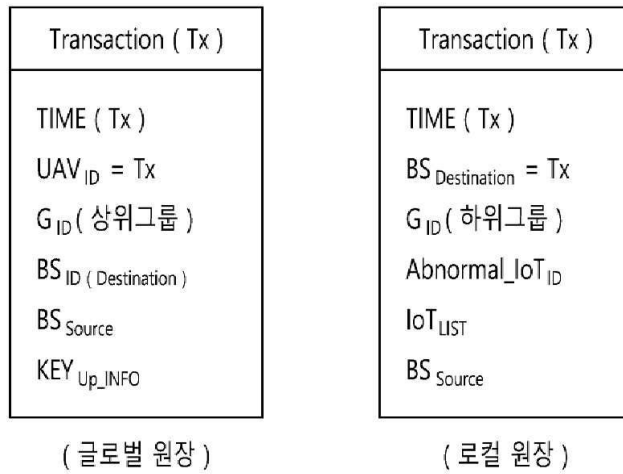
[0221] 100 : IoT 네트워크 계층 110 : 기지국
120 : IoT 기기 200 : UAV 계층
210 : UAV 300 : 클라우드 계층

도면

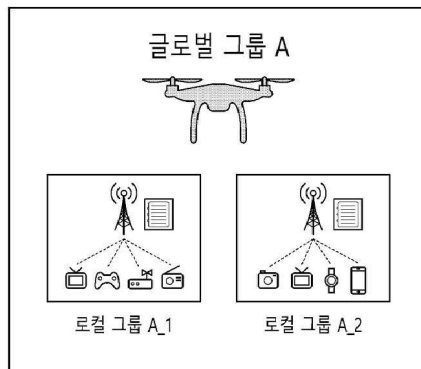
도면1



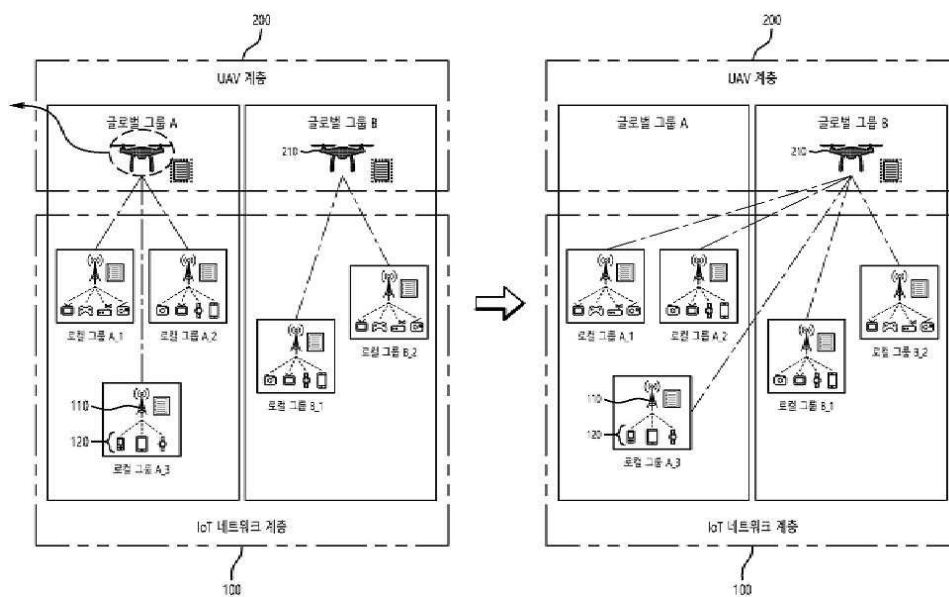
도면2



도면3

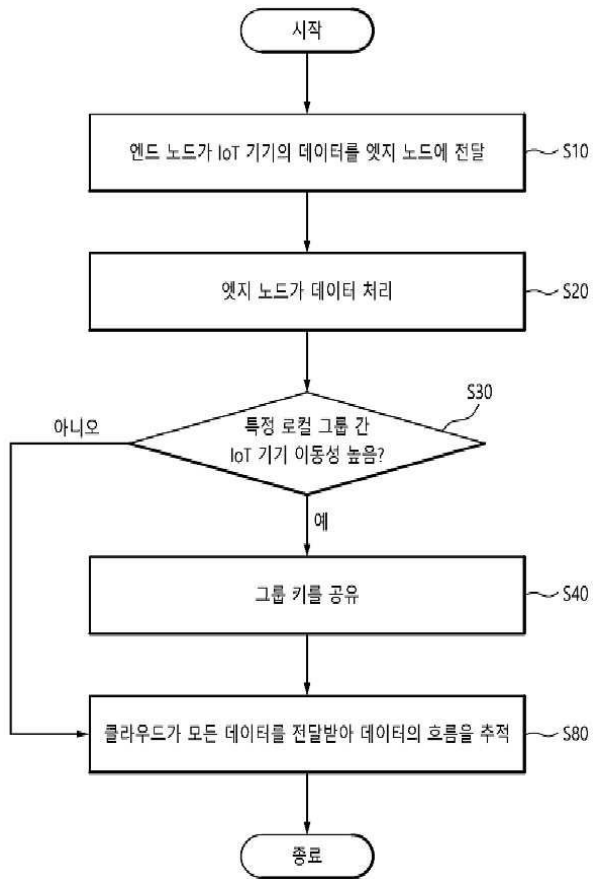


도면4

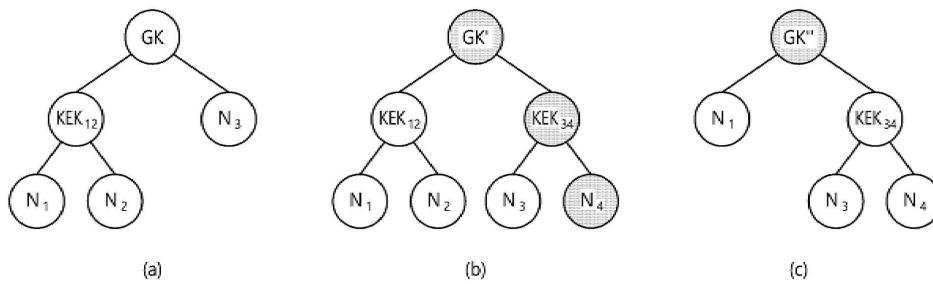


100

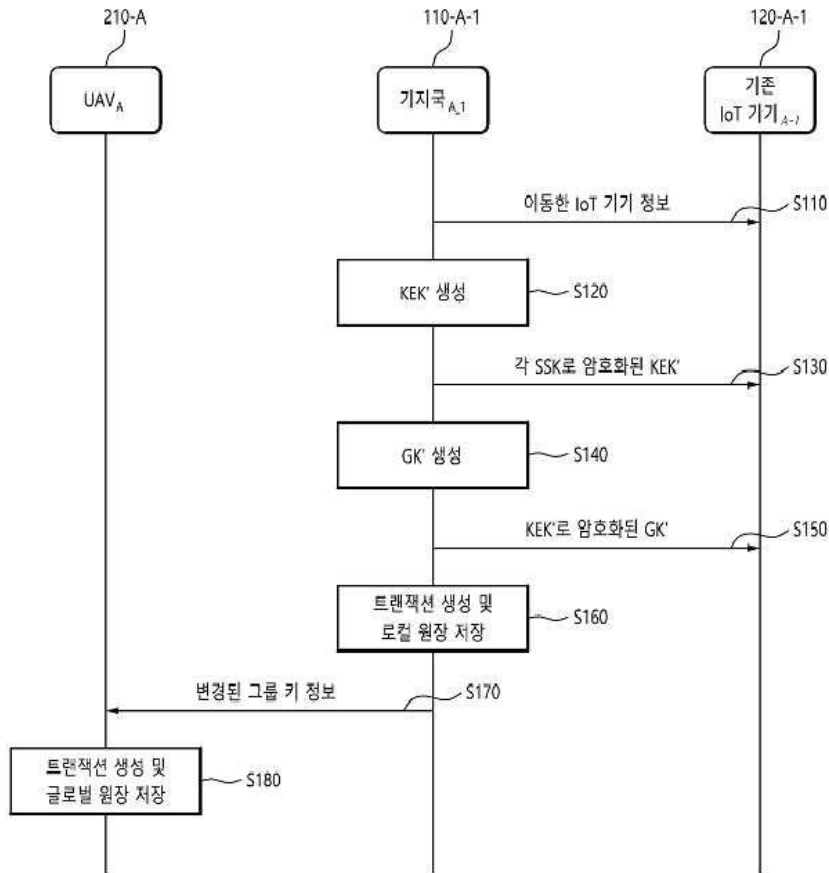
도면5



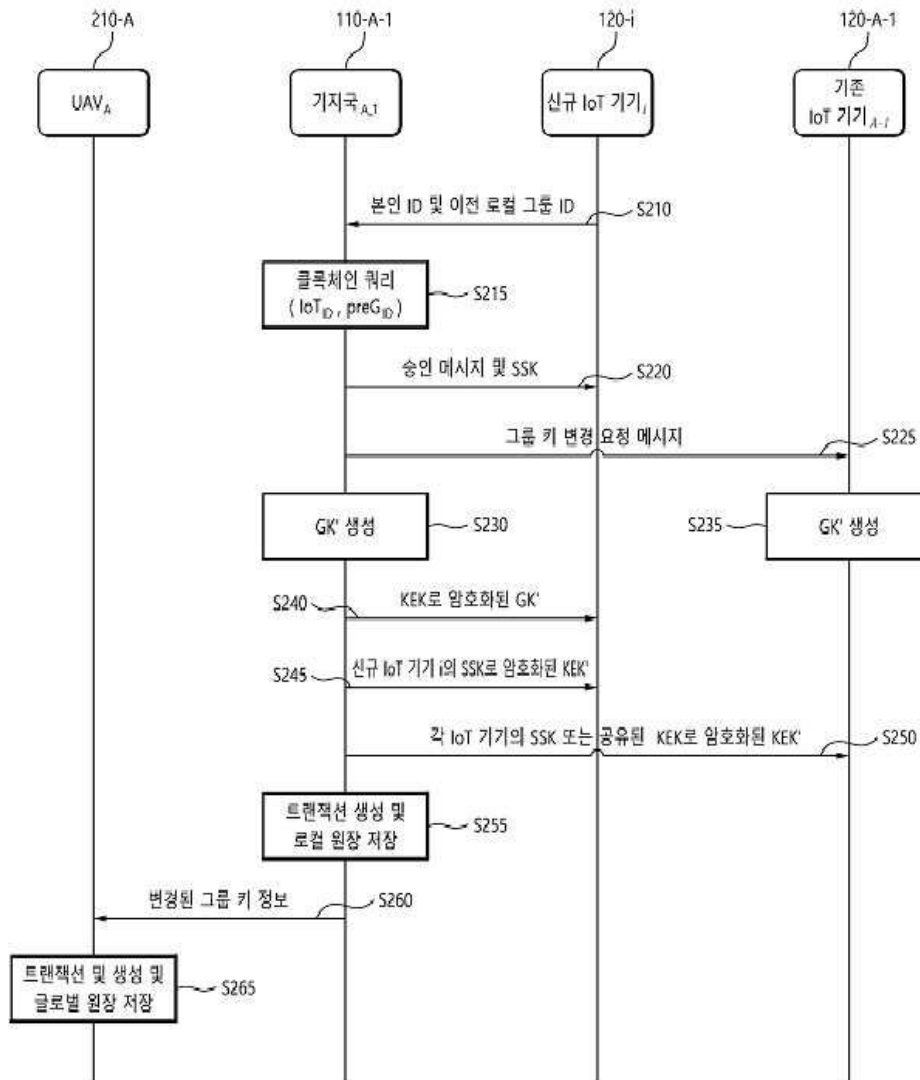
도면6



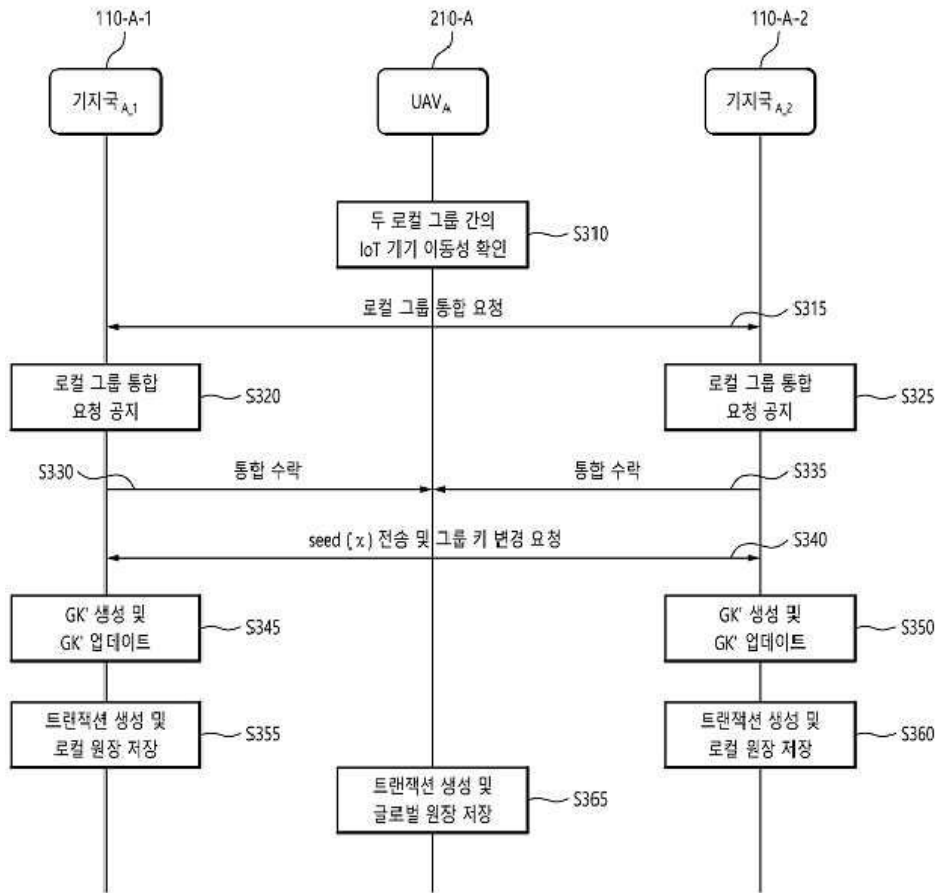
도면7



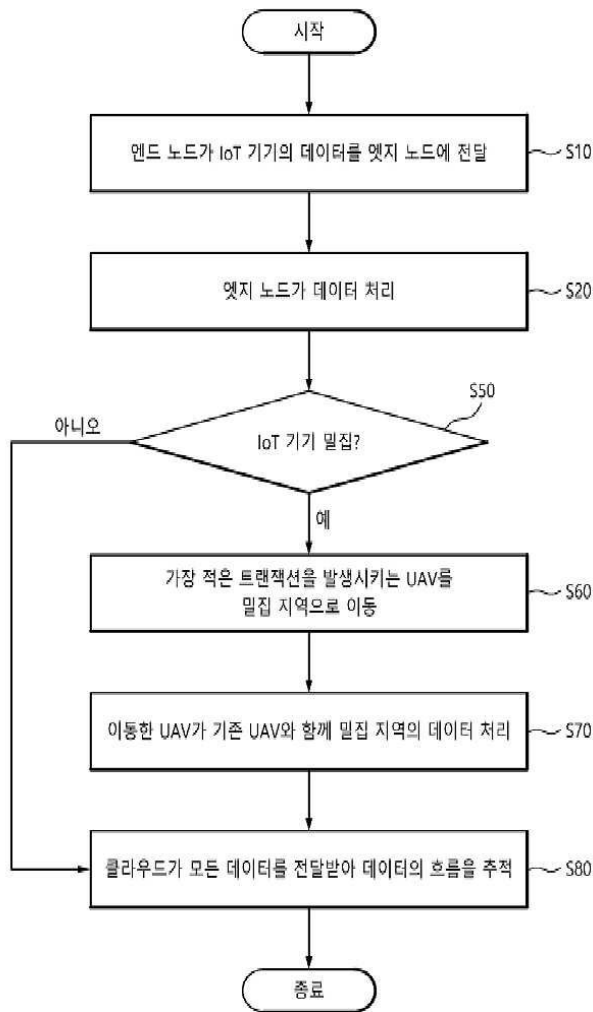
도면8



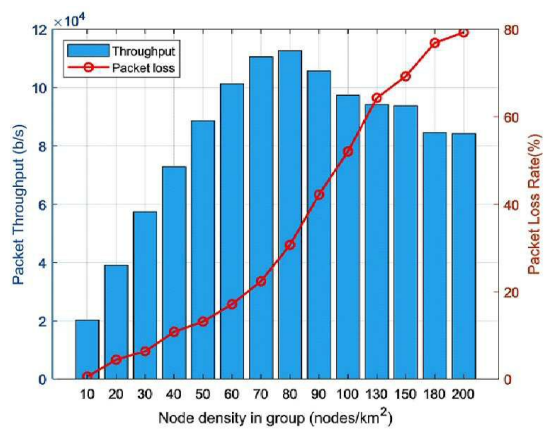
도면9



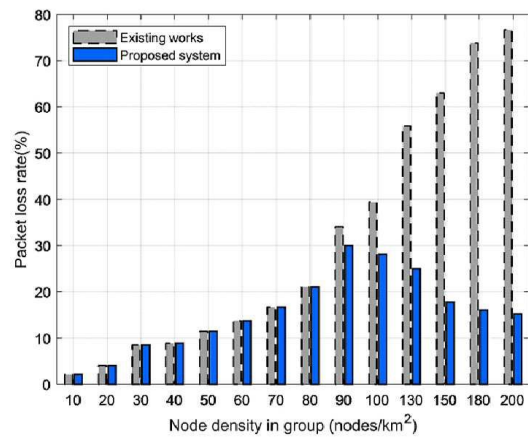
도면10



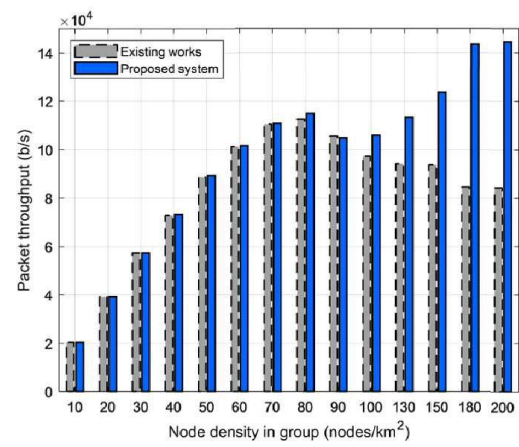
도면11



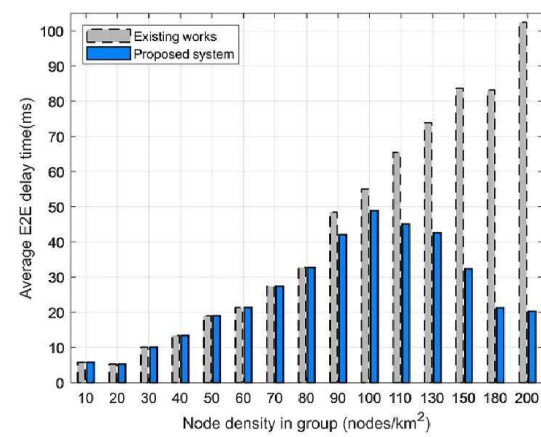
도면12



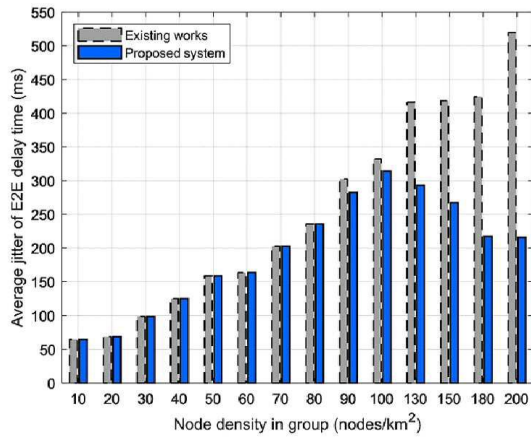
도면13



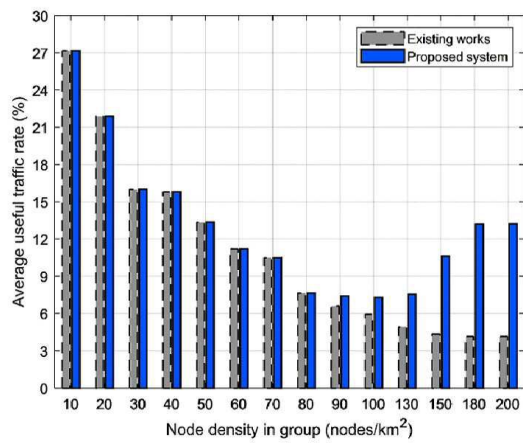
도면14



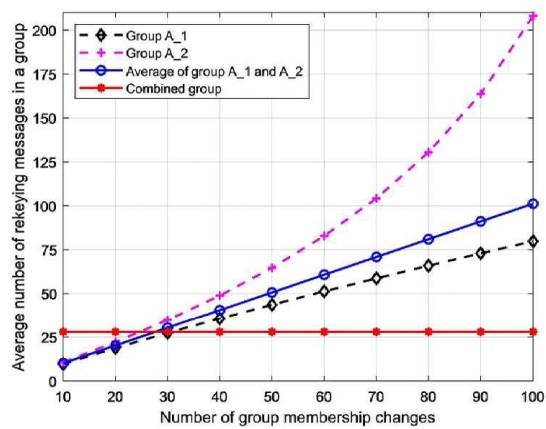
도면15



도면16



도면17



도면18

