



(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2023-0030302
(43) 공개일자 2023년03월06일

(51) 국제특허분류(Int. Cl.)

H04L 45/00 (2022.01) H04L 45/02 (2022.01)
H04L 9/06 (2006.01) H04W 40/10 (2009.01)
H04W 40/22 (2009.01) H04W 40/24 (2009.01)

(52) CPC특허분류

H04L 45/32 (2013.01)
H04L 45/08 (2022.05)

(21) 출원번호 10-2021-0112381

(22) 출원일자 2021년08월25일

심사청구일자 2021년08월25일

(71) 출원인

인천대학교 산학협력단

인천광역시 연수구 아카데미로 119 (송도동)

(72) 발명자

전광길

인천광역시 연수구 해송로 70, 209동 805호(송도동, 송도웹카운티2단지)

(74) 대리인

특허법인충정

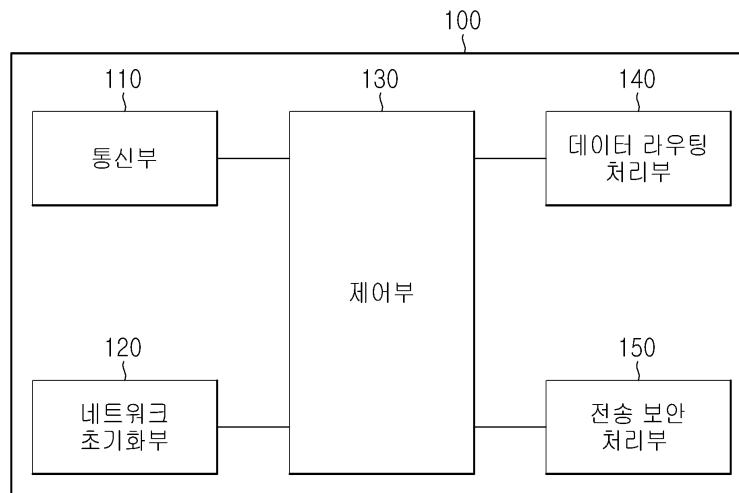
전체 청구항 수 : 총 7 항

(54) 발명의 명칭 빅데이터 기반 사물인터넷의 효율적 에너지 라우팅 제공 장치

(57) 요약

녹색 환경을 위한 빅데이터 기반 사물인터넷의 효율적 에너지 라우팅 제공 장치는 에너지와 트래픽 분석 요소를 고려하여 이웃 노드를 중계 노드로 설정하여 라우팅을 결정하고, 악성 개체로부터 빅데이터를 보호하고, 라우팅 경로의 트래픽 부하를 줄여 네트워크 안정성과 확장성을 확보할 수 있는 효과가 있다.

대표도 - 도2



(52) CPC특허분류

H04L 45/127 (2013.01)

H04L 45/26 (2013.01)

H04L 9/0637 (2013.01)

H04W 40/10 (2013.01)

H04W 40/22 (2013.01)

H04W 40/244 (2013.01)

명세서

청구범위

청구항 1

하나 이상의 이웃한 이웃 노드와 탐색 메시지, 요청 메시지, 데이터 패킷 및 제어 패킷을 송수신하는 통신부;

상기 이웃 노드로 정보 공유를 위한 요청 메시지를 전송하고, 상기 이웃 노드로부터 상기 요청 메시지에 대한 응답으로 제어 패킷을 수신하며, 상기 제어 패킷에 포함된 에너지 정보를 이용하여 랭크(Rank) 값을 계산하는 데이터 라우팅 처리부; 및

상기 계산한 랭크 값을 기초로 가장 높은 랭크 값을 갖는 이웃 노드를 중계 노드로 설정하여 라우팅을 결정하는 제어부를 포함하는 효율적 에너지 라우팅 제공 장치.

청구항 2

하나 이상의 이웃한 이웃 노드와 탐색 메시지, 요청 메시지, 데이터 패킷 및 제어 패킷을 송수신하는 통신부;

상기 이웃 노드로 정보 공유를 위한 요청 메시지를 전송하고, 상기 이웃 노드로부터 상기 요청 메시지에 대한 응답으로 제어 패킷을 수신하며, 상기 제어 패킷에 포함된 에너지 정보를 이용하여 랭크(Rank) 값을 계산하는 데이터 라우팅 처리부;

상기 에너지 정보, 트래픽 분석 요소 및 상기 계산한 랭크 값을 고려하여 상기 이웃 노드를 중계 노드로 설정하여 라우팅을 결정하는 제어부; 및

데이터 전송 전에 센서 데이터를 PCBC(Propagating Cipher Block Chaining)를 기반으로 암호화하여 전송하는 전송 보안 처리부를 포함하는 효율적 에너지 라우팅 제공 장치.

청구항 3

청구항 1 또는 청구항 2에 있어서,

상기 데이터 라우팅 처리부는 상기 랭크 값 $R(u, v)$ 을 잔여 에너지와 트래픽 분석 요인을 기반으로 하기의 수학식 1에 의해 업데이트하고, 상기 잔여 에너지를 하기의 수학식 2에 의해 계산하는 효율적 에너지 라우팅 제공 장치.

[수학식 1]

$$R(u, v) = \alpha * E + \beta * \left(\frac{1}{Tr_i} \right)$$

여기서, u 는 센서 노드, v 는 이웃 노드, α 와 β 는 기설정된 가중치, E 는 잔여 에너지, Tr_i 는 트래픽 분석용 특정 전송 링크를 나타냄.

[수학식 2]

$$E = \alpha - e_c / T_e$$

여기서, α 가 센서 노드 i 의 초기 에너지이고, e_c 가 소비된 에너지이고, T_e 는 네트워크 필드에서 모든 센서 노드에 대한 에너지 자원(Resource)의 합계임.

청구항 4

청구항 3에 있어서,

상기 데이터 라우팅 처리부는 소스 노드 i 에서 이웃 노드 j 까지의 트래픽 분석용 특정 전송 링크 $Tr_{i,j}$ 을 하기의 수학적 식 3에 의해 계산하고, 상기 계산된 트래픽 분석용 특정 전송 링크의 값이 높을수록 상기 소스 노드 i 에서 상기 이웃 노드 j 간의 데이터 라우팅에 가장 적합하다고 판단하는 효율적 에너지 라우팅 제공 장치.

[수학적 식 3]

$$Tr_{i,j} = t_L - t_F / T$$

여기서, t_F 는 첫 번째 비콘 메시지가 전송된 최초의 시간이라면, t_L 는 이웃 노드로부터 수신된 마지막 데이터 패킷, T 는 총 주기로 $t_F, t_{F+1}, t_{F+2}, \dots, t_L$ 임.

청구항 5

청구항 1 또는 청구항 2에 있어서,

상기 제어부는 상기 계산한 링크 값을 기초로 가장 높은 링크 값을 갖는 노드를 포워드(Forwarder) 목록으로 업데이트하는 효율적 에너지 라우팅 제공 장치.

청구항 6

청구항 1 또는 청구항 2에 있어서,

데이터 전송 전에 센서 데이터를 블록으로 분할하여 체인 형태의 데이터 암호화 함수 E 을 수행하고, 이전 평문 (일반 텍스트) 블록과 이전 암호문 블록을 XOR 연산하며, 센서 노드 i 에 대한 메시지 블록 mb_i 을 하기의 수학적 식 4와 수학적 식 5를 사용하여 PCBC(Propagating Cipher Block Chaining)를 기반으로 하는 각각의 암호 블록 cb_i 으로 변환하는 전송 보안 처리부를 더 포함하는 효율적 에너지 라우팅 제공 장치.

[수학적 식 4]

$$Cb_i = E_k(mb_i \oplus mb_{i-1} \oplus cb_{i-1}), mb_0 \oplus Cb_0 = IV$$

[수학적 식 5]

$$mb_i = D_k(Cb_i) \oplus mb_{i-1} \oplus cb_{i-1}), mb_0 \oplus Cb_0 = IV$$

여기서, E_k 는 대칭키 k 를 이용한 암호화 함수이고, D_k 는 동일한 키 k 를 이용한 복호화 함수이고, cb_{i-1} 은 이전 블록인 mb_{i-1} 의 암호 블록임.

청구항 7

청구항 1 또는 청구항 2에 있어서,

센서 노드 간의 링크(경로)를 연결한 그래프 $G(V, E)$ - V 를 상기 센서 노드이고, E 는 노드 간의 연결임 - 로 구성하는 네트워크 초기화부를 더 포함하는 효율적 에너지 라우팅 제공 장치.

발명의 설명

기술 분야

본 발명은 라우팅 제공 장치에 관한 것으로서, 더욱 상세하게는 에너지와 트래픽 분석 요소를 고려하여 이웃 노

드를 중계 노드로 설정하여 라우팅을 결정하는 녹색 환경을 위한 빅데이터 기반 사물인터넷의 효율적 에너지 라우팅 제공 장치에 관한 것이다.

배경 기술

- [0002] 최근 인터넷에 연결된 사물이 사람의 개입 없이 스스로 정보를 생성하고 다른 사물, 사람, 시스템과 연동하여 동작하는 사물인터넷(IoT: Internet of Things) 기술이 주목을 받고 있다. 2020년에 인터넷에 연결되는 사물의 수는 약 260억 개까지 증가할 것으로 전망된다.
- [0003] 사물인터넷에서 생산되는 데이터는 소량의 데이터와 멀티미디어 콘텐츠처럼 수십 또는 수백 메가바이트 수준의 대용량 데이터가 공존할 것이며, 향후에도 다양한 멀티미디어 콘텐츠들이 생산, 소비되겠지만 사물인터넷에서는 센싱 데이터 중심의 가벼운 연결이 기하급수적으로 증가하면서 대용량의 데이터 트래픽을 뛰어 넘는 환경이 될 것으로 예상된다.
- [0004] 무선 센서 네트워크(WSN)는 유연하고 비용 효율적인 솔루션으로 인해 의료, 군사, 추적, 차량 시스템 및 스마트 시티 영역에서 많은 인기를 얻었다. 배터리로 구동되는 초소형 센서 노드는 환경 데이터를 수집하기 위해 관찰 영역에 배치되고 나중에 센서의 데이터가 애플리케이션 사용자에게 전송된다.
- [0005] 기지국(BS)은 최종 사용자를 위한 게이트웨이로 취급되며, 모든 센서 데이터는 인터넷을 통해 라우팅된다. 애플리케이션 사용자는 요구 사항에 따라 센서 데이터에 대한 사후 분석 기능을 추가로 수행한다.
- [0006] 사물 인터넷(IoT)은 무선 센서와 통합하여 정보 수집 및 전달과 관련하여 커뮤니티에 서비스를 제공한다. 그러나 이러한 무선 센서의 제한된 제어는 제한된 에너지 관리, 데이터 저장 및 계산 능력으로 인해 상당한 연구 어려움을 야기한다.
- [0007] 대부분의 애플리케이션은 드론과 비행기를 이용하여 무작위로 노드를 분산시키고, 방대한 양의 데이터를 수집하기 위해 멀티홉 통신을 통해 서로 상호 작용한다. 그러나 네트워크 크기가 증가하면 센서 노드의 제한된 권한으로 인해 센서 노드가 환경 데이터를 보다 정확하고 효율적으로 처리하기가 매우 어렵게 된다.

선행기술문헌

특허문헌

- [0008] (특허문헌 0001) 한국 등록특허번호 제10-2054715호

발명의 내용

해결하려는 과제

- [0009] 이와 같은 문제점을 해결하기 위하여, 본 발명은 에너지와 트래픽 분석 요소를 고려하여 이웃 노드를 중계 노드로 설정하여 라우팅을 결정하는 녹색 환경을 위한 빅데이터 기반 사물인터넷의 효율적 에너지 라우팅 제공 장치를 제공하는데 그 목적이 있다.

과제의 해결 수단

- [0010] 상기 목적을 달성하기 위한 본 발명의 특징에 따른 효율적 에너지 라우팅 제공 장치는,
- [0011] 하나 이상의 이웃한 이웃 노드와 탐색 메시지, 요청 메시지, 데이터 패킷 및 제어 패킷을 송수신하는 통신부;
- [0012] 상기 이웃 노드로 정보 공유를 위한 요청 메시지를 전송하고, 상기 이웃 노드로부터 상기 요청 메시지에 대한 응답으로 제어 패킷을 수신하며, 상기 제어 패킷에 포함된 에너지 정보를 이용하여 랭크(Rank) 값을 계산하는 데이터 라우팅 처리부; 및
- [0013] 상기 계산한 랭크 값을 기초로 가장 높은 랭크 값을 갖는 이웃 노드를 중계 노드로 설정하여 라우팅을 결정하는 제어부를 포함한다.

- [0015] 본 발명의 특징에 따른 효율적 에너지 라우팅 제공 장치는,
- [0016] 하나 이상의 이웃한 이웃 노드와 탐색 메시지, 요청 메시지, 데이터 패킷 및 제어 패킷을 송수신하는 통신부;
- [0017] 상기 이웃 노드로 정보 공유를 위한 요청 메시지를 전송하고, 상기 이웃 노드로부터 상기 요청 메시지에 대한 응답으로 제어 패킷을 수신하며, 상기 제어 패킷에 포함된 에너지 정보를 이용하여 랭크(Rank) 값을 계산하는 데이터 라우팅 처리부;
- [0018] 상기 에너지 정보, 트래픽 분석 요소 및 상기 계산한 랭크 값을 고려하여 상기 이웃 노드를 중계 노드로 설정하여 라우팅을 결정하는 제어부; 및
- [0019] 데이터 전송 전에 센서 데이터를 PCBC(Propagating Cipher Block Chaining)를 기반으로 암호화하여 전송하는 전송 보안 처리부를 포함한다.

발명의 효과

- [0020] 전술한 구성에 의하여, 본 발명은 악성 개체로부터 빅데이터를 보호하고, 라우팅 경로의 트래픽 부하를 줄여 네트워크 안정성과 확장성을 확보할 수 있는 효과가 있다.
- [0021] 본 발명은 센서 노드 간의 에너지 및 트래픽 부하의 균형을 유지하여 최적의 데이터 라우팅을 통해 에너지 효율성을 향상시키는 효과가 있다.

도면의 간단한 설명

- [0022] 도 1은 본 발명의 실시예에 따른 무선 센서 네트워크의 노드의 구조를 간략하게 나타낸 도면이다.
- 도 2는 본 발명의 실시예에 따른 빅데이터 기반 사물인터넷의 효율적 에너지 라우팅 제공 장치의 구성을 나타낸 도면이다.
- 도 3은 본 발명의 실시예에 따른 에너지 소비에 대한 기존 작업에 대한 EBDS 프레임워크의 성능을 나타낸 도면이다.
- 도 4는 본 발명의 실시예에 따른 다양한 데이터 전송 속도에서 패킷 드롭 비율에 대한 다른 작업과 함께 EBDS 프레임워크의 성능을 나타낸 도면이다.
- 도 5는 본 발명의 실시예에 따른 종단 간 지연 및 다양한 데이터 전송 속도를 나타낸 도면이다.
- 도 6은 본 발명의 실시예에 따른 네트워크 처리량 및 다양한 데이터 전송 속도를 나타낸 도면이다.
- 도 7은 본 발명의 실시예에 따른 경로 안정성 및 다양한 데이터 전송 속도를 나타낸 도면이다.

발명을 실시하기 위한 구체적인 내용

- [0023] 명세서 전체에서, 어떤 부분이 어떤 구성요소를 "포함"한다고 할 때, 이는 특별히 반대되는 기재가 없는 한 다른 구성요소를 제외하는 것이 아니라 다른 구성요소를 더 포함할 수 있는 것을 의미한다.
- [0024] 도 1은 본 발명의 실시예에 따른 무선 센서 네트워크의 노드의 구조를 간략하게 나타낸 도면이고, 도 2는 본 발명의 실시예에 따른 빅데이터 기반 사물인터넷의 효율적 에너지 라우팅 제공 장치의 구성을 나타낸 도면이다.
- [0025] 본 발명의 실시예에 따른 노드(10, 20, 30, 40, 50, 60)는 통신부(110), 네트워크 초기화부(120), 제어부(130), 데이터 라우팅 처리부(140) 및 전송 보안 처리부(150)를 포함한다.
- [0026] 노드(10, 20, 30, 40, 50, 60)는 센서(sensor), 서버(server) 또는 엔진(engine) 형태일 수 있으며, 스마트폰(smartphone), 디바이스(device), 기구(apparatus), 단말 terminal), UE(user equipment), MS(mobile station), 무선기기(wireless device), 휴대기기(handheld device) 등 다른 용어로 불릴 수 있다.
- [0027] 또한, 노드(10, 20, 30, 40, 50, 60)는 에너지 효율적인 빅데이터 기반의 라우팅 제공 장치(100)로 불릴 수도 있다.
- [0028] 통신부(110)는 하나 이상의 이웃한 이웃 노드와 탐색 메시지, 요청 메시지, 데이터 패킷 및 제어 패킷을 송수신한다.
- [0029] 네트워크 초기화부(120)는 그리디(Greedy) 방법을 이용하여 복수의 센서 노드를 연결한 그래프를 구성한다. 그

래프 이론은 꼭짓점(Vertex)과 노드, 포인트로 구성되고, 이들을 에지(Edge) 즉, 선으로 연결된다. 다시 말해, 그래프 이론은 꼭짓점(센서 노드)과 2개의 꼭짓점의 연결하는 에지로 구성된다.

- [0030] 네트워크 초기화부(120)는 센서 노드 간의 링크(경로)를 연결한 그래프 $G(V, E)$ 를 구성한다. 센서 노드는 V 로 표시되고, E 는 노드 간의 연결을 나타내는 에지 세트를 나타낸다.
- [0031] 에지 $e \in E$ 와 관련된 순서 없는 쌍(u, v)이다. 여기서, 센서 노드 u , $v \in V$ 이다.
- [0032] 에지(u, v)는 센서 노드 u 에서 인접한 이웃 노드 v 와 직접 연결되는 것을 나타낸다.
- [0033] 경로 p 에서 에지들의 개수는 전체 길이를 나타낸다.
- [0034] 각각의 센서 노드는 가중치(Cost)를 측정할 수 있으며, 라우팅 테이블을 생성할 수 있다. 라우팅 테이블은 주어진 서브넷의 모든 센서 노드에 대한 정보를 포함한다.
- [0035] 라우팅 테이블은 센서 노드까지의 거리와 해당 센서 노드로 가기 위한 값을 저장한다.
- [0036] 각각의 센서 노드는 라우팅 테이블을 생성하여 인접한 이웃 노드로 전송한다.
- [0037] 또한, 각각의 센서 노드는 잔류 에너지와, 네트워크 필드에서의 위치와 같은 파라미터에 대한 정보를 이웃 노드로 전송한다.
- [0038] 각각의 센서 노드는 주변의 센서 노드들을 탐색하고, 연결된 센서 노드의 주소를 알아내고, 연결된 에지의 가중치(Cost)를 측정할 수 있다.
- [0039] 각각의 센서 노드는 가중치와 연결된 센서 노드들에 대한 정보를 담은 패킷을 생성하여 다른 센서 노드로 전송한다.
- [0040] 따라서, 센서 노드들은 라우팅 테이블에 이웃 노드에 대한 정보를 저장한다.
- [0041] 데이터 라우팅 처리부(140)는 이웃 노드로 정보 공유를 위한 요청 메시지를 전송하고, 이웃 노드로부터 요청 메시지에 대한 응답으로 제어 패킷을 수신하며, 제어 패킷에 포함된 에너지 정보를 이용하여 랭크(Rank) 값을 계산한다.
- [0042] 제어부(130)는 계산한 랭크 값을 기초로 가장 높은 랭크 값을 갖는 이웃 노드를 중계 노드로 설정하여 라우팅을 결정한다.
- [0043] 제어부(130)는 에너지 정보, 트래픽 분석 요소 및 계산한 랭크 값을 고려하여 이웃 노드를 중계 노드로 설정하여 라우팅을 결정한다.
- [0044] 데이터 라우팅 처리부(140)는 초기에 센서 노드 쌍(u, v) 간의 유클리드 거리를 기준으로 각 에지에 임시 랭크 값이 주어진다.
- [0045] 데이터 라우팅 처리부(140)는 랭크 값 $R(u, v)$ 을 잔여 에너지와 트래픽 분석 요인을 기반으로 수학적 식 1에 의해 업데이트한다. 랭크 값(Rank Value)이 가장 높은 정점은 두 개의 센서 노드 간에 강한 연관성이 있음을 나타낸다. 즉, 랭크 값은 센서 노드 간의 연관성을 나타낸다.

수학적 식 1

$$R(u, v) = \alpha * E + \beta * \left(\frac{1}{Tr_i} \right)$$

[0046]

[0047] 수학적 식 1에서 가중치 α 와 β 는 최적의 라우팅 결정에 중요한 역할을 한다.

[0048] 데이터 라우팅 처리부(140)는 $\alpha + \beta = 1$ 과 같은 에너지 및 트래픽 분석 요인에 대해 동일한 영향을 제공한다.

[0049] 데이터 라우팅 처리부(140)는 α 가 센서 노드 i 의 초기 에너지이고, e_c 가 소비된 에너지이고, 잔여 에너지 E 를 수학적 식 2와 같이 계산할 수 있다.

수학적 식 2

$$E = \alpha - e_c / T_e$$

[0051] 여기서, T_e 는 네트워크 필드에서 모든 센서 노드에 대한 에너지 자원(Resource)의 합계이다

[0052] 본 발명의 라우팅 알고리즘은 소스 노드에서 이웃 노드로의 트래픽 분석을 결정하기 위해서 RTD(Round Time Delay) 시간을 사용한다.

[0053] 소스 노드는 RTD 계산을 시작하기 위해서 고정된 시간 간격(Δt)에서 비콘 메시지를 플러딩한다(다른 노드로 보내는 트래픽 전달). 여기서, 플러딩은 네트워크에서 수정된 라우팅 정보를 모든 노드에 빠르게 전달하는 기능을 의미한다.

[0054] t_F 는 첫 번째 비콘 메시지가 전송된 최초의 시간이라면, t_L 는 이웃 노드로부터 수신된 마지막 데이터 패킷을 의미한다.

[0055] T는 총 주기로서 $T = t_F, t_{F+1}, t_{F+2}, \dots, t_L$ 이다.

[0056] 데이터 라우팅 처리부(140)는 소스 노드 i 에서 이웃 노드 j 까지의 트래픽 분석용 특정 전송 링크 $Tr_{i,j}$ 를 수학적 식 3과 같이 계산한다.

수학적 식 3

$$Tr_{i,j} = t_L - t_F / T$$

[0058] 데이터 라우팅 처리부(140)는 계산된 트래픽 분석의 값이 높을수록 소스 노드 i 에서 이웃 노드 j 간의 데이터 링크가 덜 혼잡하고, 데이터 라우팅에 가장 적합함을 판단한다.

[0059] 각각의 센서 노드의 데이터 라우팅 처리부(140)는 모든 예지들에 대한 랭크 값(Rank Value)을 계산한다.

[0060] 제어부(130)는 정보 공유를 위해서 요청 메시지를 생성하여 이웃 노드로 전송한다.

[0061] 따라서, 데이터 라우팅 처리부(140)는 이웃 노드로부터 제어 패킷을 수신하여 랭크 값을 계산한다.

[0062] 소스 노드 S_1 의 제어부(130)는 데이터 전송을 시작하기 위해서 포워더(Forwarder) 목록 F_L 을 설정하고, 처음에는 F_L 이 S_1 만으로 구성된다.

[0063] 그 후, S_1 의 제어부(130)는 라우팅 테이블에서 이웃 노드에 대한 계산된 랭크 값을 결정하고, 가장 높은 랭크 값이 속한 노드를 F_L 에 배치한다.

[0064] 따라서, 제어부(130)는 다음의 소스 노드에 대하여 각 이웃 노드의 랭크 값을 비교하고, 가장 높은 랭크 값을

기준으로 F_L 을 업데이트한다.

- [0065] 이러한 절차는 센서들의 데이터가 기지국에 도달할 때까지 가장 높은 랭크 값을 사용하여 최적의 중계 노드를 선택하기 위한 가중 에지의 식별로 계속된다.
- [0066] 또한, 임의의 중계 노드가 임계값보다 높은 에너지 자원을 소비할 때마다 본 발명의 라우팅 알고리즘은 랭크 값을 사용하여 다음 적절한 중계 노드로 센서의 데이터 및 소스 노드 유니캐스트 및 메시지를 전달하는 선택된 중계 노드를 제외합니다.
- [0067] 또한, 본 발명의 라우팅 알고리즘은 중계 노드가 임계값보다 높은 에너지 자원을 소비할 때마다 랭크 값을 사용한 중계 노드의 메시지 전송과 소스 노드 유니캐스트와, 센서 노드의 데이터 전송을 선택된 중계 노드에서 제외한다.
- [0068] 전술한 제어부(130), 데이터 라우팅 처리부(140)는 다익스트라(Dijkstra) 알고리즘을 기반으로 최적화된 라우팅 결정을 통해 효율적인 라우팅 경로를 제공한다(수학식 1, 수학식 2, 수학식 3).
- [0070] 본 발명의 보안 데이터 전송 알고리즘은 잠재적인 위협으로부터 빅데이터를 보호하고, 데이터 기밀성과 인증을 유지한다.
- [0071] 보안 데이터 전송 알고리즘은 센서 노드가 배포되기 전에 미리 로드하는 단일 네트워크 광역 키를 기초로 경량 키 배포 방법을 사용한다.
- [0072] 노드들이 배포한 후, 공유 네트워크 키를 소유한 이웃 노드들과 통신을 수행한다. 단일 키는 대칭 키로 기능하며, 전송 에지의 연속적인 노드에만 알려져 있다.
- [0073] 또한, 보안 데이터 전송 알고리즘은 데이터 암호화 및 인증을 달성하기 위해 PCBC(Propagating Cipher Block Chaining)을 활용한다.
- [0074] 전송 보안 처리부(150)는 데이터 전송 전에 센서 데이터를 PCBC(Propagating Cipher Block Chaining)를 기반으로 암호화하여 전송한다.
- [0075] 전송 보안 처리부(150)는 데이터 전송 전에 센서 노드의 데이터를 블록으로 분할하여 체인 형태의 데이터 암호화 함수 E 을 수행하여 악성 개체 존재 시 잠재적인 위협에 대한 데이터 프라이버시를 향상시킨다.
- [0076] 전송 보안 처리부(150)에서 데이터 암호화 전에 센서 데이터의 각 블록은 이전 평문(일반 텍스트) 블록과 이전 암호문 블록을 XOR 연산한다. E_k 는 대칭키 k 를 이용한 암호화 함수이고, D_k 는 동일한 키 k 를 이용한 복호화 함수이다. 그런 다음 센서 노드 i 에 대한 메시지 블록 mb_i 은 수학식 4와 수학식 5를 사용하여 PCBC 를 기반으로 하는 각각의 암호 블록 cb_i 으로 변환된다.

수학식 4

$$Cb_i = E_k(mb_i \oplus mb_{i-1} \oplus cb_{i-1}), mb_0 \oplus Cb_0 = IV$$

수학식 5

$$mb_i = D_k(Cb_i) \oplus mb_{i-1} \oplus cb_{i-1}), mb_0 \oplus Cb_0 = IV$$

$$cb_{i-1} \text{은 이전 블록인 } mb_{i-1} \text{의 암호 블록이다.}$$

[0080] 제어부(130)는 전송 보안 처리부(150)에 의해 암호화된 데이터 블록을 통신부를 거쳐 기지국으로 전송한다.

[0081] 따라서, 제어부(130)는 중계 노드 집합의 데이터 블록을 통신부를 통해 기지국으로 전송되고, 마지막으로 수학 식 6과 같이, 대칭 키를 기반으로 암호화된 모든 데이터를 복호화한다.

수학식 6

$$D_i = K_i \oplus K_{i+1}, \dots \oplus Cb_i$$

[0084] (성능 평가)

[0085] EBDS(Energy-Efficient Big Data-Based Secure) 프레임워크의 성능은 Sca-PBDA와 센서 네트워크의 효율적인 데이터 수집 방법에 대해 평가된다.

[0086] 성능은 다양한 데이터 전송 속도 측면에서 NS-3을 사용하여 평가된다. 시뮬레이션에서 네트워크 필드는 제공 크기로 간주되며, 레이아웃은 $300 \times 300m^2$ 크기이다.

[0087] IoT 기반 센서와 악성 노드는 각각 200개, 20개다. 기지국의 위치는 네트워크 필드의 외부에 설정하고 정적 상태를 유지한다. 비트 단위의 데이터 전송 속도는 50 내지 250으로 설정된다.

[0088] 가중치 요소들 α 와 β 의 값들은 0.5 및 0.5로 고정된다. 센서 노드의 잔류 에너지는 2j 내지 5j 범위에 있다. 표 1은 시뮬레이션 매개변수의 값을 나열한다.

표 1

Table 1 Simulation parameters

Parameter	Value
Simulation area	300m×300m
Sensor nodes	200
Malicious nodes	20
Transmission range	20m
Data sending rate	50 to 300 bits
α, β	0.5, 0.5
Energy resource	2j-5j
BS's position	350m×400m
Data bits per packet	32
Malicious nodes	15
Traffic flow	CBR

[0089]

[0090] 시뮬레이션은 1000번의 반복에 대해 실행되고, 각 블록의 데이터 크기는 32비트이다.

[0091] 도 3은 본 발명의 실시예에 따른 에너지 소비에 대한 기존 작업에 대한 EBDS 프레임워크의 성능을 나타낸 도면이다.

- [0092] 이 섹션에서는 에너지 소비, 네트워크 처리량, 패킷 드롭 비율, 중단 간 지연 및 경로 안정성에 대한 논의와 함께 실험 결과를 제공한다.
- [0093] EBDS 프레임워크는 다양한 데이터 전송 속도에서 에너지 소비 비율을 각각 13% 및 18% 감소시키는 것으로 관찰되었다. 노드의 주변 환경을 판단하여 추가 작업에서 소모되는 에너지 수준이 감소하기 때문이다. 또한 EBDS 프레임워크는 랭크 값을 기반으로 릴레이 노드 선택을 최적화하고 경로 수명 수준을 높인다. 다른 작업과 달리 EBDS 프레임워크는 노드의 추가 부하를 명시적으로 최소화하고 에너지 효율성을 향상시키는 추가 경로 검색 패킷을 줄인다.
- [0094] 또한, EBDS 프레임워크는 단일 홉 대신 다중 홉 전송을 사용하고 소스와 릴레이 노드 간의 부하 분산을 균형 있게 조정한다. 또한, 다중 홉 패러다임으로 인해 센서의 데이터를 기지국으로 전송하는 동안 노드당 에너지 소비가 감소한다.
- [0095] EBDS 프레임워크는 경량 암호화 작업으로 보다 안전한 경로를 제공하므로 처리 오버헤드의 균형을 유지한다.
- [0097] 도 4는 본 발명의 실시예에 따른 다양한 데이터 전송 속도에서 패킷 드롭 비율에 대한 다른 작업과 함께 EBDS 프레임워크의 성능을 나타낸 도면이다.
- [0098] 실험 결과에 따르면, EBDS 프레임워크는 데이터 손실 비율을 각각 26%, 39% 감소시키는 것으로 나타났다.
- [0099] 이는 센서 노드 측의 제한된 리소스를 고려하여 보다 에너지 효율적이고, 트래픽 웨어 릴레이 노드를 선택하기 때문이다.
- [0100] EBDS 프레임워크는 라우팅 결정을 계산할 때, 네트워크와 노드의 최신 매개변수를 추적한다. 다양한 네트워크 트래픽에서 실패하기 쉽고 경로 일관성이 떨어지는 다른 작업과 달리 본 발명의 EBDS 프레임워크는 연결 끊김 측면에서 네트워크 성능을 저하시키지 않는 보다 안정적이고 안전한 방법을 제공한다.
- [0101] 또한, EBDS 프레임워크는 중계 노드의 잔류 에너지를 주기적으로 평가하여 에너지 비효율적인 노드를 기존 라우팅 경로에서 제외할 수 있고, 궁극적으로 데이터 전달 비율을 높인다.
- [0103] 도 5는 본 발명의 실시예에 따른 중단 간 지연 및 다양한 데이터 전송 속도를 나타낸 도면이다.
- [0104] 기존 작업에 대한 EBDS 프레임워크의 성능이 나와 있다. EBDS 프레임워크는 다양한 데이터 전송 속도에서 중단 간 지연 비율을 12% 및 19% 감소시키는 것으로 나타났다.
- [0105] 그 이유는 EBDS 프레임워크가 다중 홉 통신을 이용하여 센서 노드에서 기지국으로의 전송 거리를 줄이기 때문이다.
- [0106] 또한, 가장 에너지를 인식하고 덜 혼잡한 중계 노드를 선택하여 라우팅 결정에 참여한다. 이러한 라우팅 방법은 적시에 데이터를 전달하는 효율성을 향상시킨다. 또한, EBDS 프레임워크는 다익스트라(Dijkstra) 알고리즘을 기반으로 최적화된 라우팅 결정을 통해 보다 현실적이고 지연 효율적인 라우팅 경로를 제공하여 빈번한 재전송 및 경로 재발견 메시지를 줄인다.
- [0107] 네트워크 지연이 높은 라우팅 경로를 찾기 위해 센서 노드 간에 높은 오버헤드가 발생하는 다른 솔루션과 달리 EBDS 프레임워크는 안정적이고 신뢰할 수 있는 중계 노드를 제공하고, 이웃 노드 간의 제어 메시지를 줄이며 적시에 데이터 전달 성능을 향상시킨다.
- [0108] 또한, EBDS 프레임워크에는 소스 노드의 라우팅 메트릭을 평가하기 위해 인접 트래픽 인식 정보가 포함되어 있어 데이터 라우팅을 위한 전송 링크 혼잡을 방지하고, 중단 간 지연 측정을 줄이는 데 도움이 된다.
- [0110] 도 6는 본 발명의 실시예에 따른 네트워크 처리량 및 다양한 데이터 전송 속도를 나타낸 도면이다.
- [0111] 도 6은 EBDS 프레임워크의 성능이 데이터 전달 비율 측면에서 다른 솔루션과 비교되었음을 보여준다. 시뮬레이션된 실험을 기반으로 EBDS 프레임워크는 다양한 데이터 전송 속도에 대해 데이터 전달 성능을 10%, 15% 향상시키는 것으로 나타났다. 이러한 개선의 이유는 에너지 및 트래픽 분석 요소를 사용하여 중계 노드를 선택하기 때문이다. 이러한 요소는 센서 노드 간의 추가 에너지 소비를 줄이고 대용량 빅데이터를 전송하기 위한 라우팅 경

로를 강화한다.

[0112] 또한, 데이터 패킷은 다익스트라(Dijkstra) 알고리즘을 사용하는 다중 기준을 기반으로 하는 다중 홉 전송을 통해 기지국으로 라우팅되므로 다른 솔루션에 비해 기지국으로 전송되는 패킷 수가 가장 많다. 또한, EBDS 프레임워크는 라우팅 경로를 통한 데이터 보안에 대한 임계값을 증가시키고, 메시지 전달에 영향을 미치는 잠재적인 위협 가능성을 무시한다.

[0114] 도 7은 본 발명의 실시예에 따른 경로 안정성 및 다양한 데이터 전송 속도를 나타낸 도면이다.

[0115] 도 7은 기존 작업과의 비교에서 EBDS 프레임워크의 성능을 보여준다. 시뮬레이션 실험에서 EBDS 프레임워크는 센서 노드 측에서 가장 적은 수의 제어 메시지 및 경로 재검색 패킷의 플러딩으로 인해 다양한 데이터 전송 속도에 대해 경로 안정성을 13%, 19% 증가시키는 것으로 관찰되었다.

[0116] 또한, EBDS 프레임워크는 PCBC 모드 기반의 안전하고 인증된 알고리즘을 통합하여 경로 안정성의 성능을 높인다. 이러한 방법은 체인 형태로 암호화 및 복호화 기능을 수행하므로 저전력 센서 노드에서 통신 오버헤드가 가장 적은 데이터 송수신 노드 간의 보안 수준이 균형을 이룬다. 따라서, EBDS 프레임워크는 센서 데이터가 손상될 가능성을 줄이고, 궁극적으로 데이터 수집 및 라우팅에 대한 악의적인 위협에 대해 더 강력하다.

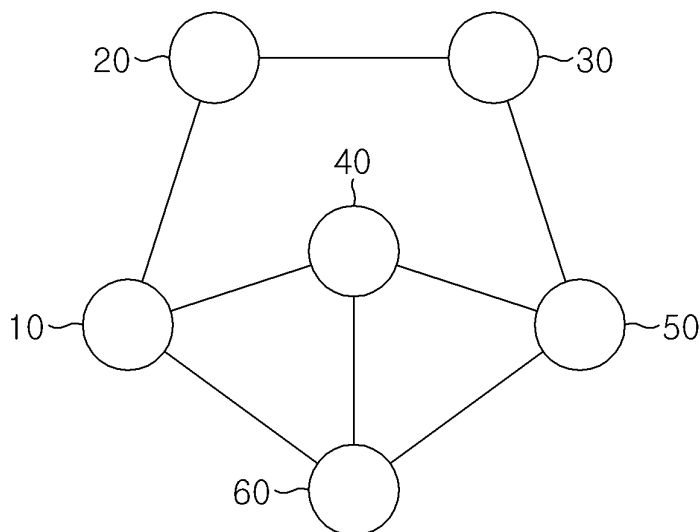
[0117] 이상에서 본 발명의 실시예에 대하여 상세하게 설명하였지만 본 발명의 권리범위는 이에 한정되는 것은 아니고 다음의 청구범위에서 정의하고 있는 본 발명의 기본 개념을 이용한 당업자의 여러 변형 및 개량 형태 또한 본 발명의 권리범위에 속하는 것이다.

부호의 설명

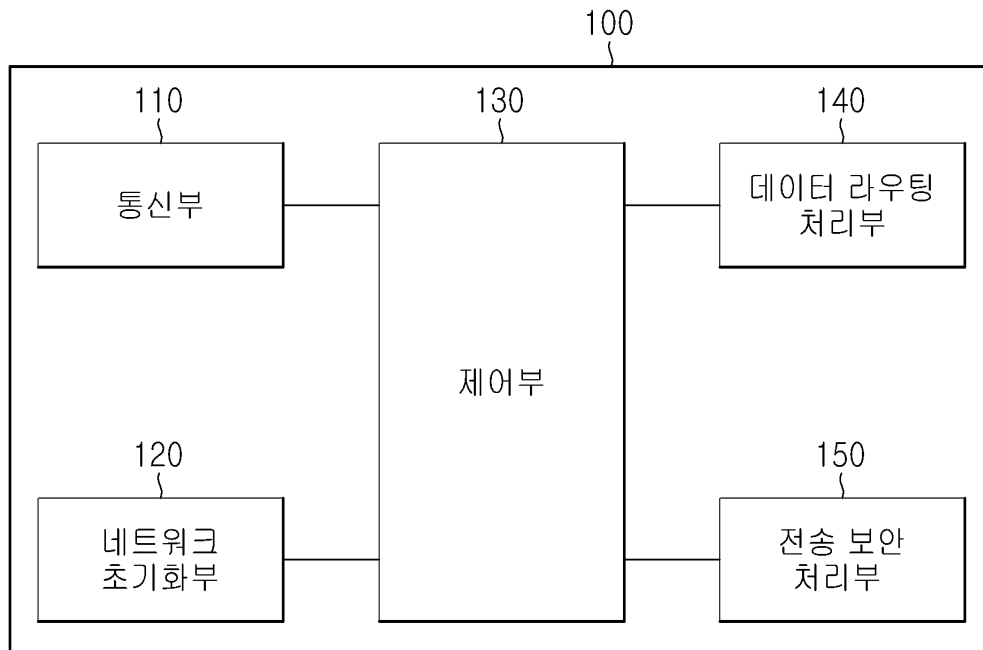
[0118] 100: 라우팅 제공 장치
110: 통신부
120: 네트워크 초기화부
130: 제어부
140: 데이터 라우팅 처리부
150: 전송 보안 처리부

도면

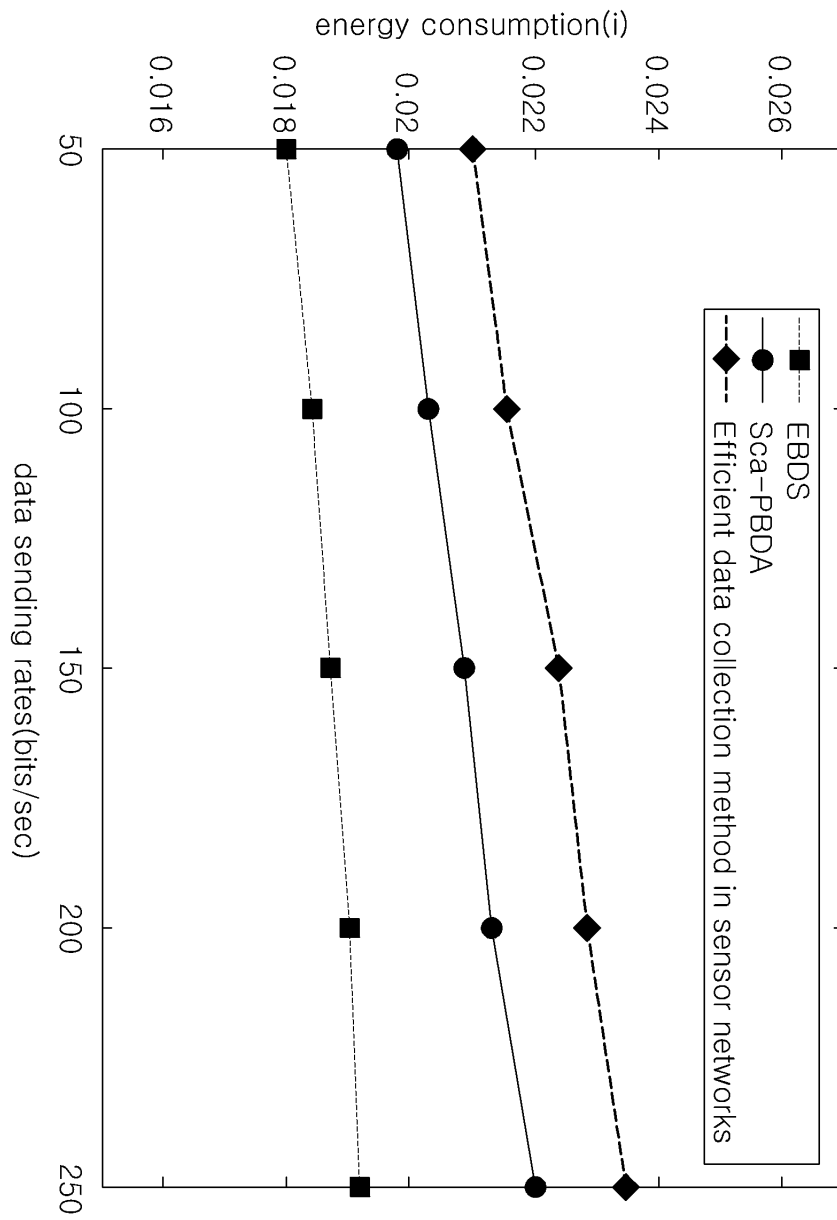
도면1



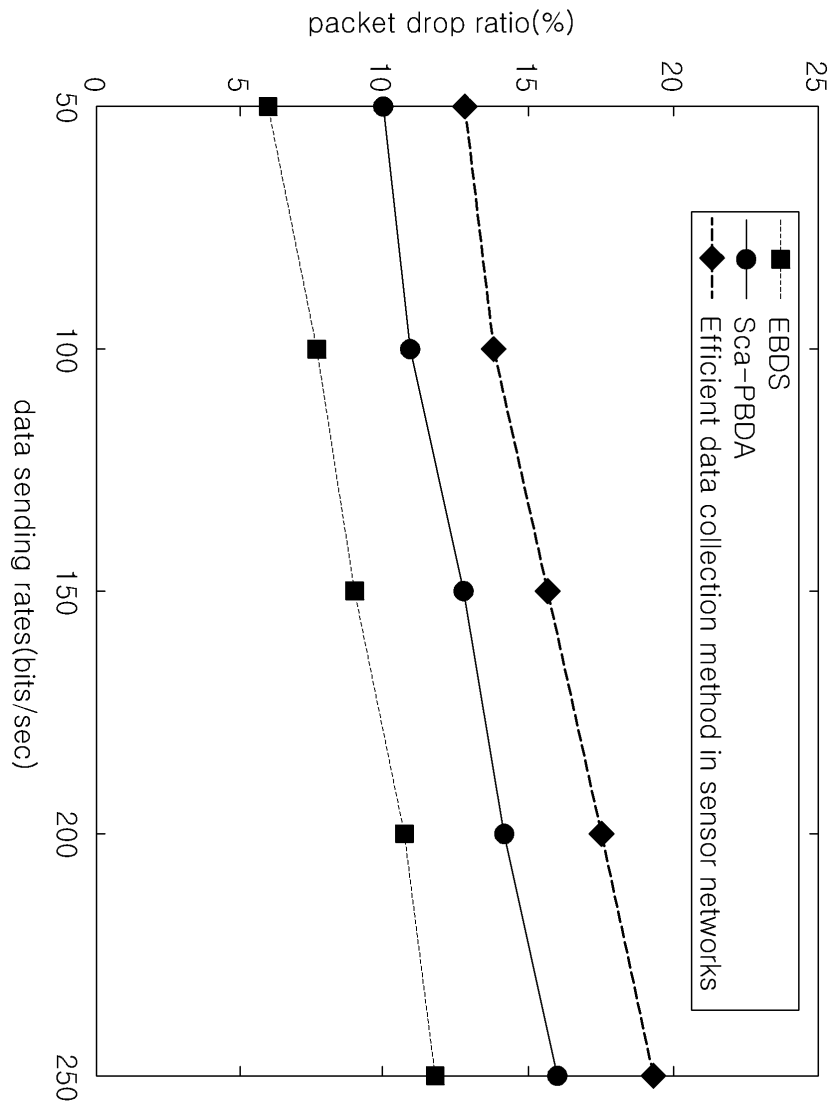
도면2



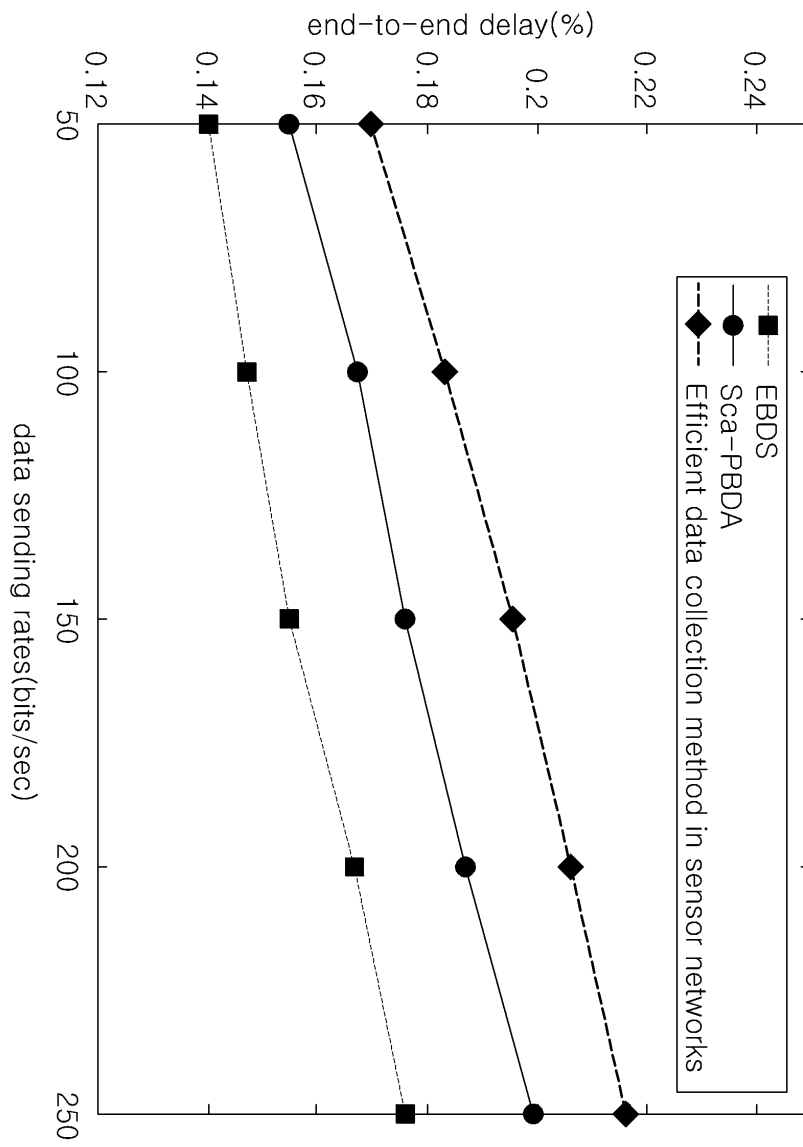
도면3



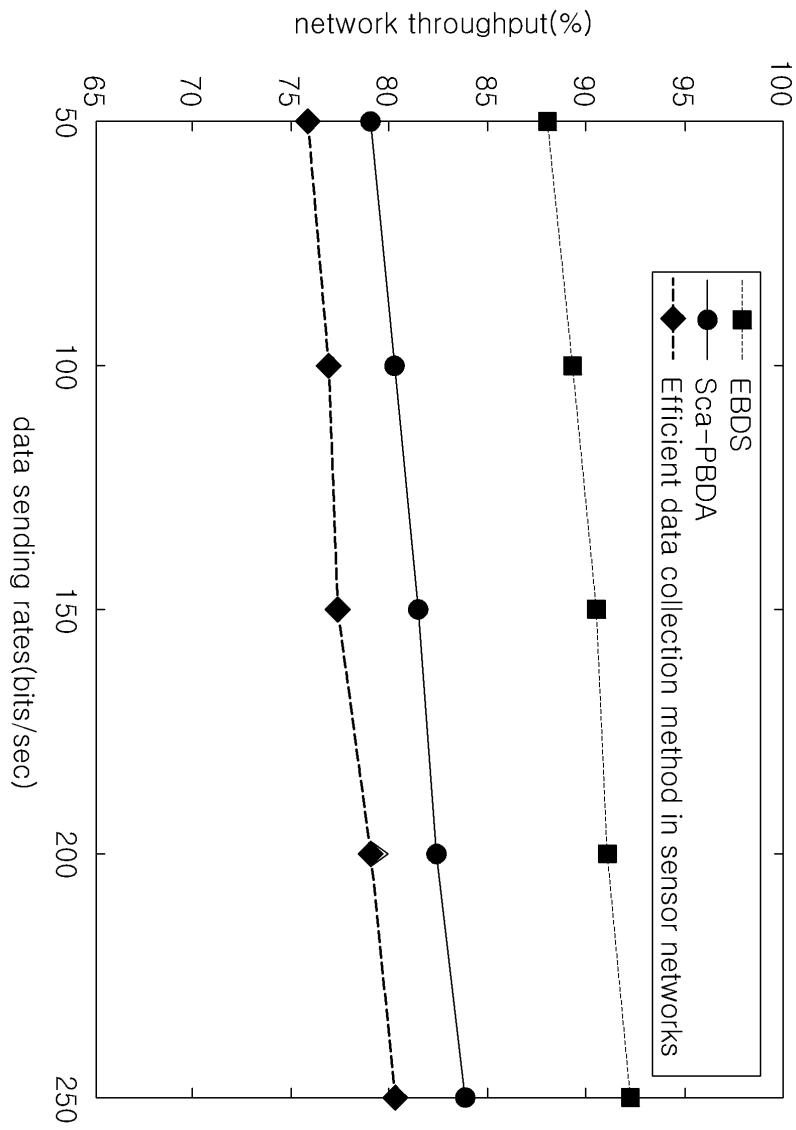
도면4



도면5



도면6



도면7

