(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2025-0009846
(43) 공개일자 2025년01월20일

(51) 국제특허분류(Int. Cl.)
H04L 67/12 (2022.01) *H04L 12/28* (2006.01)
H04L 45/12 (2022.01) *H04L 9/32* (2006.01)
(52) CPC특허분류
H04L 67/12 (2022.05)
H04L 12/2803 (2013.01)
(21) 출원번호 10-2023-0090011
(22) 출원일자 2023년07월11일
심사청구일자 2023년07월11일

(71) 출원인
인천대학교 산학협력단
인천광역시 연수구 갯벌로 27, 인천대학교 이노베이션센터(송도동)
(72) 발명자
전광길
인천광역시 연수구 해송로 70, 209동 805호(송도동, 송도웰카운티2단지)
(74) 대리인
특허법인충정

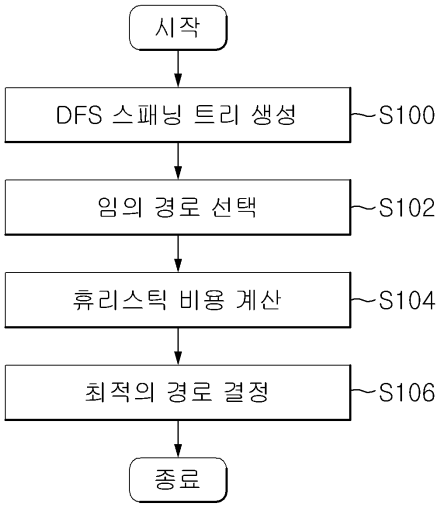
전체 청구항 수 : 총 13 항

(54) 발명의 명칭 **사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법 및 장치**

(57) 요 약

본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은, 네트워크 내 어느 하나의 소스 노드가 센서 노드로부터 수집된 정보를 이용하여 DFS(Depth-First Search) 스패닝 트리(spanning tree)를 생성하는 단계; 상기 소스 노드가 임의 경로(random routes)를 선택하는 단계; 네트워크를 관리하는 싱크 노드가 상기 소스 노드로부터 주변 노드까지의 거리와 혼잡 윈도우(congestion window)를 이용하여 휴리스틱 비용(heuristic cost)을 계산하는 단계; 및 상기 휴리스틱 비용의 최소 값을 찾아 최적의 경로를 결정하는 단계;를 포함할 수 있고, 상기 싱크 노드가 비밀 키를 생성하는 단계; 상기 비밀 키의 보증을 위해 상기 싱크 노드가 상기 SDN 컨트롤러와 통신하는 단계; 및 상기 SDN 컨트롤러의 검증이 완료되면, 신뢰할 수 있는 디지털 인증서의 발급을 시작하는 단계;를 더 포함할 수 있다.

대 표 도 - 도1



(52) CPC특허분류
H04L 45/12 (2022.05)
H04L 9/3263 (2013.01)

명 세 서

청구범위

청구항 1

네트워크 내 어느 하나의 소스 노드가 센서 노드로부터 수집된 정보를 이용하여 DFS(Depth-First Search) 스패닝 트리(spanning tree)를 생성하는 단계;

상기 소스 노드가 임의 경로(random routes)를 선택하는 단계;

네트워크를 관리하는 싱크 노드가 상기 소스 노드로부터 주변 노드까지의 거리와 혼잡 윈도우(congestion window)를 이용하여 휴리스틱 비용(heuristic cost)을 계산하는 단계; 및

상기 휴리스틱 비용의 최소 값을 찾아 최적의 경로를 결정하는 단계;를 포함하는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 2

제1항에 있어서,

상기 싱크 노드에서는 우선순위가 낮은 경로를 라우팅 테이블에서 제거하고 업데이트된 정보는 지속적으로 반영하는 것을 특징으로 하는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 3

제1항에 있어서,

패킷 드롭 비율이 임계 값을 초과하면, 소프트웨어 정의 네트워크(Software Defined Network, SDN) 컨트롤러는 상기 싱크 노드에 신호를 보내 새로운 경로 식별을 시작하고, 대체할 수 있는 중복 경로를 추가하는 단계; 및

현재 경로에서 데이터를 처리할 수 없을 때 상기 싱크 노드가 상기 중복 경로를 제공하는 단계;를 더 포함하는 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 4

제1항에 있어서,

상기 휴리스틱 비용은,

$$H(c) = min\,(d_i + C_w)$$

에 기반하여 계산될 수 있고,

여기서, d_i는 부분그래프(subgraph) G'로부터 추출한 상기 소스 노드로부터 주변 노드까지의 거리, C_w는 혼잡 윈도우(congestion window)를 나타내는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 5

제4항에 있어서, 상기 혼잡 윈도우 값은

$$C_w = \frac{P_t}{RTT} + \frac{l_b}{\alpha}$$

에 기반하여 계산될 수 있고,

여기서 P_t 는 전송된 비콘 패킷(beacon packets)의 기록, RTT는 패킷왕복시간(round trip time, RTT), l_b는 소스 노드 i와 근접 노드인 j 간 링크의 대역폭 크기, α 는 이용할 수 있는 데이터 대역폭(bandwidth)을 나타내는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 6

제1항에 있어서,

상기 싱크 노드가 비밀 키를 생성하는 단계;

상기 비밀 키의 보증을 위해 상기 싱크 노드가 상기 SDN 컨트롤러와 통신하는 단계; 및

상기 SDN 컨트롤러의 검증이 완료되면, 신뢰할 수 있는 디지털 인증서의 발급을 시작하는 단계;를 더 포함하는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 7

제6항에 있어서,

상기 싱크 노드와 상기 SDN 컨트롤러 간에 RSA 알고리즘을 활용하여 통신하는 것을 특징으로 하는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 8

제6항에 있어서, 상기 비밀 키는,

i번째 노드 n_i에 대한 초기 공유(initial share)값 Y 로부터 계산될 수 있는 것을 특징으로 하는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 9

제6항에 있어서,

상기 비밀 키를 안전하게 전송한 후, 암호화 함수를 활용하여 데이터 프라이버시를 확보할 수 있는 것을 특징으로 하는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 10

제6항에 있어서, SDN 컨트롤러와 통신하는 단계에 있어서,

상기 싱크 노드로부터 SDN 컨트롤러로 암호화된 데이터를 전송하기 위한 최단 경로 p를 계산할 수 있고, 만약 상기 싱크 노드가 SDN 컨트롤러와 직접 연결되지 않은 경우에는 가장 가까운 싱크 노드를 식별하기 위해 거리 임계값 d를 탐색할 수 있는 것을 특징으로 하는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 11

제10항에 있어서, 상기 임계값 d는

$$if\ p^{edi-edj}(len) \leq d\ then\ route_data$$

에 기반하여 계산되고,

여기서 edi 는 i번째 에지 장치, edj 는 상기 i번째 에지 장치와 가장 가까운 j번째 에지 장치, p는 가장 최소한의 노드의 개수를 거치는 경로인 것을 특징으로 하고,

상기 에지 장치는 상기 싱크 노드 중 하나인 것을 특징으로 하는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 12

제6항에 있어서, 상기 디지털 인증서는

대칭 디지털 인증서(symmetric digital certificates)를 활용할 수 있는 것을 특징으로 하는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법.

청구항 13

IoT 시스템 네트워크 내에 위치하는 복수 개의 센서 노드;

상기 센서 노드로부터 센싱된 정보를 전달받아 외부로 전송하는 싱크 노드;

높은 수준의 보안을 유지하면서 안전하게 상기 IoT 시스템의 데이터를 처리할 수 있는 소프트웨어 정의 네트워크(SDN); 및

IoT 장치들을 전체적으로 관리하는 소프트웨어 정의 네트워크(SDN) 컨트롤러;를 포함하는, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 장치.

발명의 설명

기 술 분 야

[0001] 본 발명은 SDN 기반 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법 및 장치에 관한 것이다.

배 경 기 술

[0002] 무선 센서 네트워크(WSN) 및 스마트 사물인터넷은 다용성, 내구성 및 비용 효율성 측면에서 탁월한 이점으로 인해 원격 모니터링에 널리 사용될 수 있고, 특히 무선 센서 네트워크(WSN)는 다른 기술 분야와의 높은 호환성으로 인해 광범위한 모바일 네트워크를 지원하고 다양한 소스에서 데이터를 수집할 수 있다. 현재, WSN 및 IoT 기술은 의료, 농업 및 그리드 컴퓨팅을 포함한 광범위한 스마트 애플리케이션에 널리 배포되고 있는데, 이러한 응용 프로그램을 사용하면 사람 간의 상호 작용 없이 연결된 장치로 부터 필요한 데이터를 쉽게 얻을 수 있다.

[0003] IoT 기반 무선 센서 네트워크(WSN)는 임베디드 개체를 지능적으로 모니터링, 처리 및 분석하고 인터넷을 통해 데이터를 공유할 수 있다. 특히, 무선 센서 네트워크(WSN)는 저전력 장치의 제한된 기능으로 인해 인공 지능(AI) 시스템에 의존하게 되는데, 인공지능(AI) 및 머신 러닝(ML)과 같은 새로운 기술은 복잡한 알고리즘을 도입하여 네트워크 및 시스템을 보호하고 있다.

[0004] 소프트웨어 정의 네트워크(Software-Defined Networking, SDN)는 주로 네트워크 장비 제어, 설계 및 관리에 활용되고 있는데, 이러한 SDN은 동적인 특성을 지닌 IoT 기기와 통신 시스템 간의 가교 역할을 수행할 수 있고, 연결된 개체는 분산 네트워크 시스템을 형성하여 최소한의 오버헤드로 통신 서비스의 부하를 분산시킬 수 있다. 그러나 대부분의 SDN 기반 WSN 솔루션은 모든 유형의 스마트 운영을 정확하고 신속하게 처리하기에는 부족하다는 문제점이 있다.

[0005] 한편, 스마트 기기와 센서는 다양한 소스와 물리적인 대상으로부터 많은 양의 데이터를 수집하기 때문에 최적으로 데이터를 처리하고 분석하는 것이 요구되는데, 많은 IoT 기반 스마트 도시는 자율 구조를 통해 데이터를 수집하고 원격 사용자에게 전달하기 위해 센서 노드를 사용하는 경우가 많다. 그러나 센서는 예측할 수 없는 상황에서 사용되기 때문에 시스템 리소스를 최적화하고 많은 보안 사고로부터 실시간 데이터를 보호하는 것이 IoT 시스템에서 가장 중요한 문제이다.

선행기술문헌

특허문헌

[0006] (특허문헌 0001) KR 10-2016-0003907 A

발명의 내용

해결하려는 과제

[0007] 본 발명의 목적은 상기의 문제점을 해결하기 위한 것으로, 통신 장치의 관리 부하와 비용을 낮추기 위하여 휴리스틱 컴퓨팅을 활용하여 모바일 에지의 데이터 전송 시스템을 제공할 수 있다. 특히 인공지능을 이용한 휴리스틱 평가를 도입하여 실시간 시스템의 센서 노드의 전력 소모를 감소시킨다.

[0008] 본 발명은 열린 통신 공간이라는 특성으로 인해 발생할 수 있는 악의적인 메시지 및 개인 정보 보호 문제를 포함하여 수많은 보안 취약성이 있는 IoT 네트워크를 안전하게 보호하기 위하여 중앙 집중식 컨트롤러를 사용하여 신뢰할 수 있는 데이터를 얻을 수 있다.

과제의 해결 수단

[0009] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은, 네트워크 내 어느 하나의 소스 노드가 센서 노드로부터 수집된 정보를 이용하여 DFS(Depth-First Search) 스패닝 트리(spanning tree)를 생성하는 단계; 상기 소스 노드가 임의 경로(random routes)를 선택하는 단계; 네트워크를 관리하는 싱크 노드가 상기 소스 노드로부터 주변 노드까지의 거리와 혼잡 윈도우(congestion window)를 이용하여 휴리스틱 비용(heuristic cost)을 계산하는 단계; 및 상기 휴리스틱 비용의 최소 값을 찾아 최적의 경로를 결정하는 단계;를 포함할 수 있다.

[0010] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은, 상기 싱크 노드에서는 우선순위가 낮은 경로를 라우팅 테이블에서 제거하고 업데이트된 정보는 지속적으로 반영하는 것을 특징으로 할 수 있다.

[0011] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은, 패킷 드롭 비율이 임계 값을 초과하면, 소프트웨어 정의 네트워크(Software Defined Network, SDN) 컨트롤러는 상기 싱크 노드에 신호를 보내 새로운 경로 식별을 시작하고, 대체할 수 있는 중복 경로를 추가하는 단계; 및 현재 경로에서 데이터를 처리할 수 없을 때 상기 싱크 노드가 상기 중복 경로를 제공하는 단계;를 더 포함할 수 있다.

[0012] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법에서, 상기 휴리스틱 비용은,

[0013] $$H(c) = min\,(d_i + C_w)$$

[0014] 에 기반하여 계산될 수 있고,

[0015] 여기서, d_i는 부분그래프(subgraph) G'로부터 추출한 상기 소스 노드로부터 주변 노드까지의 거리, C_w는 혼잡 윈도우(congestion window)를 나타낼 수 있다.

[0016] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법에서, 상기 혼잡 윈도우 값은

[0017] $$C_w = \frac{P_t}{RTT} + \frac{l_b}{\alpha}$$

[0018] 에 기반하여 계산될 수 있고,

[0019] 여기서 P_t는 전송된 비콘 패킷(beacon packets)의 기록, RTT는 패킷왕복시간(round trip time, RTT), l_b는 소스 노드 i와 근접 노드인 j 간 링크의 대역폭 크기, α는 이용할 수 있는 데이터 대역폭(bandwidth)을 나타낼 수 있다.

[0020] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은, 상기 싱크 노드가 비밀 키를 생성하는 단계; 상기 비밀 키의 보증을 위해 상기 싱크 노드가 상기 SDN 컨트롤러와 통신하는

단계; 및 상기 SDN 컨트롤러의 검증이 완료되면, 신뢰할 수 있는 디지털 인증서의 발급을 시작하는 단계;를 더 포함할 수 있다.

[0021] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은, 상기 싱크 노드와 상기 SDN 컨트롤러 간에 RSA 알고리즘을 활용하여 통신하는 것을 특징으로 할 수 있다.

[0022] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법에서, 상기 비밀 키는, i번째 노드 n_i에 대한 초기 공유(initial share)값 Y로부터 계산될 수 있는 것을 특징으로 할 수 있다.

[0023] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은, 상기 비밀 키를 안전하게 전송한 후, 암호화 함수를 활용하여 데이터 프라이버시를 확보할 수 있는 것을 특징으로 할 수 있다.

[0024] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은, SDN 컨트롤러와 통신하는 단계에 있어서, 상기 싱크 노드로부터 SDN 컨트롤러로 암호화된 데이터를 전송하기 위한 최단 경로 p를 계산할 수 있고, 만약 상기 싱크 노드가 SDN 컨트롤러와 직접 연결되지 않은 경우에는 가장 가까운 싱크 노드를 식별하기 위해 거리 임계값 d를 탐색할 수 있다.

[0025] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은, 상기 임계값 d는

[0026] $$if\ p^{edi-edj}(len) \le d\ then\ route_data$$

[0027] 에 기반하여 계산되고,

[0028] 여기서 edi는 i번째 에지 장치, edj는 상기 i번째 에지 장치와 가장 가까운 j번째 에지 장치, p는 가장 최소한의 노드의 개수를 거치는 경로인 것을 특징으로 하고, 상기 에지 장치는 상기 싱크 노드 중 하나인 것을 특징으로 할 수 있다.

[0029] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은, 상기 디지털 인증서는 대칭 디지털 인증서(symmetric digital certificates)를 활용할 수 있는 것을 특징으로 할 수 있다.

[0030] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 장치는, IoT 시스템 네트워크 내에 위치하는 복수 개의 센서 노드; 상기 센서 노드로부터 센싱된 정보를 전달받아 외부로 전송하는 싱크 노드; 높은 수준의 보안을 유지하면서 안전하게 상기 IoT 시스템의 데이터를 처리할 수 있는 소프트웨어 정의 네트워크(SDN); 및 IoT 장치들을 전체적으로 관리하는 소프트웨어 정의 네트워크(SDN) 컨트롤러;를 포함할 수 있다.

발명의 효과

[0031] 무선 센서 네트워크(Wireless Sensor Network, WSN) 및 스마트 IoT는 다양한 소스와 물리적인 대상으로부터 많은 양의 데이터를 수집하기 때문에 최적의 데이터 처리 및 분석 방법이 요구된다. 본 발명을 통해 대기 시간을 감소시키고, 향상된 성능과 보안 라우팅을 통해 성공적인 전송 속도를 제공할 수 있으며, 상호 인증을 위한 비밀 공유를 사용함으로써 안전한 환경을 제공할 수 있다.

도면의 간단한 설명

[0032] 도 1은 본 발명의 일 실시예로 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법을 나타내는 흐름도

도 2은 본 발명의 일 실시예로 보안 시스템의 흐름도

도 3a는 다양한 센서 노드에 따른 에너지 소비량

도 3b는 다양한 시간 간격에 따른 에너지 소비량

도 4a는 다양한 노드별 처리 지연 시간(sec)

도 4b는 다양한 시간 간격에 따른 처리 지연 시간(sec)

도 5a는 다양한 노드별 네트워크 처리량(%)

도 5b는 다양한 시간 간격에 따른 네트워크 처리량(%)

도 6a는 다양한 노드별 패킷 드랍율(%)

도 6b는 다양한 시간 간격에 따른 패킷 드랍율(%)

도 7은 본 발명의 일 실시예로 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 장치

발명을 실시하기 위한 구체적인 내용

[0033] 본 발명의 목적, 특정한 장점들 및 신규한 특징들은 첨부된 도면들과 연관되어지는 이하의 상세한 설명과 바람직한 실시예들로부터 더욱 명백해질 것이다. 이때, 각각의 도면에서 동일한 구성요소는 가능한 동일한 부호로 나타낸다. 또한, 이미 공지된 기능 및/또는 구성에 대한 상세한 설명은 생략한다.

[0034] 이하에 개시된 내용은, 다양한 실시 예에 따른 동작을 이해하는데 필요한 부분을 중점적으로 설명하며, 그 설명의 요지를 흐릴 수 있는 요소들에 대한 설명은 생략한다. 또한 도면의 일부 구성요소는 과장되거나 생략되거나 또는 개략적으로 도시될 수 있다. 각 구성요소의 크기는 실제 크기를 전적으로 반영하는 것이 아니며, 따라서 각각의 도면에 그려진 구성요소들의 상대적인 크기나 간격에 의해 여기에 기재되는 내용들이 제한되는 것은 아니다.

[0035] 본 발명의 실시예들을 설명함에 있어서, 본 발명과 관련된 공지기술에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략하기로 한다. 그리고, 후술되는 용어들은 본 발명에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다. 상세한 설명에서 사용되는 용어는 단지 본 발명의 실시 예들을 기술하기 위한 것이며, 결코 제한적이어서는 안 된다. 명확하게 달리 사용되지 않는 한, 단수 형태의 표현은 복수 형태의 의미를 포함한다. 본 설명에서, "포함" 또는 "구비"와 같은 표현은 어떤 특성들, 숫자들, 단계들, 동작들, 요소들, 이들의 일부 또는 조합을 가리키기 위한 것이며, 기술된 것 이외에 하나 또는 그 이상의 다른 특성, 숫자, 단계, 동작, 요소, 이들의 일부 또는 조합의 존재 또는 가능성을 배제하도록 해석되어서는 안 된다.

[0036] 또한, 제1, 제2 등의 용어는 다양한 구성요소들을 설명하는데 사용될 수 있지만, 상기 구성요소들은 상기 용어들에 의해 한정되는 것은 아니며, 상기 용어들은 하나의 구성요소를 다른 구성요소로부터 구별하는 목적으로만 사용된다.

[0037] 이하에서는, 첨부된 도면들을 참조하여, 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법 및 장치에 대해 설명하기로 한다.

[0039] 도 1은 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법이고, 도 7는 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 장치(700)의 블록도이다.

[0040] 도 1을 참조하면, 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은, 네트워크 내 어느 하나의 소스 노드가 센서 노드로부터 수집된 정보를 이용하여 DFS(Depth-First Search) 스패닝 트리(spanning tree)를 생성하는 단계; 상기 소스 노드가 임의 경로(random routes)를 선택하는 단계; 네트워크를 관리하는 싱크 노드가 상기 소스 노드로부터 주변 노드까지의 거리와 혼잡 윈도우(congestion window)를 이용하여 휴리스틱 비용(heuristic cost)을 계산하는 단계; 및 상기 휴리스틱 비용의 최소 값을 찾아 최적의 경로를 결정하는 단계;를 포함할 수 있다.

[0041] 본 발명의 일 실시예로, DFS 평가를 이용하여 스패닝 트리를 생성하고 포워더 정보 추출을 위한 휴리스틱 비용을 계산할 수 있다. 비용은 거리와 혼잡도 측면에서 최소가 되어야 한다.

[0042] 본 발명의 일 실시예로, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 네트워크 시스템

의 경로를 재조정하고, DFS 알고리즘을 사용하여 비용 휴리스틱 함수(cost heuristic function)를 사용하여 지능형 에너지 솔루션을 제공할 수 있다.

[0044] 한편, 도 1에 도시된 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법에서 연산과 관련된 단계들은 도 7에 도시된 장치(700)에 의해 수행될 수 있다.

[0045] 도 7에 도시된 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 장치(700)는, IoT 시스템 네트워크 내에 위치하는 복수 개의 센서 노드; 상기 센서 노드로부터 센싱된 정보를 전달받아 외부로 전송하는 싱크 노드; 높은 수준의 보안을 유지하면서 안전하게 상기 IoT 시스템의 데이터를 처리할 수 있는 소프트웨어 정의 네트워크(SDN); 및 IoT 장치들을 전체적으로 관리하는 소프트웨어 정의 네트워크(SDN) 컨트롤러;를 포함할 수 있다.

[0046] 상기와 같이 구성된 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 하기에 상세히 설명하기로 한다.

[0048] 도 7를 참고하면, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 장치(700)는 센서 노드(702)와 싱크 노드(704)를 포함할 수 있다.

[0049] 센서 노드(702)가 고정되어 있는 경우, 사전에 설정된 반경 내에서 주변 데이터를 감지할 수 있다. 각 센서에는 주변 장치 목록을 라우팅 테이블 형식으로 저장하고 근접한 위치에서 변화가 감지될 때마다 재구성할 수 있는 메모리를 충분히 갖고 있을 수 있다.

[0050] 센서 노드(702)는 외부에서 센싱된 정보 또는 센서에 관련된 특정 이벤트를 유무선 통신 기술에 의하여 전달하거나 컴퓨팅을 수행하는 노드로써, 데이터 처리, 통신 경로 설정, 미들웨어 처리 등을 수행할 수 있다.

[0051] 싱크 노드(704)는 센서 노드(702)에서 감지된 센싱 정보를 취합하거나, 이벤트성 데이터를 센서 네트워크 외부로 연계하고 관련 센서 네트워크를 관리할 수 있다.

[0052] 싱크 노드(704)는 SDN 컨트롤러(706)에 에지 장치(edge equipment)로 서비스를 제공할 수 있다. 여기서, 에지 장치란 에지 컴퓨팅(edge computing)을 제공하는 기기로 에지 노드(edge node)를 포함한다. 에지 노드는 데이터 발생 지점 부근에 위치하여 부분적으로 서버의 역할을 수행하는 네트워크 장비일 수 있다.

[0053] 싱크 노드(704)는 대기 시간이 짧은 IoT 데이터를 지원할 뿐만 아니라 SDN 컨트롤러(708)의 협업 처리를 통해 데이터를 제어할 수있다.

[0054] 소프트웨어 정의 네트워킹(Software Defined Networking, SDN)(706)은 네트워크를 제어부와 데이터 전달부로 분리하여 네트워크 관리자가 보다 효율적으로 네트워크를 제어 및 관리할 수 있는 기술이다.

[0055] 소프트웨어 정의 네트워킹 컨트롤러(708)는 중앙 집중식으로 작동하며, 지능적이고 높은 컴퓨팅 기능으로 분산 센서의 데이터 계획을 제어할 수 있다. 또한, 데이터 흐름 평면에서 악의적인 트래픽을 필터링하고 인증된 데이터만 네트워크 장치를 통과하도록 허용할 수 있다.

[0057] **< 효율적인 에너지 관리를 통한 품질 보증 데이터 전송 시스템>**

[0058] 본 발명의 일 실시예로, 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법에는 모바일 에지 컴퓨팅(mobile edge computing)이 적용될 수 있다. 모바일 에지 컴퓨팅을 통해 사용자와 가까운 곳에 서버를 위치시켜 데이터가 수집되는 현장에서 바로 데이터를 처리할 수 있다.

[0059] 구체적으로, 모바일 에지(mobile edges)는 주기적으로 최근의 위치를 업데이트하여 보고할 수 있고, 히스토리를 평가하여 설정된 경로에 우선순위를 할당할 수 있다. 즉, 우선 순위가 낮은 경로는 라우팅 테이블에서 제거하고 업데이트된 정보를 지속적으로 반영하여 신뢰도와 데이터 가용성을 높일 수 있다.

[0060] 한편, 사물인터넷 IoT의 센서 노드(702)는 환경에 무작위로 분포되며 Graph $G(E,V)$ 형태로 구성될 수 있다. $n1,n2 \in V(G)$ 이라면 $n1 \rightarrow n2$ 의 의미는 둘 다 에지 장치 E에 의해 V에 결합됨을 의미할 수 있다.

[0061] 본 발명의 일 실시예로, i번째 센서 노드(702)에 대한 초기 라우팅 테이블을 구성할 수 있다. 따라서, R_i는 수학식 1에 의해 주어진 것처럼 라우팅 테이블로부터 추출될 수 있다.

수학식 1

[0062] $$R_i = \sum_{i=0}^{n} r_i$$

[0063] 경로 r_i 각각은 그리디 원리(greedy principle)에 따르고, 아무런 루핑(looping)없이 형성한 연속적인 노드의 쌍을 의미한다. 여기서, 그리디 알고리즘은 선택의 순간마다 당장 눈 앞에 보이는 최적의 상황만을 쫓아 해답에 도달하는 방법으로, 최적해를 구하는 데에 사용되는 근사적인 방법론이다.

[0065] 본 발명의 일 실시예로, G'로 부터 추출한 노드들의 정보에 의한 휴리스틱 값 $H(c)$를 사용하여 네이버링 상태(neighboring states)가 식별될 수 있다.

[0066] 구체적으로는, 휴리스틱 값 $H(c)$의 결정은 다중 기준을 기반으로 하고, 센서 에지 커뮤니케이션 시스템을 이끌 수 있는 최적의 선택들을 제공할 수 있다.

[0067] i번째 센서 노드(702)의 전송 범위가 t_i에 의해 표시된다고 고려할 때, 만약 센서 노드(702)와 싱크 노드(704) 사이의 간격이 t_i 이내라면, 그 데이터는 즉시 전달할 수 있다. 그렇지 않으면, 본 발명은 최적의 인접 노드를 계산하기 위하여 $H(c)$ 값을 사용할 수 있다.

[0068] 수학식 2은 $H(c)$ 값을 계산한 것을 나타낸다.

수학식 2

[0069] $$H(c) = min\,(d_i + C_w)$$

[0070] 여기서, d_i은 거리, C_w는 혼잡 윈도우(congestion window)를 나타낸다.

[0071] 혼잡 제어는 네트워크의 혼잡 상태를 파악하고, 그 상태를 해결하기 위해서 데이터 전송을 제어하는 것을 의미하는데, 여기서 혼잡 윈도우란 송출기가 응답을 받기 전에 보낼 수 있는 패킷 양을 의미한다.

[0072] 구체적으로는, d_i는 서브그래프(subgraph)인 G'로부터 추출된 주변 노드들로의 소스 노드의 거리를 의미한다.

[0073] 가까운 범위 내에 있는 사용자의 위치를 찾아 메시지 전송 등을 가능하게 해주는 스마트폰 근거리 통신기술인 비콘(beacon) 기술을 활용하여, 전송된 비콘 패킷(beacon packets) P_t 의 기록을 i번째 소스 노드가 보존할 수 있다. 또한, 패킷망(인터넷)이 패킷을 목적지에 보낼 때 패킷이 목적지에 도달하고 나서 해당 패킷에 대한 응답이 출발지로 다시 돌아오기까지의 시간을 의미하는 패킷왕복시간(round trip time, RTT)의 기록을 보존할 수 있다.

[0075] 본 발명의 일 실시예로, 혼잡 윈도우 C_w는 이용할 수 있는 데이터 대역폭(bandwidth)인 α값을 활용하여 수학

식 3에 기반하여 계산될 수 있다.

수학식 3

[0076] $$C_w = \frac{P_t}{RTT} + \frac{l_b}{\alpha}$$

[0077] 여기서 α는 데이터 대역폭으로, 일정 시간 내 데이터 연결을 통과할 수 있는 정보량의 척도를 의미한다. l_b는 소스 노드 i와 근접 노드인 j 간 링크의 대역폭의 크기를 나타낸다.

[0078] depth-first 알고리즘은 계산된 $H(c)$ 값을 활용할 수 있고, 모바일 싱크로 데이터를 전달하기 위한 최적의 솔루션을 식별할 수 있다.

[0079] 우선, 서브그래프(subgraph)인 G'을 사용하여 초기 경로에서 노드 집합인 (S, N, G)를 식별할 수 있다. 여기서, S는 소스 노드, N은 인접 노드들의 집합, G는 목표 상태를 나타낸다.

[0080] 각 노드가 방문한 지점(visited vertices)에 대한 정보를 라우팅 테이블에 유지하고, $H(c)$의 최소 값을 기준으로 순서를 유지할 수 있다.

[0081] 싱크 노드(704)의 하나인 에지 장치는 SDN 컨트롤러(708)와 통신하여 IoT 시스템에 짧은 대기 시간 서비스를 제공할 수 있다.

[0082] 상기 에지 장치는 센서의 데이터 흐름에 대해 SDN 컨트롤러(708)를 지속적으로 업데이트할 수 있고, 그에 따라 SDN 컨트롤러(708)는 라우팅 토폴로지에 대한 글로벌 테이블에 최신 정보를 유지할 수 있다.

[0083] 인텔리전트 에지를 사용하고, 정보를 수신하는 탐색 패킷을 사용하여 라우팅 경로의 재구성을 관리할 수 있다.

[0085] 본 발명의 일 실시예로, 패킷 드롭 비율이 특정 임계값을 초과하면 SDN 컨트롤러(708)는 싱크 노드(704)에 신호를 보내 대체 경로 식별을 시작하고 중복 경로로 표시할 수 있다.

[0086] 또한, 현재 경로가 센서 데이터의 데이터 흐름을 처리할 수 없을 때 백업으로 중복 경로(redundant route)는 서비스를 제공할 수 있다.

[0087] 네트워크 사용자에게는 일관되고 완전히 신뢰할 수 있는 데이터만 전달될 수 있다.

[0088] 스마트 시스템은 분산 장치 간의 효율적인 에너지 관리와 함께 품질 보증 데이터 전송 시스템을 제공할 수 있다.

[0090] **< SDN 컨트롤러를 사용한 신뢰할 수 있는 데이터 가용성 >**

[0091] 도 2에서는 edge-SDN을 이용한 스마트 통신 시스템을 위한 보안 시스템 흐름도를 나타낸다.

[0092] 구체적으로는, 본 발명에서 제안하는 IoT-SDN 아키텍처를 위한 분산 및 AI 기반 에너지 효율적 모델의 흐름도이다.

[0093] 도 2를 참고하면, 소프트웨어 정의 네트워크(Software Defined Network, SDN) 컨트롤러로 인증된 데이터만 네트워크 장치(700)를 통과시키기 위하여,

[0094] 상기 싱크 노드(704)가 비밀 키를 생성하는 단계(S202); 상기 비밀 키의 보증을 위해 상기 싱크 노드(704)가 상기 SDN 컨트롤러(708)와 통신하는 단계(S204); 및 상기 SDN 컨트롤러(708)의 검증이 완료되면, 신뢰할 수 있는 디지털 인증서의 발급을 시작하는 단계(S206);를 더 포함할 수 있다.

[0095] SDN 컨트롤러(708)는 통신 오버헤드를 줄이기 위해 고비용 컴퓨팅을 수행할 수 있다.

[0096] SDN 컨트롤러(708)는 중앙 집중식으로 네트워크 인텔리전스를 제공하고 IoT 장치를 전체적으로 관리할 수 있다.

[0097] 소프트웨어 정의 네트워크(SDN)(706)는, SDN 컨트롤러(708)를 통해 높은 수준의 신뢰와 보안을 유지하면서 외부 공격으로부터 안전하게 IoT 데이터를 처리할 수 있다.

[0099] 단계 S202 및 S204에서는, 두 가지의 보안 시스템이 작동될 수 있다.

[0100] 우선, 싱크 노드(704)가 SDN 컨트롤러(708)와 직접 연결된 경우에는, 싱크 노드(704)와 SDN 컨트롤러(708) 간에 데이터가 전송될 때도 보안 시스템이 작동할 수 있다.

[0101] 싱크 노드(704)가 SDN 컨트롤러(708)와 직접 연결되지 않은 경우에는, 가장 가까운 노드를 식별하기 위해 거리 임계값 d를 계산하여 탐색 작업을 실시할 수 있다.

[0102] 싱크 노드(704)와 임의의 노드 간에 데이터가 전송될 때 보안 시스템이 작동할 수 있다.

[0103] 상기 보안 시스템에는 RSA 알고리즘을 활용할 수 있다.

[0104] 싱크 노드(704)의 하나인 네트워크 에지(network edges) X를 신뢰할 수 있다는 전제로 i번째 센서 노드(702) n_i에 대한 초기 공유(initial share)값 Y로부터 비밀 공유(secret shares)값 k_i를 수학식 4을 기반으로 계산할 수 있다.

수학식 4

[0105] $$X \rightarrow n_i : k_i, 1 \leq i \leq t$$

[0106] 비밀 키의 안전한 전송 및 재구성을 위해서는 싱크 노드(704)와 센서 노드(702) 간에 다음 두 가지 조건이 충족되어야 한다.

[0107] (a) t 또는 서브키보다 상위 값의 조합은 비밀 키 k를 쉽게 재설정될 수 있다.

[0108] (b) t의 하위 값 또는 서브키보다 하위 값은 비밀 키 k를 재설정할 수 없다.

[0109] 싱크 노드(704)의 하나인 네트워크 에지와 센서 노드(702) 간에 비밀 키를 안전하게 전송한 후, 둘 다 암호화 함수 e를 활용하여 m_i에 대한 데이터 프라이버시를 확보할 수 있다.

[0110] 수학식 5에 기반하여 암호화 함수 e를 Xor로 연산할 수 있다.

수학식 5

[0111] $$e = m_i \bigoplus k_i$$

[0113] 본 발명의 일 실시예로, i번째 싱크 노드(704) 에지 장치 edi로부터 SDN 컨트롤러(708)로 암호화된 데이터를 전송하기 위하여, 가장 최소한의 노드의 개수를 거치는 경로 p를 계산할 수 있다.

[0114] 만약, i번째 싱크 노드(704) 에지 장치 edi가 SDN 컨트롤러(708)와 직접 연결되지 않은 경우 가장 가까운 j번째 싱크 노드(704) 에지 장치 edj를 식별하기 위해 거리 임계값 d를 탐색할 수 있다.

[0115] 수학식 6에 기반하여 상기 임계값 d를 계산할 수 있다.

수학식 6

[0116] $$if\ p^{edi-edj}(len) \leq d\ then\ route_data$$

[0118] 본 발명의 일 실시예로, 단계 S206에서, 대칭 디지털 인증서(symmetric digital certificates)를 활용하여 싱크 노드(704)와 SDN 컨트롤러(708) 간의 신뢰할 수 있는 통신을 지원할 수 있다.

[0119] 단계 S202에서, 싱크 노드(704)는 비밀 키를 생성할 수 있다.

[0120] 단계 S204에서, 싱크 노드(704)는 SDN 컨트롤러(708)와 통신할 수 있다.

[0121] 단계 S206에서, 싱크 노드(704)로부터 요청을 수신하면 SDN 컨트롤러(708)는 전역 테이블에서 ID를 확인할 수 있고, ID가 확인되면 SDN 컨트롤러(708)는 싱크 노드(704)와의 상호 신뢰를 보장하기 위해 후술하는 바와 같이 디지털 인증서 발급 프로세스를 시작할 수 있다.

수학식 7

[0122] $$req^{ed(i)-S} = ID_i, E_{is}(ID_j, D)$$

수학식 8

[0123] $$res^{S-ed(i)} = E_{js}(ID_i, D)$$

[0124] 여기서, E는 암호화를 위한 대칭 알고리즘, D는 데이터 메시지, E_{is}, E_{js}는 i번째 싱크 노드(704), j번째 싱크 노드(704), SDN 컨트롤러(708)의 각 공유 키를 나타낸다.

수학식 9

[0125] $$ed(i) \rightarrow ed(j)\ :\ E_{js}(ID_i, D)$$

[0126] 본 발명의 일 실시예로, 수학식 9와 같이 SDN 컨트롤러(708)로부터 인증서가 도달하면 인증을 받기 위하여 i번째 싱크 노드(704)는 위 인증서를 j번째 싱크 노드(704)로 반환할 수 있다.

[0128] **< 시뮬레이션 환경 >**

[0129] 본 발명의 일 실시예에 의한 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 기존 작업과의 비교를 위하여 시뮬레이션하여 검증할 수 있다. 다음과 같은 조건을 기반으로 10분에서 50분 동안 10회 시뮬레이션을 실행할 수 있다.

[0130] (a) IoT 시스템은 300m X 300m의 현장에 센서 노드(702)를 50개에서 250개까지 다양하게 무작위로 배치하여 구성될 수 있다.

[0131] (b) 싱크 노드(704)는 모바일 및 에지 장치로 고려될 수 있다.

[0132] (c) 초반 센서 노드(702)의 에너지 리소스는 2J로 설정될 수 있다.

[0133] (d) 패킷 크기는 20바이트이고, 전송 범위는 5m로 설정될 수 있다.

[0134] (e) 다양한 악성 장치를 수반하는 SDN 컨트롤러(708)를 배포할 수 있다.

[0135] (f) 오픈 소스 컨트롤러인 ONOS(Open Net work Operating System)를 사용할 수 있다.

[0136] 표 1은 시뮬레이션 파라미터를 나타낸다.

표 1

[0137]

Parameter	Value
Sensors	50–250
Deployment	Random
Sink nodes	5
Network diameter	300 m × 300 m
Transmission range	5 m
Initial energy	2 J
Packet size	20 bytes
Malicious devices	3–15
Time intervals	10–50 min

[0138] 표 2는 악성 공격 및 이에 대한 보안 절차를 나타낸다.

표 2

[0139]

Security attacks	Procedures
Device authentication	Unique ID Session keys
Sensors to edges security	Encryption keys
Edges to SDN security	Digital certificates
Privacy	Xor between messages and keys
Edges verification	Using SDN global table
Indirect routes	Computing distance threshold
Identification of malicious nodes	Invalid secret share
Mutual trust	Exchanging verified digital certificates

[0140] 표 2에서는, 인증, 데이터 프라이버시, 악의적인 노드 탐지 및 상호 신뢰 측면에서 제안된 대책뿐만 아니라 수많은 보안 문제를 확인할 수 있다.

[0141] 본 발명의 일 실시예로, 제안된 보안 절차는 장치의 인증을 보장하기 위해 고유 ID 및 세션 키를 이용할 수 있다. 디지털 인증서와 상호 보장 신뢰를 탐색하여 에지-SDN 통신을 보호하는 효율적인 방법을 제공할 수 있다.

[0142] 본 발명의 일 실시예로, 제안된 보안 전략은 암호화 키를 사용하여 데이터 프라이버시를 보호하고 데이터 비트에 대해 Xor 연산을 수행하여 암호화된 코드를 생성할 수 있다.

[0143] 본 발명의 일 실시예로, 싱크 노드(704)의 하나인 네트워크 에지에서 생성된 비밀 공유를 확인할 수 있다. 임의의 노드에서 유효하지 않은 비밀 공유가 발견된 경우 해당 노드는 결함이 있고 인증되지 않은 것으로 표시될 수 있다.

[0145] **에너지 소비 측면**

[0146] 본 발명의 일 실시예로, 에너지 소비 측면에서 기존 솔루션 대비 제안 모델의 성능을 평가할 수 있다.

[0147] 도 3a 및 도3b에서는 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법과 기존 솔루션의 비교를 나타낸 것으로, 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법의 에너지 활용 효율이 평균 28%, 15% 향상되는 것을 관찰할 수 있다.

[0148] 센서 노드(702) 수가 증가함에 따라 에너지 소비율도 증가하는 것으로 나타났습니다.

[0149] 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 최소한의 제어 메시지와 재전송으로 인해 IoT 시스템의 에너지 소비 균형을 맞추고 전체 수명을 늘릴 수 있다.

[0150] 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 관리 가능한 통신 비용으로 모바일 싱크 노드(704)를 이용한 효율적인 전력 분배 시스템을 지원할 수 있다.

[0151] 또한 네트워크 에지에서 AI 접근 방식을 통합하여 통신 장치의 관리 부하와 비용을 낮출 수 있다. 제안된 모델은 라우팅 프로세스에서 혼잡 창을 탐색하여 중복 경로를 생성하여, 중요한 상황에서 통신 시스템의 응답 대기 시간을 줄일 수 있다.

[0153] **End-to-End 지연 측면**

[0154] 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법과 기존 솔루션 대비 제안 모델의 성능을 End-to-End 지연 측면에서 평가할 수 있다.

[0155] 도 4a 및 도 4b에서는, 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법과 기존 솔루션에 대한 비교를 나타낸다.

[0156] 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 대기 시간을 각각 49%, 26% 감소시키는 것으로 나타났다. 이는 싱크 노드(704)가 SDN 컨트롤러(708)와 통합되어 전송 성능이 향상되기 때문이다.

[0157] 라우팅 노드를 재평가함으로써 모바일 장치는 IoT 시스템에서 데이터를 수집하기 위한 반응 시간을 줄이고 효율적으로 무선 채널을 처리할 수 있다.

[0158] 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법의 보안 시스템은 악의적인 장치가 잘못된 전환 메시지를 보내는 것을 방지하고 통신 네트워크에서 비인증 데이터 트래픽을 낮출 수 있다.

[0160] **네트워크 처리량 측면**

[0161] 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 주된 지연율과 관련한 가장 중요한 작업에 대한 응답 시간을 증가시킬 수 있다.

[0162] 도 5a 및 도 5b에서는, 네트워크 처리량 측면에서 기존 솔루션에 대한 제안 모델의 성능 평가를 나타낸다.

[0163] 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 다양한 센서 및 시간 간격에서 네트워크 처리량을 15% 및 18% 크게 증가시키는 것을 볼 수 있다. IoT 시스템 모니터링을 위해 SDN 컨트롤러(708)를 활용하고 포워더 간의 에너지 분배를 효율적으로 관리하기 때문이다.

[0164] 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 라우팅 상태는 SDN 컨트롤러가 네트워크의 불확실한 상황을 인식할 때마다 업데이트될 수 있다.

[0165] 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 패킷 및 혼잡 창 정보를 계산하여 통신 채널 링크가 식별될 때마다 라우팅 상태를 재평가할 수 있다.

[0166] 라우팅 상태는 AI 기술을 지원하는 특정 기준에 따라 다시 계산될 수 있다.

[0167] 경량 컴퓨팅 기능은 센서의 오버헤드를 줄일 뿐만 아니라 모바일 에지의 인텔리전스를 사용하여 높은 데이터 수신률을 제공할 수 있다.

[0169] **패킷 드롭 비율 측면**

[0170] 도 6a 및 도 6b에서는, 패킷 드롭 비율 측면에서 다양한 센서 수와 다양한 시간 간격에 대한 제안된 모델의 성능 평가를 나타낸다.

[0171] 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 결함이 있는 장치가 있는 경우, 임계값 공유 방식과 비밀 키를 사용하는 장치의 상호 인증 때문에 악성 트래픽 탐지율을 각각 44%, 37% 만큼 감소시킬 수 있다.

[0172] 디지털 인증서와 비밀 키는 악의적인 장치의 적시 검증을 지원하고 스마트 네트워크 통신 시스템의 데이터 가용성을 확보할 수 있다.

[0173] 모바일 싱크 노드(704)는 보다 강력하며 IoT 네트워크에서 오는 센서 데이터에 대한 감독자 역할을 할 수 있다.

[0174] 적절한 인증 후 수집된 데이터는 SDN 컨트롤러(708)의 인텔리전스를 통해 애플리케이션 사용자에게 전달될 수 있다.

[0175] 본 발명 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법은 대부분의 이전 작업과 달리 향상된 지연 성능과 보안 라우팅을 통한 성공적인 전송 속도를 제공할 수 있다.

[0176] 악의적인 행동이 있더라도 네트워크 장치는 상호 인증을 위해 비밀 공유를 사용하고 안전한 환경을 제공할 수 있다.

[0177] 스마트 개체에 대한 실시간 데이터 수집 및 처리를 가능하게 하여 친환경적이고 효율적인 시스템을 구축할 수 있다.

부호의 설명

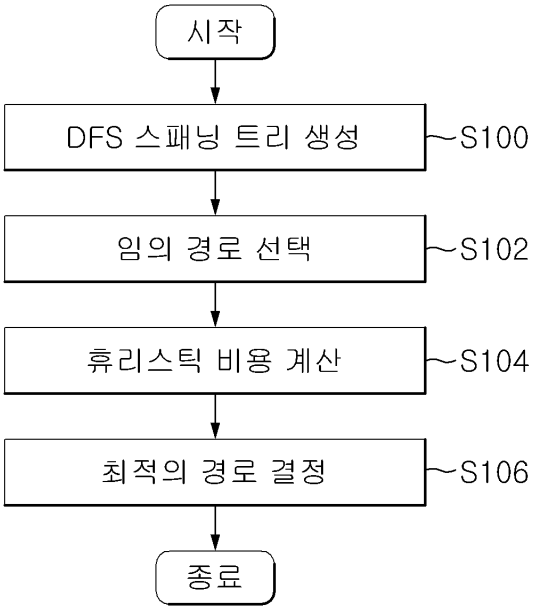
[0179] 700 : 사물인터넷(IoT)을 위한 인공지능 기반 에너지 절약 모델 제공 방법이 수행될 수 있는 네트워크 장치

702 : 센서 노드 704 : 싱크 노드

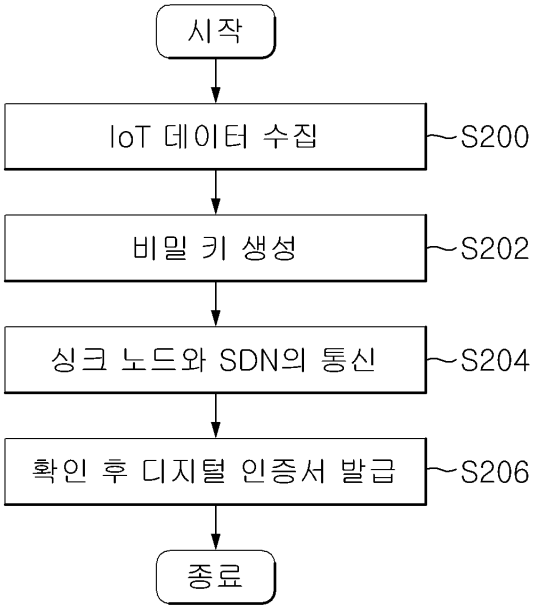
706 : SDN 708 : SDN 컨트롤러

도면

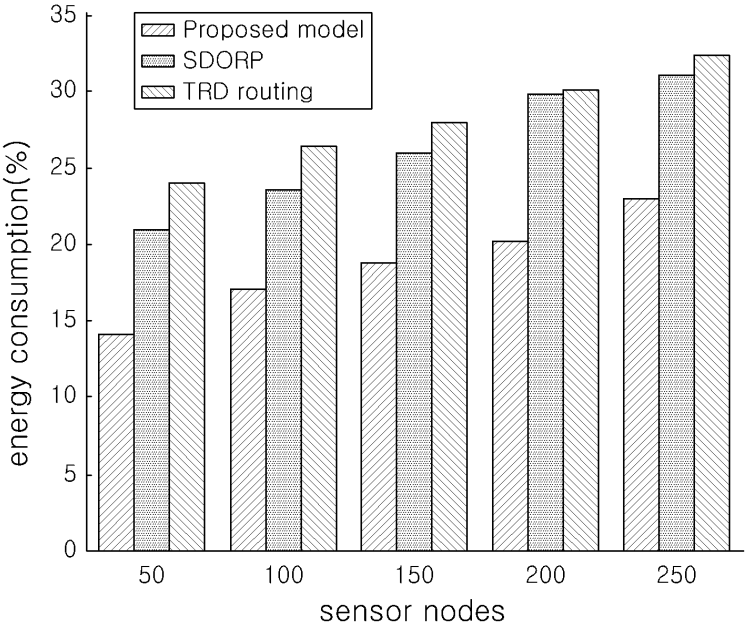
도면1



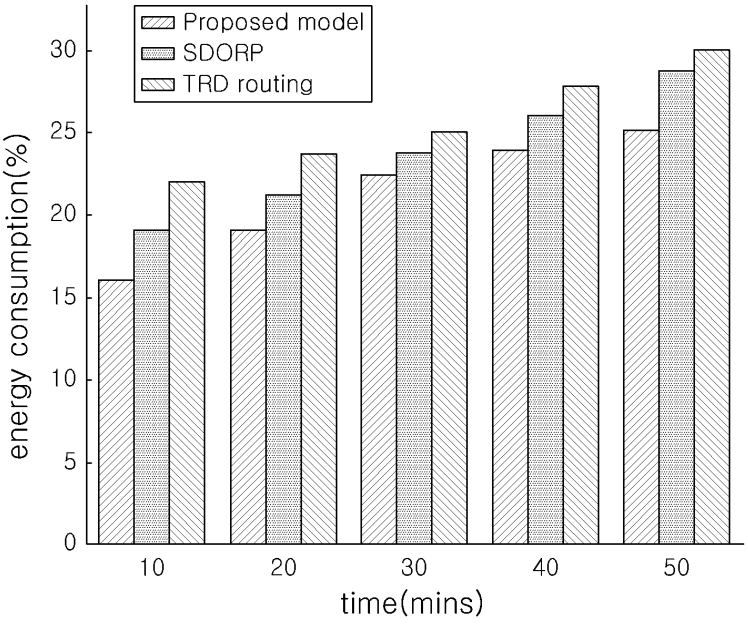
도면2


시작
IoT 데이터 수집
S200
비밀 키 생성
S202
싱크 노드와 SDN의 통신
S204
확인 후 디지털 인증서 발급
S206
종료

도면3

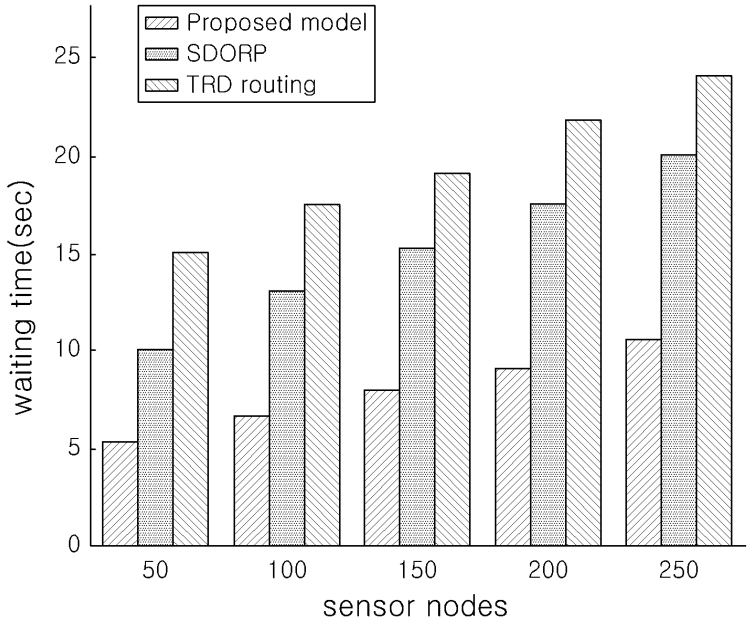

Proposed model
SDORP
TRD routing
energy consumption(%)
0
5
10
15
20
25
30
35
50
100
150
200
250
sensor nodes

(a)

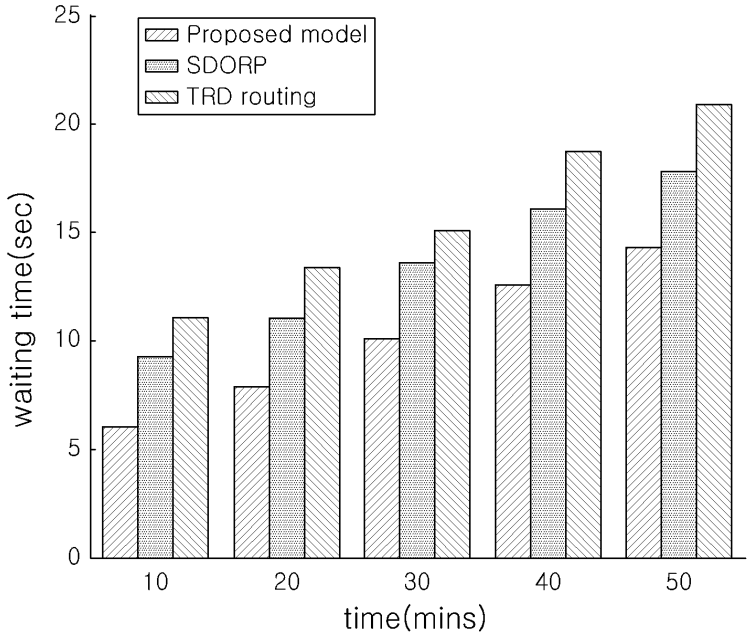

Proposed model
SDORP
TRD routing
energy consumption(%)
0
5
10
15
20
25
30
10
20
30
40
50
time(mins)

(b)

도면4

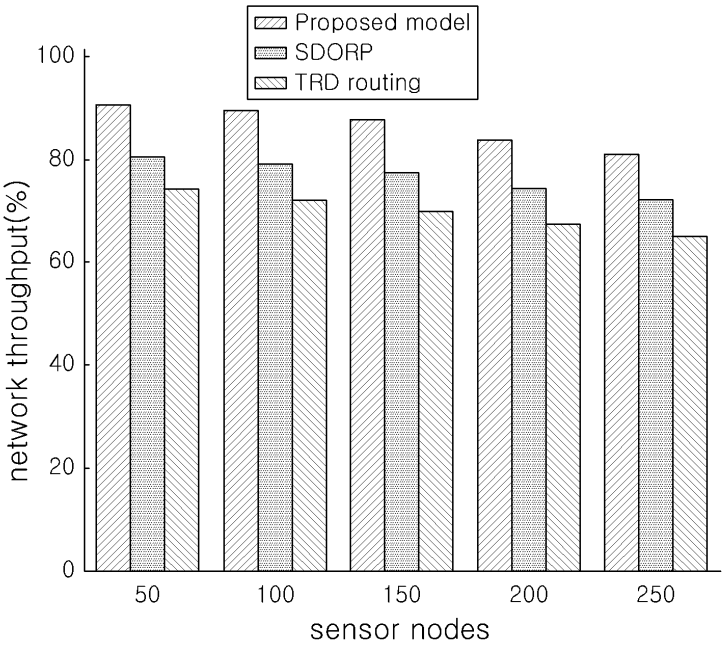

Proposed model
SDORP
TRD routing
waiting time(sec)
0
5
10
15
20
25
50
100
150
200
250
sensor nodes

(a)

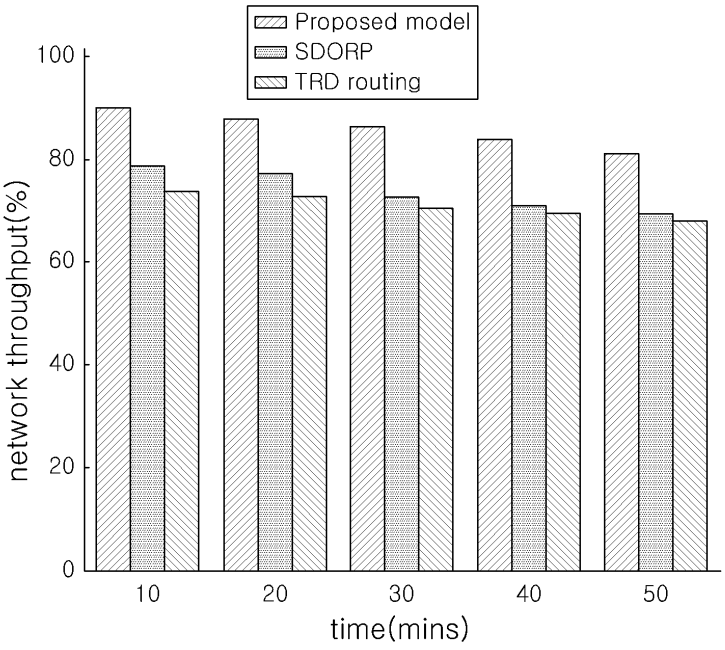

Proposed model
SDORP
TRD routing
waiting time(sec)
0
5
10
15
20
25
10
20
30
40
50
time(mins)

(b)

도면5

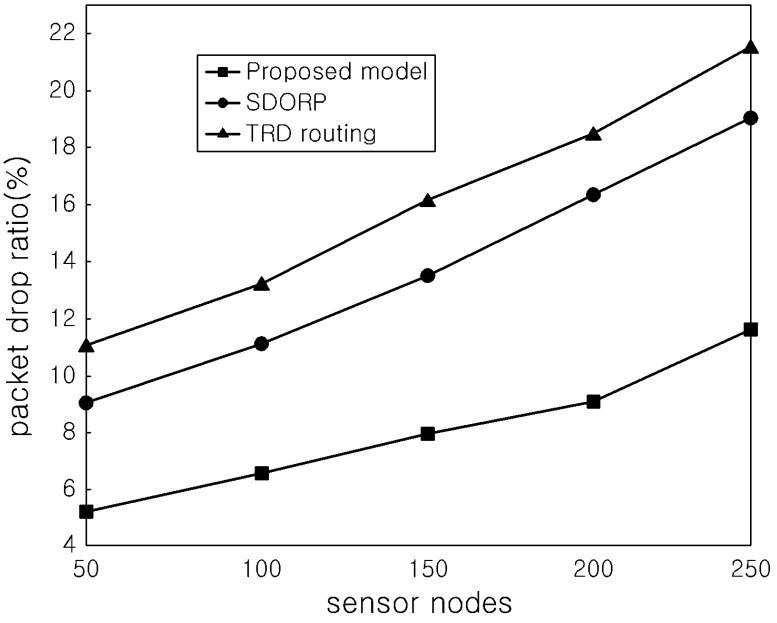

Proposed model
SDORP
TRD routing
network throughput(%)
100
80
60
40
20
0
50
100
150
200
250
sensor nodes

(a)

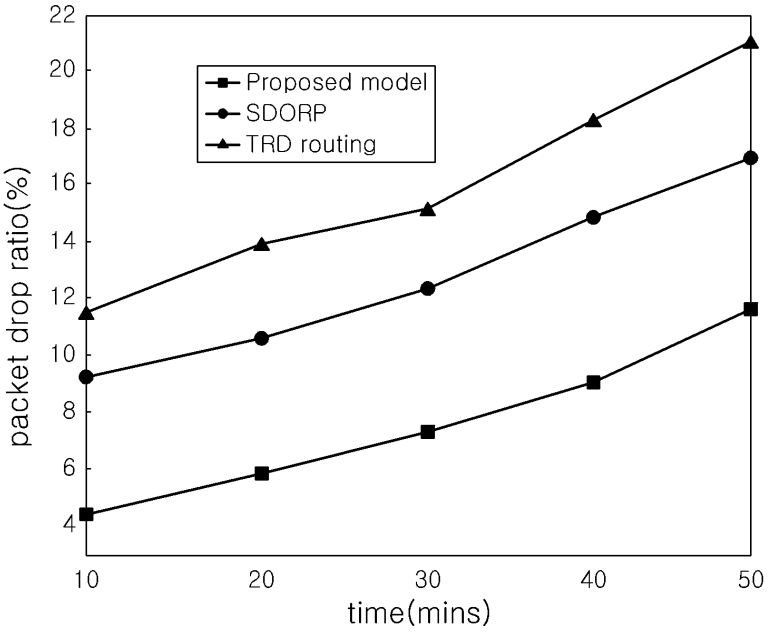

Proposed model
SDORP
TRD routing
network throughput(%)
100
80
60
40
20
0
10
20
30
40
50
time(mins)

(b)

도면6

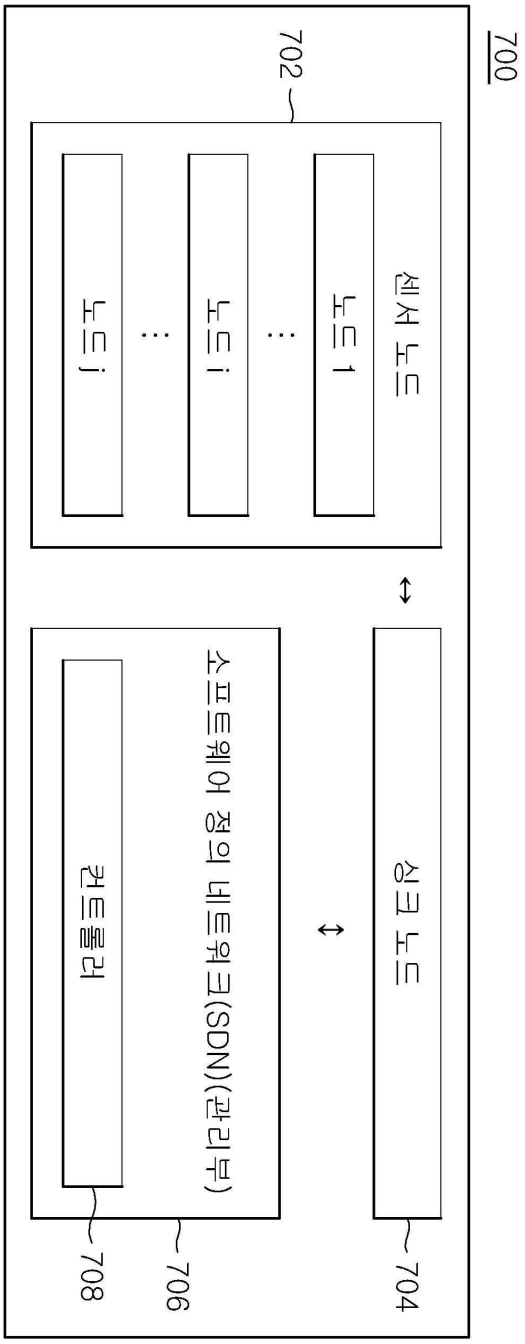

Proposed model
SDORP
TRD routing
packet drop ratio(%)
22
20
18
16
14
12
10
8
6
4
50
100
150
200
250
sensor nodes

(a)


Proposed model
SDORP
TRD routing
packet drop ratio(%)
22
20
18
16
14
12
10
8
6
4
10
20
30
40
50
time(mins)

(b)

도면7


700
702
센서 노드
노드 1
노드 i
노드 j
싱크 노드
704
소프트웨어 정의 네트워크(SDN)(관리부)
706
컨트롤러
708