클러스터 기반 센서 네트워크를 위한 효율적 라우팅 메커니즘

도인실, 채기준
이화여자대학교
isdoh@ewha.ac.kr, kijchae@ewha.ac.kr

Efficient routing mechanism for secure sensor network communication
Inshil Doh, Kijoon Chae
Ewha Womans University

요 약

센서 네트워크는 다양한 응용에 적용될 수 있는 장점을 가지고 있지만 기존의 라우팅 메커니즘을 그대로 적용할 수 없어서 센서 네트워크의 적합한 새로운 라우팅 프로토콜들이 많이 제안되고 있다. 그러나 대부분의 경우 보안성을 고려하지 못하였다는 문제점을 보였다. 본 연구에서는 센서 네트워크의 특성과 클러스터 기반의 구조를 고려하여 각 클러스터에 3차원 좌표를 할당하여 클러스터화한 센서의 최적값을 이용하여 목표지정의 라우팅 경로를 동적으로 구한다. 또한 보안을 제공하기 위한 방안으로 모션에 적합한 포스트를 두어 이 지초에서 데이터의 인위적 유출을 방지하는 데 걸려있다. 정보가 네트워크 상에서 계속 퍼져나가는 경우를 방지한다. 제안 메커니즘은 효율적인 라우팅을 제공하고 동시에 보안 기능을 수행함으로써 보안성을 강화하였다.

1. 서 론

항후 우림의 사회가 유비쿼터스 컴퓨팅 환경으로 바뀌는 것으로 예상되는 가운데 핵심 기술로서의 센서 네트워크에 대한 관심이 점차 높아지고 있다. 센서 네트워크는 굴착, 환경, 의료 등 다양한 분야의 적용에 유용하게 사용될 수 있으나, 현재선 연구에서, 물리적, 환경, 해양, 지정 농장 등의 제약으로 인해 기존의 라우팅 메커니즘을 그대로 적용시키기 어렵다. 이를 고려하여 센서 네트워크를 위한 다양한 라우팅 프로토콜들이 제안되어왔다. 대부분의 경우 여러 단계의 최적화와 최적화된 라우팅에 초점을 맞추어 보안은 비선상 간과되는 경우가 많다. 그러나 센서 네트워크의 경우 특히 보안성 측면에서의 경제성에 대한 고려가 많지 않은 클러스터도 주로 데이터를 전송하고 기능적으로 이를 다시 포함하는 형태로 라우팅이 이루어진다. 각각의 분야에 대한 대표적인 라우팅 기법을 알아보면 다음과 같다.

2. 관련 연구

지급까지 다양한 센서 네트워크 라우팅 프로토콜들이 제안되어 왔으나 이를 분류별 분류방법도 여러 가지가 있을 수 있지만 본 연구에서는 크게 공간 라우팅과 구조 라우팅으로 분류하고자 한다. 본 연구에서 제안된 라우팅 메커니즘은 구조 라우팅에 속한다. 즉, 네트워크를 클러스터화한 후 이벤트를 감지한 센서 노드들이 클러스터 단위로 데이터를 전송하고 기능적으로 이를 다시 포함하는 형태로 라우팅이 이루어진다. 각각의 분야에 대한 대표적인 라우팅 기법을 알아보면 다음과 같다.


분 논문의 구성은 다음과 같다. 2장에서 관련 연구에 대해 간단히 알아보고 3장에서 제안하는 안정적인 라우팅 메커니즘에 대하여 기술한다. 4장에서는 보안성에 대하여 간단하게 서술하고 5장에서 결론을 얻고 6장에서 연구 방향에 대하여 기술한다.
포항한 새로운 ADV 메시지를 다시 브로드캐스트하는 방식이다. 근원지 노드가 데이터를 보내려 할 때 먼저 이를 브로드캐스트하면 비용감을 비롯하여 조건에 부합하는 노드만 다시 브로드캐스트함으로써 불필요한 트래픽을 줄였다.

구조적 라우팅 방식 앞에서 언급한 바와 같이 클러스터 기반
라우팅 프로토콜이라고도 불리며 대표적으로 [5][6][7][8][9]
등이 있다. 이는 먼저 비트워크를 클러스터링한 후 각 클러스터마다 존재하는 클러스터가 데이터를 수신한 후 베이스 스트레이싱이나 상위 레이어의 클러스터헤드에게 전송하는 방식이다.

LEACH[9]는 대표적인 구조 라우팅 방식으로 클러스터헤드의 역할을 각 센서 노드들이 변할 수 가며 수행할 수 있는 노드간의 에너지 소비를 균등하게 하는 방식이다. 이는 동적 클러스터헤드를 사용함으로써 일부 선택된 클러스터헤드들이 에너지가 고갈되는 현상을 줄이고 확장성을 증진시켰다. 이 방식은 또한 정보의 양을 줄이기 위해 데이터 전송 방식을 차례로 했다.


중성위체로 확장의 체인을 따라 데이터가 전송되면 노드는 자신이 가진 데이터와 정보를 기반으로 작동한다. 그 밖에도 많은 라우팅 프로토콜이 제안되어 있다.

3. 제안 메커니즘
3.1 기본 가정
제안하는 메커니즘의 기본 가정은 다음과 같다.

- 센서 네트워크는 6각형의 클러스터로 사전에 클러스터링 된 다.
- 각 클러스터에는 클러스터헤드가 존재하며 엠בר 노드들로부터 받은 정보를 수집하여 새로운 형태의 패킷을 만들어 목적지로 노드들 전송한다.
- 클러스터헤드는 일반 노드들에 비해 에너지와 계산 능력이 뛰어난다.
- 각 클러스터헤드는 다른 클러스터헤드와의 pairwise 키를 통


3.2 기본 메커니즘
그림 1에와 같이 각 클러스터는 6각형의 클러스터로 사전에 클러스터링되어 각 클러스터는 3차원 좌표 (x,y,z)를 갖는다. 이 좌표값을 이용하여 각 클러스터 내의 클러스터헤드가 목적지의 라우팅 경로를 결정함으로써 클러스터 내에서는 기본적으로 브로드캐스트 방식으로 데이터가 전송된다. 각 클러스터가 다음 클러스터로 전달할 수 있는 경우는 그림 2와 같이 이 가소화 기반은 체인의 형태로 존재하며 클러스터 메시지로 전송됨으로써 클러스터 내에는 클러스터헤드가 자신의 위치를 클러스터로부터 모든 다른 클러스터로 전달하는 메커니즘과 기반의 정보를 찾기 위해서 사용하는 위치 정보를 알고 있는 그룹 3과 같다.

즉, 근원지 클러스터의 목적지 클러스터의 동일한 x축 상에 있는 경우 그림 2의 규칙에 따라 목적지로 이동하며, 목적지로 기존으로 1사분면 혹은 2사분면에 위치하는 경우 목적지와 동일한 z축에 존재하는 클러스터를 찾고 해당 클러스터에서부터 그림 2의 규칙에 따라 이동하며, 2사분면 혹은 4사분면에 위치 하는 경우 목적지와 동일한 y축상에 존재하는 클러스터를 찾고 이 클러스터에서부터 그림 2의 규칙에 따라 이동한다. 만일 1,2 혹은 3,4 사분면의 경계선 상에 위치하는 경우 랜덤으로 한쪽을 선택한다.

3.3 보안 수준을 향상시키기 위한 방안
근원지 클러스터헤든의 목적지로 가는 경로 상에서 적절한 위치

의 클러스터헤드를 포스트로 설정하는데, 이는 해당 클러스터헤드와의 pairwise 키를 이용하여 아 카로 MAC을 사용하여 메시지를 보안이 위장된다. 알고리즘에서 포스트를 설정하는 부분을 보면 먼저 2번 단계에서 동일 y축, 혹은 동일 z축을 찾아 해당 위치의 클러스터를 포스트로 설정할 수 있다. 그 다음 단계에서는 상황에 따라 적절한 키의 포스트를 임의로 선택한다. 근원지 클러스터로부터 목적지 클러스터로의 거리가 멀어지면 이에 비해하여 몇몇 많은 수의 포스트가 설정될 것이다. 특히 포스트를 임의로 설정함으로써 외부의 공격자가 이를 예상하여 다처할 수 없도록 하는 장점을 갖는다.
3. 경로 선택 알고리즘

4. 효율성 분석
재난 메커니즘의 가장 큰 장점은 각 클러스터나 센서 노드가 사전에 결정된 라우팅 정보를 노드 내에 저장하지 않음으로써 경제적 효과를 얻을 수 있다는 점이다. 본 문단에서는 어떤 장치를 점검하는 것이 가장 효율적일지에 대해 논의할 것이다. 또한 실제 상황에서 사용하는 것을 후보로 평가하는 노드의 메커니즘 고려할 때 비트워크의 수명을 단축시킬 수 있으나 재난 메커니즘을 최적의 경로를 찾는 대신 상황에 따라 조절할 수 있는 다른 경로를 제공함으로써 일부 노드의 효율적 메커니즘 오류를 줄일 수 있다는 장점을 갖는다. 본 문단에서는 경제기간을 보장하기 위한 방법으로 제시한 포스트 설정 방식을 사용한 경우에 따라 클러스터링 및 pairwise 기반 MAC을 사용하여 추가적으로 중간 경로를 메커니즘을 갱신함으로써 트래픽을 조절할 기능을 갖는다.

오버헤드를 줄이기 위해 포스트 개수를 고려할 경우 MAC의 제거와 검증이 필요하다. 한 가지의 MAC 검증에는 1바이트를 검증하는 정도의 메커니즘을 포함할 수 있다. 또한 목적지 노드로 전송되는 패킷에 포스트 개수만큼의 MAC이 포함되는 만큼의 전송이 요구되지만 클러스터링 기반의 MAC의 크기가 크지 않을뿐 아니라 MAC의 검증을 통해 위치 변위에 따른 메커니즘의 갱신을 충분히 가능하다 할 수 있다.

5. 결론 및 향후 연구 방향
본 연구에서는 센서 비트워크를 위한 클러스터 기반의 네트워크 구조를 제시하고 이 구조에 기반한 효율적인 동적 라우팅 메커니즘을 제시하였다. 특히, 효율성 뿐 아니라 보안성을 강화하기 위해 각 클러스터화가 라우팅 경로 중간에 포스트 위치를 결정하여 이 위치에서 근거리 클러스터화와 포스트 클러스터화 간의 pairwise 키를 이용한 MAC를 추가하고 이를 결정함으로써 데이터의 전송을 암호화 하여 데이터가 외부로부터의 공격에 의한 해킹을 방지하는 것과의 브로크 내에서 발생한 트래픽을 압박하게 하지 않도록 하였다.

향후 연구로는 정밀도 라우팅 메커니즘에 대한 시뮬레이션을 수행하여 기존에 제안된 메커니즘과 비교를 통한 효율성을 입증할 계획이 있으며 단일 내부, 혹은 외부로부터의 공격에 대한 분석을 추가하여 이에 대응할 수 있는 공격 탐지 및 방지 방안을 제안하고자 한다.

Acknowledgement
본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 융성-지원사업의 연구결과로 수행되었음.

6. 참고 문헌