클러스터 기반 센서 네트워크를 위한 효율적 라우팅 메커니즘

도인실° 채기준
이화여자대학교
isdoh@ewhain.net°, kjchae@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 가지는 반면 기본적인 제약으로 인해 기존의 라우팅 메커니즘을 그대로 적용할 수 없어 센서 네트워크에 적합한 새로운 라우팅 프로토콜들이 많이 제안되었다. 그러나 대부분의 경우 안전성을 고려하지 못하였다는 문제점을 갖는다. 본 연구에서는 센서 네트워크를 육각형의 클러스터 기반의 구조로 정의하고 각 클러스터에 3차원 좌표를 할당하여 클러스터헤드가 이 좌표값을 이용하여 목적지로의 라우팅 경로를 동적으로 찾는다. 또한 보안을 제공하기 위한 방안으로 중간에 적절한 포스트를 두어 이 지점에서 데이터의 진위를 파악하여 잘못된 정보를 걸러줌으로써 잘못된 정보가 네트워크 상에서 계속 트래픽을 증가시키는 것을 방지한다. 제안 메커니즘은 효율적인 라우팅을 제공함과 동시에 보안 기능을 수행함으로써 보안성을 강화하였다.

1. 서 론

향후 우리의 사회가 유비쿼터스 컴퓨팅 환경으로 나아갈 것으로 예상되는 가운데 핵심 기술로서의 센서 네트워크에 대한 관심이 점차 높아가고 있다. 센서 네트워크는 군사, 환경, 의료 등 다양한 분야에 적용되어 유용하게 사용될 수 있으나 한정된 에너지, 관리의 어려움, 계산이나 저장 능력 등의 제약으로 인해 기존의 라우팅 메커니즘을 그대로 적용시키기 어렵다. 이를 고려하여 센서 네트워크를 위한 다양한 라우팅 프로토콜들이 제안되어왔으나 대부분의 경우 에너지 효율이나 최적화된 라우팅에 초점이 맞추어져 보안은 사실상 간과되는 경우가 많았다. 그러나 센서 네트워크의 경우 특히 보안상 취약한 지역에 배치되는 경우가 많아 일반 네트워크보다도 더욱 보안이 보장되지 않으면 그 목적을 이룰 수 없다. 이에 본 연구에서는 효율적인 네트워킹을 위해 네트워크 클러스터 구조를 정의하고 이 구조에 기반하여 동적인 라우팅 메커니즘을 제시함으로써 공격자에 의한 라우팅 경로 노출 가능성을 줄이고 라우팅 경로 저장을 위한 저장장소를 절약할 수 있는 방안을 제시하였다. 뿐만 아니라 추가적으로 보안을 강화하기 위한 방안으로 메커니즘에 따른 라우팅 경로의 일정 지점에서 MAC 값을 체크하여 잘못된 정보를 걸러줌으로써 안전성을 보완한 라우팅을 제안하였다. 제안하는 라우팅 메커니즘은 언제나 최적의 경로를 찾는 것은 아니지만 고정된 경로를 저장하지 않음으로써 경로 노출의 위험을 줄일 뿐 아니라 경로상의 노드들이 지나치게 에너지를 소비함으로써 전체적인 네트워크 수명을 단축시킬 가능성을 더욱 줄일 수 있다는 장점을 갖는다.

본 논문의 구성은 다음과 같다. 2장에서 관련 연구에 대해 간단히 알아보고 3장에서 제안하는 안전한 라우팅 메커니즘에 대하여 기술한다. 4장에서는 효율성에 대하여 간략하게 서술하고 5장에서 결론을 맺고 향후 연구 방향에 대하여 기술한다.

2. 관련 연구

지금까지 다양한 센서 네트워크 라우팅 프로토콜들이 제안되어 왔다. 이들을 분류하는 방법도 여러 가지가 있을 수 있지만 본문에서는 크게 평면 라우팅과 구조 라우팅으로 분류하도록 한다. 본 연구에서 제안된 라우팅 메커니즘은 구조 라우팅에 속한다. 즉, 네트워크를 클러스터링한 후 이벤트를 감지한 센서 노드들이 클러스터 단위로 데이터를 전송하고 기능적으로 이들을 다시 취합하는 형태로 라우팅이 이루어진다. 각각의 분류에 대하여 대표적인 라우팅 기법을 알아보면 다음과 같다.

먼저 평면 라우팅 기법은 각 센서 노드들이 동등한 자격으로 라우팅 메커니즘에 참여하는 방식이다. 대표적인 연구로 [1][2][3][4] 등이 있는데 먼저 SPIN[1] 방식에서는 모든 센서 노드들을 센싱하는 주체인 동시에 베이스 스테이션의 역할을 할 수 있는 노드로 본다. 각 노드는 메타데이터를 가지고 있어 실제 데이터를 전송하기 전에 메타데이터 협상 단계를 거친다. 이러한 방식으로 네트워크상에 중복된 데이터가 전송되는 것을 막는 방법이다. 최소비용전송(Minimum cost forwarding) 방법[2]는 베이스 스테이션이 자신의 비용을 포함한 ADV 메시지를 이웃 노드에게 먼저 브로드캐스트하면 이를 받은 노드들이 타이머를 세팅하고 타이머가 소진되면 비용을 새로운 값으로 바꾼 후 이 값을

포함한 새로운 ADV 메시지를 다시 브로드캐스트하는 방식이다. 근원지 노드가 데이터를 보내려 할 때 먼저 이를 브로드캐스트하면 비용값을 비교하여 조건에 부합하는 노드만 다시 브로드캐스트함으로써 불필요한 트래픽을 줄인다.

구조적 라우팅 방식은 앞에서 언급한 바와 같이 클러스터 기반 라우팅 프로토콜이라고도 불리며 대표적으로 [5][6][7][8][9] 등이 있다. 이는 먼저 네트워크를 클러스터링한 후 각 클러스터마다 존재하는 클러스터가 데이터를 수집한 후 베이스 스테이션이나 상위 레이어의 클러스터헤드에게 전송하는 방식이다. LEACH[9]는 대표적인 구조 라우팅 방식으로 클러스터헤드의 역할을 각 센서 노드들이 번갈아 가며 수행함으로써 센서 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 퓨전 방식을 채택하였다. Power-Efficient Gathering in Sensor Information Systems (PEGASIS)[6]는 LEACH 방식을 이용한 체인 기반 프로토콜로서 각 노드들이 다른 노드의 위치를 알고 있다는 가정 하에 체인이 형성되며 체인을 따라 데이터가 전송되면 노드는 자신이 가진 데이터와 퓨전시키는 과정을 거친다. 그 밖에도 많은 라우팅 프로토콜이 제안되어왔다.

3. 제안 메커니즘

3.1 기본 가정

제안하는 메커니즘의 기본 가정은 다음과 같다.

- 센서 네트워크는 6각형의 클러스터로 사전에 클러스터링 된다.
- 각 클러스터에는 클러스터헤드가 존재하며 멤버 노드들로부터 받은 정보를 수집하여 새로운 형태의 패킷을 만들어 목적지 노드로 전송한다.
- 클러스터헤드는 일반 노드에 비해 에너지와 계산 능력이 뛰어나다.
- 각 클러스터헤드는 다른 클러스터헤드와의 pairwise 키를 동적으로 계산할 수 있는 키 정보를 사전에 분배받는다. 본 연구에서는 Blom의 스킴[10]을 기반으로 하였다.

3.2 기본 메커니즘

그림 1에서와 같이 각 클러스터는 6각형의 클러스터로 사전에 클러스터링되며 각 클러스터는 3차원 좌표 (x,y,z)를 갖는다. 이 좌표값을 이용하여 각 클러스터 내의 클러스터헤드가 목적지로의 라우팅 경로를 동적으로 찾으며 클러스터 내에서는 기본적으로 브로드캐스트 방식으로 데이터가 전송된다. 각 클러스터가 다음 클러스터로 지정할 수 있는 경우는 그림 2와 같이 6가지 경우가 존재하며 목적지로부터 자신의 상대적 위치에 따라 6가지 경우 중에 다음 이동 클러스터를 선택하여 이 정보를 목적지로 전송하는 패킷 내에 포함시킨다. 클러스터헤드가 자신이 위치한 클러스터로부터 목적지의 좌표로 가는 경로를 찾기 위해 사용하는 경로 탐색 알고리즘은 그림 3과 같다.

즉, 근원지 클러스터가 목적지 클러스터와 동일한 x 축 상에

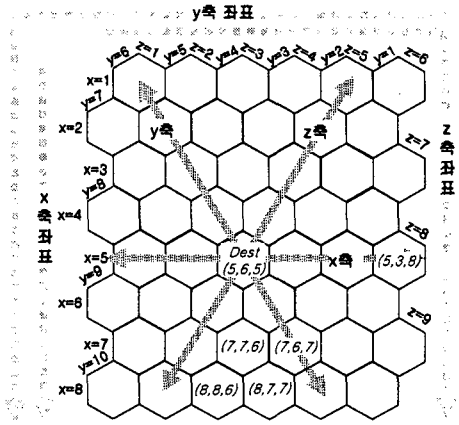

그림 1 네트워크 클러스터링 및 3차원 좌표

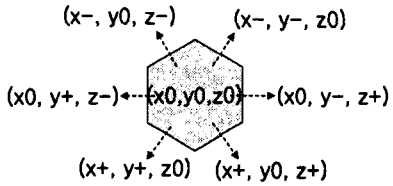

그림 2 좌표값 변환 규칙

있는 경우 그림 2의 규칙에 따라 목적지로 이동하며, 목적지를 기준으로 1사분면 혹은 3사분면에 위치하는 경우 목적지와 동일한 z축에 존재하는 클러스터를 찾고 해당 클러스터에서부터 그림2의 규칙에 따라 이동하며, 2사분면 혹은 4사분면에 위치하는 경우 목적지와 동일 y축상에 존재하는 클러스터를 찾고 이 클러스터에서부터 그림 2의 규칙에 따라 이동한다. 만일 1,2 혹은 3,4 분면의 경계선 상에 위치하는 경우 임의로 한쪽을 선택한다.

3.3 보안 수준을 향상시키기 위한 방안

근원지 클러스터헤드는 목적지로 가는 경로 상에서 적절한 위치의 클러스터헤드를 포스트로 설정하는데, 이는 해당 클러스터헤드와의 pairwise 키를 이용하여 이 키로 MAC을 생성하여 패킷에 붙이기 위함이다. 알고리즘에서 포스트를 설정하는 부분을 보면 먼저 2번 단계에서 동일 y축, 혹은 동일 z축을 찾아 해당 위치의 클러스터를 포스트1로 설정함을 볼 수 있다. 그 다음 단계에서는 상황에 따라 적절한 개수의 포스트를 임의로 선택한다. 근원지 클러스터로부터 목적지 클러스터로의 거리가 멀면 이에 비례하여 좀더 많은 수의 포스트가 설정될 것이다. 특히 포스트를 임의로 설정함으로써 외부나 내부의 공격자가 이를 예상하여 대처할 수 없도록 하는 장점을 갖는다.

```
Source : (x,y,z), Destination : (x',y',z')
1.If x=x' then
    if y<y' then (y++ and z--)
                until(y=y' and z=z')
    else if y>y' then (y-- and z++)
                until(y=y' and z=z')
    select posts randomly on the way
2. Else if x!=x' then
    2.1 if (x,y,z) is in 1'st or 3'rd quarter from
        (x',y',z') then
      2.1.1 find a cluster on the same z axis as
        (x',y',z') with closer y value
      2.1.2 set the cluster as the post1
      2.1.3 move toward (x',y',z')
      2.1.4 select posts randomly on the way
    2.2 else if (x,y,z) is in 2'nd or 4'th quarter
        from (x',y',z') then
      2.2.1 find a cluster on the same z axis as
        (x',y',z') with closer y value
      2.2.2 set the cluster as the post1
      2.2.3 move toward (x',y',z')
      2.2.4 select posts randomly on the way
    2.3 else if (x,y,z) is on the border line
        between (1'st and 2nd) or (3'rd and 4'th)
      then randomly select 2.1 or 2.2
```

그림 3 경로 선택 알고리즘

4. 효율성 분석

제안 메커니즘의 가장 큰 장점은 각 클러스터나 센서 노드가 사전에 결정된 라우팅 정보를 노드 내에 저장하지 않음으로써 공격자가 어떤 경로로 이동할지 예측하기 힘들다는 점이다. 뿐만 아니라 이는 저장 공간을 절약한다는 추가적인 장점을 갖는다. 또한 정해진 경로를 반복해서 사용하는 경우는 라우팅 기능을 해주는 노드의 에너지 고갈을 앞당겨 네트워크의 수명을 단축시킬 수 있으나 제안 메커니즘은 최적의 경로를 찾는 대신 상황에 따라 조금씩 다른 경로를 제공해줌으로써 일부 노드의 집중적 에너지 소비를 줄일 수 있다는 장점을 갖는다. 뿐만 아니라 보안을 강화하기 위한 방안으로 제시한 포스트 설정 방법은 설정된 중간 지점의 클러스터헤드와의 pairwise 키로 MAC을 계산하여 추가함으로써 중간 공격자로 인한 데이터의 위·변조 여부를 체크함으로써 트래픽을 조절하는 기능을 한다.

오버헤드를 살펴보면, 포스트 개수만큼의 MAC의 계산과 검증이 필요하나 한 개의 MAC 검증에는 1바이트를 전송하는 정도의 에너지면 충분하므로 무시할 수 있는 수준이다. 또한 목적지 노드로 전송되는 패킷에 포스트 개수만큼의 MAC이 추가되는 만큼의 저장장소의 오버헤드가 발생하지만 MAC의 크기가 크지 않을 뿐 아니라 MAC의 검증을 통해 위조나 변조된 데이터를 걸러내어 트래픽을 줄인다는 점을 고려할 때 충분히 가치가 있는 부분이라 할 수 있다.

5. 결론 및 향후 연구 방향

본 연구에서는 센서 네트워크를 위한 클러스터 기반의 네트워크 구조를 제시하고 이 구조에 기반한 효율적인 동적 라우팅 메커니즘을 제안하였다. 특히, 효율성 뿐 아니라 보안성을 강화하기 위해 각 클러스터헤드가 라우팅 경로 중간 중간에 포스트 위치를 지정하여 이 위치에서 근원지 클러스터헤드와 포스트 클러스터헤드 간의 pairwise 키를 이용한 MAC값을 추가하고 이를 검증함으로써 데이터의 진위를 파악하고 데이터가 위·변조된 경우 이를 적절히 걸러줌으로써 잘못된 정보가 네트워크 내에서 불필요한 트래픽을 야기하지 않도록 하였다.

향후 연구로는 제안된 라우팅 메커니즘에 대한 시뮬레이션을 수행하여 기존에 제안된 메커니즘과의 비교를 통한 효율성을 입증할 계획이며 가능한 내부, 혹은 외부로부터의 공격 패턴을 분석하여 이에 대응할 수 있는 공격 탐지 및 방지 방안을 제안하고자 한다.

Acknowledgement

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음.

6. 참고 문헌

[1] W. Heinzelman, J. Kulik, and H. Balakrishnan, Negotiation-based Protocols for Disseminating Information in Wireless Sensor Networks, Proc. of the 5th Annual ACM/IEEE International Conf. on Mobile Computing and Networking, 1999.

[2] F. Ye, A. Chen, S. Liu, and L. Zhang, A Scalable Solution to Minimum Cost Forwarding in Large Sensor Networks, Proc. of the 10th International Conf. on Computer Communications and Networks, 2001.

[3] K. Sohrabi, J. Gao, V. Ailawadhi, and G. Pottie, Protocols for Selforganization of a Wireless Sensor Network, IEEE Personal Communications, vol. 7, Issue 5, 2000.

[4] D. Estrin, R. Govindan, and J. Heidemann, Next Century Challenges: Scalable Coordination in Sensor Networks, Proc. of the 5th Annual ACM/IEEE International Conf. on Mobile Computing and Networking, 1999.

[5] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, Span: an Energy-efficient Coordination Algorithm for Topology Maintenance, Proc. of the 7th Annual International Conf. on Mobile Computing and Networking, July 2001.

[6] S. Lindsey and C. Raghavendra, PEGASIS: Power-Efficient Gathering in Sensor Information Systems, International Conf. on Communications, 2001.

[7] D. Estrin, R. Govindan, and J. Heidemann, Next Century Challenges: Scalable Coordination in Sensor Networks, Proc. of the 5th Annual ACM/IEEE International Conf. on Mobile Computing and Networking, 1999.

[8] A. Manjeshwar and D. Agrawal, TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks, Proc. of the 15th Parallel and Distributed Processing Symposium, 2001.

[9] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy efficient Communication Protocol for Wireless Micro Sensor Networks, Proc. of the 33rd Annual Hawaii International Conf. on System Sciences, 2000.

[10] R. Blom, An optimal class of symmetric key generation systems. Advances in Cryptology, Proc. of EUROCRYPT 84, LNCS 209, pp.335-338, 1985.