무선 센서네트워크에서의 위치정보 은닉을 이용한 에너지 효율적인 보안기법

현재명*, 김성수
아주대학교 정보통신전문대학원
e-mail : {jmhyun78, sskim}@ajou.ac.kr

Energy Efficient Security Scheme for Wireless Sensor Network With Hiding Location Information

Jae-Myung Hyun*, Sung-Soo Kim
Graduate School of Information Communication, Ajou University

요 약

무선 센서 네트워크는 저가의 많은 노드들로 구성되어 있으며. 이 노드들은 정보수집, 계산, 통신을 위한 전력등을 가지고 있다. 센서 네크워크에서의 보안을 위하여 주로 암호화 방법이 사용되고 있으나 자원이 제약적인 센서 네크워크에서 많은 에너지와 계산을 필요로 하는 암호화 방법은 센서 노드의 수명을 단축시킨다. 이를 보완하기 위하여 본 논문에서는 위치정보 은닉을 이용한 저전력 보안방법을 제안한다. 제안된 방법에서는 위치정보의 은닉을 위하여 상대거리정보를 사용하며, 센서 노드간 통신에서는 상대좌표로부터 구할 수 있는 노드사이의 상대거리정보가 사용된다.

1. 서론

저가의 많은 센서 노드들로 구성된 센서 네트워크는 앞으로 여러 분야에서 다양한 방법으로 사용될 것이다. 이런 센서 네트워크에서 가장 민감한 부분은 센서노드의 전력이다. 수백, 수천개로 이루어진 센서노드는 주로 자신의 배터리로부터 전력을 공급받아 수행한다. 관리자가 센서노드의 배터리를 일일이 교환할 수 있으나, 이것은 매우 비효율적인 방법이다. 그러므로 센서 네크워크에서 가장 중요한 문제 중 하나가 센서 노드의 수명을 극대화 시키는 방법이다. 센서네트워크에서의 보안 또한 중요하다. 비록 센서 노드가 작고, 에너지 한정적인 노드이지만, 이 센서 노드는 정보수집을 주 목적으로 하므로 이 정보를 보호하기 위한 방법이 필요하다. 그러나 센서네트워크의 보안분야는 다른 분야(라우팅, 에너지, 위치정보 등)에 비하여 많은 연구가 이루어지지 않고 있다.

본 논문에서는 상대좌표를 이용한 에너지 효율적인 보안방법을 제안하고자 한다. 센서 네트워크에서의 위치정보는 다양한 용도로 사용되며 위치정보가 없는 정보는 거의 무의미한 정보로 여겨진다[1]. 이러한 점을 이용하여 센서 네크워크에서의 보안을 제공한다. 상대좌표를 이용하여 위치정보를 은닉함으로써 센서 노드의 정보를 무의미한 정보로 만들어 외부의 악의적인 공격자가 이 정보를 습득하더라도 공격자에게 필요 없는 정보로 만드는 것이다. 본 논문에서는 이 보안방법을 EESMRC(Energy Efficient Security Method using Relative Coordinate)로 부르고자 한다.

EESMRC 에서는 상대좌표가 사용되므로 상대좌표를 구하기 위한 알고리즘이 필요하다(상대좌표를 구하기 위한 알고리즘은 이미 제시되어 있다[4][5]). 그러나 [4]에서는 GPS 를 사용하지 않고 상대좌표를 구하였기 때문에 많은 양의 계산이 필요하며 또한 이 상대좌표를 다시 절대좌표로 바꿀 수 없다는 단점이 있다. 그러므로 본 논문에서는 최소한의 GPS 를 사용하고 기존에 이미 제시된 노드의 위치를 찾는 알고리즘을 이용하여 상대좌표를 구한다(TOA(Time of Arrival), 3/2NA(3/2 Neighbor Algorithm)[2]). 네크워크 구성비용의 최소화를 위하여 단지 3 개의 GPS 를 사용하였으며, 또한 통신간 상대좌표의 노출을 최소화하기 위하여 상대 거리정보(이웃한 노드와의 상대 거리정보는 두 노드간 상대좌표의 차이로 구한다)를 이용하여 노드간 통신하게 하였다.

본 연구는 정보통신부 21 세기프론티어연구개발사업의 일환으로 추진되고 있는 유비쿼터스컴퓨팅네트워크원천기술개발사업의 지원에 의한 것임.
이 논문은 2005 년도 두뇌한국 21 사업에 의하여 지원되었음.

2. 상대위치 및 절대위치 정보

2.1 상대거리정보와 상대좌표

상대거리정보는 상대좌표를 구한 뒤 노드간 통신을 통해 구할 수 있으므로 먼저 상대좌표를 구하는 방법에 대하여 설명한다. 상대좌표를 구하기 위한 과정은 두 단계로 나눌 수 있다. 싱크노드 그룹에서 수행하는 과정과, 모든 노드에서 수행되는 과정이다. 아래의 과정은 싱크노드 그룹에서 수행된다.

- 싱크노드 그룹의 절대좌표를 구한다.
- GPS 사용을 중지한다.
- 싱크노드 그룹의 상대좌표를 설정한다.

싱크노드 그룹은 하나의 싱크노드와 GPS 를 장착한 두 개의 Node 들로 구성된다(Sink-Node, GPS-Node1, GPS-Node2). 네트워크 설정 시 GPS 노드들은 GPS 를 이용하여 각각 자신의 절대좌표를 구하여 싱크노드로 전달한다. 그 다음 에너지의 소모를 막기 위하여 GPS 사용을 중지한다. GPS 사용을 중지하였으나 GPS 노드들은 계속적으로 동작한다. 그 결과 싱크노드는 3 개의 절대좌표를 가지고 있으며, 이 절대좌표는 노드의 상대좌표로부터 절대좌표를 구하기 위한 레퍼런스로 사용된다. 이 절대좌표는 오직 싱크노드만이 가지고 있으며 다른 node 로 전송되지 않는다.

상대좌표를 구하기 위해서는 기준점이 필요하며, 이를 위하여 싱크노드가 기준점(0,0)이 된다. GPS-Node1 의 상대좌표는 싱크노드와 GPS-Node1 의 거리를 x 좌표로 하고, 0 이 y 좌표인 상대좌표로 설정한다. 이를 기준으로 다시 GPS-Node2 의 상대좌표를 결정한다. 다음 과정은 모든 노드에서 수행되는 과정이다.

- One hop 이웃 노드를 찾는다. (K_i)
- 이웃 노드와의 거리를 측정한다. (D_i)
- K_i 와 D_i 를 모든 one hop 이웃노드로 전송한다.
- K_i 에 포함된 j의 수가 3보다 클 때 TOA 알고리즘을 이용하여 상대좌표를 구하고, 3보다 작을 경우 3/2NA 방법을 이용하여 상대좌표를 구한다.
- 상대좌표로부터 Node의 상대거리정보를 구한다.

K_i 를 노드 i 와 one hop 에 있는 이웃 노드로 i 와 통신할 수 있는 노드의 집합으로, D_i 는 one hop 이웃 노드와의 거리를 나타내는 집합으로 정의한다. 통신할 수 있는 이웃노드의 거리를 측정 후 TOA 와 3/2NA 방법을 통하여 노드의 상대좌표를 계산한다.

상대거리정보를 구하기 위한 방법은 간단하다. 위에서 설명한 2 가지 과정을 통하여 모든 노드는 상대좌표를 가진다. 상대좌표를 가진 노드는 자신과 통신할 수 있는 이웃노드의 좌표를 얻으며, 자신의 좌표에서 이웃노드의 좌표를 뺀 값이 상대거리정보이다. 이 값을 상대거리정보 테이블에 저장한다. 다음 표 1 은 각 노드가 가지고 있는 상대정보 테이블을 나타낸 것이다.

표 1 상대거리정보 테이블

NodeA (x,y)	
ID	상대거리정보
NodeB-1	NodeA(x,y) - NodeB-1(x,y)
NodeB-2	NodeA(x,y) - NodeB-2(x,y)
NodeB-3	NodeA(x,y) – NodeB-3(x,y)

2.2 절대좌표

절대좌표를 구하는 과정은 오직 싱크노드에서만 수행된다. 싱크노드가 노드로부터 상대좌표를 받았을 때 상대좌표를 절대좌표로 변환시켜 사용한다. 다음 과정은 싱크노드에서 수행되는 과정이다.

- GPS-Node1의 절대좌표를 상대좌표상으로 매핑한다. (단지 GPS-Node1의 절대좌표에서 싱크노드의 절대좌표만큼 감소시킨다).
- 상대좌표와 절대좌표의 회전각도를 계산한다.
- 구하고자 하는 Node의 상대좌표를 회전시킨 뒤 싱크노드의 절대좌표를 더한다.

GPS-Node1 의 절대좌표에서 싱크노드의 절대좌표 값을 빼면 GPS-Node1 의 절대좌표는 상대좌표와 같은 중심점을 가지고 있으나 다른 방향의 x, y 축을 가진 좌표가 된다. 그림 1 에서 보여주는 것과 같이 GPS-Node1 의 절대 좌표를 상대좌표상으로 매핑 하였을 경우 GPS-Node1 의 상대좌표와 절대좌표 사이에 α 만큼의 회전 각도가 존재하는 것을 알 수 있다. 이것은 상대좌표가 절대좌표로부터 α 각도만큼 회전된 상태란 것을 나타내는 것이며, 노드의 상대좌표를 α 만큼 회전 시키면 절대좌표와 같은 방향의 x, y 축을 가질 수 있다. 여기서 절대좌표를 구하고자 하는 노드를 NodeA 라 한다. NodeA 의 상대좌표와 x 축과의 각도를 β 라 할 때, $\alpha+\beta$ 는 회전된 NodeA 의 좌표와 x 축과의 각도를 나타내며 이 좌표를 $RAN(x,y)$ 라 정의를 한다. 상대좌표를 절대좌표로 변환하기 위해 필요한 좌표를 표현하면 다음과 같다.

상대좌표		절대좌표
Sink-Node $(0,0)$	$\rightarrow$	(PS_x, PS_y)
GPS-Node1 $(R1_x, R1_y)$	$\rightarrow$	$(P1_x, P1_y)$
NodeA (RA_x, RA_y)	$\rightarrow$	(PA_x, PA_y)

다음 식을 이용하여 NodeA 의 $RAN(x,y)$ 를 구할 수 있다.

$$RAN_x = \cos(\alpha+\beta)\cdot\sqrt{RA_x^2+RA_y^2}$$
$$= \cos(\alpha)\cos(\beta)-\sin(\alpha)\sin(\beta)\cdot\sqrt{RA_x^2+RA_y^2}$$

$$RAN_y = \sin(\alpha+\beta)\cdot\sqrt{RA_x^2+RA_y^2}$$
$$= \sin(\alpha)\cos(\beta)+\cos(\alpha)\sin(\beta)\cdot\sqrt{RA_x^2+RA_y^2}$$

$RAN(x,y)$ 의 좌표를 구했으나 이것은 단지 NodeA 의 상대좌표를 각도 α 만큼 회전시킨 좌표이며 NodeA 의 절대좌표는 아니다. 그러므로 이 좌표에 싱크노드의 절대좌표 값을 더하면 NodeA 의 절대좌표를 구할 수 있다.

$$PA(x,y) = RAN(x,y) + PS(x,y)$$

이 과정의 통하여 모든 노드의 상대좌표는 절대좌표로 변환될 수 있다.

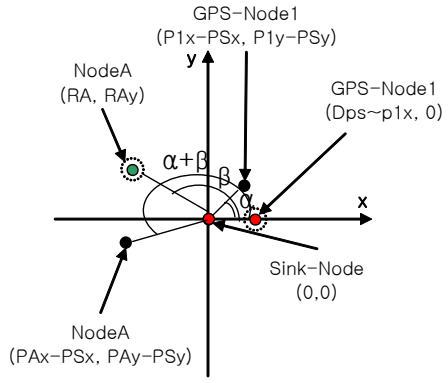

그림 1 상대좌표와 절대좌표의 회전 각도

3. 네크워크 설계

3.1 기본설계

EESMRC 는 실외환경을 목표로 하고 있으며 중앙집중적인 방법을 사용한다. 대부분의 노드는 단지 주변환경으로부터 정보를 수집하며 싱크노드에서 거의 모든 정보에 관한 처리가 수행된다. 또한 각 노드는 ID 를 가지고 있다. 기본적으로 네크워크는 N 개의 위치를 알 수 없는 노드로 구성되어 있으며 GPS 를 장착한 2 개의 노드와 싱크노드가 하나의 그룹이 되어 네트워크 지역 A 에 분포되어 있다고 가정하였다. 노드의 통신범위는 r 로 모두 똑같다고 가정하였다. 본 논문에서는 상대좌표를 구하기 위하여 TOA 와 3/2NA 방법을 사용한다. TOA 와 3/2NA 방법은 기본적으로 3 개의 이웃된 노드와 통신할 수 있어야 노드 자신의 위치를 구할 수 있으므로 네크워크의 기본적인 노드의 수에 관하여 생각하여야 한다. 센서 네크워크 지역 A 안에 N 개의 노드가 불특정하게 분포되어 있다고 할 때, 노드의 통신범위 r 안에 있는 노드의 수는 $n \supset \frac{N\pi r^2}{A}$ (1)로 나타낼 수 있다. TOA 와 3/2NA 방법에서는 통신할 수 있는 3 개의 노드가 필요하므로 n 의 수는 4 가 되어야 한다. 그러므로 전체 노드수 N 은 n 이 4 를 만족하는 수가 되어야 한다.

3.2 추가적인 통신방법

각 Node 는 상대거리정보 테이블을 가지고 있다. 테이블은 상대좌표, 상대거리정보 그리고 노드의 ID 를 가지고 있다. 노드가 싱크노드로 데이터를 보내고자 할 때 노드가 싱크노드와 직접 통신을 하지 않는다면 데이터는 몇 개의 노드를 거쳐서 싱크노드로 전달 되어질 것이다. 예로 NodeA 가 싱크노드로 데이터를 보내려 하고 NodeB 는 싱크노드와 직접 통신을 할 수 있으며 NodeA 의 통신거리 안에 있다고 할 때, NodeA 는 자신의 데이터를(노드의 ID 와 상대거리정보(0,0) 포함) 브로드캐스트하고 NodeB 는 이 데이터를 받을 것이다. NodeB 의 상대거리정보 테이블에는 NodeA 에 대한 상대거리정보가 있으므로 이를 NodeA 의 데이터에 더한 후 다시 브로드캐스트한다. 싱크노드는 이 데이터를 받고 다시 자신의 상대거리정보 테이블에 있는 NodeB 의 상대거리를 데이터에 더한다. 이로서 싱크노드는 NodeA 의 상대좌표를 구할 수 있게 된다. 그림 2 는 이 방법을 설명한 것이다.

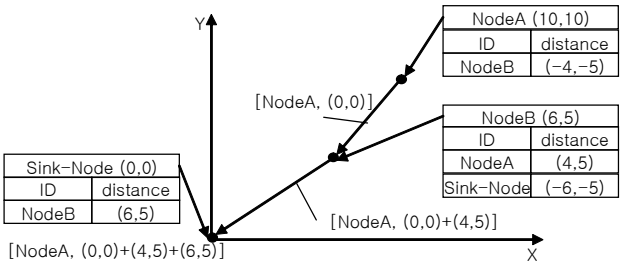

그림 2 추가적인 통신방법

4. 보안 관점

EESMRC 에서 상대좌표를 사용하는 이유는 절대좌표를 상대좌표로 표현함으로써 위치정보를 은닉하는데 있다. 상대좌표를 설정하는 방법은 상대좌표를 절대좌표를 바꾸는데 필요한 상대좌표와 절대좌표의 수에 따라 틀려진다. 이 논문에서는 상대좌표로부터 절대좌표를 구하는데 2 개의 상대좌표와 절대좌표를 사용한다. 그러므로 상대좌표의 x, y 축 방향과 절대좌표의 x, y 축 방향이 틀리며, 싱크노드의 상대좌표와 절대좌표는 서로 전혀 다른 위치를 나타내게 된다. 상대좌표 설정 시 임의적으로 싱크노드의 좌표를 (0,0)으로 하였다. 이로 인해 상대좌표는 절대좌표와 기준점이 전혀 다른 좌표가 된다. 또한 GPS-Node1 의 상대좌표 설정 시 GPS-Node1 과 싱크노드의 거리를 x 좌표로, 0 을 y 좌표로 설정하였기 때문에 절대좌표와 상대좌표의 x, y 축이 서로 다른 방향을 나타내는 것이다. 결과적으로 공격자가 상대좌표를 획득 하였을 경우 이 상대좌표는 실제지형에서 어떠한 형태로도 표현될 수 있다. 그림 3 은 실제지형에서 상대좌표의 표현 가능한 위치를 나타낸 것이다.

노드간 통신에서 상대좌표를 직접 사용하지 않고 상대좌표로부터 구해진 상대거리정보만을 이용하였다. 중앙집중적인 네트워크에서 정보에 관한 거의 모든 처리가 싱크노드에서 수행되므로 가장 중요한 노드는 싱크노드이다. 이런 네트워크에서 상대좌표를 사용할 경우 공격자는 상대좌표로부터 쉽게 노드로 부터 싱크노드의 거리를 구할 수 있다. 그러나 상대거리정보만을 노드간 위치정보를 전달하기 위한 방법으로 사용함으로써 공격자가 상대거리정보를 획득하여도 싱크노드까지의 거리가 아닌 데이터를 보낸 노드와 데이터를 받은 노드의 거리만을 알 수 있다.

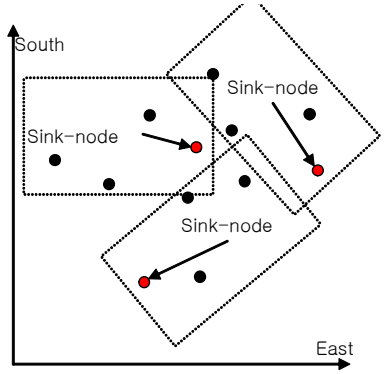

그림 3 실제지형에서 상대좌표의 표현 가능한 좌표

5. 성능평가

EESMRC 의 성능평가를 위하여 이미 측정되어 있는 기존의 값과 비교하였다. Sparc 440 하드웨어 플랫폼을 사용하였고, EESMRC 의 에너지 소비량을 측정하기 위하여 EESMRC 의 수행간 프로세스에 의하여 사용되는 클럭수를 측정하였다.

$$amount\ of\ enery\ consumption \approx$$
$$execution\ time \approx \frac{a + b \cdot \lceil text\_length / blocksize \rceil}{processor\_freq \cdot bus\_width} \quad (2)$$

표 2 는 식(2)의 변수 값을 설명한 것이며 표 3 은 성능비교를 위한 암호화 방법의 변수를 나타낸 것이다.

표 2 성능평가를 위한 변수

a	초기화 오버헤드
b	암호화 처리를 위한 시간
Text_length	Data의 길이
Blocksize	암호화 데이터의 크기
Processor_freq	processor 클럭
Bus_width	CPU bus의 용량

표 3 비교 암호화 방법의 변수

알고리즘	a 값	b 값	블록크기
MD5	203656	86298	512
SHA1	77337	233082	512
RC4	69240	13743	8

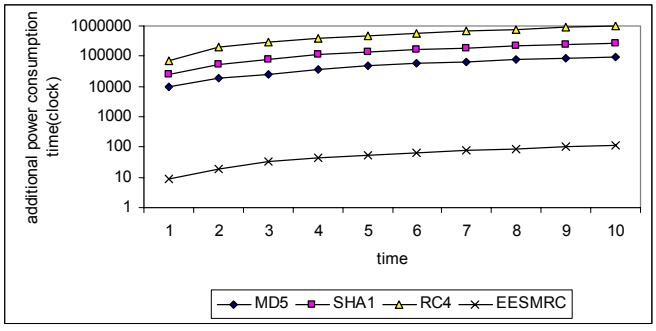

그림 4 보안방법의 시간당 추가적인 에너지 소비량

그림 4 가 보여주듯이 EESMRC 는 많은 양의 에너지를 필요로 하지 않는다. 반면 다른 암호화 방법 RC4, SHA1, MD5 는 평균적으로 각각 100000, 50000, 10000 의 클럭수를 소모한다.

6. 결론

본 논문에서 상대좌표를 이용하여 위치정보를 은닉하는 보안기법을 제시함으로써 노드에서의 에너지 효율을 높일 수 있는 방법을 제안하였다. 에너지가 제한된 센서 네크워크에서 암호화 방법은 많은 양의 에너지를 소비하므로 센서노드의 수명을 단축시킬 수 있으나 본 논문에서 제시한 EESMRC 는 적은 량의 에너지만을 소비한다는 것을 실험을 통하여 검증하였다. 이 방법을 통하여 센서노드의 에너지 소모를 줄여 노드 수명을 증가시킬 수 있으며 또한 정보에 대한 보안효과를 얻을 수 있다. 그러므로 EESMRC 는 에너지가 제한된 센서 네크워크에서 효과적으로 사용될 수 있을 것으로 기대한다.

참고문헌

[1] J. Beutel, “Location Management in Wireless Sensor Networks,” chapter in Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems, CRC Press, July 2004.

[2] M. Barbeau, et al., “Improving Distance Based Geographic Location Techniques in Sensor Networks,” proceeding of International Conference on Ad Hoc Networks and Wireless, pp. 197-210, July 2004.

[3] P. Ganeasn, et al., “Analyzing and Modeling Encryption Overhead for Sensor Network Nodes,” Proceedings of ACM Workshop on Wireless Sensor Networks and Applications, pp. 151-159, Sep. 2003.

[4] S. Capkun, et al., “GPS-free Positioning in Mobile Ad-Hoc Networks,” Proceedings of the 34th Annual Hawaii International Conference on System Sciences, Vol. 9, pp. 9008, Jan. 2001.

[5] N. Patwari, et al., “Relative Location Estimation in Wireless Sensor Networks,” IEEE Transactions on Signal Processing, Special Issue on Signal Processing in Networks, No. 8, Vol. 51, pp. 2137-2148, Aug. 2003.

[6] S. Slijepcevic, et al., “On Communication Security in Wireless Ad-Hoc Sensor Networks,” IEEE International Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, pp. 139-144, June 2002.

[7] H. Cam, et al., “Energy-Efficient Secure Pattern Based Data Aggregation for Wireless Sensor Networks,” Proceedings of IEEE International Performance Computing and Communications Conference, Apr. 2005.

[8] 박수용, 김성수, "센서 네트워크의 다층형 데이터 보안 방법," 2004 년 한국정보과학회 춘계학술발표대회, 한국정보과학회, 제 31 권 1 호, pp. 355-357, 2004. 4.