무선 센서 네트워크에서 위치 기반 기법들에 대한 재고찰

*천지영 **김용호 ***이동훈

고려대학교 정보경영공학전문대학원

*jychun@korea.ac.kr

Location-based Key Management Schemes Revisited in Wireless Sensor Networks

*Ji Young Chun **Yong Ho Kim ***Dong Hoon Lee

CIST, Korea University

요약

무선 센서 네트워크 환경에서 센서 필드에 배치된 센서 노드들 사이에 안전한 통신 인프라를 구성하기 위해 보안 키 설립이 필요하다. 현재까지 센서 노드들 사이의 보안 키 설립에 대한 여러 가지 기법들이 제안되어 왔으며 최근에는 배치 전 센서 노드들의 예측 위치를 이용한 개선된 기법들이 제안되고 있다. 현재까지 제안된 위치기반 기법들은 선택적인 노드포획에 안전하게 설계하기 위해 상대적으로 높은 키 저장량과 키 생성을 위한 많은 연산량을 요구한다. 우리는 위치 기반 기법에서는 단순히 piar-wise키를 저장하는 것이 저장량이나 연산량 면에서 효율적이라는 분석을 제시하고 pair-wise키를 이용하여 공격자의 선택적인 노드 포획에도 강한 효율적인 위치 기반 기법을 제안한다.

1. 서론

무선 센서 네트워크는 초경량, 저 전력의 많은 센서 노드들로 구성된다. 센서 노드들은 배치 전에 구축해야할 네트워크에 대한 사전 정보 없이 센서 필드에 배치된 후 자가 구성(Self-Organizing)을 통해 네트워크 인프라를 형성한다. 센서 노드들은 센서 장치를 통해 주위 환경을 감지하여 실제 데이터를 수집하며, 수집된 데이터를 네트워크 통해 전송하게 된다. 하지만 무선 센서 네트워크는 센서 노드들의 제한된 자원과 무선 통신을 이용한 데이터 전송 등으로 인하여 보안상의 많은 위험 요소를 가지고 있다. 따라서 군사적인 목적으로 사용되는 경우와 같이 수집된 데이터의 보안이 중요한 환경에서는 센서 노드들 사이의 안전한 통신을 위한 안전한 보안키 설립이 필요하다.

무선 센서 네트워크에서의 키 설립은 센서 노드들의 제한된 자원 때문에 매우 어렵다. 무선 센서 네트워크는 일반적으로 수천 개 이상의 센서 노드들로 구성되고 또한 전력이 전부 소모되었거나 유실된 센서 노드들에 대해서는 추가적인 관리를 하지 않으므로 센서 노드의 가격이 높아서는 안 된다. 따라서 저가의 센서 노드는 메모리 내용을 보호하기 위한 조작방지기술(Tamper-Resistance)이 불가능하므로 공격자의 노드 포획에 대해 취약할 수밖에 없다. 또한 센서 노드들은 낮은 계산 능력을 가진 프로세서를 사용하고 저전력 배터리를 사용하게 되므로 연산량이 많은 공개키 방식은 무선 센서 네트워크 환경에 적합하지 않다. 게다가 배치 전에 센서 노드들의 정확한 위치를 예측하는 것이 불가능하기 때문에 이웃 노드들에 대한 정보를 사전에 알기 어렵다. 따라서 배치 전에 임의의 키들을 할당하는 방법을 사용하는데 센서 노드는 매우 적은 용량의 메모리 자원을 사용하므로 사전에 많은 키를 저장하기 어렵다. 따라서 키관리 기법 설계 시 이러한 제약사항을 최대한 고려해야 한다.

현재까지 센서 노드들 사이의 안전한 키 설립에 대한 여러 가지 기법들이 제안되고 발전되어 왔다. 최근에는 이러한 기법들을 더욱 향상시키기 위하여 배치 전에 센서 노드들의 예측 위치를 이용한 기법들[2,3,7,8]이 제안되고 있다. 비록 센서 노드들이 배치되고 난 후 정확한 위치를 사전에 예측할 수는 없지만 근접한 위치를 예측하는 것은 가능하다. 만약 센서 노드들을 작은 그룹으로 나누어 순차적으로 비행기에서 떨어뜨린다고 가정한다면 같은 그룹에 있는 센서 노드들은 같은 시간에 같은 위치에서 배치되므로 가까운 위치에 분포하여 이웃이 될 확률이 높아진다. 따라서 배치 전 센서 노드들의 예측된 위치 정보를 기반으로 키를 사전 분배하고 배치 시 예측된 위치에 배치될 수 있도록 오류를 최소화하여 배치시킴으로써 센서 노드들 간에 보안키 설립 시 성능을 향상 시켰다. 또한 센서 노드들의 예측 위치를 이용함으로써 키 저장 요구량을 줄였고 임의의 노드 포획에 대한 안전성도 높였다.

예측 위치를 기반으로 한 기법들[2,3,7,8]은 임의의 노드 포획에 대한 안전성은 높였지만 공격자의 선택적인 노드 포획에는 여전히 취약하다. 일반적으로 임의의 노드 포획에 대한 가정은 너무 약하다. 현명한 공격자라면 적은 노력으로 더 많은 정

이 논문은 2006년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임 (No.R01-2004-000-10704-0)

보를 얻기 위해 선택적으로 노드를 포획할 것이다. Huang 등은 최초로 선택적인 노드 포획에 강한 Grid-Group Deployment 기법[5](이후 GGD 기법)을 제시하였다. 하지만 이 기법은 임계값(Threshold) 이하로 키 사용 개수를 제한함으로써 노드 추가가 어렵다. 또한 보안 키 공유 시 많은 법(Modulus) 연산이 필요하고, 같은 영역과 다른 영역에서의 키 설립 방법이 다르기 때문에 두 가지 키 설립 방법이 필요하다. 또한 한 그룹 안에 있는 노드의 수가 이웃 그룹과의 연결성에 영향을 미치게 되므로 고립되는 그룹이 생길 가능성도 크다[6].

GGD 기법에서의 문제점을 해결하기 위해 Lee 등은 Multi-layer Grid-Group Deployment 기법[6](이후 ML-GGD 기법)을 제시하였다. 하지만 이 기법에서도 GGD 기법과 마찬가지로 임계값(Threshold) 이하로 키 사용 개수를 제한함으로써 노드 추가가 어렵고 많은 키 저장량과 연산량을 요구한다.

본 논문에서는 위치 기반 기법들에 대한 문제점을 지적하고 이러한 문제를 해결하기위한 효율적인 기법을 제시한다.

2. 위치 기반 기법 재고찰

위치 기반 기법에서는 센서 노드들을 그룹 단위로 나누고 각 그룹 별로 키를 사전 분배한다. 따라서 전체 센서 노드들의 개수가 N개이고 그룹의 개수가 G라면 한 그룹의 센서 노드의 수는 N/G개 이다. 따라서 위치를 고려하지 않은 기법들에서는 한 노드가 다른 N-1개의 노드들과 pair-wise키를 저장하는 것이 저장량 측면에서 불가능 하였지만 위치 기반 기법에서는 한 그룹의 센서 노드의 수가 상대적으로 작기 때문에 자신의 그룹과 이웃 그룹에 있는 노드들과 pair-wise키를 저장하는 것이 가능하다. pair-wise키를 사전에 저장하는 것이 안전성이나 계산량 측면에서 매우 효율적이다.

GGD 기법은 기존 기법들에 비해 선택적인 노드 포획에 안전하면서도 적은 저장량을 요구한다. 하지만 pair-wise키를 사용하면 선택적인 노드 포획에 대해 100% 안전하고, 키를 공유하기 위해 복잡한 연산이 필요하지 않다. [표 1]은 GGD 기법과 같은 조건하에 pair-wise 키를 이용할 때 필요한 저장량을 나타낸다. [표1]에서 살펴보면 pair-wise 키를 사전 분배하는 것이 GGD 기법보다 더 적은 저장량을 요구하는 것을 알 수 있다.

[표 1] 위치기반 기법들 사이에 키 저장량 비교

p	EG-D 기법[2]	GGD 기법[5]	PairWise 기법
p = 0.4167	58개	56개	50개
p = 0.4643	64개	60개	56개
p = 0.5238	72개	68개	62개
p = 0.6000	86개	78개	68개

앞에서 지적한 대로 GGD 기법에서의 문제점을 해결하기 위해 제시된 ML-GGD 기법에서의 단점은 많은 저장량을 요구한다는 것이다. [표2]는 [6]에서 제시한 ML-GGD 기법의 저장량을 분석한 표이고 뒤에 노란 부분은 ML-GGD 기법과 같이 자신이 속한 그룹과 상·하·좌·우의 이웃 그룹들과의 노드들과 pair-wise 키를 사전 분배했을 때 필요한 저장량을 표시한 것이다.

$$p_1 = 1 - \frac{\binom{\omega}{\tau}\binom{\omega-\tau}{\tau}}{\binom{\omega}{\tau}^2} = 1 - \frac{((\omega-\tau)!)^2}{(\omega-2\tau)!\omega!}$$

ω=7, τ_E=1(τ=2)일 때 위 식[5]에 의해 이웃 노드와 연결될 확률은 p=0.5238이므로 같은 연결성을 가지고 pair-wise 키를 사전 분배했을 때 요구되는 저장량을 $n=\frac{m}{p}$[1]의 식에 적용시켜 다음 표의 값을 얻을 수 있다.

[표 2] ML-GGD 기법과 저장량 비교

n_z	ω	τ_E	Size (bit)	ML-GGD (byte)	PairWise p=0.5238 (byte)
50	7	1	64	512	1048
100	7	1	64	960	2096
200	7	1	64	1888	4192
50	7	1	128	1024	2096
100	7	1	128	1920	4192
200	7	1	128	3776	8384
n_z	ω	τ_E	Size (bit)	ML-GGD (byte)	PairWise p=1 (byte)
50	7	2	64	1920	1992
100	7	2	64	3776	3992
200	7	2	64	7424	7992

[표 2]에서 알 수 있듯이 ω=7, τ_E=2일 때 ML-GGD와 pair-wise 기법은 거의 비슷한 저장량을 나타내고 있다. 하지만 ML-GGD 기법을 사용할 때 필요한 계산량과 노드 포획에 대한 안전성을 고려한다면 같은 저장량 하에서 pair-wise 기법을 사용하는 것이 훨씬 효율적이다. 따라서 위치 기반 기법에서는 어떤 확률 이상의 연결성을 기대할 때 단순히 pair-wise 키를 사전 분배하는 것이 다른 여러 방법을 사용하는 것보다 안전성이나 연산량 측면에서 훨씬 효율적일 수 있다.

3. 개선된 기법

위치 기반 기법에서는 단순히 pair-wise 키를 사전 분배하는 것이 다른 기법을 사용하는 것보다 효율적일 수 있다는 것을 2장에서 살펴보았다. 이번 장에서는 위치 정보를 이용한

pair-wise 키 사전 분배 기법을 제안한다.

가. 네트워크 모델

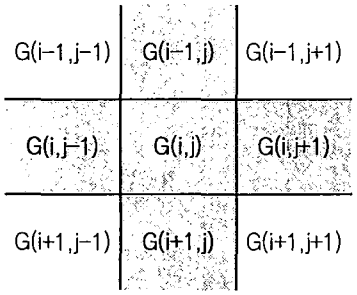
전체 센서 노드의 개수를 N이라 하고 전체 그룹의 수를 G라고 하자. 각 그룹 G(i,j)에 센서 노드가 n(=N/G)개씩 있고, 센서 노드 S_k의 ID는 그룹 ID와 노드의 유일한 값인 k로 이루어진 ID_k={G(i,j), k}값을 갖는다고 하자.

나. 같은 그룹에서의 키 사전 분배 방법

Chan 등의 Random pair-wise keys 스킴[1]에서 $n=\frac{m}{p}$ 이므로 이웃 노드와 연결될 확률 p에 따라 사전 저장해야 하는 키의 개수 m이 결정된다. 각각의 센서 노드 S_k에 대해 같은 그룹에 있는 n-1개의 센서 노드들 중에서 임의로 m개의 노드를 선택한 후 선택된 노드들과의 pair-wise 키를 사전 저장한다.

다. 다른 그룹과의 키 사전 분배 방법

다른 그룹과의 키 사전 분배 방법도 같은 영역에서의 방법과 비슷하다. 그룹 G(i,j)에 있는 각각의 센서 노드 S_k에 대해 <그림1>과 같이 상·하·좌·우의 그룹에 있는 노드를 임의로 m개씩 선택한 후 선택된 노드들과의 pair-wise 키를 사전 저장한다. 따라서 다른 그룹의 노드들과의 키 설립을 위해 사전 분배된 키는 4m개이다. 결국 각각의 센서 노드들이 저장해야 할 키의 개수는 5m개 이다.



<그림1> G(i,j)에 있는 노드가 pair-wise 키를 저장해야하는 노드들이 속한 그룹들

4. 분석

단순히 pair-wise키를 사전 분배하는 방법이 한 그룹 내의 센서 노드의 수가 상대적으로 작은 위치 정보를 이용한 키 사전 분배 방법에서 효율적일 수 있다. 다른 위치 기반 기법들과 같은 연결성을 가지고 사전 분배해야하는 키 저장량을 살펴보았을 때 pair-wise 키를 사전 분배하는 저장량이 동등하다면 pair-wise 키를 사전 분배하는 방법이 훨씬 효율적이다. pair-wise 키를 사전 분배하게 되면 키 공유를 위한 연산이 필요 없고 노드 포획에 대해서도 100% 안전하다. 따라서 위치 기반 기법에서는 어떤 확률 이상의 연결성을 기대할 때 pair-wise 키를 사전 저장하는 방법이 효율적이다.

5. 결론

이 논문에서 우리는 배치 전 위치 정보를 이용한 사전 키 분배 기법들에 대해 살펴보았고 이러한 기법들이 효율성을 높이기 위해 사용한 방법들이 이웃노드와의 연결성에 따라 단순히 pair-wise 키를 사전 저장하는 방법보다 효율성이 떨어질 수도 있다는 것을 제시하였다. 앞으로 저장량에 따라 pair-wise 키를 사용하는 것이 더 효율적인 경우에 대한 자세한 분석이 요구된다.

[참고문헌]

[1] Chan, H., Perrig, A., and Song, D., "Random key predistribution schemes for sensor networks.", In IEEE Symposium on Research in Security and Privacy., 2003.

[2] Du, W., Deng, J., Han, Y., Chen, S., and Varshney, P., "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge.", In IEEE Infocom'04., 2004.

[3] Du, W., Deng, J., Han, Y., Chen, S., and Varshney, P., "A Key Pre-distribution Scheme for Sensor Networks Using Deployment Knowledge.", Accepted with minor revision by the IEEE Transactions on Dependable and Secure Computing., 2005.

[4] Eschenauer, L. and Gligor, V. D., "A Key-Management Scheme for Distributed Sensor Networks.", In 9th ACM conference on Computer and Communications Security., 2002.

[5] Huang, D., Mehta, M., Medhi, D., and Harn, L., "Location-aware Key Management Scheme for Wireless Sensor Networks.", in Proceedings of 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks., 2004.

[6] Lee, J., Kwon, T. and Song, J., "Location-Aware Key Management Using Multi-layer Grids for Wireless Sensor Networks", In ACNS., 2006.

[7] Liu, D. and Ning, P., "Location-Based Pairwise Key Establishments for Static Sensor Networks.", In 1st ACM Workshop on Security of Ad Hoc and Sensor Networks., 2003.

[8] Liu, D. and Ning, P., "Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks.", In 1st ACM Workshop on Security of Ad Hoc and Sensor Networks., 2005.