센서 네트워크에서의 자가 위치 추정을 이용한 키 분배 메커니즘

김은아°, 도인실, 채기준
컴퓨터학과, 이화여자대학교
{dmsk999°, isdoh}@ewhain.net, kjchae@ewha.ac.kr

A Key Management Scheme for Wireless Sensor Networks using Self-Positioning with Deployment Knowledge

Eunah Kim°, Inshil Doh, Kijoon Chae
Dept. of Computer Science and Engineering, Ewha Womans Univ.

요 약

센서 네트워크는 많은 수의 센서 노드들로 구성된 네트워크로 센서를 통한 주변 정보 감지 및 감지된 정보를 처리하는 기능을 수행한다. 최근 유비쿼터스 컴퓨팅 개념의 도입과 함께 이를 실생활에 구현하기 위한 기반 기술로 큰 관심을 모으고 있다. 그러나 센서 네트워크의 일상 생활 시스템에서의 의존도가 높아질수록 이로 인한 위험성 또한 높아 질 수밖에 없다. 본 논문에서는 센서 네트워크에서의 보안 서비스를 제공하기 위하여 필수적인 키 관리 기술을 고찰하고 효율적인 키 관리 방법을 제안하고자 한다. 센서 네트워크의 구축 시 센서 노드들의 배치 특성을 고려하여 키 스트링 풀을 설정하고, 배치된 센서 노드의 위치에 따라 필요한 키를 집중적으로 분배하여 센서 네트워크 내의 공통 키 설정 확률을 높이고 센서 노드의 메모리 소모량을 줄이는 키 관리 방법을 고안하였다.

1. 서 론

최근 전자 통신 및 컴퓨터 네트워크 분야의 발전은 무선 센서 네트워크(Wireless Sensor Network: WSN)의 급속한 발전을 용이하도록 하였다. 센서 네트워크는 유비쿼터스(Ubiquitous) 컴퓨팅 구현을 위한 기반 기술의 하나로 초경량, 저전력의 많은 센서들로 구성된 무선 네트워크이다. 이는 특히 네트워크를 구성하는 센서의 수가 매우 많고 각 센서 노드는 제한된 전력과 컴퓨팅 능력을 가지며, 빈번한 센서 노드들의 삽입과 제거에 의해 센서 네트워크의 토폴로지가 쉽게 변화될 수 있다는 특성을 갖는다. 센서 네트워크에서의 대표적인 응용을 살펴보면 센서 노드들을 임의의 영역에 배치하여 이들을 통한 정보 감지 및 감지된 정보를 처리하는 기능을 수행하도록 하는 경우가 일반적이다. 센서 네트워크를 구축한 대표적인 프로젝트의 예로는 SmartDust[1]와 WINS[2]가 있다.

센서 네트워크는 군사 목적과 환경 모니터링, 병원에서의 환자의 상태 모니터링 및 스마트 환경 등의 다양한 분야에 적용되고 있다[3]. 이렇게 센서 네트워크가 우리의 삶을 자동화시키고 편리함을 제공하지만 일상 생활의 시스템에서의 의존도가 높아질수록 이로 인한 위험성 또한 높아질 수 밖에 없다. 특히 센서 네트워크가 안전성이 낮은 환경에 구축될 경우 보안의 필요성은 극대화 되고, 다양한 악의적인 공격에 노출될 수 있다. 그러므로 센서 네트워크를 통해 제공되는 정보들을 신뢰하고 동시에 개인의 프라이버시를 보장 받을 수 있도록 하기 위한 보안 연구가 반드시 병행되어야 한다. 센서 네트워크에서의 보안 서비스를 제공하기 위해서는 암호화된 통신과 인증 서비스가 필요하며, 현재 이를 위하여 필수적인 키 관리 기술에 관한 연구가 활발히 진행 중이다.

기존의 키 관리 기술은 크게 세 가지로 나눌 수 있다: 신뢰성 있는 서버를 이용하는 방법(Trusted-server scheme), 자가 강화 방법(Self-enforcing scheme), 키 선 분배 방법(Key pre-distribution scheme)이다. 신뢰성 있는 서버를 이용하는 방법은 노드들 간의 키 설정을 지정된 서버가 담당하는 방법으로, Kerberos[4]가 이에 속한다. 그러나 이는 안전한 인프라가 구축되어 있지 않은 경우가 대부분인 센서 네트워크에 적합하지 않다. 자가 강화 방법은 관용 암호화와 같은 비대칭 암호화를 사용하는 방법으로 제한된 전력과 컴퓨팅 능력을 가진 센서 네트워크에 적합하지 않다. 키 선 분배 방법은 센서 네트워크의 구축 이전에 모든 센서 노드들에게 사용될 키를 미리 분배하는 방법이다. 이는 기존의 네트워크에 비해 많은 제약사항을 가진 센서 네트워크에 적합하지만, 임의적으로 노드들이 배치되는 센서 네트워크의 특성상 키의 분배 방법이 중요한 문제로 대두되고 있다. 즉, 배치될 센서 노드들의 위치에 따라 통신하게 될 이웃 노드들이 달라지기 때문에 가능한 한 통신이 잦은 노드들 간의 공통 키 설정의 확률을 높이는 것이

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

키 분배의 중요한 문제가 된다. 따라서 본 논문에서는 센서 네트워크 구축 시 노드들의 배치 특성과 센서 노드 자체의 제한적인 특성을 고려한 키 분배 방법을 제안하였다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 키 선 분배 방법과 그에 따른 문제점을 살펴본다. 3장에서는 기존의 키 선 분배 방법을 보완한 새로운 키 분배 방법을 설명한다. 4장에서는 결론 및 향후 연구 방향을 제시한다.

2. 기존 연구

Eschenauer-Gligor[5](이하 EG)는 랜덤 키 선 분배 방법을 제안하였다. 센서 노드들이 배치되기 전에 공용의 키 풀에서 임의의 키들을 센서 노드의 메모리에 저장시키고, 노드들의 배치 후에 공통 키를 설정하도록 한다. 이는 통신하고자 하는 두 센서 노드들이 공통 키를 설정할 때, 각 센서 노드가 저장하고 있는 키들이 한 개의 공용 키 풀에서 임의로 선택된 키들이기 때문에 공통 키를 설정할 수 있는 확률이 낮으며 센서 노드들이 멀리 떨어진 노드들과의 통신보다 이웃 노드들과의 통신이 잦음에도 불구하고 키 분배 방법이 이러한 특성을 반영하지 못하는 단점을 가진다.

Welnliang Du[6](이하 WD)는 이러한 단점을 보완하여 센서 노드들의 배치 정보를 이용한 키 선 분배 방법을 제안하였다. 실제로 센서 노드들이 배치될 때 그룹 기반의 배치 특성을 가진다는 점에 착안하여, 한 개의 공용 키 풀을 사용하지 않고 각 배치 그룹별 서브 키 풀을 사용하도록 한다. 또한 센서 노드들이 전송 범위 내의 노드들과 주로 통신한다는 점을 반영하여, 위치상 가까운 배치 그룹들의 키 풀이 공유 키를 가지도록 설정한다. 각 센서 노드는 자신의 배치 그룹에 할당된 서브 키 풀에서 EG와 같은 방법으로 임의의 키들을 분배 받고 공통 키를 설정한다. 실험을 통하여 WD 방법이 공통 키 설정 확률을 높이는 것으로 나타났지만 이는 배치 그룹의 넓이에 비해 센서 노드들의 전송 범위가 좁은 경우에는 효율적이지 못하다. 일반적으로 센서 노드들은 공중에서 낙하시키는 방법으로 배치되고, 배치 영역의 중앙에 센서 노드들이 다량 배치될 확률이 높으며 노드들의 전송 범위가 제한적이므로 배치 영역의 중앙에 위치한 다수 노드들은 이웃 배치 그룹과의 통신이 불필요하다. WD는 이러한 특성을 반영하지 못하고, 센서 노드들이 이웃 배치 그룹과의 공통 키 설정을 위한 불필요한 키들을 저장하고 있어야 한다는 단점을 갖는다.

3. 자가 위치 추정을 이용한 키 분배 메커니즘

2절에서 살펴본 문제점들을 보완하기 위하여 센서 네트워크 구축 시 센서 노드들의 배치 특성을 고려한 새로운 키 분배 방법을 제안하고자 한다. 센서 노드들의 배치 위치를 정확히 알 수 있으면 공통 키를 설정할 노드들을 예측하여 키 분배를 쉽게 해결할 수 있다. 그러나 센서 노드들의 배치가 임의적으로 이루어지기 때문에 키 선 분배 방법은 공통 키 설정 확률을 높이는데 제한적이다. 본 논문에서는 이를 해결하기 위하여 메모리 소모량이 적은 키 풀을 센서 노드들의 메모리에 미리 할당하고, 노드들의 배치 후에 자신의 위치에 따라 통신에 필요한 키를 분배하도록 한다. 이를 위하여 센서 노드들의 배치 특성을 알아보고, 적합한 키 풀의 설정 방법 및 노드들의 배치 후 공통 키 설정 방법을 제시하도록 한다.

3.1 그룹 기반 배치 모델

센서 노드들의 배치는 WD 그룹 기반 배치 모델을 적용한다[6]. 즉, 센서 네트워크 구축 시 센서 노드들은 일련의 그룹으로 나누어져 배치 지점을 중심으로 배치된다

1) n 개의 센서 노드들은 $s \times t$ 개의 동일 크기의 그룹으로 나누어진다. 각 그룹은 배치 위치에 따라 $G_{i,j}$ ($i = 1, \cdots, s$, $j = 1, \cdots t$)라 정의하고, 배치 지점은 (x_i, y_j) 로 정의한다.
2) 각 배치 그룹은 그리드 형태로 나열되고 배치 영역인 그리드 셀의 중심이 배치 지점이 된다.
3) 센서 노드들은 2차 가우시안 분포(정규 분포)형태로 배치 된다고 가정한다. $G_{i,j}$에 속한 임의의 센서 노드 k는 $f_k^{ij}\left(x, y \middle| k \in G_{i,j}\right) = f\left(x - x_i, y - y_j\right)$에 따라 배치된다 [그림 1].

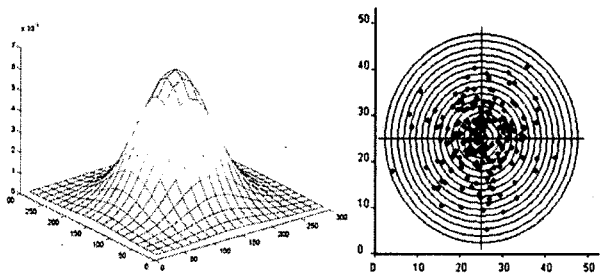

그림 1. 배치 그룹 내의 센서 노드들의 배치 형태

3.2 키 풀 설정

각 센서 노드들은 공통 키 설정에 필요한 키들을 미리 분배 받는 대신 메모리 소모량이 적은 키 풀을 할당 받고, 노드들의 배치 후에 자신의 위치에 따라 통신에 필요한 키를 분배하도록 한다. 이를 위하여 개별 키 들로 이루어진 키 풀이 아닌 키 스트링 풀을 이용한다. 오버랩 키 공유 방법(Overlap key sharing)은 키 스트링 풀에서 일정 길이의 스트링을 추출 한 후 공유된 부분을 공통 키로 설정한다[7]. [그림 2]와 같이 공용 키 스트링 풀 KP 의 일부인 K_A 와 K_B 의 공통 부분이 공통 키로 설정된다. 이는 개별적인 키들 중에 공통 키를 설정할 때보다 공통 키 설정 확률을 높여준다.

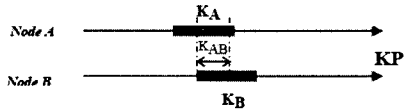

그림 2. 오버랩 키 공유 프로토콜

오버랩 키 공유 방법을 그룹 기반 센서 노드 배치 방법에 적용하기 위하여 키 스트링 풀을 서브 키 스트링 풀로 나누어 각각의 배치그룹에 할당하되, 이웃하는 그룹간 서브 키 스트링 풀이 공유되도록 **환형의 키 스트링 풀**을 구성한다. [그림 3]과 같이 3×3 그리드 셀로 구성된 배치 영역을 고려하여 키 스트링 풀을 설정하면 다음과 같다.

1) 공용 키 스트링 풀 KP 를 서브 키 스트링 풀 $sKP_{i,j}$ 로 나누어 각 센서 노드 배치 그룹 $G_{i,j}$ 에 할당한다.
2) [그림 3]에서 서브 키 스트링 풀이 할당되지 않은 내부 그룹 $G_{1,1}$ 에 대하여는 가로, 세로 방향에 위치하는 이웃 배치 그룹에 할당된 서브 키 스트링 풀의 해쉬 값으로 얻은 스트링들을 연결하여 서브 키 스트링 풀을 구성하여 할당한다.
3) $G_{1,1}$ 를 제외한 배치 그룹들은 서로 다른 키 스트링 풀을 할당 받음과 동시에 이웃 배치 그룹과의 공유 스트링을 가진다. 또한 어느 이웃 그룹도 동일한 공유 스트링을 갖지 않을 수 있기 때문에 보안상 유리하다. $G_{1,1}$ 에 할당된 서브 키 스트링은 가로, 세로에 위치한 이웃 배치 그룹의 서브 키 스트링으로 구할 수 있으므로 공유 스트링을 가지는 효과를 가진다.
4) 배치 그룹이 3×3 이상으로 확장되는 경우, 1), 2), 3)에서 제안된 방식을 확장하여 적용한다.

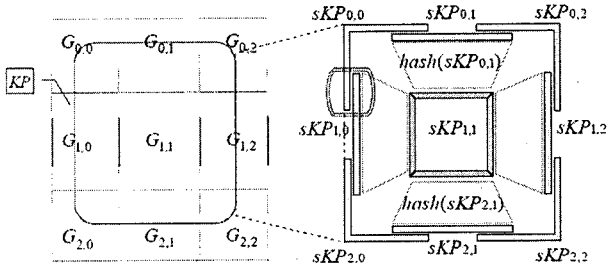

그림 3. 키 스트링 풀 설정

3.3 키 분배 및 공통 키 설정

그룹 기반 센서 노드 배치 방법을 고려한 키 스트링 풀의 설정이 오프라인으로 이루어지면, 센서 노드들은 배치 정보를 저장하고 분포된 후 키 분배 및 공통 키 설정을 한다.

1) $G_{i,j}$ 그룹에 속한 센서 노드 k 는 배치 그룹 식별자 $ID(G_{i,j})$, 서브 키 스트링 풀 $sKP_{i,j}$, 이웃하는 배치 그룹의 서브 키 스트링 풀의 일부를 구하기 위한 해쉬 함수 $h(sKP_{i,j})$ 를 저장하고 배치된다.
2) 자가 위치 추정
   - 센서 노드는 '*hello*'*msg* 를 통하여 전송 범위 내에 위치한 노드들의 그룹 식별자를 알아낸다. 대부분의 통신이 전송 범위 내에서 이루어지므로 이웃 노드들의 배치 정보는 키 분배시 유용하게 사용될 수 있다.
   - 전송 범위 내의 센서 노드들의 배치 정보를 이용하여 센서 노드 자신의 위치를 추정한다. 전송 범위 내의 노드들이 같은 배치 그룹 소속이면 배치 셀의 중앙에 가깝게, 다른 배치 그룹 소속이면 배치 셀의 경계면에 위치하는 것으로 본다.
3) 키 분배
   - 배치 셀의 중앙쪽에 배치된 경우, 같은 배치 그룹의 노드들과의 공통 키를 설정해야 하므로 저장하고 있는 서브 키 스트링 풀의 중앙 부분에서 키 스트링들을 랜덤하게 선택한다.
   - 배치 셀의 경계면에 배치된 경우, 이웃하는 배치 그룹의 노드들과 공통 키를 설정해야 하므로 저장하고 있는 서브 키 스트링 풀의 이웃 배치 그룹과의 공유 부분에서 키 스트링들을 랜덤하게 선택한다.
   - 해쉬 함수를 이용하여 생성된 서브 키 스트링 풀을 할당받은 배치 그룹의 센서 노드와의 공통 키를 설정해야 하는 경우, 저장하고 있는 서브 키 스트링 풀을 이용하여 해쉬값을 얻어 내고 랜덤하게 키 스트링들을 선택한다.
   - 키 분배 후 저장된 서브 키 스트링 풀을 삭제한다.
4) 공통 키 설정

분배된 키 스트링을 이용하여 전송 범위 내의 노드들과의 공통 키를 설정한다. 공통 키를 설정하지 못한 노드들과는 경로 키를 설정한다.

3.4 분석

제안된 키 분배 방법은 센서 네트워크의 구축 시 센서 노드들의 배치 특성과 센서 노드의 제약적 특성을 고려하여 그룹 기반 센서 네트워크 배치에 적합한 키 스트링 풀을 운용하도록 한다. 또한 배치된 센서 노드의 위치에 따라 키 스트링을 분배하여, 공통 키 설정에 필요한 키만을 집중적으로 분배하는 효과를 가진다. 이로 인하여 최소의 키를 분배하여 메모리 사용량을 줄이고, 전체 네트워크의 공통 키 설정 확률을 높일 수 있다.

4. 결 론

본 논문에서는 다량의 센서 노드들로 구성된 센서 네트워크에서의 효율적인 키 관리 방법을 제안하였다. 그룹 기반의 센서 노드 배치 방법을 고려하여 배치된 센서 노드의 위치에 따라 필요한 키를 집중적으로 분배하여 공통 키 설정 확률을 높이고, 메모리 소모량을 줄일 수 있었다. 향후 실제 네트워크 환경에 적용하여 분석하는 실험을 하고자 한다.

참 고 문 헌

[1] J.M. Kahn, R.H. Katz, and K.S.J. Pister, " Next century challenges: Mobile networking for smart dust," Proceedings of the 5th ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom' 99), pp. 483- 492, 1999.
[2] Wireless Integrated Network Sensors, University of California, Available: http://www.janet.ucla.edu/WINS.
[3] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, " A survey on sensor networks," IEEE Communications Magazine, vol. 40, no. 8, pp. 102- 114, 2002.
[4] B.C. Neuman and T. Tso, " Kerberos: An authentication service for computer networks," IEEE Communications, vol. 32, no. 9, pp. 33- 38, 1994.
[5] L. Eschenauer and V.D. Gligor, " A key management scheme for distributed sensor networks," Proceedings of the 9th ACM conference on Computer and communications security, pp. 41- 47, 2002.
[6] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen and Pramod Varshney, " A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," Proceedings of the IEEE INFOCOM' 04, pp. 586-597, 2004.
[7] B.C. Lai, D. Hwang, S. Kim, and I. Verbauwhede,, " Reducing radio energy consumption of key management protocols for wireless sensor networks," Proceedings of ACM/IEEE International Symposium on Low Power Electronics and Design (ISLPED' 04), pp. 351-356, 2004.