USN 보안을 위한 키 관리 프로토콜 제안 및 적용

이준희*, 정영지**
*원광대학교 교육대학원 정보·컴퓨터 교육전공
**원광대학교 컴퓨터공학과
e-mail:{ljhz80, yjchung}@wonkwang.ac.kr

Key Management protocol and its application for the Security of USN

Jun-hui Lee*, Yeong-Jee Chung**
*Dept of Computer Engineering, graduate school of Education
Wonkwang University
**Dept of Computer Engineering, Wonkwang University

요 약

무선 센서 네트워크는 자신의 주변 환경의 변화나 상태에 대해 감지가 가능한 센서를 가지는 센서 노드로 이루어진 네트워크이다. 하지만 센서 네트워크는 무선통신을 하고 이러한 통신을 통해 데이터가 유출되거나 변형되면 심각한 문제가 발생하게 된다. 따라서 본 논문에서는 USN의 정보보호 기술에 대해 수행된 연구들과 장단점을 살펴보고 클러스터 단위로 다항식을 사전에 분배하는 방식과 자가 위치 추정을 이용한 키 분배 메커니즘 방식을 이용 센서 노드간의 공유키가 존재할 가능성을 증가시켜 통신 채널을 쉽게 형성할 수 있도록 고안하였다.

1. 서론

무선 센서 네트워크는 자신의 주변 환경의 변화나 상태에 대해 감지가 가능한 센서를 가지는 센서 노드로 이루어진 네트워크이다. 이러한 센서 네트워크는 많은 수의 센서 노드로 이루어져 있으며 각 각의 센서 노드의 위치는 설치시 임의적으로 결정된다. 센서 노드는 환경의 변화나 상태에 따라 감지된 데이터를 단독으로 싱크노드에 전송하거나 주변의 다른 노드와 데이터를 결합하여 싱크노드로 전송하게 된다. 싱크노드는 전송받은 데이터에 기반해 규정된 특정한 작업을 수행하여 사용자가 원하는 서비스를 제공하게 된다. 또한 다양한 응용 분야를 통해 생성된 데이터는 유용하게 사용되어지기 위해 중앙에 믿을 만한 노드에게 전달되어 처리된다. 하지만 센서 네트워크는 무선통신을 하고 이러한 통신을 통해 데이터가 유출 되거나 변형되면 심각한 문제가 발생하게 된다. 이러한 이유로 센서 네트워크는 보안을 위해 사용되어지는 키 방식에 따라 대칭키방식과 비대칭키방식으로 나뉠 수 있다. [1]하지만 센서 노드는 에너지와 계산, 통신능력 면에서 한계를 가지고 있어, 상대적으로 많은 양의 계산이 필요한 비대칭키 기반의 암호화 방식은 비효율적이다. 현재 암호화방식은 대칭키 기반의 연구가 이뤄지고 있다.

본 논문의 구성은 다음과 같다. 2장에서는 센서 네트워크에서 키 분배를 위하여 지금까지 수행된 연구들과 장단점을 살펴보고 3장에서는 클러스터 단위로 다항식을 사전에 분배하는 방식에 대한 개요와 자가 위치 추정을 이용한 키 분배 메커니즘 방식을 이용 센서 노드간의 공유키가 존재할 가능성을 증가시켜, 통신 채널을 쉽게 형성할 수 있도록 하려한다. 마지막으로 4장에서는 결론 및 고찰, 향후 과제를 제시하였다.

이 논문은 2005년도 교육인적자원부 지방연구중심대학육성사업 헬스케어기술개발사업단의 지원에 의하여 연구되었음.

2. 기존 연구

최근 USN을 위한 키 분배는 크게 기반 시스템을 활용하거나 키 사전 분배 방식을 고려하고 있는 실정이다. 서브 시스템간의 통신을 위하여 게이트웨이 역할을 하는 싱크 노드를 가정함으로써 키 분배와 키 관리가 용이한 USN을 구현하는 것이다. 싱크 노드는 워크스테이션과 유사한 성능을 갖는 신뢰된 센서 노드로서, 보안에 좀더 많은 강한 환경을 구성할 수 있다. 또한 중앙의 싱크노드가 시스템 전체를 통제함으로써, 서브시스템은 인증되고 기밀성있는 통신뿐만 아니라, 인증된 브로드캐스팅을 지원할 수 있다. 따라서 정기적으로 대칭키를 갱신함으로써 키 관리가 가능하도록 하였다. 그러나 키 분배 후의 비밀성이 보장되지 않는다는 단점이 있다. 또한 실제로 강력한 기능을 가진 싱크노드가 존재하기도 어렵고, 대규모의 센서 네트워크 환경을 통제하는 것은 불가능하다. 따라서 본 논문에서는 싱크노드의 역할을 줄이면서, 전체 센서 네트워크 환경을 통제할 수 있는 방법론을 제안한다.

표 1. 키 사전분배 프로토콜의 장점과 단점
(BS: Base station)

	장점	단점
단일키	단일키 하나만 저장하면 됨.	단일키 깨지면 전체 네트워크 깨짐.
Pair-wise키	BS 없이 안전성 제공, 노드 간 상호인증 제공.	센서 노드의 자원에 비해 너무 많은 키를 저장해야함.
랜덤-키	인접한 노드와 링크 생성 가능.	어떤 두 노드 사이의 키를 다른 인접한 노드가 가질 수 있음.
q-합성수 랜덤 키 사전분배	랜덤-키 사전분배 프로토콜에 비해 안전성 증가, 적은 수의 노드가 캡쳐당했을 경우 전체 네트워크에 미치는 영향 작음.	랜덤-키 사전분배 프로토콜과 같은 문제 가짐, 인접한 노드이더라도 q를 만족하지 못하면 링크 생성하지 못함.
Multipath 키 강화 스킴	랜덤-키 사전분배 문제 해결.	경로 찾기 위한 오버헤드, 중간노드 신뢰가 전제조건.
랜덤 Pair-wise 키 스킴	BS 없이 안전성 제공, 노드 간 상호인증 제공	인접한 노드와의 Pair-wise 키가 키링에 없을 경우 링크 생성 불가능, 키가 없는 새로운 노드 추가 불가능.

또한 좌표 또는 위치를 기반으로 하는 다항식 사전 분배 방식은 다항식을 사용하기 때문에 그 다항식이 t차식일 경우 t+1개의 노드가 노출되면 그 다항식을 공유하는 모든 센서들의 키가 노출될 수 있다는 단점을 가진다.

또 다른 제안 구조는 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 반영, 위치상 가까운 배치 그룹들의 키 풀이 공유 키를 가지도록 설정한다. 각 센서 노드는 자신의 배치 그룹에 할당된 서브 키 풀에서 임의의 키들을 분배 받고 공통 키를 설정한다. 다만 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. Welnliang Du[5]는 이러한 특성을 반영하지 못하고, 센서 노드들이 이웃 배치 그룹과의 공통 키 설정을 위한 불필요한 키들을 저장하고 있어야 한다는 단점을 갖는다.

3. 제안 스킴

본 논문에서는 다항식을 공유하는 키의 수를 줄이고자 클러스터 단위로 다항식을 사전에 분배하고, 클러스터 헤드에게는 근접 노드와의 키를 사전에 분배하는 방식과 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. 따라서 본 논문에서는 이를 해결하기 위하여 클러스터 단위로 다항식을 사전에 분배하고 메모리 소모량이 적은 키 풀을 클러스터 노드들의 메모리에 미리 할당하고, 노드들의 배치 후에 자신의 위치에 따라 통신에 필요한 키를 분배하도록 한다. 이를 위하여

센서 네트워크의 target field를 육각형 모양의 클러스터 형태로 나눈다. 기존 연구에서 사용 하였던 사각의 클러스터 보다 육각구조를 사용함으로써 상호키 설립 확률을 높이는 이점을 가진다. 각 클러스터에는 클러스터 헤드가 존재 사각형에서 육각형으로 target field를 나누게 되면 클러스터 헤드가 저장해야 하는 pair-wise 키의 수는 6개지만 4개의 pair-wise키를 갖는 기존의 방법보다 직접 키 설립 확률이 더 크기 때문에 통신 채널을 설립하는 비용이 적게 든다.

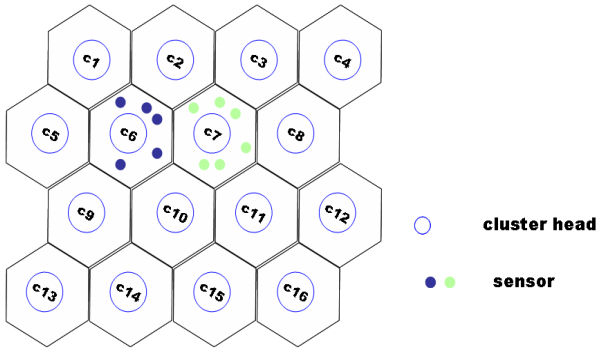
센서 네트워크의 구성요소로는 싱크노드와 클러스터 헤드, 클러스터 안에 존재하는 센서들로 구성되어 있다. 싱크 노드는 모든 정보를 수집하여 전달하는 게이트웨이 역할을 한다. 클러스터 헤드가 설치 될 위치를 싱크 노드는 정확히 알고 있어 클러스터 헤드에는 6개 이웃 클러스터에 존재하는 클러스터 헤드와의 pair-wise키가 미리 분배되어 있다.

싱크노드는 클러스터 내에 존재하는 센서들의 위치와 센서 노드들이 배치될 때 이 위치에 해당하는 다항식을 클러스터 헤드에 포함한 사전 분배 방식을 다항식을 사용한 기존의 방법들도 다항식을 사전 분배하여 이를 공유하는 센서간 키를 설립하는 기법을 사용하였다. 그러나 센서 수가 t개를 넘었을 경우에 전체 센서 네트워크 자체가 마비되는 상황이 될 수 있다.

따라서 본 논문은 기존에 제안 되었던 방법을 응용하여 클러스터에 헤드를 두어, 클러스터간 통신은 클러스터 헤드 만의 고유 키를 사용하게 함으로써 다항식을 공유하는 센서의 수를 줄일 수 있다. 또한 센서 노드들의 배치는 Welnliang Du[5] 그룹 기반 배치 모델을 적용한다. 즉 센서 네트워크 구축 시 센서 노드들은 일련의 그룹으로 나누어져 배치 지점을 중심으로 배치된다.

이와 같은 구조를 위해 가정하고 있는 내용은 다음과 같다.

- 싱크노드는 네트워크의 전송범위를 알고 있다.
- 클러스터 Ci에 존재하는 클러스터 헤드는 ID로 Ci를 사용하고 센서들은 각각의 고유한 정수 ID를 가짐.
- 클러스터간 통신은 반드시 클러스터 헤드를 통해 이루어진다.
- 패킷은 멀티홉을 거쳐 목적지에 도달할 수 있다.
- 센서 네트워크는 애드 혹 네트워크 만큼 이동성이 크지 않다.



[그림 1]

제안한 키 분배 및 그룹 기반 센서 노드 배치 방법

사전 키 분배

센서 네트워크의 target field를 s = n x n 육각 클러스터로 구획을 나누어 싱크 노드는 임의의 s개의 다항식을 생성한다. 여기서 클러스터 위치는 물리적인 위치가 아닌 논리적 위치로 생각한다. 따라서 지역 Ci에 해당 하는 다항식은 f_{ci}이 된다. 각 셀은 하나의 클러스터 헤드를 가진다. [그림1]에서 싱크 노드는 C6의 근처에 위치 하고 있는 6개의 클러스터 헤드 C1, C2, C5, C7, C9, C10와의 키 $K_{c6,c1}$, $K_{c6,c2}$.. $K_{c6,c5}$, $K_{c6,c7}$, $K_{c6,c9}$, $K_{c6,c10}$ 를 생성하여 노드에게 미리 분배 한다. 센서들의 예상 배치위치를 아는 싱크 노드는 논리 주소 C6에 위치하고자 하는 클러스터 헤드를 포함한 센서들에게 이 지역에 해당하는 다항식 f_{c6}을 할당한다.

자가 위치 추정

센서 노드는 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.

그룹 기반 배치 모델

센서 노드들의 배치는 Welnliang Du[5] 그룹 기반

배치 모델을 적용한다. 즉, 센서 네트워크 구축 시 센서 노드들은 일련의 그룹으로 나누어져 배치 지점을 중심으로 배치된다.

1) n 개의 센서 노드들은 s × 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 $f_k^{ij}(x,y|k\in G_{i,j})=f(x-x_i,y-y_j)$에 따라 배치된다 [그림 2].[3]

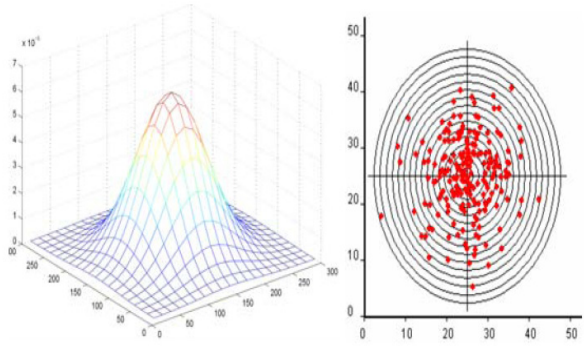


그림 2. 배치 그룹 내의 센서 노드들의 배치 형태

키 분배 및 키 추가

센서 대 센서

각 센서에 키가 사전에 분배되어 있다면 센서들은 그 정보를 이용 직접 키로 사용할 수 있다. 예를 들어 셀 C6에 배치되는 센서는 이미 이 위치에 해당하는 다항식 f_{c6}을 할당 받았기 때문에 이 셀에 위치하는 어떤 센서들과도 상대방의 ID만 알고 있으면 공통의 키를 구할 수 있다.

키 추가

센서 네트워크의 존속 기간 동안 센서들이 추가되거나 손상되는 경우가 발생 할 수 있다.

클러스터 내의 센서 노드

새로운 센서를 추가하고자 하면 싱크 노드는 새로운 센서가 위치하고자 하는 예상 지역의 그룹 기반 센서 노드 배치 방법을 고려하고 다항식을 미리 나눠주기만 하면 된다.

클러스터 헤드 노드

새로운 클러스터 헤드가 추가 되고자 하면 싱크노드는 키의 그룹 기반 센서 노드 배치 방법 중 배치 그룹내의 공통키를 설정하여 배치된 센서들에게 새로운 센서와 관련된 상호 키를 안전한 채널을 통해 알려준다.

4. 결론

본 논문에서는 다량의 센서 노드들로 구성된 센서 네트워크 환경에서의 효율적인 네트워크 구조와 키 관리 방법을 제안하였다. 본 연구는 기존 논문에서 제안 되었던 네트워크 구조와 그룹 기반의 센서 노드 배치 방법을 고려하여 배치된 센서 노드의 위치와 육각의 클러스터 형태로 센서의 target field를 나눔으로써 클러스터 헤드간에 키 설립 확률을 높였다. 향후 실제 네트워크 환경에 적용하여 분석하는 실험을 하고자 한다.

참고문헌

[1] 천은미, 도인실, 채기준, “센서 네트워크에서의 하이브리드 방식의 키 분배 구조” 2004년도 한국정보과학회 가을 학술발표논문집 Vol. 31, No.2

[2] 조정식, 여상수, 김순석, 김성권, “무선 센서 네트워크에서 정보보호를 위한 키 관리 프로토콜” 2004년도 한국정보과학회 가을 학술발표논문집 Vol. 31, No.2

[3] 김은아, 도인실, 채기준, “센서 네트워크에서의 자가 위치 추정을 이용한 키 분배 메커니즘” 한국컴퓨터종합학술대회 2005 논문집 Vol. 32, No. 1(A)

[4] 신수연, 권태경, “센서네트워크의 랜덤 키 설정 기법에 관한 연구” 한국컴퓨터종합학술대회 2005 논문집 Vol. 32, No. 1(A)

[5] 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.

[6] Donggang Liu and Peng Ning, Location-Based Pariwise Key Establishments for Static Sensor Networks, First ACM Workshop, SASN 2003.