무선 센서 네트워크에서 레벨 키를 이용한 효율적인 키 분배 방법에 관한 연구

김도회*, 최진영**, 정태명***
*성균관대학교 컴퓨터공학과
** 성균관대학교 전자전기컴퓨터공학과
***성균관대학교 정보통신공학부
e-mail : superttogi@gmail.com, jychoi@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

A Study on Key Distribution Using Level-key in Wireless Sensor Networks

Do-Hoi Kim*, Jin-Young Choi**, Tai-Myoung Chung***
*Dept. of Computer Engineering, Sungkyunkwan University
**Dept. of Electrical and Computer Engineering, Sungkyunkwan University
***School of Information Communication Engineering, Sungkyunkwan University

요 약

최근 유비쿼터스 시대가 도래하면서 센서 네트워크의 중요성이 대두되고 있다. 센서 네트워크란 필요한 모든 곳에 전자태그를 부착하고, 이를 통해 사물의 인식 정보를 기본으로 주변의 환경정보까지 각종 센서를 통해 실시간으로 수집하여 관리, 통제할 수 있도록 구성한 네트워크를 말한다. 이러한 센서 네트워크에서 각 노드들은 에너지, 계산 능력, 대역폭 등에 상당한 제한을 받으며, 정보가 저장된 장치를 쉽게 도난 당할 수도 있다. 특히 보안 통신을 하기 위해 키 설정 및 관리는 필수적이며 지금까지 그로 인해 여러 가지 키 분배 및 관리 방법이 제안되었다. 본 논문은 군대 등의 특정 상황과 같이 계층적 구조를 가지는 센서 네트워크에서 더욱 효율적으로 통신을 할 수 있는 키 관리 방법을 소개하고자 한다. 기존의 계층적 구조의 취약점을 분석하고, 이를 바탕으로 레벨 키를 제안하여 같은 레벨에서 다른 그룹간 통신이 가능한 효율적인 키 분배 방안을 제시한다.

1. 서론

최근 유비쿼터스 시대가 도래하면서 센서 네트워크의 중요성이 대두되고 있다. 센서 네트워크란 필요한 모든 곳에 전자태그를 부착하고, 이를 통해 사물의 인식 정보를 기본으로 주변의 환경정보까지 각종 센서를 통해 실시간 수집하여 관리, 통제할 수 있도록 구성한 네트워크를 말한다. 이러한 센서 네트워크는 실생활이 많은 응용되고 있다. 예를 들어, 군사적 목적으로 적군의 위치나 움직임을 파악할 수 있으며, 재난 구조시 접근이 힘든 지역에 신속히 네트워크를 구축하여 주변 환경 등의 정보를 파악할 수도 있다.

센서 네트워크는 상대적으로 많은 수의 센서 노드 때문에 ID 를 관리하는 오버헤드가 크므로 광범위한 주소 스키마를 쓰는 것은 불가능하다는 특징이 있다. 즉, IP 기반의 통신이 불가능하다. 그리고 각 센서 노드들은 에너지, 계산 능력, 대역폭 등이 제한되어 있으며, 악의적인 사용자에 의해서 정보가 쉽게 노출될 수 있다.

센서 네트워크는 거의 인프라가 없는 상태에서 무작위로 배포된 각 노드들이 라우터 역할을 겸하여 안전한 네트워크를 구축해야 하며, 센서의 수신 정보를 안전하게 보호하기 위해 보안에 사용될 비밀 키 설정과 그에 따른 키 관리가 필수적이다. 키 설정 및 관리는 관리자가 정한 보안 정책에 따라 키의 생성, 저장, 분배, 갱신, 삭제의 모든 과정을 말한다. 비밀 키의 설정 및 관리에 있어서 초기 센서 네트워크에서는 공개키 암호 방식이 먼저 대두되었다. 하지만 에너지, 그리고 관련된 노드의 계산 능력 및 통신의 제한으로 인해 공개키 암호 방식을 무선 센서 네트워크에 사용하는 것이 부적합하여 대칭키 암호 방식이나 해쉬 함수를 이용한 방식이 더 적합성을 갖게 된다[1].

이러한 센서 네트워크를 위해 다양한 키 관리 방법이 제안되었으며, 각각의 방법은 키 분배시 생기게 되는 에너지 소모를 효율적으로 관리하거나 주어진 환경에 맞춰 성능을 향상시키도록 설계되었다. 예를 들어 센서 네트워크의 여러 제한사항들을 극복하기 위해 Random Key Predistribution Scheme[1]은 각각의 노드들이 무작위한 pairwise 키를 가지며 이를 통해 상대 노드를 서로 인증하여 높은 보안성을 제공한다. 그 밖에 q-composite Random Key Predistribution Scheme[2]부터 Exclusion Basis Systems[3] 와 t-degree Bivariate Key Polynormials[4, 5]를 이용한 방법 등이 제안되었다.

특히, Xian Chen 이 제안한 방법[6]은 군대 등의 상

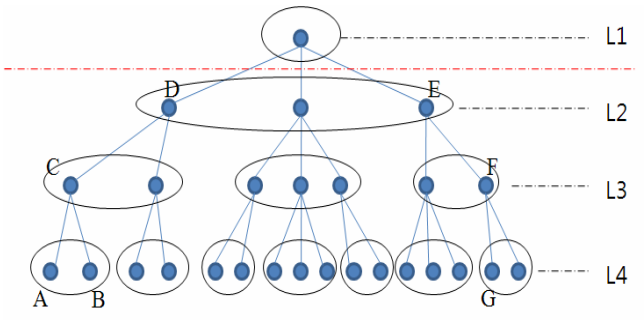
황과 같이 계층적 구조를 가지는 센서 네트워크를 위한 키 분배 방법이다. 이 방법에서 사용한 네트워크 구조는 트리 구조와 비슷한 계층적 구조를 가지고 있기 때문에 키 분배 방법이 간단하며 또한 효율적이다. 하지만 단점으로 하위 레벨의 센서끼리의 통신에서는 많은 오버헤드가 발생한다. 따라서 이를 개선하기 위해서 본 논문에서는 계층적 구조를 가지는 센서 네트워크를 위해 같은 레벨에 있는 센서 노드들끼리 레벨 키를 공유하여 좀 더 효율적으로 통신을 할 수 있는 키 관리 방법을 소개한다.

본 논문의 구성은 다음과 같이 이루어져 있다. 섹션 2 에서는 계층적 센서 네트워크 모델에 대한 관련 연구를 알아보고, 섹션 3 에서는 레벨 키를 이용한 키 분배 방법을 설명한다. 섹션 4 에서는 제안한 방법의 성능을 분석 및 평가하며, 마지막 섹션 5 에서는 결론에 대해 기술한다.

2. 관련 연구

2.1 계층적 센서 네트워크 모델 개요

Xian Chen 이 제안한 효과적인 키 분배 방법은 군대라는 특정한 상황에서 계층적 센서 네트워크를 구성하고 효과적인 키 분배 방법을 적용하고 있다[6]. 군대라는 상황에서 계층적인 형태를 갖춘 군대 조직은 주로 상위 지휘권자의 명령에 의해 하위 조직을 관리하는 프로세스로 형성된다. 각각 그룹의 구성원은 전장에 배치되기 전에 통신을 위한 센서가 주어질 것이며, 그들은 이 센서를 이용하여 통신을 한다. 다시 말하면 계층적 네트워크 구조를 사용하여 통신하는 이유는 군대라는 특징의 부대 체계 때문이다. 작은 단위의 소대들이 모여 중대를 만들고, 중대가 모여 대대를 만드는 식으로 이루어져 있으며, 대부분의 명령은 상급 부대에서 하급 부대로 전달되어 통신이 이루어진다. 따라서 네트워크의 구성이 계층적으로 되어 있어야 한다. (그림 1)은 계층적으로 구성된 센서 네트워크 모델의 예를 나타낸 것이다.



(그림 1) 계층적 센서 네트워크 구조

이 계층적 센서 네트워크에서는 다음과 같은 전제 조건을 가지고 있다.

① 그룹 내에 있는 노드들끼리는 서로 직접 통신이 가능하다.

② 상위 노드는 자신에 속한 하위 노드 모두와 각각 자유롭게 통신이 가능하다.

③ 그 이외의 통신은 이웃 노드를 거쳐서 이루어진다.

이러한 조건을 기반으로 동작하는 (그림 1)의 모델에서 A 와 B 는 같은 그룹이므로 직접 통신이 가능하다. C 는 A 와 B 의 부모 노드이므로 C 와 A, C 와 B 의 통신 역시 가능하다. 만약 A 가 D 와 통신을 하고 싶다면, A 는 먼저 C 와 통신을 한 후, C 와 D 가 통신을 하는 방법을 사용한다. 군대라는 상황을 고려할 때 다른 소대와 긴급하게 통신을 할 필요성이 생길 수 있다. 즉 A 가 자신과 다른 그룹에 속해있는 G 에게 메시지를 보내려고 한다면 A 와 C, C 와 D 의 통신을 하고, 같은 그룹 내의 D 와 E 의 통신을 한 다음, E 에서 다시 F 를 거쳐 G 와의 통신을 하게 된다.

2.2 계층적 센서 네트워크에서의 키 분배 방법

센서 노드가 전쟁터에 보내어지기 전에 루트(root)와 최하위 노드(leaf node)를 제외한 모든 노드들은 각각 네 가지 키를 받는다. 그것들은 각각 그룹 키(Group Key), 상위 단계 쌍 방향 키(Uplevel Pair-wise Key), 하위 단계 그룹 키(Downlevel Group Key), 하위 단계 쌍 방향 키(Downlevel Pair-wise Key)라고 불린다. 이중 하위 단계 쌍 방향 키만 여러 개가 있을 수 있으며, 나머지는 한 개씩만 존재한다.

최하위 노드는 그룹 키와 상위 단계 쌍 방향 키만 가지며, 루트 노드는 하위 단계 그룹 키와 하위 단계 쌍 방향 키만 가지게 된다.

- **그룹 키(Group key)**
  서로 같은 그룹의 구선원끼리 통신할 때 쓰이며 송신자는 이 키로 보낼 문장을 암호화하여 수신자에게 보내면 수신자는 이 키를 이용해 복호화하여 문장을 인식한다.

- **상위 단계 쌍 방향 키(Uplevel Pair-wise Key)**
  부모 노드와 통신할 때 암호화하는 키로 사용한다. 부모 노드가 받으면 자신의 하위 단계 쌍 방향 키로 복호화 하여 문장을 인식한다.

- **하위 단계 그룹 키(Downlevel Group Key)**
  자신에 속한 하위 단계의 모든 노드들에게 통신할 때 암호화하는 키로 사용한다. 이 때 수신자는 자신의 그룹 키를 이용해 복호화한다. 실제로 이것은 군대에서 지휘자가 병사들 전체에게 명령할 때 쓰이게 된다.

- **하위 단계 쌍 방향 키(Downlevel Pair-wise Key)**
  자식 노드와 통신을 할 때 암호화하는 키로 사용한다. 수신자는 자신의 하위 단계 쌍 방향 키로

복호화 하여 문장을 인식한다.

2.3 센서의 추가, 삭제 그리고 교체

센서의 노드를 추가할 때에는 추가하려는 노드의 상위 노드에게 하위 단계 그룹 키를 하위 단계 쌍 방향 키로 암호화 하여 받아서 이루어진다.

삭제의 경우는 삭제하려는 노드의 상위 노드가 하위 단계 그룹 키를 새로 생성한 후 그 노드를 제외한 그룹의 나머지 노드에게 각각 하위 단계 쌍 방향 키로 암호화하여 보낸다.

그리고 교체의 경우는 다음과 같다. 먼저 교체를 할 노드의 상위 노드는 새로운 하위 노드 그룹 키를 생성해서 교체가 되는 노드를 제외한 하위 그룹의 모든 노드와 새로 교체가 되어 들어오는 노드에게 각각의 하위 단계 쌍 방향 키로 암호화 하여 보내어준다. 그런 다음, 교체되어 노드에서 새로운 하위 단계 그룹 키를 생성해서 그 하위의 모든 노드들에게 하위 단계 쌍 방향 키로 암호화하여 보내어 준다.

2.4 기존 연구의 취약점

실제 군대에서 다른 소대원과의 이야기를 할 필요성이 생길 수가 있다. 예를 들어, (그림 1)에서 A 와 G 의 통신을 의미한다. 하지만 A 와 G 가 통신할 경우, 기존의 방법으로는 많은 상위 경로를 지나게 된다. 이 과정에서 이들의 통신내용을 들을 필요가 없는 상위의 지휘관까지 이 내용을 듣게 되어 불필요한 에너지 소모를 발생시킨다. 또한 지휘관이 죽으면, 그 지휘관 휘하의 모든 병사들과의 통신은 두절된다. 이것은 굉장히 큰 손실이며, 적은 상위 단계의 지휘관을 공격함으로써, 쉬운 승리를 가져올 수 있다. 이것은 모든 통신은 상위 노드를 통해서만 가능한 계층적 구조의 단점에서 기인한다.

3. 레벨 키를 이용한 효율적인 키 분배 방법

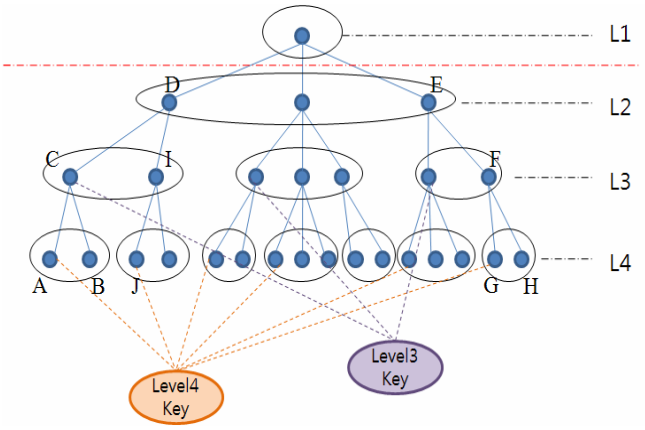
3.1 레벨 키의 정의와 기능

같은 레벨에 있는 다른 그룹의 노드와 통신을 할 경우의 많은 에너지 소모가 생기게 되는 취약점을 극복하기 위해 레벨 키(Level Key)라는 것을 추가로 제안한다. 이것의 정의와 기능은 다음과 같다.

- **레벨 키(Level Key)**

  레벨 키란 같은 레벨의 그룹 중 대표(그룹장)를 뽑아 그들끼리의 통신을 가능하게 하는 키이다. 평상시에는 같은 레벨의 다른 그룹원들끼리 통신할 때 사용되지만, 악의적인 사용자에 의해 상위 노드가 제 기능을 못하거나 에너지가 고갈되어 작동하지 않을 때 그 이하의 부대원과의 통신을 하는 우회 통로로도 사용될 수 있다. 이 레벨 키의 전제조건은 3 레벨 이상의 계층적 구조에서만 사용하게 되는 것이다. 즉 레벨 1 은 루트 하나만 존재하며, 레벨 2 에서는 그룹이 1 개만 존재하므로 그룹 키를 이용해서 통신이 가능하기 때문이다.

(그림 2)는 레벨 키를 적용한 계층적 네트워크 구조를 나타낸 것이다.



(그림 2) 레벨 키를 이용한 계층적 네트워크 구조

3.2 레벨 키 동작 메커니즘

레벨 키를 설명하기 위해 다음과 같은 표시법을 사용한다. s 는 송신자, d 는 수신자, 그리고 m 은 메시지를 뜻하며, k 는 메시지를 암호화하여 통신할 때 사용하는 키를 의미한다.

$$s \rightarrow \{d\} : \{m\}k ;$$

같은 레벨의 다른 그룹간의 통신은 이 레벨 키를 이용하여 통신한다. 예를 들어, (그림 2)에서 B 와 H 가 통신하고자 할 때에는 다음과 같은 과정을 거친다.

$$B \rightarrow \{A\} : \{m\}K_{G\{AB\}} ;$$
$$A \rightarrow \{G\} : \{m\}K_{L4} ;$$
$$G \rightarrow \{H\} : \{m\}K_{G\{GH\}} ;$$

따라서 다른 그룹과 통신하기 위해 상위 그룹을 통하여 통신하여 에너지 소모를 발생시켰던 기존의 방법과는 달리 레벨 키를 이용하여 통신 홉 수를 줄여 같은 레벨의 다른 그룹과의 통신에서 소모되는 에너지를 줄였다.

3.3 노드의 추가, 삭제, 그리고 교체

센서를 추가할 경우에는 레벨 키가 존재하는 그룹에 추가되는 것이므로 기존의 Xian Chen 가 제안한 방법과 동일하게 동작한다.

삭제할 경우에는 기존의 방법에 추가하여 하위 노드를 상위 레벨의 노드로 조정하는 메커니즘과 삭제되는 노드가 레벨 키를 가지고 있는 노드 (즉, 그룹장)일 수도 있으므로 반드시 루트에서 레벨 키를 재설정 하는 메커니즘이 함께 수반되어야 한다.

만약 (그림 2)에서 C 노드를 삭제를 할 경우에 기존의 메커니즘이 끝난 후 아래와 같은 메커니즘이 추

가된다.

$$D \rightarrow \{I\} : \{K_{G\{I\}}\}K_{DI} ;$$
$$I \rightarrow \{J\} : \{K_{G\{I\}}\}K_{IJ};$$
$$J \rightarrow \{A\} : \{K_{G\{I\}}\}K_{G\{L4\}} ;$$

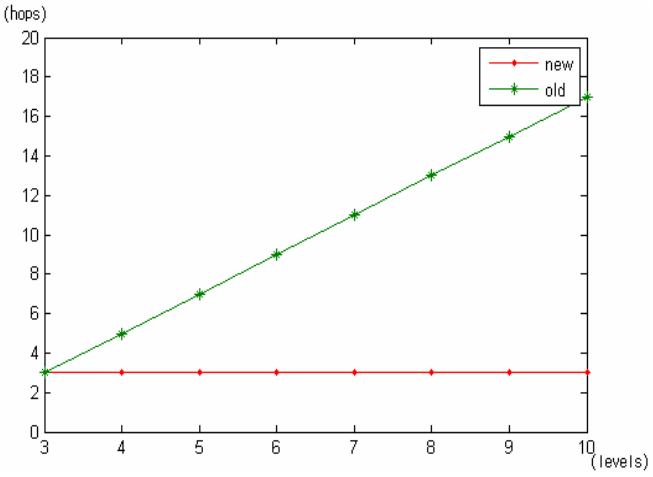
이 과정을 통해 A 가 이전의 C 자리를 대체해 지휘관 역할을 수행하게 된다. 그 후에 A 는 앞의 삭제 과정을 재귀적으로 반복하여 자신의 하위 노드들에 대한 정보를 갱신한다. 마지막으로 레벨 4 와 그 하위 레벨에 대해 루트에서 레벨 키를 재설정한다.

교체는 기존 방법대로 수행하고, 마지막에 루트에서 현재 교체가 실시된 레벨의 레벨 키를 재설정해준다.

4. 성능 평가

기존의 Xian Chen 이 제안한 효과적인 키 분배 방법은 같은 레벨에 있는 다른 그룹과 통신을 할 경우 최대 가장 멀리 떨어져 있는 그룹과 통신하려면 레벨 2 까지 메시지를 전송하고 레벨 2 의 그룹 키를 이용하여 이동한 후, 목적했던 그룹의 노드로 이동하여 통신을 한다. 예를 들어 (그림 2)에서 A 와 H 가 통신할 경우에 A 에서 C 를 거쳐 D 까지 올라갔다가 D 가 속해있는 L2 의 그룹 키를 이용해 E 까지 전송한 후 다시 F 를 거쳐 H 까지 전송이 이루어진다. 최대 홉 수는 레벨이 아래로 내려갈수록 증가되며 이것을 수식화 하면 $2 \times \{(\text{current level}) - 2\} + 1$ 이 된다.

(그림 3)에서 기존의 방법은 계층적 구조의 레벨이 증가할수록 같은 레벨의 다른 그룹과 통신하게 되는 홉 수가 증가하는 반면에 제안된 방법은 통신하고자 하는 두 노드가 모두 그룹장(레벨 키를 가지고 있는 노드)일 경우에 최대 홉 수가 생기며 이는 3 홉이 되어 에너지 소모를 효율적으로 향상 시킨 것을 보인다.



(그림 3) 같은 레벨에서 다른 그룹간 최대 통신 홉 수

5. 결론

특정 상황 즉 군대 조직과 같은 계층적 구조의 센서 네트워크에서 기존에 없던 레벨 키를 사용함으로써 다른 그룹에 속해 있는 센서끼리의 통신에서 홉 수를 줄여 더 효율적으로 통신을 할 수 있는 키 관리 방법을 제안하여 기존의 방법보다 효율적인 에너지 소모로 성능을 향상시켰다. 향후 특수한 상황뿐만 아니라 널리 사용되고 있는 환경에서 레벨 키의 효과적인 분배 방법에 대해 연구할 것이다.

참고문헌

[1] Laurent Eschenauer and Virgil D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks", In Proceedings of the 9th ACM Conference on Computer and Communication Security, Page(s):41--47

[2] Haowen Chan, Adrian Perrig and Dawn Song, "Random Key Predistribution Schemes for Sensor Networks", Security and Privacy, 2003. Proceedings. 2003 Symposium, Page(s):197-213

[3] Mohamed Eltoweissy, Ashraf Wadaa, Stephan Oariu and Larry Wilson, "Group Key Management Scheme large-scale sensor networks", J. Ad Hoc Networks, Sept. 2005, Page(s):796–802

[4] D. Liu and P. Ning, "Improving Key Pre-Distribution with Deployment Knowledge in Static Sensor Networks" ACM Trans. Sensor Networks, 2005, Page(s):204–239

[5] D. Liu, P. Ning, and W. Du, "Group-Based Key Pre-Distribution in Wireless Sensor Networks", Proc. 2005 ACM Wksp. Wireless Security (WiSe 2005), Sept. 2005, Page(s):11–20

[6] Xiao Chen and Jawad Drissi, "An Efficient Key Management Scheme in Hierarchical Sensor Networks", Mobile Adhoc and Sensor Systems Conference, 2005. IEEE International Conference