계층적 센서 네트워크에서 안전한 통신을 위한 키 갱신 프로토콜

이 주 영[†] · 박 소 영[††] · 이 상 호[†††]

요 약

센서 네트워크는 유비쿼터스 컴퓨팅 환경을 실현하기 위한 네트워크로 센싱 및 통신 능력으로 인간이 접근하기 어려운 다양한 곳에 설치되어 감시나 탐지 등을 통하여 데이터를 수집한다. 이러한 환경의 구현을 위하여 센서 네트워크에서 센서 노드가 수집한 데이터는 사용자에게 전달될 때 안전한 통신을 보장하기 위해 데이터의 암호화가 필요하다. 따라서 초소형, 빈번한 데이터 이동, 제한적인 계산 능력 및 저장 능력 그리고 배터리 전력 사용이라는 특성을 갖는 센서 노드에 알맞은 암호화를 위한 키 관리 구조가 요구된다.

본 논문은 계층 구조를 가진 센서 네트워크에 적합한 키 관리 메커니즘을 제안한다. 센서 노드는 자신의 부모 노드에게 데이터를 전달하므로 모든 센서 노드에게 데이터를 보내는 기존의 방식보다 데이터 라우팅에 소모되는 에너지를 줄일 수 있다. 그리고 센서 노드는 각 계층에 따라 다른 능력을 가지고 있으며, 능력에 따라 센서 노드에게 다른 키 생성 프로토콜을 적용한다. 본 논문에서는 키 생성을 위한 정보를 공유하는 센서 노드의 수에 제한을 두어 키가 노출되었을 때 피해 범위를 줄인다. 또한 각 센서 노드는 키 갱신을 수행하여 새로운 키를 사용하며 효과적으로 안전한 데이터 암호화를 위하여 각 계층별로 다른 주기에 따른 키 갱신을 수행한다. 따라서 데이터를 보다 안전하게 암호화하며 효율적으로 키 갱신을 수행할 수 있다.

키워드 : 센서 네트워크, 보안, 계층적, 키 갱신

Key Update Protocols in Hierarchical Sensor Networks

Jooyoung Lee[†] · Soyoung Park[††] · Sang-Ho Lee[†††]

ABSTRACT

Sensor network is a network for realizing the ubiquitous computing circumstances, which aggregates data by means of observation or detection deployed at the inaccessible places with the capacities of sensing and communication. To realize this circumstance, data which sensor nodes gathered from sensor networks are delivered to users, in which it is required to encrypt the data for the guarantee of secure communications. Therefore, it is needed to design key management scheme for encoding appropriate to the sensor nodes which feature continual data transfer, limited capacity of computation and storage and battery usage. We propose a key management scheme which is appropriate to sensor networks organizing hierarchical architecture. Because sensor nodes send data to their parent node, we can reduce routing energy. We assume that sensor nodes have different security levels by their levels in hierarchy. Our key management scheme provides different key establishment protocols according to the security levels of the sensor nodes. We reduce the number of sensor nodes which share the same key for encryption so that we reduce the damage by key exposure. Also, we propose key update protocols which take different terms for each level to update established keys efficiently for secure data encoding.

Key Words : Sensor Network, Security, Hierarchical, Key Update

1. 서 론

센서 네트워크란 센싱 기술과 통신 능력으로 유비쿼터스 환경을 구현하는 네트워크 기술로 데이터를 감지하는 센서 노드와 기반 망에 연결되어 데이터를 전달해주는 베이스 스테이션으로 구성된다. 사람의 접근이 어려운 곳에 설치되어 데이터를 수집하여 전달하는 센서 노드는 초소형, 빈번한 데이터 이동, 제한적인 계산 능력 및 저장 능력 그리고 배터리 전력 사용이라는 특성을 갖는다. 따라서 센서 노드가 수집한 데이터는 효율적인 이동을 통하여 최종 사용자에게 전송되어야 하며 센서 노드는 수집한 데이터의 안전한 통신을 보장해야하므로 제한적인 센서 노드의 특성에 알맞은 효율적인 데이터 라우팅 프로토콜과 안전한 데이터의 전달을 제공해 줄 수 있는 암호화를 위한 키 관리 구조가 요구된다.

† 준 회 원 : 이화여자대학교 컴퓨터학과 석사과정
†† 준 회 원 : 이화여자대학교 컴퓨터학과 박사과정
††† 종신회원 : 이화여자대학교 컴퓨터학과 교수
논문접수 : 2005년 12월 22일, 심사완료 : 2006년 8월 10일

데이터를 전달하는 라우팅 프로토콜에 대한 연구는 자신의 전송 범위 내 모든 센서에게 정보를 전달하는 브로드캐스팅 방법[1]과 라우팅 리스트의 경로에 따라 데이터를 전송하며 최적의 경로 발견 시 리스트를 업데이트하여 새로운 리스트를 형성하는 방법[2], 네트워크를 여러 개의 클러스터로 나누어 자신이 속한 클러스터헤드에게만 데이터를 보내는 방법[3, 4] 등이 있다. 이 중 제한된 에너지를 가지고 있는 센서의 특성을 고려하여 최소의 에너지를 사용하여 정보를 최종 사용자에게 전달할 수 있는 방법이 주로 연구되고 있다.

또한, 안전한 데이터의 전송을 위하여 데이터의 키를 이용한 암호화를 위해 다양한 키 관리 방법이 연구되고 있는데 계산력이나 에너지의 한계를 가지고 있는 센서 노드의 특성상 기존의 비대칭 키 알고리즘인 RSA 방식이나 Diffle-Hellman 방법은 사용할 수 없다. 따라서 적은 계산으로도 암호화 알고리즘을 수행할 수 있는 대칭 키 암호화 방법이 이용되고 있으며 특히, 키 셋업 서버가 사전에 키를 분배하여 각 센서 노드는 그 키를 이용하여 암호화를 수행하는 사전 키 분배 방식이 연구되고 있다.

본 논문에서는 데이터의 라우팅 에너지를 줄이기 위하여 계층에 따라 센서 노드의 능력을 달리하며 데이터를 자신의 부모 노드에게만 전송하는 계층 구조를 제안한다. 예를 들어, 환자의 몸에 부착되어 환자의 혈압, 혈당 등 데이터를 수집한 센서 노드는 침대에 설치된 센서 노드에게 전송하며, 데이터를 받은 센서 노드는 다시 입원실에 존재하는 센서 노드에게 전달한다. 입원실에 존재하는 센서 노드는 그 데이터를 병원의 중앙 데이터베이스에 저장하며 의사나 간호사는 데이터베이스 정보를 확인하여 환자 상태를 수시로 체크한다. 본 논문에서 제안한 프로토콜은 병원과 같이 센서 노드들이 비교적 고정적인 환경에서 응용될 수 있을 뿐 아니라, 센서 노드가 초기에 위치할 때 계층이 구분될 수 있는 환경에서 응용될 수 있다. 하지만 센서 노드들의 빈번한 위치 이동으로 인하여 그 계층이 쉽게 깨져 센서 노드의 계층 지정에 대한 오버헤드가 큰 환경에서는 응용될 수 없다.

또한 계층 구조간 안전한 데이터 통신을 위한 키 관리 구조를 제안한다. 적은 계산량으로도 안전한 데이터의 전송을 보장하기 위하여, 기존의 다항식 기반의 키 분배 방식과 랜덤 키 풀 기반 키 분배 방식을 응용하여 계층 구조에 적합한 키 분배 방식을 제안하고, 키의 안전성을 강화시키기 위한 효율적인 키 갱신 프로토콜을 제안한다.

본 논문은 기존 연구에서 제안하지않았던 계층별로 주기를 달리하여 키를 갱신하는 프로토콜을 제안하는데 큰 특징이 있으며, 각 갱신은 베이스 스테이션이 아닌 각 노드별로 수행한다. 이것은 베이스 스테이션의 오버헤드를 줄이며 센서 노드의 능력에 따라 주기를 달리하여 수행한다. 이러한 갱신 프로토콜을 통하여 데이터의 전방향 안정성을 보장한다.

본 논문은 1장의 서론에 이어 2장에서는 센서 네트워크에서 기존의 키 관리 기법을 설명하고, 3장에서는 제안하는 계층적 센서 네트워크에서의 키 관리 및 키 갱신 프로토콜을 기술한다. 4장에서는 제안하는 프로토콜의 안정성 및 효율성을 분석한 후 5장에서는 본 논문의 결론을 기술한다.

2. 센서 네트워크에서의 키 관리

2.1 센서 네트워크에서의 키 관리 기법

이 장에서는 지금까지 연구된 센서 네트워크에서의 키 관리 기법에 대해 살펴본다. 제한적인 능력을 가진 센서 노드 사이의 안전한 이동을 위하여 각 데이터는 키에 의해 암호화되는데 이러한 암호화를 위한 키의 생성 및 분배에 대한 연구가 진행되고 있다. 지금까지 제안된 센서 네트워크를 위한 키 관리 기법은 크게 그룹 키, pair-wise 키, 계층적 키 관리 기법으로 구분되며 본 장에서는 이와 같은 키 관리 기법에 대하여 간단히 기술한다.

키 셋업 서버가 그룹에 따라 키를 만들어서 분배하고 그룹 내 센서 노드들은 하나의 키를 이용하여 센서 노드 간 안전한 통신을 지원하는 그룹 키 방식[5,6]은 모든 센서가 하나의 그룹 키만 유지, 관리하면 되므로 키 관리에 있어서 효율적이다. 하지만 그룹 키가 노출 되었을 경우 그룹 전체의 통신이 위험에 처하는 단점이 있다.

각 센서 노드 간 서로 다른 키를 이용하는 pair-wise 키 방식은 센서 노드별로 서로 다른 키를 사용하여 각 노드와 통신하므로 키가 노출 되어도 다른 센서 노드는 안전한 통신을 보장한다는 장점이 있다. 하지만 각 센서 노드는 다른 모든 센서 노드와의 키를 저장해야하기 때문에 제한적인 저장 공간을 가지는 센서 노드에게는 제약이 따르는 단점이 있다. 그러므로 효율적인 pair-wise 키 관리 방법에 대한 다양한 연구가 진행되고 있으며 대표적으로 랜덤 키 풀 기반 방식[7, 8]과 다항식 및 그리드 기반 키 사전 분배 방식[9] 등이 있다.

다양한 보안 레벨에 따라 서로 다른 메커니즘을 이용하여 데이터의 암호화를 수행하는 계층적 키 관리 방식[10, 11]은 네트워크의 일부가 노출되어도 다른 부분은 안전할 수 있게끔 레벨 별로 보안을 달리 제공하여 효율적인 에너지 소비가 가능한 장점이 있다. 하지만 다양한 보안 레벨을 기준에 따라 정해야하는 단점을 가지고 있다.

본 논문에서는 기존의 pair-wise 키 관리 기법을 응용하여 계층적 센서 네트워크에 적합한 pair-wise 키 분배 및 갱신 프로토콜을 제안한다.

2.2 Pair-wise 키 관리 기법

이 장에서는 본 논문에서 제안하는 프로토콜에서 사용되는 대표적인 pair-wise 키 관리 방식인 랜덤 키 풀 기반 키 분배 방식과 다항식 기반 키 분배 방식에 대하여 간략하게 기술한다.

2.2.1 랜덤 키 풀 기반 키 분배

베이스 스테이션은 다수(약 $2^{17}\sim 2^{20}$개)의 랜덤 키를 생성하여 키 풀을 형성한 후, 각 센서 노드 i에게 r개의 임의의 키를 추출하여 분배한다. 이 때 센서 노드 i에게 분배된 r개의 키로 이루어진 키 셋을 키 링 KR_i라고 하며 $KR_i=\{k_1, k_2, \ldots, k_r\}$로 나타낸다. 센서 노드들은 자신의 키 링 정보를 다른 센서 노드에게 브로드캐스트하여 주고받은 후, 자신과의 공유 키를 찾은 다음 그 공유 키를 두 센서 노드 간 pair-wise 키로 사용한다. 그리고 Q-composite 방식은 노출에 따른 피해를 줄이기 위해서 랜덤 키 분배 방식을 확장하여 제안된 방법으로 두 센서 노드 사이에 적어도 q개 이상의 공유 키가 존재하도록 키 풀과 키 링을 생성한 후, q개의 키를 공유 한 다음 해쉬시켜 pair-wise 키, $K=hash(k_1||k_2||\ldots||k_q)$로 사용하는 방식이다.

이와 같이 랜덤 키 풀 기반 방식은 키 풀과 키 링의 크기에 따라 두 노드 사이에 공유 키가 존재할 확률 및 공유 키 개수가 결정되므로 항상 pair-wise 키가 생성된다고 보장할 수 없는 단점이 있다. 하지만 키 링의 형성 후 pair-wise 키 생성을 위하여 많은 계산이 필요하지 않아 계산량 및 메모리의 제약이 많은 센서 네트워크에서 사용될 수 있다.

2.2.2 다항식 기반 키 분배

베이스 스테이션은 다항식을 생성하여 자신의 다항식 풀을 생성한다. 이 다항식 풀에서 다항식을 선택하여 임의의 센서 노드에게 분배하는 것은 랜덤 키 풀 기반 키 생성 방식과 유사하나 다항식 기반 키 분배 방식은 키 셋업 서버가 직접 키를 생성하여 분배하는 대신 pair-wise 키를 유도할 수 있는 다항식을 생성하여 분배한다. 동일한 다항식을 공유하는 센서 노드는 다항식, 자신의 식별자, 상대 센서 노드의 식별자를 이용하여 pair-wise 키를 생성한다.

베이스 스테이션은 소수 q에 대한 유한체 F_q상에서 임의의 t차 이변다항식 $f(x,y)=\sum_{i,j=0}^{t} a_{ij}x^i y^j$을 생성한다. 이 때, $a_{ij}\in Z_q^*$(Z_q: 정수체)이며 다항식은 $f(x,y)=f(y,x)$를 만족한다. 이 후 각 센서 노드 i에게 변수 x 대신 센서 노드의 식별자를 입력하여 계산된 결과 값 $f(i,y)$를 분배한다. 임의의 두 센서 i와 j는 자신이 분배받은 다항식 $f(i,y)$와 $f(j,y)$의 변수 y에 상대의 식별자를 입력하여 $f(i,j)$, $f(j,i)$를 계산한다. 가정에 의하여 두 계산 값은 같으므로 두 센서 노드 사이의 pair-wise 키로서 사용될 수 있다.

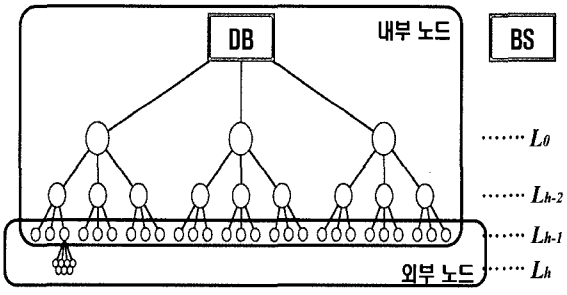
다항식 기반에서 사용하는 t차 이변 다항식은 공유한 노드의 수가 t이하일 경우 이변 다항식을 알아낼 수 없다. 즉 공격자는 최소한 $t+1$개의 센서 노드를 공격해야만 이변 다항식을 알아내어 그들 사이의 통신을 방해할 수 있으므로 최소한 $t+1$개의 노드가 공격당하지 않는 한 안전한 통신을 보장할 수 있다. 이와 같이 다항식 기반 방식은 키 생성을 위하여 센서 노드들의 계산을 필요로 하지만 센서 노드가 하나의 다항식을 공유할 경우 항상 pair-wise 키를 생성할 수 있다는 장점이 있다.

3. 계층적 센서 네트워크에서의 키 관리 프로토콜

본 논문에서 제안하는 센서 네트워크는 데이터 저장을 위한 데이터베이스(이후 DB로 표기), 키 셋업을 위한 베이스 스테이션(이후 BS로 표기) 그리고 계층적 구조를 가진 센서 노드들로 구성된다.

3.1 계층구조

DB는 최종 데이터가 저장되어 있는 데이터베이스이며 BS는 키 생성에 필요한 정보를 관리하는 키 셋업 서버이다. 계층적 구조를 가진 센서 노드들의 집합 $N=\{N_1, N_2, \ldots, N_n\}$ (n: 센서 노드의 수)은 차수(degree)가 d이고 높이가 h인 트리 형태의 구조를 가지며 이 계층 트리를 T라 한다. 트리의 각 노드는 센서 노드를 의미하며 $N_{id,l}$로 표기하는데 id는 노드의 식별 번호, l은 노드의 레벨을 나타낸다. 단, $l=0, 1, \ldots, h$ 이다. 트리의 각 레벨은 센서 노드의 계층을 나타내며 L_i로 표기하며 루트 레벨은 L_0이다. 계층 센서 네트워크 구조는 (그림 1)과 같다. DB와 레벨 L_0부터 L_{h-1} 까지 노드를 내부 노드 그룹, 레벨 L_{h-1}와 L_h의 노드를 외부 노드 그룹으로 구분하며 상위 레벨일수록 센서 노드의 메모리나 전력, 계산 능력이 증가한다. 이 때, 레벨 L_{h-1}의 노드는 내부 노드 그룹과 외부 노드 그룹에 모두 포함된다.



(그림 1) 센서 네트워크 구조

3.2 데이터 통신

센서 노드가 수집한 데이터는 자신의 부모 노드에게 전송되어 최상위 레벨 노드를 거쳐 DB로 전송된다. 또한 안전한 데이터 전송을 위해 노드 사이의 통신은 pair-wise 키를 이용하여 암호화되어 전송되는데, 이 때 임의의 두 노드 N_i와 N_j사이의 pair-wise 키를 PK_{ij}로 표기한다. 메시지 M은

PK_{ij}를 키로 하는 대칭 키 암호 알고리즘에 의해 암호화되며, 이 때 생성된 암호문을 $C = E(PK_{ij}, M)$로 표기한다.

3.3 제안한 키 관리 메커니즘

본 논문에서 제안하는 키 관리 프로토콜은 크게 계층 센서 네트워크의 외부 노드 그룹에 대한 키 관리 구조와 내부 노드 그룹에 대한 키 관리 구조로 구분된다. 이것은 센서 노드의 특성을 고려하여 적은 메모리와 계산 능력을 가진 외부 노드는 키 생성에 있어서 큰 계산을 필요로 하지 않는 랜덤 키 풀 기반의 방식을 적용하며, 상대적으로 계산 능력이 큰 내부 노드는 키 생성 시 계산 능력을 필요로 하지만 항상 키가 생성하는 것을 보장하는 다항식 기반의 키 생성 방식을 적용하기 위함이다. 키 관리 과정은 초기 설정 단계, 초기 키 생성 및 분배 단계 그리고 키 갱신 단계로 구성된다.

3.3.1 키 생성을 위한 초기 설정

BS는 내부 노드의 키 생성에 이용되는 다항식 집합 $F = \{F_1, \ldots, F_{n'}\}$(n': 다항식 개수)와 외부 노드의 키 생성에 이용되는 랜덤 키 풀 $P = \{K_1, \ldots, K_{n''}\}$(n'': 키의 개수)을 생성한다. BS는 각 다항식 F_i를 내부 노드들에게 클러스터별로 분배하는데 자세한 분배 방법은 이후에 기술한다. 또한 랜덤 키 풀에서 r개의 키를 무작위로 추출하여 키 링을 형성하고 각 키 링을 외부 노드들에게 분배한다.

가. 내부 노드

내부 노드는 BS로부터 분배받은 t차 이변다항식을 이용하여 pair-wise 키를 생성한다. 이 때 내부 노드는 클러스터로 나뉘어 클러스터별로 다른 다항식을 분배받는데 클러스터 수를 N_c 라고 하면, BS는 $n = N_c$개의 다항식을 생성한다. 하나의 클러스터는 각 노드 $N_{id,l}$를 루트로 하고 그것의 자식 노드들을 단말 노드로 하는 깊이(depth)가 2인 부트리이다. 이 클러스터를 $C_{id,l}$라 표기하며 각 클러스터 내 부모-자식 노드 사이의 키 생성을 위한 BS의 초기 설정은 다음과 같다.

1) 이변다항식 F_{id}를 $C_{id,l}$내 노드에게 분배한다.
   가) 클러스터 $C_{id,l}$의 루트 노드 $N_{id,l}$ 에게 $F_{id}(id, y)$ 분배한다.
   나) $N_{id,l}$의 자식 노드의 식별자를 j라고 할 때 자식노드는 $N_{j,l+1}$로 표기되며 $F_{id}(j, y)$를 분배한다.

나. 외부 노드

외부 노드의 pair-wise 키 생성을 위한 BS의 초기 설정 과정은 다음과 같이 진행된다.

1) $h-1$와 h레벨의 노드 수의 합이 w일 경우 P에서 r개의 키를 추출하여 w개의 키 링을 형성한다. 이 때 r는 임의의 부모-자식 노드 사이에 반드시 2개 이상의 키가 공유되도록 정한다.
2) $h-1$와 h레벨의 노드에게 각각의 키 셋을 분배하여 노드의 키 링을 형성한다. 이 때, 각 노드 $N_{id,l}$ ($l = h-1$ or h)에게 분배된 의 키 링은 KR_{id}로 표기한다.

3.3.2 Pair-wise 키 생성 및 키 갱신

센서 노드들은 BS로부터 받은 정보를 이용하여 초기 pair-wise 키를 설정한 후, 주기적으로 갱신하여 새롭게 생성한다. 매 주기마다 랜덤 수를 사용하여 새로운 키를 생성함으로써 키의 안전성을 보장한다. 키 갱신 주기는 외부 노드와 내부 노드에 따라 다르게 정의한다. 내부 노드의 키 갱신 주기를 t라 했을 때, t가 시작되는 시점에 새로운 키를 갱신하고, 두 노드 N_i와 N_j사이의 pair-wise 키는 $PK_{ij(t)}$로 표기한다. 외부 노드는 세션(session)별로 새로운 키를 갱신하는데 하나의 세션은 단말 노드가 수집한 데이터를 부모 노드에게 전송하기 시작하여 그 전송이 완료되기까지의 통신과정을 의미한다. 이 세션을 s라 했을 때 s가 시작되는 시점에 키를 생성하고, 두 노드 N_i와 N_j사이의 s번째 pair-wise 키는 $SK_{ij(s)}$라고 표기한다.

부모-자식 노드 사이이의 키 생성은 다음과 같이 초기 pair-wise 키 생성과 키 갱신 과정으로 구성된다.

가. 내부 노드

매 시간주기 t가 시작될 때 클러스터 별로 새로운 다항식 $F_{id(t)}$을 생성하여 새로운 pair-wise 키를 생성한다.

1) 초기 pair-wise 키 생성 과정($t = 0$)
   가) $N_{i,l}$, $N_{j,l+1}$: 임의의 부모-자식 노드 $N_{i,l}$, $N_{j,l+1}$ 는 다음과 같이 초기 pair-wise 키를 생성한다.
   $N_{i,l}$: $F_{i(0)}(i, j) = PK_{ij(0)}$
   $N_{j,l+1}$: $F_{i(0)}(j, i) = PK_{ji(0)}$
2) 키 갱신 과정($t = 1, \ldots, m'$)
   매 시간주기 t가 시작할 때 $PK_{ij(t)}$는 다음과 같이 갱신된다.
   가) $N_{i,l}$: $PK_{ij(t)}$의 생성에 필요한 랜덤 수 $r_{i(t)}$를 생성하여 다음과 같이 이전 키 $PK_{ij(t-1)}$를 이용하여 암호화한 후 $N_{j,l+1}$에게 전송한다.
   $E(PK_{ij(t-1)}, r_{i(t)} \| Hello)$
   나) $N_{j,l+1}$: 다음과 같은 과정을 수행한다.
   (1) $PK_{ij(t-1)}$을 이용해 암호문을 복호화하여 $r_{i(t)}$를 알아내고 새로운 랜덤 수 $r_{j(t)}$를 생성한다.
   (2) $r_{i(t)}$와 $r_{j(t)}$를 이용하여 $r_{ij(t)}$를 다음과 같이 생성한다.

$$r_{i(t)} \oplus r_{j(t)} = r_{ij(t)}$$

(3) $t-1$ 주기에서 키 생성 과정에서 사용했던 다항식 $F_{i(t-1)}$의 상수항을 $r_{ij(t)}$으로 교체하여 새로운 다항식 $F_{i(t)}$을 생성한다.

(4) $F_{i(t)}$을 이용하여 새로운 $PK_{ij(t)}$을 다음과 같이 생성한다.

$$F_{i(t)}(j, i) = PK_{ji(t)}$$

(5) $PK_{ji(t)}$를 이용하여 응답메시지 ACK을 암호화한 후, $r_{j(t)}$정보와 함께 다음과 같이 암호화하여 $N_{i,l}$에게 전송한다.

$$E(PK_{ji(t-1)},\ r_{j(t)} \| E(PK_{ij(t)},\ ACK))$$

다) $N_{i,l}$: $PK_{ij(t-1)}$를 이용하여 $r_{j(t)}$를 복호화하여 알아낸 후 $r_{i(t)}$를 이용하여 $PK_{ij(t)}$를 생성한다. $PK_{ij(t)}$의 생성과정은 $N_{j,l+1}$가 수행한 나)의 (2) ~ (4)과정과 동일하다.

나. 외부 노드

$h-1$와 h레벨의 임의의 부모-자식 노드인 $N_{j,h-1}$와 $N_{i,h}$ 는 세션 s마다 새로운 랜덤 수를 이용하여 세션 키 $SK_{ij(s)}$를 생성한다.

1) 초기 pair-wise 키 생성 과정 ($s=0$)

가) $N_{i,h}$: 자신의 키 링이 포함하는 키의 식별자를 다음과 같이 전송한다.

$Hello \| (N_{i,h}$의식별자$) \| (KR_i$가포함하는 키들의 식별자정보)

나) $N_{j,h-1}$: 받은 키 식별자 중 자신과 같은 키 식별자를 갖는 것을 발견하여 해당키의 식별자를 다음과 같이 $N_{i,h}$에게 전송한다.

($N_{j,h-1}$의 식별자)$\|$($RN_{j,h-1}$의 키 중 $N_{i,h}$가 보낸 키와 공통인 키 식별자 정보)

다) $N_{i,h}, N_{j,h-1}$: 초기 pair-wise 키를 생성한다. 두 노드 사이에 공통으로 존재하는 두 개의 키가 K_1과 K_2일 경우 다음과 같이 초기 pair-wise 키를 생성한다.

$$PK_{ij} = hash(K_1 \oplus K_2) = SK_{ij(0)}$$

2) 세션 키 생성 과정($s=1, .., m''$)

두 노드는 각 세션마다 새로운 세션 키를 사용하는데 세션 키는 단말 노드가 매 세션 s마다 생성하는 랜덤 수 $r_{(s)}$를 이용하여 생성된다.

가) $N_{i,h}$: 다음과 같은 과정을 수행한다.

(1) 각 세션마다 랜덤 수 $r_{(s)}$를 생성한다.

(2) $r_{(s)}$를 이용하여 세션 키를 다음과 같이 생성한다.

$$SK_{ij(s)} = hash(SK_{ij(s-1)} \| r_{(s)})$$

(3) $SK_{ij(s)}$를 이용하여 메시지를 암호화하고, $r_{(s)}$은 $s-1$ 세션에서 생성했던 키 $SK_{ij(s-1)}$를 이용하여 다음과 같이 암호화하여 $N_{j,h-1}$에게 전송한다.

$$E(SK_{ij(s-1)},\ r_{(s)} \| E(SK_{ij(s)}, M))$$

나) $N_{j,h-1}$: $SK_{ij(s-1)}$를 이용하여 $r_{(s)}$를 복호화한 후 가)의 (2)와 같은 방식으로 새로운 $SK_{ij(s)}$를 생성한다. 갱신된 키 $SK_{ij(s)}$을 이용하여 보낸 메시지 M을 복호화한다.

4. 분 석

본 장에서는 제안한 프로토콜의 안전성 및 효율성을 분석하고 기존의 연구와 다양한 측면에서의 비교를 기술한다.

4.1 안전성 분석

본 논문에서 센서 네트워크는 트리형태의 계층 구조를 이루며 센서 노드가 수집한 데이터는 pair-wise 키를 이용한 암호화 된 후 자신의 부모 노드에게 전달된다. 이렇게 전송된 데이터는 최종적으로 최상위 레벨의 노드를 거쳐 DB에게 전달된다. 즉, 모든 데이터는 최상위 레벨의 노드를 거쳐야만 DB로의 접근이 가능한데, 이 때 최상위 레벨의 노드는 다른 센서 노드에 비해 충분한 계산 및 저장 능력을 가지고 있다. 따라서 다른 센서 노드보다 공격자의 공격으로부터 안전하므로 DB에게 데이터를 비교적 안전하게 전송할 수 있다.

또한 pair-wise 키는 초기에 생성된 후 주기적인 갱신을 통하여 새롭게 생성된다. 이 때 키 갱신은 내부 노드와 외부 노드에 따라 다르게 진행되는데 내부 노드의 경우 초기에 동일 클러스터 내 노드는 동일한 다항식을 분배받아 키를 생성한 후 매 주기마다 랜덤 수를 생성하여 새로운 다항식을 생성한다. 즉, 각 센서 노드는 네트워크가 형성될 때 BS로부터 부모와 공유하는 다항식과 자식과 공유하는 다항식을 분배받지만 통신이 진행될수록 각 자식 노드와 공유하는 새로운 다항식을 생성하여 자식 노드의 수가 d일 경우 부모 노드와 공유하는 다항식을 포함하여 $d+1$개의 다항식을 저장한다. 따라서 자신의 부모-자식 노드 이외의 노드는 키를 알 수 없다. 마찬가지로 외부 노드도 초기에는 다른 노드들과 공통의 키 풀에서 키 링을 생성하여 pair-wise 키를 생성했지만 이후 세션마다 랜덤 수를 이용하여 새로운 세션 키를 생성한다. 따라서 자신과 통신하는 센서 노드 이외의 노드의 키는 알 수 없다. 그리고 세션 키를 사용하므로 센서 노드가 노출되어도 이전의 데이터를 복호화할 수 없으므로 전방향 안전성을 만족한다.

또한 센서 노드의 노출로 인한 키 노출 시 피해 범위를 최소화하기 위하여 하나의 다항식을 공유하는 센서 노드의 수를 줄이기 위하여 클러스터별로 서로 다른 다항식을 이용하여 키를 생성한다. 그리고 같은 클러스터 내 노드라도 키

〈표 1〉 기존 연구와 비교

비 교	다항식기반		키 풀 기반	제안한 프로토콜	
	(풀 기반)	(그리드 기반)		내부 노드 (다항식기반)	외부 노드 (키 풀 기반)
센서 노드의 키 갱신 수행	X	X	X	O	O
키 노출 시 피해 범위	동일 다항식 공유 노드	행과 열	동일 키 공유 노드	해당 센서 노드	해당 센서 노드
키 갱신 오버헤드	전체 네트워크 수행(BS수행)	행과 열 (BS수행)	전체 네트워크 수행(BS수행)	동일 클러스터 내 노드	동일 부모 노드의 자식 노드

갱신 과정 이후에는 초기에 분배받은 공통의 다항식을 더 이상 사용하지 않으므로 센서 노드들 사이에는 각각 다른 다항식에 기반한 키를 사용한다. 따라서 센서 노드가 노출되어도 노출된 센서 노드 이외의 노드에게는 영향을 끼치지 않는다. 외부 노드 또한 각 센서 노드마다 키를 갱신하여 새로운 키를 사용하므로 센서 노드가 노출되어도 노출된 센서 노드 이외의 노드에게는 영향을 끼치지 않는다. 그리고 센서 노드가 캡쳐되거나 에너지를 모두 소모하였을 경우에는 BS는 그것을 감지할 수 있으며 이 때, 임의로 그것을 대처할 수 있는 노드를 추가할 수 있다고 가정한다.

4.2 효율성 분석

제안한 프로토콜에서는 계층적 네트워크를 제안하여 수집한 데이터를 모든 노드에게 전송하는 기존의 연구와는 달리 자신의 부모 노드에게만 전송한다. 따라서 라우팅 에너지를 줄인다. 또한 계산량 및 저장 능력의 제약이 많은 외부 노드의 경우 랜덤 키 풀 기반의 키 생성 방식을 적용하여 키 생성에 있어서 많은 계산이 필요하지 않아 계산량을 줄인다. 그리고 데이터의 전송과 동시에 세션 키의 생성을 위한 정보가 전송되므로 추가적인 데이터 전송이 필요하지 않아 효율적이다.

또한 기존 다항식 기반의 키 분배 방식과 랜덤 키 풀 방식에서는 센서 노드가 노출되어 키가 노출 될 경우 해당 다항식 혹은 해당 키를 공유하는 모든 센서 노드에게 새로운 다항식이나 키 링을 분배해야 한다. 따라서 공유하는 센서 노드의 수가 많아질수록 BS의 오버헤드가 커진다. 또한 각 센서 노드의 키를 갱신하기 위해서는 모든 센서 노드에게 새로운 키를 분배하므로 BS의 오버헤드가 커지게 된다. 하지만 본 프로토콜에서는 내부 노드의 경우 클러스터별로 다항식을 공유하므로 하나의 다항식을 공유하는 센서 노드의 수가 적다. 또한 키 갱신 과정을 수행하여 키 갱신이 수행된 이후에는 각각 서로 다른 키를 사용하므로 센서 노드의 노출로 키가 노출되었을 경우 BS는 해당 센서 노드에 해당하는 키 정보만 분배한다. 그리고 BS는 각 계층별로 주기를 달리하여 새로운 다항식 혹은 키 링을 분배하므로 키 갱신을 위한 BS의 오버헤드를 줄인다.

이 프로토콜의 경우 초기 네트워크 형성 시 각 노드에게 다항식과 키 링을 형성하기 때문에 기존에 다항식만 분배할 경우, 키 링만을 분배하는 경우 보다는 초기 형성 시간이 길어질 수 있다. 하지만 이것은 초기에 단 한번만 수행되기 때문에 전체 BS의 효율성에는 큰 영향을 끼치지 않는다.

4.3 기존 연구와 비교

본 절에서는 기존의 랜덤 키 풀 기반 및 다항식 기반의 키 관리 프로토콜과 제안한 프로토콜을 비교하였다. <표 1>을 보면 제안한 프로토콜은 기존 프로토콜에 비해 키 노출 시 피해 범위를 해당 센서 노드로 줄이며 그로 인하여 키가 노출 되었을 때 해당 센서 노드에게만 키를 분배하여 BS의 키 갱신 오버헤드를 줄인다. 또한 전체 네트워크의 키를 갱신하는 다항식과 랜덤 키 풀 기반의 방식과 달리 제안한 프로토콜에서는 주기적으로 각 센서 노드끼리 키 갱신 과정을 수행하며 BS는 키 생성을 위한 정보를 일정 주기마다 각 계층별로 분배한다.

5. 결 론

센서 네트워크에서는 여러 제한적인 특성을 가진 센서 노드가 적은 계산으로도 안전한 암호화가 가능한 키 관리 방법이 필요하며 데이터 전송이 효율적으로 이루어져야 한다. 본 논문에서는 이러한 센서 노드의 특성을 고려하여 계층별로 센서 노드의 능력을 달리하는 계층 구조를 가진 센서 네트워크를 제안하여 상위 레벨과 하위 레벨의 노드에 따라 다른 키 관리 구조를 사용하였다. 또한 센서 네트워크가 형성될 때 키 생성을 위한 정보의 전달 시 센서 노드를 클러스터별로 나누어 하나의 정보를 공유하는 센서 노드의 수를 줄였다.

센서 노드가 수집한 데이터는 자신의 부모 노드에게만 전달하도록 하여 모든 센서 노드에게 브로드캐스트하여 많은

에너지가 소모되는 것을 방지하였다. 또한 센서 노드를 내부 노드와 외부 노드로 구분하여 키 분배 방식을 달리하여 안전성을 차별화하였다. 능력이 상대적으로 많은 내부 노드는 항상 키가 생성될 수 있는 다항식 기반의 키 분배 방식을 수행하였고 상대적으로 적은 메모리와 계산 능력을 가진 외부 노드에게는 항상 키가 생성된다고 보장할 수는 없지만 적은 계산으로도 키 생성이 가능한 랜덤 키 풀 기반의 키 생성 방식을 적용하여 센서 노드의 계산을 줄였다.

그리고 초기 pair-wise 키 생성 후 주기적인 키 갱신을 수행하는데 이것은 기존 계층적 센서 네트워크에서 사용하지 않았던 방식으로 이를 통하여 센서 노드가 노출되어도 이전 데이터를 복호화할 수 없어 전방향 안전성을 만족시키도록 했다. 이 때 계층별로 다른 센서 노드의 특성을 고려하여 계층별로 다른 주기를 적용하고 적은 계산으로도 키를 갱신할 수 있도록 하기 위하여 랜덤 수를 생성하여 키 갱신에 이용하였다. 또한 외부 노드의 경우 데이터의 이동과 동시에 키 갱신을 위한 정보를 함께 전달하므로 키 갱신을 위한 추가적인 정보 전달 과정을 수행하지 않는다.

또한 주기마다 해당 계층의 센서 노드만 키 갱신을 수행하므로 전체 네트워크의 키 갱신을 수행해야하는 기존의 방법보다 키 셋업 서버의 오버헤드를 줄이고 키 갱신 과정을 통하여 자신의 키를 새롭게 생성하므로 초기에 같은 정보를 받았던 다른 노드가 공격당하여 키가 노출되어도 영향을 끼치지 않는다. 이러한 프로토콜은 앞으로 센서 네트워크와 같이 제약은 많지만 안전한 데이터의 이동이 보장되어야 하는 무선 네트워크 통신에서 사용될 수 있다.

본 프로토콜은 완전 트리의 형태를 가지는 센서 네트워크를 가정하였지만 이를 확장하여 다양한 트리의 형태를 가진 센서 네트워크에 대한 연구가 필요하다.

참 고 문 헌

[1] M. Bohge and W. Trappe, "An Authentication Framework for Hierarchical Ad-Hoc Sensor Networks," Proc. of ACM Workshop on Wireless Security, pp.79-87, 2003.

[2] D. Braginsky and D. Estrin, "Rumor Routing Algorithm For Sensor Networks," Proc. of the First ACM International Workshop in Wireless Sensor Networks and Applications, pp.22-31, 2002.

[3] M. Tubaishat, J. Yin, B. Panja and S. Madria, "A Secure Hierarchical Model for Sensor Network," Proc. of ACM SIGMOD Record, Vol.33, No.1, pp.7-13, 2004.

[4] S. Doshi and A. Eswaran, "A Hierarchical Security Architecture for Group Communication in Sensor Network," Project Report, 2003.

[5] S. Zhu, S. Setia and S. Jajodia, "LEAP : Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc. of the 10th ACM Conference on CCS, pp.210-217, 2003.

[6] J. D. Richard and S. Mishra, "Security Support for In-Network Processing in Wireless Sensor Network," Proc. of ACM Workshop on SASN, pp.83-93, 2003.

[7] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. of the 9th ACM Conference on CCS, pp.41-47, 2002.

[8] H. Chan, A. Perrig and D. Song, "Random Key Predistribution Schemes for Sensor Networks," Proc. of IEEE Symposium on Security and Privacy, pp.197-213, 2003.

[9] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," Proc. of the 10th ACM Conference on CCS, pp.52-61, 2003.

[10] G. Jolly, M. C. Kuscu, P. Kokate and M. Younis, "A Low-Energy Key Management Protocol for Wireless Sensor Networks," Proc. of the 8th IEEE International Symposium on Computers and Communication, 2003.

[11] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck and M. B. Srivastava, "On Communication Security in Wireless Ad-Hoc Sensor Network," Proc. of WETICE, pp.139-144, 2002.

이 주 영

e-mail : jjoo5021@ewhain.net

2002년 2월 가톨릭대학교 컴퓨터공학과 학사

2002년 2월~2003년 11월 (주)마이크로인포

2004년 3월~현재 이화여자대학교 컴퓨터학과 석사과정

관심분야 : 정보보호, 암호프로토콜, 센서 네트워크 보안

박 소 영

e-mail : soyoung@ewhain.net

1998년 2월 이화여자대학교 컴퓨터학과 학사

2000년 2월 이화여자대학교 컴퓨터학과 석사

2000년 3월~현재 이화여자대학교 컴퓨터학과 박사과정

관심분야 : 정보보호, 암호프로토콜, 암호 알고리즘

이 상 호

e-mail : shlee@ewha.ac.kr

1979년 2월 서울대학교 계산통계학과 학사

1981년 2월 한국과학기술원 전산학과 석사

1987년 8월 한국과학기술원 전산학과 박사

1983년 9월~현재 이화여자대학교 컴퓨터학과 교수

관심분야 : 정보보호, 암호프로토콜, 알고리즘 설계, 계산기하 그래프 드로잉, 데이터 마이닝, Bioinformatics