WSN 환경에서 논리적 그룹 형성과 키 분배 방법

(A Logical Group Formation and Key Distribution Scheme in WSN)

이 재 원 † 허 준 †† 홍 충 선 †††
(Jae Won Lee) (Joon Heo) (Choong Seon Hong)

요 약 본 논문에서는 무선 센서 네트워크 환경에서 보안 서비스를 제공하고자 할 때 필수적인 안전한 그룹 관리 방법과 키 전송 방법을 다루었다. 수많은 센서 노드들로 구성되는 광범위한 네트워크로 인해 효율적인 보안 서비스 제공을 위해서는 여러 개의 보안 그룹으로 나누어 네트워크가 구성되어야 하고 그 그룹에서 사용할 그룹 키의 분배 그리고 그룹의 관리에 대한 연구가 필요하다. 본 논문에서는 센서 노드가 위치한 지리적인 정보를 통한 기존의 그룹 관리 방식이 아닌 논리적인 그룹 구성 알고리즘에 따라 효율적으로 그룹을 구성하고 관리하는 메커니즘을 제안하였다. 또한 기존 그룹 키 전송 방법은 센서 노드가 배치되기 전에 베이스 스테이션과 반드시 비밀 키를 사전에 공유하고 있어야 한다는 전제 조건을 가진다. 본 논문에서는 베이스 스테이션과 센서 노드가 비밀 키를 공유하지 않는 키 전송 메커니즘을 제안한다.

키워드 : 무선 센서 네트워크, 보안, 키, 그룹

Abstract This paper deals with essentially secure group management and key transfer methods in a wireless sensor network environment. To provide an efficient security service to a widespread network with a large number of sensor nodes, the network has to be made up by several security groups, and Group Key distribution and group management are needed. In this paper we propose a mechanism for efficiently constructing and managing a security node by constructing a group using an algorithm to construct a logical group. Previous Group Key Transport method has special condition. When Base Station transports Group Key, all sensor nodes must share Secret Key with Base Station before it is intended to be deployed. Hence, we also propose a Key transport mechanism without sharing Secret Key between Base Station and sensor node.

Key words : Wireless Sensor Networks, Security, Key, Group

1. 서 론

소형 센서 간 통신이 가능한 무선 센서 네트워크는 제한적 메모리와 프로세서, 작은 배터리 전력과 같은 물리적 제약을 가진다. 이러한 센서 네트워크를 위한 주요 연구로는 기기의 소형화, 센싱 능력의 향상, 안전하고 효율적인 라우팅, 파워 관리 등이 있다. 안전한 네트워크를 위한 보안 문제 또한 매우 중요한 요소라고 할 수 있다.

· This work was supported by MIC and ITRC Project.
† 정 회 원 : 시큐아이닷컴 연구원
jwlee@networking.khu.ac.kr
†† 학생회원 : 경희대학교 컴퓨터공학과
heojoon@khu.ac.kr
††† 종신회원 : 경희대학교 컴퓨터공학과 교수
cshong@khu.ac.kr
논문접수 : 2006년 8월 16일
심사완료 : 2007년 5월 17일

센서 네트워크는 상호간 통신을 위해 무선 매체를 사용하며, 센서는 물리적 한계를 가지므로 기존의 유무선 기술보다 보안에 더욱 취약할 수밖에 없다. 무선 매체를 사용하므로 암호화, 인증, 데이타 무결성 등이 보장되어야하나, 물리적 제약으로 인해 기존 유무선 프로토콜에서 사용된 보안 기술을 그대로 적용할 수 없다. 센서네트워크에서의 보안에 관한 주요 연구로는 인증 방법[1], 키 관리 기법[2-4], 센서 노드 간 Pairwise Key 설정 기법[5-7] 등이 있다.

Perrig등은 논문 [1]에서 대표적인 센서 네트워크 인증 방법인 'SPINS'을 제안하였다. 이 방법은 데이타의 기밀성을 제공하기 위한 SNEP 구조와 브로드캐스팅 되는 데이타 인증을 위한 μTESLA 메커니즘을 제시하고 있다.

키 관리 방법으로는 베이스 스테이션과 클러스터 구조를 중심으로 중간에 aggregator를 두는 방법[2], 각 센서 노드를 위한 네 가지 형식의 키에 대한 설정 구조와 노드간 인증 프로토콜을 제시한 방법[3], 전송되는 데이타를 그 중요도에 따라 다양한 보안 레벨을 적용하여 레벨에 따른 암호화 키를 사용하는 방법[4] 등이 제안 되었다.

Pairwise Key 설정기법으로는 키 집합을 선택하여 키 링을 생성하고 이를 분배하는 방법[5], 키를 유도할 수 있는 다항식을 생성하여 분배하는 방법[6], 보안성을 강화하기 위한 세 가지 메커니즘을 제시[7]하는 방식 등이 제안되었다.

이러한 연구들이 제안하는 보안 서비스에 앞서 우선적으로 처리되어야 하는 문제는 센서노드들의 그룹형성이다. 센서 네트워크는 다수의 센서 노드로 구성되며, 각 노드는 전송범위의 한계를 가지므로 그룹화되어야 하고, 또한 이 그룹은 안전하게 관리되어야 한다. 본 논문에서는 센서노드가 위치한 지리적인 정보를 통한 기존의 그룹 관리 방식[8-10] 대신 논리적인 그룹 구성 알고리즘에 따라 효율적으로 그룹을 형성하는 메커니즘을 제안한다. 또한, 센서 네트워크에서 키의 사전 분배를 통한 보안 유지 방식이 아닌, 사전에 키가 설정되지 않은 노드가 네트워크에 조인했을 때 Key Scramble 알고리즘을 사용해 안전하게 그룹 키를 전송하는 메커니즘을 제안한다. 본 논문은 다음과 같이 구성되었다. 2장에서는 지금까지 제안된 그룹 키 기반 보안 기법 중 그룹 구성 기술과 그룹 키 전송 기술들을 소개하고 문제점을 살펴본다. 3장에서는 제안된 논리적 그룹 구성 메커니즘과 그룹 키 전송 메커니즘의 개념과 동작과정을 상세히 설명한다. 4장에서는 시뮬레이션을 통한 성능을 평가하고, 마지막으로 결론과 향후과제에 관하여 논한다.

2. 관련 연구

2.1 그룹 키 기반 보안 기법

그룹 키 기반 보안 기법은 위치적으로 가까운 노드들끼리 그룹을 구성하여 운영하고 그룹 내 보안 유지를 위하여 그룹 키를 사용하는 기법이다. 대표적인 방법은 클러스터 구조를 중심으로 베이스 스테이션과 클러스터마다 aggregator를 두는 형태로, 이 연구에서는 각 클러스터가 하나의 그룹이 되고 각 그룹에서 보안 유지를 위해 사용할 그룹 키는 베이스 스테이션이 aggregator에게 전달하고, 다시 aggregator가 그룹 내 노드들에게 전달한다[2].

그림 1은 이 기법의 단계를 각각 표현하는 것인데, 그림에서 (a)는 그룹 선언 단계로 사전에 그룹을 나누고

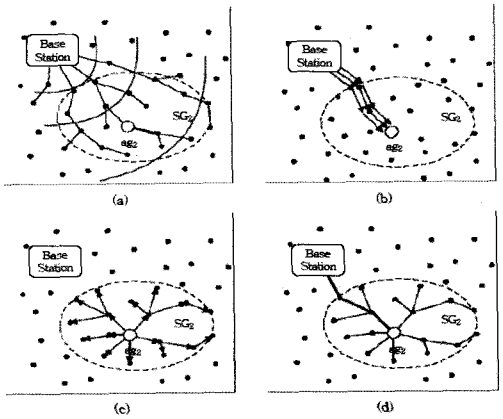

그림 1 그룹 키 기반 보안 기법의 예

aggregator를 선정하여 베이스 스테이션이 그룹의 정보와 각 그룹의 aggregator의 정보를 모든 센서노드들에게 브로드캐스트하는 단계이다. 두 번째 단계 (b)에서는 베이스 스테이션이 각 그룹의 aggregator에게 해당 그룹에 포함되는 노드와 그룹에서 사용할 그룹 키를 전달한다. (c)단계에서는 각 그룹의 aggregator가 그룹 분별 아이디와 그룹 키를 자신의 그룹에 속한 노드들에게 전달한다. 마지막 단계 (d)에서는 각 노드들이 자신이 속한 그룹을 인식하고 그룹 키를 안전하게 수신하는 단계이다.

2.2 그룹 구성 방법

앞서 언급한 그룹키 기반 보안 기법에서 중요한 문제는 그룹을 어떻게 구성할 것인가이다. 그룹 구성 방법에 관한 연구로 센서 노드들을 미리 분할된 위치에 배치하여 배치 정보를 이용하는 방법[8,10]과 노드의 물리적인 위치를 파악하는 위치 인식 시스템을 이용하는 방법이 있다.

센서 노드들의 배치 정보를 이용한 방법은 사전에 노드들을 일정 수의 그룹으로 나누어 한 번에 하나의 그룹씩 배치하는 방법으로, 노드가 배치될 센서 필드는 사전에 일정한 크기의 여러 구획으로 분할되어 있고 각 그룹은 센서 필드의 분할해 놓은 배치 포인트에 각각 배치된다. 그러나 이 방법은 그림 2처럼 항상 센서 필드를 어떻게 나눌 것인가를 사전에 결정해야 하고, 센서 노드가 수시로 조인 및 탈퇴하는 동적인 네트워크에는 적합하지 않은 단점이 있다.

또 다른 방법으로는 GPS(Global Positioning System)와 Ad-hoc 위치 인식 시스템[9,11]과 같은 위치 인식 시스템을 이용한 그룹 구성 방법이 있다.

Ad-hoc 위치 인식 시스템은 그림 3처럼 레퍼런스 노드와 일반 노드로 구성된다. 레퍼런스 노드는 자신의 위치를 미리 알고 있는 노드로 자신의 위치 정보를 담은

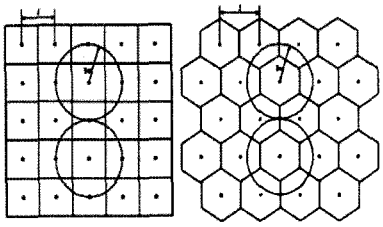

그림 2 센서 필드의 분할

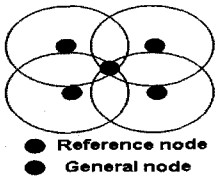

그림 3 Ad-hoc 위치 인식 시스템

비컨을 브로드캐스트 한다. 일반 노드는 레퍼런스 노드들로부터 오는 비컨들을 수집하여 자신의 위치를 계산한다[9]. 계산된 위치 정보에 따라 위치적으로 가까운 노드끼리 그룹을 형성할 수 있다. 그러나 이 방법은 일정한 전송 범위를 갖는 레퍼런스 노드가 반드시 사전에 배치되어야 하고 환경적인 장애물이나 무선 노이즈에 영향을 받는 다는 단점이 있다.

본 논문에서는 기존의 배치 정보나 위치 인식 시스템을 이용하지 않은 논리적인 그룹 구성 메커니즘을 제안한다.

2.3 그룹 키 전송 방법

그룹 키 기반 보안 기법에서 또 하나의 중요 이슈는 어떠한 방법으로 그룹 키를 안전하게 해당 그룹에 전달하는가에 관한 부분이다. 앞서 소개한 기존의 연구들은 베이스 스테이션이 노드들에게 그룹 키를 분배 할 때, 모든 센서 노드는 사전에 베이스 스테이션과 비밀 키를 갖는다는 전제 조건을 가진다.

클러스터 구조를 중심으로 베이스 스테이션과 클러스터마다 aggregator를 두는 형태의 연구에서는 각 센서 노드는 사전에 베이스 스테이션과의 1대1 비밀 키를 갖는다는 가정 하에 단방향 해시 함수와 μTESLA를 사용하여 안전한 그룹 키를 전달하는 메커니즘이다[2]. 또한 LEAP[3]은 일부 노드의 노출이 근접 이웃 노드까지 노출시키는 위협을 최소화하기 위한 키 관리 프로토콜이지만, 이 메커니즘 또한 모든 센서는 베이스 스테이션과 공유하는 비밀 키인 개인 키를 사전에 가지고 있어야 한다. 이러한 비밀 키를 통해 각 노드들은 Pairwise Key를 안전하게 설정하고, 그룹 키에 해당하는 Cluster Key는 설정된 Pairwise Key를 통해 암호화 하여 전달한다.

이러한 방법들은 그룹 키를 안전하게 전송하기 위해서는 반드시 사전에 비밀 키를 설정해야 한다는 공통적인 조건이 있다. 따라서 사전에 비밀 키를 갖지 않는 노드들이 네트워크에 조인했을 때 그룹 키를 안전하게 수신할 수 없다. 본 논문에서는 베이스 스테이션과 센서 노드 간에 사전에 비밀 키를 공유하지 않는 상태에서도 안전하게 그룹 키를 전송할 수 있는 메커니즘을 제안한다.

3. 논리적 그룹형성과 그룹 키 분배

3.1 표기 및 가정 사항

표 1은 본 논문에서 정의하여 사용한 표기들이다.

표 1 용어의 정의 및 표기

표기	설명
MC, MD	Max Children(최대 자식의 수), Max Depth(최대 깊이)
Gvalue	*GID* 할당을 위한 값
GID	그룹과 관련된 각 센서의 ID
d	Depth(깊이)
L	키의 길이
a	A primitive element of the finite GF(p) $(1 < a < p)$
p	Modulo (a prime)
x	Base Station이 생성한 비밀 값
y	node가 생성한 비밀 값
SD	*L*의 길이와 같게 랜덤으로 생성된 스크램블 데이타
ModSet	스크램블링 할 간격을 나타내는 값들의 집합
KSF, RKSF	키 스크램블링 함수, 역 키 스크램블링 함수
Hash	해쉬 함수

본 논문에서 제안하는 메커니즘은 네트워크를 트리 토폴로지로 구성한다고 가정한다. 그러므로 노드는 크게 부모 노드와 자식 노드로 나눌 수 있다. 만약 하나의 부모 노드가 수용할 수 있는 자식 노드의 수를 n이라고 하면, MC는 n과 같거나 커야 한다. 또한, 각 노드는 네트워크에 조인하기 전에 어떠한 키를 가지고 있지 않다. 그러므로 각 노드는 베이스 스테이션으로부터 키를 수신해야 한다.

3.2 Gvalue 계산

논리적인 그룹 구성 알고리즘은 *Gvalue* 계산과 *GID*의 할당으로 이루어진다. *Gvalue*는 *GID*를 할당하기 위해 사용되는 값으로, 최대 깊이를 나타내는 *MD*(Max Depth)와 최대 자식의 수를 나타내는 *MC*(Max Children)를 고려하여 각 깊이(*d*: depth)마다 그 값을 계산할 수 있다.

$$Gvalue(d) = \frac{MC^{MD-d} - 1}{MC - 1}$$

그림 4 Gvalue 유도 수식

*Gvalue*를 계산하기 위한 공식은 ZigBee NWK specification[12]을 참조하여 유도되었다. *Gvalue*를 유도하기 위한 수식은 그림 4와 같다. *MC*를 4로 *MD*를 3으로 가정하여 수식에 대입하면 각 depth별로 표 2와 같은 *Gvalue*값이 도출된다.

표 2 *MC*=4, *MD*=3일 때 *Gvalue*값 예시

d : depth	*Gvalue(d)*
0	21
1	5
2	1
3	0

3.3 GID 할당

GID 할당은 부모 노드로부터 이루어진다. 베이스 스테이션은 자신의 *GID*를 0으로 셋팅한다. 부모 노드는 자신에게 조인하는 첫 번째 노드에게는 자신의 *GID*에 1을 더하여 할당한다. 부모 노드는 자신에게 조인하는 두 번째 노드부터는 자신에게 마지막으로 조인했던 노드의 *GID*와 깊이에 따른 *Gvalue*값을 더하여 할당한다. 이 메커니즘을 의사 코드로 표현하면 그림 5와 같다.

의사 코드에서, *GIDj*는 조인하는 노드의 *GID*를 나타낸다. *GIDp*는 부모 노드의 *GID*를 나타내고, *GIDl*은 부모 노드가 마지막으로 할당한 *GID*를 나타낸다. *Gvalue(d)*는 깊이 *d*에 해당하는 *Gvalue*를 나타낸다. 그림 6은 처음 베이스 스테이션에 조인하는 노드에게 할당된 *GID*를 보여준다.

그림 6에서 0x01의 *GID*로 할당된 노드는 베이스 스테이션에 처음 조인한 노드로 *GID* 할당 알고리즘에 의해 베이스 스테이션의 *GID*인 0x00에 1을 더하여 할당되었음을 알 수 있다. 이 때 베이스 스테이션이 마지막으로 할당한 *GID*는 0x01이 된다. 그리고 또 다른 새로운 노드가 조인하였을 때 마지막으로 할당한 *GID*인 0x01에 깊이 0의 *Gvalue* 값인 21을 더한 0x22를 할당한다. 이 때 베이스 스테이션이 마지막으로 할당한 *GID*는 0x22로 갱신 되며 새로운 노드가 또 다시 조인하면 마지막으로 할당한 *GID*인 0x22에 깊이 0의 *Gvalue* 값인 21을 더한 0x43을 할당한다. 0x64의 *GID*도 같은 방식으로 할당되었음을 알 수 있다.

베이스 스테이션이 아닌 다른 노드가 자신에게 조인하는 자식노드에게 *GID*를 할당하는 것은 베이스 스테이션이 조인하는 노드에게 *GID*를 할당 하는 것과 유사하나 더해주는 *Gvalue* 값이 깊이 0의 *Gvalue* 값이 아니라 자신이 현재 존재하는 depth에 해당하는 *Gvalue* 값이어야 한다. 예를 들어, 그림 7에서 *GID*가 2인 노드는 *GID*가 1인 노드에서 봤을 때 처음 조인한 노드로 *GID* 할당 알고리즘에 의해 *GID* 1에 1을 더하여 할당되었음을 알 수 있다. 이 때, *GID* 1인 노드가 마지막으로 할당한 *GID*는 2가 된다. 그리고 새로운 노드가 또 조인하였을 때 마지막으로 할당한 *GID*인 2에 *Gvalue* 값을 더해 주는데, 이 때는 깊이 1의 *Gvalue* 값인 5를 더한 *GID* 7을 할당한다.

```
Begin
        If join sequence is for the first
        time
                GIDj ← GIDp + 1
        Else
                GIDj ← Gvalue(d) +
                       GIDl
        Endif
        assign GIDj to join node
        GIDl ← GIDj
End
```

그림 5 GID 할당 의사 코드

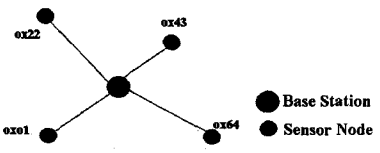

그림 6 *GID* 할당 예(깊이 1)

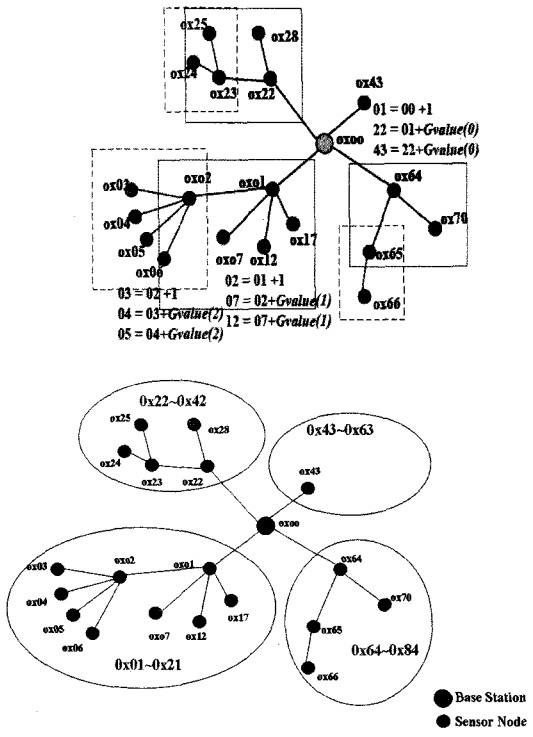

그림 7 *GID* 할당 예(MC: 4, MD: 3)

GID 할당이 끝난 후, 할당된 *GID*의 범위에 따라 그룹으로 나눌 수 있다. 그림 7에서 나타내는 것처럼, *GID* 1에서 *GID* 21까지는 첫 번째 그룹, *GID* 22에서 *GID* 42까지는 두 번째 그룹, *GID* 43에서 *GID* 63까지는 세 번째 그룹, *GID* 64에서 *GID* 84까지는 마지막 그룹인 네 번째 그룹이다.

이렇게 그룹 구성이 완료되고 각 그룹 내의 센서 노드가 자신이 속한 그룹을 인식하는 방법은 노드 자신의 *GID*를 깊이 0의 *Gvalue*인 *Gvalue*(0)으로 나눈 몫에 1을 더하여 속한 그룹을 인식한다. 예를 들어 *GID* 7의 노드는 1번 그룹(7/21+1)에 속하고, *GID* 25의 노드는 2번 그룹(25/21+1)에 속하고, *GID* 43의 노드는 3번 그룹(43/21+1 =3)에 속한다. *GID* 66의 노드는 같은 방식에 의해 4번 그룹에 속하는 것을 알 수 있다.

3.4 그룹키 전송 메커니즘

그룹키 전송 메커니즘의 핵심은 키 스크램블 알고리즘이다. 키 스크램블 알고리즘은 스크램블링 할 간격을 나타내는 값들의 집합인 *ModSet*이 필요한데, 이 범위 값을 송신 측과 수신 측이 결정하기 위하여 Diffie-Hellman 알고리즘[13]을 이용한다. *ModSet*은 *a*, *p*, *x*, *y*에 따라 결정이 된다. 예를 들어, *a*는 2, *p*는 11, *x*는 11, *y*는 4로 설정이 되었다면 Diffie-Hellman 알고리즘에 따라 $(a^x)^y \pmod p$는 $2^8 \pmod{11}$로 계산이 되고, *ModSet*은 a^1 에서 a^{xy}까지의 각 나머지들을 원소로 가진다. 이 경우, 그림 8처럼 *ModSet*이 {2, 4, 8, 5, 10, 9, 7, 3}으로 구성된다.

$$2^1 \pmod{11} = 2$$
$$2^2 \pmod{11} = 4$$
$$2^3 \pmod{11} = 8$$
$$2^4 \pmod{11} = 5$$
$$2^5 \pmod{11} = 10$$
$$2^6 \pmod{11} = 9$$
$$2^7 \pmod{11} = 7$$
$$2^8 \pmod{11} = 3$$

그림 8 *ModSet* 예시

구성된 *ModSet*은 *L*에 맞게 팽창되어야 하는데, 각 원소를 순환시키며 모든 원소 값의 합이 *L*을 넘지 않도록 팽창시킨다. *ModSet*을 팽창시키고 *ModSet*의 마지막 원소는 *L*에서 모든 원소 값의 합을 뺀 값으로 정한다. 앞의 예에서 *ModSet*이 {2, 4, 8, 5, 10, 9, 7, 3}으로 구성됐을 때 *L*이 128이라면 팽창된 *ModSet*은 {2, 4, 8, 5, 10, 9, 7, 3, 2, 4, 8, 5, 10, 9, 7, 3, 2, 4, 8, 5, 10, 3}으로 구성된다.

ModSet 구성이 완료된 후 *L*의 길이와 같게 랜덤 함수를 이용하여 *SD*를 생성한다. 그 후 *ModSet*의 원소 값에 따라 원래 키와 *SD*를 *ModSet*의 원소 값의 간격마다 바꿔가며 복사를 하여 전송할 키를 생성하고 마지막으로 전송할 키에 *ModSet*의 마지막 원소값 만큼 왼쪽으로 순환 쉬프트 연산을 수행한다.

그림 9는 베이스 스테이션과 노드 사이의 키 전송을 전체적으로 설명하고 있다.

그림 10은 베이스 스테이션에서의 내부적인 전체 동작을 나타낸다. 우선, 베이스 스테이션은 *x*를 선택한다. 그리고 나서 a^x를 계산하여 노드로 전송하고, 노드로부터 a^y를 수신한다. 다음으로 $a^{xy} \pmod p$에 따라 *ModSet*을 구성한 후 *SD*를 생성하고 키 스크램블 함수인 *KSF*를 실행한다. 마지막으로 베이스 스테이션은 왼쪽으로 순환 쉬프트 연산을 수행한 다음 *TransportKey*를 노드로 전송한다.

노드에서의 내부적인 전체 동작은 베이스 스테이션의 전체 동작과 유사하나 동작의 순서나 키 스크램블 방법이 다르다. 조인하는 노드는 수신된 *TransportKey*를

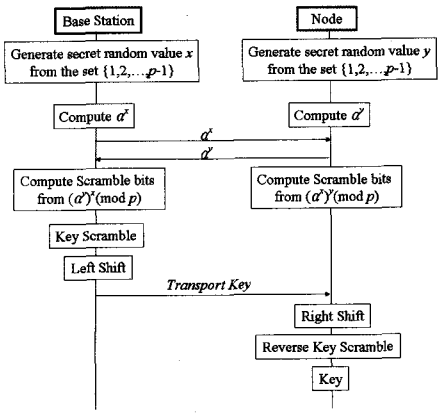

그림 9 베이스 스테이션과 노드 사이의 키 전송

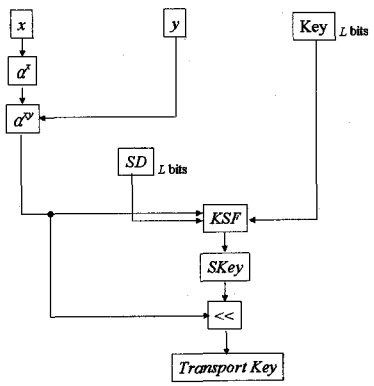

그림 10 베이스 스테이션에서의 내부 동작

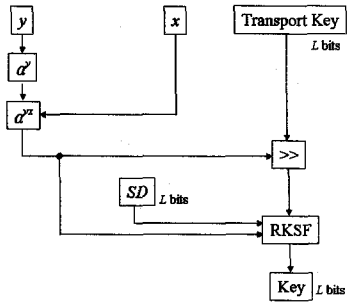

그림 11 노드에서의 내부 동작

오른쪽으로 순환 쉬프트 연산을 수행하고 키 스크램블 알고리즘을 역으로 수행하는 함수인 *RKSF*를 수행하여 네트워크에서 사용될 원래 그룹키를 생성할 수 있다. 그림 11은 노드에서의 내부적인 전체 동작을 나타낸다.

4. 성능 평가

본 논문에서 제안한 논리적 그룹 구성 메커니즘의 성능 평가를 위하여 기존의 위치 인식에 기반한 그룹 구성 방법과 논리적 그룹 형성 방법을 비교하였으며, 그룹 형성을 완료하는데 걸리는 정량적 시간을 측정하여 비교하였다.

비교 대상인 위치 인식에 기반한 그룹 구성 방법으로는 Centroid[9]를 사용하였다. Centroid는 레퍼런스 노드와 일반 이동 노드로 구성되어 있다. 각 레퍼런스 노드들은 동일한 무선 전송 범위를 가지고 네트워크에 중첩되어 배치되어 있다. 레퍼런스 노드들은 자신의 위치를 알고 있으며, 주기적으로 자신의 위치 정보를 담은 비컨을 방송한다. 각각의 이동 노드들은 특정 시간 동안 주변 레퍼런스 노드들로부터 방송되는 모든 비컨 신호를 수집한다. 각 이동 노드는 수집한 비컨 신호로 주변 레퍼런스 노드들의 위치 정보를 알 수 있으며, 연결된 모든 레퍼런스 노드들이 커버하는 중첩 영역을 자신의 위치로 인식한다. 실험에 사용된 인자 값들은 다음과 같다. 네트워크를 구성하는 노드의 수는 10개부터 300개까지 범위를 나누었고, 제안하는 그룹 구성 방법에서 네트워크를 구성하는 최대 노드의 수가 300이므로 MC값은 20, MD값은 2로 주었다.

- 최대 노드 수 :
  10,20,30,40,50,100,150,200,250,300
  (레퍼런스 노드 제외)
- Max Children(*MC*): 20
- Max Depth(*MD*): 2
- 위치 기반 그룹 구성의 완료시간 :
  네트워크에 조인하는데 걸리는 시간 + 위치 인식 시간 + 그룹화 하는데 걸리는 시간
- 논리적 그룹 구성의 완료시간 :
  Gvalue 계산 시간 + 네트워크에 조인하는데 걸리는 시간 + *GID* 할당 시간

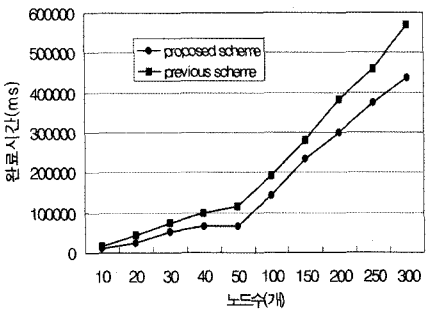

그림 12 그룹 구성 완료 시간

그림 12는 실험 결과를 나타내고 있다. 위치 인식에 기반한 그룹 구성 방법에서 그룹 구성을 완료하는데 걸리는 시간에 영향을 미치는 요소를 살펴보면, 위치 인식 기반 그룹 구성은 그룹 구성을 하기 전에 각 노드의 위치를 우선적으로 파악해야 하는데 이 때 위치 파악을 위한 딜레이가 생기며, 이 딜레이는 네트워크의 상태에 따라 매우 커질 수도 있다. 또한 위치 파악이 끝난 후 베이스 스테이션이 위치에 따라 그룹을 구성한 후 각 노드에게 노드가 어느 그룹에 속하는지 관한 정보를 전달해야 한다. 이 때 또 다시 그룹 위치 전달을 위한 딜레이가 생긴다. 제안한 논리적 그룹 구성 방법은 그룹 구성을 완료하는데 걸리는 시간에 영향을 미치는 요소는 단지 *GID*를 계산하여 할당하는 것 뿐이다. 이는 위치 인식에 기반한 그룹 구성 방법에 비해 적은 시간을 소비한다. 그림 12에서 나타내듯 네트워크를 구성하는 노도의 수가 소수일 때는 그룹 구성을 완료하는데 기존의 위치기반 방법과 제안한 논리적인 방법이 큰 차이가 없지만, 노드의 수가 증가 할수록 제안하는 논리적인 그룹 구성 방법이 그룹 구성을 완료하는데 시간이 더 적게 소모되고 있음을 알 수 있다.

다음으로 키 스크램블 알고리즘에 기반한 그룹 키 전송 메커니즘의 성능을 측정하였는데 키 전송 과정에서 베이스 스테이션에 요구되는 메모리양과 키 전송을 완료하는데 걸리는 시간을 측정하는 두 가지 실험을 하였다. 실험 환경은 다음과 같다.

- MCU : ATMEL Atemega128L(8MHz)
- Program Flash Memory : 128 Kbytes
- EEPROM : 4 Kbytes
- RAM : 36 Kbytes
- 컴파일러 : IAR AVR C compiler
- 최대 전송 속도 : 250 Kbps

- 암호화/복호화 알고리즘 : AES-CCM
- 키의 길이 : 128 bits

그림 13은 제안하는 메커니즘에서 네트워크에 조인하는 노드 수에 따른 베이스 스테이션에 요구되는 메모리 양을 측정한 것이다. 각 측정은 설정한 p(modulo) 값의 변화를 주어 이루어 졌으며 이때 선택되는 a, x, y는 가장 나쁜 경우가 아닌 일반적인 경우로 설정되었다.

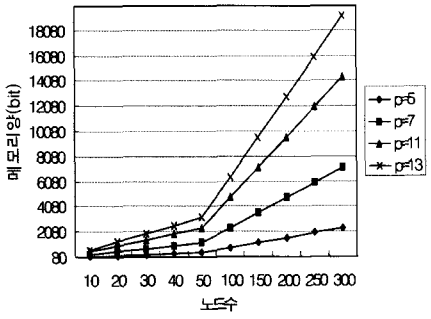

그림 13 베이스 스테이션에 요구되는 메모리양

그림 13에서 나타내듯 설정된 p 값이 클수록 요구되는 메모리양이 많다는 것을 알 수 있다. 이는 p값이 클수록 보안의 안정성은 높아지나 지나치게 높은 설정은 성능을 감소시킬 수 있음을 의미한다.

그림 14는 설정한 p 값에 따라 a, x, y가 가장 나쁜 경우로 설정되었을 때와 사전에 키를 분배하는 기존 메커니즘과의 베이스 스테이션에 요구되는 메모리양을 비교한 것이다.

비교 대상으로 사전에 키를 분배하는 방법으로는 베이스 스테이션이 먼저 다량의 랜덤 키를 생성하여 이를 키 풀(pool)에 저장하고 키 풀에서 무작위로 임의의 키 집합을 선택하여 키 링을 생성하고 이를 각 센서 노드에게 분배하는 방식[5]을 사용하였다. 이 방식은 센서 노드들이 자신이 갖고 있는 키 링의 키 정보를 이웃 노드들에게 브로드캐스팅 함으로써 무선 통신 반경 내에서 자신의 이웃하는 노드들과 공유키를 찾는다.

그림 14는 제안하는 방법에서 선택되는 a, x, y를 가장 나쁜 경우로 설정했음에도 불구하고 노드 수가 증가할수록 기존 사전 분배 방법에 비해 상대적으로 낮은 메모리를 요구하는 것을 알 수 있다.

다음은 키 전송을 완료하는데 걸리는 시간을 측정하는 실험으로 제안한 메커니즘에서 p를 11로 설정했을 때 선택되는 a, x, y에 따라 키 전송이 완료되는 시간을 측정하였다. 그림 15는 그 결과를 보여준다.

그림 15에서 선택되는 a, x, y값이 클 수록 키 전송을 완료하는데 소요되는 시간이 더 많다는 걸 알 수 있다. 이는 앞서 실험한 베이스 스테이션에 요구되는 메모리양 측정 실험에서 본 것처럼 강력한 보안과 성능의 트레이드오프 관계를 알 수 있다.

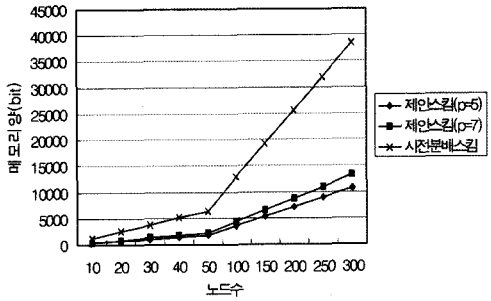

그림 14 베이스 스테이션에 요구되는 메모리양 비교

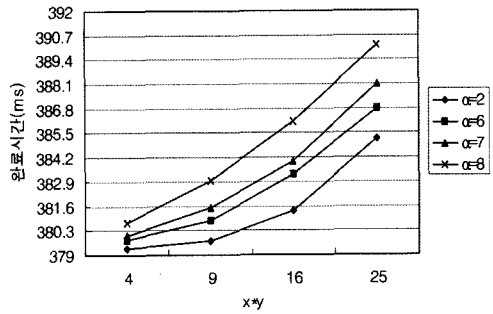

그림 15 키 전송 완료 시간

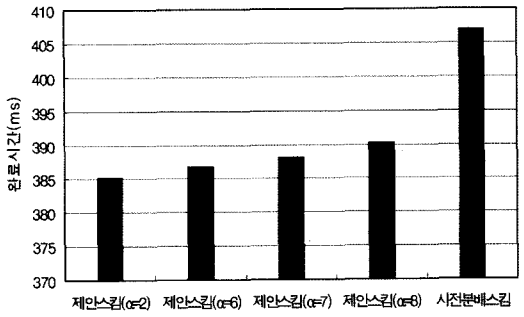

그림 16 키 전송 완료 시간 비교

그림 16은 제안하는 메커니즘과 기존의 사전 키 분배 메커니즘의 키 전송 완료 시간을 비교한 것이다. 사전 키 분배 메커니즘은 앞서 실험에서 사용했던 방식[5]을 사용하였다. 이 메커니즘에서 두 링크 또는 그 이상 떨어져 있으면서 서로 공유하는 키가 없는 임의의 두 노드가 공유키를 갖기 위해서는 Path key를 생성하여 공유한다. Path key를 설정하고자 하는 두 노드는 direct link path를 통해 키를 교환하여 공유키를 설정한다. 하나의 센서 노드가 자신의 키 링에서 사용하지 않은 키

중 하나를 path key로 설정한 후, 해당 노드까지 이르는 path 상에 있는 중간 노드들을 거쳐 상대 노드에게 전송한다. 이때, path 키 정보는 중간 노드들 간의 공유키로 암호화되어 전송된다.

그림 16은 제안한 방법이 기존의 방법보다 키 전송을 완료하는데 소요되는 시간이 더 적다는 것을 보여주는 실험으로 성능이 더 뛰어남을 알 수 있다.

위 실험들을 통하여 제안하는 센서 네트워크에서의 보안 서비스를 위한 논리적 그룹 관리 방법과 그룹 키 전송 방법이 기존의 위치 기반 그룹관리 방법과 기존 키 사전 분배 방식보다 앞서 서술한 여러 면에서 더 안정적이고 효율적임을 알 수 있다.

5. 결론 및 향후 과제

본 논문에서는 효율적으로 보안 서비스를 제공하기위해 센서 노드들을 어떻게 그룹화 하고 그룹의 보안을 위해 필요한 그룹키의 전송을 다루어 센서 네트워크 환경에서의 그룹 관리 방법을 다루었다.

그룹 구성 방법으로 기존의 GPS 또는 Ad-hoc 위치 인식 시스템 등을 이용한 센서 노드의 지리적인 위치에 기반한 그룹 구성 메커니즘에서 벗어나 최대 자식의 수와 최대 깊이를 고려한 수식을 통해 서로 겹치지 않고 노드가 속한 그룹을 쉽게 인식할 수 있는 논리적인 그룹 구성 아이디 분배를 통한 그룹 구성 메커니즘을 제시하였다. 논리적인 그룹 운영은 센서노드에 GPS수신기를 장착해야 하는 추가적인 비용을 절감할 뿐만 아니라 노드의 위치를 찾기 위해 레퍼런스 노드를 설치하고 레퍼런스 노드를 통해 노드의 위치를 인식하는 부가적인 메커니즘이 필요하지 않으므로 더 효율적이라고 할 수 있다.

또한, 본 논문에서는 노드가 센서 필드에 배치되기 전에 사전에 키를 할당하지 않는 시스템에 유용한 그룹키 전송 메커니즘을 제안하였다. 제안한 메커니즘은 사전에 키를 분배하는 메커니즘보다 그룹키를 전송하는데 시간이 더 적게 소모되고 베이스 스테이션에 요구되는 메모리양도 작아서 성능 면에서 앞선다는 것을 성능 평가를 통해 증명되었다.

향후 연구 과제로는 제안한 논리적 그룹 구성 기반 위에 구성된 그룹간의 효율적이고 보안이 유지되는 통신 메커니즘에 대한 연구를 들 수 있다. 그리고 사전에 키를 설정하지 않고 안전한 그룹키 전송을 하기 위한 메커니즘에서 키 스크램블 범위 값의 효율적인 설정과 키 스크램블 알고리즘의 최적화에 대한 연구가 필요하다. 또한 센서 네트워크의 중요 이슈인 에너지 효율에 관련하여 에너지 효율적인 그룹 운영에 관한 연구도 필요하다.

참 고 문 헌

[1] A. Perrg, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proc. of the 7th ACM/IEEE International Conference on MobiCom, 2001.

[2] J. Deng, R. Han, and S. Mishra, "Security Support for In-Network Processing in Wireless Sensor Networks," Proc. of the 1st ACM Workshop on the SASN 2003.

[3] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc. of the 10th ACM Conference on Computer and Communication Security(CCS), 2003.

[4] S. Slijepcevic, M. Potkonjak, V. Tsiatsis, S. Zimbeck and Mani B. Srivastava, "On Communication Security in Wireless Ad-Hoc Sensor," Proc. of WETICE02, 2002.

[5] L. Eschenauer and V. Gligor, "A Key-Management Scheme for Distributed Sensor Network," Proc. of the 9th ACM Conference on Computer and Communication Security, 2002.

[6] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," Proc. of the 10th ACM Conference on Computer and Communication Security(CCS), 2003.

[7] H. Chan, A. Perrig and D. Song, "Random Key-Assignment for Secure Wireless Sensor Networks," Proc. of the 1st ACM Workshop on the Security of Ad Hoc and Sensor Networks(SANS), 2003.

[8] Zhen Yu and Yong Guan, "A Key Pre-Distribution Scheme Using Deployment Knowledge for Wireless Sensor Networks," IPSN 2005. Fourth.

[9] N. Bulusu, J. Heidemann and D. Estrin, "GPS-less Low Cost Outdoor Localization for Very Small Devices," IEEE Personal Communications Magazine, 7(5):28-34, October 2000.

[10] W. Du, J. Deng, Y. S. Han, S. Chen. And P. K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment knowledge," in IEEE INFORCOM 2004.

[11] Tian He, Chengdu Huang, B. M. Blum, John A. Stankovic, and Tarek F. Abdelzaher, "Range-Free Localization Schemes in Large Scale Sensor Networks," CS-TR-2003-06. Submit to MobiCom 2003.

[12] ZigBee Document 053474r06, Version 1.0, December 14th, 2004, ZigBee Alliance.

[13] Man Young Rhee, "Internet Security," pp.161-165, WIIEY, 2003.

이 재 원

2004년 경희대학교 컴퓨터공학과(공학사). 2006년 경희대학교 컴퓨터공학과(공학석사). 2006년~현재 시큐 아이닷컴 플랫폼 그룹 기술본부 연구원. 관심분야는 보안 플랫폼, Firewall, 유무선 네트워크 보안

허 준

정보과학회논문지 : 정보통신
제 34 권 제 3 호 참조

홍 충 선

정보과학회논문지 : 정보통신
제 34 권 제 3 호 참조