# WSN에서 데이터 무결성을 보장하는 계층적인 키 관리 기법

정회원 정 윤 수*, 황 윤 철*, 이 상 호**

# An Hierarchical Key Management Scheme for Assure Data Integrity in Wireless Sensor Network

Yoon-Su Jeong*, Yoon-Cheol Hwang*, Sang-Ho Lee** ***Regular Members***

요 약

센서 네트워크의 주요 애플리케이션은 저 전력 센서 장치로 이루어진 무선 네트워크를 이용하여 악의적인 환경을 감시하고 이에 대한 정보를 유선 네트워크와 연결된 기지국으로 전송한다. 이 과정에서 개별 센서노드의 전력을 보존하기 위해서는 중간 네트워크 노드가 개별 센서로부터 전송되는 결과를 수집해야 한다. 그러나 이런 방법은 위태롭게 된 단일 센서 노드가 전체 센서 네트워크를 무용지물로 만들거나 더 심하게는 운영자로 하여금 잘못된 판독을 신뢰하게 만들 위험을 야기한다. 이 논문에서는 무선 네트워크 환경에서 중간 노드가 안전하게 데이터를 수집하면서 악의적인 센서를 해당 네트워크로부터 안전하게 제거하기 위한 프로토콜을 제안한다. 제안 프로토콜은 안전한 세션이 센서 노드와 게이트웨이 사이에서만 성립하는 다중 네트워크 구조에 유용하며 시뮬레이션을 통해 기존 LHA-SP기법과 비교분석한 결과 제안 기법이 LHA-SP 기법보다 키 관리로 인해 발생된 에너지 소비 부하가 3.5% 낮았으며, 키 전달 시간 및 처리 시간은 LHA-SP 기법보다 각각 0.3%와 0.6% 개선된 결과를 얻을 수 있었다.

**Key Words** : 무선 센서 네트워크, 계층적 키 관리, 악의적 노드, 프로토콜

ABSTRACT

A main application of sensor networks are to monitor and to send information about a possibly hostile environment to a powerful base station connected to a wired network. To conserve power from each sensor, intermediate network nodes should aggregate results from individual sensors. However, it can make it that a single compromised sensor can render the network useless, or worse, mislead the operator into trusting a false reading. In this paper, we propose a protocol to give us a key aggregation mechanism that intermediate network nodes could aggregate data more safely. The proposed protocol is more helpful at multi-tier network architecture in secure sessions established between sensor nodes and gateways. From simulation study, we compare the amount of the energy consumption overhead, the time of key transmission and the ratio of of key process between the proposed method and LHA-SP. The simulation result of proposed protocol is low 3.5% a lord of energy consumption than LHA-SP, the time of key transmission and the ration of key process is get improved result of each 0.3% and 0.6% than LHA-SP.

## Ⅰ. 서 론

최근 센서 및 컴퓨터 기술의 발전은 무선 센서 네트워크(WSNs: Wireless Sensor Networks)의 확산을 가능하게 하였다[1,2]. 센서 네트워크는 그 수량이 수개에서 수백개까지 많을 수 있으며 주로 환경으

* 충북대학교 전자계산학과 네트워크보안 연구실(bukmunro@gmail.com), (dolpin98@netsec.cbnu.ac.kr)
** 충북대학교 전기전자컴퓨터공학부 컴퓨터공학전공(shlee@chungbuk.ac.kr)
논문번호 : KICS2007-05-212, 접수일자 : 2007년 5월 8일, 최종논문접수일자 : 2007년 11 월 12일

로부터 데이터를 수집하는 데 이용되는 자원 제한적인 센서 노드로 구성된다. 일반적으로 자원이 더 많은 소수의 제어 노드가 제어 노드의 통제하에 있는 센서 노드를 제어할 수 있으면 센서 네트워크를 중앙 데이터 처리 서버와 연결할 수 있다.

센서 네트워크는 군사적 감시 및 추적, 환경 감시, 환자 간호, 유비쿼터스 전산 환경 등 다방면에 이용된다[3]. 악의적인 환경에 배치되는 센서 네트워크의 경우, 보안은 가장 중요한 이슈 중의 하나이다. 특히 무선 센서 네트워크의 경우, 적은 트래픽을 쉽게 포착하고, 또 다른 네트워크 노드로 가장하거나, 구문상 또는 의미상으로 부정확한 메시지를 고의적으로 다른 노드로 전송할 수 있다. 무선 센서 네트워크의 보안을 보장하기 위해서는 메시지를 암호화하고 통신 중인 노드를 인증해야 한다. 따라서 센서 노드간의 안전한 통신을 부트스트랩하는-즉 통신 중인 노드간에 비밀 키를 설치하는-방법은 중요한 이슈이다[4]. 보안 메커니즘을 센서 네트워크에 통합하는 것은 센서가 가지고 있는 전력 제약사항 때문에 쉬운 일이 아니다[5,6]. 현재까지 잘 알려진 보안 메커니즘은 많은 계산 및 메모리 부하를 발생시키기 때문에 센서 네트워크에는 적합하지 않다. 따라서 센서 네트워크용 보안 프로토콜 설계는 센서 자원간의 대화식에 맞춰야 한다[7-9].

최근까지 안전한 통신을 위하여 무선 센서 네트워크를 대상으로 하는 키 관리 방법에 대한 다양한 연구가 진행되어 왔다. 키 관리는 키 분배 방법에 따라 크게 3가지로 구분된다. 첫째, 신뢰된 인증서버에 의하여 키를 분배받는 방법으로 이는 센서 네트워크와 같이 구조적인 기반 구조가 없는 환경에서는 적용이 어렵다. 둘째, 공개키 인증서를 활용한 비대칭 암호화 방법으로 한정된 계산력과 에너지로 구성된 센서 노드에서 Diffie-Hellman이나 RSA 방법을 적용하는 것은 바람직하지 않다. 마지막으로 사전 키 분배 방법은 센서 노드를 배치하기 전에 키 정보를 미리 저장하는 것으로 모든 정보가 사전에 결정되어야 하나 센서 노드의 설치는 임의적으로 이루어지므로 이러한 많은 사전 지식을 보유하는 것은 어렵다.

최근 Oliveira에 의해 제안된 LHA-SP 프로토콜[18]에서는 센서 노드들의 정보를 안전하게 수집하기 위해서 센서 노드들을 계층적으로 구성하여 키 분배로 인해 발생할 수 있는 에너지 소비를 최적화하는 방법과 네트워크를 구성하고 있는 노드의 계층 레벨 정보를 이용하여 계층 간 공유키를 공유하는 방법을 제안하였다. 그러나 LHA-SP에서는 네트워크 내에 존재하는 악의적인 센서 노드가 명령 노드와 공유하게 될 공유키를 획득할 경우 명령 노드의 인증 없이 다른 노드들과 상호인증 할 수 있을 뿐만 아니라 센서 노드가 수집한 정보를 명령 노드에게 안전하게 전달할 수 없는 문제점을 가지고 있다.

이 논문에서는 LHA-SP 기법을 향상시켜 무선 센서 네트워크 환경에서 중간 노드가 안전하게 데이터를 수집하고 악의적인 센서를 네트워크로부터 효과적으로 제거하기 위한 계층적 키 관리 프로토콜을 제안한다. 제안 프로토콜의 목적은 센서 네트워크에서 센서 노드의 전력 부하를 줄이면서 중간 노드가 안전하게 데이터를 수집할 수 있도록 센서 네트워크 내의 악의적인 행위를 최소화 하는데 있다. 특히, 이 논문에서는 센서 네트워크가 수집하는 정보를 손상하려는 공격자를 네트워크에서 추출하는데 초점을 맞추고 있다. 제안 프로토콜에서는 센서 노드 내 에너지 소비를 절감하기 위해서 센서 노드간 직접적인 단 대 단 통신 대신에 홉 대 홉 경로 배정 기능을 유지하도록 하여 효율성을 극대화하였다.

이 논문은 구성은 다음과 같다. Ⅱ장에서는 센서 네트워크와 관련된 클러스터링 구조, 감시 시스템 및 기존 보안 연구의 문제점등에 대해서 기술한다. Ⅲ장에서는 악의적인 센서 노드로부터 안전하게 중간 노드가 데이터를 수집할 수 있는 계층적 키 관리 프로토콜을 제안한다. Ⅳ장에서는 제안 프로토콜의 안전성과 효율성을 입증하기 위한 대한 시뮬레이션 결과를 제공한다. 마지막으로 Ⅴ장에서는 결론을 내린다.

## Ⅱ. 관련연구

센서 네트워크에서는 센서 노드들이 필드에 배치된 이후에 안전한 네트워크를 구축하기 위해서 여러 보안 프로토콜에서 사용할 키를 생성 및 분배 해주어야 한다. 하지만 센서 노드들이 처음 설치되면 신뢰할 수 없는 상태이기 때문에 키 관리 기법은 어렵고도 중요한 부분이다. 이 장에서는 무선 센서 네트워크를 위해 기존에 연구된 키 관리 기법을 그룹 통신을 위한 키 관리, 확률적인 키 분배, pair-wise 키 관리등으로 나뉘어 장·단점을 기술하도록 한다.

### 2.1 그룹 통신을 위한 키 관리

이 방식은 그룹 간의 통신을 위하여 게이트웨이 역할을 하는 BS(Base Station)를 가정함으로써 키 분배와 키 관리가 용이한 WSN을 구현하는 것이다.

BS는 워크스테이션과 유사한 성능을 갖는 신뢰된 센서 노드로서 보안에 좀 더 강한 환경을 구성할 수 있다. 또한 중앙의 BS가 시스템 전체를 통제함으로써, 그룹은 인증되고 기밀성 있는 통신뿐만 아니라 인증된 브로드캐스팅을 지원할 수 있다. [10,12]의 키 관리 방법은 정기적으로 대칭키를 갱신함으로써 키 관리가 가능하도록 하였으나 키 분배 전후의 비밀성이 보장되지 않는 단점이 있으며, 실제로 강력한 기능을 가진 BS가 존재하기도 어려울 뿐만 아니라 대규모의 센서 네트워크 환경을 통제하는 것도 불가능하다.

[11]에서는 두 통신 주체 사이에 키를 공유하기 전에 클러스터 헤드가 자신의 멤버 호스트들을 대신하여 인증을 수행하는 방법이 제안되었다. 이 방법에서는 임의의 두 클러스터 헤드가 각자 상대편 클러스터 헤드의 공개키를 이용하여 상호인증을 수행한다. 따라서 클러스터 헤드의 공개키가 먼저 모든 클러스터 헤드에 분배되어 있어야 한다. 클러스터 헤드 간 인증 후에 대칭키 기반의 세션키가 분배되고, 이는 다시 통신 주체인 멤버 호스트에게 분배된다. 이 방법은 클러스터 헤드들이 자신의 공개키를 모든 클러스터 헤드에게 분배해야 하므로 통신 오버헤드가 크며, 두 멤버 호스트간 비밀키인 세션키 분배 시 헤드의 개인키로 암호화되어 해당 노드에 분배함으로써 세션키가 클러스터 내의 모든 호스트들에게 노출 될 수 있다.

### 2.2 확률적인 키 분배

확률적인 키 분배 방법과 랜덤 키 사전 분배 방법은 설치 전에 각 센서 노드가 대규모 키 풀로부터 부분 키 집합을 받는 것이다. 센서 노드들이 통신을 하기 위하여 임의의 두 노드는 그들의 키 집합 내에서 공통키를 찾고, 노드간 통신을 위한 공유키로 사용한다. Eschenauer-Gigor기법을 기반으로 [13]은 이들 방법에 q-composite 랜덤 키 사전 분배 방법을 적용하여 키 셋업에 대한 보안성을 강화하였다. 그러나 이 기법은 센서 네트워크 특성을 고려하지 않고, 확률적으로 랜덤하게 키를 분배하므로 센서 노드간의 공유키가 존재하지 않을 가능성이 매우 높다. 또한 공유키가 존재하더라도 공유키를 발견하는데 소용되는 시간과 에너지가 많아 에너지 사용이 효율적이지 못하다.

Blundo는 노드 사이의 충돌에 대해서 안전하도록 공통키를 계산하기 위해서 $t$ 파티 그룹으로 여러 기법들을 제안했다[14,15,16]. 이러한 기법들은 메모리 소비가 그룹 멤버에 있지 않도록 통신 비용을 줄이는데 초점을 가진다. Perriget에 의해 제안된 SPINS는 센서 네트워크에 대해 특별하게 설계된 보안 구조이다[17]. SPINS에서 각 센서 노드는 베이스 스테이션과 함께 비밀키를 공유한다. 두 센서 노드들은 직접 비밀키를 만들지 못한다. 그러나 비밀키를 설정하기 위해서는 신뢰할만한 제3자의 베이스 스테이션을 사용해야 한다. Tatebayashi, Matsuzaki와 Newman은 이동 환경에서의 자원 소비를 위해 키 분배를 생각했으며, Park의 방식보다 더 향상된 방식이다[18,19]. 그러나 공유키를 발견하는데 시간과 에너지가 많이 소요되어 효율성면에서는 효율적이지 못하다.

### 2.3 Pair-wise 키 관리

Chen[20]과 Oliveira[21]은 pair-wise 키를 사용하여 계층적 센서 네트워크 환경을 위한 키 관리 기법을 같은 시기에 제안하였다. Chen이 제시한 키 관리 기법은 계층적 센서 네트워크를 기본 구조로 하여 그룹 내의 그룹 멤버와 부모 노드사이에 직접적인 통신이 가능하다. 또한, 대칭키 암호화 방식을 기반으로 하는 사전 키 분배 방식을 이용하여 안전한 통신을 제공하고 있다. 그러나 Chen 기법은 새로운 센서 노드가 추가할 경우 하위 레벨 노드와 공유하는 pair-wise 키를 생성해서 자식 노드에게 전송 할 때, 아무런 보안 기법 없이 pair-wise키를 전송하기 때문에 악의적인 중간 노드가 있을 경우 많은 보안 공격이 발생할 수 있다.

반면, Oliveira에 의해 제안된 LHA-SP 프로토콜은 Chen이 제안한 프로토콜보다 전송과정에서 pair-wise 키를 더 보호할수 있도록 하여 이질적인 환경에서 계층적으로 구성된 센서 노드들의 정보를 안전하게 수집하고 키 분배로 인해 발생할 수 있는 네트워크 최적화 문제를 해결하고 있다[21]. LHA-SP 프로토콜에서는 홉-대-홉 통신을 제공하기 위해서 h 레벨의 노드가 h-1 레벨과 h+1 레벨 사이에서 안전하게 센싱 정보를 수집하는 하이브리드 접근 방법을 사용하지만 악의적인 센서가 명령 노드와 공유하게 될 공유키를 획득하여 그룹키를 이용할 수 있는 문제점을 가지고 있다. 또한 공유키를 보유한 센서가 계층적 레벨에 따라 재배치가 가능하여 특정 h 레벨 계층의 게이트웨이와 공유된 공유키를 제 3자가 획득하여 h 레벨 하단의 센서들과 타협될 수 있는 문제점이 있다. 이러한 보안 취약점은 센서 노드의 추가 및 재배치 시에 명확하게 나타난다. 새로운 센서 노드의 추가 시 부모 노드는 하위 레벨 pair-wise 키를 생성하여,

자식노드에게 전송하고, 자식 노드는 전송 받은 양단키를 저장한다. 여기서 부모 노드가 pair-wise 키를 생성해서 자식노드에게 전송할 때, 아무런 보안 기법 없이 pair-wise 키를 전송하기 때문에 보안에 취약하다. 또한 기존 센서 노드를 새로운 센서 노드로 교체 할 경우에도 센서 노드의 추가와 같은 보안 취약점이 발생한다. 이 논문에서는 이러한 문제점을 해결하기 위해 게이트웨이 역할을 하는 중간 노드의 보안 기능을 강화하여 계층적으로 동작되는 노드들의 정보를 보호할 수 있도록 pair-wise 키 관리 및 악의 적인 노드를 추출할 수 있는 계층적인 키 관리를 Ⅲ장에서 제안하려고 한다.

## Ⅲ. 중간 노드의 안정성을 보장하는 계층적 키 프로토콜

이 절에서는 중간 노드가 보유하고 있는 공유키를 악의적인 노드가 획득할 수 없도록 중간 노드의 보안 기능 및 관리를 강화함으로써 센서 노드의 추가 및 재배치 시에 발생할 수 있는 보안 취약점을 해결할 수 있는 계층적 키 관리 프로토콜을 제안한다.

### 3.1 가정

이 절에서는 제안 프로토콜에서 동작되는 각 객체들의 동작 가정을 다음과 같이 정의한다.

① 센서(Sensors)

센서 노드가 신뢰성이 있다거나 악의적으로 사용할 수 있다는 가정을 만들지 않는다. 각 센서 노드는 네트워크 배치전에 pair-wise 키를 부여 받으며, 네트워크가 동작되는 동안 센서는 정지된다. 그리고 센서 노드만이 센서 판독 정보를 수집 한다.

② 게이트웨이(Gateways)

네트워크상에 존재하는 모든 게이트들은 서로 직접 통신 할 수 있다. 이 때 게이트웨이간 통신은 브로드캐스트 통신을 한다고 가정한다. 또한 게이트웨이 사이에는 안전한 그룹통신을 한다고 가정한다. 통신에 사용되는 클러스터링 알고리즘은 안전한 통신 설정을 할 수 있도록 쉽게 확장할 수 있다. 게이트웨이의 주요 임무는 센서 노드로부터 전달받은 데이터를 수집 및 전송하는 역할을 한다.

③ 명령 노드(Command node)

명령노드는 센서 네트워크의 모든 노드들에 대해서 안전하고 신뢰적이라고 가정한다. 침입탐지 메커니즘은 명령 노드에서 완벽하게 동작되고, 약속된(타협된) 노드의 제거는 침입탐지 메커니즘에 따른다.

### 3.2 용어

제안된 키 관리 프로토콜은 대칭 키 메커니즘을 이용하며, 아래 표 1은 제안된 키 관리 프로토콜에서 사용되는 용어를 정의하고 있다.

### 3.3 계층적 키 관리 프로토콜

제안기법의 계층적 키 관리 프로토콜은 프로토콜 동작 방법에 따라 프로토콜 설정, 프로토콜 동작, 프로토콜 유지보수 등으로 구분된다.

#### 3.3.1 프로토콜 설정

제안 기법의 설정 구문은 키 분배와 클러스터링 과정으로 구성되며, 네트워크를 구성하고 있는 센서 노드들은 그림 1처럼 계층적으로 관리할 수 있도록 top-down 형태의 구조를 가지게 된다. 그림 1에서 중간 노드는 네트워크의 안전성을 보장하기 위해서 상위 노드와 하위 노드 사이에서 중재자 역할을 하며, 네트워크에 배치된 센서 노드는 센서 키와 ID를 오프라인으로 명령 노드에 등록하게 된다. 이 때, 에너지 효율을 극대화하기 위해서 클러스터링은 LEACH와 같은 알고리즘을 이용해 센서 노드들을 계층적으로 형성한다. 일단 클러스터가 형성되면 게이트웨이 역할을 하는 센서 노드는 구성 요소의 센서 노드용 게이트웨이 공유 키를 수신한다. 이 과정을 통해 게이트웨이와 센서 노드는 상호간의 안전한 통신에 이용되는 키를 보유하게 된다.

표 1. 용어정리

| 용어 | 개념 |
|---|---|
| C | 명령 노드 |
| $G_i$ | i번재 게이트웨이 |
| $id_i$ | 네트워크 노드 $i$의 인식자 |
| $nonce$ | 랜덤 난수 값 |
| $sdata$ | 센서 위치와 에너지 레벨을 포함한 센서정보 |
| $SN(G_i)$ | 게이트웨이 $G$에 포함된 센서 노드 집합 |
| $CK_{G_j}$ | 모든 네트워크 노드가 공유한 현 클러스터 비밀키 |
| ‖ | 전송된 메세지 |
| [ ] | 폐지를 위해 사용된 헤드 게이트웨이 |
| $E_K()$ | 키 $K$를 사용한 대칭 암호 함수 |
| $K_m$ | 모든 네트워크 노드들이 공유한 마스터 키 |
| $K_S^G$ | 게이트웨이 내의 센서 노드들간 비밀키 |
| $K_S^C$ | 센서노드와 명령 노드와의 비밀키 |
| ‘$K_G^C$ | 게이트웨이와 명령 노드와의 비밀키 |

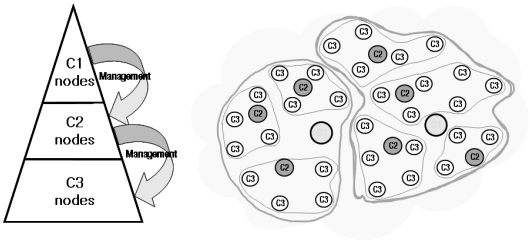



그림 1. 계층적 무선 센서 네트워크 관리 구조

제안기법에서는 계층적으로 구성된 노드들 간에 단일 홉 방식으로 모든 통신이 이루어지기 때문에 일반적으로 메시지 무결성을 보증하기 위해 사용되는 MAC(Message Authentication Code)을 사용하지 않는다. MAC 함수를 사용하지 않는 이유는 계층적 구조로 동작되는 제안기법에서는 단-대-단 통신이 아닌 홉-대-홉 통신으로 동작되어지기 때문에 $i^{th}$ 계층의 노드가 악의적인 노드에 의해서 메시지가 위조될 경우 $i^{th}$ 계층이하의 모든 노드가 보안 침해가 발생하기 때문이다. 이것은 MAC 함수가 암호학적 해쉬함수와 거의 동일하게 동작되기 때문에 사용자가 생성한 비밀키를 선택적 평문 공격(chosen plaintext)에 의해 위조 가능하기 때문이다. 통신과정 중에 메시지는 중간노드가 선택적 평문 공격과 같은 공격으로 인해 악의적으로 타협될 수 있기 때문에 단-대-단으로 전송하지 않으며 선택적 평문 공격에 의해 악의적인 동작이 없도록 하기위해 제안기법에서는 CRC(Cyclic Redundancy Check)과 같은 메커니즘을 제안기법에 적용하여 선택적 평문 공격을 예방하려고 한다. 또한 제안 기법은 CRC 메커니즘을 적용하여 사용하였기 때문에 목적지까지 전송하려고 하는 원본 메시지에 추가적인 바이트를 피할 수 있어 통신 에너지도 저장될 수 있는 장점을 가진다.

프로토콜 설정 단계의 세부적인 동작 과정은 그림 2와 같다.

- 1단계 : h 레벨에 있는 노드 $s_h$가 게이트웨이 역할을 하는 노드 $G_{h-1}$에게 $E_{K_{s_{h-2}}^{G_{h-1}}}$로 암호화된 정보를 브로드캐스트한다.

$$s_{h-2} \Rightarrow G_{h-1} : [id_{s_{h-2}} \| E_{K_m}(sdata \| nonce)]_{E_{K_{s_{h-2}}^{G_{h-1}}}}$$

- 2단계: 클러스터 형성

1단계에 의해 수신된 센서 노드들의 정보를 기반으로 게이트웨이와 관련된 센서 노드들을 LEACH[12]와 같은 클러스터링 알고리즘을 이용하여 클러스터한다.

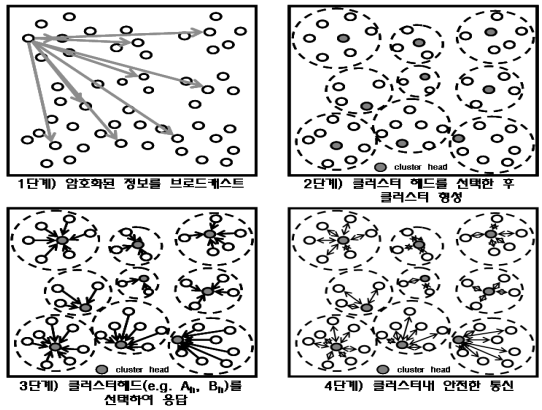



그림 2. 프로토콜 설정 단계

클러스터가 형성된 후 각 게이트웨이 $G_{h-1}$는 클러스터 내의 센서 노드 세트 $SN(G_{h-1})$를 인식하게 된다.

- 3단계: 노드들은 $G_{h-1}$로부터 자신들의 $CHs$(e.g., $A_h$,$B_h$)을 선택하여 응답한다.

$$G_{h-1} \rightarrow CH_h : [id_{s_{h-2}} \| id_{CH_h} \| s_{h-2} \in SN(G_{h-1}) = msg \| h(msg \| nonce_{G_{h-1}})]_{K_{G_{h-1}}^{CH_h}}$$

각 게이트웨이는 명령 노드와의 공유 키 $K_{G_{h-1}}^{CH_h}$로 센서 노드의 ID인 $id_{s_{h-2}}$의 목록과 게이트웨이 ID인 $id_{CH_h}$을 명령 노드에게 전달한다. $K_{G_{h-1}}^{CH_h}$로 암호화된 ID는 일종의 전자 서명 역할을 하는데, 암호화된 ID는 명령 노드에 의해 센서 노드의 정체를 검증하는데 이용된다. 그리고 해시 코드 h()는 메시지의 무결성을 확인하는 데 이용된다.

- 4단계: $CHs$는 게이트웨이와 센서 노드간 공유할 공유키 $K_{s_h}^{G_{h-1}}$를 전송한 후 각 게이트웨이는 임의로 비밀키 $CK_{G_{h-1}}$을 만든 후 클러스터내의 안전한 통신에 이용한다.

$$CH_h \rightarrow G_{h-1} : [id_{CH_h} \| id_{s_{h-2}} \| (K_{s_{h-2}}^{G_{h-1}}, s_{h-2}) \in SN(G_{h-1}) = msg \| h(msg \| nonce_{CH_h})]_{K_{G_{h-1}}^{CH_h}}$$

$$G_{h-1} \rightarrow s_h : [id_{s_h} \| CK_{G_{h-1}} \| h(CK_{G_{h-1}})]_{E_{K_{s_h}^*}}$$

### 3.3.2 프로토콜 동작

프로토콜 동작과정은 센싱 정보를 수집하는 단계와 수집된 정보를 기반으로 네트워크를 관리하는

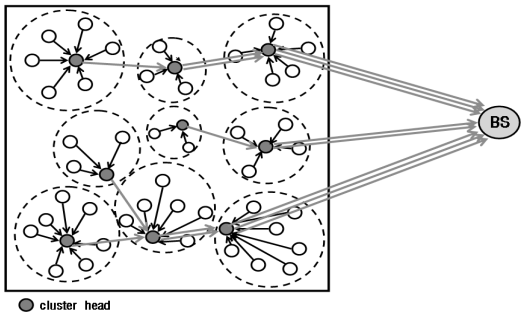


그림 3. 센싱 정보를 수집하는 단계

단계로 나뉜다.

센서 정보를 수집하는 단계에서는 단순히 센서 노드 $s_{h-2}$가 센싱 정보와 메시지 $m_{s_{h-2}}$를 비밀키 $CK_{G_{h-1}}$을 이용하여 암호화하여 전송한다. 메시지의 최신성을 위해 센서 노드 $s_{h-2}$는 센싱 정보를 암호화하기 전에 난수 $nonce_{s_{h-2}}$을 추가한다.

$$s_{h-2} \rightarrow G_{h-1} : [sensing\ information \| nonce_{s_{h-2}} \| m_{s_{h-2}}]_{CK_{G_{h-1}}}$$

각 홉에서 $G_{h-1}$는 수신된 메시지를 복호화하고 센싱 정보를 수집한 후 공유된 홉 간 비밀키를 이용하여 메시지를 암호화한 후 메시지를 포워드한다. 센싱 정보를 전달하는 과정 중 선정된 게이트웨이 $G_{h-1}$는 명령 노드에 센서 노드의 검증 데이터 $(id_{s_{h-2}})_{K_{s_{h-2}}^{CH_h}}$를 전송한다.

$$G_{h-1} \rightarrow CH_h : [id_{G_{h-1}} \| id_{CH_h} \| (id_{s_{h-2}})_{K_{s_{h-2}}^{CH_h}} \| nonce_{G_{h-1}}]_{K_{G_{h-1}}^{CH_h}}$$

네트워크를 관리하는 단계에서는 수집된 정보를 기반으로 계층간 인증된 키를 이용하여 그룹간 클러스터를 수행한다. 이 때 명령 노드에서는 센서 노드간 인증된 게이트웨이 공유키를 게이트웨이에게 전송하여 게이트웨이 내에 존재하는 노드와 안전하게 통신하기 위해 비밀 키 $CK_{G_{h-1}}$을 이용하여 다른 노드에게 클러스터 정보를 통보한다.

$$CH_h \rightarrow G_{h-1} : [nonce \| id_{s_{h-2}} \| h(id_{s_{h-2}} \| K_{S_{h-2}}^{G_{h-1}})]_{K_{G_{h-1}}^{CH_h}}$$

$$G_{h-1} \rightarrow s_{h-2} : [id_{G_{h-1}} \| CK_{G_{h-1}} \| h(id_{G_{h-1}} \| CK_{G_{h-1}})]_{K_{s_{h-2}}^{G_{h-1}}}$$

### 3.3.3 프로토콜 유지보수

유지보수 단계에서는 전송 메시지를 암호화하기 위해 홉 간 공유키를 사용하는데, 네트워크 생명주

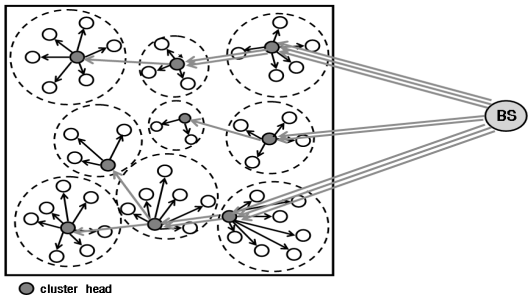


그림 4. 네트워크를 관리하는 단계

기동안 지정된 공유키를 변경하지 않고 사용할 경우 악의적인 노드의 보안 공격이 발생할 수 있다. 이런 보안 공격이 발생한다면 [21]의 경우 보안상 매우 취약하기 때문에 제안 프로토콜에서는 노드의 추가/삭제 시 클러스터 보안 키를 정기적으로 갱신하는 방법을 이용하고 있다. 다음은 클러스터 보안 키를 갱신하여 프로토콜 유지보수 과정을 보여주고 있다.

- 1단계: 게이트웨이는 *prepare*_key_renewal 메시지를 그 구성 요소 센서 노드에 전송함으로써 이들 센서 노드가 현재 클러스터 키 $CK_{G_{h-1}}$를 갱신할 수 있도록 한다.

$$G_{h-1} \rightarrow s_{h-2} : [prepare\_\text{key\_renewal}]_{K_{s_{h-2}}^{G_{h-1}}}$$

- 2단계: 센서 노드 $S_{h-2}$는 키 갱신을 위해 진행 중인 통신의 지속과 같은 조치를 취하며 *readyto*_key_renewal 메시지를 게이트웨이 $G_{h-1}$에 전송한다.

$$s_{h-2} \rightarrow G_{h-1} : [readyto\_\text{key\_renewal}]_{K_{s_{h-2}}^{G_{h-1}}}$$

- 3단계: 게이트웨이가 *readyto*_key_renewal 메시지를 모든 센서 노드로부터 수신하면 새로운 클러스터 키 $CN'_{G_{h-1}}$을 센서 노드로 전송한다.

$$G_{h-1} \rightarrow s_{h-2} : [CN'_{G_{h-1}}, new\_\text{cluster\_key}]_{K_{s_{h-2}}^{G_{h-1}}}$$

- 4단계: 일단 *new*_cluster_key 메시지를 센서 노드가 수신하면 각 센서 노드는 현재 클러스터 키를 갱신하며, 적용 가능한 경우에 통신을 재 시작한다.

프로토콜의 마스터 키 $K_m$은 초기 키 분배와 센서 노드 추가에만 이용되지만 중간 노드의 악의적인 공격을 막기 위해서 제안 프로토콜에서는 초기

키 분배 이후 정기적인 시간간격($t$) 이후에 아래와 같이 신규 마스터 키를 변경한다.

- 1단계: 명령 노드는 *new*_master_key 메시지를 신규 마스터 키 $K_m^{'}$를 이용해 전송한다.

$$A_h \rightarrow G_{h-1} : [K_m^{'} \| new\_master\_key]_{K_{G_{h-1}}^{A_h}}$$

- 2단계: 각 게이트웨이는 수신된 마스터 키를 그 하위 센서 노드로 전송한다.

$$G_{h-1} \rightarrow s_{h-2} : [K_m^{'} \| new\_master\_key]_{K_{s_{h-2}}^{G_{h-1}}}$$

### 3.4 클러스터내 악의적인 노드처리

센서 네트워크를 구성하고 있는 일부 게이트웨이 및 센서 노드들은 악의적인 노드들에 의해 위협해질 수 있다. 제안 기법에서는 클러스터스가 모두 수행된 이후에 IDS가 탑제된 명령노드가 [19, 24]와 동일한 방법으로 악의적인 노드를 식별할 수 있다고 가정한다. 제안 기법에서는 식별된 악의적인 노드를 안전하게 처리하기 위해 크게 2가지 방법을 사용하고 있다. 첫째, 센서 노드가 가지고 있는 키와 ID 정보를 게이트웨이 노드와 명령 노드가 공유한 공유키를 이용하여 명령 노드가 데이터를 검증하는 방법(데이터 무결성 보장)을 사용한다. 둘째, 일정시간 이후에 네트워크 구성이 재 클러스터링된 후 센서 노드와 중간 노드 사이에 공유된 공유키를 갱신하여 센서 노드들에게 전달함으로써 backward/forward secrecy를 예방할 수 있다. 클러스터내 악의적인 노드처리를 위한 방법을 노드 역할에 따라 기술하면 다음과 같다.

① 악의적인 게이트웨이 처리: 센서 네트워크 내의 게이트웨이가 악의적인 노드로 식별되면 명령 노드는 다른 모든 노드들에게 이 정보를 통보함으로써 노드들로 하여금 악의적인 노드와 통신하지 않도록 조정한다. 악의적인 게이트웨이를 격리하는 프로토콜은 다음과 같다.

- 1단계: 센서 네트워크 내의 게이트웨이 $G_{h-1}$가 악의적인 노드라는 통보를 받으면 명령 노드 $C$는 $G_{h-1}$가 악의적이라는 사실을 알리기 위해 $G_{h-1}$를 제외한 모든 게이트웨이에게 *compromised* _gateway라는 메시지를 전송한다.

$$C \rightarrow G_{h-1} : [K_m^{'} \| new\_master\_key]_{K_{G_{h-1}}^{C}}$$

- 2단계: $G_{h-1}$에 대한 *compromised* _gateway 메시지를 센서 네트워크내의 모든 센서 노드들이 수신하면 각 게이트웨이는 $G_{i-1}$를 이웃 게이트웨이 목록으로부터 배제함으로써 게이트웨이 $G_{i-1}$는 물론 $G_{h-1}$의 클러스터와의 통신을 방지하게 된다.
- 3단계: 명령 노드 $C$는 $G_{i-1}$를 게이트웨이 노드 목록으로부터 배제하며, 네트워크 마스터 키 $K_m$을 마스터 키 변경 프로토콜을 이용하여 변경한다.

② 악의적인 센서 노드 처리: 센서 네트워크내의 특정 센서 노드가 악의적인 것으로 식별되면 해당 게이트웨이는 현재의 클러스터 키를 변경함으로써 악의적인 센서 노드를 클러스터로부터 격리한다. 악의적인 센서 노드 $s_{h-2}$를 격리하기 위해서는 해당 게이트웨이가 보유하고 있는 센서 노드 목록으로부터 노드 $s_{h-2}$를 제거하고, 키 갱신 프로토콜을 이용하여 남은 세서 노드용 클러스터 보안 키를 수정한다.

③ 악의적인 센서 노드 복구: 격리된 센서 노드가 악의적인 상태로부터 회복되는 경우, 회복된 센서 노드는 신규 센서 노드 추가 프로토콜을 이용하여 센서 네트워크에 합류할 수 있다. 센서 노드가 동일한 공격으로 악의적으로 되는 것을 피하기 위해서는 네트워크 합류 전에 노드를 위한 명령 노드 공유 키와 게이트웨이 공유 키가 재생산되어야 한다.

## Ⅳ. 평 가

### 4.1. 보안 분석

무선 센서 네트워크에서 발생할 수 있는 공격유형은 크게 보안 메커니즘에 따른 공격유형과 라우팅 메커니즘과 같은 기본 메니지즘에 따른 공격유형으로 나뉘지만 이 절에서는 무선 센서 네트워크에서 발생할 수 있는 가장 대표적인 공격유형으로 제안기법의 안전성을 평가하도록 한다.

#### 4.1.1 전송되는 과정에서의 정보 공격에 따른 보안

센서 네트워크에서의 센서들은 센서 노드의 특정 파라미터나 값들의 변화를 모니터하고 요구사항에 따라 정보를 싱크 노드로 보고하는 역할을 수행한다. 그러나 센서 노드의 데이터 수집 및 전송 범위

가 제한적이기 때문에 높은 처리 파워나 넓은 통신 범위를 가진 악의적인 노드가 있을 경우 싱크 노드로 전달중인 정보를 수정하여 여러 센서 노드를 공격할 수 있다. 기존에 단-대-단 통신을 하는 메커니즘에서는 악의적이 노드를 추출하기 위해서 수집된 정보내에 MAC을 포함하도록 하여 데이터를 판독하지만 일정 기간 동안 악의적인 노드가 올바른 판독작업을 방해하기 때문에 문제가 발생할 수 있다. 제안 기법에서는 이 같은 문제를 해결하기 위해서 단-대-단 방식 대신 홉-대-홉 방식을 사용하여 노드를 인증하기 때문에 베이스 스테이션이 정보를 판독하는 동안 악의적인 노드가 판독작업을 방해하지 못하도록 한다. 이것은 모든 키를 부모 노드가 집중 관리하지 않고 중간 역할을 하는 노드에게 키 관리 역할을 분배하였기 때문에 가능하다. 그리고 베이스 스테이션이 정보를 수집한 후 통신 범위내에 침입 노드를 인식하면 수신되는 모든 메시지 전송을 중지함으로써 침입자 노드 공격을 예방할 수 있다.

#### 4.1.2 Blackhole/Sinkhole 공격에 따른 보안

Blackhole/Sinkhole 공격에서는 악의적인 노드가 센서 네트워크의 모든 트래픽을 끌어들이기 위해서 blackhole처럼 동작한다. 특히 악의적인 노드가 플로딩 기반 프로토콜을 사용하는 통신 노드사이에 존재할 경우 패킷 패싱과 같은 공격을 할 수 있지만 이러한 공격은 베이스 스테이션으로부터 멀리 떨어져 있는 센서 노드에게만 영향을 미친다. LEACH와 같은 클러스터링 작업을 수행하는 제안기법에서는 Blackhole/Sinkhole 공격이 발생할 수 없다. 그 이유는 $t$ 시간 간격으로 클러스터링이 수행되어 각 클러스터 헤드가 생성한 그룹키 $K$를 클러스터 내 노드들과 베이스 스테이션에게 전달하여 클러스터링 이전에 사용한 그룹키 $K$를 갱신하기 때문이다. 이 때, 계층적으로 구성된 네트워크의 중간노드가 pair-wise 키를 사용하여 센서 정보와 키 정보를 암호화한 후 홉-대-홉 방식으로 CRC(Cyclic Redundancy Check)을 전송함으로써 베이스 스테이션은 암호화된 데이터 값만을 수집하게 된다.

#### 4.1.3 Hello 플로우 공격에 따른 보안

Hello 플로딩 공격은 높은 주파수 전송 범위와 프로세스 파워를 가지는 악의있는 노드가 WSN 전 지역에 분산된 많은 센서 노드에게 HELLO 패킷을 보냄으로써 악의있는 노드를 이웃 노드로 인식하여 스푸프(spoof)하게 한다. Hello 플로우 공격을 예방하기 위해서 제안기법에서는 키 분배 과정 중 이동하는 패킷을 버퍼에 저장한다. 노드는 이전의 키로 패킷을 복호화하고, 새로 생성된 키로 암호화하여 패킷을 전송하게 된다. 제안된 프로토콜은 키 분배 중 이동하는 패킷의 보안을 위해 아래와 같은 보안 특성을 가지고 수행한다.

① 데이터 비밀 유지: 강력한 대칭 키 암호 기법 알고리즘(가령 RC5)의 이용은 클러스터 내 노드간 안전한 통신을 보장한다.
② 데이터 인증: 데이터와 함께 암호화된 서명은 인증을 보장하는 소스 ID를 지닌다. 제안 프로토콜은 브로드캐스트 통신 인증을 제공하지 않는다. 이 방법은 암호 기호 알고리즘 키의 주기적 변경에 의존하므로 적은 네트워크의 일부가 될 수 없다.
③ 데이터 무결성: 서명 내의 CRC는 메시지가 수정되지 않도록 보장한다. 서명은 암호화돼 있으므로 데이터 무결성을 보장한다.
④ 데이터 최신성: 세션과 서명 내의 계수기 모두 약한 데이터 신선도에 기여한다. 수신자는 세션과 착신되는 패킷의 서명 내의 계수기를 기대한다. 이 세션이 현재 세션보다 높은 경우, 약한 신선도가 확보된다. 반면에 이 세션이 현재 세션과 동일하면 계수기를 확인하게 된다. 서명 내의 더 큰 계수기값은 약한 데이터 신선도를 보장한다. 또한 본 연구의 방식은 적절한 수신자가 패킷을 수신하도록 보장한다. 이는 몇 가지 종류의 서비스 거부(DoS: denial of service) 공격을 방지한다.

#### 4.1.4 웜홀 공격에 따른 보안

웜홀(Wormhole) 공격은 공격자가 네트워크의 특정 위치에서 패킷(또는 비트)을 기록하고 다른 위치에 있는 노드와 직접 터널을 맺는 위험한 공격방법이다. 패킷의 터널링이나 재전송 방법은 선택적으로 수행되지만 웜홀 공격은 무선 센서 네트워크에서 매우 위협적이다. 그 이유는 공격자가 네트워크내 센서들과 타협을 요구하지 않거나 센서 노드가 이웃 노드의 정보를 복구하기 시작할 때 초기 구문에서 수행될 수 있기 때문이다. 제안 기법에서는 웜홀 공격을 예방하기 위해서 신규 노드가 합류하려고 할 때 신뢰성 있는 비밀 키 $K_m$를 가지고 있도록 한다. 이 신규 노드는 합류하고자 하는 클러스터 내에 있는 임의의 노드에게 요청 메세지를 전송한다. 전송 후에 클러스터 내의 노드는 임의의 수 $nonce$

를 신규 노드에게 전송한다. 신규 노드는 단방향 기능을 이용해 $P'$를 $P' = F(nonce, P)$로 계산한다. 클러스터 내의 노드와 신규 노드는 공통의 숫자 $P'$를 지니게 된다. 신규 노드는 클러스터내의 현재 키를 획득함으로써 센서 네트워크에 포함된다.

① 노드의 클러스터내 이동: 제안 프로토콜은 노드의 클러스터내 이동을 지원한다. 클러스터 내의 노드들은 공통 키 $K_m$를 지니고 있기 때문에 클러스터 내에서 자유롭게 이동이 가능하다. 따라서 클러스터내 센서 이동은 추가 보안 작업이 필요하지 않다.

② 노드의 클러스터간 이동: 제안 프로토콜은 노드의 클러스터간 이동을 지원한다. 노드는 클러스터 $G_i$를 떠나면서 클러스터 $G_i$의 키를 삭제하게 된다. 또한 노드가 클러스터 $G_j$에 합류하기 위해서는 클러스터 $G_j$의 키를 필요로 한다. 이런 경우는 클러스터에 합류하는 신규 노드와 동일한다. 신규 노드에 신뢰성 있는 비밀 키 $K_m$이 있는 경우 제안 프로토콜은 노드의 합류를 지원한다.

#### 4.1.5 Sybil 공격에 따른 보안

Sybil 공격은 무선 센서 네트워크에서 임무를 수행하는 여러 센서 노드들의 정보를 합병하기 위해서 합법적인 인식자를 사용하여 위장하는 공격 방법이다. Sybil 공격은 분산된 저장공간, 라우팅 메커니즘, 데이터 수집, voting, 공정한 자원 할당과 오용탐지등에서 발생될 수 있다. 제안 기법에서는 Sybil 공격을 예방하기 위해서 2개 이상의 클러스터에  포함되는 공통 노드를 지원하는 프로토콜을 사용한다. 공통 노드는 공통 노드들이 속하는 모든 클러스터의 키를 보유한다. 이웃 클러스터에서는 일정 시간 간격을 두고 키 변경이 발생할 수 있다. 패킷을 클러스터 $C_i$로부터 클러스터 $G_j$로 전송하기 전에 센서 노드는 우선 $C_i$의 키로 패킷을 암호화하고, 그 후에 $G_j$의 키로 복호하게 된다. 이 같은 과정을 홉-대-홉 방식으로 진행해 나감으로써 Sybil 공격을 예방하게 된다.

### 4.2. 성능 분석

성능 분석을 위해서 제안 프로토콜은 NS-2을 이용하여 시뮬레이션을 하였다. 그러나 NS-2가 센서 네트워크용으로 개발된 것이 아니므로 NS-2에서 센서 에이전트, 에너지 모델 및 [22]에 의해 개발된 다중 채널 모델을 플러그하면 센서 네트워크 환경이 조성된다. 실험 환경에서 사용된 파라미터는 [22]에서 정의한 파리미터값을 동일하게 사용하였다: Mica2 모드 전송 및 수신의 경우에는 각각 1 바이트당 16.25 $\mu J$ 및 1 바이트당 12.25 $\mu J$, 그리고 RC5를 이용해 8 바이트의 데이터를 암호화(또는 복호)하는 경우에는 1 바이트당 15 $\mu J$J였다. 비록 클록 속도(4 MHz 대 8 MHz)가 더 느리기 때문에 소비율이 더 낮으나 Mica2dot 모트에도 동일한 값을 고려했다. 여기에서는 36 바이트 짜리 패킷(TinyOS에서 이용되는 최고치)을 전제했다[23]. 이 논문에서는 WSN 보안을 수행하기 위해 저 에너지 비용 방식을 제시하는 데 있다. 그런데 계산 요소는 통신에 소비되는 에너지에 비하면 미미하므로 성능분석에서는 암·복호에 필요한 최소치를 적용하여 실험한다. 전체 네트워크의 성능을 측정하기 위해 [22, 23]에서 사용한 능력 비용과 에너지 비용을 동일하게 이용하였다. 키 관리 메커니즘의 통신 부하, 노드당 키 처리 시간 및 전달 시간 등을 측정하기 위해 보안 네트워크와 관련하여 최근 연구된 프로토콜, 즉 LHA-SP[21]와 제안 프로토콜을 이용해 실험하였다.

그림 5는 노드 수 증가에 따른 부하를 보여주는데, 그림 5의 결과를 통해 세 가지 사실이 관찰되었다. 첫째, 부하는 배치된 프로토콜과는 무관하게 노드 수에 따라 증가한다. 둘째, 부하는 노드의 증가에 비해 느리게 증가하는데, 이는 네트워크의 제한된 크기로 인해 노드가 그 수에 정비례로 증가하지 않기 때문이다. 셋째, LHA-SP기법의 경우 시뮬레이션에 이용되는 상이한 트래픽 패턴을 통한 트래픽 부하가 제안 포로토콜 기법보다 크게 나타나고 있다. 이와 같은 결과로 인해 제안 프로토콜이 LHA-SP 기법보다 키 관리로 인해 발생된 에너지 소비 부하가 3.5% 낮게 나타났다.

그림 6는 노드 수 증가에 따른 클러스터 키 전달

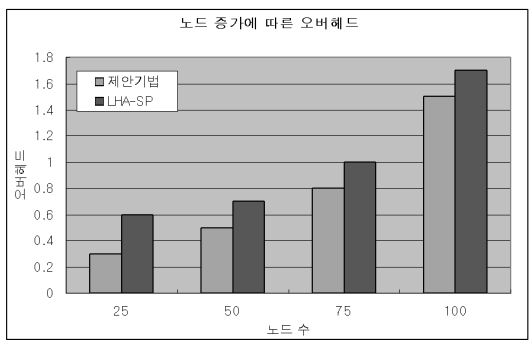


그림 5. 노드 증가에 따른 오버헤드

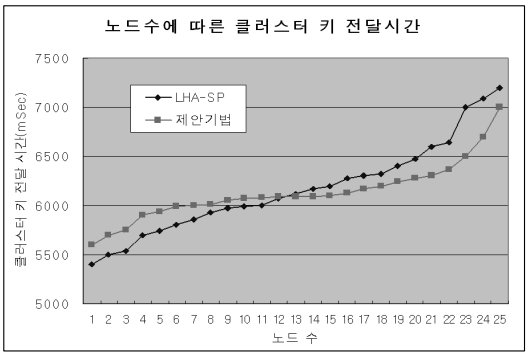



그림 6. 노드수에 따른 클러스터 키 전달시간

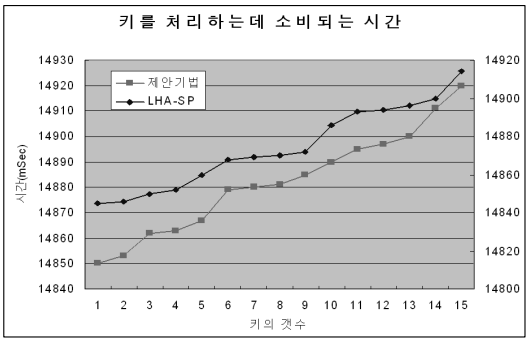



그림 7. 키를 처리하는데 소비되는 시간

시간을 나타내고 있다. 무선 센서 네트워크가 특정 h레벨의 계층으로 구성될 경우 LHA-SP 기법은 제안기법보다 클러스터 키를 전달하는 시간이 증가하고 있다. 이것은 LHA-SP가 계층적 네트워크로 노드를 구성할 경우, 특정 h 레벨이하에 존재하는 노드들에게 일정시간 경과 후 마스터 키 $K_m$로 데이터를 암호화하여 h 레벨 이하의 모든 노드들에게 암호화된 데이터를 전달한 후 복호화하는 과정이 발생하기 때문이다. 그러나 제안기법은 전달하려고 하는 데이터를 홉 간 공유하고 있는 공유 키를 이용하여 전달하기 때문에 노드 수가 증가할수록 LHA-SP보다 키 전달 시간이 평균 0.3% 빠르게 전달된다.

그림 7는 네트워크를 구성하고 있는 노드가 보유하고 있는 키의 갯수에 따라 처리하는데 소비되는 시간을 나타내고 있다. 제안 기법에서는 홉 대 홉 방식으로 노드를 인증하기 위해 MAC 대신 CRC 방식을 사용하기 때문에 LHA-SP보다 해당 키를 구하는 시간이 적게든다. 이것은 모든 키를 부모 노드가 집중 관리하지 않고 중간 역할을 하는 노드에게 키 관리 역할을 분배하였기 때문에 나타나는 현상이고 그림 7의 시뮬레이션 결과 제안 기법이 LHA-SP보다 평균 0.6%의 높은 효율성 나타내고 있다.

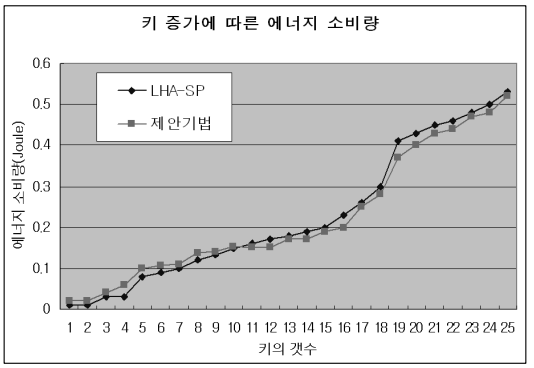



그림 8. 키 증가에 따른 에너지 소비량

그림 8은 네트워크를 구성하는 노드의 키 증가수에 따른 에너지 소비량을 나타내고 있다. 키의 갯수가 적을 경우 제안 기법은 LHA-SP 기법보다 에너지 소비량이 높게 나타났다. 이것은 키의 갯수가 적을 경우 홉 대 홉으로 통신하는 제안기법이 그룹키로 통신하는 LHA-SP보다 계층적으로 구성된 노드의 키 처리량이 많기 때문이다. 그러나 노드에 사용되는 키의 갯수가 많아질 수록 LHA-SP는 클러스터내에 존재하는 모든 노드들에게 마스터 키로 암호화된 정보를 전달하기 때문에 키 증가에 따른 에너지 소비량이 제안기법보다 높게 나타나고 있다.

## V. 결 론

이 논문에서는 노드 간 안전한 정보를 수집, 전달하기 위해 중간노드의 안전성을 확보하는 동시에 악의적인 센서를 네트워크로부터 제거하기 위한 계층적 키 관리 프로토콜을 제안하였다. 제안 프로토콜은 경량급 그룹 키 기반 메커니즘을 이용해 클러스터 헤드와 그 자식 노드간에 키 쌍을 설정하여 센서 노드 간 직접적인 단 대 단 통신 대신에 홉 대 홉 경로 배정 기능을 유지하도록 하여 효율성을 극대화하였다. 특히 제안 기법에서는 센서 노드의 전력 부하를 줄이면서 중간노드가 안전하게 데이터를 수집하고 센서 네트워크 내의 악의적인 행위를 최소화 하도록 중간노드가 키 관리 역할을 할 수 있도록 하였다. 중간 역할을 하는 노드는 악의적인 노드 공격과 침입 공격을 감지하여 키 분배 중 이동하는 패킷 보안을 할 수 있어 기존 LHA-SP의 보안 문제점을 해결하였다. 시뮬레이션에서는 제안 기법이 모든 키를 부모 노드가 집중 관리하지 않고 중간 역할을 하는 노드에게 키 관리 역할을 분배하였기 때문에 제안 기법이 LHA-SP 기법보다 키 관

리로 인해 발생된 에너지 소비 부하가 3.5% 낮았으며, 키 전달 시간 및 처리 시간은 LHA-SP 기법보다 각각 0.3%와 0.6% 개선된 결과를 얻을 수 있었다. 향후 연구에서는 제안 기법을 다양한 WSN환경에 적용하여 중간 노드의 역할에 따른 키 사용 에너지양과 키 전달시간을 비교 평가 할 예정이다.

## 참 고 문 헌


〔1〕 W. Du, J. Deng, Y. S. Han, S. Chen, and P. K. Varshney, A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge, IEEE, 2004.

〔2〕 I. F. Akyldiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, Wireless sensor networks:a survey, Computer Networks, 38:393-422, December. 2002.

〔3〕 F. Stajano, Security for Ubiquitous Computing, John Wiley and Sons Ltd, 2002.

〔4〕 M. Eltoweissy, H. Heydari, L. Morales, and H. Sudborough, Combinatorial Optimization for Key Management in Secure Multicast Environments, Journal of Network and Ssytem Management, Kluwer Publishing, 2004.

〔5〕 A-S. K. Pathan, H. W. Lee, C. S. Hong, Security in Wireless Sensor Networks: Issues and Challenges, ICACT 2006, vol.2, pp.1043-1048, Feb, 2006.

〔6〕 A. Perrig, R. Szewczyk, V. Wen, D. Culler, J. D. Tygar, SPINS : Security Protocols for Sensor Networks, Proceedings of Seventh Annual International Conference on Mobile Computing and Networks MOBICOM 2001, July 2001.

〔7〕 L. Zhou, and Z. J. Haas, Securing ad hoc networks, IEEE Network, Vol.13, Issue 6, pp. 24-30, Nov.-Dec. 1999.

〔8〕 B. Strulo, J. Farr, and A. Smith, Securing Mobile Ad hoc Networks -A Motivational Approach, BT Technology Journal, Vol.21, Issue 3, pp. 81-89, 2003.

〔9〕 H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, Security in Mobile Ad Hoc Networks: Challenges and Solutions, IEEE Wireless Communications, Vol.11, Issue 1, pp.38-47, Feb. 2004.

〔10〕 K. Wu, C. Liu, V. King, Very low cost sensor localization for hostile environments, ICC 2005, Vol.5, pp.3197-3201, 16-20 May, 2005.

〔11〕 T. Dimitriou, I. Krontiris, and F. Nikakis, “Key establishment in sensor networks with resiliency against node capture and replication,” December 2003. Submitted to 5th ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc) 2004.

〔12〕 W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan, Energy efficient communication protocol for wireless microsensor networks, IEEE Proceedings of the Hawaii International conference on System Sciences, pp.1-10, January 2000.

〔13〕 H. Chan, A. Perrig, and D. Song, “Random key predistribution schemes for Sensor networks,” In IEEE Symposium on Research in Security and Privacy, pp.197-213, May, 2003.

〔14〕 L. Echenauer and V. D. Gligor, “A Key-Management scheme for Distributed sensor networks,” In Proceedings of the 9th Computer Communication Security, pp.41-47, Nov. 2002.

〔15〕 H. Chan, A. Perrig, and D. Song, ″Random key predistribution schemes for Sensor networks,″ In IEEE Symposium on Research in Security and Privacy, pp.197-213, May, 2003.

〔16〕 S. Zhu, S. Setia, and S. Jajodia, “A distributed group key managemet protocol for ad hoc networks,” Unpublished manuscript, George Mason University, Dec. 2002.

〔17〕 Gupta G, Younis M, “Performance Evaluation of Load-Balanced Clustering in Wireless Sensor Networks,” In the proc. of 10th International Conference on Telecommunications (ICT 2003), Tahiti, French Polynesia, pp. 1577-1583, Feb. 2003.

〔18〕 M. Tatebayashi, N. Matsuzaki, and D. B. Newman, “Key distribution protocol for digital mobile communication systems,” Advances in Cryptology -CRYPTO’89, pp.324-334, 1989, INCS Vol. 435, Springer-verlag.

〔19〕 A. Aimbola, S. Qi and M. Merabti, “Nethost-sensor: a novel concept in intrusion detection systems,” Proceedings. Eighth IEEE International Symposium on Computers and Communication,

2003(ISCC 2003), pp.232-237, 2003
〔20〕 Xiao Chen, Jawad Drissi, "An Efficient Key Management Scheme in Hierarchical Sensor Network," Mobile Adhoc and Sensor Systems Conference 2005 IEEE International Confercence, pp. 6, Nov. 2005.
〔21〕 L. B. Oliveira, H. C. Wang, A. A. Loureiro, "LHA-SP:secure protocols for hierarchical wireless sensor networks," In 9th IFIP/IEEE International Symposium on Integrated Network Management, pp. 31-44, 15-19. May. 2005.
〔22〕 F. Yea, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies in INFOCOM 2004, pp.2446-2457, March. 2004.
〔23〕 J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, "System architecture directions for networked sensors," In ACM 9th ASPLOS'03, pp. 93-104, 2000.
〔24〕 A. Siraj, R. B. Vaughn, S. M. Bridges, "Intrusion sensor data fusion in an intelligent intrusion detection system architecture," Proceedings of the 37th Annual Hawaii International Conference on System Sciences, Jan, 2004.

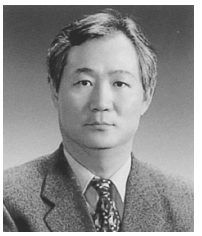
**정 윤 수** (Yoon-Su Jeong) 정회원

1998년 2월 청주대학교 이학사
2000년 2월 충북대학교 대학원 전자계산학과 이학석사
2003년 3월~현재 충북대 전자계산학과 박사수료
<관심분야> 무선 센서 네트워크 보안, 암호이론, 정보보호, Network Security, 이동통신보안, 전자상거래보안

**황 윤 철** (Yoon-Cheol Hwang) 정회원

1994년 한남대학교 전자계산공학과
1996년 한남대학교 전자계산공학과 공학석사
1999년~현재 충북대 전자계산학과 박사수료
<관심분야> 인터넷, 정보보호, Network Security

**이 상 호** (Sang-Ho Lee) 정회원



1976년 숭실대학교 전자계산학과
1981년 숭실대학교 전자계산학과 (MS)
1989년 숭실대학교 전자계산학과 (PHD)
1976년 1월~1979년 5월 한국전력 전자계산소
1981년 6월~현재 충북대학교 전기전자컴퓨터공학부 교수
<관심분야> Protocol Engineering, Network Security, Network Management, Network Architecture