클러스터 기반에서의 인증을 통한 안전한 키 관리 기법

Secure Key Predistribution Scheme using Authentication in Cluster-based Routing Method

김진수*, 최성용*, 정경용**, 류중경***, 임기욱****, 이정현*****
인하대학교 정보공학과*, 상지대학교 정보정보공학부**, 대림대학 컴퓨터정보과***,
선문대학교 컴퓨터정보학부****, 인하대학교 컴퓨터공학부*****

Jin-Su Kim(kjspace@inha.ac.kr)*, Seong-Yong Choi(sychoi@inha.ac.kr)*,
Kyung-Yong Chung(kyjung@sangji.ac.kr)**, Joong-Kyung Ryu(jkryu@daelim.ac.kr)***,
Kee-Wook Rim(rim@sunmoon.ac.kr)****, Jung-Hyun Lee(jhlee@inha.ac.kr)*****

요약

클러스터 기반의 라우팅 기법에서의 안전한 데이터 통신을 위해서는 기존의 키 관리 방식은 적합하지 않다. 왜냐하면 클러스터 기반에서는 매 라운드 마다 클러스터 헤드가 변경되기 때문에, 안전한 통신을 위해 각 멤버 노드들과 인증이나 공유키 설정 단계를 거쳐야 한다. 또한 기존의 키 관리 메커니즘에서는 대부분 센서 네트워크 안의 모든 노드에 대해 이동성을 부여하지 않았기 때문에, 노드의 이동성을 고려하게 되면 안전한 통신을 위한 커다란 오버헤드가 발생한다. 따라서 본 논문에서는 이동성과 새로운 노드의 삽입이 빈번한 경우에도 안전하고 효율적인 클러스터 기반에 적합한 키 관리 메커니즘을 제안한다.

■ 중심어 : | 보안 프로토콜 | 무선 센서 네트워크 | 클러스터 기반 라우팅 |

Abstract

The previous key management methods are not appropriate for secure data communication in cluster-based routing scheme. Because cluster heads are elected in every round and communicate with the member nodes for authentication and share-key establishment phase in the cluster. In addition, there are not considered to mobility of nodes in previous key management mechanisms.

In this paper, we propose the secure and effective key management mechanisim in the cluster-based routing scheme that if there are no share keys between cluster head and its nodes, we create the cluster key using authentication with base station or trust autentication and exchange the their information for a round.

■ keyword : | Secure Protocol | Wireless Sensor Networks | Cluster-based Routing Scheme |

I. 서 론

무선 센서 네트워크(Wireless Sensor Network; WSN)는 유비쿼터스 컴퓨팅 구현을 위한 기반 네트워크로, 초경량, 저 전력, 제한적인 메모리와 프로세서 등과 같은 자원의 제약성을 갖는 많은 센서들로 구성된

* 본 연구는 지식경제부 및 정보통신산업진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (NIPA-2009-C1090-0902-0020)
접수번호 : #090710-003
접수일자 : 2009년 07월 10일
심사완료일 : 2009년 07월 24일
교신저자 : 김진수, e-mail : kjspace@inha.ac.kr

무선 네트워크이다. 특히 무선 매체를 통한 상호간의 통신으로 인해 유선 네트워크에 비해 보안이 매우 취약하다. 센서 노드는 매우 제한된 통신 및 계산 능력과 작은 메모리 공간을 가지므로 RSA (Rivest-Shamir-Adelman)나 Diffie-Hellman 기법 등과 같은 기존의 공개키 암호 기술을 적용하는 것이 어렵다. 또한 물리적으로 안전하지 않은 환경에 배치되고, 매우 많은 수의 센서 노드가 오류 및 장애를 허용해야 하며, 자율적인 네트워크 구성을 통해서 연결되므로 효과적인 관리 및 보안 기능 강화가 중요한 요소라고 할 수 있다. 최근에 WSN에서 안전한 키 분배를 통한 다양한 암호화 방법들이 집중적으로 연구되고 있다[1-6]. 그러나 이러한 안전한 통신을 위해 제안된 방법들은 키 분배 해결안이 특정한 구조에만 적합한 국한된 특성을 가진다[7]. 일반적인 ad hoc 네트워크나 WSN에서 효율적인 에너지 관리를 위해 클러스터 기반의 라우팅 프로토콜 구조가 제안되었다[8-10]. 클러스터 기반의 네트워크에서는 일반적으로 멤버 노드들은 클러스터를 형성하고, 클러스터 헤드(CH)에게 정보를 전송하고, CH는 이러한 정보를 압축하여 기지국(Base Station;BS)에 전송한다. LEACH[8], LEACH-C[9], 3DE_var[10]과 같은 프로토콜은 클러스터 기반으로 이루어진 WSN에서 확장성과 에너지 효율을 향상시키는 대표적인 방법이다. 매 라운드마다 CH를 선출하여 일정한 시간동안 라우팅의 역할을 하기 때문에, 악의적인 목적을 갖는 공격자는 라우팅 요소를 인증하기 어렵게 만들거나 손상시키려는 주요한 공격의 목표가 된다. 따라서 클러스터 기반의 프로토콜에 안전한 통신을 강화하기 위해 동적으로 또는 일정 시간 후에 분배된 키를 재배치하여 노드들 간의 링크를 변경하게 되면 수반되는 오버헤드가 상당히 크기 때문에 꼭 필요한 경우가 아니면 부적절하다.

기존의 안전한 키를 이용한 대부분의 키 관리 방식에서는 네트워크 내의 노드들에 이동성을 부여하지 않고 배치된 고정된 위치에서 수명을 다하는 특수한 구조였지만, 네트워크 장애, 특정 지역에서의 센서 노드 밀도가 너무 높거나 낮은 경우에 원활한 정보 수집을 위해 전체 네트워크를 효율적인 구조로 재형성하기 위해서는 센서 노드의 이동성이나 새로운 노드의 삽입이 부여되어야 한다.

본 논문에서는 클러스터 기반의 라우팅 기법의 장점인 클러스터 형성을 위한 효율적인 에너지 사용뿐만 아니라, 클러스터 내에서의 안전하고 효율적인 통신이 가능하도록 하며, 새로운 노드의 추가나 기존 노드의 이동성이 부여되었을 때 기존의 클러스터에 안전하게 참여하여 전체적인 네트워크 효율을 높이고자 한다.

II. 기존의 키 관리 기법

WSN에서 제안된 키 관리 기법들은 노드 배치 이전에 키 분배의 유무, 마스터 키의 사용 여부에 따라 사전 키 분배 방식[1][3][4][11], 마스터 키 기반 방식[5], 베이스 스테이션 기반 방식[12]으로 구분할 수 있다.

1. 사전키 분배 방식(Random Key Predistribution)

사전키 분배 방식(RPK)[1]은 Random Key Predistribution, Shared Key Discovery, Path Key Establishment의 3단계의 과정을 거쳐 노드들 간의 안전한 인증을 보장한다. 사전키 분배 방식은 연결 정도가 확률적으로 구성되기 때문에 WSN를 나타내는 전체 그래프가 완전하게 연결되지 않을 수 있으며, 센서 노드의 배치가 불규칙적이거나 배치된 환경에 물리적으로 통신을 방해하는 요소가 있는 경우 더욱 심해진다. 특히 네트워크 연결 강도를 증가시키기 위해서는 센서 노드마다 저장해야할 키 링의 크기가 증가되어야 하는 문제가 발생하며[13], 이는 악의적인 공격자는 노드 탈취를 통해 더 많은 키를 획득할 수 있다. 이를 개선하기 위해 센서 노드의 배치 정보를 활용하는 방법이 제안되었으나 악의적인 공격자는 노드 탈취를 통해 획득한 키를 센서 네트워크 내의 다른 영역에서 활용할 수 있다는 점에서 여전히 문제가 발생하며, 탈취된 노드들이 서로 협력을 통해 보다 효율적인 감청 및 탈취 여부를 숨길 수 있는 안전성 분석이 전혀 고려되지 않았다[14]. 그러나 사전키 분배 방식은 새로운 노드의 추가나 기존 노드의 클러스터 변경과 같은 이동성이 부여되었을 때, 각 노드가 가진 공유키를 이용하여 안전한 통신을 위한

클러스터를 형성할 수 있다는 장점이 있다.

2. LEAP(Localized Encryption and Authentication Protocol)

하나의 키를 사용하는 메커니즘으로는 대량의 센서가 흩어져 있는 센서 네트워크에서는 안전한 키 메커니즘의 설계가 어렵다는 판단으로, 4개의 암호키와 키 설정 프로토콜을 가진 LEAP 프로토콜[5]가 제시되었다. 4개의 암호키는 BS와 공유하는 개인키, BS가 네트워크에 있는 모든 노드와 공유하는 브로드캐스팅 키인 그룹키, 다른 센서 노드와 공유하는 Pairwise 키, 그리고 몇 개의 이웃 노드와 공유하는 클러스터 키이다. LEAP은 공격 노드는 개인키를 알 수 없으며, pair-wise 키와 클러스터 키는 주위의 이웃 노드를 인증하기 위해서만 사용되고 그룹키는 방송되는 메시지를 복호화하기 위해서만 사용되므로, 위협 노드를 가진 센서 네트워크의 생존성을 극대화 할 수 있는 방법이다. 개인키와 그룹키는 센서 노드가 배치되기 전에 탑재되기 때문에 악의적인 공격자에게 센서 노드가 탈취될 수 있다. 또한, 일반적인 마스터 키 기반의 방식과 동일하게 초기화 과정이 끝나기 전에 센서 노드가 탈취될 경우 악의적인 공격자는 1분 이내에 센서 노드에 저장된 모든 정보를 획득하여 WSN에서 사용되는 모든 키들을 생성할 수 있는 문제점을 가지고 있다[15]. 또한 네트워크 내의 모든 노드들은 고정된 위치에 존재한다는 이동성을 고려하지 않았다.

3. HIKES (Hierachial Key Establishment Scheme)

HIKES[12]는 BS가 신뢰된 인증기관(TA)의 역할을 담당하면서 그 기능 중 일부를 CH에게 위임하는 방법으로, 모든 노드에 partial key escrow 테이블을 가지고 키를 생성하며 CH로 선출될 수 있고, 데이터 통합 후 CH들 간의 메시지 교환을 통해 BS에 정보를 전송한다. 그러나 센서 노드의 인증이 BS을 통해 이루어지고, 모든 노드에 partial key escrow 테이블을 저장하고 있어야 하기 때문에 추가적인 저장 공간이 필요하다. 또한 악의적인 공격자가 노드 탈취를 통해 partial key escrow 테이블을 획득한 경우 이를 이용하여 다른 지역에 위치한 CH와 센서 노드간의 pairwise 키를 유추할 수 있고, 클러스터에 속한 노드들의 수가 증가함에 따라 CH는 노드 인증을 위해 전송해야 하는 메시지의 크기가 증대되기 때문에 전체 네트워크 생존 시간을 줄어들 수 있다.

III. 안전한 클러스터 기반 라우팅 기법에서 제안하는 키 관리 기법(3DE_sec)

악의적인 공격자가 노드를 탈취하여 다른 클러스터에서 사용할 수 있다는 것은 자체적인 노드들 간의 통신에서는 많은 문제의 원인으로 될 수 있으나, 신뢰할 수 있고 안전한 BS의 인증을 획득한 노드가 이동 혹은 새로운 노드의 추가로 인해 새로운 클러스터에서 포함된다면, 새로운 이웃 노드들과 공유키를 생성하기 위해서는 많은 정보 교환과 같은 불필요한 송수신을 최소화해야 한다.

클러스터 기반의 라우팅 프로토콜에 기존의 키 관리 스킴을 적용하여 안정적인 정보 교환을 통한 CH를 선출하고 수집된 정보를 전송할 수 있으나 새로운 노드의 추가 또는 기존 노드에 이동성이 부여되었을 때 기존의 키 관리 기법에는 한계가 있다.

따라서 본 논문에서는 이동성이 부여된 노드나 새로운 노드의 삽입 또는 삭제에도 CH의 부하를 최소화할 수 있는 키 관리 기법을 제안한다. 이러한 키관리 기법을 3DE_sec라 하고, 3DE_sec는 다음과 같이 세 단계로 되어 있다.

1. 사전키 분배 단계

사전키 분배 단계는 k개의 랜덤 키를 분배하는 과정과 BS와 유일하게 통신 가능하도록 공유하는 개인키 설정 과정의 두 과정으로 이루어진다. 사전키 분배 과정에서는 모든 노드들이 WSN에 배치되기 전에 P개의 키를 가진 커다란 풀과 그들의 키 식별자를 생성하고, 각 센서 노드의 메모리에 P개의 키 중 k($k \ll P$)개의

키를 무작위로 가져온다. 이 때, 전체 P개의 키를 유일하게 생성하기 위한 각 키의 크기가 N 비트일 때, 2^N개의 서로 다른 키를 생성할 수 있기 때문에($P \leq 2^N$), 풀에 생성될 키의 크기는 $log_2 P$ 비트 이상이면 키의 유일성은 보장된다.

클러스터 기반의 라우팅 기법에서 모든 노드들은 BS에게 클러스터 내의 다른 노드들로부터 받은 정보를 전송하거나 BS로부터 질의를 수신하기 위해 BS와의 공통의 키를 생성하여야 한다. 이 키를 개인 키라 한다. 개인키는 노드가 배포되기 전에 생성하여 미리 적재한다. 즉, BS에 의해 각 노드(u)가 갖는 유일한 키(K_u^m)는 $K_u^m = f_{K^m}(u)$을 이용하여 생성된다. 이때 f는 의사 난수 함수이고, K^m은 단지 컨트롤러가 알고 있는 마스터키이다. 이 개인키 생성은 의사 난수 함수의 효율적인 계산 능력으로 BS 측면에서의 계산 가능한 오버헤드는 무시해도 된다.

2. 공유키 탐색 단계

공유키 탐색 과정에서는 CH로부터 무선 통신 범위 내의 멤버 노드들과의 공유키를 탐색하는 단계로, CH는 자신의 키 ID를 브로드캐스트하여 멤버 노드들과 공유하는 키를 가지고 있는지를 알 수 있다. 이러한 공유된 키를 통해 노드들과의 안전한 링크를 설정하며 안전한 통신을 보장할 수 있다. 각 노드에 부여된 키 링은 이웃 노드들과 하나 이상 공유할 수 있는 확률은 식 (1)과 같이 P와 k의 수에 의해 다음과 같이 계산할 수 있다.

$$p' = 1 - \frac{((P-k)!)^2}{(P-2k)!P!}, 0 \leq p' \leq 1 \qquad (1)$$

이 때, 전체 풀, P의 수는 매우 큰 수이기 때문에 팩토리얼 연산이 불가능하므로, $n!$ 연산을 간략화하기 위해 식 (2)의 스털링 공식(스털링 근사)을 적용하면, 이웃 노드들과 하나 이상 공유할 수 있는 확률은 다음 식 (3)과 같이 간략화된다.

$$n! \approx n^n e^{-n} \sqrt{2\pi n} \qquad (2)$$

$$p' = 1 - \frac{(1-\frac{k}{P})^{2(P-k+\frac{1}{2})}}{(1-\frac{2k}{P})^{(P-2k+\frac{1}{2})}} \qquad (3)$$

식 (3)을 이용하여, 전체 P개의 키들 중에서 미리 정의된 확률 값에 만족하는 적절한 k 값을 계산할 수 있다.

3. 인증을 통한 공유키 생성 단계

2단계의 공유키 설정 단계에서 CH와 공유키를 설정하지 못한 경우, 사전키 분배 방식의 경로키와 같은 공유키를 설정하여야 한다. 클러스터 기반에서는 CH가 일정한 주기마다 변경되고, 키 링의 크기 k가 클러스터 내의 전체 노드 수보다 작기 때문에, 공유키를 갖지 않은 노드들과 경로키 설정이 빈번해질 가능성이 크며, 그 때마다 마스터키를 이용하여 재설정이 불가능하다.

본 논문에서는 각 노드들간의 고유의 공유키를 통한 인증, BS 혹은 BS로부터 위임된 인증기관으로부터의 인증을 통해 보다 안정적인 통신을 설정하려 한다. 따라서 각 노드들은 적어도 한번 이상 인증 절차를 거치기 때문에 기존의 방법론에 비해 더욱 안전하고 신뢰성 있는 통신을 수립할 수 있다.

1) 공유키를 통해 인증(1차 인증)

사전키 분배 단계를 거친 후, 각 노드에는 k개의 키 링과 BS와 안전한 통신을 위한 유일한 개인키를 가진다. 이때 각 노드에 부여된 k개의 키들을 이용하여 노드들 간의 공유키 설정을 통한 인증이고, 이를 1차 인증이라 하며 안전한 통신로가 수립된다.

2) BS로부터 신뢰된 인증 노드를 통한 인증(2차 인증)

공유키를 통해 인증할 수 없는 경우, 이전 클러스터 형성 단계에서 BS로부터 신뢰된 인증 노드들로부터 인증을 받는다. 즉, 새로 선출된 CH와 클러스터 내의 노드사이에 공유키가 존재하지 않는 경우, BS를 통해 인증을 획득하면 BS의 오버헤드가 가중되며 전체 네트워크 트래픽을 증대할 수 있다. 따라서 기존의 CH로부터

획득한 클러스터 내의 노드들의 정보를 재활용하여 인증을 빠르게 수행할 수 있어 전체 지연시간을 최소화할 수 있다. 3DE_var와 같은 경우에서는 기존의 CH가 다양한 정보를 취합하여 최적의 CH를 선출할 수 있기 때문에 신뢰할 수 있는 노드로부터 인증 받을 수 있다. 또한 상위 클러스터 헤드를 통해 이전에 속했던 노드인지를 클러스터 키를 통해 인증하며, 이를 2차 인증이라 한다. 이때 BS로부터 신뢰된 인증 노드로부터 이전에 사용된 클러스터 키를 공유키로 사용한다.

3) BS를 통한 인증(3차 인증)

1차, 2차 인증 단계를 통해 인증을 받지 못한 노드인 경우, [그림 1]과 같이 BS에 의해 직접 인증을 설정해야 한다. 즉 공유키나 직전의 클러스터 키와 같은 인증 가능한 정보가 없는, 새로운 노드의 삽입이나 다른 클러스터로부터 이동된 노드들의 경우 1차, 2차 인증 단계로부터 인증 받기가 거의 희박하다. 따라서 이러한 노드들은 각 노드에게 부여된 키 링의 키들을 랜덤한 위치의 값들을 선택하여 BS에게 인증 요청 패킷(Authentication Request Packet, AREQ)을 전송하여 BS의 인증 절차를 거친다. 즉 BS에게 인증받기 위해 자신의 키 링의 일부 값들을 무작위로 추출하고 개인키를 이용하여 암호화한 메시지를 선출된 CH에 전송한다. CH는 공유키를 갖지 않은 노드들로부터 획득한 암호화된 메시지를 BS에 전송하며, BS는 암호화된 메시지를 복호화하여 송신한 노드 ID의 인증 샘플 코드인 $< idx, BA, length, val >$ 쌍들의 집합과 일치하는지를 확인한다. 이 때 적용된 idx는 노드의 키 링에 존재하는 순서를 의미하고, BA는 기준 주소(Base Address), $length$는 길이, val은 값(value)을 의미하며, 이러한 값들은 랜덤 함수를 이용하여 선택하고, val은 BA로부터 $length$ 만큼 떨어진 위치까지의 키 값들을 나타낸다. 일치하는 경우에 인증 응답 패킷(Authentication Reply Packet, AREP)을 전송하며, 일치하지 않고 통신 방해를 위한 악의적인 노드들의 ID를 검출하여 각 CH에 전송하여 모든 노드들의 키 링으로부터 제거하도록 한다. 이때 클러스터 기반의 특성인 일정한 시간 간격마다 CH가 바뀌어야 하기 때문에 AREP에는 인증 후 BS에 의해 부여된 공유키를 포함한다. [그림 1]에서 Join_REQ 메시지를 전송하는 노드들은 1차 인증을 거친 노드들을 의미한다.

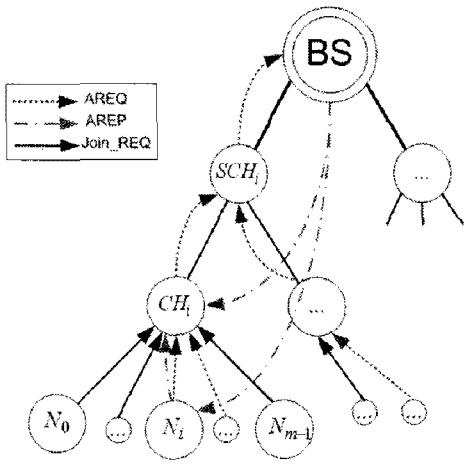


그림 1. 공유키가 없는 노드의 BS를 통한 인증 요청 및 응답 처리 과정

CH와 공유되지 않은 노드들이나 새로 삽입되는 등의 면역성이 떨어지는 노드들은 BS로부터 인증을 받아야 한다. 따라서 BS에는 키 배포 전에 커다란 풀 P와 각 노드에 배포된 k개의 키 링들 안에 포함된 정보인 $< NodeID, idx >$의 쌍들을 풀 데이터베이스 안에 사전키 배포와 동시에 [그림 2]와 같이 구축된다. 이때 $NodeID$는 각 노드의 ID를, idx는 각 노드 ID가 가진 키 링 내의 순서를 나타낸다.

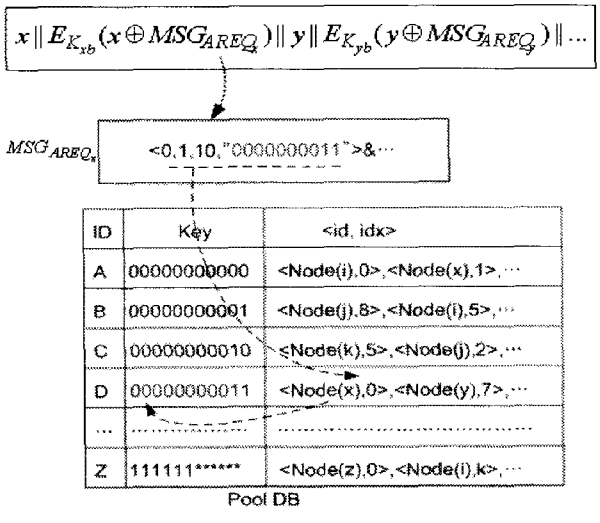


그림 2. BS의 암호화 메시지 인증 검증 과정의 예

[그림 2]는 BS가 가진 풀 데이터베이스와 공유키를 가지고 있지 않은 노드가 전송한 인증 샘플 코드가 일치하는 지를 나타내는 과정을 보인다. 노드 ID가 x가 자신의 개인키로 인증 샘플 코드를 암호화(MSG_{AREQ})한 메시지를 BS가 복호화한 내용의 일부가 $< 0,1,10,$ "0000000011 "$>$이다. 이는 x노드의 0번 위치의 키로부터 1만큼 떨어진 곳부터 10비트의 값이 "0000000011"이라는 것을 의미한다. 이 값이 BS내의 데이터베이스에 존재하는 값과 일치하면 노드 ID가 x를 인증하며, AREP를 전송하여, 클러스터 헤드와 x가 공유키를 설정할 수 있도록 3차 인증을 한다. AREP로 전송되는 메시지도 MSG_{AREQ}와 동일하게 값을 전송하여 노드와 CH가 재확인 후 공유키를 사용한다. 인증을 통해 생성된 공유키는 클러스터 키로 사용하여 현재 라운드동안 수집된 데이터를 안전하게 수신할 수 있도록 한다.

IV. 시뮬레이션 성능 및 평가

본 논문에 사용된 시뮬레이터는 Visual C++로 구축하였다. 기존의 연구에는 네트워크 내의 안전한 통신을 위한 노드 수에만 언급하고, 네트워크의 크기($M \times M$)에 대한 언급이 없이 단순한 전체 노드수를 확장하여 실험하였다. 그러나 네트워크의 밀도는 전체 클러스터 형성 시간의 지연시간과 밀접한 관계를 가지고 있으며, 전체 네트워크의 크기 또한 무선 센서에게는 큰 오버헤드로 작용한다. 따라서 실험에서는 네트워크의 크기($100m \times 100m$)를 제한하고, BS로부터 네트워크 영역까지의 거리에 따른 최적의 클러스터 수(k_{opt})[9]를 이용하여 클러스터를 형성하였다.

$$k_{opt} = \frac{\sqrt{P}}{\sqrt{2\pi}} \sqrt{\frac{\epsilon_{fs}}{\epsilon_{mp}}} \frac{M}{d_{toBS}^2} \quad (4)$$

P은 WSN을 구성하는 노드들의 수이고, d_{toBS}는 BS까지의 거리이고, ϵ_{fs}는 $10pJ/bit/m^2$이고, ϵ_{mp}는 $0.0013pJ/bit/m^4$이다. 본 논문에서는 WSN의 크기 M을 $100m$, 전체 노드 수 P는 $10,000$으로 설정하였다. 이 값을 식 (4)에 대입했을 때, 최적의 클러스터 수 k_{opt}는 62이다. 따라서 3DE_sec에서의 키 링의 크기(k)를 162($\simeq$10000/62)으로 설정하였다.

3DE_sec에서의 매 라운드마다 미인증 노드의 인증을 위해 BS까지의 전송 에너지량은 $n \times E_{TX} \times Length'$이고, HIKES에서의 BS까지의 전송 에너지량은 $N \times E_{TX} \times Length''$이라고 했을 때, 본 논문이 HIKES에 비해 효율적인 에너지 성능을 위해서는 총 에너지 사용량이 적어야 하며 다음 식 (5)와 같다.

$$n \times E_{TX} \times Length' < N \times E_{TX} \times Length''$$
$$Length' < \frac{N \times Length''}{n} \quad (5)$$

여기서, $Length''$는 각 키의 크기를 나타내며, $Length'$는 BS와의 인증을 위한 인증 샘플 코드의 크기, $\{< idx, BA, length, val >\}^*$를 나타낸다.

[표 1]은 P가 10,000일 때, 키 링의 크기에 따른 공유되지 않는 키들의 수와 에너지 효율을 최적화할 수 있는 인증 샘플 코드의 크기를 나타낸다. 여기서, 키 링의 최소값이 94개 이상일 경우에, HIKES에 비해 에너지 효율을 가지며 안전한 키 관리를 할 수 있음을 보인다. 또한 인증 샘플 코드의 크기가 적어도 39 bit를 가져야 유일성을 입증할 수 있다.

표 1. 에너지 효율을 위한 키 링의 크기에 따른 인증 샘플 코드의 크기(P=10,000)

k	p'	비공유키수	인증 샘플 코드 크기의 최대값	Length'
50	0.2222	7,778	< 20.5708 bit	38 bit
94	0.5901	4,099	< 39.0339 bit	39 bit
95	0.5979	4,021	< 39.7911 bit	39 bit
100	0.6358	3,642	< 43.9319 bit	39 bit
162	0.9306	694	< 230.548 bit	40 bit
200	0.9831	169	< 946.746 bit	40 bit
220	0.9929	71	< 2253.52 bit	40 bit
250	0.9984	16	< 10000 bit	40 bit

표 2. 기존 키 관리 기법과의 저장 용량의 비교

Cryptographic Primitive	LEAP	RKP	HIKES	3DE_sec
Initialization key	0	N/A	1	1
Cluster-wide key	1	N/A	1	1
Node-to-cluster head key	1	N/A	50	1
Node-to-node keys	50	250	50	k
Node-to-sink key	1	N/A	1	1
Global key	1	N/A	1	1
Backup key	N/A	N/A	1	1
Commitment keys	50	N/A	N/A	N/A
Length of Key Chain	20	N/A	N/A	N/A
Size of Key Escrow Table	N/A	N/A	16	N/A
Total Primitives	124	250	121	$k+6$

[표 2]는 기존의 키 관리 기법과 본 논문에서 제안한 3DE_sec와의 필요한 저장 용량[12]을 비교한 것이다. 전체 노드의 수가 10,000개일 때, 키 링의 크기 k의 값을 94로 가정하면, 각 노드가 갖는 공간 사용량이 $100 \times |Key|$으로 LEAP, RPK, HIKES에 비해 필요한 공간 성능이 각각 19.4%, 60%, 그리고 17.4% 적게 사용됨을 알 수 있다. 이때 $|Key|$는 키의 크기를 나타내며, 에너지 효율보다 WSN 내의 안정성을 높이기 위해서는 k의 값을 높이면 된다.

다음 [그림 3]은 매 라운드마다 BS와의 인증에 사용되는 CH의 평균 에너지 소모량을 보여준다. 보안을 위한 키 관리 메커니즘에서 키의 크기가 16bit일 때, 3DE_sec가 HIKES에 비해 평균 576.4% 정도 적게 사용되어 전체 네트워크의 에너지를 효율적으로 사용할 수 있다.

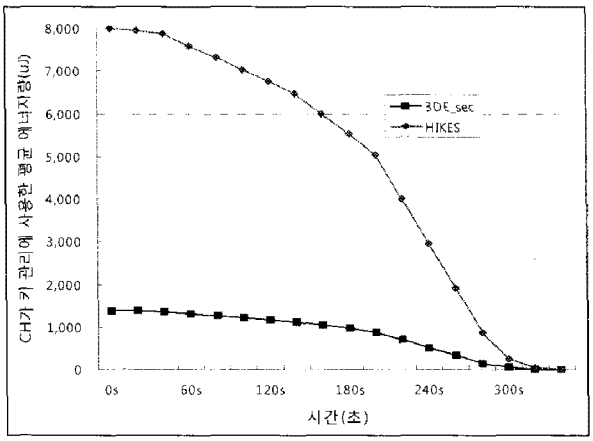


그림 3. 매 라운드마다 BS와의 인증에 사용되는 CH의 평균 에너지 소모량

V. 결 론

본 논문은 WSN 내의 클러스터 기반에서 클러스터 형성시 각 노드에게 배포 전에 적재된 복수개의 키 링을 이용하여 공유키 설정을 빠르고 안전하게 수행할 수 있는 키 관리 기법을 제안하였다. 또한 이 키 관리 기법은 노드들에 이동성 혹은 새로운 노드 삽입과 같은 경우에도 기존 키 관리 기법에 비해 에너지 효율적으로 형성할 수 있음을 보였다. 향후 과제로는 클러스터 기반의 라우팅 프로토콜에 적용하였을 때, 클러스터 형성시의 지연 시간을 최소화시켜 전체 네트워크 성능을 향상시켜야 한다.

참 고 문 헌

[1] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks," In 9th ACM conference on Computer and communications security, pp.41-47, 2002.

[2] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key pre-distribution scheme for wireless sensor networks," ACM Transactions on Information and System Security, Vol.8, pp.228-258, 2005.

[3] J. Hwang and Y. Kim, "Revisiting random key predistribution schemes for wireless sensor networks," In 2nd ACM workshop on Security of ad hoc and sensor networks, pp.43-52, 2004.

[4] D. Liu, P. Ning, and R. Li, "Establishing pairwise keys in distributed sensor networks," ACM Transactions on Information and System Security (TISSEC), Vol.8, pp.41-77, 2005.

[5] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," In 10th ACM conference on Computer and communication security, pp.62-72. 2003.

[6] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "Establishing pairwise keys for secure communication in ad hoc networks: A probabilistic approach," In 11th IEEE International Conference on Network Protocols (ICNP'03), pp.326-335, 2003.

[7] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, Vol.40, pp.102-114, Aug. 2002.

[8] W. R. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan,"Energy-Efficient Communication Protocol for Wireless Microsensor Networks," Proc. 33rd Hawaii Int'l. Conf. Sys. Sci., 2000(1).

[9] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Trans. Wireless Commun., Vol.1, No.4, pp.660-670, 2002(10).

[10] J. S. Kim, S. Y. Choi, S. J. Han, J. H. CHoi, J. H Lee, and K. W. Rim, "Alternative Cluster Head Selection Protocol for Energy Efficiency in Wireless Sensor Networks," In First Software Technologies for Future Dependable Distributed Systems (STFDDS'09), pp.159-163, 2009(5).

[11] M. G. Sadi, D. S. Km, and J. S. Park, "GBR: Grid Based Random Key Predistribution for Wireless Sensor Network," Proceedings of the 11th Annual IEEE International Conference on Parallel and Distributed Systems(ICPADS '05), Vol.2, pp.310-314, 2005(7).

[12] J. Ibriq and Imad Mahgoub, "A Hierarchical Key Establishment Scheme or Wireless Sensor Networks," Proceedings of 21st International Conference on Advanced Networking and Applications(AINA'07), pp.210-219, 2007.

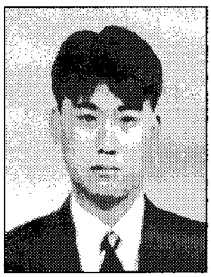
[13] R. M. S. Silva, N. S. A. Pereira, M. S. Nunes, "Applicability Drawbacks of Probabilistic Key Management Schemes for Real World Applications of Wireless Sensor Networks," Proceedings of the Third International Conference on Wireless and Mobile Communications (ICWMC'07), 2007.

[14] T. Moore, "A Collusion Attack on Pair-wise Key Predistribution Schemes for Distributed Sensor Networks," Proceedings of the Fourth Annual IEEE International Conference Pervasive Computing and Communications Workshops (PERCOMW06), pp.13-17, 2006(3).

[15] C. Hartung, J. Balasalle and R. Han, *Node Compromise in Sensor Networks: The Need for Secure Systems*, Technical Report CU-CS-990-05, 2005(1).

저 자 소 개

김 진 수(Jin-Su Kim) 정회원



- 1998년 2월 : 인천대학교 전자계산공학과(공학사)
- 2001년 8월 : 인하대학교 컴퓨터공학과(공학석사)
- 2001년 9월 ~ 현재 : 인하대학교 컴퓨터정보공학과 박사과정

<관심분야> : 유비쿼터스 컴퓨팅, 무선 센서 네트워크, 데이터마이닝, 정보검색

최 성 용(Seong-Yong Choi) 정회원

- 1993년 2월 : 인하대학교 통계학과(이학사)
- 2001년 2월 : 인하대학교 통계학과(이학석사)
- 2001년 3월 ~ 현재 : 인하대학교 컴퓨터정보공학과 박사과정

<관심분야> : 유비쿼터스 컴퓨팅, 무선 센서 네트워크, 데이터마이닝, 정보검색

정 경 용(Kyung-Yong Chung) 정회원

- 2000년 2월 : 인하대학교 전자계산공학과(공학사)
- 2002년 2월 : 인하대학교 컴퓨터정보공학과(공학석사)
- 2005년 8월 : 인하대학교 컴퓨터정보공학과(공학박사)
- 2005년 9월 ~ 2006년 2월 : 한세대학교 IT학부 교수
- 2006년 3월 ~ 현재 : 상지대학교 컴퓨터정보공학부 교수

<관심분야> : 유비쿼터스 컴퓨팅, 인공지능시스템, 데이터마이닝, U-CRM, HCI

류 중 경(Joong-Kyung Ryu) 정회원

- 1988년 2월 : 한국방송통신대학교 전자계산학과(이학사)
- 1991년 2월 : 인하대학교 산업대학원 정보공학과(공학석사)
- 1983년 ~ 1991년 : 대림산업 정보시스템실 대리
- 2003년 2월 : 인하대학교 컴퓨터정보공학과 박사수료
- 1992년 3월 ~ 현재 : 대림대학 컴퓨터정보계열 부교수

<관심분야> : 소프트웨어공학, HCI, ERP, CRM

임 기 욱(Kee-Wook Rim) 정회원

- 1977년 2월 : 인하대학교 전자공학과(공학사)
- 1987년 2월 : 한양대학교 전자계산학(공학석사)
- 1994년 8월 : 인하대학교 전자계산학(공학박사)
- 1977년 ~ 1988년 : 한국전자통신연구소 시스템소프트웨어 연구실장
- 1989년 10월 ~ 1996년 12월 : 한국전자통신연구원 시스템연구부장, 주전산기(타이컴)III,IV 개발사업 책임자
- 1997년 1월 ~ 1999년 12월 : 정보통신연구진흥원 정보기술전문위원
- 2001년 7월 ~ 2003년 2월 : 한국전자통신연구원 컴퓨터소프트웨어 연구소장
- 2000년 3월 ~ 현재 : 선문대학교 컴퓨터정보학부 교수

<관심분야> : 실시간데이터베이스시스템, 운영체제, 시스템구조

이 정 현(Jung-Hyun Lee) 정회원

- 1977년 2월 : 인하대학교 전자공학과(공학사)
- 1980년 9월 : 인하대학교 전자공학과(공학석사)
- 1988년 2월 : 인하대학교 전자공학과(공학박사)
- 1979년 ~ 1981년 : 한국전자기술연구소 연구원
- 1984년 ~ 1989년 : 경기대학교 전자계산학과 교수
- 1989년 1월 ~ 현재 : 인하대학교 컴퓨터공학부 교수

<관심분야> : 자연어처리, HCI, 음성인식, 정보검색, 고성능 컴퓨터구조