논문 2006-43TC-7-4

# 애드 혹 센서 네트워크를 위한 키 관리 방안

## ( A Key Management Scheme for Ad hoc Sensor Networks )

김 승 해*, 정 병 호**, 왕 기 철***, 조 기 환**

( Kim Seung Hae, Chung Byung Ho, Wang Gi Cheol, and Cho Gi Hwan )

요 약

무선 센서 네트워크에서 두 노드사이에 안전하게 pairwise키를 설정하고 분배하는 것은 매우 중요한 문제이다. 센서 네트워크는 물리적으로 취약한 보안성을 갖는 노드로 구성되므로 공격자에 의해 오염되기 쉽다. 그러나 기존의 선행 키 분배를 이용한 pairwise 키설정이나 1홉 지역키를 이용한 pairwise키 설정은 작은수의 노드들이 오염되더라도 보안성을 크게 약화시킨다. 본 논문은 무선 센서 네트워크에서 각 노드들이 네트워크 구성 초기에 3홉 지역키를 설정하고, 이후의 pairwise 키 설정에 이들 3홉 지역키들을 이용하는 방법을 제안한다. 임의의 두 노드가 pairwise키를 설정할 때, 두 노드 사이의 경로상에 존재하는 노드들은 자신들의 비밀키들을 두 노드에게 전송하는것에 의해 pairwise키의 생성에 공헌한다. 이로인해, 제안방법은 노드 밀집도와는 상관없이 두 노드사이의 경로길이에 의해 키설정을 위한 전송메시지수가 결정된다. 이때 경로상의 노드들로부터의 비밀키들을 안전하게 다른 노드들에게 전달하기 위해 3홉 지역키들이 비밀키들의 암호화에 사용된다. 따라서, 제안방법은 공격자가 1홉 지역키를 이용하는 방법에 비해 보다 많은 노드들을 오염시키도록 괴롭힌다. 실험결과는 제안된 방안이 선행 키 분배 방법에 비해 단위 키설정 동안 교환되는 메시지수 와 암호화/복호화 연산횟수, 그리고 안전성 면에서 보다 우수함을 입증하였다.

Abstract

It is very important to establish a pairwise key securely in wireless sensor networks. Because sensor networks consist of devices with weak physical security, they are likely to be compromised by an attacker. However, some approaches using key pre-distribution and other approaches using one hop local keys are known to be very vulnerable to threats caused by compromised nodes, even a small number. This paper proposes a scheme where each node establishes three hop local keys and employs them for a later pairwise key establishment. When any two nodes agree a pairwise key, all nodes on the route between two nodes contribute to the agreement of the pairwise key. Here, the initial three hop local keys are employed for encrypting a secret key delivered from a node to other nodes. Therefore, the proposed scheme bothers attackers to compromise much more nodes than the scheme using one hop local keys only. The simulation results have proven that the proposed scheme provides better performance and higher security than the scheme using one hop local keys in terms of message exchange, the number of encryption and decryption, and pairwise key exposure rate.

**Keywords :** Key Management, Sensor Network, Pairwise Key

## I. 서 론

센서 네트워크는 일반적으로 많은 수의 극히 작은 센서로 구성되는 네트워크이다. 이러한 네트워크에서 각 센서 노드는 제한된 전원을 가지고 동작하며 다양한 센서들을 통해 데이터를 감지하고 이를 수집하여 사용자에게 전달한다. 따라서, 센서 네트워크는 군사목적의 탐지 및 추적, 환경감시, 환자감시 및 추적 등과 같은 다양한 분야에 활용될 것으로 보인다.

센서 네트워크가 널리 사용되기 위해서는 네트워크 상의 각 노드들에게 안전한 통신을 보장할 수 있어야

* 정회원, 한국과학기술정보연구원, 전북대학교 정보보호공학과
(KISTI, Dept. of Information Security, Chonbuk National University)
** 정회원, 전자통신연구원 정보보호기반 그룹
(Division of Information Security Research, ETRI)
*** 정회원, 전북대학교 영상정보신기술 연구소
(Center for Advanced Image and Information Technology, Chonbuk National University)
**** 정회원, 전북대학교 전자정보공학부
(Division of Electronics and Information Engineering)
접수일자: 2006년6월15일, 수정완료일: 2006년7월14일

한다. 이는 일반적으로 센서 노드들이 무방비 상태의 환경이나 적대적인 환경에 배치되기 때문이다. 즉, 이러한 적대적인 환경하에서 임의의 공격자는 손쉽게 데이터 트래픽을 엿듣거나 수정할 수 있으며, 정당한 사용자인 것처럼 위장할 수 있다. 그러므로, 센서노드들 간의 통신은 기밀성과 인증을 보장할 수 있어야 한다. 즉, 센서 네트워크에서 임의의 두 노드간에 안전하게 키를 설정하고 분배하는 것은 매우 중요하다. 이러한 다른 노드 쌍으로부터 유일한 두 노드간의 키를 이후에는 pairwise키라 언급한다.

일반적으로 유선 네트워크 상에서의 키 관리는 인증기관(Certification Authority)이나 신뢰할만한 키분배 서버(Key Distribution Server)를 통하여 이루어진다. 일반 노드들은 그들의 서비스를 받아 키를 안전하게 분배받아 사용한다. 그러나 센서 네트워크는 신뢰할 만한 제삼의 기관이 존재하지 않으므로, 네트워크에 참여한 노드들끼리 협력적으로 키의 분배 및 관리를 수행하여야 한다. 즉, 기지국과의 공유된 키를 이용한 pairwise 키 설정 방법[1]은 센서 네트워크에는 부적합하다. 또한 센서 노드의 제한된 계산 및 에너지 자원으로 인해, Diffie-Hellman 프로토콜[2]이나 RSA[3]와 같은 공개키 암호화에 기반한 접근[4]은 적용될 수 없다. 이런 이유로, 대부분의 센서 네트워크를 위한 키관리 방법들은 모든 센서 노드들이 임의의 키 서버로부터 미리 키들을 분배받고 이 키들을 이용하여 임의의 두 노드간에 키 일치를 만들어 낸다. 그러나, 네트워크 구성 이전에 미리 키를 분배받는 방법은 보안 상 문제를 일으킬 수 있다. 예를 들어, 임의의 노드가 가지고 있는 키들은 임의의 키 분배 확률에 따라 네트워크 내의 다른 노드들에도 존재한다. 따라서, 이 방법에서 임의의 노드가 오염되면 같은 키들을 보유하는 다른 노드들에도 영향을 미치게 된다. 즉, 오염된 노드의 수가 증가하면 할수록, 많은 노드들의 pairwise 키 설정이 공격자에게 노출되게 된다. 또 다른 접근들은 각 노드가 모든 노드에게 공유된 키를 이용하여 네트워크 구성 초기에 자신의 이웃들과 초기키를 설정하고 이들을 pairwise 키설정에 이용하는 방법들[5-6]이다. 각 노드는 초기키들을 이용하여 상대방의 이웃 노드들에게 부분키들을 전달하고, 그 이웃 노드들은 또한 초기키들을 이용하여 부분키들을 상대방에게 전달한다. 이후에 pairwise 키 설정의 주체들은 같은 부분키들을 이용하여 키일치를 만들어 낸다. 그러나 이러한 방법들은 많은 통신부하와 계산부하를 유발한다. 더구나, 키 선행 분배 방법처럼 오염된 노드들의 증가에 취약하다.

본 논문에서는 제안하는 방법 또한 네트워크 구성 초기에 자신의 주변에 있는 노드들과 초기키를 설정하고 이 초기키들을 pairwise 키 설정을 위해 이용한다. 그러나 pairwise 키 설정을 위한 기본 원리와 초기키 설정의 범위, 그리고 초기 키를 이용하는 방법은 이전 방법과 크게 다르다. 먼저, 이전 방법은 키 설정의 기원자 노드가 과정을 주도하는 반면에 제안방법은 키설정의 주체사이에 존재하는 모든 노드가 키의 생성에 기여한다. 둘째, 제안하는 방법에서 대부분의 메시지 교환은 키설정의 주체간의 경로길이에 비례하므로, 노드의 밀집도에 비례하는 이전 방법에 비해 전송 메시지수를 크게 감소시킨다. 마지막으로, 위와 같은 이유로, 제안하는 방법은 이전 방법에 비해 암호화 연산 및 복호화 연산의 횟수를 크게 감소시킨다. 마지막으로, 제안하는 방법은 초기키 설정의 범위를 확장시켜 오염된 노드에 따르는 위협을 감소시킨다. 즉, 많은 초기키들이 키설정을 위한 부분키의 암호화에 이용되므로, 임의의 공격자가 이들 부분키들을 얻기 위해서는 많은 노드들을 오염시켜야 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 센서 네트워크에서 임의의 두 노드간에 안전하게 키를 설정하기 위한 기존의 기법들을 간략히 기술한다. Ⅲ장에서는 먼저 제안방법에 적절한 초기 초기키를 설정의 범위를 실험을 통해 선택하고 제안하는 키설정 방법에 대해 자세히 기술한다. Ⅳ장에서는 실험을 통해 제안된 방법과 기존의 초기키를 이용하는 방법을 효율성과 안전성 측면에서 분석을 한다. 본 논문의 결론은 Ⅴ장에서 다루어진다.

## Ⅱ. 관련연구

참고문헌 [7]은 선행 비밀 정보분배 기반의 pairwise 키설정방법에 관한 프레임워크를 제안하였다. 이 방법은 먼저 키 설정서버가 이변수 $t$차 다항식들을 담고 있는다항식 pool에서 임의의 갯수만큼의 다항식들을 랜덤하게 뽑고 그 다항식들의 부분키들을 각 노드들에게 분배한다. 각 노드는 이 부분키들을 이용하여 같은 부분키들을 가지는 노드와 직접 pairwise키를 설정한다. 만일 임의의 두 노드가 같은 부분키들을 가지지 못하는 경우에는, 두 노드와 공유된 부분키들을 가지거나 직접 pairwise키를 설정한 노드들을 검색한다. 이후에 검색된 노드들을 이용하여 간접적으로 pairwise키를 설정한다.

이 방법에서, 다항식 pool에 하나의 다항식만 남게되면 다항식 기반 키 선행 분배 방법으로 바뀌게 된다. 반대로 모든 다항식의 차수가 0이 되면 key pool 기반 선행 분배 방법으로 바뀐다. 이 방법은 선행 비밀정보 분배 시에 사용되는 다항식이 $t$번 이하로 사용되도록 함으로써 더욱 안전성을 높일 수 있다.

참고문헌 [8]은 임의의 키풀로부터 키들을 미리 분배받고 이들을 이용하여 이웃노드들과 pairwise키를 설정하는 방안을 제안했다. 이후 각 노드는 이 키들과 미리 분배된 키들을 이용하여 1홉 이상의 거리에 있는 노드들과 pairwise키를 설정한다. 참고문헌 [9]는 노드들의 대략적인 위치정보를 안다는 가정하에서, 임의의 노드가 작은 수의 키들만 분배받아도 이웃의 노드와 안전하게 pairwise키를 설정하는 방안을 제시하였다. 그러나 위의 두 방법들은 노드들이 이동하지 않고 고정되어 있는 상황에서만 적용이 가능한 방법들이다. 이는 만일 노드들이 이동한다면, 이웃 노드와 설정된 pairwise키를 이용하여 다중 홉 사이에 존재하는 노드간의 pairwise 키설정이 불가능하기 때문이다.

참고문헌 [10]은 노드들이 이동하는 상황에서 선행 키 분배방법을 이용하여 pairwise키를 설정하는 방법을 제안하였다. 이 방법에서 pairwise 키를 설정하고자 하는 소스노드는 요구되는 보안 수준에 따라 적절한 부분키의 개수를 정하고, 이 수만큼의 프록시 노드를 획득한다. 이때 프록시 노드들은 소스노드는 물론 목적노드와도 공유된 키들을 가지는 노드들이다. 소스노드는 임의의 pairwise키를 생성하고 이를 부분키의 수만큼 분할한 후에 이들을 각각의 프록시 노드들을 통해 목적노드에게 전송한다. 즉, 소스노드는 임의의 프록시 노드와 공유된 키들을 이용하여 부분키를 암호화해서 프록시 노드로 전송하고, 프록시 노드는 이를 해독하여 다시 목적노드와 공유된 키들로 부분키를 암호화하여 전송한다. 따라서 임의의 악의적인 노드는 임의의 두 노드간의 pairwise키를 얻기 위해서는 부분키들의 암호화에 사용된 모든 초기 분배 키들을 획득해야 한다. 이 방법의 가용성은 요구되는 보안 수준을 만족시키기 위한 프록시 노드의 수에 의해 좌우된다. 즉, 요구되는 보안수준이 높아질수록, 프록시 노드의 수는 증가한다. 즉, 임의의 소스노드가 요구되는 수만큼의 프록시 노드를 발견하지 못하면 키 설정은 실패로 끝나게 된다. 더구나 요구되는 보안 수준은 한번 정해지면 수정이 불가하므로, 노드들간의 연결성이 저하되면 키 설정 서비스의 가용성은 크게 감소한다. 이 방법의 안전성은 key pool에 있는 각 키가 임의의 노드에게 분배될 확률에 따라 좌우된다. 즉, key pool에 있는 각 키가 임의의 노드에게 분배될 확률이 작을수록 네트워크의 보안성이 향상된다. 또한 부분키의 개수가 많으면 많을수록 네트워크의 보안성은 크게 향상된다. 그러나 이는 많은 부분키의 전송을 위한 높은 통신부하를 유발하여 시스템의 성능을 저하시킨다. 그러나, 이 방법의 가장큰 문제점은 오염된 노드의 수가 증가한다면 이들에 의해 영향을 받는 pairwise key들의 수가 빠르게 증가한다는 것이다.

참고문헌 [5]에서 각 노드는 먼저 초기 네트워크 전역 키(initial network-wide key)를 이용하여 이웃 노드간에 초기키(즉, 1홉 pairwise키)를 설정한다. 이후에 각 노드는 이 1홉 pairwise키들을 이용하여 자신의 클러스터 키를 각 이웃노드에게 전송한다. 이 클러스터 키는 이웃노드에게 방송메시지를 안전하게 전송하고자 할 때 이용된다. 만일 임의의 소스노드가 자신의 이웃 (1홉)에 있지 않은 목적노드와 pairwise키를 설정하고자 한다면, 소스노드는 이웃노드간에 설정된 1홉 pairwise키들과 클러스터 키들을 이용하여 목적노드와 pairwise키를 설정한다. 즉, 소스노드는 클러스터 키를 이용하여 목적노드와 이웃에 위치하는 프록시 노드들을 찾아내고 임의의 pairwise키를 생성한다. 소스노드는 pairwise키들을 분할한 후에 프록시 노드들을 통해 부분키들을 목적노드에게 전송한다. 이때 부분키들은 전송에 앞서 1홉 pairwise키로 암호화된다는 것에 유의하라. 목적노드는 모든 부분키들을 수신한 후에, 원래의 pairwise키를 복원한다. 이 기법의 안전성은 검색된 목적노드와 연결된 프록시 노드의 수에 의해 좌우된다. 즉, 목적노드와 연결된 모든 프록시 노드가 오염되지 않는 한 안전하다. 따라서 가능한 많은 노드가 목적노드와 연결될수록 이 기법은 안전하다. 그러나 이는 또한 통신 오버헤드 및 계산 오버헤드를 크게 증가시킨다. 더구나 이 기법은 위의 선행 키분배 방법처럼 작은 수의 노드들만 오염되더라도, 이들에 의해 영향을 받는 pairwise키의 수가크게 증가한다.

참고문헌 [6]에서는 임의의 센서 네트워크에서 모든 노드들에게 공유된 임의의 키들을 이용하여 이웃하는 각 노드간에 1홉 pairwise키를 설정하는 방안을 제안했다. 이후 이 pairwise 키들은 그룹키를 주기적으로 갱신할 때 이용된다. 그러나 이 방법은 1홉 이상의 거리에 있는 노드간에 pairwise키를 설정하는 방안에 대해 다루고 있지 않다.

## Ⅲ. 초기 지역키 설정에 기반한 키관리 방법

### 1. 초기 지역키 설정의 범위 결정

참고문헌 [5]과 [6]의 접근은 임의의 두 노드 사이에 선행 비밀정보 없이 pairwise키를 설정하기 위해 네트워크 구성 초기에 자신의 이웃에 위치하는 노드들과 초기키들을 설정한다. 이 키들을 이후에는 지역 키들이라고 부르기로 한다. 그러나 이러한 지역키들을 이용한 프록시와의 메시지 교환은 노드들의 오염에 영향 받기 쉽다. 즉, 만일 소스로부터 임의의 프록시 노드로의 경로 사이에 존재하는 노드들 중에서 하나만 오염되어도, 그 프록시로 전송되는 부분키는 바로 노출된다. 이는 각 노드가 초기에 자신의 이웃들과만 지역키를 설정하기 때문이다. 따라서, 제안하는 방법은 이 문제를 완화시키기 위해 더 많은 노드들을 부분키 전송에 참여시킨다. 즉, 제안하는 방법은 부분키 전송을 위해 자신의 이웃노드들이 가진 지역키들을 이용하도록 한다. 이를 위해서는 초기키 설정의 범위를 확장시킬 필요가 있다.

지역키 설정의 범위를 결정하기 위해 다음과 같은 파라미터를 이용하여 시뮬레이션을 수행했다. 초기에 100개의 센서 노드가 500m*500m의 영역 내에서 랜덤하게 배치되었고 각 노드의 전송거리는 30m였다. 또한 센서가 파괴되거나 손실되기 쉬운 센서 네트워크 환경을 고려하여, 네트워크 구성 이후에, 전체 노드의 10%를 통신할 수 없는 "불능상태"의 노드로 지정하였다. 각 노드는 "불능상태"의 노드를 제외한 자신의 이웃노드들과 지역키를 설정했다. 이때 각 노드와 지역 키를 설정한 이웃노드들은 그 노드의 친구 노드들이라고 불린다.

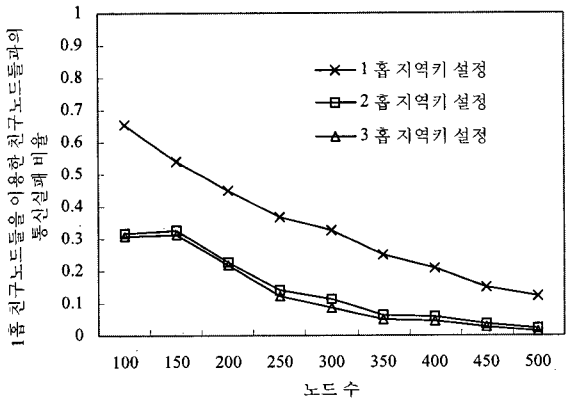


그림 1. 불능노드로 인한 친구노드들과의 통신실패비율 vs. 노드수의 증가

Fig. 1. Communication failure rate with friends vs. number of nodes.

사실, 이동성이 거의 없는 센서 네트워크에서 네트워크 구성 초기에 설정된 지역키들이 노드들간의 부분키 전송에 이용되므로, 초기 지역키 설정의 범위는 노드간 안전한 통신 거리를 결정한다고 볼 수 있다. 만일 임의의 노드가 초기 지역키 설정의 범위보다 먼 거리에 있는 노드에게 부분키 전송을 하고자 할 경우에, 이 노드는 자신의 친구들을 이용하여야만 안전하게 그 부분키를 전송할 수 있다. 또한 초기 지역키 설정의 범위는 각 노드가 자신의 주변에 있는 노드들로의 경로들을 자연스럽게 획득하는 계기가 되기도 한다. 초기 지역키 설정 이후에, 모든 노드가 자신의 친구 노드들과 부분키 교환을 시도한다. 이때 각 노드는 자신의 1홉 이웃에 존재하는 친구노드들의 지역키만을 이용하여 자신의 부분키를 전송하려고 한다. 따라서 각 노드는 1홉 이웃에 존재하는 친구노드들의 친구리스트들을 획득하고 이를 통합한다. 각 노드는 통합된 리스트와 자신의 친구리스트와 비교하여 이 통합 리스트가 얼마나 많은 다른 친구들을 포함하지 않는지 측정한다. 만일 이 통합리스트가 임의의 친구노드들을 포함하지 않는다면, 그 친구노드들과는 부분키 교환이 불가능해진다. 측정값은 파손된 센서노드가 존재하는 상황에서, 임의의 노드가 1홉 친구노드들의 도움을 통해 다른 친구노드들과 안전하게 통신할 수 없는 비율을 나타낸다. 다음으로, 초기에 각 노드가 자신의 지역키 설정의 범위를 확장시켰을 때, 이 측정값이 어떻게 변하는 지를 측정했다.

그림 1은 노드수의 증가에 따른 이 비율의 변화를 보여준다. 그림 1에서 보는 것처럼, 노드들의 밀집도가 증가할수록 비율이 감소하는 것은 매우 당연하다. 만일 각 노드가 초기에 1홉 local키를 설정하면 이웃노드들을 통해 친구들과 안전한 통신을 하는 것은 매우 어렵다. 이는 "불능상태"에 있는 노드들로 인한 것이다. 만일 loca 키 설정의 범위를 2홉 이상으로 확장시키면, "불능상태"를 가진 노드들을 제외하고 다른 이웃노드들을 통해서 친구노드들과 통신할 수 있는 비율이 매우 높아진다. 특히, 각 노드가 초기에 이웃노드들과 3홉 지역키를 설정하면, "불능상태"의 노드가 존재하는 상황에서도 부분키 전송에 실패하는 비율은 크게 감소된다. 이러한 이유로, 제안하는 방법은 각 노드가 모든 노드들과 공유된 초기 네트워크 전역키를 사용하여 초기에 3홉 local키를 설정한다고 가정한다.

### 2. 3홉 지역키를 이용하는 키 관리 방안

참고문헌 [5]와 [6]은 각각 1홉 지역 키를 설정하는

방안에 대해서만 기술하고 있다. 참고문헌 [11]에서는 지역키 설정의 범위를 3홉 까지 확장하는 방안을 기술하였다. 본 논문에서도, [11]의 방법을 이용하여 각 노드가 초기에 3홉 지역키를 설정한다고 가정한다.

임의의 센서노드가 자신의 친구노드와 키를 설정하고자 하면, 그 노드는 친구노드로의 경로를 찾을 필요가 없다. 이는 초기 3홉 지역키 설정과정에서 이미 친구노드들에 대한 경로를 손쉽게 얻기 때문이다. 그러나 만일 친구가 아닌 노드와 키설정을 할 경우에는, 그 노드로의 경로를 찾아야 한다. 이 경우에도 역시 제안방법은 최대 3홉 거리내에 있는 노드로의 경로를 미리 알고 있으므로, 작은 통신오버헤드로 빠르게 경로를 획득할 수 있다. 예를 들어, 임의의 노드 $u$가 친구가 아닌 노드 $v$로의 경로를 찾는다고 가정해보자. 먼저 노드 $u$는 $v$의 ID를 담은 경로질의 메시지를 임의의 3홉 거리에 있는 노드에게 전송한다. 경로질의 메시지를 수신한 노드는 노드 $v$가 자신의 친구노드인지 아닌지 확인한다. 만일 $v$가 친구노드이면, $v$로의 경로를 담고있는 경로응답메시지를 노드 $u$에게 전송한다. 그렇지 않다면, 응답하지 않는다. 만일 노드 $u$는 경로응답 메시지를 일정시간 동안 수신하지 못하면, 경로질의 메시지를 다른 3홉 거리노드에게 전송한다. 위의 과정은 노드 $v$로의 경로를 발견할 때 까지 반복된다. 물론, 3홉 거리 노드들 사이의 메시지 교환은 3홉 지역키들에 의해 보호된다.

제안하는 방법은 만일 임의의 두 노드가 pairwise 키 설정을 원하면, 그림 2에서처럼 두 노드사이의 경로상에 존재하는 모든 노드들이 키 생성에 참여하는 방식을 택했다. 경로상의 각 노드는 동일한 길이의 비밀키를 생성하여 각각 두 노드들에게 전송하고 두 노드들은 이 비밀키들을 XOR연산을 수행하여 pairwise키를 생성한다. 예를 들어, 그림 2에서 두 노드 $u$와 $v$사이의 경로상에 존재하는 노드 $u$, $w$, $x$는 각각 자신의 비밀키를 생성하고 이를 $u$와 $v$에게 전송한다. 이때, 각 노드는 비밀키를 전송할 순서가 되었다는 것을 키설정 메시지의 수신을 통해 알게 된다. 또한 pairwise키의 안전성은 경로상의 각 노드로부터 전송되는 비밀키의 안전성에 의해 좌우되므로, 비밀키의 안전한 전송을 위한 방법이 요구된다. 이를 위해서 각 노드는 초기에 설정된 지역키를 이용하여 비밀키를 암호화한 뒤에 전송한다. 이때 이용되는 지역키들은 이웃노드들로부터 획득된 지역키 일수도 있고 자신의 메모리에 저장된 것 일수도 있다. 이러한 선택은 각 노드가 생성한 비밀키에 의해 좌우된다. 즉, 자신이 생성한 비밀키를 2로 나누어 나머지가 0이면 자신의 메모리에 저장된 지역키를 이용하고 그렇지 않은 경우에는 이웃 노드들로부터 획득한다. 예를들어, 그림 2에서 노드 $w$와 $x$는 비밀키를 전송하기에 앞서, 이웃 노드들로부터 지역 키들을 획득한다. 물론, 이웃노드들은 그들이 적어도 키설정의 주체들과 적어도 하나의 노드와 공유된 지역키를 가질 경우에만 지역키를 제공한다. 키설정의 한 주체인 노드 $v$는 수신한 비밀키들을 이용하여 자신의 비밀키 암호화에 이용될 키 (i.e. $K_{part}$)를 생성한다. 이때 같은 방법으로 노드 $u$또한 $K_{part}$를 생성할 수 있음을 유의하라. 또한 노드 $v$는 수신한 비밀키들과 자신의 비밀키를 XOR연산하여 노드 $u$와의 pairwise키 (i.e. $K_{uv}$)를 생성한다. 이후에 노드 $v$는 자신의 비밀키($k_v$)와 pairwise키로 인증된 DONE메시지를 노드 $u$에게 전송한다. 노드 $u$는 비밀키와

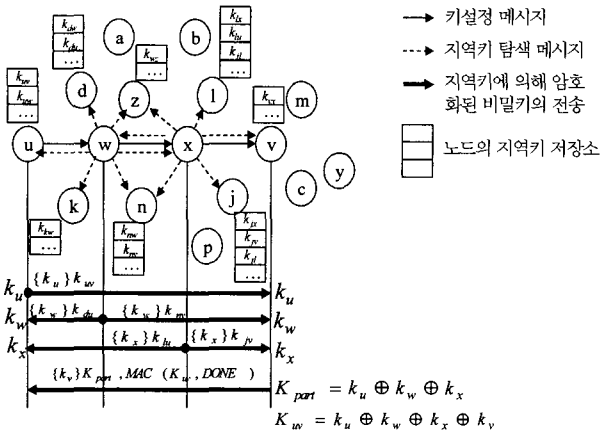


그림 2. 최대 3홉 거리에 위치한 노드와의 키 설정 절차
Fig. 2. Key establishment procedure between at most three hop distance nodes.

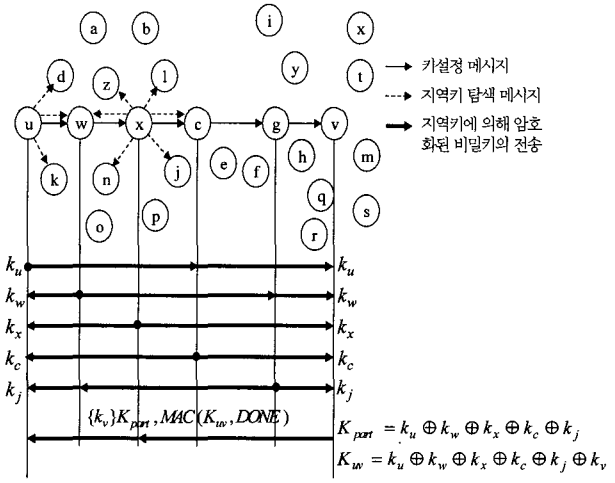


그림 3. 3홉 거리 이상의 노드와의 키설정 절차
Fig. 3. Key establishment procedure between nodes further away than three hops.

DONE메시지를 검증하고, $v$와 같은 방법으로 pairwise 키를 생성한다. 즉, 키 설정의 두 주체가 가진 비밀키의 개수가 다르거나 서로 다른 비밀키를 가지게 되면, 그 키설정은 실패로 끝나게 된다. 또한, 만일 키설정의 개시자(즉, 그림 2에서의 $u$)가 일정시간 동안 상대방 노드(즉, 그림2에서 $v$)로부터 DONE메시지를 수신하지 못하면, 그 키설정은 중단된다. 이후, 키설정의 소스는 시간이 지난 후에, 다시 키설정을 시도한다.

위의 pariwise키 설정 절차는 두 노드 사이의 거리가 3홉 이내에 있을 경우에만 적용될 수 있다. 이는, 두 노드 사이의 거리가 4홉 이상이 되면 키 설정의 주체와 직접 비밀키 교환을 하기가 어려워 지기 때문이다. 예를 들어, 그림 3에서 처럼, 노드 $u$는 설령 이웃노드들로부터 지역키들을 얻는다 하더라도, 자신의 비밀키를 상대방 노드인 $v$에게 직접 전송할 수 없다. 이는 노드 $v$와 지역키를 설정한 노드들이 이웃에 존재하지 않기 때문이다. 같은 문제가 노드 $w$와 $v$ 사이에서도 발생한다. 이런 경우에, 경로상의 각 노드는 자신과 3홉 거리에 있는 경로상의 노드에게 자신의 비밀키를 중계해주도록 요청한다. 예를들어, 그림 3에서, 노드 $u$는 노드 $c$를 통해 자신의 비밀키를 노드 $v$에게 전달한다. 같은 방법으로, 노드 $w$는 노드 $j$를 통해 자신의 비밀키를 노드 $v$에게 전달한다. 나머지 pairwise 키 설정 절차는 3홉거리 노드들 간의 비밀키 교환방법과 같다.

## Ⅳ. 분 석

제안하는 방법의 효율성 및 안전성을 입증하기 위해, 이산사건중심의 실험도구인 CSIM 18엔진과 C언어를 이용하여 실험환경을 구축하였다. 제안하는 방법은 선행비밀 정보의 분배 없이 pairwise키설정을 수행하므로, 선행 비밀정보를 이용하는 방법들[7-10]은 비교 대상에서 제외되었다. 따라서 제안하는 방법은 초기에 자신의 이웃노드들과 지역키를 설정하고 이들을 이용하여 pairwise키를 설정하는 방법인 LEAP[5]과 비교되었다. 성능분석을 위한 시뮬레이션 파라미터와 그 값들은 표 1과 같다.

표 1. 실험 파라미터들
Table 1. Simulation parameters.

| 파라미터 | 값 |
|---|---|
| 노드수 | 200~500 |
| 실험영역 | 500 미터 * 500미터 |
| 전송범위 | 40 미터 |
| 센서노드간 경로생성 | Shortest path algorithm |
| 실험시간 | 600 초 |
| 오염된 노드의 비율 | 10%~70% |
| 키설정 주기 | 2 초 |

효율성을 위한 척도로 키 설정 동안 교환되는 메시지 수가 선정되었다. 이때 제안하는 방법에서 네트워크 구성 초기에 이웃간에 지역키를 설정하기 위해 교환된 메시지는 포함되지 않았다. 효율성을 위한 또 다른 척도로 키 설정 동안 수행되는 암호화 및 복호화 연산의 실행횟수가 선정되었다.

만일 일단의 노드들이 적에게 오염 (compromise)된 경우에 그 적은 그 노드들이 보유하고 있는 초기 지역키들을 확보할 수 있다. 이는 곧 임의의 두 노드 간에 설정되는 pairwise키의 안전성에 심각한 위협이 발생할 수 있음을 의미한다. 다시 말하면, 임의의 적이 오염된 노드들로부터 확보한 지역 키들이 pairwise키 설정 동안 비밀정보 교환에 이용되는 지역 키들을 모두 포함하게 되면 그 pairwise키는 바로 노출된다. 따라서 안전성을 위한 척도로 오염된 노드들이 있는 상황에서 pairwise키 설정 동안 이용되는 지역키들의 노출비율이 선정되었다. 이때 오염되는 노드들은 임의로 선정되었다. 모든 실험결과에서 제안하는 방법은 THLKBS (Three Hop Local Key Based Scheme)로 명명 되었음을 유의하라

### 1. 효율성 분석

그림 4는 노드수의 증가에 따른 키설정 동안 교환되는 메시지 수의 변화를 보여준다. 그림 4에서 보는 것처럼, LEAP는 노드수의 증가에 민감하게 반응한다. 이는 고정된 실험영역 하에서 노드수가 증가하면 밀집도

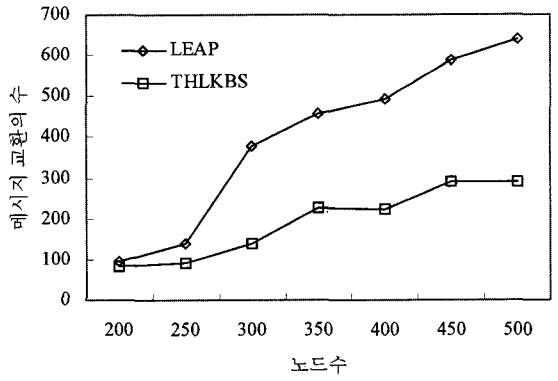


그림 4. 노드수의 증가에 따른 메시지 교환수의 변화
Fig. 4. Number of messages exchanged vs. number of nodes.

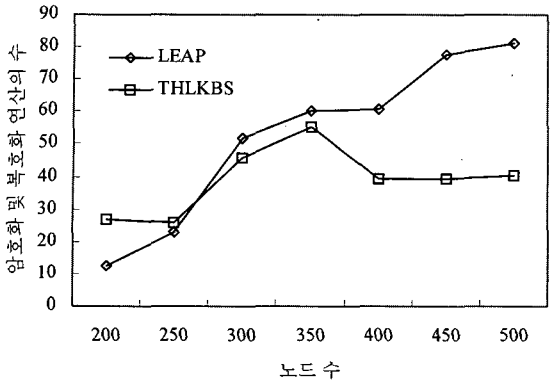


그림 5. 노드수의 증가에 따른 암호화 및 복호화 연산의 수

Fig. 5. Number of encryptions and decryptions vs. number of nodes.

가 증가하기 때문이다. 즉, 높은 밀집도 하에서 임의의 키 설정 소스는 키설정 대상 노드의 이웃들인 프록시 노드들을 검색하기 위해 훨씬 많은 메시지 교환을 수행해야 한다. 또한 프록시 노드들의 수도 많아지므로, 소스와 프록시 노드들과의 통신비용도 증가하게 된다. 반면에 제안하는 방법은 제안하는 방법은 프록시 노드들을 파악하기 위한 검색메시지가 불필요하므로 전송되는 메시지 수를 크게 감소시킨다. 더구나 키 설정과정 동안 단지 1홉 거리에 있는 이웃노드와만 통신하므로 노드 밀집도의 영향을 훨씬 적게 받는다.

그림 5는 노드수의 증가에 따른 암호화 연산 및 복호화 의 실행횟수의 변화를 보여준다. 그림 5에서 보는 것처럼, 낮은 밀집도 (노드수 250미만)에서 제안하는 방법은 LEAP에 비해 보다 많은 암호화 및 복호화 연산을 실행한다. 만일 노드 밀집도가 낮다면, LEAP에서 키설정의 소스는 오직 작은 수의 프록시 노드들만을 파악할 수 있다. 즉, 키설정의 소스와 프록시 노드들간의 경로수가 감소하므로, 이에 따라 암호화 및 복호화 연산의 실행횟수도 감소된다. 반면에, 제안하는 방법에서, 암호화 및 복호화 연산의 횟수는 노드 밀집도 보다는 키 설정의 소스와 목적노드 사이의 경로길이에 더 영향을 받는다. 이는 경로상의 각 노드가 이웃노드로부터 지역키를 제공받을 때 및 경로상의 각 노드가 자신의 비밀키를 전송하고 수신할 때 암호화 연산 및 복호화을 이용하기 때문이다. 이런 이유로, 제안하는 방법은 노드 밀집도가 증가하여도, 암호화 연산 및 복호화 연산의 실행횟수를 크게 증가시키지 않는다.

## 2. 안전성 분석

다음으로, 오염된 노드들의 존재가 설정되는 pairwise 키의 안전성에 어떤 영향을 미치는 지 파악하기 위해, 오염된 노드수의 증가에 따라 pairwise 키설정을 위해 요구되는 지역키들의 노출비율이 측정되었다. 그림 6에서 보는 것처럼, LEAP는 오염되는 노드들의 비율이 20% 이상이 되면 pairwise키 설정을 위해 이용되는 지역키들의 80%이상이 노출된다. 이는 LEAP에서 소스로부터의 부분키들은 프록시 노드들을 거쳐서 키 설정의 목적노드에게 전달되기 때문이다. 이때 소스와 프록시 사이의 경로상의 노드들 중에서 하나만 노출되어도 전달되는 하나의 부분키는 공격자에게 알려지게 된다. 이것이 시사하는 바는 매우 의미가 있다. 만일 임의의 공격자가 임의의 두 노드사이의 pairwise키를 알고싶다면, 부분키가 전송되는 모든 경로상에 존재하는 노드들이 아니라 그들 중에서 일부만 오염시켜도 되기 때문이다. 반면에, 제안하는 방법은 키 설정의 소스 와 목적노드 사이의 경로상에 존재하는 노드는 물론 그 이웃노드들도 키 설정에 연루되므로, 오염시켜야 되는 대상의 수가 크게 늘어나게 된다. 따라서, 제안하는 방법은 노드들의 오염에 훨씬 덜 민감하다. 그림 6에서 보는 것 처럼, 제안하는 방법은 오염된 노드들의 비율이 70%까지 증가하더라도 pairwise 키 설정을 위해 이용되는 지역키들의 약 12%만 공격자에게 노출된다.

그림 7은 오염되는 노드의 수를 20개로 고정시킨후, 노드수의 증가에 따른 pairwise 키설정을 위해 사용된 지역키들의 노출비율을 보여준다. 그림 7에서 보는 것처럼, LEAP는 중간의 노드수가 약간 증가하면(노드수

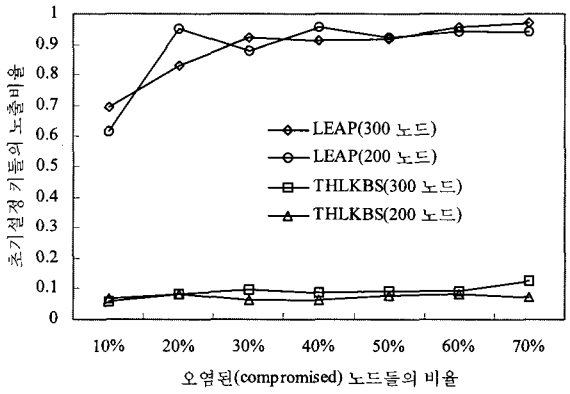


그림 6. 오염노드들의 비율증가에 따른 초기설정 키들의 노출비율

Fig. 6. Exposure rate of initially established keys vs. rate of compromised nodes.

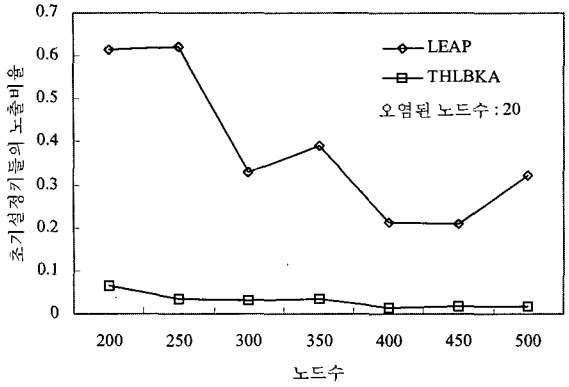


그림 7. 노드수의 증가에 따른 초기설정 키들의 노출비율

Fig. 7. Exposure rate of initially established keys vs. number of nodes.

300) local키들의 노출비율이 급격히 감소한다 하지만 노드수가 계속 증가하면, local키들의 노출비율이 그다지 영향을 받지 않는다. 다시 말하면, 이 방법은 극히 작은 수의 노드가 오염 되더라도 전체 네트워크의 보안에 큰 영향을 준다. 반면에, 제안하는 방법은 노드수가 증가함에 따라 local키 노출비율이 점차 감소한다. 이것은 제안하는 방법이 공격자가 임의의 임계치 이상의 노드를 오염시키지 못하는 동안, 노드의 증가에 따라 더욱 높은 안전성을 제공한다는 것을 의미한다.

## V. 결 론

제안한 방법은 키 설정의 주체 사이에 존재하는 각 노드들의 협력에 의해 키를 설정하므로, 키설정 동안 교환되는 메시지의 수 및 암호화/복호화 연산 실행 횟수가 노드 밀집도에 영향을 받지 않도록 하였다. 또한, 제안 방법은 미리 임의의 비밀정보를 분배 받지 않고 네트워크 구성 초기에 3홉 지역키를 생성하여 이들을 이후의 pairwise키 설정에 이용한다. 따라서 제안하는 방법의 보안성은 비밀정보의 선행분배에 의한 확률에 의해 좌우되지 않으며, 많은 노드들이 키 설정에 참여하므로 노드들의 오염에도 잘 견디는 내구성을 지닌다. 제안하는 방법은 실험결과에 의해 1홉 지역키만을 이용하는 LEAP에 비해 키설정 동안 교환되는 메시지수가 작고 암호화 및 복호화 연산의 실행도 작은 빈도로 발생함을 증명하였다. 또한 제안하는 방법은 많은 노드들이 오염되더라도, 이들이 다른 노드들의 pairwise키 설정에 미치는 영향을 최소화시킴을 보여주었다.

## 참 고 문 헌

[1] A. Perrig et al,. "SPINS: Security Protocols for Sensor Networks," in Proc. of the 7th ACM/IEEE Int'l Conf. on MbiCOM, pp. 189-199, July 2001.

[2] W. Diffie and M. E. Hellman, "New Directions in Cryptography," *IEEE Trans. on Information Theory*, Vol. 22, No. 9, pp. 33-38, 1976.

[3] R. Rivest et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Communications of the ACM*, Vol. 2, No. 2, pp. 120-126, 1978.

[4] G. Wang, G. Cho, and S. Bang, "A Pair-wise Key Establishment Scheme without Pre-distributing Keys for Ad-hoc Networks," in CD Proc. of IEEE ICC'05, May 2005.

[5] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," in Proc. of the 10th ACM Conference on CCS '03, Oct. 2003.

[6] B. Dutertre, S. Cheung, and J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust," SRI International, Tech. Rep. SRI-SDL-04-02, 2004.

[7] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," in Proc. of the 10th ACM CCS '03, pp. 52-61, Oct. 2003.

[8] L. Eschenauer and V. D. Gilgor, "A Key-Management Scheme for Distributed Sensor Networks," in Proc. 9th ACM Conf. on CCS '02, pp. 41-47, Nov. 2002.

[9] W. Du et al., "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," in Proc.of IEEE INFOCOM, Vol. 1, pp. 586-597, Mar. 2004.

[10] S. Zhu et al., "Establishing Pair-wise Keys For Secure Communication in Ad Hoc Networks: A Probabilistic Approach," in Proc. of the 11th Int'l Conf. on Network Protocols, 326-335, Nov. 2003.

[11] G. Wang and G. Cho, "Compromise-Resistant Pairwise Key Establishments for Mobile Ad hoc Networks," *ETRI Journal*, Vol. 28, No. 3, pp. 375-378, June 2006.

## 저 자 소 개


**김 승 해**(정회원)
1997년 한남대학교 정보통신 공학과 학사 졸업
2003년 전북대학교 정보과학과 석사 졸업
2006년 전북대학교 정보보호 공학과 박사수료
1996년 12월~1999 한국전자통신연구원
2000년 1월 ~현재 한국과학기술정보연구원 선임연구원
<주관심분야 : 차세대인터넷, Routing, Security >

**왕 기 철**(정회원)
1997년 광주대학교 전자계산학과 졸업
2000년 목포대학교 멀티미디어 공학과 석사 졸업
2005년 전북대학교 컴퓨터통계 정보학과 박사 졸업
2005년 12월~현재 전북대학교 영상정보신기술 연구소 연구원
<주관심분야 : 이동컴퓨팅, Ad hoc 네트워크, 무선네트워크 보안>

**정 병 호**(정회원)
1988년 전남대학교 전산통계학과 학사 졸업
2000년 충남대학교 컴퓨터과학과 석사 졸업
2005년 충남대학교 컴퓨터과학과 박사 졸업
1998년 2월~2000년 6월 국방과학연구소 선임연구원
2000년 6월~현재 한국전자통신연구원 정보보호 기반그룹 선임연구원
<주관심분야 : 무선 LAN보안, 무선 네트워크, Ad-Hoc 네트워크>

**조 기 환**(정회원)
1985년 전남대학교 계산통계학과 학사 졸업
1987년 서울대학교 계산통계학과 석사 졸업
1996년 영국 Newcastle 대학교 전산학과 박사 졸업
1987년~1997년 한국전자통신연구원 선임연구원
1997년~1999년 목포대학교 컴퓨터과학과 전임강사
1999년~현재 전북대학교 전자정보공학부 부교수
<주관심분야 : 이동컴퓨팅, 컴퓨터통신, 무선네트워크 보안, 센서네트워크, 분산처리시스템>