논문 2010-47TC-2-15

센서 네트워크에서 복원력을 지닌 키갱신 방안

(A Resilient Key Renewal Scheme in Wireless Sensor Networks)

왕 기 철*, 조 기 환**

(Gicheol Wang and Gihwan Cho)

요 약

센서 네트워크에서, 센서들은 보호되지 않는 환경에 배치되므로 공격자들의 오염타깃이 되기 쉽다. 만일 오염센서들의 수가 급격히 증가하면, 키 관리 자체가 무력화 된다. 특히, 클러스터 기반의 센서 네트워크에서 클러스터 헤드 (CH: Cluster Head)들의 오염은 일반센서들의 오염보다 훨씬 더 위협적이다. 따라서, 최근에는 오염된 센서들에게 노출된 키들을 그들에게 알려지지 않은 키들을 이용하여 변경시키는 키 갱신 기법들이 부상하고 있다. 그러나 이들은 클러스터 내에서의 그룹키 사용, 매우 소극적인 오염노드 퇴출, 과도한 통신 및 연산오버헤드 유발과 같은 문제점들을 발생시킨다. 본 논문에서는 클러스터 기반의 센서 네트워크에서 클러스터 조직의 갱신을 이용한 선행적인 키갱신 기법을 제안한다. 제안방법에서, 각 센서들은 네트워크 구성시간에 이웃센서들과 개별키들을 설정하며, 이 키들은 클러스터내의 통신에 이용된다. 주기적인 클러스터 재조직에 의해 오염노드들은 네트워크로부터 퇴출되며, 임의의 클러스터 내에서 사용되는 개별키들은 계속해서 변경된다. 또한 새로 선출된 CH들은 자신의 멤버들을 싱크에게 알리는 것에 의해 싱크와 안전하게 키를 일치시킨다. 실험결과는 제안방법이 오염노드들의 증가에도 불구하고 기밀성과 무결성을 크게 향상 시킴을 보여주었다. 또한 실험결과는 제안방법이 SHELL에 비해 소중한 에너지를 더 효율적으로 사용함을 보여주었다.

Abstract

In sensor networks, because sensors are deployed in an unprotected environment, they are prone to be targets of compromise attack. If the number of compromised nodes increases considerably, the key management in the network is paralyzed. In particular, compromise of Cluster Heads (CHs) in clustered sensor networks is much more threatening than that of normalsensors. Recently, rekeying schemes which update the exposed keys using the keys unknown to the compromised nodes are emerging. However, they cause some security and efficiency problems such as single group key employment in a cluster, passive eviction of compromised nodes, and excessive communication and computation overhead. In this paper, we present a proactive rekeying scheme using renewals of cluster organization for clustered sensor networks. In the proposed scheme, each sensor establishes individual keys with neighbors at network boot-up time, and these keys are employed for later transmissions between sensors and their CH. By the periodic cluster reorganization, the compromised nodes are expelled from network and the individual keys employed in a cluster are changed continuously. Besides, newly elected CHs securely agree a key with sink by informing their members to sink, without exchangingany keying materials. The simulation results shows that the proposed scheme remarkably improves the confidentiality and integrity of data in spite of the increase of compromised nodes. Also, they show that the proposed scheme exploits the precious energy resource more efficiently than SHELL.

Keywords: sensor networks, confidentiality, energy efficiency, integrity, key management

* 정회원, 한국과학기술정보연구원
(Korea Institute of Science and Technology Information)
** 정회원, 전북대학교 영상정보신기술센터, 전북대학교
(CAIIT at Chonbuk National University, Chonbuk National University)
※ 이 논문은 2009년도 정부(교육과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임
(2009-0083985)
접수일자: 2008년8월5일, 수정완료일: 2010년2월17일

Ⅰ. 서 론

센서 네트워크에서 센서들은 보호되지 않는 환경에 배치되므로, 공격자들에 의해 포획되기 쉽다. 따라서, 센서들 내에 저장된 키를 계속해서 변경시켜주는 키 갱신기법이 키 관리기법 내에 포함되어야 한다. 센서 네트워크에서 기존의 키 갱신기법들은 두 가지로 구분된다. 먼저, 무갱신 기법이 있다. 이 방법들에서 센서들은 미리 분배된 관리키들을 가지며 이들을 이용하여 다른 센서들과의 통신키를 생성한다. 여기서, 미리 분배받은 관리키들은 이후에 변경되지 않고 네트워크가 소멸될 때까지 이용된다[1~6]. 또한, 이 관리키들은 여러 다른 센서들 내에도 미리 정해진 확률에 따라 존재한다. 그러므로, 이 방법들은 오염된 노드수가 증가하면 네트워크의 보안성이 심각하게 저하된다.

또 다른 기존의 갱신기법은 반응적인 갱신 기법이다. 이 기법은 오염된 센서들이 발견될 때 마다 오염된 센서들에게 알려진 키들을 갱신한다[7~11]. 클러스터 기반의 센서 네트워크에서 키 관리 임무는 싱크로부터 지역 키 관리자인 클러스터 헤드(Cluster Head: CH)들에게 위임된다. 이때, 싱크는 오염된 CH들을 탐지할 수 있는 능력을 지닌다. 만일 CH가 오염되면, 오염된 CH의 지배하에 있던 센서들을 순수한 CH들에게 재배치한다. CH들은 자신들의 영역 내에서 키 갱신을 위하여 이용되는 관리키들을 센서들에게 분배하고 갱신한다. CH들은 자신들의 영역 내에서 오염된 센서들을 탐지할 수 있는 능력을 지닌다. 만일, CH들이 그들의 영역 내에서 오염된 센서들을 발견하면, 그들의 활동을 억제하기 위하여 그들이 알고 있는 관리키들을 먼저 갱신한다. 이후에 CH들은 갱신된 관리키들을 이용하여 그 클러스터 내에서 이용되는 그룹키를 갱신한다. 이 방법은 임의의 클러스터내의 통신에 사용되는 그룹키가 하나뿐이므로, 단일 센서의 오염에도 그 그룹키가 노출된다. 또 다른 문제점은 관리키들의 갱신을 통한 소극적인 오염노드 퇴출방법이다. 단일 클러스터 내에서 이용되는 관리키의 수는 오히려 무갱신 기법보다 훨씬 적다. 따라서, 오염노드의 수가 증가하면, 관리키들의 갱신을 통한 오염노드들의 퇴출은 아무 효과를 발휘하지 못한다. 물론, 반응적인 갱신기법들은 타이머를 이용하여 선행적으로 수행될 수도 있다. 그러나, 반응적 기법들의 선행적 수행은 많은 통신 및 연산 오버헤드를 유발한다.

본 논문에서 우리는 이러한 오버헤드를 줄이면서도 선행적으로 키 갱신을 수행하는 방법을 제안한다. 제안하는 방법에서, 각 센서는 배치후에 이웃센서들과 개별키들을 설정한다. 개별키들은 링크마다 다른 키들을 의미한다. 이 키들은 나중에 CH와 멤버들간의 통신을 지원한다. 이후에, 두 가지 키 갱신, 즉 CH-센서 키 갱신과 싱크-CH키 갱신, 이 수행된다. 먼저, 첫번째 키 갱신은 네트워크의 클러스터 구조를 바꾸는 것에 의해 수행된다. 이는 클러스터 구조의 변경으로 인해 이전과 다른 CH-센서 키들이 이용됨을 의미한다. 두 번째 키 갱신은 새로 선출된 CH들이 변경된 멤버들을 싱크에게 알리는 것에 의해 수행된다. 이를 통해 새로 선출된 CH들은 싱크와 새로운 싱크-CH키를 공유한다.

본 논문의 나머지는 다음과 같이 조직된다. Ⅱ장에서는 기존의 키갱신 기법들을 간략히 살펴본다. Ⅲ장에서는 본 논문에서 가정된 네트워크와 위협모델을 기술하고 Ⅳ장은 제안방법을 자세히 기술한다. Ⅴ장에서는 실험결과를 제공한다. 마지막으로, Ⅵ장에서 우리는 논문의 결론을 내린다.

Ⅱ. 관련 연구

Eschenauer와 Gilgor는 최초로 키 선분배를 이용한 이웃 센서들 간의 통신키설정을 제안하였다[1]. 이 방법에서, 임의의 두 이웃 센서는 두 센서사이에 공유된 선분배 키들을 이용하여 통신 키를 설정한다. 이 방법은 두 센서 사이에 공유된 선분배 키들의 수가 1인 경우에도 통신 키설정이 가능하므로, 센서들의 오염에 매우 취약하다. Chan등은 통신키 설정을 위해 요구되는 선분배 키들의 최소갯수를 $q(>1)$개로 한정함으로써 이 문제를 해결하였다[2]. Du등은 오염된 센서들의 수가 임의의 임계치를 넘지 않으면, 오염된 센서들이 순수한 센서들의 키를 획득하지 못하도록 하는 방법을 제안하였다[3]. Du등은 또한 각 센서에게 미리 분배되는 키들의 수를 줄이기 위해 노드들의 배치정보를 이용하는 방법을 제안하였다[4]. 이 방법에서 인접하는 영역에 배치되는 센서들은 많은 키들을 공유하므로 임의의 센서내에 존재하는 키들의 수가 작다하더라도, 이웃 센서들과의 통신 키 설정을 쉽게 할수있다. Liu등은 그룹별로 임무현장에 배치되는 센서들의 통신키 설정 방법을 제안하였다[5]. 이 방법에서, 동일 그룹에 속하는 센서들은 많은 선분배 키들을 공유한다. 만일, 임의의 두 인접센서들이 동일 그룹에 속하지 않는 경우에 그들은 두 그룹간의 간접키 설정을 지원하는 키 설정 게이트웨이로 동작한다.

Oliveira등은 클러스터 기반의 센서 네트워크에서 키 선분배 방법을 이용한 LEACH 프로토콜[12]의 보안 확장을 제공하였다[6]. 이 방법에서 공유된 선분배키를 가지지 않는 외부 공격자는 CH나 멤버로 위장을 할 수 없으므로, 이 방법은 네트워크를 외부 공격자들로부터 보호한다. 그러나, 이 방법은 내부의 오염된 노드로부터 발생되는 위협에는 대처할 수 없다. 더구나 오염된 노드들의 수가 증가하면 다른 방법들처럼 네트워크가 공격자의 수중에 놓이게 된다.

최근에는 노드오염에 대한 반작용으로 오염노드들에게 알려진 키들을 갱신하는 반응적 갱신 기법들이 떠오르고 있다. Eltoweissy등은 임의의 통신 그룹내에서 사용되는 그룹키를 오염된 노드들로부터 보호하기 위한 EBS(Exclusion Basis System)를 제안하였다[11]. 임의의 EBS에서 키 분배 서버는 각 멤버들에게 $k+m$개의 키들 중에서 k개씩의 관리키들을 분배한다. 만일, 임의의 노드가 오염이 되면, 키 분배 서버는 그 노드가 알지 못하는 m개의 관리키들을 이용하여 오염된 k개의 관리키들을 갱신한다. 또한 Eltoweissy는 이 EBS를 무선 센서 네트워크에 적용시킨 방법을 제공하였다[9]. 이 방법에서 센서들은 먼저 기지국에서 방송되는 위치정보를 통해 자신이 속할 클러스터를 결정한다. 각 클러스터는 자신만의 그룹키를 유지하며, 이 그룹키들을 갱신하기 위해 EBS가 전체 네트워크에 적용된다. Jolly등은 센서 네트워크에서 EBS에 의존하지 않는 키 갱신기법을 제공하였다[7]. 싱크는 센서-게이트웨이 (CH)키들을 미리 생성하여 게이트웨이들과 센서들에게 미리 분배한다. 이때, 싱크는 센서-싱크 키 및 게이트웨이-싱크 키를 함께 분배한다. 각 게이트웨이는 자신의 영역내에 속한 센서들 중에서 보유하지 않은 센서-게이트웨이키들을 이웃 게이트웨이들 과의 통신을 통해서 확보한다. 이 방법은 센서들이 보유해야 할 키들의 수를 크게 감소시키는 (단지 2개만 필요) 반면에 통신 오버헤드가 크다. 이는 키 갱신이 클러스터들의 재조직 및 센서-게이트 웨이 키들의 재분배를 유발하기 때문이다.

EBS를 이용한 키 갱신기법은 인접노드들 간의 협력 공격에 매우 취약하다. Younis등은 센서들의 위치에 기반한 관리키 분배를 수행하는 SHELL (Scalable, Hierarchical, Efficient, Location-aware, and Lightweight)기법[10]을 제안하였다. SHELL은 인접한 센서들이 많은 관리키들을 상호간에 공유하도록 함으로써, 인접센서들을 오염시킴으로써 얻는 공격자들의 이들을 최소화 하였다. Eltoweissy등은 SHELL을 확장한 LOCK (LOcalized Combinatorial Keying)을 제안하였다[8]. LOCK은 센서들과 CH간의 키 갱신에는 물론 CH들과 싱크와의 키 갱신에도 EBS를 적용한다.

Panja등은 임의의 클러스터에 소속된 모든센서들이 그 클러스터내에서 이용되는 그룹키를 생성하는데 공헌하는 그룹키 생성방법을 제안하였다[13]. 모든 센서 들로부터의 부분키가 모아지면 CH는 그들을 이용하여 그룹키를 생성하고 그 키를 센서들에게 방송한다. 만일 특정 노드의 오염이 감지되면, CH는 그 오염된 센서를 통신 그룹에서 제외하기 위한 메시지를 방송한다. 이 메시지에는 그 오염노드의 부분키를 그룹키로부터 제거하거나 임의의 다른 멤버의 부분키를 추가하라는 명령이 담겨져 있다. Landstra는 그룹키 생성에 참여하는 센서들의 부분키들의 수를 제한하는 것에 의해 Panja의 방법을 개선시켰다[14]. 즉, 이 방법에서는 미리 그룹키 생성 및 갱신에 필요한 부분키의 수가 정해져 있다. 이 정해진 수에 따라 그룹키 생성에 참여할 부분 클러스터들이 선택된다. 이후에, 선택된 부분 클러스터에 포함된 센서들만 그룹키 생성에 참여한다. 따라서 이 방법은 그룹키 생성 및 갱신에 소요되는 지연시간과 소모되는 에너지를 크게 감소시킨다.

III. 네트워크 및 위협 모델

1. 네트워크 모델

본 논문에서의 네트워크는 하나의 싱크와 몇몇의 CH들, 그리고 CH들의 지배하에 있는 센서들로 구성된다. 센서들은 모두 준고정 상태이며 모두 CH의 역할을 수행할 수 있다. 일반센서는 오직 하나의 CH에만 속하며 자신이 감지한 정보를 CH노드에게 전송한다. CH센서는 일반센서로부터 수신한 정보를 집약하며 집약된 데이터를 싱크에게 전송한다. 네트워크의 수명을 증가시

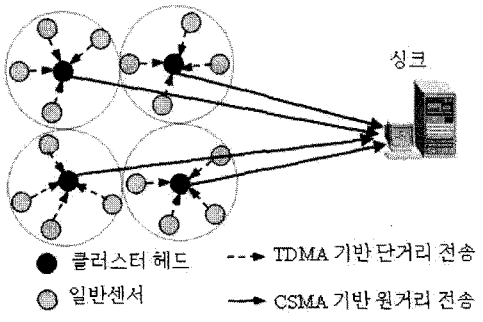


그림 1. 클러스터 기반 센서 네트워크 모델
Fig. 1. Network model of clustered sensor networks.

키기 위해, 각 일반센서는 자신에게 허용된 시간에만 데이터를 전송하고 나머지 시간에는 sleep상태로 존재한다. 이를 위해 각 CH는 자신의 역할을 확정한 후에 멤버들을 위한 TDMA (Time Division Multiple Access) 스케쥴을 방송하고, 센서들은 CH에게 직접 데이터를 전송한다. 싱크는 많은 양의 가용자원을 보유하고 있으며, 안전한 곳에 위치하여 공격들에 대해 자유롭다. 반면에, CH와 일반센서들은 가용자원이 빈약하고 언제든지 공격자들에 의해 포획될 수 있다. 그림 1은 클러스터 구조를 가진 센서 네트워크에서의 통신구조를 보여준다.

2. 위협모델

본 논문에서 가정하는 공격자들의 목표는 2가지 이다. 먼저, 센서들로부터 싱크로 전달되는 데이터들을 모두 불법으로 획득하는 것이다. 두번째, 센서들로부터 싱크로 전달되는 데이터중에서 많은 양의 데이터를 오염시켜서 그릇된 의사결정을 하도록 만드는 것이다. 이러한 목표를 달성하기 위해 공격자들은 물리적으로 취약한 센서노드들을 포획할 필요가 있다. 이때 포획노드들 사이에서 획득한 정보들을 교환하고 공격자에게 전달하는 손쉽고 빠른 방법이 존재한다고 가정한다. 또한, 본 논문에서의 공격자들은 랜덤하게 포획타깃을 정한다고 가정한다.

본 논문에서, 우리는 오염노드들과 순수노드들이 혼재하는 상황에서 통신에 이용되는 키들의 주기적인 변경을 통해 공격자들의 불법 데이터 획득 및 변경을 최소화하고자 한다. 다시 말해서, 우리의 키 변경 방법의 목표는 오염노드들이 상호간에 획득된 키들을 교환하고 공유한다고 하여도 전체 네트워크의 키들을 확보하기 어렵게 만드는 것이다.

Ⅳ. 클러스터 구조 변경을 통한 주기적인 키 갱신

제안된 방법의 기술을 위해, 우리는 다음과 같은 가정을 한다.

- 각 센서는 네트워크 배치 이전에 미리 정해진 수만큼의 관리키들과 네트워크 전역 키를 분배 받는다. 네트워크에 배치된 후에 각 센서는 미리 분배된 키들을 XOR연산하여 센서 키를 생성한다. 이 센서 키는 CH와 싱크간의 키 일치를 위해 사용된다. 이후부터는 CH와 싱크간의 키를 클러스터 키라 부르기로 한다.
- 싱크와 센서들의 클록은 초기에 동기화되어 있다. 동기화된 타이머가 만료된 후에, 싱크는 자신의 시간을 센서들에게 방송하는 것에 의해 이러한 시간 동기화를 유지한다.
- 각 센서와 싱크는 오염된 노드들을 감지할 수 있다. 임의의 CH는 자신의 관리하에 있는 센서들의 오염을 감지하며, 싱크는 CH들의 오염을 감지한다. CH는 센서들로부터 수신된 데이터를 싱크에게 전송할 때 오염된 노드들의 리스트를 첨부함으로써 싱크에게 오염된 노드들을 알린다. 싱크는 다음 키 갱신 주기 시작시간에 자신의 시간과 함께 새로 오염된 노드들의 리스트를 방송한다.

제안방법은 이웃노드간 개별키 설정, 클러스터 갱신, 클러스터키 갱신, 그리고 싱크의 동기화 및 오염노드 보고의 4단계로 구성된다. 개별키 설정은 센서배치 후에 네트워크 구성시간에만 한번 수행된다. 반면에 나머지 세과정은 네트워크가 살아있는 동안에 주기적으로 수행된다. 그림 2는 제안방법의 구성요소와 절차를 보여준다. 다음 절은 네트워크 배치 후에 센서 노드들간의 개별 키 설정을 기술한다. Ⅳ장 2절에서는 클러스터 변경을 통한 오염노드 퇴출 및 센서-CH간 키 갱신 방법이 기술된다. Ⅳ장 3절은 CH-싱크간의 클러스터키 일치 방법을 다룬다. 마지막으로, Ⅳ장 4절에서는 싱크의 동기화 및 오염노드 보고 방법이 기술된다.

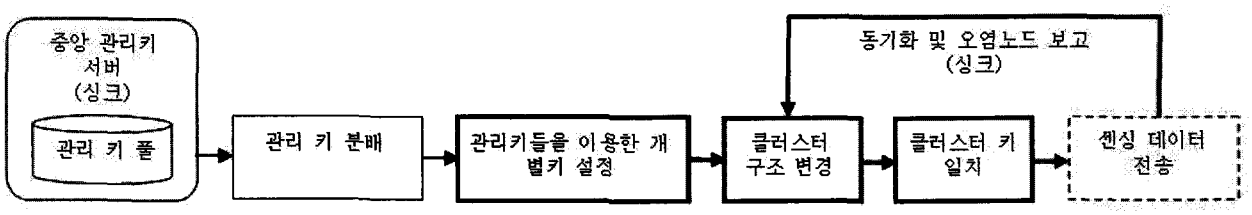


그림 2. 클러스터 구조 변경을 통한 키 갱신 절차
Fig. 2. Key renewal procedures using cluster reformations.

1. 개별키 설정

우리의 방법은 임의의 CH와 멤버들간의 통신키 갱신을 위해서 클러스터 내의 키들을 바꾸지 않고 클러스터 구성원을 바꾸는 방법을 이용한다. 이를 가능하게 하기 위해서는 모든 이웃 센서들간에 공유된 키들이 미리 존재하여야 한다. 따라서, 센서들은 네트워크 구성 시간에 이웃 센서들과 개별키 설정을 한번만 수행한다. 이웃 센서들과 개별키 설정은 키 선분배 방법 [1]과 ID기반의 방법 [15]을 혼용한다. 즉, 임의의 센서는 공통의 분배 키들을 가진 이웃 센서들과 그 공통의 키들을 이용하여 개별 키를 설정한다 [1]. 반면에, 임의의 센서가 공통의 분배키가 없는 이웃 센서를 발견하면, 네트워크 전역키와 센서들의 ID를 이용하여 개별 키를 설정한다 [15]. 그림 3은 임의의 두 이웃 센서간에 공유된 키가 없을 경우에 두 노드 사이에 네트워크 전역키 및 ID를 이용한 개별 키 설정 과정을 보여준다. 다음은 그림 3에서 사용되는 표기법들이다.

- K_I : 네트워크 전역 키
- F_K : 키 K를 이용하는 의사 랜덤 함수
- $MAC(K,M)$: 키 K를 사용한 메시지 M의 메시지 인증 코드
- n_A : 노드 A에 의해 생성된 난수
- K_A : 노드 A의 마스터 키
- K_{AB} : 노드 A와 B의 비중첩 키
-

그림 3에서, 노드 u와 v는 각각 난수값과 ID를 담고 있는 Hello 메시지를 방송한다. 각 노드는 ID가 더 큰 노드로부터의 Hello메시지는 무시한다. 노드 v는 노드 u의 ID가 자신의 것보다 작으므로, 네트워크 전역키를 이용하여 자신의 마스터 키(K_u)를 생성하고 이 키와 노드 u의 식별자를 이용하여 통신 키를 생성한다(K_{uv}). 이후에 노드 v는 K_v를 이용하여 노드 u의 난수에 대한 응답을 전송한다. 응답을 수신할 때, 노드 u는 노드 v의 마스터 키(K_v)를 생성하고, 노드 v의 응답을 검증한 후에 노드 2와의 통신 키(K_{uv})를 생성한다. 이웃 센서들과 통신 키들을 설정한 후에, 각 센서는 센서의 저장공간을 절약함은 물론 미리 분배된 키들의 노출로 인한 위험을 방지하기 위해서 미리 분배된 키들을 삭제한다.

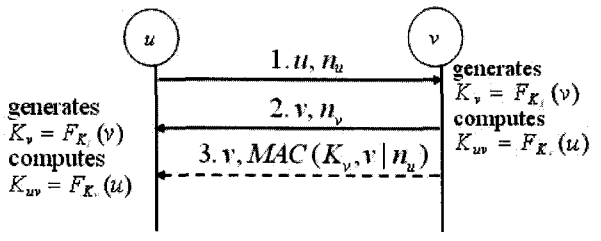


그림 3. 공통 관리키가 없는 경우의 개별키 설정
Fig. 3. Distinct key establishment in case of sharing no common keys.

2. 클러스터 구조 변경

제안방법은 CH역할을 수행하는 노드들을 주기적으로 변경한다. 이러한 변경은 다음의 두 가지 이유에서 기인한다. 먼저, 만일 CH역할을 수행하는 노드가 오염되면, 그 클러스터내의 센서로부터 전송된 데이터는 모두 오염이 된다. 따라서, 네트워크의 안전성을 향상시키기 위해서는 CH역할을 수행하는 노드들이 자주 변경될 필요가 있다. 두 번째, CH역할을 수행하는 노드들은 장거리 전송을 수행하므로, 일반 센서에 비해 많은 양의 에너지를 소모한다. 따라서 가장 많은 에너지를 가진 노드가 CH역할을 수행해야 한다.

클러스터 변경 도중에, 오염된 노드들은 계속해서 센서들의 데이터를 엿듣거나 위조하기 위하여 자신이 CH임을 선언할 수 있다. 이러한 경우의 센싱된 데이터의 기밀성은 물론 무결성이 크게 훼손된다. 따라서, 제안된 방법을 포함하는 모든 키 갱신 기법은 오염노드들을 식별할 수 있는 성숙한 침입탐지시스템이 필요하다 이러한 침입탐지 시스템의 설계는 다른 문헌들[16~17]에서 다루고 있으며 본 논문의 범위를 벗어나므로 본 논문에서 다루지 않는다. 매 키 갱신 시작시간에 각 센서들은 싱크의 방송을 통해 오염된 노드들을 알게 되며, 이들과의 통신을 거부함으로써 이들을 네트워크에서 퇴출시킨다. 즉, 각 센서들은 오염노드들로부터 수신된 메시지를 즉각 폐기한다.

클러스터 구조의 변경은 이웃노드들과 에너지 잔량

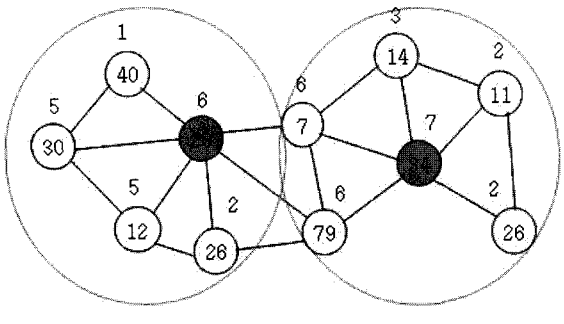


그림 4. 클러스터 구조 변경 예제
Fig. 4. An example of cluster reformation.

을 비교해서 에너지 잔량이 가장 많은 노드가 CH가 되는 방식으로 진행된다. 만일, 에너지 잔량이 동일할 경우에는 ID가 낮은 노드가 우선순위를 가진다. 그리고 만일 임의의 노드가 둘 이상의 노드로부터 클러스터 가입요구를 받게 되면, 먼저 메시지를 전송한 CH에게 가입한다. 그림 4는 클러스터 구조 변경에 대한 예제를 보여준다. 그림 4에서, 각 노드 위에 쓰인 숫자는 임의의 클러스터 구조 변경시점에 각 노드의 에너지 잔량을 의미한다. 그림 4에서 노드 34는 모든 노드들 중에서 가장 에너지 잔량이 높으므로, CH로 선출되고 그 사실을 CH선언 메시지를 통해 방송한다. 방송메시지를 직접 청취하는 노드 7, 11, 14, 26, 그리고 79는 CH 34의 그룹에 가입한다. 이 가입메시지 또한 이웃 노드들에게 방송된다. 이제 노드 29는 CH가 될 자격이 생긴다. 왜냐하면 우선순위를 가진 노드 7이 CH 34의 그룹에 가입했기 때문이다. 노드 29는 CH선언 메시지를 방송하고 노드 12, 26, 30, 그리고 40은 CH 29의 그룹에 가입한다. 하지만 노드 7과 79는 이미 34의 그룹에 가입했으므로, CH 29의 메시지를 무시한다.

클러스터 구조 변경이 완료되면, 두 가지 변화가 발생한다. 먼저, 새로운 노드들이 CH 역할을 수행하게 된다. 두 번째, 새로운 CH들의 선출로 인해, 클러스터들 내에서 이용되는 센서-CH키들이 변경된다. 즉, 만일 임의의 새로운 CH가 선출되면, 그 CH와 멤버 센서들간에는 새로운 링크들이 사용된다. 이때, 그 링크들이 이미 개별키들을 가진다는 것을 기억해야 한다. 따라서 멤버들과 그 CH사이의 링크들은 이미 생성된 개별키들에 의해 보호된다.

3. 클러스터 키 일치

임의의 노드가 CH로 선정되면, 그 CH는 싱크와 클러스터 키를 일치시킨다. 먼저, 각 CH는 자신의 센서키와 멤버노드들 과의 개별 키들을 XOR연산하는 것에 의해 싱크와의 클러스터 키를 생성한다. 이후에 각 CH는 자신과 멤버들의 ID들을 싱크에게 알린다. 싱크는 각 센서에게 분배되었던 키들을 이미 알고 있으므로, 임의의 CH의 센서 키와 그 CH가 멤버들과 설정했던 개별키들을 바로 생성할 수 있다. 그 후에, 싱크는 그 CH가 클러스터 키를 생성하는 것과 같은 방법을 통해 그 CH와 같은 클러스터 키를 생성한다. 클러스터 키 일치가 완료되면, 각 CH는 자신의 멤버들을 위한 TDMA 스케쥴을 생성하여 방송한다. 각 센서들은 이 스케쥴을 통해 자신이 전송할 시간과 쉬게 될 시간을 계산하게 된다.

표 1. 실험파라미터
Table 1. Simulation parameters.

파라미터	값
실험시간	3600 초
초기 에너지	10 Joules/battery
대역폭	1 Mbps
데이터 패킷 크기	500 bytes
패킷 헤더 크기	25 bytes
오염된 노드수 (CH수)	10~50(2~4: SHELL)
오염된 시간 분포	무작위, 0~900 초
클러스터의 수	5(SHELL)
EBS[21] 파라미터(k+m)	7+3(SHELL)
키 갱신 주기	20 초(SHELL)
클러스터 반경	30 meter(제안방법)
타이머 만료시간	60, 120, 180 초

센서들은 자신에게 할당된 시간에 센싱된 데이터들을 그들의 CH에게 전송하며, 그 CH들은 집약된 데이터를 싱크에게 전송한다. 이때 CH들은 자신의 CH내에서 새로 식별한 오염노드들을 집약데이터에 포함시킨다. 이를 통해, 싱크는 네트워크 내에 존재하는 모든 오염노드들을 파악하게 된다. 이 과정은 클러스터 구조변경과정에서 설정된 타이머가 만료될 때까지 반복된다.

4. 오염노드 보고 및 동기화

싱크는 초기에 설정된 타이머가 만료되면, 알려진 모든 오염노드들과 자신의 시간을 모든 센서 노드들에게 방송메시지를 통해 알린다. 이후에 싱크는 자신의 타이머를 다시 설정한다. 이 메시지를 수신하는 센서들은 모든 현재의 작업을 중단하고, 타이머를 재설정하며, Ⅳ장 2절의 클러스터 구조 변경을 수행한다.

V. 실험 결과

우리는 제안방법의 안전성과 에너지 효율성을 평가하기 위해 ns-2 시뮬레이터(버전 2.27)를 이용하여 실험환경을 구축하였다. 실험환경에서 100개의 노드들은 (100m., 100m.)의 영역내에서 랜덤하게 배치되며, 싱크는 (50m., 175m.)에 위치한다. 실험에서 이용된 에너지 소비 모델은 참고문헌[12]의 것들을 차용한다. 실험동안 우리는 각 방법을 오염노드수의 변화에 따라 30번씩 실

행하였으며, 그 결과를 통계적으로 수치화 하였다. 표 1은 실험에 사용된 파라미터들과 그 값들을 보여준다. EBS 파라미터에서 $k+m$은 각 CH가 가지는 키링의 크기이며, k는 각 멤버센서가 가지는 키링의 크기이다.

우리는 제안방법을 무갱신 기법 및 반응형 키 갱신 기법과 비교한다. 우리는 무갱신 기법의 대표로써 Chan의 기법[2]을 그리고 반응적 키갱신 기법의 대표로써 SHELL[12]을 선정하였다.

Chan의 기법에서, 라우팅은 MTE(Minimum Transmission Energy)라우팅[18]을 사용한다. 만일, 임의의 노드가 공유키를 가진 다음 홉 노드를 찾을 수 없는 경우에는 싱크에게 직접 자신이 수신한 데이터를 전송한다. 이때, 암호화에 사용되는 키는 자신이 분배받은 모든 관리키들을 XOR연산한 값이다.

SHELL은 클러스터 내에서 멀티 홉 통신을 수행함으로써, 클러스터 내에서 TMDA통신이 불가능 할 뿐만 아니라 자연적으로 오염노드들의 공모에 의한 공격에 취약한 문제점을 보인다. 따라서, 우리는 클러스터 내의 통신이 단일 홉이 되도록 SHELL의 동작을 수정하였다. 또한, 우리는 에너지 및 통신 효율성을 증가시키기 위해 SHELL에서 오염노드 탐지 및 키 갱신이 일정주기(즉, 20초)에 의해 수행되도록 수정하였다. 우리는 다음과 같은 메트릭들을 고려하였다.

- 데이터의 노출 비율 : 센서들로부터 전송된 데이터가 오염된 노드들에게 노출되는 비율. 이는 키 갱신기법의 기밀성을 측정하기 위한 메트릭이다.
- 데이터의 오염 비율 : 싱크에 의해 수신된 데이터 중에서 공격자들에 의해 변경된 데이터의 비율. 이는 키 갱신기법의 무결성을 측정하기 위한 메트릭이다.
- 에너지 소모 비율 : 전체 에너지 소모에서 키 갱신 부분이 차지하는 비율. 이는 키 갱신기법의 에너지 효율성을 측정하기위한 메트릭이다.

1 보안성 분석

그림 5에서 보는 것 처럼, SHELL은 작은 수의 오염노드에서 (< 40) 데이터 노출비율을 완화시키지만 오염노드 수가 더 증가하면 Chan의 방법과 유사한 비율을 보여준다. SHELL은 클러스터 내에서 단일 그룹키를 사용하기 때문에 하나의 센서만 오염되어도 그 오염된 센서의 수신범위 내에서 이루어지는 통신은 즉각 노출된다. 오염된 노드수가 증가할수록 노출되는 데이터는 더 많아지게 된다. 특히, 오염 CH들의 수가 4가 되면 Chan의 방법보다 더 많은 데이터를 노출시킨다.

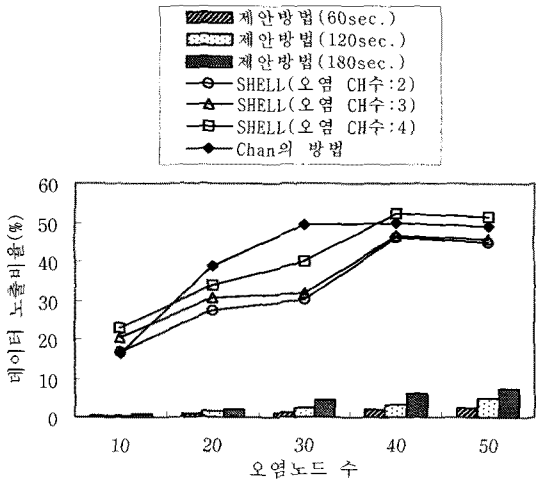


그림 5. 데이터 노출 비율 vs. 오염노드 수
Fig. 5. Data exposure rate vs. the number of compromised nodes.

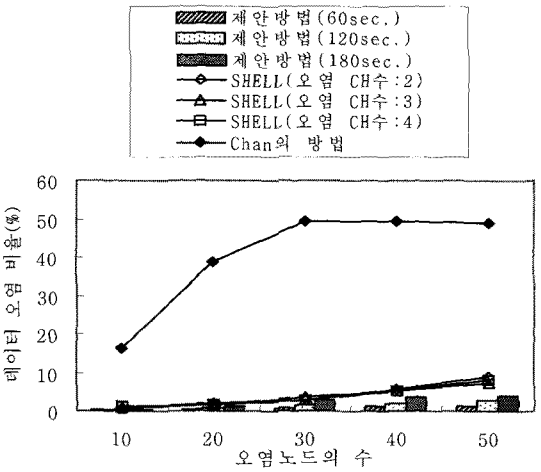


그림 6. 데이터 오염 비율 vs. 오염노드 수
Fig. 6. Data exposure rate vs. the number of compromised nodes.

SHELL에서 오염된 CH(들)가 발견되면, 오염된 CH에 속했던 센서들은 순수한 CH들에게 재배치된다. 이는 임의의 클러스터에 소속된 센서들의 밀집도를 증가시킨다. 따라서, 그 클러스터 내에 존재하는 오염된 노드들은 더 많은 센서들의 데이터를 불법적으로 획득할 수 있다.

제안방법은 임의의 클러스터 내에서 각 센서가 개별적인 키를 사용해서 CH에게 데이터를 전송하므로, 센서들의 오염에 훨씬 둔감하다. 즉, 공격자는 단일 센서의 오염을 통해 다른 센서들의 데이터를 획득할 수 없다. 또한, CH들이 오염된 경우에는, 순수한 센서들 사이에서 새로운 CH를 선출하므로, 클러스터들의 밀집도

가 증가하지 않는다.

그림 6은 오염노드수의 증가에 따른 센서들의 데이터 위조비율을 보여준다. Chan의 방법은 다른 두 방법에 비해 훨씬 많은 데이터 위조비율을 보여준다. 이것은 Chan의 방법에서 센서들의 데이터가 다중 홉을 통해 싱크에게 전송되기 때문이다. 즉, 임의의 소스센서와 싱크사이의 경로상에서 하나의 노드만 오염된다고 하더라도, 소스 센서의 데이터는 오염노드에 의해 위조된다. 이러한 위조비율은 오염노드 수의 증가에 따라 같이 늘어난다.

SHELL은 Chan의 방법에 비해 위조비율을 크게 감소시킨다. 그러나, 오염노드의 수가 증가할수록, 그 위조비율은 대응되게 증가한다. SHELL은 오염노드들에게 알려진 관리 키들을 먼저 갱신하고, 갱신된 관리키들을 이용하여 그룹 키를 갱신한다. 이러한 퇴출방법은 만일 클러스터 내의 관리 키들이 일부만 오염노드들에게 알려지더라도 오염노드들이 갱생하는 문제점을 발생시킨다. 이 경우에, 갱생한 노드들은 계속해서 센서들의 데이터를 위조할 수 있다.

제안방법은 오염된 노드들을 제외한 클러스터 재구성을 통해 오염노드들을 확실히 제거한다. 따라서, 제안방법은 오염노드들이 증가되어도, 데이터 위조비율의 경사를 훨씬 더 부드럽게 만든다.

2 에너지 효율성 분석

그림 7은 오염노드들의 증가에 따른 키 갱신기법들의 에너지 소모율을 보여준다. Chan의 방법에서, 센서들은 이웃 센서들과 개별키 설정이 끝나면, 더 이상 어떠한 키 갱신도 수행하지 않는다. 따라서, 오염노드수의 증가와는 상관없이 거의 일정한 에너지 소모비율을 보인다. 반면에, 다른 두 방법은 오염노드들을 퇴출시키기 때문에, 퇴출되지 않은 노드들만 키 갱신을 위해 에너지를 소모한다. 따라서, 오염노드수가 증가하면, 두 방법의 에너지 소모율은 감소한다.

SHELL은 키 갱신과정에서 에너지를 많이 소모하는3개의 구성요소들을 지닌다. 그들은 "클러스터 구성", "관리키 갱신 및 분배", "관리키를 이용한 그룹키 갱신 및 분배"이다. 많은 에너지소모를 유발하는 이유는 그들이 많은 센서들을 통신과 연산에 참여하도록 만들기 때문이다. SHELL 에서 일반 센서들이 오염된 경우에는 마지막 2단계만 수행하면 된다. 그러나 CH들이 오염된 경우에는 센서들이 먼저 클러스터 구성에 참여해야 하므로, 추가적인 통신 오버헤드가 발생한다. 따라서, 센서들은 오염 CH들의 수가 증가하면, 더 많은 양의 에너지를 소모한다.

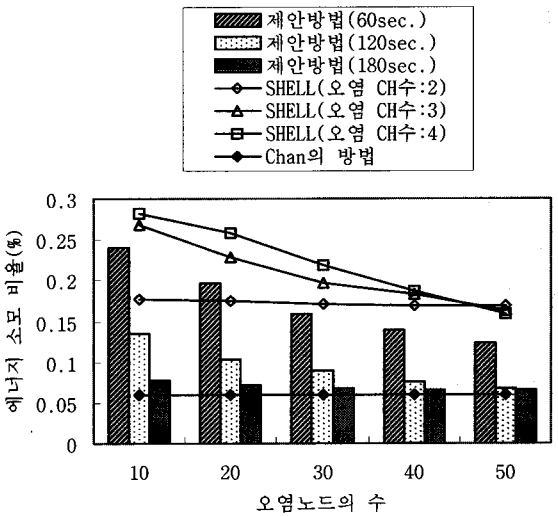


그림 7. 에너지 소모 비율 vs. 오염노드 수
Fig. 7. Energy consumption rate vs. the number of compromised nodes.

제안방법은 4개의 구성요소로 구성되어 있다 개별키 설정, 클러스터 구조변경, 클러스터 키 일치, 오염노드 보고 및 동기화. 그러나 이들 중에서 에너지를 많이 소모하는 구성요소는 클러스터 변경뿐이다. 개별 키 설정은 센서들의 배치 후에 한번만 수행된다. 또한, 클러스터 키 일치는 작은 수의 센서들만 이 과정에 참여시킨다. 마지막으로, 오염노드 보고 및 동기화는 센서들이 하나의 메시지를 수신하는 양의 에너지만 소모하게 만든다. 클러스터 타이머가 180초인 경우에, 제안방법은 작은 수의 오염노드 하에서(<=20) SHELL에 비해 더 많은 양의 에너지를 소모한다. 하지만, 오염노드의 수가 더 많이 증가하면, 제안방법은 에너지 소모를 SHELL에 비해 크게 감소시킨다. 이는 SHELL이 오염노드들을 대부분 생존하게 하는 반면에 제안방법은 이들을 모두 확실히 제거하기 때문이다.

VI. 결론 및 향후 연구

제안하는 클러스터 구조의 변경을 통한 키갱신은 두 가지 효과를 유발한다. 첫째, 클러스터들의 멤버쉽 변화를 유발하며, 따라서 클러스터 내에서 이용되는 센서-CH키들이 변경된다. 각 센서들은 다른 센서들로부터 구분되는 센서-CH키를 사용하므로, 센서들의 데이터 기밀성을 크게 향상시킨다. 또한, 오염된 센서들은 갱신

되는 클러스터 조직에 참여할 수 없게 되므로, 오염노드들의 활동시간을 크게 감소시키고 센서들의 데이터 무결성을 크게 향상시킨다. 실험결과는 제안방법이 오염노드들이 존재하는 가운데에 센싱 데이터의 기밀성 및 무결성을 다른 방법들에 비해 훨씬 더 향상시킴을 보여주었다. 또 다른 실험결과는 그럼에도 불구하고 제안방법이 키설정을 위해 소모되는 에너지를 감소시킴을 보여주었다.

향후연구는 기존의 센서들을 대체하기 위해 투입되는 센서들과 기존의 센서들 간의 안전한 pairwise키 설정을 지원하도록 제안하는 방법을 개선하는 것이다.

참 고 문 헌

[1] L. Eschenauer and V. D. Gilgor, "A Key Management Scheme for Distributed Sensor Networks," in Proc. 9th ACM Conf. Comp. and Comm. Sec., Nov. 2002, pp. 41-47

[2] H. Chan, A. Perrig, and D. Song, "Random Key Predistribution Schemes for Distributed Sensor Networks," in Proc. IEEE Symp. Security and Privacy, May. 2003.

[3] 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 Proc. IEEE Infocom '04, Mar. 2004.

[4] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A Pairwise Key Predistributino Scheme for Wireless Sensor Networks," in Proc. 10th ACM Conf. Computer and Communication Security (CCS '03), Oct. 2003.

[5] D. Liu, P. Ning, and W. Du, "Group-Based Key Pre-distribution in Wireless Sensor Networks," in Proc. 2005 ACM Wksp. Wireless Security (WiSe 2005), pp. 11-20, Sep. 2005.

[6] L. B. Oliveira, H. C. Wong, M. Bern, R. Dahab, and A. A. F. Loureiro, "SecLEACH - A Random Key Distribution Solution for Securing Clustered Sensor Networks," in Proc. of 5th IEEE Int'l Symp. Network Computing and Applications (NCA '06), pp. 145-154, May 2007.

[7] G. Jolly, M. C. Kuscu, P. Kokate, and M. Younis, "A Low-Energy Key Management Protocol for Wireless Sensor Networks," in Proc. IEEE Int'l Symp. Comp. and Comm. (ISCC '03), pp. 335-340, Jun. 2003.

[8] M. Eltoweissy, M. Moharrum, and R. Mukkamala, "Dynamic Key Management in Sensor Networks," *IEEE Communications Magazine*, vol. 44, issue 4, pp. 122-130, Apr. 2006.

[9] M. Eltoweissy, A. Wadaa, S. Olariu, and L. Wilson, "Group Key Management Scheme for Large-Scale Sensor Networks," *Ad Hoc Networks*, vol. 3, issue 5, pp. 668-688, Sep. 2005.

[10] M. Younis, K. Ghumman, and M. Eltoweissy, "Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks," *IEEE Tans. Parallel and Distributed Systems*, vol. 17, no. 8, pp. 865-882, Aug. 2006.

[11] M. Eltoweissy, M. H. Heydari, L. Morales, and I. H. Sudborough, "Combinatorial Optimization of Group Key Management," *J. Network and Systems Management*, vol. 12, no. 1, pp. 33-50, Mar. 2004.

[12] W. Heinzelman, A. P. Chandrakasan, H. Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," *IEEE Trans Wireless Communications*, vol. 1, no. 4, pp. 660-670, Oct. 2002.

[13] B. Panja, S. Madria, and B. Bhargava, "Energy and Comminication Efficient Group Key Management Protocol for Hierarchical Sensor Network," in Proc. IEEE Int'l Conf. Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC'06), pp. 384-393, Jun. 2006.

[14] T. Landstra, M. Zawodniok, S. Jagannathan, "Energy-Efficient Hybrid Key Management Protocol for Wireless Sensor Networks," in Proc. 32nd IEEE Conf. Local Computer Networks, pp. 1009-1016, Oct. 2007.

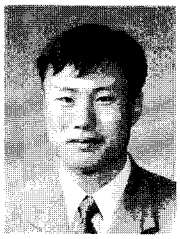
[15] G. Wang and G. Cho, "Pairwise Key Establishments without Key Pre-distribution for Mobile Ad hoc Network Environment," *IEE Proceedings-Communications*, vol. 153, no. 6, pp. 822-827, Dec. 2006.

[16] V. Bhuse and A. Gupta, "Anomaly Intrusion Detection in Wireless Sensor Networks," *J. High Speed Networks*, vol. 15, issue 1, Jan.-Mar. 2006.

[17] K. Ioannis, T. Dimitriou, and F. C. Freiling, "Towards Intrusion Detection in Wireless Sensor Networks," in Proc. 13th European Wireless Conf., Paris, Apr. 2007.

[18] M. Ettus, "System Capacity, Latency, and Power Consumption in Multihop-routed SS-CDMA Wireless Networks," in Proc. Radio and Wireless Conf. (RAWCON), Colorado Springs, Aug. 1998, pp. 55-58

저 자 소 개



왕 기 철(정회원)

1997년 광주대학교 전자계산학과 학사 졸업
2000년 목포대학교 전산통계학과 석사 졸업
2005년 전북대학교 컴퓨터 통계정보 학과 박사 졸업
2006년 1월~2007년 12월 전북대학교 Post-doc 연구원
2008년 1월~2008년 12월 전남대학교 Post-doc 연구원
2009년 1월~현재 한국과학기술정보연구원 선임연구원

<주관심분야 : Ad hoc 네트워크, 센서 네트워크, 무선네트워크 보안, 이동 컴퓨팅>

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 교수

<주관심분야 : 이동컴퓨팅, 컴퓨터통신, 무선네트워크 보안, 센서네트워크, 분산처리시스템>