감시정찰 센서네트워크 및 주요 시설물 관리에서의 키 관리 기법 비교 *

김장성† , 권미영‡ , 김이형‡ , 곽민혜† , 한규석† , 김광조†

† 한국정보통신대학교 암호화 정보보호 연구실

‡ 국방과학연구소

Comparison among key management schemes over wireless sensor network for surveillance reconnaissance and critical infrastructure monitoring application

Jangseong Kim, Miyoung Kwon, Leehyung Kim, Minhea Kwak, Kyusuk Han and Kwangjo Kim
Cryptography And Information Security Lab in Information and Communications University

요 약

무선 센서네트워크는 유비쿼터스 환경 구축을 위한 기반기술로 각광받고 있으나 센서네트워크를 구성하는 센서 노드의 본질적인 특성으로 인해 다양한 보안 취약점을 내포하고 있다. 키 관리 기법은 센서네트워크에서 비밀 통신을 지원하기 위해 반드시 필요하기 때문에, 안전한 센서네트워크를 구축하기 위해서는 무엇보다도 키 관리가 주요하다. 본 논문에서는 다양한 응용분야 중에서도 주요 시설물 및 감시정찰을 위해 활용되기 위한 센서네트워크의 보안 요구사항을 살펴본 다음, 기존에 제안된 키 관리 기법들의 장·단점을 분석하고자 한다.

Ⅰ. 서 론

오늘날 무선 센서네트워크는 유비쿼터스 환경을 구축하기 위한 기반기술로 각광을 받고 있으나, 연산 능력, 저장 공간, 배터리 측면에서 제한된 리소스를 가진 센서 노드들로 구성되기 때문에 일반적인 네트워크에 비해 상대적으로 많은 보안 취약점(DoS 공격, Sinkhole / Wormhole / Sybil 공격, 탈취된 노드를 통한 키 정보 획득, 메시지 위·변조, 트래픽 분석 등)을 내포하고 있다 [1,2]. 따라서 무선 센서네트워크를 실생활에 응용하기 위해서는 이러한 보안 취약점을 제거 혹은 보완하기 위한 보안 프레임워크가 필요하며, 보안 프레임워크는 크게 키 관리, 안전한 통신 지원, 노드 탈취 대책과 같은 세부 목표로 구분할 수 있다. 이 중에서 키 관리는

* 본 연구는 국방과학연구소의 민군겸용기술사업(Dual Use Technology Program) 지원으로 수행하였습니다.

DoS 공격과, 탈취된 노드를 통한 키 정보 획득을 제외한 대부분의 공격에 직접적으로 연관되어 있기 때문에 가장 우선적으로 고려되어야 한다.

키 관리는 크게 생성 / 분배, 업데이트, 폐기로 이루어진다. 키 생성 / 분배 단계는 키를 생성해 통신 상대자에게 전송하거나 혹은 동일한 키 생성을 유도하는 단계, 키 업데이트는 기존에 일정시간동안 사용한 키를 업데이트하는 단계, 키 폐기 단계는 더 이상 사용하지 않거나 노출된 키를 폐기하는 단계이다. 이러한 키 설정 단계 중에서 키 업데이트 및 폐기는 키 생성 / 분배 과정에서 베이스 스테이션과 센서 노드 간에 공유된 키를 통해 쉽게 이루어 질 수 있기 때문에 기존에 제안된 키 관리 기법들은 이러한 연구 중에서 키 생성 / 분배 단계에 집중되어 있다.

본 논문은 다음과 같이 구성된다. 2장에서는 감시정찰 및 주요 시설물 관리용 센서네트워크의 보안요구사항을 설명하고, 3장에서는 기존에 제안된 센서네트워크용 키 관리 기법을 노드 배치 이전에 키 분배여부, 마스터 키 사용여부, 베이스 스테이션 참여여부에 따라 구분한 다음 각각의 대표적인 예를 통해 각 방식의 장·단점을 분석한다. 4장에서는 기존에 제안된 키 관리 기법이 감시정찰 및 주요 시설물 관리용 센서네트워크에 적합성 여부를 분석할 예정이다.

Ⅱ. 감시정찰 및 주요 시설물 관리용 센서네트워크 키 관리를 위한 보안요구사항

일반적으로 센서네트워크를 위한 키 관리는 다음과 같은 사항들이 고려되어야 한다 [3]. 첫째, 센서 노드들이 랜덤하게 배치되기 때문에 네트워크 토폴로지 정보를 사전에 획득하기 어렵다. 둘째, 센서 노드는 제한된 리소스를 가지고 있기 때문에 경량화된 암호 알고리즘이 고려되어야 한다. 셋째, 센서 노드들의 오동작, 배터리 방전 등으로 인해 센서 노드를 추가적으로 설치할 수 있어 키 추가 및 제거가 용이해야 한다. 넷째, 센서네트워크는 운용목적에 전장과 같은 적대적인 환경에 배치될 수 있기 때문에 물리적인 접근을 통한 노드탈취가 발생할 수 있다. 다섯째, 확장성이 고려되어야 한다.

그러나 센서네트워크를 감시정찰 및 주요 시설물 관리를 목적으로 활용할 경우 다른 응용분야보다 보안을 더욱 고려해야 한다. 악의적인 공격자는 해당 센서네트워크를 공격해 기밀 정보 획득과 같은 다양한 이득을 얻을 수 있기 때문이다. 따라서 기본적으로 알려진 다양한 공격 방법에 내성을 지니고 있어야 한다. 특히, 공격자는 키 생성 및 분배과정에서의 트래픽 분석 공격을 통해 키 생성 정보 및 네트워크 토폴로지 정보를 손쉽게 획득할 수 있기 때문에 중요 메시지 암호화 및 메시지 송신자에 대한 익명성이 보장되어야 한다.

또한, 감시정찰 및 주요 시설물 관리용 센서네트워크는 운용목적에 따라 적대적인 환경에 배치될 수 있다. 예를 들어, 센서네트워크가 작전지역에 배치될 경우, 악의적인 공격자가 배치된 센서네트워크에 물리적으로 접근할 수 있다. 이 경우 공격자는 해당 노드를 탈취해 노드에 저장된 키 정보, 네트워크 토폴로지, 베이스 스테이션의 위치, 네트워크의 운용목적 등 중요정보를 획득할 수 있으며 [4], 획득된 정보는 센서네트워크 공격에 활용될 수 있다. 따라서 감시정찰 및 주요 시설물 관리용 센서네트워크는 센서 노드가 탈취되더라도 그 영향은 최소화되며, 노드 배치 이후에는 칩 디버깅을 통한 정보 획득이 불가능해야 한다.

더욱이, 모든 센서 노드들은 감시정찰을 위한 응용 프로그램을 운용하기 때문에 배터리 소모가 상대적으로 심하며, 저장 공간에 제약이 발생하기 때문에 감시정찰용 센서네트워크에는 공개키 기반 및 하이브리드 기반의 키 관리 시스템은 부적합하다(공개키 기반의 암호화 알고리즘을 센서네트워크에 탑재에 약 21K byte 저장 공간이 필요하며 [5], 대칭키 기반의 암호화 알고리즘도 약 15K byte가 필요하다 [6]). 그러나 대칭키 기반의 키 관리 시스템은 키를 공유하고 있는 두 개체 중 어느 하나라도 탈취될 경우 공유하고 있는 키가 노출되어 비밀 통신이 불가능해지며, 악의적인 공격자는 탈취된 키를 추가적인 공격(네트워크 토폴로지 변경, 잘못된 이벤트 정보 삽입)에 활용할 수 있다.

그러므로 다른 응용분야용 센서네트워크에서의 키 관리 기법에 비해 보다 안전하면서도 경량화된 키 관리 기법이 필요하다.

Ⅲ. 기존 키 관리 기법

센서네트워크에서 제안된 키 관리 기법들은 노드 배치 이전에 키 분배여부, 마스터 키의 사용여부, 베이스 스테이션의 참여 여부에 따라 사전키 분배 방식, 마스터 키 기반 방식, 베이스 스테이션 기반 방식으로 구분할 수 있다. 본 논문에서는 각 분배방식의 대표적인 예를 통해 각 방식의 장·단점을 분석하고자 한다. 사전키 분배 방식의 대표적인 예로는 2002년에 Eschenauer *et. al*이 제안한 사전키 분배 기법 [7], 마스터 키 기반 방식의 경우 2003년 S. Zhu *et. al.*이 제안한 LEAP [8], 베이스 스테이션 기반 방식의 경우 2007년 J. Ibriq *et. al.*이 제안한 HIKES [3]가 있다.

1. Eschenauer *et. al.* 의 사전키 분배 [7]

사전키 분배는 2002년에 Eschenauer *et. al.* 이 제일 처음 제안하였으며, 이후 노드 탈취에 대한 내성을 개선하기 위해 다양한 기법들 [9-14]이 제안되었으나 본 논문에서는 Eschenauer *et. al.*이 제안한 기법 [7]을 중심으로 설명하고자 한다. 사전키 분배는 초기화, 키 구성, 패스 키 생성 단계로 이루어진다. 초기화 단계는 센서네트워크 전체에서 사용할 하나의 키 풀에서 m개의 키를 선택해 각각의 노드에 저장한다. 키 구성 단계는 인접 노드들 간에 공유하고 있는 키 비교와 키 소지여부를 확인한다. 공유하고 있는 키 비교는 모든 노드들의 배치 이후에 각 노드가 가지고 있는 키에 대한 정보를 주변 노드들에게 알려주고 이웃 노드들로부터 받은 키 정보를 통해 이루어진다. 인접한 노드와 공유하고 있는 키가 있으면 해당 노드와 안전한 링크(link)를 만들고, 그 중 하나를 선택해 Challenge-response 프로토콜을 통해 해당 노드가 키를 가지고 있는지에 대해 확인하는 것으로 구성된다. 패스 키 생성은 인접한 노드들과 공유하고 있는 키가 없어 안전한 링크를 생성할 수 없는 경우 안전한 링크들로 연결된 그래프를 통해 해당 노드로의 패스가 있는 경우 새로운 키를 상호간에 생성하는 단계이다.

그러나 이 방식은 연결 정도가 확률적으로 구성되기 때문에 센서네트워크를 나타내는 전체 그래프가 완전하게 연결되지 않을 수도 있으며, 이는 센서 노드의 배치가 불규칙적이거나 배치된 환경에 물리적으로 통신을 방

해하는 요소가 있는 경우 더욱 심해진다. 특히, 네트워크 연결 정도를 증가시키기 위해서는 센서 노드마다 저장해야 할 키 사이즈가 증가되어야 하는 문제가 발생하며, 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 센서네트워크 다른 영역에서 활용할 수 있다는 점에서 여전히 문제가 발생하며, 탈취된 노드들이 서로 협력을 통해 보다 효율적인 감청 및 탈취 여부를 숨길 수 있는 점이 안전성 분석에 전혀 고려되지 않았다 [15]. 또한, 다수의 센서 노드들로 구성된 센서네트워크 및 임의의 노드마다 다수의 인접한 이웃 노드들이 있다고 가정했으나, 이는 노드간 간섭으로 인한 에너지 소모가 증대된다. 간섭으로 인한 에너지 소모를 줄이기 위해서는 센서 노드마다 공유하고 있는 확률을 높여야 하며 이는 센서 노드마다 필요로 하는 키 사이즈를 증가하는 문제가 발생한다 [16].

2. LEAP(Localized Encryption and Authentication Protocol) [8]

LEAP(Localized Encryption and Authentication Protocol) [8]는 2003년 S. Zhu *et. al.*이 제안한 마스터 키 기반의 방식이다. 일반적인 마스터 키 기반의 방식과는 달리 노드 식별자를 이용해 인접 노드와 공유키를 생성한 다음 마스터 키를 지워서 노드 탈취가 발생하더라도 인접 노드와 공유한 키를 악의적인 공격자에게 노출되지 않을 수 있다.

모든 센서 노드는 개인키, pairwise 키, 클러스터 키, 그룹키를 가지고 있다. 개인키는 베이스 스테이션과 공유하는 키이며, 해당 키를 통해 센싱한 이벤트 보고용 MAC(Message Authentication Code)를 생성하는데 사용한다. Pairwise 키는 모든 노드들이 인접한 노드들과 공유한 키이며, 이를 통해 인접한 노드들과의 안전한 통신 채널 설정이 가능하다. 클러스터 헤더가 랜덤하게 생성한 클러스터 키는 pairwise 키를 통해 인접한 이웃 노드들에게 전달한다. 해당 키는 동일 클러스터에 속한 노드들 간의 안전한 통신 및 데이터 통합에 활용된다. 그룹키는 베이스 스테이션이 센서네트워크를 구성하는 모든 노드들에게 공지 메시지(쿼리 메시지 / 이벤트 등록 및 삭제 / 탈취된 노드 알림 등)를 전송하기 위해 사용된다. 그림 1은 LEAP에서 사용되는 개인키, Pairwise 키, 클러스터 키, 그룹키 사이의 상관관계를 보여준다.

그러나 개인키 및 그룹키는 센서 노드가 배치되기 전에 탑재되기 때문에 악의적인 공격자에게 센서 노드가 탈취될 수 있다. 더욱이, 일반적인 마스터 키 기반의 방식과 동일하게 초기화 과정이 끝나기 전에 센서 노드가 탈취될 경우 악의적인 공격자는 1분 이내에 센서 노드에 저장된 모든 정보를 획득해 센서네트워크에서 사용되고 있는 모든 키들을 생성할 수 있는 문제가 있다 [4].

3. HIKES (Hierarchical Key Establishment Scheme) [3]

2007년에 J. Ibriq *et. al.*은 베이스 스테이션이 신뢰된 인증기관(TA: Trusted Authority)의 역할을 담당하면서 그 기능 중 일부를 클러스터 헤더에게 위임하는 방법을 채택 [3] 하였다.

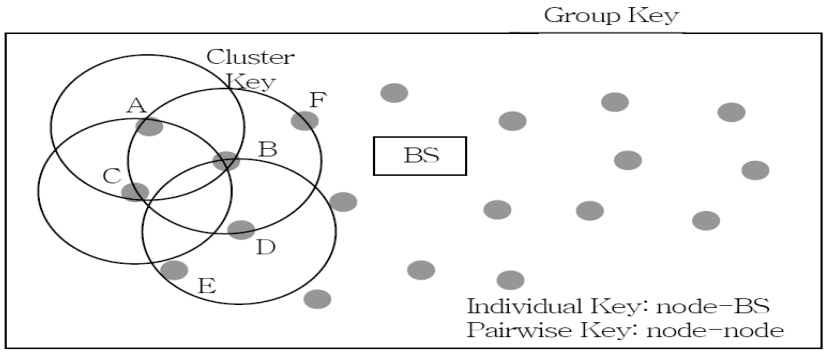

그림 1 LEAP에서 사용되는 개인 키, Pairwise 키, 클러스터 키, 그룹키 사이의 상관관계

이를 통해 현존하는 대부분의 공격에 내성을 지닐 수 있으며, 모든 노드에 partial key escrow table을 가지고 있어 모든 노드가 클러스터 헤더로 선출될 수 있어 네트워크 수명 연장이 가능하다. 게다가 메시지 라우팅이 트리 기반으로 이루어지기 때문에 클러스터 헤더에서 일차적인 데이터 통합이 이루어진 후에는 클러스터 헤더들 간의 메시지 포워딩을 통해 베이스 스테이션에게 전송한다.

제안된 기법은 키 사전 분배, 이웃 탐색, 키 생성과 같은 3가지 단계로 이루어진다. 먼저, 키 사전 분배는 16 bit offset으로 구성된 16개의 entry를 가지는 partial key escrow table, 베이스 스테이션이 암호화한 nonce N_R, 7개의 키(노드 키 K_i, 세션 키 K_s, primary key K_{ib}, 클러스터 키 K_{ic}, 그룹 키 K_g, 마스터 키 K_m, 백업 클러스터 키 K_{backup})를 센서 노드에게 저장하는 단계이다. 여기서 Partial key escrow table을 통해 각각의 entry는 2^{16}개의 키들을 포함할 수 있기에 최대 2^{20}개의 노드 ID를 지원할 수 있다.

이웃 탐색단계에서는 모든 노드는 자신의 노드 ID와 nonce를 포함하고 있는 Hello 메시지 $u||N_u||e_{K_u}(u||N_u)$를 인접한 이웃 노드에게 전송한다. 해당 메시지를 수신한 인접 노드는 마스터 키 K_m를 이용해 K_u를 유도해 수신한 메시지를 복호화한 다음 응답 메시지 $u||v||N_v||e_{K_v}(u||v||N_u||N_v)$를 생성해서 전송한다. 인접한 이웃 노드에게서 응답 메시지를 수신한 노드는 자신이 해당 메시지를 받았음을 알리는 메시지를 전송한다.

키 생성단계에서는 6개의 세부 단계를 거쳐서 베이스 스테이션까지의 라우팅 경로 상의 노드 간에 pairwise 키를 생성한다. 그림 2는 키 생성 과정을 간략화 시켜 보여준다.

1 단계: 노드 u는 자신의 부모 v에게 세션 키 생성을 요청하기 위해 $(u||v||N_u)||e_{K_{ub}}(u\oplus R_u)$ $||e_{K_{uc}}(u\oplus C_u)||h$를 전송한다. 여기서 h는 $e_{K_u}(u\oplus N_u)$이다.

2 단계: 노드 v는 노드 u로부터 수신한 메시지를 확인한 다음 TA의 권한 일부를 받은 클러스터 헤더 c에게 $(c||v||u||N_v)||e_{K_{vb}}(v\oplus R_v)||e_{K_{ub}}(u\oplus R_u)||e_{K_{vc}}(v\oplus C_v)||h$를 전송한다. 여기서 h는 $e_{K_v}(v\oplus N_v)$이며, C_v는 $e_{K_{uc}}(u\oplus C_u)$이다.

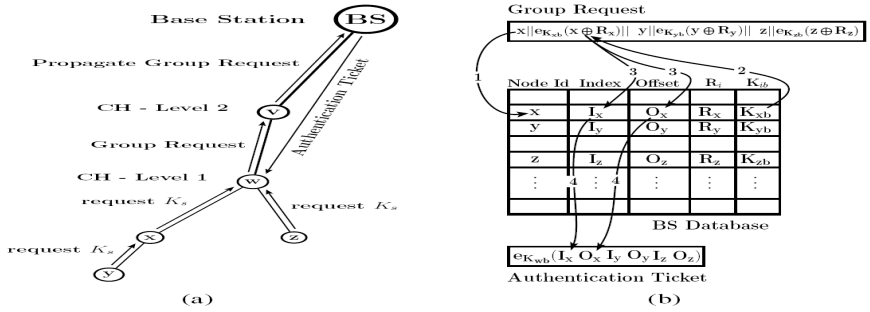

그림 2 (a) 네트워크에서 pairwise 키 생성 과정, (b) BS에서 인증 티켓 생성 과정

3 단계: 클러스터 헤더 c는 자신의 클러스터에 속하는 멤버들로부터 수신한 메시로부터 그룹 인증 메시지 $(b||c||N_c)||e_{K_{cb}}\left(\left(i_1||e_{K_{i_1b}}(i_1\oplus R_{i_1})\right)||\left(i_2||e_{K_{i_2b}}(i_2\oplus R_{i_2})\right)||\cdots\left(i_j||e_{K_{i_jb}}(i_j\oplus R_{i_j})\right)\right)||e_{K_{cb}}(c\oplus C_c)||h$를 베이스 스테이션에게 전송한다. 여기서 h는 $e_{K_{cb}}(b\oplus c\oplus N_c)$이다.

4 단계: 베이스 스테이션은 클러스터 헤더 c에게서 받은 메시지를 K_{cb}로 복호화한 다음 수신한 i_x에 저장된 테이블에 있는 K_{i_xb}와 R_{i_x}를 가져와 개별 암호화된 메시지를 복호화해서 수신한 i_x와 비교해 일치할 경우 해당 i_x에 저장된 인덱스 I_{i_x}와 오프셋 O_{i_x}를 클러스터 헤더에게 보낼 인증 티켓에 포함시킨다. 만약, 일치하지 않는 경우 경고 메시지를 추가한다. 인증 티켓은 $(c||b||C_c||N_b)||e_{K_{cb}}\left(\left(I_{i_1}||O_{i_1}\right)||\left(I_{i_2}||O_{i_2}\right)||\cdots||\left(I_{i_j}||O_{i_j}\right)\right)||e_{K_{cb}}(c||b||C_c||N_c)$이다 (그림 2-b).

5 단계: 베이스 스테이션으로부터 인증 티켓을 받은 클러스터 헤더는 $e_{K_{cb}}(c||b||C_c||N_c)$를 확인한 다음, K_{cb}로 수신한 메시지를 복호화해 $\left(I_{i_1}||O_{i_1}\right)||\left(I_{i_2}||O_{i_2}\right)||\cdots\left(I_{i_j}||O_{i_j}\right)$를 얻어 인접한 노드들을 위한 인덱스와 오프셋을 저장하며, 공유키 K_{ic}를 생성한다 (그림 3). 생성된 공유키를 이용해 노드 u와 v로부터 수신한 $e_{K_{uc}}(u\oplus C_u)$와 $e_{K_{vc}}(v\oplus C_v)$를 복호화해 u, v, C_u, C_v를 확인하고 $(v||c||N_c)||e_{K_{vc}}(K_s||L||C_v||K_g)||e_{K_{uc}}(K_s||L||C_u||K_g)||h$를 생성해 노드 v에게 전송한다. 여기서 h는 $e_{K_{vc}}(v\oplus c\oplus N_c)$이다.

6 단계: 노드 v는 클러스터 헤더로부터 수신한 메시지 중 $e_{K_{vc}}(K_s||L||C_v||K_g)$를 K_{vc}를 이용해 복호화한 다음 C_v를 확인한다. 만약 C_v가 전송한 내용과 일치하면, K_s를 이용해 $(u||v||N_v)||e_{K_s}(N_u||N_v||IV)||e_{K_{uc}}(K_s||L||C_u||K_g)||h$를 생성해 노드 u에게 전송한다. 여기서 h는 $e_{K_v}(v\oplus N_v)$이다.

그러나 노드 인증이 베이스 스테이션을 통해 이루어진다는 점에서 봤을 때 클러스터 헤더가 전송해야 하는 메시지 사이즈가 증가되며, 모든 노드는 partial key escrow table을 저장하고 있어야 하기에 추가적인 저장 공간이 필요하다. 게다가 악의적인 공격자가 노드탈취를 통해 partial key escrow table을 획득할 경우 이를 키 복구에 활용할 수 있다.

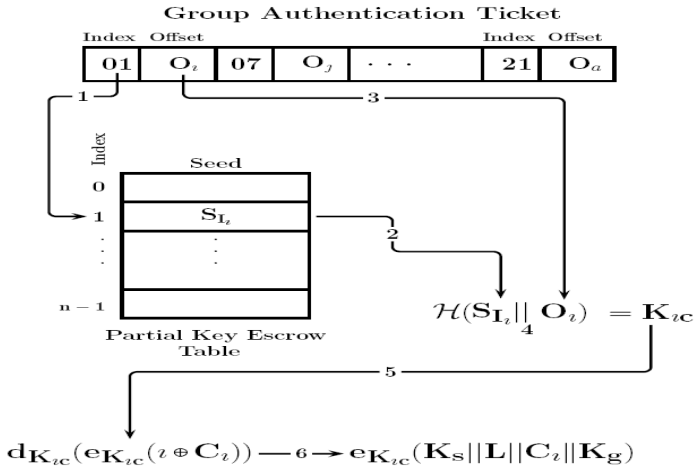

그림 3 클러스터 헤더에서 인증 티켓을 활용해 노드 인증 및 키 발급 과정

Ⅳ. 분석결과

기존에 제안된 키 관리 기법을 분석해 정리하면 표 1과 같다. 먼저, 노드탈취에 있어 사전에 분배된 키를 통해 pairwise 키를 생성하는 프로토콜 [7]은 악의적인 공격자가 노드를 탈취해 획득한 키를 센서네트워크 전체에서 사용할 수 있기 때문에 매우 취약하다. LEAP [8]는 마스터 키를 이용해 pairwise 키를 생성하고 해당 마스터 키를 지운다고 가정했으나 공격자가 마스터 키를 지우기 전에 노드를 탈취할 수 있으며, 이 경우 공격자는 모든 pairwise 키를 생성할 수 있기 때문에 노드탈취에 취약하다. 반면에 HIKES [3]는 노드가 탈취되더라도 탈취된 정보는 탈취된 노드가 속하는 클러스터에서만 활용할 수 있기 때문에 상대적으로 노드탈취에 강하다. 이것은 노드 인증 및 키 생성이 베이스 스테이션을 거쳐서 이루어지기 때문이다. 저장 공간의 경우 사전키 분배 방식은 높은 네트워크 연결도를 보장해 주기 위해 노드에 저장하고 있는 키를 증가시켜야 하기 때문에 다른 기법들에 비해 상대적으로 많은 저장 공간이 필요하다. 표 1에서 저장 공간에서 수치는 키 풀(P)이 10000이며, 인접 노드의 수(d)가 50인 경우 센서 노드마다 250개 키가 필요하며, $|K_A|$는 키 사이즈를 의미한다. LEAP는 마스터 키를 통해 인접노드와의 pairwise 키를 생성하기 때문에 상대적으로 키는 $3\times d+2+L$개가 필요한 반면에, HIKES는 베이스 스테이션과 인접한 노드와 공유한 키만 필요하기 때문에 $2\times d+21$개의 키가 필요하다. 이때, d는 단일 클러스터에 속하는 노드들의 수를 의미하며, L은 키 체인을 저장하기 위해 노드가 저장해야 하는 키의 수를 의미한다. 익명성과 책임성은 어떠한 키 관리 기법에서도 제공되지 않는다. 또한, 확장성 측면에서 LEAP가 가장 좋다. 이는 사전키 분배 방식에 비해 노드가 증가하더라도 저장 공간에 대한 요구사항이 낮으면서도 베이스 스테이션이 노드 인증 및 키 생성에 참여하지 않기 때문에 단일 클러스터에 속한 노드들의 인증에 가장 적은 메시지 사이즈가 필요하기 때문이다.

그러나 기존에 제안된 키 설정 기법들은 이러한 요구사항을 만족하지 않기 때문에 새로운 키 설정 기법이 필요하다. 특히, HIKES는 선택적인 전송 공격을 제외하고 현재까지 알려진 다양한 공격에 내성을 가지며, 저장

공간에 대한 요구사항이 상대적으로 적다. 그러나 모든 노드들이 partial key escrow table을 가지고 있으며, 이를 활용해 키를 생성하므로 악의적인 공격자는 partial key escrow table을 활용해 다른 지역에 위치한 클러스터 헤더와 센서 노드간의 pairwise 키 유추가 가능하다. 또한, 클러스터에 속한 노드들의 수가 증가함에 따라 클러스터 헤더가 노드 인증을 위해 전송해야 하는 메시지 사이즈가 증가해 네트워크 운영시간이 짧아지는 문제가 발생한다. 이러한 측면에서 봤을 때 기존에 제안된 키 설정 기법들은 감시정찰용 센서네트워크에 부적합하다. 따라서 새로운 키 설정 기법은 HIKES보다 적은 저장 공간을 필요로 하면서도 노드탈취에 강하고, 알려진 공격에 내성을 가져야 하며, 확장성이 더 좋아야 한다.

표 1 기존의 키 관리 기법 비교

	Eschenauer *et. al.* [7]	LEAP [8]	HIKES [3]
노드탈취의 영향	하	중	상
베이스 스테이션 참여여부	X	X	O
저장 공간	$250\times\|K_A\|$	$(3\times d+2+L)\times\|K_A\|$	$(2\times d+21)\times\|K_A\|$
네트워크 연결도	0.998356	1	1
익명성	X	X	X
책임성	X	X	X
알려진 공격에 내성 여부	언급되어 있지 않음	HELLO flood 공격 / wormhole을 제외한 대부분의 외부 공격에 내성	악의적인 라우팅 정보 / sinkhole 공격 / sybil 공격 / wormhole 공격 / HELLO flood 공격에 내성
확장성	하	상	중

Ⅴ. 결론

본 논문에서는 센서네트워크 키 관리 기법을 노드 배치 이전에 키 분배 여부, 마스터 키 사용여부, 베이스 스테이션 참여여부에 따라 3가지로 구분했으며 대표적인 논문 3가지를 설명하였다. 또한, 감시정찰 및 주요 시설물 관리 센서네트워크에서의 키 관리 요구사항을 살펴보았으며, 기존에 제안된 키 관리 기법들은 감시정찰 및 주요 시설물 관리 센서네트워크에 적합하지 못함을 보였다. 추후 이러한 문제점을 개선한 새로운 키 관리 기법을 제안하고자 한다.

참 고 문 헌

[1] Y. Law and P. Havinga, "How to Secure a Wireless Sensor Network", *in Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP '05),* IEEE Computer Society Press, 2005, pp. 89-95.

[2] D. R. Raymond and S. F. Midkiff, "Denial-of-Service in Wireless Sensor Networks: Attacks and

Defenses", *in Pervasive Computing*, IEEE, Vol. 7, Issue 1, Jan.- Mar. 2008 Page(s):74 - 81.

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

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

[5] A. Liu and P. Ning, "TinyECC: A Configurable Library for Elliptic Curve Cryptography in Wireless Sensor Networks", *Information Processing in Sensor Networks (IPSN '08)*, 22-24 April, 2008, pp. 245-256.

[6] Y. W. Law, J. Doumen and P. Hartel, "Survey and Benchmark of Block Ciphers for Wireless Sensor Networks", *ACM Transactions on Sensor Networks*, Vol. 2, No. 1, February, 2006, pp. 65-93.

[7] L. Eschenauer and V. D. Gligor, "A key management scheme for distributed sensor networks." *in Procedings of the 9th ACM conference on Computer and Communications Security (CCS),* Washington. DC. USA. November 18-22 2002. pp. 41-47.

[8] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *Proc. of the 10th ACM Conference on Computer and Communication Security (CCS)*, 2003, pp.62-72.

[9] H. Chan, A. Perrig, and D. Song, "Random KeyPredistribution Schemes for Sensor Networks." *in IEEE Symposium on Security and Privacy,* Berkeley, California, May 11-14 2003 pp. 197-213.

[10] W. Du, J. Deng, Y. S. Han and P. K. Varshney, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks.", *in Proceedings of the 10th ACM conference on Computer and Communications Security (CCS),* Washington, DC. USA, October 27-31 2003, pp. 42-51.

[11] D. Liu and P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks", *Proc. of the 10th ACM Conference on Computer and Communication Security (CCS)*, 2003, pp.52-61.

[12] J. Hwang and Y. Kim, "Revisiting Random Key Pre-distribution Schemes for Wireless Sensor Networks", *ACM* Special Interest Group on Security, Audit, and Control (SIGSAC), 2004, pp. 43-52.

[13] 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.

[14] M. G. Sadi, D. S. Kim, 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, 20-22 July 2005 pp.310-314.

[15] T. Moore, "A Collusion Attack on Pairwise Key Predistribution Schemes for Distributed Sensor

Networks", *Proceedings of the Fourth Annual IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOMW '06)*, 13-17 March 2006.

[16] 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)*, IEEE 2007.