한국시뮬레이션학회 논문지
Vol. 17, No. 3, pp. 95-105 (2008. 9)

무선센서네트워크를 위한 다중계층 클러스터 기반의 분산형 인증모델

신종회[1] · 유동영[1†] · 김석규[2]

Distributed Authentication Model using Multi-Level Cluster for Wireless Sensor Networks

Jong-Whoi Shin · Dong-Young Yoo · Seog-Gyu Kim

ABSTRACT

In this paper, we propose the DAMMC(Distributed Authentication Model using Multi-level Cluster) for wireless sensor networks. The proposed model is that one cluster header in *m*-layer has a role of CA(Certificate Authority) but it just authenticates sensor nodes in lower layer for providing an efficient authentication without authenticating overhead among clusters. In here, the *m*-layer for authentication can be properly predefined by user in consideration of various network environments. And also, the DAMMC uses certificates based on the threshold cryptography scheme for more reliable configuration of WSN. Experimental results show that the cost of generation and re-configuration certification are decreased but the security performance are increased compared to the existing method.

Key words : Wireless sensor network, Multi-level cluster, Cluster head, Distributed authentication, Threshold cryptography

요 약

본 논문에서는 무선 센서네트워크에서 센서노드의 효율적 인증을 제공하기 위한 다중계층 클러스터 기반의 분산형 인증모델(DAMMC: Distributed Authentication Model using Multi-level Cluster)을 제안한다. 제안된 인증모델은 하나의 클러스터 헤드가 CA 기능을 갖되 사용자가 정의한 *m*개의 다중계층을 두고 상위 클러스터가 하위클러스터를 인증하는 구조로서, 클러스터들끼리의 상호 인증 오버헤드를 해결할 수 있는 기법이다. 특히 노드 인증서 발급의 경우, 임계값 *t*개 이상의 클러스터 멤버 노드가 분할인증서를 제공하는 경우에만 인증서가 생성되도록 비밀분산기법을 사용하여 센서노드의 효과적인 신뢰관계를 구축하였다. 제안된 DAMMC는 시뮬레이션을 통해 초기인증과정에서의 인증발급 연산시간, 노드 추가에 따른 인증발급 연산시간 등이 기존 인증프로토콜에 비해 우수함을 확인하였으며, 보안성능도 변형공격, 속임 경로 공격 및 비인가된 노드 추가, 재사용 공격 등의 공격기법으로부터 안전함을 확인하였다.

주요어 : 무선센서네트워크, 다중계층 클러스터, 클러스터 헤드, 분산형 인증, 비밀분산법

1. 서 론

무선센서네트워크(Wireless Sensor Network)는 RFID 태그 노드나 센서 노드(sensor nodes) 등으로 이루어진 네트워크이며, 이들 노드는 어느 곳에나 쉽게 설치되어 자율적으로 네트워크를 구성하고, 사물 및 환경 정보를 감지·저장·가공·통합하여 무선으로 전송하게 된다. 무선센서네트워크는 각 노드들이 지리적으로 넓게 분산되어 있어 공격자로부터 탈취 및 분석 공격을 당하기 쉽고, 배터리 소모를 촉진시키거나 불필요한 통신을 야기 시켜 서비스를 불능상태로 하는 DoS(Denial-of-Service) 공격에도 매우 취약하다. 이와 같은 위협에 대비한 여러 가지 다양한 방어 기법들이 현재 활발히 연구되고 있는데 특히, 방어 기법의 기초가 되는 노드 간의 인증 및 메시지 인증 등이 매우 중요하게 다뤄지고 있다[1-4]. 일반적으로 무선센서네트워크에서는 싱크노드가 인증기관(CA: Certificate

2008년 7월 25일 접수, 2008년 8월 26일 채택
[1] 한국정보보호진흥원
[2] 안동대학교 전자정보산업학부
주 저 자 : 신종회
교신저자 : 유동영
E-mail; ydy@kisa.or.kr

Authority)으로서 하위의 모든 센서노드를 인증하는 중앙집중형 인증모델[5-7]을 사용하는데, 이는 프로토콜이 단순하여 컴퓨팅 능력이 떨어지는 센서노드에서 사용하기 적합하기 때문이다. 그러나 네트워크 규모가 커지고 인증을 원하는 노드와 인증을 담당하는 CA가 멀어질 경우 인증을 위한 통신 시간이 길어질 뿐만 아니라 통신을 위해 노드들에게 주어지는 오버헤드가 급격히 증가하게 되는 문제점이 있다.

이와 같은 문제점 해결을 위하여 본 논문에서는 무선 센서네트워크 라우팅 프로토콜의 일종인 CBRP(Cluster Based Routing Protocol)[8]에서 정의한 '클러스터' 단위로 센서노드들을 구성하고 클러스터 헤드(CH: Cluster Head)가 CA 기능을 갖되 클러스터 간의 사용자가 정의한 m개의 계층을 두어 상위 클러스터가 하위클러스터를 인증하는 구조를 갖는 다중계층 클러스터 기반의 분산형 인증모델(DAMMC: Distributed Authentication Model using Multi-level Cluster)을 제안한다. 여기서 클러스터 간 상호 신뢰는 공통의 상위 클러스터가 보장하게 되므로 각 클러스터들끼리 상호 인증으로 발생하는 오버헤드의 문제점을 해결할 수 있다. 또한, 무선 센서네트워크는 토플로지와 구성원이 수시로 변하는 동적인 구성을 가지고 있어서 어떤 노드가 훼손 되었을 때, 노드들의 신뢰관계도 변하게 되어 있어 일반적인 무선 네트워크와는 달리 빈번히 발생하는 노드의 가입 및 탈퇴에 즉각적으로 적응할 수 있는 시스템이 필요하다. 이에 우리는 센서노드의 효과적인 신뢰관계 구축을 위하여 비밀분산법(Threshold Cryptography)[9-10]을 사용하는 DAMMC기법을 제안한다.

2. 관련연구

2.1 다중계층 클러스터

무선 센서네트워크 라우팅 프로토콜의 하나인 CBRP (Cluster Based Routing Protocol : 클러스터 기반 라우팅 프로토콜)는 일련의 노드들을 하나의 클러스터 헤드와 다수의 클러스터 멤버로 이루어진 클러스터로 묶어 라우팅한다. 여기서 클러스터 헤드는 클러스터 멤버의 추가 혹은 탈퇴 시에 인증서를 발급 하거나 인증서를 폐기하는데 주도적인 역할을 하게 되는데, 다중계층 클러스터는 기존 LEACH, TEEN 등에서 입증된바와 같이 집성(aggregation)을 통하여 통신비용을 줄일 수 있는 구조를 말한다. 즉, 각 노드들이 센싱한 정보를 자신이 속한 클러스터의 클러스터 헤드로 보내면, 클러스터 헤드는 노드들이 보내온 메시지를 집성하여 메시지의 사이즈를 줄이게 된다. 클러스터 헤드는 상위의 클러스터로 메시지를 전달하고, 상위 클러스터의 클러스터 헤드는 하위 클러스터에서 보내온 메시지를 집성하여 자신의 상위 클러스터로 메시지를 전달하게 된다. 또한 클러스터 헤드에 오버헤드가 집중되어 특정 노드만 전력을 빨리 소모하는 것을 막기 위하여 일정 시간을 한 라운드로 정하고 라운드가 끝나면 클러스터 멤버 중 하나를 새로운 헤드로 바꾸는 작업을 하게 된다[11-14].

2.2 중앙집중형 인증모델

중앙집중형 인증모델에서는 싱크 노드가 모든 인증을 담당함에 따라 싱크 노드에 인증의 모든 오버헤드가 집중되어 인증을 위한 라우팅 오버헤드가 크다. 그러나 인증구조가 단순하기 때문에 각 노드에 주어지는 오버헤드는 줄일 수 있는 장점이 있다. 따라서 인증을 위한 라우팅 오버헤드가 노드들이 인증에 참가하여 생기는 인증 오버헤드보다 적은 경우에 유리한 모델이다. 또한, 노드 인증에 필요한 정보를 다른 노드들이 알고 있지 않기 때문에 인증정보의 물리적인 탈취 공격에 비교적 안전하다. 중앙집중형 인증모델은 싱크 노드와 인증을 요구하는 노드의 거리가 가까운 소규모 네트워크에 적합한 시스템이다. 그림 2

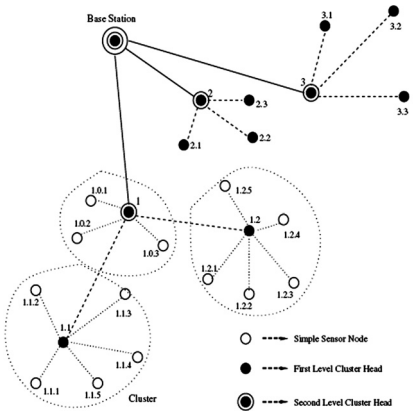

그림 1. TEEN에서의 다중클러스터 구조

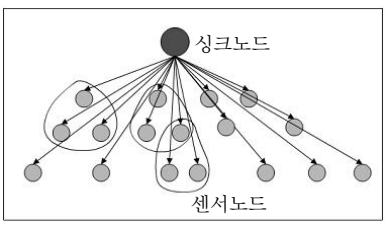

그림 2. 중앙집중형 인증모델

와 같이 CA가 생성되는 계층 값 m을 1로 정하면 싱크 노드만이 CA역할을 하는 중앙집중형 네트워크 설치가 가능하다.

표 1은 중앙집중형 인증모델에 사용되는 대표적인 5가지의 인증방식을 정리하여 장단점을 나타낸 것이다.

2.3 비밀분산기법

무선 센서네트워크에서는 노드의 신분이 서로에게 불확실하며, 악의적인 중간노드에 의해 라우팅 보안이 취약할 수 있다. 이를 막기 위한 방법으로, 올바른 노드들이 충분히 존재하기만 하면, 라우팅 프로토콜은 훼손된 노드들 주변을 우회 할 수 있는 경로를 찾을 수 있을 것이다. 이를 위해, 비밀분산기법(Threshold Cryptography)이 제안되었다. Shamir가 제안한 비밀분산기법[15]은 그림 3과 같이 공개키와 비밀키 쌍을 이용하는데, 공개키는 한 개만 존재하는 반면에 비밀키는 n개의 노드로 이루어진 그룹에 의해 비밀정보가 일부분씩 공유된다. 임계값 t 이하의 노드는 비밀키를 얻을 수 없으므로, 원문을 복구해 내지 못하고, $t+1$ 이상의 노드가 모여야만 비밀 키를 얻어낼 수 있다[16].

이 시스템에서는 송신자가 메시지 수신자에게 전송하고자 하는 경우, n개 그룹의 공개키를 가지고 원문을 암호화 하여 전송한다. 수신자는 각자가 가지고 있는 비밀정보를 믿을 수 있는 노드(Trusted Party)에게 안전한 채널을 통해 전송한다. 신뢰된 노드는 $t+1$이상의 비밀정보를 모아서 비밀 키를 만들어낸 후, 원문을 구하여 각각의 수신자에게 데이터를 전송한다.

표 1. 중앙집중형 인증모델에 사용되는 인증방식

인증방식	특 징	장 점	단 점
대칭키 인증방식	모든 노드들이 대칭키를 갖고 상호간 인증	간단한 인증구조	인증키 증가에 따른 키 관리 효율성 저하
비대칭키 인증방식	싱크노드가 공개키를 사용하여 센서노드 인증	싱크노드의 공개키 연산 수행으로 센서 노드의 연산 오버헤드 감소	노드인증을 위해 외부 CA 필요
TESLA 인증방식[5]	동기화된 싱크노드와 센서 노드간 시간 간격에 맞추어 인증키 송수신	해시 체인을 이용하여 효과적으로 데이터 인증	인증에 일정 시간 이상이 필요
Merkle 트리 해쉬 인증방식[6]	모든 센서 노드의 해쉬 값을 만들고 트리구조를 형성하여 루트 노드를 인증	연산이 빠르고 연산 량이 적음	한번 해쉬 트리가 구성되면 갱신이 어려움
Lightweight 인증방식[7]	크기가 작은 공개키 사용하여 노드인증	송신자 확인 기능이 있음	연산시간이 느림

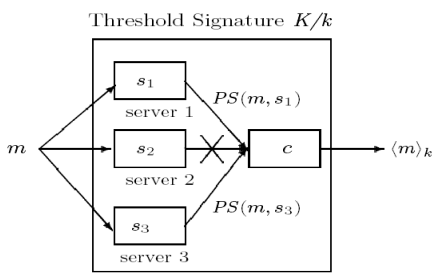

그림 3. 비밀분산 기법

3. DAMMC 제안

다중계층 클러스터형 무선 센서네트워크에서의 대표적인 인증모델에는 중앙집중형 인증모델과 분산구조형 인증모델이 있다. 중앙집중형 인증 모델의 경우에는 싱크노드가 모든 인증을 담당하는 모델로서 인증을 위한 라우팅 오버헤드가 노드들이 인증에 참가하여 생기는 인증 오버헤드보다 적은 경우에 유리한 모델이다. 반면 분산구조형 인증모델의 경우, 각 클러스터 헤드가 CA가 되어 인증을 주도하게 되고, 모든 클러스터 멤버가 자신이 속한 클러스터의 인증 작업에 참가하는 모델로서 인증을 위한 라우팅 오버헤드가 노드들이 인증에 참가하여 생기는 인증 오버헤드보다 클 경우에 유리한 모델이다. 이에 반해 우리가 제안하는 DAMMC 모델의 경우에는 네트워크에 적합하도록 인증계층 m 값을 조절하여 클러스터 헤드들에게 CA 역할을 부여함으로서 인증서를 발급에 따른 오버헤드를 최소화하는 모델이다. 표 2는 제안된 DAMMC 모델과 기존의 중앙집중형 및 분산구조형 인증모델과의 특징을 비교분석한 것이다.

3.1 다중계층 클러스터의 구성

다중계층 클러스터는 한 계층의 클러스터가 생성되면 해당 클러스터의 헤드가 상위 계층의 클러스터 멤버가 되도록 구성된다. 즉, 1-level의 클러스터 헤드들은 상위 클러스터인 2-level 클러스터를 이루게 된다. 2-level 클러스터의 클러스터 멤버들은 1-level 클러스터의 헤드들로 이루어지게 되고, 2-level 클러스터의 클러스터 헤드들은 다시 3-level 클러스터를 구성하게 된다. 위와 같은 방식으로 싱크 노드를 헤드로 하는 단일의 클러스터를 구성하게

표 2. WSN에서의 인증모델간 특징 비교분석

인증모델	설 명	특 징
중앙집중형 모델	싱크 노드가 모든 인증을 담당하는 모델로 싱크 노드와 인증을 요구하는 노드의 거리가 가까운 소규모 네트워크에 적합	인증구조가 단순하기 때문에 각 노드에 주어지는 오버헤드가 적으나, 네트워크의 규모가 커지고 노드와 인증을 담당하는 CA가 멀리 떨어질 경우 인증을 위한 노드의 통신 오버헤드 증가
분산구조형 모델	계층별로 구성된 각 클러스터 헤드가 CA가 되어 인증을 주도하며, 싱크 노드와 인증을 요구하는 노드의 거리가 먼 대규모 네트워크에 적합	인증 오버헤드가 네트워크에 속한 모든 노드들에게 분산되어 인증을 위한 라우팅 오버헤드가 적으나, CA가 많아 질 수 록 CA들 간의 상호 인증을 위하여 인증서 구성이 복잡해지고 통신 오버헤드가 증가
DAMMC 모델	네트워크에 적합하도록 인증계층 m 값을 조절하여 CA 역할을 부여함으로서 인증서 발급에 따른 오버헤드를 최소화하며 싱크 노드와 인증을 요구하는 노드의 거리가 먼 대규모 네트워크와 비교적 가까운 중규모 네트워크에 적합	클러스터 간의 상호 신뢰는 m 값에 의해 지정된 공통의 상위 CA가 보장함으로 분산구조형 모델에서와 같이 각 클러스터들끼리 상호 인증해야 하는 오버헤드를 제거

된다. 세부적인 다중계층 클러스터의 구성은 다음과 같은 단계를 거쳐 이뤄진다.

(1) 브로드캐스트 단계

모든 노드들은 p의 확률로 0 혹은 1의 클러스터 헤드 생성 메시지를 주위 노드에게 브로드캐스트 한다. 노드들은 자신이 받은 메시지를 합하고, 만약 그 합이 일정 임계값(Threshold)에 미치지 못할 경우 클러스터 헤드가 된다. 다시 말해, 이 임계값은 효율적 인증을 위한 클러스터의 크기를 결정하는 값이 되는 것이다. 클러스터 헤드가 된 노드는 인근 노드들에게 클러스터 가입 메시지를 보내게 되는데 클러스터 가입 메시지는 인근 노드들에 의해서 k-hop만큼 라우팅 된다.

(2) 클러스터 설정 단계 (1-level)

클러스터 가입 메시지를 받은 노드들은 메시지가 k-hop만큼 라우팅 되지 않았다면 메시지의 라우팅 횟수에 1을 더하고 다시 한 번 주위 노드에게 라우팅 하게 된다. 라우팅 후, 클러스터 헤드에게 자신의 정보를 담은 피드백(Feedback) 메시지를 보내고 클러스터 멤버가 된다. 클러스터 헤드는 보내온 정보를 저장하고 클러스터를 구성한다. 이때 초기에 받은 클러스터 헤드 생성 메시지들의 합이 임계값에 미치지 않아 클러스터 헤드가 되지 못한 노드와 일정 시간이 지난 후에도 클러스터의 가입 메시지를 받지 못한 노드들은 스스로 클러스터 헤드가 된다.

(3) 다중계층 클러스터 구성 단계 (*m*-level)

1-level 클러스터가 구성되면 2-level의 클러스터를 구성할 수 있게 된다. 1-level 클러스터의 헤드들은 p'의 확률로 주변 헤드 노드들에게 0 혹은 1의 메시지를 보내게 되고 그 합이 임계값에 미치지 못하는 노드가 2-level 클러스터의 헤드가 된다. 2-level 클러스터 헤드는 주변 k'-hop까지 클러스터 가입 메시지를 보내게 된다. 이 메시지는 1-level 클러스터의 헤드 노드들만을 대상으로 한다. 2-level 클러스터 가입 메시지를 받은 1-level 클러스터 헤드들은 자신의 정보를 담은 피드백 메시지를 보내게 되고 2-level 클러스터 헤드는 이 정보들을 저장하여 2-level 클러스터를 생성하게 된다. 이때 역시 2-level 클러스터 헤드도 아니고 2-level 클러스터 가입 메시지도 받지 못한 1-level 클러스터 헤드는 일정시간이 지난 후 스스로 2-level 클러스터 헤드가 된다. 이와 같은 방식으로 상위의 클러스터를 생성하여 싱크 노드를 헤드로 하는 단일 클러스터를 생성한다.

(4) 클러스터 키의 분배

클러스터 생성 후에는 클러스터 내부의 그룹 통신을 위해 그룹 키를 지정하게 된다. 클러스터 헤드는 임의의 대칭키를 만들어 클러스터 멤버들에게 나눠주게 되고, 클러스터 키는 클러스터 헤드가 싱크 노드로부터의 메시지를 클러스터 멤버에게 전달하거나 인증서 발행을 위한 메시지를 보낼 때, 그리고 클러스터 멤버가 클러스터 헤드로 분할복호화 메시지(Partial decrypt message)를 보낼 때 사용된다. 그림 4는 다중계층 클러스터의 구성 알고리즘을 나타낸 것이다.

3.2 인증모델 제안

네트워크 구성이 끝나고 다중계층 클러스터를 구성한 후 노드들은 클러스터 헤드에게 인증서 발급 요청을 하게 된다. 본 논문에서 제안하는 DAMMC는 그림 5와 같이 CA의 생성 레벨 m을 네트워크 규모에 맞게 정하면 상위 m 레벨 클러스터 까지 CA역할을 하는 구조로 싱크 노드와 인증을 요구하는 센서노드의 거리가 먼 대규모 네트워크와 비교적 가까운 중규모 네트워크에 적합한 시스템이다. 즉 중앙집중형 모델의 경우는 싱크 노드가 모든 노드

```
// 브로드캐스트 단계
  Repeat-On Node (v) broadcast (m) if p = 1;
    until  z:= Sum of broadcast (m);
    if z < threshold
      then Cluster_Head (v) := v
    else if Cluster_Node (v) := v
    end;
    Send_Msg (Invited) On Cluster_Head (v);
    until k-hop < count(v);

// 클러스터 설정 단계 (1-level)
    if routing_count < k-hop
    then
      routing_count++;
      Send_Msg(feedback) On Cluster_Node(v);
      Cluster_Head (v). Node (x): = feedback;
      Join(v, x);
    end;
    if (Sum(feedback)  < threshold) || (Rev_Msg(Invited)
       cluster_node(v)) > time_t
    then
      Cluster_Head (v) := Cluster_Node (v) :
    end;

// 다중계층 클러스터 구성 단계 (m-Level)
    Join (Cluster_Head (m), Cluster_Head (m-1));
```

그림 4. 다중계층 클러스터 구성 알고리즘

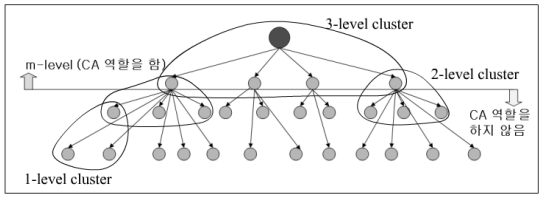

그림 5. DAMMC의 구조

들의 인증을 담당하게 되는 반면 DAMMC는 클러스터 계층 m 값에 따라 CA 역할을 하지 않는 하위 클러스터가 존재하게 되는데, 이 클러스터에 속한 노드들은 상위의 CA 역할을 하는 클러스터로부터 인증을 받게 된다. 이러한 인증 계층의 조절은 인증서를 발행하는 CA를 하위 클러스터로 위임하여 모든 계층에 인증서를 발급함에 따라 발생하는 오버헤드를 최소화하기 위한 것이다. 인증서는 최상위 m 계층 클러스터 헤드가 CA가 되어 자신이 속한 클러스터의 클러스터 멤버들에게 발급하게 되는데, 인증 절차를 살펴보면 우선 최상위 클러스터의 클러스터 멤버가 싱크 노드에게 자신의 정보를 담은 인증 요청 메시지를 보내게 된다. 싱크 노드는 해당 메시지의 적합성을 판단한 후 해당 메시지가 적합하다면 해당 노드의 인증서와 클러스터의 CA 인증키에 대한 인증서를 발급하게 된다. 인증서를 발급 받은 노드, 즉 하위 클러스터의 클러스터 헤드는 상위 클러스터로부터 인증 받은 CA 인증키를 이용하여 자신이 속한 클러스터의 클러스터 멤버들과 하위 클러스터의 CA 인증키를 인증하게 된다. 초기 인증이 끝나면 클러스터 멤버들에게 인증키를 분할하여 나눠주고 새로운 노드의 추가/이동 시에 새로운 인증서를 발행하고 갱신하는데 주도적인 역할을 한다. 또한 클러스터 멤버들의 인증서와 하위 클러스터의 인증서를 보관하는 DS(Directory Service)역할을 수행한다.

초기인증의 경우는 CA 혼자서 인증서를 발급하지만 그 이후의 인증에는 클러스터 멤버들이 인증에 참가하여 인증서 발급을 돕는다. 즉 모든 노드들이 인증된 후에는 CA의 인증 개인키를 비밀분산기법을 이용하여 클러스터 멤버들에게 나누어 주게 된다. CA의 인증키를 분할하는 것은 만약 한, 두개의 노드가 탈취된다 하여도 인증키의 유출을 막을 수 있기 때문이다. 추후에 새로운 노드가 추가될 때는 임계값을 이용하여 분할 인증키를 가진 각 노드들이 분할인증서를 생성하여 해당 노드에 전달하게 되고, 해당 노드는 임계값 t개 이상의 분할인증서가 모아지면 완전한 인증서를 만들어 낼 수 있게 된다. 인증서 발급은 초기화 단계를 통한 클러스터 생성이 이루어지고, 클러스터 헤드와 클러스터 멤버간의 관계가 형성된 후에 시작된다. 하나의 노드가 특정 클러스터의 멤버가 되면, 비밀분산기법을 사용하여 클러스터 내의 멤버노드들로부터 분할인증서를 발급 받는다. 분할 인증키를 나눠받는 클러스터 멤버의 수 x 는 다음과 같다.

$t+1 \le x \le n$ (t : 임계값(threshold),
n : 전체 클러스터 멤버의 수)

4. 인증프로토콜

4.1 노드 초기인증

초기 인증은 처음 네트워크가 구성되고 클러스터를 생성한 이후 상대(Pair-wise) 키[14]로 인증된 노드에 대한 인증서를 발급하는 것이다. 즉 노드가 설치되고 클러스터를 구성한 후 각 노드들은 CA에게 인증 요청을 하게 되는데 초기 인증의 경우는 아직 인증키 분배가 이루어지기 전이기 때문에 그림 6과 같이 CA 단독으로 인증서를 발급하게 된다. 인증서 발급절차를 살펴보면 우선 해당 노드는 DS(최상위 m계층의 클러스터 헤드)를 통해서 CA의 공개키를 얻어낸다. 이때 CA는 자신이 속한 클러스터에서 가장 가까운 CA 인증키를 가지고 있는 클러스터 헤드가 된

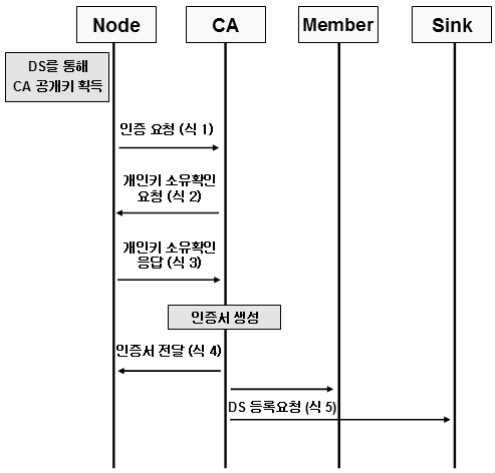

그림 6. 초기 인증

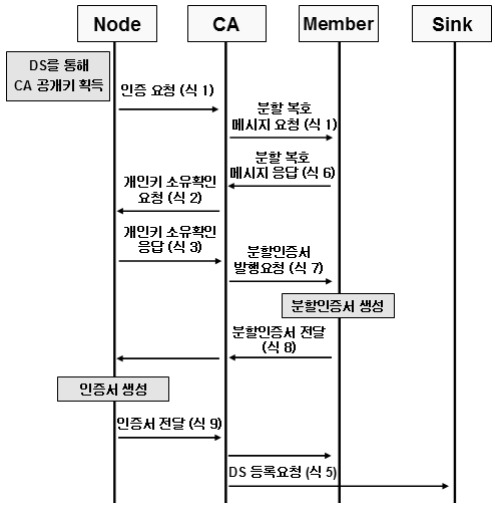

그림 7. 노드의 추가

다. CA의 공개키를 얻어내면 노드 자신의 공개키와 *nonce*, 그리고 상대키로 인증되었음을 알리는 메시지를 CA의 공개키로 암호화 하여 (식 1)과 같이 CA로 보내게 된다.

$$\text{Node}\rightarrow\text{CA}:[E_{CA\_pub}(\text{node\_pub} \parallel E_{pair\_wise}(\text{Msg}) \parallel \text{nonce} \parallel \textit{time})] \quad \text{(식 1)}$$

CA는 해당 노드의 메시지가 적합한지를 판단한 후 노드가 보내온 노드의 공개키 소유 여부를 확인하게 된다. CA가 해당 노드의 공개키로 *nonce2*를 암호화 하여 (식 2)와 같이 해당 노드에게 보내면, 해당 노드는 자신의 개인키로 메시지를 복호화 하여 *nonce2*를 얻어낸다. 개인키 소유 확인을 위해서 *nonce2*를 다시 CA의 공개키로 암호화하여 (식 3)과 같이 CA에게 전달하면 개인키 확인 작업이 끝나게 된다.

$$\text{CA}\rightarrow\text{Node}:[E_{node\_pub}(\textit{nonce2})] \quad \text{(식 2)}$$

$$\text{Node}\rightarrow\text{CA}:[E_{CA\_pub}(\textit{nonce2+1})] \quad \text{(식 3)}$$

개인키 확인 작업을 마치게 되면 CA는 해당 노드의 인증서를 생성한다. 초기 인증의 경우는 아직 CA의 인증키가 클러스터 멤버들에게 분배되지 않았으므로 CA 단독으로 인증서를 생성하게 된다. 생성된 인증서는 (식 4)와 같이 해당 노드에 보내게 되고 CA는 해당 인증서를 DS에 저장한다. 또한 클러스터 멤버들과 싱크 노드에게도 발행된 인증서를 (식 5)와 같이 보내어 DS를 갱신하도록 한다.

$$\text{CA}\rightarrow\text{Node}:[E_{node\_pub}(\textit{certificate} \parallel \textit{nance2+2} \parallel \textit{e} \parallel \textit{time})] \quad \text{(식 4)}$$

$$\text{CA}\rightarrow\text{Member(Sink)}:[E_{CA\_pub}(\textit{certificate} \parallel \textit{e} \parallel \textit{time})] \quad \text{(식 5)}$$

4.2 새로운 노드의 추가

상대키로 인증된 노드의 추가는 CA와 CA가 속한 클러스터의 클러스터 멤버들이 참가하는 분산 인증을 통해서 그림 7과 같이 인증서를 발급하게 된다. 우선 해당 노드는 자신이 상대키로 인증되었음을 알리는 메시지를 CA에 (식 1)과 같이 보내게 된다. CA는 해당 노드가 보내온 메시지를 복호화 하기 위해서 분할 인증키를 가지고 있는 각 멤버들에게 메시지를 (식 1)과 같이 라우팅하면 각 멤버들은 자신이 가진 분할 인증키로 메시지를 복호화하여 분할복호메시지를 생성하여 CA로 전송한다. CA는 이러한 분할복호메시지를 모아 완성된 메시지를 만들게 되고, 해당 노드가 보내온 메시지가 적합한지를 판단한다.

$$\text{Member}\rightarrow\text{CA}: \text{partial\_decrypt\_message} \quad \text{(식 6)}$$

인증 요청 메시지가 적합하다면 해당 노드가 보내온 공개키의 소유 확인을 위해서 노드의 공개키로 *nonce2*를 암호화 하여 해당 노드에 (식 2)와 같이 보내게 된다. 해당 노드는 자신의 개인키로 메시지를 복호화 하여 얻은 *nonce2*를 다시 CA의 공개키로 암호화하여 (식 3)과 같이 CA에 돌려주게 된다. 개인키 소유 확인이 끝나면 해당 노드의 인증서를 생성한다. CA는 분할 인증키를 가지고 있는 멤버들에게 해당 노드의 공개키를 보내고 분할인증서 생성을 요청한다. 이때 멤버들에게 보내는 메시지는 (식 7)

과 같이 클러스터 키로 암호화 하여 보내진다.

CA→Member:[$E_{cluster\_key}$(node_pub, *nonce2+1*)] (식 7)

메시지를 받은 각 멤버들은 (식 8)과 같이 자신이 가진 분할 인증키를 이용하여 분할인증서를 생성하고 해당 노드에게 전달한다.

Member→Node:[E_{node_pub}(*partial_certificate, nonce2+2*)] (식 8)

마지막으로 해당 노드는 분할인증서를 임계값 *t*개 이상 모아 완전한 인증서를 생성한다. 생성된 인증서는 (식 9)와 같이 CA에게 보내지게 되고, CA는 인증서가 문제없이 발행되었음을 알리는 메시지를 해당 노드에게 보냄과 동시에 발급된 인증서를 (식 5)와 같이 클러스터 멤버와 싱크노드에게 보내 DS를 갱신하도록 한다.

Node→CA:[E_{CA_pub}(*certificate* ‖ *nonce2+2* ‖ *e* ‖ *time*)] (식 9)

5. 실험 결과 및 성능 분석

본 장에서는 3장에서 제안한 다중계층 클러스터 구성 알고리즘의 성능과 4장에서 제안한 인증프로토콜의 성능 및 안전성 분석결과를 서술한다. 시뮬레이션 도구로는 MATLAB을 사용하였고, 다중계층 클러스터 구성 알고리즘의 성능 확인을 위하여 클러스터 구성에 따른 에너지 소모량을 측정하였으며, 인증프로토콜에 대한 성능 분석을 위하여 인증서 발급 연산시간을 측정하였다. 마지막으로 DAMMC의 안전성분석을 위하여 변형공격, 속임경로 공격 및 비인가된 노드추가, 재사용 공격 등 3가지 공격기법에 대응한 인증프로토콜 보안 성능을 분석하였다.

5.1 클러스터 헤드 구성의 에너지 소모량 분석

무선 센서네트워크에서의 센서노드는 한정된 배터리, 연산능력 등의 한계로 노드가 소모하는 에너지 량은 전체 네트워크 수명시간에 큰 영향을 미치게 된다. 특히, 클러스터 헤드는 일반 노드보다 많은 연산을 수행하기 때문에 더욱 적은 량의 에너지 소모가 요구됨으로 에너지 소모량에 대한 성능분석은 매우 중요하다. 우리는 클러스터 헤드 구성의 에너지 소모량 분석을 위해 센서노드의 밀도를 λ, 무선영역 내에 있는 주위노드에게 클러스터 헤드 생성 메시지를 브로드캐스트하여 클러스터 헤드가 될 확률을 p, 그리고 인근 노드들이 포워딩하는 클러스터 가입 메시지의 최대 홉 수를 k라고 정의하였다. 시뮬레이션 환경을 구성하기 위한 노드 위치는 [0, 2a]라는 2개의 랜덤넘버를 생성하여 정의하게 되는데 여기서 2a는 노드가 분산 위치한 구역의 변 길이가 된다. 모든 실험에서 각 노드의 통신영역은 1유닛이라고 가정하고 최적의 p와 k값을 도출하기 위해 Seema 등 (2003)[12]이 정의한 (식 10), (식 11)에 따라 에너지 소모량을 연산하였다.

$$p=\left(\frac{1}{3c}+\frac{\sqrt[3]{2}}{3c\left(2+27c^2+3\sqrt{3c}\,\sqrt{27c^2+4}\right)^{1/3}}+\frac{\left(2+27c^2+3\sqrt{3c}\,\sqrt{27c^2+4}\right)^{1/3}}{3c}\frac{1}{\sqrt[3]{2}}\right)^2 \quad \text{(식 10)}$$

c : 클러스터링 알고리즘에 의해 생성된 *m* 계층 클러스터에서, 센서로부터 클러스터 헤드로 데이터가 전달되는데 소요되는 총 통신비용

$$k=\left[\frac{1}{r}\sqrt{\frac{-0.917\ln(\alpha/7)}{p\lambda}}\right] \quad \text{(식 11)}$$

λ : 2차원 공간에서의 Poisson 밀도
α : 거리 r안에 센서가 있을 확률
r : 무선통신영역(*radii*) 거리

클러스터 헤드 구성 알고리즘은 10입방미터 내에 100개 노드가 규칙적으로 분산되어있는 상태에서, *m* 계층 값을 0~5로 구분하여 시뮬레이션하였다. 무선영역 내에서의 통신 손실은 고려하지 않았으며, 에너지 값 1유닛은 데이터 1유닛을 전송하기 위해 소모되는 에너지량으로 정의하였다. 첫 번째 시뮬레이션은 우리가 제안한 DAMMC에서 클러스터 헤드가 될 확률 p값을 고려하여 실험한 것으로, 최대 홉 수 k는 (식 11)을 사용하여 계산하였다. 그림 8은 클러스터링 계층 수(*m*-level)와 에너지 소모량과의 상관관계를 나타낸 것이다. 실험 결과에 따르면 에너지 소모량은 계층 수가 높아질수록 무선통신영역거리(r)의 크기별로 비슷한 형태의 감소율을 보였다. 즉, 클러스터를 생성할 때의 에너지 소모량은 클러스터 계층 수와 밀접한 관계를 나타내는 것을 알 수 있다. 실험을 통해 0~3계층까지는 계층 수가 증가할 때마다 평균 10%이상의 에너지 소모량이 감소하는 것으로 확인되었고, 4~5 level부터는 에너지 소모의 변화가 거의 없어 우리가 정의

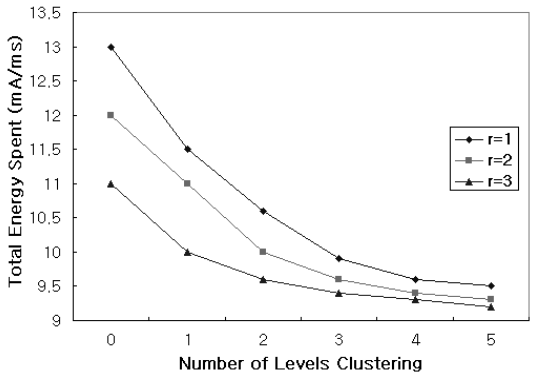

그림 8. 클러스터링 계층 수와 에너지 소모량 상관관계

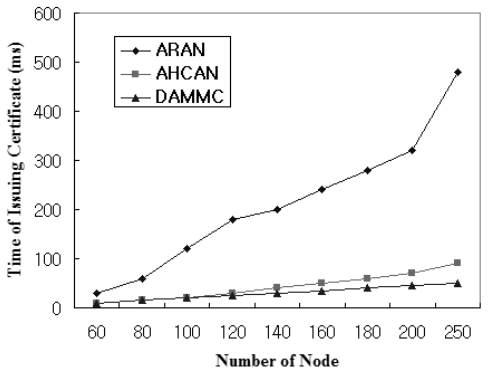

그림 9. 초기인증에서의 인증발급 연산시간

한 실험환경에서는 *m* 값이 3일 때 최적의 에너지 소모량을 보이는 것으로 분석되었다.

5.2 인증연산시간 분석

무선 센서네트워크에서 인증연산에 대한 오버헤드가 증가할 경우에는 에너지 소모량이 늘어 전체 네트워크 수명시간이 줄어드는 문제가 발생 할 수 있다. 따라서 본 절에서는 대표적인 인증기법들의 인증연산 오버헤드를 비교분석하고자 한다. 인증연산시간 측정을 위한 환경구성은 10입방미터 내에 노드들이 규칙적으로 분산되어있다고 가정하였으며, 여기에서 노드간 홉의 거리, 전파세기 저하 등의 통신 오버헤드는 고려하지 않았다. 인증연산시간 분석은 가상적인 노드 수에 대비한 초기인증에서의 인증발급 연산시간과 노드 추가에 따른 인증발급 연산시간을 시뮬레이션하여 기존의 무선 Ad-hoc 네트워크 환경에서의 인증프로토콜인 ARAN(Authenticated Routing for Ad hoc Network)[17], AHCAN(Authentication using Hierarchical Cluster in Ad hoc Networks)[18]의 인증연산시간과 상호 비교분석하였다. DAMMC 초기인증에서의 인증발급 연산시간 T_{node_int}을 계산해보면 (식 12)와 같이 노드가 수행하는 인증요청 시간($T_{cert\text{-}req}$)과 CA의 노드 개인키 확인 시간($T_{node\text{-}req}+T_{node\text{-}resp}$), 인증서 발급시간($T_{issue\_cert}$)을 합한 값이며, 노드추가에 따른 인증발급 연산시간 T_{node_add}는 (식 13)과 같이 노드가 수행하는 인증요청 시간($T_{cert\text{-}req}$)과 CA의 멤버노드에 대한 분할복호메시지 요청시간($T_{msg\_decryp\_req}+T_{msg\_decryp\_resp}$), CA의 노드 개인키 확인 시간($T_{node\text{-}req}+T_{node\text{-}resp}$), 멤버 노드의 분할인증서 생성 시간($T_{part\_cert\_req}+T_{part\_issue\_cert}+T_{part\_cert\_resp}$), 완전한 인증서 생성시간($T_{com\_issue\_cert}$)을 합한 값이 된다.

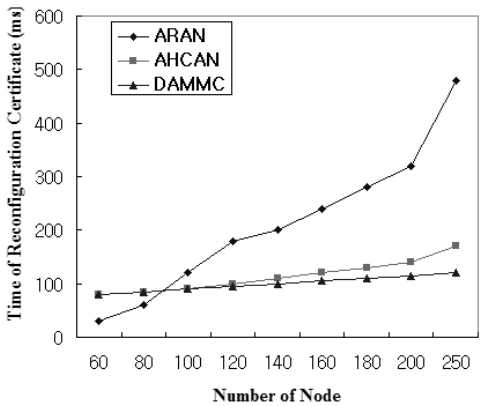

그림 10. 노드 추가에 따른 인증발급 연산시간

$$T_{node\_int} = T_{cert\text{-}req}+T_{node\text{-}req}+T_{node\text{-}resp}+T_{issue\_cert} \quad \text{(식 12)}$$

$$T_{node\_add} = T_{cert\text{-}req}+T_{msg\_decryp\_req}+T_{msg\_decryp\_resp}+T_{node\text{-}req}+T_{node\text{-}resp}+T_{part\_cert\_req}+T_{part\_issue\_cert}+T_{part\_cert\_resp}+T_{com\_issue\_cert} \quad \text{(식 13)}$$

시뮬레이션 결과, 초기 인증에서 소요되는 인증발급 연산시간은 그림 9에서와 같은 결과를 나타내었다. 특히, 노드 추가에 따른 인증발급 연산시간의 경우 그림 10에서와 같이 DAMMC는 인증서 생성과 갱신에 소요되는 총 연산시간이 80～100ms 범위에 있었으며, *m* 값이 1인 경우에는 AHCAN과 연산시간이 유사한 결과를 얻었지만 *m* 값이 2이상(임계값을 100노드로 설정)인 경우부터 연산시간이 개선되어 *m* 값이 3이상인 경우 평균 연산시간 효율이 20%이상 개선되는 결과를 확인하였다. 노드 수에

따른 실험결과를 분석해보면 노드수가 60개 일 경우 그림 9에서와 같이 초기인증 발급시간은 기존에 연구된 ARAN, AHCAN과 비교해 비슷하였으나, 노드 수가 120개 이상으로 증가할수록 기존 방법보다 연산시간이 개선되는 것으로 분석되었다. AHCAN과 비교해보면 노드수 120개까지는 비슷한 성능을 보였으나, 그 이후부터는 연산시간이 짧아졌는데 이는, DAMMC의 경우 인증계층이 3계층 이상으로 구성되어 인증 연산시간에 대한 오버헤드가 분산되는 반면 AHCAN은 2계층의 인증계층으로 구성되기 때문에 연산 오버헤드가 클러스터 헤드(인증노드)에 집중되기 때문인 것으로 분석되었다. 노드 추가에 따른 재구성 시간의 경우 그림 10에 나타낸 것과 같이 ARAN은 클러스터 헤드를 재구성을 할 때, 60노드 규모에서는 클러스터 계층을 설정하는 과정이 불필요하여 연산시간이 우수한 것으로 나타났지만, 노드의 수가 100개 이상으로 증가할 경우, 급격하게 연산시간이 증가하는 결과를 보였다. 이러한 실험결과를 종합해 볼 때 DAMMC는 중규모 이상의 대규모 무선 센서네트워크에 적합한 모델이라 할 수 있다.

5.3 보안성능 분석

본 절에서는 변형공격, 속임 경로 공격 및 비인가된 노드추가, 재사용 공격 등 3가지 공격기법에 대응한 인증프로토콜의 보안성능을 분석하기로 하겠다.

(1) 변형공격 : 일반적으로 라우팅 연산의 무결성에 대한 공격으로서, 라우팅 정보 수정을 통하여 공격자는 네트워크 링크 두절, 상이한 목적지로의 패킷전송, 목적지보다 긴 라우팅 등을 유발하는 통신지연 등을 야기시킬 수 있다. 이에, DAMMC에서는 초기인증에서 E_{CA_pub}(node_pub ‖ E_{pair_wise}(Msg)), E_{node_pub}(*certificate* ‖ *nance2+2* ‖ *e* ‖ *time*)와 같이 CA의 공개키와 노드의 공개키를 상호간에 사용하여 메시지를 암호화하여 송수신하고, 노드추가 과정에서도 $E_{cluster\_key}$(node_pub., *nonce2+1*), E_{node_pub} (*partial_certificate*, *nonce2+2*), E_{CA_pub}(*certificate* ‖ *nonce2+2* ‖ *e* ‖ *time*)와 같이 각각 멤버의 클러스터 키, 노드의 공개키, CA의 공개키(CA_{pub}) 등으로 메시지를 암호화하여 송수신함으로서 기밀성과 무결성을 보장하여 변형공격이 불가능하도록 하였다.

(2) 속임 경로 공격 및 비인가된 노드추가 : 악의적인 노드는 자신의 MAC과 IP 주소를 정상적인 노드인 것처럼 스푸핑(Spoofing)하여 이웃노드에 대한 위장 공격 또는 비인가된 노드임에도 공식적인 멤버 추가 요청 등의 여러 가지 공격을 행할 수 있다. 그러나, DAMMC에서는 E_{CA_pub}(node_pub ‖ E_{pair_wise} (Msg))와 같이 초기 인증시 미리 분배된 상대키로 서명된 메시지와 자신의 공개키를 CA로 송신하여 CA로부터 개인키 확인 절차를 거쳐 자신이 정당한 노드임을 증명하는 인증서를 발급받게 됨으로 속임 경로 공격과 비인가된 노드의 추가가 차단될 수 있다.

(3) 재사용 공격 : 재사용 공격은 전자서명이나 인증서와 같은 암호화된 데이터를 주고받을 때 권한 없는 공격자가 이를 복사했다가 나중에 합법적인 이용자로 위장하는 공격이다. 제안된 DAMMC에서는 노드 인증 과정에서 노드와 CA가 송수신하는 메시지에 *nonce*와 타임스탬프(*time*)를 각각 포함시킴으로서 재사용 공격을 막을 수 있도록 설계하였다. 즉, 노드가 CA로 메시지 [E_{CA_pub}(node_pub ‖ E_{pair_wise} (Msg) ‖ nonce ‖ *time*)]를 송신하면, CA는 [E_{node_pub} (*nonce2*)] 메시지를 노드에 송신하여 정당한 노드인지를 확인하게 된다.

6. 결 론

본 논문에서는 클러스터 헤드가 CA 기능을 갖되 클러스터 간의 사용자가 정의한 *m*개의 계층을 두고 상위 클러스터가 하위클러스터를 인증하는 구조를 갖는 다중계층 클러스터 기반의 분산형 인증모델을 제안하였다. 여기서 클러스터 간 상호 신뢰는 공통의 상위 클러스터가 보장하게 되므로 각 클러스터들끼리 상호 인증의 오버헤드를 해결할 수 있다. 또한, 다중계층 클러스터 기반의 인증모델에서는 클러스터간의 효과적인 신뢰관계 구축을 위한 인증기법으로 CA의 인증 공개키를 클러스터 멤버들에게 나누어주고, CA가 인증서를 발행 할 때 각 노드들이 각자 자신이 가진 인증키 조각을 이용하여 partial certificate를 생성하고, 인증서를 발급 받는 노드는 partial certificate를 모아 완전한 인증서를 생성 할 수 있도록 한 비밀분산법을 사용하였다. 실험결과 제안된 인증프로토콜은 초기 인증에서의 인증발급 연산시간과 노드 추가에 따른 인증발급 연산시간에서 기존 인증프로토콜인 ARAN(Authenticated Routing for Ad hoc Network)과 AHCAN(Authentication using Hierarchical Cluster in Ad hoc Networks)보다 우수한 성능을 보였다. 보안성능에 있어서도 변형공격, 속임경로 공격 및 비인가된 노드 추가, 재사용 공격 등 3가지 공격기법으로부터 안전함을 확인하였다. 향후계

획으로는 본 논문의 실험환경이 250개의 비교적 적은 노드 수를 대상으로 수행되었기 때문에 향후에는 보다 많은 노드수를 적용하여 CA의 생성 레벨 m 값을 네트워크 규모에 맞게 적정하게 설정할 수 있는 정교한 기법연구를 수행할 예정이며 아울러, 우리가 제안한 알고리즘을 실제 Tiny-OS 기반 센서노드에 탑재하여 클러스터 헤드를 선정하는 알고리즘과 완전한 인증서를 생성하기 위한 멤버 노드의 분할인증서 임계값 t의 최적화에 대한 보완 연구도 수행할 계획이다.

참 고 문 헌

1. M. Bechler, H.-j. Hof, D. Kraft, F. Rahlke, L. Wolf, “A Cluster-Based security architecture for ad hoc networks,” in: Proceedings of IEEE Conference on Computer Communications (INFOCOM) Hong Kong, March. 2004.
2. K. Sanzgiri, B. Dahill, B.N. Levine, C. Shields, E.M. Belding-Royer, “A secure routing protocol for ad hoc networks,” in: Proceedings IEEE Network Protocols, pages 78-87, 2002.
3. Aldar C-F. Chan, “Distributed symmetric key management for mobile ad hoc networks,” in: Proceedings of IEEE Conference on Computer Communications (INFOCOM) Hong Kong, March. 2004.
4. 전자통신 동향분석 제20권 제1호 2005년 2월 센서 네트워크 보안 연구 동향.
5. Mathias Bohge, Wade Trappe, “An Authentication Framework for Hierarchical Ad Hoc Sensor Networks”, WiSE 2003.
6. Wenliang Du, Peng Ning, “An Efficient Scheme for Authenticating Public Keys in Sensor Networks”, MobiHoc 2005.
7. Ronald Watro, Derrick Kong, Sue-fen Cuti, Charles Gardiner, Charles Lynn and Peter Kruus TinyPK: Securing Sensor Networks with Public Key Technology.
8. M. Jiang, J. Li, and Y.C. Tay, “Cluster based routing protocol (CBRP),” functional specification, IETF Internet Draft, MANET working group, draft-ietf-manet-cbrp-spec-01.txt, Aug. 1999.
9. Ida Svejdarova “Threshold signature schemes”
10. Sunder Lal and Manoj Kumar “A Directed Threshold-Signature Scheme”
11. Jamil Ibriq, Imad Mahgoub “Cluster-Based Routing in Wireless Sensor Networks : Issues and Chanllenges”, SPECTS 2004.
12. Seema Bandyopadhyay, Edward J, Coyle “Minimizing Communication Costs in Hierarchically Clustered Networks of Wireless Sensors”, IEEE 2003.
13. Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan “Energy-Efficient Communication Protocol for Wireless Sensor Networks”, IEEE 2000.
14. Sencun.Z, Sanjeev.S, Sushil.J, “LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks,” CCS’03, 2004.8
15. Adi Shamir, How to share a secret, Communications of the ACM, 22:612-613, Nov. 1979.
16. E. Ayanoglu, C.-L. I, R. D. Gitlin, and J. E. Mazo. Diversity coding for transparent self-healing and fault-tolerant communication networks. IEEE Transactions on Communications, 41(11):1677-1686, Nov. 1993.
17. K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine, C. Shields, E. M. Belding-Royer, “Authenticated routing for Ad hoc networks,” IEEE Journal on Selected Area in Communications, Vol. 23, No. 3, pp. 598610, March 2005.
18. Keun-Ho Lee, Sang-Bum Han, Heyi-Sook Suh, SangKeun Lee, Chong-Sun Hwang, “Authentication Protocol Using Threshold Certification in Hierarchical-Cluster-based Ad hoc Networks”, Journal of Information Science and Engineering, 2006.

신 종 회 (jshin@kisa.or.kr)

1990 강원대학교 전자공학과 학사
2001 고려대학교 정보산업학과 석사
2007 고려대학교 컴퓨터학과 박사
2002～현재 한국정보보호진흥원 수석연구원

관심분야 : 무선네트워크, USN MAC, USN 라우팅, USN 보안

유 동 영 (ydy@kisa.or.kr)

1997 숭실대학교 전자계산학과 학사
2000 숭실대학교 컴퓨터학과 석사
2007～현재 고려대학교 컴퓨터·전파통신공학과 박사과정
2000～현재 한국정보보호진흥원 선임연구원

관심분야 : 무선네트워크, USN MAC, USN 보안, Formal Method

김 석 규 (sgkion@andong.ac.kr)

1990 연세대학교 전자공학과 학사
1992 연세대학교 전자공학과 석사
1997 연세대학교 전자공학과 박사
2007～현재 안동대학교 전자정보산업학부 교수

관심분야 : 무선네트워크, USN MAC, USN 라우팅, USN 보안