Journal of Security Engineering
Vol. 1, No. 1, August, 2005

무선 센서네트워크 환경에 적합한 클러스터 기반의 보안 프로토콜 구조

정윤수, 백승호, 황윤철, 이상호
충북대학교 전자계산학과
e-mail : {bukmunro, manitto,dolpin98}@netsec.cbnu.ac.kr, shlee@chungbuk.ac.kr

Cluster-Based Security Protocol Design for Wireless Sensor Network Environment

Yoon-su Jeong, Seung-ho Baek, Yoon-cheol Hwang and Sang-ho Lee
Department of Computer Science, Chungbuk National University

요 약

To achieve security in wireless sensor networks (WSN), it is important to be able to encrypt messages sent among sensor nodes. Due to resource constraints, many key agreement schemes used in general networks such as Diffie-Hellman and public-key based schemes are not suitable for wireless sensor networks. But, it is not efficient to find public-key because of the problem for time and energy consumption. Therefore, we propose a new cryptography management protocol, which is based on the clustering scheme but does not depend on probabilistic key. The protocol can increase efficiency to manage keys because, before distributing keys in bootstrap, using public-key shared among nodes can remove processes to send or to receive key among sensors. Also, to find out compromised nodes safely on network, it solves safety problem by applying a function of lightweight attack-detection mechanism.

1. 서론

컴퓨터와 통신기술의 최근 발전은 무선 센서 네트워크(WSN : Wireless Sensor Network)의 확대를 용이하게 하였다[7,8]. 그러나 WSN 은 고정된 인프라의 도움없이 이동 센서만으로 이루어지기 때문에 네트워크의 독립성과 융통성을 높일 수 있지만 이동 센서의 참여와 이탈이 자유로우므로 네트워크의 유지 관리에 어려움이 많다.

센서 노드가 위험 지역에 설치된 경우 보안성은 매우 중요하다. 예를 들면, 공격자는 쉽게 트래픽을 엿볼 수 있고, 주변 노드에게 잘못된 정보를 제공함으로써 네트워크 센서 노드로 흉내 낼 수도 있다. WSN 에 보안성을 제공하려면 통신이 암호화되고 인증되어야 한다. 이러한 문제는 센서 노드간의 안정적인 통신을 위하여 비밀키를 설정하도록 함으로써 부분적으로 해결가능하다[5].

안전한 통신을 위하여 일반적으로 네트워크를 대상으로 키 관리 방법에 대한 다양한 연구가 진행되어 왔다[1,2,3]. 첫째, 신뢰된 인증서버에 의하여 키를 분배받는 방법으로 이는 센서 네트워크와 같이 구조적인 기반 구조가 없는 환경에서는 적용이 어렵다[4]. 둘째, 공개키 인증서를 활용한 비대칭 암호화 방법으로 한정된 계산력과 에너지로 구성된 센서 노드에서 Diffie-Hellman 이나 RSA 방법을 적용하는 것은 바람직하지 않다[6]. 마지막으로 사전 키 분배 방식은 센서 노드를 배치하기 전에 키 정보를 미리 저장하는 것으로 모든 정보가 사전에 결정되어야 하나 센서 노드의 설치는 임의적으로 이루어지므로 이러한 많은 사전 지식을 보유하는 것은 어렵다[9].

따라서, 이 논문에서는 WSN 환경에서 사용하고 있는 센서간 사전 키 분배 방식의 문제를 키 재사용/추가에 유연성을 갖는 ID 기반 대칭 키 기법을 확장하여 해결하고 있다. 제안 기법은 부트스트랩 동안 사전 배치 전 센서간 공유한 공통키를 사용하여 센서의 키 전송/수용 과정을 제거하기 때문에 키 관리 측면에서 기존 기법보다 효율적이다. 또한 네트워크상에 존재하는 타협된 노드들을 탐지하기 위해 lightweigt 침입 탐지 메커니즘 기능을 적용함으로써 안전성 문제를 해결한다. 그리고 성능평가를 통해 노드 증가에 따른 오베헤드, 전체 센서 노드의 에너지 소비 현황과 클러스터당 소비되는 평균 통신 에너지 등을 평가한다.

이 논문의 구성은 다음과 같다. 2 장에서는 무선 네트워크 환경에서 지금까지 연구된 키 분배 방식

을 분석하고, 3 장에서는 이 논문에서 제안하는 클러스터 기반의 키 관리 프로토콜을 기술한다. 4 장에서는 시뮬레이션 환경과 제안 프로토콜에 대한 보안평가와 성능 평가 결과를 서술한다. 마지막으로 5 장에서 결론을 내린다.

2. 관련연구

2.1 확률적인 키 분배

확률적인 키 분배 방법과 랜덤 키 사전 분배 방법은 설치 전에 각 센서 노드가 대규모 키 풀로부터 부분 키 집합을 받는 것이다. 센서 노드들이 통신을 하기 위하여 임의의 두 노드는 그들의 키 집합 내에서 공통키를 찾고, 노드간 통신을 위한 공유키로 사용한다. Eschenauer-Gigor 기법을 기반으로 Chan, Perrig 그리고 Song 은 이들 방법에 q-composite 랜덤 키 사전 분배 방법을 적용하여 키 셋업에 대한 보안성을 강화하였다[10]. 그러나 이 기법은 센서 네트워크 특성을 고려하지 않고, 확률적으로 랜덤하게 키를 분배하므로 센서 노드간의 공유키가 존재하지 않을 가능성이 매우 높다. 또한 공유키가 존재하더라도 공유키를 발견하는데 소용되는 시간과 에너지가 많아 에너지 사용이 효율적이지 못하다.

SPINS 에서 각 센서 노드는 베이스스테이션과 함께 비밀키를 공유한다. 두 센서 노드들은 직접 비밀키를 만들지 못한다. 그러나 비밀키를 설정하기 위해서는 신뢰할 만한 제 3 자의 베이스스테이션을 사용해야 한다. Tatebayashi, Matsuzaki 그리고 Newma]. SPINS 에서 각 센서 노드는 베이스스테이션과 함께 비밀키를 공유한다. 두 센서 노드들은 직접 비밀키를 만들지 못한다.

2.2 클러스터 기반의 메시지 인증 방법

[10]에서는 두 통신 주체사이에 키를 공유하기 전에 클러스터 헤드가 자신의 멤버 호스트들을 대신하여 인증을 수행하는 방법이 제안되었다. 이 방법에서는 임의의 두 클러스터 헤드가 각자 상대편 클러스터 헤드의 공개키를 이용하여 상호인증을 수행한다. 따라서 클러스터 헤드의 공개키가 먼저 모든 클러스터 헤드에 분배되어 있어야 한다. 클러스터 헤드 간 인증 후에 대칭키 기반의 세션키가 분배되고, 이는 다시 통신주체인 멤버 호스트에게 분배된다.

이 방법은 클러스터 헤드들이 자신의 공개키를 모든 클러스터 헤드에게 분배해야 하므로 통신 오버헤드가 크다. 또한 두 멤버 호스트간 비밀키인 세션키 분배 시 헤드의 개인키로 암호화되어 해당 노드에 분배함으로써 세션키가 클러스터내의 모든 호스트들에게 노출 될 수 있다.

2.3 ID-based threshold cryptography

Khalili 는 ID 기반 암호화 기법의 편리성과 효율성, 임계치 암호화 기법의 유연성 및 안전성의 이점을 결합하여 Ad Hoc 네트워크에서 각 노드의 공개키와 개인키를 생성하는 기법을 제안하였다. 이 방식은 노드가 네트워크에 참여할 때 공통적으로 분배받는 마스터 공개키와 공개되어 있는 호스트의 ID 로 해당 노드의 공개키를 유도하고 임계 개수만큼 주변 노드들로부터 ID 에 해당하는 부분 개인키를 얻어내어 완전한 개인키를 획득한다. 그러나 이 방식은 비밀키를 요청하는 주체를 분명히 인증하지 못하므로 중간자 공격에 매우 취약하다.

3. 클러스터 기반의 효율적인 키 관리 프로토콜 설계

이 논문에서 제안하고 있는 클러스터 기반의 키 관리 프로토콜은 대칭키 방식을 사용하고 있으며, 무선 센서 네트워크를 위한 위치 알고리즘으로 프로토콜을 표현한다.

3.1 가정

① 키 관리 동작 동안에 각 센서는 게이트웨이와 직접 통신한다.

② 센서 네트워크에 대한 악의 노드의 침입을 탐지하거나 노드의 작업표시를 표시할 수 없어도 침입탐지의 기능은 명령노드에서 이용 가능하다.

③ 센서와 게이트웨이는 임의로 분배하고 배치 전에는 망에 대한 정보를 알지 못한다.

3.2 프로토콜

이 논문에서 제안한 키 관리 프로토콜의 목적은 높은 에너지를 가지는 게이트 노드들간에 효율적으로 센서 네트워크를 클러스터 하는데 있다. 제안 프로토콜은 센서 네트워크의 생명주기 동안 키 분배/추가/폐기/갱신 등의 4 개 하부 프로토콜이 수행된다. 각각의 세부적인 하부 프로토콜 접근방법은 키 관리와 관련있는 확장성 있는 계산을 수행하거나 키를 생성하는 센서를 호출하는 기능을 한다.

3.2.1 키 분배

키 분배는 비밀키 메커니즘을 이용하고, 사전분배 방식을 통해 사전에 2 개의 키를 센서에 저장한다. 센서에 저장된 키 중 하나는 게이트웨이와 공유하고 다른 하나는 명령(command) 노드와 공유한다. 일반적으로 센서들은 신뢰적이지 못하고 메모리 소비가 있어 적은수의 키만이 센서에 저장되지만 이런 점이 네트워크 보안에는 잇점이 된다.

게이트웨이는 메모리 자원이 풍부하고 많은 키를 저장할 수 있지만 게이트웨이를 완전히 신뢰할 수는 없다. 게이트웨이에 할당된 모든 키들은 전체 네트워크뿐만 아니라 단일 게이트에서 타협된다. 명령 노드는 안전하다고 가정하고 충분한 메모리를 가지고 있어 네트워크의 모든 비밀키들을 저장할 수 있다. 그리고, 센서키는 사전에 센서에 분배되도록 센서 메모리에 프로그램된다. 센서에 저장된 키들은 플래쉬 RAM 에 저장될 수 있고 필요에 따라서는 지울 수 있다. [표 1]은 프로토콜의 기술

에 사용하는 주요 용어를 기술한 것이다.

[표 1] 프로토콜 주요 용어

개 념	설 명
C	명령 노드
G_i	게이트웨이 i
S_i	센서 노드 i
G	전체 게이트웨이
S	전체 센서노드
id_i	노드 인식 i
nonce	랜덤 난수 값
sdata	센서 위치 및 에너지 레벨 데이터
$E_k()$	키 K를 사용한 대칭 암호 함수
$\|$	연계 동작자
G_h	복구에 사용될 헤드 게이트웨이

3.2.2 초기구문

분배 기간에 각 게이트웨이는 임의로 |S|/|G|개의 키를 할당받는다. 각 게이트웨이는 클러스터 형성 알고리즘을 사용하여 클러스터를 형성하고 다른 게이트웨이로부터 클러스터 내에 있는 센서 키를 요구한다. 게이트 레벨에서 키가 교환 된 후 각 게이트웨이는 클러스터 내에 있는 센서의 키를 유지하고 나머지 키들은 제거한다. 이것은 게이트웨이가 수집한 클러스터의 키가 적에게 이용될 수 있기 때문에 초기구문에서는 필수적인 과정이다.

초기 구문 프로토콜의 동작과정은 다음과 같다.

① $S_i \rightarrow S$

$id_{S_i} \| id_{G_i} \| E_m$ [sdata||nonce|| k_c^t ||h(k_c^t ||sdata)]

각 센서는 공유된 키를 얻기위해서 게이트웨이의 식별번호와 함께 사전 로드(preload)된다. 'hello' 메시지에 식별번호를 포함한 센서는 배치후에 브로드캐스트한다.

② 클러스터링 과정

③ $G_i \rightarrow G$

$id_{G_i} \| E_{K_m}$ [nonce||{ k_c^t, id_i }||h($k_c^t \| id_i$)]

클러스터 형성후에 각 G_i는 클러스터에 위치한 센서 설정 { k_c^t, id_i }를 표시하고 다른 게이트웨이에게 브로드캐스트한다. 브로드캐스트는 게이트웨이간 트래픽의 볼륨을 줄이는데 도움을 준다.

④ $G_i \leftarrow G_j$

E_{K_m} [nonce||($k_c^t, \{id_{S_k}\}_i$)] || ticket

각 G_j는 키 설정 $k_c^t, \{id_{S_k}\}_i$와 함께 G_i와 교체된다. 그리고, 게이트웨이를 인식하기 위해 티켓(ticket)을 부여하여 전송한다. 이때, 티켓을 이용하는 것은 네트워크에 존재하는 타협된 노드들을 안전하게 탐지할 수 있는 역할을 하면서 lighweight 침입탐지 기능도 포함하고 있기 때문에 무선 네트워크의 안전성 문제를 해결하고 있다. 키 설정 중 $\{id\}_i$는 $\{id\}_j$의 하위 설정값이다.

⑤ $S_i \leftarrow G_i$

$id_{G_i} \| E_m$ [nonce|| id_{G_i} || k_c^t ||msg||h(k_c^t ||msg)] ||ticket

게이트웨이 G_i의 클러스터에 있는 각 센서 S_l은 게이트웨이 G_i에 할당하여 로부터 메시지를 수신한다.

3.2.3 센서 추가

네트워크에 추가되는 새로운 센서는 인위적으로 배치된다. 이 센서들은 클러스터에 미리 할당되지는 않지만 다른 센서와 동일하게 두개의 키를 미리 저장한다. 명령 노드는 새로 추가되는 센서의 키를 게이트웨이가 공유할 수 있도록 임의의 게이트웨이 G_H에 (identifier, key)쌍의 리스트를 전송한다. G_H는 전체 게이트웨이 그룹이 아니며 타협의 위험을 줄이기 위해 사용된다.

3.2.4 폐기, 철회

키 철회(노드 폐기)는 타협노드를 탐지한 후에 수행되며 침입탐지 메커니즘은 타협노드의 명령 노드에게 통보한다. 센서 그룹이 타협(compromised)된다면 게이트웨이에서 클러스터까지 명령 노드의 센서 리스트를 제거한다. 게이트웨이 (G_j) 키의 철회의 경우 명령 노드는 G로부터 G_j를 제거하고 타협하지 않은 헤드 게이트웨이 G_h를 선택한다. 선택된 G_h에는 센서간 새로운 게이트웨이 G_i의 식별번호와 G_i와 공유된 새로운 키를 보낸다. 또한, 새로운 게이트웨이-센서 비밀 키는 그룹 브로드캐스트를 통해 G_i에게 보낸다. 이런 과정 후에 재 클러스터링 단계를 수행한다.

3.2.5 키 갱신

확장기간동안 동일한 암호키를 사용하는 것은 암호학적 위험을 초래할 수 있다. 센서 전지가 빨리 소모되는 네트워크에서는 센서전지의 복구가 위협으로부터 적당히 무시될 수 있다[21]. 경우에 따라서는 다른 네트워크를 위해 암호 키를 새로 만들 필요가 있다[19]. 센서 키의 갱신을 수행하기 위해 명령 노드는 새로운 키를 생성하고 철회와

같은 경우가 발생할 경우 게이트웨이에게 키를 넘긴다. 연속적인 갱신이 이루어지는 동안에 시간 간격은 데이터 트래픽 볼륨, 암호학적 이론의 길이 그리고 게이트웨이에서 발생하는 여분의 처리 로드에 의존한다.

4. 클러스터 기반의 효율적인 키 관리 프로토콜 설계

4.1 환경설정

제안 프로토콜은 [표 2]의 실험 시나리오를 통해 임의적으로 생성되는 모델을 사용한다

[표 2] NS-2 실험 시나리오

노드의 수(Nodes number)	1000
크기(Scene)	1000m × 1000m
초기 에너지값(Initial energy)	0.5 joules
무선 범위(Wireless range)	200 m
버퍼(buffer)	50 packet
소스 수(Number of sources)	10
트래픽(Traffic)	4 pkts/s

실험에서 설정된 센서 필드의 크기는 1,000 m^2 이며 센서 노드의 개수는 1000 개이다. 소스 노드는 초당 1 개의 데이터 패킷을 싱크 노드에게 전송한다. 셀 사이즈는 200 m^2 으로 설정하고 600 초 동안 실험을 수행한다. 그리고 각 센서의 초기에너지는 0.5 줄(Joule)의 에너지를 가지는 것으로 가정하고 버퍼의 크기는 50 패킷의 크기를 가진다. 만약 노드의 에너지 레벨이 0 줄이 되면 노드는 동작되지 않는다.

각 패킷은 패킷 전송동안 매 패킷 에너지를 계산하기 위해 업데이트되는 에너지 필드를 가지며, 이때 패킷 드롭 확률은 0.01 과 같다. 이것은 실제 상황에 맞는 시뮬레이션을 만들기 위해서 사용되고 활동적인 에너지로부터 게이트 에너지 모델의 유추를 시뮬레이트하기 위해 사용된다.

4.2 성능 측정규준(Performance Metrics)

성능 측정규준은 실험에 사용된 제안기법의 성능평가를 측정하는데 사용한다.

① 라우팅 오버헤드

네트워크에서 타협된 노드와 노드의 라우팅 오버헤드 사이의 관계를 정의한다. 비록 효율적인 에너지 관리가 필요할지라도 몇몇 센서 네트워크 미션에서는 민감성이 떨어진다.

② 네트워크 처리량

시뮬레이션 시간에 따른 게이트웨이에 도착한 패킷 전송비율로써 정의한다.

③ 클러스터당 소비되는 평균에너지

클러스터당 소비되는 평균통신 에너지로 정의한다. 그리고, 일반적으로 에너지를 최소화하는 라우팅 알고리즘은 에너지 저장이 더 좋은 분야이다.

4.3 성능평가

이 절에서는 센서 노드 수의 변화에 따른 평균 통신 에너지, 오버헤드, 센서 노드의 에너지 소비 비율등을 시뮬레이션을 통해 분석한다.

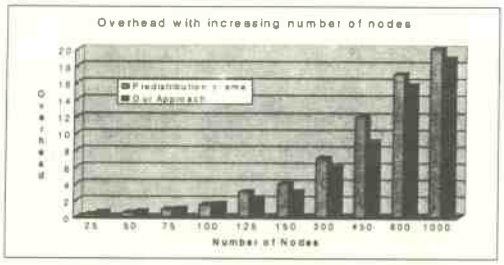
4.3.1 안전성 분석

{IP address, key} 묶음 보안은 비밀키 암호 알고리즘 보안과 해쉬함수의 두 번째 사전 이미지 저항(second pre-image resistance) 속성에 의존한다. 이러한 두 가지 가정은 센서 네트워크 환경에서 매우 실용적이다. 예를 들어 비밀 키 암호시스템은 제안 시스템의 보안 요구사항에 효과적이다. 더욱이 MD5 나 SHA-1 이 판독되는 두 번째 사전 이미지 저항과 64 비트의 출력을 가지는 해쉬함수는 공격자가 주어진 IP 지역의 두 번째 비밀키를 찾기위해 평균 2^{62}번 시도한다.

이러한 작업은 공격자가 빠른 작업처리를 하지 못하게 할 뿐만 아니라 공격자가 시도한 비밀키에 대해 인위적인 추측이 불가능하다. 만약 공격자가 해쉬함수 입력에 대한 추측을 한다면 두 번째 pre-image resistant 해쉬함수를 빠르게 처리하여 실제 공격자가 사용하지 못하도록 한다.

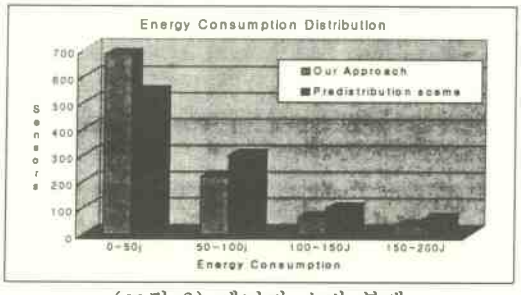
4.3.2 효율성 분석

(그림 1)은 노드 증가에 따른 트래픽 오버헤드를 평가한 결과이다.



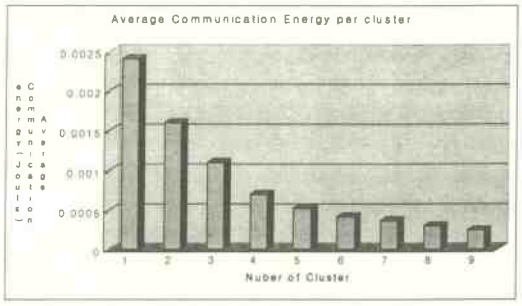
(그림 1) 노드 증가에 따른 오버헤드

이 결과에서 보면 사전분배 방식이 제안기법보다 오버헤드가 평균 1.5%씩 높게 나타났다. 이것은 전체 트래픽 오버헤드 측면에서 볼 때 사전분배 방식이 제안기법보다 평균 0.33% 높은 트래픽 오버헤드를 가진다.



(그림 2) 에너지 소비 분배

(그림 2)는 실험에 사용된 1000 개 센서들의 에너지 소비 비율을 나타내고 있다. (그림 2)의 결과는 게이트웨이의 밀집상태와 수행상태에 따라 평균 에너지 소비가 다르다. 특히 사전분배 방식은 시간이 지남에 따라 처리해야 할 데이터가 늘어나기 때문에 제안 기법보다 많은 에너지를 소비하는 노드들이 필요하다.



(그림 3) 클러스터당 평균 통신 에너지

[그림 3]은 클러스터 내의 게이트웨이와 모든 센서 사이의 통신으로부터 요구된 평균 통신 에너지를 측정한 결과이다. 통신 에너지는 직접적으로 두 노드 사이의 거리에 비례적이다. 그러나 클러스터 수의 증가에 따른 평균 통신 에너지 비율은 반비례적이다.

5. 결론

무선 센서 네트워크 환경에서는 센서 노드간에 전송되는 메시지를 암호화하고 인증하는 것이 매우 중요하다. 이 논문에서는 무선 센서 네트워크 환경에서 센서간 사전키 분배 문제를 해결하기 위하여 확률적 키에 의존하지 않는 새로운 키 관리 프로토콜을 제안하였다. 제안 프로토콜은 센서의 키 전송/수용 과정을 제거하였기 때문에 키 관리 측면에서 효율적이며, lightweight 침입탐지 메커니즘 기능을 프로토콜에 적용하여 노드의 안전성 문제를 해결하였다.

그리고, 성능평가를 통해 기존기법과 트래픽 오버헤드를 평가한 결과 제안기법이 사전 분배방식보다 0.33% 낮게 나타났다. 이런 결과는 네트워크 크기로 인해 노드수가 선형적으로 증가하지 않으며 시뮬레이션에 사용된 트래픽이 서로 다르기 때문이다.

앞으로 제안 기법에 센서노드의 중복 비용 부분을 함께 접목시키는 방안과 재클러스터링을 통하여 헤드노드 결함문제를 해결하는 대표적 알고리즘인 LEACH(Low Energy Adaptive Clustering Hierarchy)를 개선하는것 등에 대한 연구가 필요하다.

참고문헌

[1] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "Spins: Security protocols for sensor networks," in Proceedings of the 7th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom), Rome, Italy, July 2001, pp. 189- 199.

[2] W. Fumy and P. Landrock, "Principles of key management," IEEE Journal of Selected Areas in Communications, vol. 11, pp. 785-793, June 1993.

[3] T. Dimitriou, I. Krontiris, and F. Nikakis, "Key establishment in sensor networks with resiliency against node capture and replication," December 2003. Submitted to 5th ACM Symposium on Mobile Ad Hoc Networking and Computing, (MobiHoc) 2004.

[4] B. C. Neuman and T. Tso, "Kerberos: An authentication service for computer networks," IEEE Communications, vol. 32, no. 9, pp. 33- 38, September 1994.

[5] R. L. Rivest, A. Shamir, and L. M. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120- 126, 1978.

[6] W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. 22, pp. 644- 654, November 1976.

[7] M. Horton, et al., "Mica: The commerciatlization of microsensor motes," Sensors Online Magazine, April 2002.
http://www.sensorsmag.com/articles/0402/40/main/shtml

[8] W. Heinzelman, A. Chandrakasan, H. Balakrishnan, "Energy Efficient Communication protocol for Wireless Microsensor Networks," Proceedings of the 33rd Annual Hawaii International Conference on System Sciences, pp. 3005-3014, Jan. 2000.

[9] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," in Proceedings of the 9th ACM conference on Computer and communications security, Washington, DC, USA, November 18-22 2002, pp. 41- 47.

[10] T. Dimitriou, I. Krontiris, and F. Nikakis, "Key establishment in sensor networks with resiliency against node capture and replication," December 2003. Submitted to 5th ACM Symposium on Mobile Ad Hoc Networking and Computing, (MobiHoc) 2004.

저자소개

정윤수(Jeong Yoon Su)

1998 년 청주대학교(이학사)
2000 년 충북대학교 대학원 전자계산학과 (이학석사)
2003 년 ~ 현재 충북대 전기전자컴퓨터공학부 전자계산학과 박사과정 수료

관심분야 : 암호이론, 암호알고리즘, 정보보호, Network Secu-rity, 이동통신보안, 전자상거래보안

백승호(Baek Seung Ho)

2003 년 ~ 현재 충북대 전기전자컴퓨터공학부 전자계산학과 석사과정

관심분야 : 침입탐지, 정보보호, Network Security

황윤철(Hwang Yoon Cheol)

1994 년 한남대학교 전자계산공학과
1996 년 한남대학교 전자계산공학과(공학석사)
1999 년~현재 충북대 전기전자컴퓨터공학부 전자계산학과 박사수료

관심분야 : 인터넷, 정보보호, Network Secu-rity

이상호(Lee Sang Ho)

1976 년 숭실대학교 전자계산학과 졸업
1981 년 숭실대학교 전자계산학과 (MS)
1989 년 숭실대학교 전자계산학과 (PHD)
1976 년 ~ 1979 년 한국전력 전자계산소
1981 년 ~ 현재 충북대학교 전기전자컴퓨터 공학부 & 컴퓨터 정보통신연구소교수
관심분야 : Protocol Engineering, Network Security, Network Management, Network Architecture