한국시뮬레이션학회 논문지
Vol. 18, No. 3, pp. 133-138 (2009. 9)

인터리브드 멀티홉 인증을 적용한 무선 센서네트워크에서 퍼지로직을 이용한 서비스 거부 공격에 대한 방어 기법

김종현[1] · 조대호[1†]

Interleaved Hop-by-Hop Authentication in Wireless Sensor Network Using Fuzzy Logic to Defend against Denial of Service Attack

Jong-Hyun Kim · Tac-Ho Cho

ABSTRACT

When sensor networks are deployed in open environments, an adversary may compromise some sensor nodes and use them to inject false sensing reports. False report attack can lead to not only false alarms but also the depletion of limited energy resources in battery powered networks. The Interleaved hop-by-hop authentication (IHA) scheme detects such false reports through interleaved authentication. In IHA, when a report is forwarded to the base station, all nodes on the path must spend energies on receiving, authenticating, and transmitting it. An dversary can spend energies in nodes by using the methods as a relaying attack which uses macro. The Adversary aim to drain the finite amount of energies in sensor nodes without sending false reports to BS, the result paralyzing sensor network. In this paper, we propose a countermeasure using fuzzy logic from the Denial of Service(DoS) attack and show an efficiency of energy through the simulataion result.

Key words : Wireless Sensor Network, IHA, Fuzzy Logic, DoS

요 약

무선 센서 네트워크는 열린 환경에 배치되기 때문에 노드는 공격자들로부터 포획당하고 허위 보고서를 삽입 될 수 있다. 허위 보고서 삽입 공격은 허위 경보를 유발할 뿐만 아니라 네트워크의 제한된 에너지를 고갈 시킨다. Interleaved hop-by-hop authentication(IHA)은 인터리브드 검증을 통하여 허위 보고서를 탐지하는 기법이다. 하지만 모든 센서 네트워크에서와 같이 IHA에서도 보고서를 BS로 전달 할 때 모든 전송 노드들은 보고서를 송/수신, 인증만으로도 에너지를 소비한다. 공격자는 이것을 이용함으로써 허위 보고서 배포 목적이 아닌 단지 에너지 소비만을 유도하여 결과적으로 네트워크의 마비를 초래하는 것을 목표로 서비스 거부 공격을 한다. 본 논문에서는 이러한 서비스 거부 공격에 대응하기 위하여 퍼지 로직 시스템를 이용하여 허위 보고서 재전송 공격을 방어하는 기법을 제안한다. 그리고 시뮬레이션을 통해 기존의 기법과 제안한 기법을 비교하여 에너지 효율성을 증명한다.

주요어 : 무선 센서 네트워크, IHA, 퍼지로직, 서비스 거부 공격

1. 서 론

최근 마이크로 전자장치시스템과 무선 통신 기술의 발전은 저비용, 저전력, 다기능을 갖춘 센서 네트워크 발전을 가져왔다. 이러한 무선 센서네트워크(wireless sensor network; 이하 WSN)의 발전은 군사, 의료, 환경 등에서 응용이 실현 가능하게 되었다. WSN는 수 많은 센서노드들이 조밀하게 배치되어 있고 이러한 센서 노드들은 감지, 데이터 처리, 그리고 통신으로 구성되며 무선 센서 노드는 오직 제한된 전력 자원으로 이루어져 있으므로. 센서 노드 생존기간은 배터리 생존기간과 강하게 의존된다[1].

WSN에서 센서 노드들은 일반적으로 열린 환경에서 독립적으로 동작하기 때문에 보안 공격에 취약하다[2]. 만

* 이 논문 또는 저서는 2008년 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임 (KRF-2008-313-D00827).

2009년 6월 30일 접수, 2009년 9월 8일 채택

[1] 성균관대학교 정보통신공학부
주 저 자 : 김종현
교신저자 : 조대호
E-mail; taecho@ece.skku.ac.kr

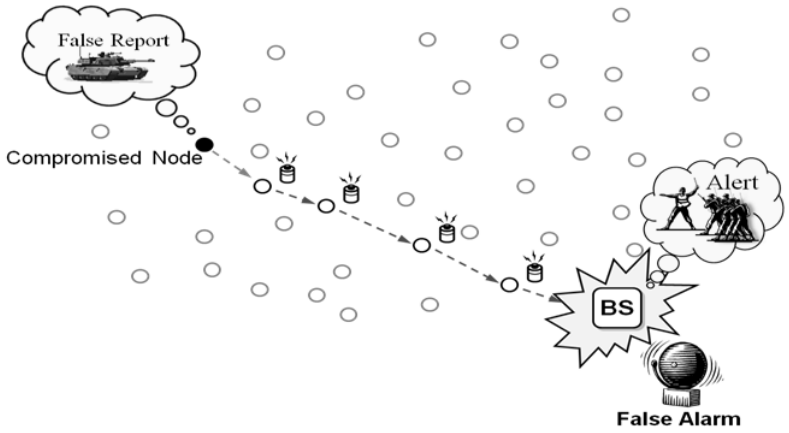


그림 1. 허위보고서 삽입 공격

약 공격자가 노드를 포획하여 허위 정보를 담은 허위 보고서(false report)를 생성해서, 이 허위 보고서를 공격자에게 포획 당한 노드를 통해 센서 네트워크에 삽입할 수 있다. 이 허위 보고서 공격은 그림 1과 같이 허위 보고서를 베이스 스테이션(base staion 이하 BS)에 전달함으로써 허위 경보(false alarm)을 유발시킬 수 있을 뿐 아니라, 센서 노드들의 제한된 에너지 자원을 고갈시킨다. 이는 센서 네트워크 전체 수명을 단축시켜 네트워크 기능의 마비를 초래하게 된다[4]. 허위 보고서의 피해를 최소화하기 위해서는 가능한 빨리 허위 보고서를 전송 중에 탐지고 폐기되어야 하며, 폐기되지 않은 허위 보고서는 BS에서 탐지하고 폐기 되어야 한다[3]. 허위 보고서 삽입 공격을 방어하기 위해 다양한 기법들[4-7] 이 제안되었다.

Interleaved hop-by-hop authentication(이하 IHA) 기법은 노드에서 감지된 이벤트 보고서를 전달 노드를 통해 전달 중 허위 보고서를 탐지 및 폐기할 수 있는 기법 중 하나이다. 그러나 모든 센서 네트워크에서와 같이 IHA에서도 보고서를 BS로 전달 할 때 모든 전달 노드들은 보고서를 송/수신, 인증만으로도 에너지를 소비한다[8]. 이러한 특성을 이용하여 공격자는 허위 보고서가 탐지되어 폐기되어도 상관하지 않고, 단지 허위 보고서를 인증하고, 송/수신 하여 센서 노드의 에너지 소모를 목적으로 허위 보고서를 재전송하는 DoS(Denial of Service)공격을 시도한다.

본 논문은 이러한 허위 보고서 재전송 공격을 방어하기 위해 퍼지 로직 시스템을 이용하여 전송 노드에 보고서에 대한 인증 및 수신하는 것을 제한하는 기법으로써 에너지 소모를 줄일 수 있는 방안을 제시한다.

본 논문은 다음과 같이 구성된다. 2장에서는 배경이론으로 IHA의 개념 및 동작원리와 동기에 대해 설명하며 3장에서는 퍼지기반 경계 값 결정기법을 기술한다. 마지막으로 4장에서는 결론 및 향후과제에 대해 언급한다.

2. 배경이론 및 동기

2.1 Interleaved hop-by-hop authentication scheme

이 장에서는 IHA기법의 동작원리를 설명한다. IHA는 노드의 초기화 및 배치(node initialization and deployment), 연합 노드 발견(association discovery), 리포트 서명(report endorsement), 그리고 여과 단계(en-route filtering) 4가지 단계로 구성된다.

- **노드의 초기화 및 배치**

키 서버에 모든 노드 u에 대해서 각 노드의 ID 와 각각의 Ku를 적재한다. 노드 u가 배치되어진 후, 각 노드는 하나의 홉에 이웃노드를 발견하고 그 이웃 노드들과 각각 페어와이즈(pairwise) 키가 생성된다. IHA는 LEAP을 사용하여 한 홉의 페어와이즈 키를 생성한다[11].

- **연합노드 발견**

각 노드는 그 노드와 연합된 노드들의 ID들 찾는다. 각 노드는 t + 1 홉수 만큼 떨어진 페어와이즈 키를 공유하는 연합된 상위노드와 하위노드를 갖는다. t는 파라미터를 나타낸다. 각 클러스터는 센서노드 t + 1를 갖는다. 예를들어, 그림 2를 보면 t = 3이다. u3은 4홉 떨어진 상위 연합 노드(upper associated node) u7를 선택하고, 하위 연합 노드(lower associated node) v3를 나타낸다.

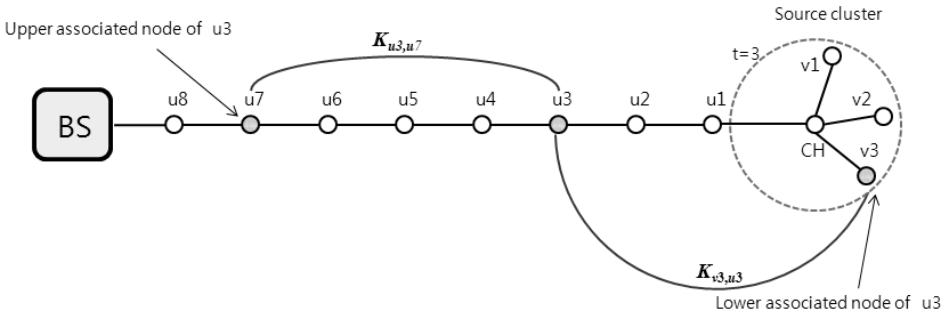


그림 2. IHA에서의 연합된 상위노드와 하위노드

• **리포트 서명**

이벤트가 발생되면, t + 1 클러스터 노드들은 협력하여 두 종류의 메시지 인증 코드(message authentication code 이하; MAC)들을 계산하여 보고서를 생성한다. 하나는 BS와 공유된 키를 사용한 MAC 그리고 상위 연합 노드와 공유된 페어와이즈 키를 사용하여 MAC을 생성한다. 그리고 생성된 보고서는 BS쪽으로 전달된다.

• **여관단계**

이벤트를 탐지하고 생성된 보고서는 BS로 전달되어진다. 중간 노드가 보고서를 받았을 때, 다음 절차를 통하여 인증을 통하여 확인한다. 연합된 하위 노드와 공유된 페어와이즈 키를 사용한 페어와이즈 MAC을 계산한다. 다음 보고서에 첨부된 첫 번째 페어와이즈 MAC과 새로 생성된 MAC을 비교하고 인증이 되었다면 연합된 상위 노드와 공유된 키를 사용하여 다른 MAC을 생성하고 보고서에 첨부해서 BS쪽으로 전달한다.

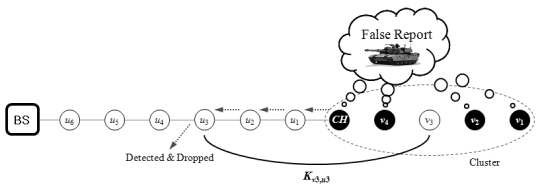


그림 3. 허위보고서 탐지 및 폐기

만약 그림 3과 같이 v3노드를 제외한 나머지 노드가 포획된 후 허위보고서를 전달하여도 v3는 포획당하지 않았기 때문에 전달 노드 u3에서 MAC을 비교하여 탐지 및 폐기된다.

2.2 동기

IHA는 비록 허위 보고서를 여과 하는데 매우 효율적이라도 여전히 결점은 남아 있다. 센서 네트워크에서 보고서를 BS로 포워드 할 때 모든 전송 노드들은 보고서를 송/수신, 인증만으로도 에너지를 소비한다. 공격자는 이러한 특성을 이용한다. IHA에서 허위 보고서가 탐지되고 인증하여 폐기 되어도 공격자는 MAC을 인증함으로써 사용된 에너지를 목표로 한다. 그림 4와 같이 공격자는 계속 허위보고서를 이용한 재전송 공격을 하여 노드의 에너지를 고갈시켜 결국 센서 네트워크를 마비시킬 수 있다.

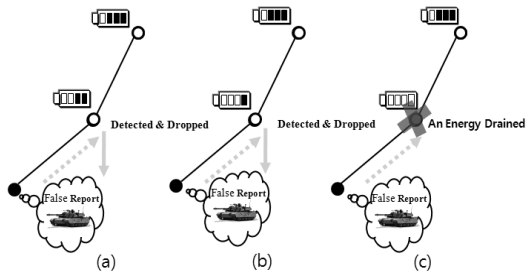


그림 4. 허위보고서 재전송 공격에 따른 노드의 에너지 고갈

3. 퍼지 기반 경계 값 결정 기법

3.1 가정

각 노드들은 배치 후 여러 개의 클러스터로 구성되어진다고 가정한다. CH는 노드 간의 에너지 균형을 위해서 순차적으로 교대되어진다. BS는 클러스터 내의 노드 수를 알 수 있고, 방송 메시지를 인증할 수 있는 메카니즘을 가지고 있으며, 각 노드들은 이를 검증 할 수 있다고 가정한다[6]. 또한 BS는 물리적 공격으로부터 안전하다고 가정한다.

3.2 개요

본 논문에서는 허위 보고서에 대한 재전송 공격을 방어

하기 위해 IHA내에 퍼지 로직 기반 시스템을 적용하였다. 퍼지 로직은 1960년대 중반 Lotfi-Zadeh[12]이 소개하였고 오직 참 그리고 거짓만을 선택할 수 있는 디지털 장치의 특성을 보안하기 위한 기법으로 IF-THEN 규칙을 통하여 명확하게 이분화되지 않는 상황에서 적절한 결과 값을 도출해내기 위한 방법 중 하나이다[13]. 노드가 같은 노드에서 또 다시 허위보고서가 재전송되면 퍼지를 이용하여 입력 값 노드의 에너지 잔여량(이하 NEL), MAC인증 실패 횟수(이하 FMC), 수신된 보고서 횟수(이하 RRC)를 도출된 보안 경계 값(이하 ST)이 BS로 전달되고 BS는 모든 노드들에게 방송한다. 각 노드는 ST값으로 허위보고서 재전송 공격을 당하면 인증을 안거치고 바로 허위 보고서를 무시함으로써 에너지 소모를 줄일 수 있다. 또한 인증을 하지 않더라도 보고서를 받는 자체만으로도 에너지 소모가 되므로 계속 적인 허위 보고서를 보내면 퍼지를 이용하여 공격 받는 노드를 강제로 대기모드로 전환시킨다.

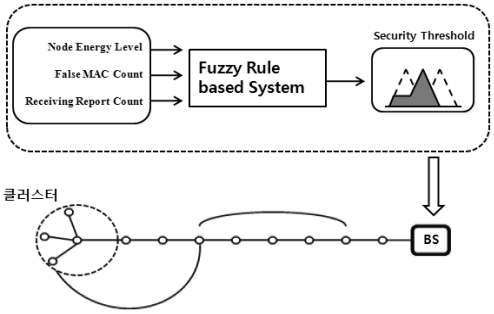


그림 5. 제안된 퍼지 기반 기법의 개요

3.3 퍼지 논리 설계

다음 그림은 제안된 퍼지 로직 시스템의 입력 값 3가지(NEL, FRC, RRC)에 대한 멤버쉽 함수이다.

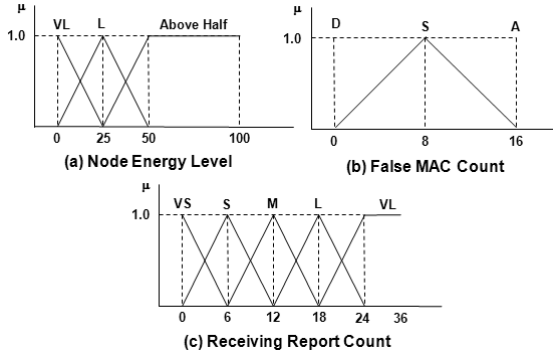


그림 6. 퍼지 입력 값 멤버쉽 함수

다음은 퍼지 입력 변수들의 명칭을 나타낸다.

- NEL = { Very Low, Low, Above Half }
- FMC = { Small, Medium, Large }
- RRC = { Very Small, Small, Medium, Large, Very Large }

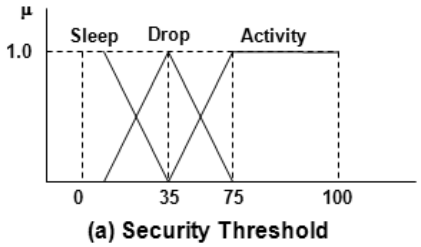


그림 7. 퍼지 출력 값 멤버쉽 함수

그림 7은 제안된 퍼지 로직 시스템의 출력 값을 나타내며, 각 명칭들은 다음과 같다.

- ST = { Activity, Drop, Sleep }

다음은 퍼지 규칙들의 일부이다. 기본적으로 퍼지 규칙 시스템은 NEL를 기반으로 ST를 결정한다.

RULE 3 : IF Node Energy Level is Very Low
AND False MAC Count is Small
AND Receiving Report Count is Small
Then Security Threshold is Activity

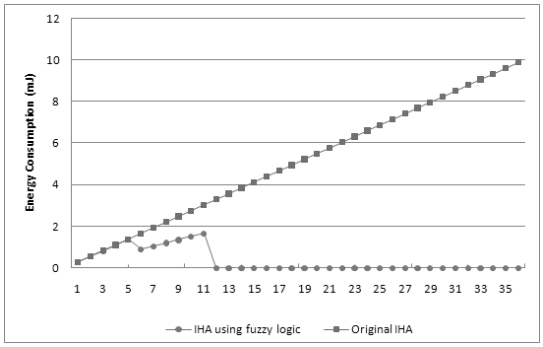
RULE 12 : IF Node Energy Level is Low
AND False MAC Count is Large
AND Receiving Report Count is small
Then Security Threshold is Drop

RULE 24 : IF Node Energy Level is Above Half
AND False MAC Count is Very Large
AND Receiving Report Count is Large
Then Security Threshold is Sleep

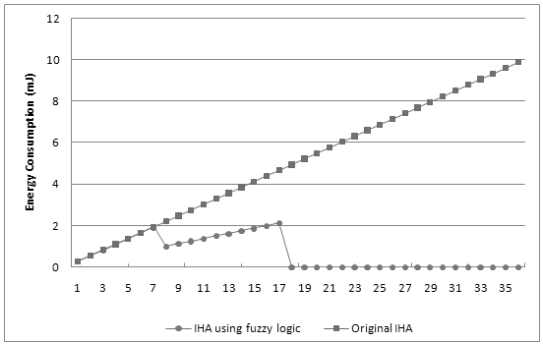
4. 시뮬레이션 분석

제안 기법의 에너지 효율성을 증명하기 위해 허위 보고서를 이용한 재전송 공격에 따른 기존 IHA에서와 퍼지를 적용한 IHA의 에너지 효율성을 비교한다. 각 노드는 송수신에너지로 각각 16.25μJ, 12.5μJ를 소모한다고 가

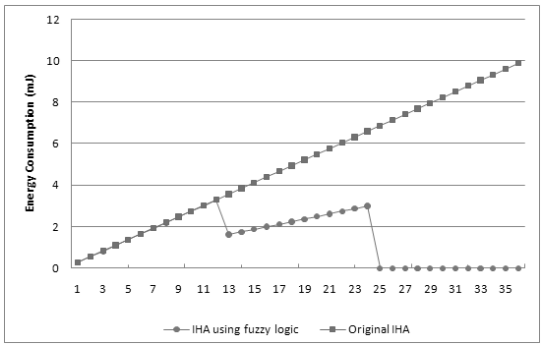
정했으며, 보고서 검증을 위해서 소비되는 에너지는 15μJ이다[11]. 최초 전송 메시지 크기는 24byte이고, MAC은 1byte이다. 그림 8은 재전송 공격에 기존의 IHA와 퍼지를 입력한 IHA의 시뮬레이션 결과이다. 그림 8(a), (b), (c)는 노드의 에너지 잔여량을 다르게 하여 허위 보고서 재전송 수에 따른 에너지 소모를 보여준다. 그림 8을 보면 IHA에서 허위 보고서를 폐기 하여도 인증 에너지와



(a) NEL 25% 미만



(b) NEL 25%~50%



(c) NEL 50%이상

그림 8. 노드 에너지 잔여량에서 허위 보고서 재전송 수에 따른 에너지 소비량 측정

수신에너지가 계속 적으로 소모되는 것을 볼 수 있다. 결국 노드는 에너지가 고갈되어 네트워크의 마비를 초래할 수 있다. 그러나 퍼지로직을 이용 할 경우 그림 8(a)와 같이 노드 에너지가 25%미만일 경우 에너지를 고려하여 허위 보고서가 5번이상 인증 실패를 하면 노드는 더 이상 인증을 거부하고 보고서를 바로 폐기하게 된다. 하지만 허위보고서를 재전송시 메시지를 수신하는 것만으로도 소모가 되므로 12회이상 보고서가 수신되면 노드는 강제 대기 모드로 들어 간다. 각 그림 8(a), (b), (c)들은 노드에 너지의 잔여량에 따른 퍼지로직에 시뮬레이션 값을 보여준다.

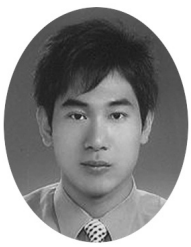
6. 결론 및 향후 과제

본 논문에서는 IHA를 적용한 무선 센서네트워크에서 서비스 거부 공격에 대한 방어 기법을 제안하였다. IHA는 조합된 노드들의 페어와이즈 MAC을 이용함으로써 허위 보고서를 검증하나 허위 보고서 재전송 공격에 대한 에너지 소모를 줄일 수 있는 대책은 없었다. 본 논문은 기존의 IHA에서 퍼지 로직 시스템을 적용하여 입력 값을 받아 출력 값 ST를 적용하여 에너지 소모를 줄일 수 있는 효율적인 방안을 제시하고 기존의 IHA와 비교하여 시뮬레이션을 통해 효율성을 검증하였다. 그러나 제안기법은 정상 보고서를 허위보고서로 오인할 수도 있다는 단점이 있다. 본 논문에서 보여준 ST를 좀 더 효율적으로 도출하기 위한 입력 값 및 다른 방식을 찾아보고자 한다.

참 고 문 헌

1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirici, “A survey on sensor networks,” IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, Aug. 2002.
2. J.N. Al-Karaki, and A.E. Kamal, “Routing techniques in wireless sensor networks: a survey,” IEEE Wireless Communication Magazine, Vol. 11, No. 6, pp. 6-28, 2004.
3. H. Yang, S. Lu, “Commutative Cipher Based En-route Filtering in Wireless Sensor Networks,” in IEEE Vehicular Technology Conference(VTC) 2004-Fall Symposium on Wireless Technologies for Global Security, 2004.
4. Ye, F., Luo, H., Lu, S., Zhang, L. (2005), “Statistical En-route Filtering of Injected False Data in Sensor Networks”, IEEE Journals on Selected Areas in Communications, Vol. 23, No. 4, pp. 839-850.

5. Yu, Z. Guan, Y. (2005), “A Dynamic En-route Scheme for Filtering False Data Injection in Wireless Sensor Networks”, Proc. of SenSys, pp. 294-295, ACM.
6. Yang, H., Lu, S. (2004), “Commutative Cipher Based En-route Filtering in Wireless Sensor Networks”, Proc. of VTC, pp. 1223-1227, IEEE.
7. Zhu, S., Setia, S., Jajodia, S., Ning, P. (2004), “An Interleaved Hop-by-Hop Authentication Scheme for Filtering of Injected False Data in Sensor Networks”, Proc. S&P, pp. 259-271.
8. Thao P. Nghiema, and Tae Ho Cho, “A fuzzy-based interleaved multi-hop authentication scheme in wireless sensor networks”, J. Parallel Distib. Comput. Vol. 69, pp. 441-450. May. 2009.
9. H.Y Lee, T.H. Cho, “Fuzzy-Based Adaptive Threshold Determining Method for the Interleaved Authentication in Sensor Networks”, Lect. Notes Artif. Int., Vol. 4293, pp. 112-121, Nov. 2006.
10. Chris Karlof and David Wagner, “Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures,” First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.
11. F. Ye, H. Luo, S. Lu, “Statistical En-Route Filtering of Injected False Data in Sensor Networks,” IEEE J. Sel. Area Comm., Vol. 23, No. 4, pp. 839-850, 2005.
12. A. A. Elsamiee, The development of AWS AND introductory to the IWS, intelligent weather system, in: TECO 2006–WMO Technical Conf., 2006.
13. M. Yusuf, T. Haider, Energy-aware fuzzy routing for wireless sensor networks, in: IEEE International Conf. on Emerging Technologies, 2005.



김 종 현 (jonghkim@ece.skku.ac.kr)

2009 단국대학교 컴퓨터과학과 학사
2009～현재 성균관대학교 정보통신공학부 석사

관심분야 : 무선 센서 네트워크, 모델링 및 시뮬레이션, 인공 지능, 정보 보안

조 대 호 (taecho@ece.skku.ac.kr)

1983 성균관대학교 전자공학과 학사
1987 Univ. of Alabama 전자공학과 석사
1993 Univ. of Arizona 전자 및 컴퓨터공학과 박사
1995～현재 성균관대학교 정보통신공학부 교수

관심분야 : 무선 센서 네트워크, 모델링 및 시뮬레이션, 지능 시스템, 모델링 방법론