Journal of the Korea Academia-Industrial cooperation Society
Vol. 13, No. 11 pp. 5487-5495, 2012

http://dx.doi.org/10.5762/KAIS.2012.13.11.5487

대규모 센서 네트워크에서 그룹을 기반으로 한 에너지 효율적인 클러스터키 관리 방안

김진수[1*]
[1]동명대학교 항만물류시스템학과

An Energy Efficient Group-Based Cluster Key Management for Large Scale Sensor Networks

Jin-Su Kim[1*]
[1]**Department of Port & Logistics System, Tongmyong University**

요 약 무선 센서 네트워크 환경에서 클러스터키 등의 보안키를 적용하기 위한 중요한 고려 사항은 보안키 갱신이 안전하게 이루어져야 하고, 보안키 갱신 시 요구되는 시간과 비용이 적어야 한다는 점이다. 각 센서 노드는 제한된 에너지를 보유하기 때문에 보안키 갱신에 소모되는 에너지가 클 경우 전체 네트워크 수명에 많은 영향을 준다. 따라서 안전하고 에너지 효율적인 보안키 관리 방법이 요구된다.
본 논문에서는 그룹을 기반으로 한 에너지 효율적인 클러스터키 관리 방안을 제안한다. 제안하는 방법에서 대규모 센서 네트워크에서 안전하고 효율적인 키 관리를 위해 5개의 보안키를 사용하고, 섹터, 클러스터 및 그룹 수준의 보안 적합도를 관리하여 보안키 갱신 주기 및 보안에 사용되는 다항식의 차수를 차별화시킨다. 실험을 통해 이전의 보안키 관리 기법보다 네트워크 에너지 효율성이 향상됨을 입증한다.

Abstract The important issue that applies security key are secure rekeying, processing time and cost reduction. Because of sensor node's limited energy, energy consumption for rekeying affects lifetime of network. Thus it is necessary a secure and efficient security key management method. In this paper, I propose an energy efficient group-based cluster key management (EEGCK) in the large scale sensor networks. EEGCK uses five security key for efficient key management and different polynomial degree using security fitness function of sector, cluster and group is applied for rekeying and security processing. Through both analysis and simulation, I also show that proposed EEGCK is better than previous security management method at point of network energy efficiency.

Key Words : large scale sensor networks, cluster key management, security fitness function, polynomial degree, five security key, lifetime of network, network energy efficiency

1. 서론

무선 센서 네트워크의 클러스터링 시스템에서 노드들은 클러스터로 구분되고 두 가지 모드로 작동된다. 즉, 센싱 모드와 클러스터 헤드 모드이다. 노드가 센싱 모드인 경우, 노드는 센싱된 데이터를 클러스터 헤드로 보낸다. 클러스터 헤드 모드인 경우, 노드는 클러스터 멤버로부터 수신된 데이터를 병합하고 기지국으로 전송한다. 기지국은 클러스터 헤드 선정에 대한 중요한 일을 수행한다[1]. 클러스터 헤드는 안전하고 제한된 통로를 통해 다른 클러스터 멤버와 통신하기 위한 클러스터키 및 그룹키를 생성한다[2].

무선 센서 네트워크 환경에서 클러스터키 등의 보안키를 적용하기 위한 중요한 고려 사항은 두 가지이다[3]. 첫

*Corresponding Author : Jin-Su Kim
Tel: +82-10-4553-8543 email: kjs8543@tu.ac.kr
접수일 12년 08월 23일 수정일(1차 12년 09월 26일, 2차 12년 10월 05일) 게재확정일 12년 11월 08일

째, 보안키 갱신이 안전하게 이루어져야 한다. 센서 노드는 쉽게 포획가능하기 때문에 공격자는 포획한 센서 노드를 통해 사용되고 있는 보안키 및 비밀정보를 얻을 수 있으며, 획득한 정보를 통해 네트워크상에 흘러가는 모든 메시지를 도청하거나 공격에 이용할 수 있다. 그러므로 센서 노드가 공격자에게 포획되었을 경우, 포획된 노드를 제외한 나머지 센서 노드에게 안전하게 보안키를 갱신해 주는 것이 매우 중요하다.

둘째, 보안키 갱신 시 요구되는 시간과 비용이 적어야 한다는 점이다. 보안키 갱신은 네트워크 확장에 따라 센서 노드가 추가될 때 또는 공격자에 의해 특정 보안키가 노출되었을 때 이루어지며, 보안키를 생성하는 조건에 따라 새로운 보안키를 갱신해 주어야 한다. 각 센서 노드는 특성상 제한된 에너지를 보유하기 때문에 보안키 갱신에 소모되는 에너지가 클 경우 전체 네트워크 수명에 많은 영향을 준다. 따라서 안전하고 에너지 효율적인 보안키 관리 방법이 요구된다.

본 논문에서는 대규모 센서 네트워크에서 그룹을 기반으로 한 에너지 효율적인 클러스터키 관리 방안(EEGCK: Energy Efficient Group-based Cluster Key management)을 제안한다. 제안된 접근 방법의 네트워크는 전체가 환형으로 여러 개의 섹터로 나누어지고 각 섹터는 여러 개의 계층으로 나누어진다. 이 섹터별 계층에 하나 이상의 클러스터를 형성한다. 이러한 클러스터는 여러 그룹으로 나누어 관리하고, 클러스터 헤더(CH: Cluster Head) 및 각 그룹별 리더(GL: Group Leader)는 그룹과 센서 노드의 보안적합도를 이용하여 기지국(BS: Base Station)이 정한다.

EEGCK는 하나의 키를 사용하는 방법으로는 대규모의 센서 네트워크에서 안전하고 효율적인 키 관리가 어렵다고 판단되어[4] 5개의 보안키를 사용하는 방안을 제시한다. 이 방법은 일부 노드의 노출 및 오염이 근접 이웃 노드까지 노출시키는 위험을 최소화한다. 5개의 보안키는 섹터키(SK: Sector group Key), 클러스터키(CK: Cluster group Key), 그룹내 멤버 노드(GM: Group Member)들의 쌍방향키(GMPK: Group Member Pair-wise Key), 초기 센서 노드가 필드에 배치될 때 사전에 할당되는 개인키(PK: Primary Key) 및 마스터키(MK: Master Key) 등이다. MK는 초기 클러스터 생성이 완료되면 폐기한다. 네트워크 보안에 사용되는 에너지의 효율적인 관리를 위해 섹터, 클러스터 및 그룹 수준의 보안적합도를 관리하여 보안키의 보안 강도를 차별화한다. 이러한 키의 효율적인 관리를 위해 섹터 내에서 데이터를 송수신할 때 사용되는 SK는 네트워크의 같은 섹터 내에 있는 CH가 많은 데이터를 병합하여 높은 안전성을 요구하기 때문에 멀티캐스팅에 의해 키가 안전하게 생성되는 방식[3]을 이용한다. 그리고 CH가 자주 변경되는 점을 고려해서 CK는 보안적합도에 따라 그 적합도가 임계값 이하이면 BS에서 다시 배포하고, 그 이상이면 B-PCGR[5]을 이용하여 내부적으로 시간별 카운터를 이용하여 새로운 키를 생성하므로 새로운 키를 생성하는 에너지 소모량을 줄인다. 또한 CK 및 GMPK를 지정할 때 계층(layer)별로 보안 강도를 차별화하여 에너지 효율을 증진시킨다. BS에 가까운 계층일수록 더 많은 데이터를 병합하여 BS에 송신하므로 BS에 가까운 계층은 보안을 더 강화할 필요가 있다. 이러한 보안 강도 차별화는 보안적합도와 계층번호를 이용하여 보안에 사용되는 다항식의 차수를 조절하는 알고리즘을 통하여 처리한다.

본 논문의 구성은 다음과 같다. 2장에서는 관련 연구에 대해 알아보고, 3장에서는 본 논문에서 제안한 EEGCK 클러스터키 관리 방안을 설명한다. 4장에서는 제안된 기법과 기존 기법에 대해서 비교 분석하고, 마지막으로 5장에서 결론을 맺는다.

2. 관련 연구

클러스터키 또는 그룹키 관리 프로토콜은 접근방법에 따라 세 가지로 분류할 수 있다. 하나의 키 분배 센터를 통해 멀티캐스트 그룹키를 관리하는 중앙 집중형 방식, 멀티캐스트 그룹을 여러 개의 하위 그룹으로 나누어 관리하는 비중앙 집중형 방식, 그룹 내 모든 멤버를 통해 키를 생성하는 분산형 방식이 존재한다[3].

중앙 집중형 방식에서 그룹키를 생성하고, 모든 노드에게 전달하는 역할은 키 서버 혹은 그룹 리더에 의해 이루어진다. 이에 대한 연구로는 그리드 구성을 통하여 그룹을 지정하고 효율적인 다항식을 이용하여 그룹키를 분배하는 GRSM[3], 그룹 통신에 대한 데이터 보안 문제를 극복하기 위해서 지역을 기반으로 한 이동형 애드혹 네트워크에 있어서의 키관리에 대한 접근 방법을 제시한 SERGK[2] 등이 있다. 중앙 집중형 방식은 그룹키 갱신 시 네트워크 전체적으로 전달되어야 하기 때문에 통신 오버헤드가 크다는 단점이 있다.

비 중앙 집중형 방식에서는 네트워크를 여러 개의 클러스터로 나누어서 관리한다. 클러스터는 보통 클러스터를 대표하는 클러스터 헤드가 그 구성 멤버인 클러스터 멤버를 통제한다. 이에 대한 연구로는 클러스터를 구성하는 노드들에게 그리드 기반 키 분배 방법을 적용하여 기존의 키 분배 방법에 비해 향상된 보안을 제공하는 SDDC[6], 동적으로 그룹을 생성하여 중앙집중형 방법이

가지는 단점을 해소한 BALADE 기법[7] 등이 있다.

분산형 방식은 키를 관리하는 주체가 없이 그룹 내 모든 노드들이 스스로 그룹키를 생성하는 방식이다. 대표적인 기법으로 B-PCGR[5]이 있다. 이 기법은 그룹키를 자체적으로 갱신하기 때문에 에너지 효율은 좋으나 선택적 포획 공격에 강하지 않기 때문에 보안 강도가 높아야 할 경우에 사용하는 것은 무리가 있다.

GRSM[3]은 무선 센서 네트워크 환경에서 가장 취약한 포획 공격에도 높은 안전성을 제공하는 멀티캐스트 기법으로, 센서 노드가 배치되는 장소를 그리드 형태로 구성, 그룹키 생성 및 분배, 그룹키 갱신 등의 3단계로 되어 있다. 이 기법은 공격자에게 센서노드가 포획되어 비밀정보가 노출되더라도, 공격자는 갱신되는 그룹키에 대한 어떠한 정보도 획득할 수 없다. 따라서 높은 안전성을 가지고 있다. 그러나 그룹키를 구성하는 다항식은 해당 그룹의 노드수가 많으면 그 차수가 높아져서 다항식을 계산하는 데 오버헤드가 많고 그룹키 메시지의 크기가 커지므로 이를 수신하는 각 노드의 에너지 효율이 떨어진다. 그러므로 이 방식은 많은 수의 센서 노드를 가진 클러스터링 시스템에 바로 적용하기에는 무리가 있다.

B-PCGR[5] 기법은 그룹키 사전 분배, 지역적인 협력을 기반으로 한 키 방어, 지역적인 협력을 기반으로 한 그룹키 변경의 3단계로 되어 있다. B-PCGR은 센서 노드에 그룹을 미리 지정한 다항식 키를 사전 분배하고, 이를 이용하여 시간에 따라 키를 갱신하는 방법을 이용한다. 이 방식은 센서 노드 및 클러스터 헤드의 설정 위치가 인위적이지 않은 환경의 클러스터링 모델에서는 미리 설정한 다항식 키의 사전 분배를 통해 클러스터를 지정할 수 없는 단점이 있다.

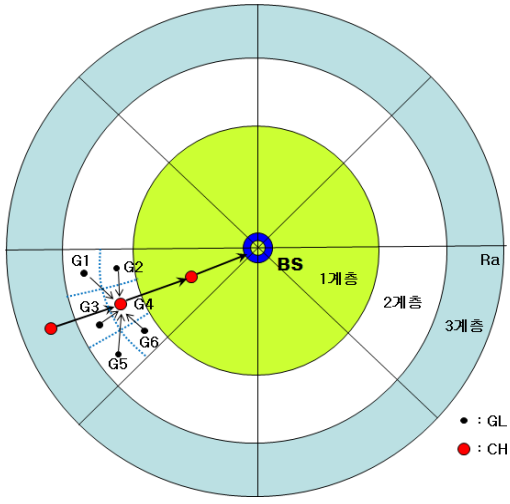
SDDC[6]는 동적 클러스터 모델의 라운드별 단위 클러스터 노드에 BS에서 CH에 분배한 서브 그리드 키를 할당하여 클러스터 내부의 연결성과 보안을 높이는 키 분배 기법이다. 이 방법은 클러스터 생성, 키 분배, 직접 키 설정, 간접 키 설정 등으로 구성되어 있다. SDDC는 동일 클러스터 내의 노드들은 동일 CH에게 받은 다항식 일부분을 이용한 클러스터 구분키와 클러스터 내 서브 그리드에 할당된 행과 열의 다항식 일부분 값에 의한 키를 사용하므로 보안이 향상된다. 그러나 키 분배시 BS에서 CH로 분배한 다항식 키 자료를 센서 노드로 분배하는 과정에서 많은 에너지가 소모된다.

3. EEGCK 클러스터키 관리 방안

3.1 네트워크 모델(Network Model)

제안하는 방법은 다음과 같은 가정을 갖는다.

- 한정된 자원을 가진 많은 수의 센서로 구성된 무선 센서 네트워크이다.
- BS는 컨트롤러(key server)로서 동작되고, 오래 지속되는 전력을 가진 장치이다. 또한 센서 노드로부터 획득하는 정보들을 수집하고, 각각의 센서 노드를 통제한다.
- 센서 노드 및 클러스터 헤드의 설정 위치가 인위적이지 않은 환경의 클러스터링 모델이다. 즉, 센서 노드는 공중 살포되거나 물리적인 설치에 의해 배치될 수 있다. 그러나 사전에 인접한 이웃 노드에 대한 정보는 알 수 없다.
- 모든 센서 노드는 필드에 배치되기 전에 랜덤하게 생성된 유일한 비밀키와 고유한 ID를 저장하고, 필드에 배치된 후 고정되어 있어서 BS가 그 위치를 알 수 있다.
- 각 노드는 배치 전에는 오염이 되지 않았고, 배치될 처음 몇 분 동안은 포획될 수 없다.
- 포획당한 노드는 포획 탐지하는 각종 기법을 이용하여 탐지할 수 있고, BS는 그 내역을 알 수 있다.



[그림 1] 여러 개의 계층으로 구성된 네트워크 모델
[Fig. 1] Network Model with Multi Layers

제안하는 방법의 네트워크 구조는 그림 1과 같이 중간에 BS가 위치해 있고 그 주위에 센서 노드가 환형으로 배치된 형태로 그 내역은 다음과 같다.

- 네트워크의 반지름은 Ra, 노드 수는 N이다.
- 네트워크는 여러 개의 섹터로 구분되고 각 섹터는 여러 계층으로 나누어진다. 각 섹터에 소속된 계층은 하나 이상의 클러스터로 구성된다. 이 클러스터

는 여러 개의 그룹으로 구성되고, 각 그룹에는 GL이 있고, BS는 그룹에 소속된 센서 노드 중에서 수식 (1)의 센서 노드 보안적합도가 큰 노드를 GL로 지정한다. 또한 CH는 이 GL 중에서 수식 (3)의 그룹 보안적합도를 이용하여 선택한다.

- 그룹에 소속된 GM에서 센싱된 데이터는 GMPK를 이용하여 GL로 보내지고, GL에서는 그 데이터를 하나의 보고서로 병합하여 클러스터키를 이용하여 CH로 송신하고, CH는 여러 GL에서 수신된 데이터를 병합하여 여러 계층의 중간 CH를 거쳐 SK를 이용하여 BS로 송신한다.
- 클러스터 내의 초기 그룹 멤버를 지정하는 것은 BS가 모든 센서 노드의 좌표 정보를 받아, 그 내역을 이용하여 적절하게 지정하고, 노드가 삭제되거나 새로운 노드가 추가될 때 역시 이러한 방법을 이용한다.
- 각 노드는 자기의 ID, 위치 및 잔여 에너지 정보를 가지고 있다. 또한 각 계층의 CH는 같은 섹터에 속한 다른 계층의 CH에 대한 ID와 위치 정보를 BS로부터 제공받는다.

3.2 클러스터 생성

센서 필드에 위치하는 모든 노드는 노드 ID, 개인키 및 BS와 공유하는 마스터키를 할당받고 필드에 배치된다. 필드에 배포된 각 센서 노드는 마스터키를 이용하여 노드 ID와 자기의 위치를 BS에게 알린다. BS는 그림 1과 같은 섹터 및 계층으로 나누어지는 클러스터와 그에 속하는 그룹 데이터를 이용하여 각 센서 노드들에게 섹터 ID, 클러스터 ID 및 그룹 ID를 알린다. BS는 클러스터에 속한 GM 중에서 센서 노드의 보안적합도에 따라서 GL을 지정하고 개인키를 이용하여 해당 노드에게 알린다. GL이 된 센서 노드는 그룹 내의 모든 노드에게 자기가 GL이라는 사실을 알린다. BS는 GL 중에서 그룹 보안적합도가 제일 좋은 노드를 CH로 선정하고, 개인키를 이용하여 해당 노드에게 알린다. CH 역시 자기가 CH로 선정되었다는 사실을 마스터키를 이용하여 GL에게 알린다. 초기 클러스터를 생성할 때 대부분의 데이터 송신은 마스터키 또는 개인키를 이용하여 암호화하고, 클러스터가 생성되고 그룹에 소속된 센서 노드들의 GMPK 생성이 완료되면 마스터키는 폐기된다.

생성된 클러스터는 매 라운드마다 시스템 보안적합도인 수식 (6)의 $FIT_{S\text{-}secu}$를 이용하여 재구성할지 여부를 결정한다. 즉, $FIT_{S\text{-}secu}$값이 임계값 이하이면 전체적으로 클러스터를 재구성하고, 아니면 현재 클러스터를 그대로 유지한다. 클러스터가 재구성되면 3.4절과 같은 키분배 과정을 다시 수행한다.

3.3 보안적합도

수식 (1)의 센서 노드 보안적합도($FIT_{N\text{-}secu}$)는 GL을 선정할 때 사용하고, 수식 (3)의 그룹 보안적합도($FIT_{G\text{-}secu}$)는 CH를 선정할 때 사용하고, 수식 (5)의 클러스터 보안적합도($FIT_{C\text{-}secu}$)는 클러스터키를 갱신할 때 이용한다. 또한 수식 (6)의 시스템 보안적합도($FIT_{S\text{-}secu}$)는 클러스터 재구성 여부에 대한 기준으로 이용한다. 보안적합도가 1에 가까울수록 보안 유지에 적합하다.

$$FIT_{N-\mathrm{secu}} = \frac{E_{N_{res(i)}} - E_{GL(i)}}{E_{N_{\mathrm{base(i)}}}} \tag{1}$$

$$E_{GL(i)} = \sum_{j=1}^{N_g - 1} l\left(E_{elec} + \epsilon fs \times d_{jtoGL(i)}^2\right) \tag{2}$$

수식 (1)에서 $E_{N_{res}(i)}$ 는 노드 i의 에너지 잔량이고 $E_{N_{\mathrm{base}}(i)}$ 는 노드 i의 초기 에너지 량이다. $E_{GL(i)}$는 현재 센서 노드 i를 GL로 가정했을 때, 그룹 내의 모든 노드와의 쌍방향키를 갱신할 때 사용되는 에너지량이다. 소모되는 에너지는 T. Rappaport[10]의 에너지 모델을 이용해서 구한다. 수식 (2)에서 N_g는 그룹에 소속된 노드 수, l은 데이터를 송수신할 때의 메시지 길이(bit), E_{elec}은 데이터 송수신 에너지로서 50 nJ/bit, ϵ_{fs}는 무선 통신의 자유 공간 모델 상수로서 10 pJ/bit/m^{2}이다. 또한 $d_{\mathrm{toGL}(i)}$은 그룹에 소속된 센서 노드 j에서 예상 GL까지의 거리이다. BS는 새로운 GL을 지정할 때 수식 (1)을 이용하여 그룹 내에서 에너지 예상 잔량 비율이 제일 높은 노드를 선택한다.

$$FIT_{G-\mathrm{secu}} = \frac{\sum_{i=1}^{N_g} E_{N_{res(i)}} - E_{CH(i)}}{\sum_{i=1}^{N_g} E_{N_{\mathrm{base(i)}}}} \times \frac{N_g - CT_{CH}}{N_g} - \frac{N_p}{N_g} \tag{3}$$

$$E_{CH(i)} = \sum_{j=1}^{CT_g - 1} l\left(E_{elec} + \epsilon fs \times d_{jtoCH(i)}^2\right) \tag{4}$$

수식 (3)에서 $E_{CH(i)}$는 현재 GL 노드 i를 CH로 가정했을 때, 클러스터 내의 모든 GL의 클러스터키를 갱신할 때 사용되는 에너지량이다. N_p는 그룹에서 오염된 적이 있는 노드 수, CT_{CH}는 그룹의 노드 중 CH가 된 적이 있는 노드의 수이다.

수식 (4)에서 CT_g는 클러스터에 소속된 그룹수, $d_{\mathrm{toCH}(i)}$은 클러스터에 소속된 GL 노드 j에서 예상 CH

i까지의 거리이다. BS는 새로운 CH를 지정할 때 수식 (3)을 이용하여 클러스터 내의 그룹 중에서 에너지 예상 잔량 비율, CH가 된 횟수 및 오염된 노드수를 고려하여 그룹 보안적합도가 가장 좋은 그룹의 GL을 CH로 선택한다.

$$FIT_{C-secu} = \frac{\sum_{i=1}^{CT_g} FIT_{G-secu}(i)}{CT_g} \quad (5)$$

BS는 클러스터에 대한 보안을 강화하기 위하여 일정한 시간 간격으로 클러스터키를 갱신하는데, 수식 (5)의 $FIT_{C\text{-}secu}$를 이용하여 특정 클러스터키를 자체적으로 갱신하든지 또는 BS가 네트워크 전체적으로 클러스터키를 다시 배포하는지를 결정함으로써 클러스터키를 갱신하는데 소모되는 에너지를 줄인다. 그리고 BS에 가까운 계층일수록 더 많은 데이터를 병합하여 BS에 송신하므로 보안을 더 강화할 필요가 있다. 그래서 클러스터키를 지정할 때 클러스터키 분배 알고리즘에서 $FIT_{C\text{-}secu}$를 이용하여 다항식 차수를 조절하여 계층별 또는 보안에 취약한 클러스터에 대해 보안 강도를 차별화시켜 에너지 효율을 증진시킨다.

$$FIT_{S-secu} = \frac{\sum_{i=1}^{CT_C} FIT_{C-secu}(i)}{CT_C} \quad (6)$$

BS는 네트워크의 수명을 증진시키기 위하여 라운드별로 네트워크를 점검하여 클러스터를 재구성한다. 이 때 수식 (6)의 $FIT_{S\text{-}secu}$를 이용하여 전체적으로 클러스터를 재구성할 지 여부를 결정한다. 이 때 CT_C는 네트워크의 클러스터수이다.

3.4 키 분배 및 쌍방향키 생성

본 논문에서는 하나의 키를 사용하는 방법으로는 대규모의 센서 네트워크에서 안전하고 효율적인 키 관리가 어렵다고 판단되어 5개의 보안키를 사용하는 방안을 제시한다. 5개의 보안키는 SK, CK, GMPK, PK 및 MK이다. 네트워크에서 노드수는 많지 않지만 높은 안전성을 요구하는 같은 섹터 내에 있는 CH 사이의 SK는 멀티캐스트 방법[3]을 이용하여 키를 분배하고, 빈번하게 교체할 필요가 있는 CK는 키 갱신(rekeying)이 쉽고 효율적으로 에너지를 사용하는 B-PCGR[5]을 이용하여 키 분배 및 갱신을 한다. 또한 BS는 클러스터키 분배 알고리즘에서 지정한 다항식 차수를 가진 이변 다항식을 생성하고 개인키를 이용하여 각 그룹의 GL을 통하여 각 노드에게 보내면 그룹의 각 노드는 그룹의 서로 다른 노드끼리 GMPK를 생성한다.

3.4.1 섹터키와 클러스터키의 생성 및 분배

섹터키의 생성 및 분배 단계에서 BS는 수식 (7)과 같은 섹터키 SK_j를 포함한 다항식 $f_1(x)$를 생성하고, 생성된 다항식의 계수와 MAC을 수식 (8)과 같이 섹터키 메시지를 구성하여 섹터에 소속된 CH에게 멀티캐스트 방식으로 전송한다[3]. 이렇게 함으로써 다항식에 CH의 개인키 PK_i를 대입하면 섹터키 SK_j값을 얻어낼 수 있다.

$$f_1(x) = SK_j + \prod_{i=1}^{CT_{sc}} (x - PK_i) \bmod M, \ (CT_{sc} \geq 5) \quad (7)$$

$$\text{Message-SK} = \{\text{S}-\text{ID}, \{\text{a}_1 \| \text{a}_2 \| \cdots \| \text{a}_{\text{CT}_{\text{SC}}}\}.\text{PK}_\text{i}, MAC_{SK_j}(a_1 \| a_2 \| \cdots \| a_{CT_{SC}})\} \quad (8)$$

수식 (7)에서 SK_j는 섹터 j의 SK, PK_i는 CH i의 개인키, M은 160비트 길이의 모듈러값, CT_{sc}는 섹터에 소속된 클러스터 수이다. CT_{sc}가 5보다 크지 않을 때는 강제적으로 차수를 늘리는 방법을 이용한다. 수식 (8)에서 S-ID는 섹터 ID, $\{\text{a}_1 \| \text{a}_2 \| \cdots \| \text{a}_{\text{CT}_{\text{SC}}}\}.\text{PK}_\text{i}$는 각 노드의 개인키 PK_i로 암호화한 다항식의 계수, MAC_{SK_j}는 섹터키 SK_j로 다항식 계수의 MAC을 생성하고, MAC 인증을 통해 계산된 섹터키 SK_j가 올바른지 검증할 수 있다.

클러스터키의 생성 및 분배 단계에서 BS는 클러스터키 분배 알고리즘을 이용하여 수식 (9)와 같은 임의의 일변수 다항식(UP: Univariate Polynomial)을 생성하고, 생성된 다항식의 계수와 MAC을 수식 (10)과 같은 클러스터 헤드 ID(CH-ID)를 포함한 클러스터키 메시지를 구성하여 CH에게 전송한다. CH는 수신된 다항식의 일부분을 B-PCGR[5]을 이용하여 클러스터에 속한 GL에게 송신하고 키를 갱신할 때 서로 협력하여 처리한다.

$$f_2(x) = \sum_{i=0}^{DEP_{CL}} c_j x^i \quad (9)$$

$$\text{Message-CK} = \{\text{CH}-\text{ID}, \{\text{c}_1 \| \text{c}_2 \| \cdots \| \text{c}_{\text{DEP}_{\text{CL}}}\}.\text{PK}_\text{i}, MAC_{CK_k}(c_1 \| c_2 \| \cdots \| c_{DEP_{CL}})\} \quad (10)$$

수식 (9)에서 DEP_{CL}은 수식 (11)에서 생성한 해당 클러스터의 다항식 차수이다. 섹터키 갱신이 필요시 BS은 수식 (7)과 같은 방법을 이용하여 이전에 사용되지 않은 새로운 섹터키를 생성하여 섹터에 소속된 CH에게 송신한다. 반면 클러스터키 갱신이 필요시 CK는 빈번하게 교체할 필요가 있기 때문에 키 갱신이 쉽고 효율적으로 에

너지를 사용하는 그림 2와 같은 클러스터키 갱신 알고리즘을 이용한다.

3.4.2 클러스터키 분배 알고리즘

알고리즘 1은 클러스터키를 지정할 때 보안적합도를 이용하여 다항식 차수를 조절함으로써 계층별 및 클러스터별로 보안 강도를 차별화시켜 에너지 효율을 증진시키는 알고리즘이다. 알고리즘에서 $UP_{\mathrm{DEG_{CL}}}$은 다항식 차수가 수식 (11)과 같은 GF(q)에 소속된 계수로 생성된 임의의 일변수 다항식이다.

$$\mathrm{DEG_{CL}} = \mathrm{round}((\mathrm{P_{base}} + \omega(\mathrm{CT_{CL}} - \mathrm{Ln})) / FIT_{C-SECU}) \quad (11)$$

수식 (11)에서 $\mathrm{P_{base}}$는 분배할 기본적인 다항식 차수, $\mathrm{CT_{CL}}$은 네트워크 계층별 클러스터 개수, Ln은 해당 클러스터의 계층 번호이다. 단, ω는 계층별로 다항식 차수를 차등시키기 위한 가중치(weight)이다. 각 클러스터의 계층이 높을수록 또한 보안적합도가 낮을수록 다항식 차수를 높인다.

알고리즘 1에서 C-ID는 현재 계층 번호에 소속된 클러스터 번호, $\mathrm{CT_L}$은 네트워크의 전체 계층수, $\mathrm{CT_{CL}}$은 네트워크 계층별 클러스터 개수, $\mathrm{CT_C}$는 네트워크의 전체 클러스터 개수, P(i)[ID]는 노드 i에 분배하는 다항식이다.

```
for Ln=1 to CT_L
    for C-ID=1 to CT_CL
        P[Ln][C-ID] = UP_DEG_CL
    next C-ID
next Ln

for i=1 to CT_C
    P(i)[ID] = P[Ln][C-ID]
next
```

[알고리즘 1] 클러스터키의 분배 알고리즘
[Algorithm 1] Algorithm for Distribution of Cluster Key

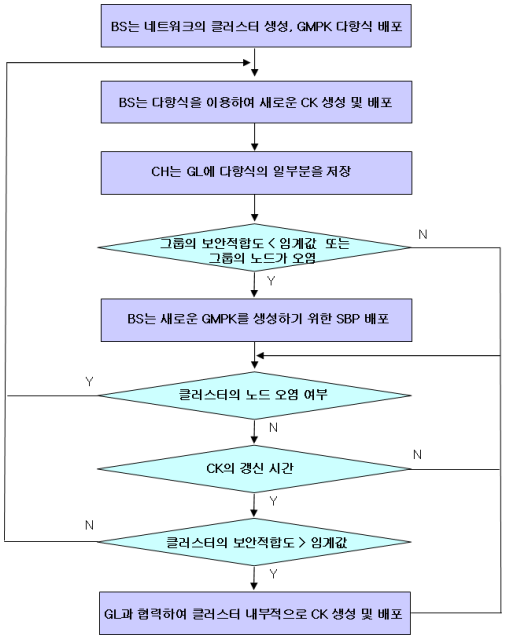
3.4.3 그룹에 소속된 센서 노드들의 쌍방향키 생성

임의의 두 센서 노드가 동일한 t차 대칭 이변 다항식(SBP: Symmetric Bivariate Polynomial)을 공유하면 두 노드는 그 다항식으로부터 서로 공통되는 키 값을 유도할 수 있다[8]. BS은 소수 q에 대한 유한체 F(q) 상에서 f(x, y)=f(y, x) 의 성질을 만족하는 $\mathrm{DEG_{CL}}$차 이변 다항식을 수식 (12)와 같이 생성하여 개인키를 이용하여 각 그룹의 GL에게 보낸다. GL은 마스터키를 이용하여 GM에게 {ID, f(ID, y)}를 배포하면 GM과 GL은 상호간의 ID를 y 값에 입력하여 $f(ID_i, ID_j)$ 와 $f(ID_j, ID_i)$ 를 생성할 수 있으며 $f(ID_i, ID_j) = f(ID_j, ID_i)$ 이므로 그룹 노드 상호간에 쌍방향키(GMPK)를 생성할 수 있다. 이와 같은 방법으로 그룹의 모든 노드는 다른 노드와 상호간에 GMPK를 생성하여 서로 원활하게 송수신하도록 한다. 마스터키는 GMPK가 생성된 후 폐기된다. 그룹 내의 노드 중 하나가 오염되거나 그룹의 보안적합도가 임계값 이하가 되어 GMPK를 갱신할 때에는 BS에서 멀티캐스트 방법[3]을 이용하여 마스터키를 분배한 다음, BS는 위에서 기술한 방법과 동일한 방법으로 $\mathrm{DEG_{CL}}$차 이변 다항식을 GL을 통해 분배하고 마스터키를 이용하여 새로운 GMPK를 생성한다. 역시 마스터키는 GMPK가 생성된 후 폐기된다.

$$f(x,y) = \sum_{i,j=0}^{\mathrm{DEG_{CL}}} a_{ij} x^i y^j \quad (12)$$

3.5 그룹에 소속된 센서 노드들의 쌍방향키 및 클러스터키 갱신

그림 2는 그룹에 소속된 노드들의 GMPK 및 클러스터키 갱신에 대한 순서도이고, 그 세부 내역은 다음과 같다.



[그림 2] 클러스터키 갱신 순서도
[Fig. 2] Flowchart of Rekeying for Cluster Key

1) BS는 각 노드로부터 보내온 ID 및 위치 정보를 이용하여 네트워크의 클러스터를 생성하고, 그룹에 속된 센서 노드들의 쌍방향키(GMPK)를 생성하기 위한 대칭 이변 다항식을 생성 및 배포한다.
2) BS는 보안적합도와 클러스터 계층번호에 따라 다른 차수를 적용한 일변수 다항식을 이용하여 새로운 클러스터키를 생성하고 CH에 배포한다.
3) CH는 GL에 일변수 다항식의 일부분을 저장하고, 클러스터 내부적으로 클러스터키를 생성할 때 이용한다. BS는 그룹의 노드 중에서 보안적합도가 제일 높은 노드를 GL로 지정하고, GL이 변경되면 다항식 관련 정보를 새로운 GL에 전송한다.
4) 임계값이 그룹의 보안적합도보다 크거나 그룹의 노드가 오염된 경우, BS는 새로운 GMPK를 생성하기 위한 대칭 이변 다항식(SBP)을 배포한다. 그룹내 노드들은 이 SBP를 이용하여 GMPK를 생성한다.
5) 클러스터의 노드 중에서 일부의 노드가 오염된 경우 2)~4)의 절차를 되풀이한다.
6) 클러스터키를 갱신할 시간이 되면 클러스터의 보안적합도를 검사한다.
7) 클러스터의 보안적합도가 임계값보다 높으면 GL과 협력하여 클러스터 내부적으로 새로운 클러스터키를 생성하고 그 키를 각 그룹의 GL에 배포하고, 낮으면 2)~4)의 절차를 되풀이하고 클러스터의 노드 오염 여부를 검사한다.

4. 성능 분석

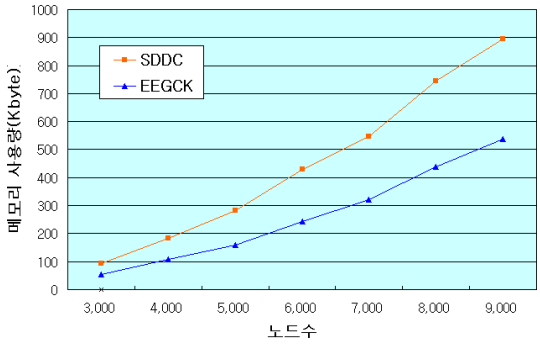
제안된 EECGK 방법에 대한 성능을 평가하기 위해서 메모리 사용량과 에너지 소모량을 비교 분석한다. 메모리 사용량은 SDDC 기법과 제안된 EECGK 방법을 비교하고, 에너지 소모량은 GRSM[3], SDDC[6] 및 제안된 EEGCK 방법을 비교한다.

4.1 메모리 사용량 분석

이 절에서는 무선 센서 네트워크의 자원이라는 측면에서 분석적이고 수학적인 방법을 이용하여 제안하는 방법에 대한 메모리 사용량을 측정한다.

GF(q)내의 계수를 갖는 차수 t의 SBP f(x, y)는 f(t + 1) * log(q)의 비트로 표현할 수 있다[9]. 클러스터 i에 할당할 다항식 차수 $DEP_{CL}(i)$, 클러스터 i에 소속된 그룹의 노드수 $N_g(i)$로 했을 때 메모리 사용량(비트)은 수식 (13)과 같다.

$$M_{total} = \sum_{i=1}^{CT_i} (\mathrm{DEG_{CL}(i)} + 1) \times (CT_g(i)((N_g(i)^2 - N_g(i))/2 + 2))\log(q) \quad (13)$$



[그림 3] 네트워크 크기(노드수)별 총 메모리 사용량
[Fig. 3] Total Memory Consumption per Network Size (Node Count)

제안된 EEGCK 방법은 네트워크 계층번호 및 보안적합도에 따라 다항식 차수를 조정함으로써 보안강도를 차등화시킨다. 그림 3은 제시한 네트워크 모델에서 네트워크 크기 즉, 노드수별 보안 처리시 사용되는 네트워크 전체의 메모리량을 나타낸다. 실험에 사용되는 실험 환경 파라미터는 수식 (1)~(4)에서 사용하는 상수와 같고, 네트워크 계층수는 3, 계층별 클러스터수는 16, 클러스터에 소속된 그룹수는 6, 네트워크 크기(반경)는 500m이다. 실험은 제안된 EECGK와 SDDC를 비교하였다. 제안된 EEGCK 방법에서 BS에 가까운 1계층은 BS에 전송될 중요 데이터가 많이 집결되므로 보안강도를 높이고, 계층이 BS와 멀어질수록 보안강도를 낮추었다. 또한 보안적합도에 따라 클러스터의 보안강도를 조절하였다. 이와 같이 네트워크의 보안 환경에 따라 다항식 차수 즉 보안강도를 차별화함으로써 그림 3에서와 같이 노드수가 많아질수록 SDDC 기법보다 메모리 사용량이 줄어드는 것을 알 수 있다.

4.2 에너지 소모량 분석

4.2.1 에너지 소모 비용 수식

실험을 위해 네트워크의 각 클러스터에서 GM들의 GMPK와 CK를 한 번 갱신할 때 사용되는 에너지($E_{cluster}$)는 Rappaport[10]의 무선 에너지 소모 모델을 이용하면 수식 (14)와 같고 전체 네트워크에서 키를 한 번 갱신할 때의 에너지(E_{total})는 수식 (15)와 같다. 이를 이용하여 제안된 방법에 대한 성능을 분석한다.

$$E_{cluster} = (CT_g \times l\, E_{elec}) + CT_g^2 \times l\,(E_{elec} + \epsilon fs \times d_{toCH}^2) + (N_g + CT_g \times N_g(N_g - 1)/2) \times l\,(E_{elec} + \epsilon fs \times d_{toGL}^2) \quad (14)$$

$$E_{total} = \sum_{i=1}^{CT_c} E_{cluster}(i) \quad (15)$$

수식 (14)에서 d_{toCH}는 클러스터에 소속된 GL에서 CH까지의 평균 거리, d_{toGL}는 그룹에 소속된 GM에서 GL까지의 평균 거리이다.

네트워크의 각 클러스터에서 GL의 밀도가 클러스터 면적 전체에서 균등하다고 가정하면, 각 클러스터의 GL에서 CH까지의 예상 거리의 곱은 수식 (16) 및 (17)과 같다[11]. 이 때, k_1은 1 계층, k_i는 i번째 계층의 클러스터 수이고, R_1은 1 계층, R_i는 i번째 계층의 네트워크 반경이다.

$$\mathrm{Exp}[d_{toCH}^2] = R_1^2/2k_1 \quad (16)$$

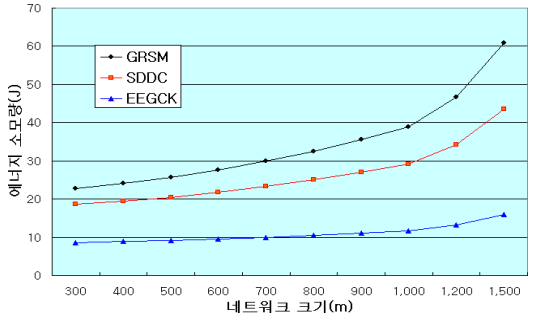
$$\mathrm{Exp}[d_{toCH}^2] = (R_i^2 - R_{i-1}^2)/2k_i \quad (\mathrm{i} \geqq 2) \quad (17)$$

같은 방법으로 각 클러스터의 각 그룹에서 GM의 밀도가 그룹 면적 전체에서 균등하다고 가정하면, 각 그룹의 GM에서 GL까지의 예상 거리의 곱은 수식 (18) 및 (19)와 같다.

$$\mathrm{Exp}[d_{toGL}^2] = R_1^2/(2k_1 \times CT_g) \quad (18)$$

$$\mathrm{Exp}[d_{toGL}^2] = (R_i^2 - R_{i-1}^2)/(2k_i \times CT_g) \quad (\mathrm{i} \geqq 2) \quad (19)$$

4.2.2 실험 결과

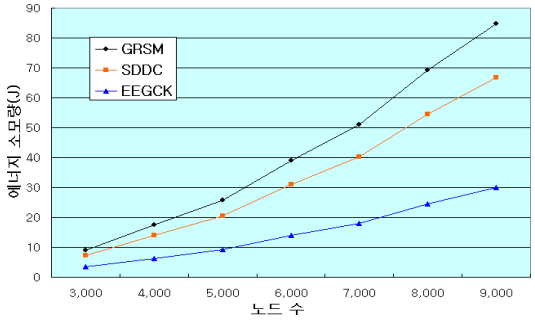


[그림 4] 네트워크 크기(m)별 보안키 갱신 총 에너지 소모량
[Fig. 4] Total Energy Consumption for Rekeying per Network Size(m)

그림 4는 네트워크 전체 보안키를 한 번 갱신할 때 사용되는 총 에너지 소모량(J)을 GRSM, SDDC 및 EEGCK 방법에서 네트워크 크기에 따라 비교 분석한 것이다. 즉, 네트워크의 노드수가 4,896, 계층별 클러스터수가 16, 클러스터별 그룹수가 6 및 그룹별 노드수가 17일 때 네트워크 크기(반경)에 따라 보안키 갱신 에너지 소모량에 대한 그래프이다. 이 때, GRSM에서는 그룹을 클러스터로 간주하였다.

그림 4에서 GRSM과 SDDC는 네트워크 크기가 커질수록 에너지 소모량이 급격하게 증가하나 EEGCK는 완만하게 증가한다. 이는 제안한 EEGCK 방법은 보안적합도에 따라 다항식 차수를 차별화하고 클러스터 내에 그룹을 두어서 보안키를 에너지 효율적으로 관리하기 때문이다. SDDC가 GRSM보다 에너지 효율이 좋은 것은 GRSM은 일반적인 그룹 방식으로 보안키를 관리하고, SDDC는 클러스터링 방식에 의한 보안키 관리 방법의 차이에서 온 것으로 판단된다. 네트워크 크기가 700m일 경우 제안한 EEGCK 방법은 위와 같은 제한된 실험 환경에서 에너지 소모량이 SDDC에 비해 57%, GRSM에 비해 67% 줄어든다. 그래서 EEGCK 방법은 SDDC에 비해 에너지 소모량을 많이 줄이고 또한 네트워크 크기가 커질수록 에너지 소모량이 서서히 증가를 하므로 네트워크 수명을 늘리는 장점이 있다.

그림 5는 네트워크 전체 보안키를 한 번 갱신할 때 사용되는 총 에너지 소모량(J)을 GRSM, SDDC 및 EEGCK 방법에서 네트워크 노드수에 따라 비교 분석한 것이다. 즉, 계층별 클러스터수가 16, 클러스터별 그룹수가 6 및 네트워크 크기(반경)가 500m일 때 네트워크 노드수에 따라 보안키 갱신 에너지 소모량에 대한 그래프이다.



[그림 5] 네트워크 노드수별 보안키 갱신 에너지 소모량
[Fig. 5] Total Energy Consumption for Rekeying per Network Node Count

그림 5에서 GRSM과 SDDC는 네트워크 노드수가 많아질수록 에너지 소모량이 급격하게 증가하나 EEGCK은 증가폭이 크지 않다. 이는 제안한 EEGCK 방법은 클러스터 내에 그룹을 두어서 네트워크 노드수가 많아질수록 GMPK를 생성할 때 에너지 소모량이 크게 증가하지 않기 때문이다. 반면에 SDDC와 GRSM 방법은 네트워크 노드수가 많아질수록 GMPK를 생성할 때 보안키를 지정

할 상호 노드수가 많아지기 때문에 에너지 소모량이 크게 증가한다고 판단된다. 네트워크 노드수가 6,000일 경우 제안한 EEGCK 방법은 위와 같은 제한된 실험 환경에서 에너지 소모량이 SDDC에 비해 55%, GRSM에 비해 64% 줄어든다.

5. 결론

본 논문에서는 대규모 센서 네트워크에서 그룹을 기반으로 한 에너지 효율적인 클러스터키 관리 방안(EEGCK)을 제안한다. EEGCK는 대규모의 센서 네트워크에서 안전하고 효율적인 키 관리를 위해 클러스터에 여러 개의 그룹을 두고 5개의 보안키 즉, SK, CK, GMPK, PK 및 MK를 사용한다. 또한 섹터, 클러스터 및 그룹 수준의 보안적합도를 관리하여 보안키 갱신 주기 및 보안에 사용되는 다항식의 차수를 차별화한다. 제안한 방법은 일부 노드의 노출 및 오염이 근접 이웃 노드까지 노출시키는 위험을 최소화하고, 네트워크 보안에 사용되는 에너지를 효율적으로 관리한다. GRSM과 SDDC는 네트워크 크기가 커질수록 에너지 소모량이 급격하게 증가한다. 제안한 EEGCK 방법은 보안적합도에 따라 다항식 차수를 차별화하고 클러스터 내에 그룹을 두어서 보안키를 에너지 효율적으로 관리하기 때문에 GRSM과 SDDC에 비해 제한된 환경의 실험 환경에서 에너지 소모량이 SDDC에 비해 55%, GRSM에 비해 65% 줄어든다. 그래서 EEGCK 방법은 GRSM과 SDDC에 비해 에너지 소모량을 줄이고 또한 네트워크 크기가 커질수록 에너지 소모량이 서서히 증가를 하므로 네트워크 수명을 늘리는 장점이 있다.

본 논문에서는 보안에 대한 모든 관리를 BS가 통제하도록 되어있다. 그러나 전술 센서 네트워크의 경우는 BS와 센서 노드와의 통신이 일부 단절되는 상황이 발생할 수 있으므로 향후에는 이러한 경우를 대비해서 클러스터 및 그룹 수준에서 지역적인 보안 관리를 할 수 있도록 하는 연구가 필요하다.

References

[1] Jin-Su Kim, Seung-Soo Shin, “A Cluster Group Head Selection using Trajectory Clustering Technique,” Journal of the Korea Academia- Industrial Cooperation Society Vol. 12, No. 12 pp. 5865-5872, 2011

[2] N. Vimala, B. Jayaram, Dr. R. Balasubramanian, "Efficient Group Key Management Protocol for Region Based MANETs," IACSIT International Journal of Engineering and Technology, Vol.3, No.1, February 2011

[3] Wan Nam-Goong, Kwan-tae Cho, Dong Hoon Lee, "Fast Group Rekeying Scheme for Secure Multicast in Wireless Sensor Networks," KIISC, Vol.21, No.3, June 2011, pp. 75-88

[4] S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," In 10th ACM conference on Computer and communication security, pp. 62-72. 2003.

[5] Wensheng Zhang, Sencun Zhu, Guohong Cao, “Predistribution and local collaboration- based group rekeying for wireless sensor networks,” Ad Hoc Networks 7, 2009, pp. 1229–1242

[6] Dong-Min Choi, Yeo-Jin Lee, Il-Yong Chung, “A Secure Key Distribution Scheme on Wireless Sensor Networks Using Dynamic Clustering Algorithms,” Journal of Korea Multimedia Society Vol. 10, No. 2, February 2007, pp. 236-245

[7] M. Bouassida, I. Chrisment and O. Festor, “Group Key Management in Manets,” International Journal of Network Security, pp. 67-79, 2008

[8] D. Liu, P. Ning, "Establishing Pairwise Keys in Distributed Sensor Networks," Proc. of the 10th AC conference on Computer and communications Security, pp. 52-61. 2003.

[9] DaeHun Nyang and Mohaisen Abedelaziz, “Strongly-Connected Hierarchical Grid-Based Pairwise Key Predistribution Scheme for Static Wireless Sensor Networks,” IEEK, Vol.43, TC-No.7, July 2006, pp. 726–735.

[10] T. Rappaport, "Wireless Communications: Principles & Practice," Englewood Cliffs, NJ: Prentice-Hall, 1996.

[11] Jin-Su Kim, Seung-Soo Shin, "An Energy Consumption Model using Hierarchical Unequal Clustering Method," Journal of KAIS, Vol. 12, No. 6, 2011.

김 진 수(Jin-Su Kim) **[정회원]**

- 1982년 2월 : 영남대학교 전기공학과 (공학사)
- 1990년 2월 : 숭실대학교 정보산업학과 (이학석사)
- 2007년 6월 : 영남대학교 컴퓨터공학과 (공학박사)
- 1992년 8월 : 정보처리 기술사
- 2006년 3월 ~ 현재 : 동명대학교 항만물류시스템학과 교수

<관심분야>
데이터베이스, 센서 네트워크, 소프트웨어 공학