情報保護學會論文誌
第 22 卷 第 1 號, 2012. 2

계층적 클러스터 센서 네트워크의 키 사전 분배 기법에 대한 연구*

최 동 민,† 심 검, 정 일 용‡
조선대학교 컴퓨터공학과

A Study of Key Pre-distribution Scheme in Hierarchical Sensor Networks*

Dongmin Choi,† Jian Shin, Ilyong Chung‡
Dept. of Computer Engineering, Chosun University

요 약

무선 센서 네트워크는 재사용이 불가능한 배터리와 제한된 처리능력, 저장 공간을 갖는 다량의 소형 노드로 이루어진다. 이 네트워크에서 노드들은 광범위한 영역에 배치되게 되며 이 노드들은 또한 무선 링크를 통해 노드들 사이에 단거리 통신을 수행한다. 네트워크의 에너지 효율을 위해 동적 클러스터링 기법이 네트워크 수명, 확장, 부하 분산에 효과적인 수단이다. 이 기법은 다수의 노드에 의해 수집되는 데이터가 클러스터 헤드 노드에 의해 집성되어 재전송되는 특징이 있어 해당 노드가 공격자에 노출될 경우 네트워크의 안전을 보장할 수 없게 된다. 그러므로 이러한 클러스터링 기법의 안전한 통신을 위해 노드들 사이에 전송되는 메시지의 암호화와 클러스터 헤드 노드의 보안 유지가 중요하다. 특히, 에너지 효율을 목적으로 설계된 클러스터 기반 프로토콜에서 충분한 데이터 안정성을 보장하기 위해서는 클러스터 구조에 적합한 키 관리 및 인증 기법이 필요하다. 이에 본 논문에서는 계층 클러스터 구조를 갖는 센서 네트워크에 적합한 키 관리 기법을 제안한다. 제안하는 기법은 다항식 키 풀 기반 기법에 기초하며 키 인증 절차를 통해 안정된 네트워크를 유지한다.

ABSTRACT

Wireless sensor networks consist of numerous small-sized nodes equipped with limited computing power and storage as well as energy-limited disposable batteries. In this networks, nodes are deployed in a large given area and communicate with each other in short distances via wireless links. For energy efficient networks, dynamic clustering protocol is an effective technique to achieve prolonged network lifetime, scalability, and load balancing which are known as important requirements. this technique has a characteristic that sensing data which gathered by many nodes are aggregated by cluster head node. In the case of cluster head node is exposed by attacker. there is no guarantee of safe and stable network. Therefore, for secure communications in such a sensor network, it is important to be able to encrypt the messages transmitted by sensor nodes. Especially, cluster based sensor networks that are designed for energy efficient, strongly recommended suitable key management and authentication methods to guarantee optimal stability. To achieve secured network, we propose a key management scheme which is appropriate for hierarchical sensor networks. Proposed scheme is based on polynomial key pool pre-distribution scheme, and sustain a stable network through key authentication process.

Keywords: Sensor network, key pre-distribution, cluster

접수일(2010년 10월 27일), 수정일(2011년 7월 30일), 게재확정일(2011년 10월 10일).
* 본 연구는 2011년도 조선대학교 학술연구비의 지원을 받아 연구되었음.
† 주저자, cdm1225@gmail.com
‡ 교신저자, iyc@chosun.ac.kr

I. 서 론

센서 네트워크는 다양한 응용분야를 가지고 있으며 이곳에 사용되는 센서 네트워크는 다양한 공격에 노출되어 있어 높은 보안성을 요구하고 있다. 그러나 만족할만한 안전성을 제공하는 공개키 기반 키 협의 기법은 센서 네트워크의 가용자원의 한계[1-2] 및 내부와 외부환경의 제약[3-5]으로 인해 적용하기에 어려움이 따른다. 이러한 특징을 고려해 비교적 적용하기 쉬운 대칭키 기반의 키 협업 기법들이 연구되고 있다. 그러나 대칭키를 기반으로 하는 기술들은 네트워크 내 키 분배와 관련된 문제가 존재한다. 기 제안된 연구들 중 일부는 관심영역에 배치되는 노드들에게 할당되는 키의 사전 분배를 이용해 이러한 문제를 개선하고자 하였다[6-13]. 그러나 이러한 방법들은 WSN 환경에서 기 제안되었던 에너지 효율적인 라우팅 방법들과 네트워크 구조에 있어 상이한 형태를 갖는다. 따라서 두 가지 영역-에너지 효율과 보안 안전성-의 융합이 어렵다. WSN에서 에너지 효율적인 라우팅 방법으로 주목을 받고 있는 클러스터 기반의 라우팅 방법들[14-21]은 네트워크 구조에 있어 네트워크 데이터 수집자인 BS(base station), 클러스터 내의 데이터 수집자인 CH(cluster head node), 클러스터 내의 참여자인 클러스터 멤버 노드 CM(cluster member node)로 이루어지는 노드의 역할이 다른 계층적 클러스터 구조로 이루어진다. 이와 같은 네트워크에서 CM은 데이터를 수집하여 자신이 속한 클러스터의 CH에 전송하며, CH는 정보를 모아 BS로 전송하는 동작을 한다.

이러한 클러스터 네트워크에서 발생할 수 있는 공격 유형에는 selective forwarding, HELLO flood, sybil attack 과 같은 유형의 공격[22]이 가능하며, 이에 대한 대응이 필요하다.

본 논문의 구성은 다음과 같다. 2장에서는 제안되었던 키 선 분배 기법들을 소개하고, 3장에서는 제안하는 기법에 대해 설명한다. 4장에서는 분석을 통해 제안 기법의 우수함을 보이며, 5장에서 결론을 맺는다.

II. 관련 연구

2.1 키 풀 기반

L. Eschenauer 와 V. D. Gligor[6]가 제안한 센서 노드들의 공유키 설정 기법으로 base station은 다수의 랜덤 키가 저장된 key pool에서 임의의 키 셋을 각 노드에 분배한다. 키 셋을 분배받은 노드들은 상호 공유되는 키를 공유키로 사용하고 공유되는 키가 없을 경우 path key를 생성하여 이를 공유키로 사용한다.

D. Liu and P. Ning[9]이 제안한 기법은 랜덤 키 선 분배 기법에서와 같이 키 값을 노드에 할당하지 않고, 키 셋업 서버에서 키를 유도할 수 있는 다항식을 생성하여 분배한다. 만약 어떤 두 노드가 동일한 차수를 갖는 다항식을 공유한다면 이 두 노드는 공유키를 유도하여 사용할 수 있다. 이 다항식은 셋업 서버에서 소수 q에 대한 유한체F_q상에서 $f(x,y)=\sum_{i,j=0}^{t} a_{ij}x^i y^j$, $f(x,y)=f(y,x)$인 t차 이변 다항식을 랜덤하게 생성한다. BS은 다수의 임의의 다항식이 저장된 pool에서 각 센서 노드에 할당할 임의의 polynomial set을 생성하여 분배받을 노드의 ID를 입력 값으로 다항식을 만들어 분배한다. 분배받은 노드는 서로 동일한 다항식으로부터 생성된 다항식이 있으면 공유키를 생성하여 사용하며 공유하는 다항식이 없을 때에는 중간 노드를 통하여 path key를 생성하여 사용한다.

2.2 그리드 기반

D. Liu and P. Ning[9]이 제안한 또 다른 기법은 센서 노드들을 $m\times m$그리드의 행(column)과 열(row)이 교차하는 지점에 위치시키고 각각의 행r과 열c에 해당하는 2m개의 다항식 $\{f_i^c(x,y),f_i^r(x,y)\}_{i=0,\ldots,m-1}$을 생성한다. 이후, i열 j행에 있는 노드에게 행과 열에 해당하는 두 개의 다항식 $f_i^c(x,y)$와 $f_j^r(x,y)$를 배분하고 ID=〈i,j〉인 다항식$\{ID,f_i^c(j,x),f_j^r(i,x)\}$를 할당한다. 행이나 열이 동일한 노드는 pair-wise key를 바로 생성할 수 있으며 간접 키 생성 단계에 노드의 위치정보를 이용하므로 쉽게 찾을 수 있고 2m개의 다항식을 사용하여 전체 네트워크에 키를 분배할 수 있으므로 효율적이다.

2.3 위치 기반

D. Liu, P. Ning[12]의 location based 기법은 필드를 정사각형의 셀$\{C_{i_c,i_r}\}_{i_c=0,1,\ldots,C-1,i_r=0,1,\ldots,R-1}$로 나누고 $\{f_{i_c,i_r}(x,y)\}_{i_c=0,1,\ldots,C-1,i_r=0,1,\ldots,R-1}$인 다항식을 각 셀에 할당하여 해당 셀에 위치한 노드는 그

셀에 할당된 다항식$\{f_{i_c,i_r}(x,y)\}$과 인접한 4개 셀의 다항식을 할당받아 인접 셀과 pair-wise key를 생성한다.

Ngo Trong Canh[13]등이 제안한 기법은 D. Liu, P. Ning[12]의 인접 셀을 8개로 정하고 인접하는 두 셀 (i,j)와 (u,v)는 동일한 키 $f_{(u,v)(i,j)}=f_{(i,j)(u,v)}$를 사용하여 보안성은 향상 시키면서 사용되는 키의 개수는 상대적으로 적게 사용하도록 하였다.

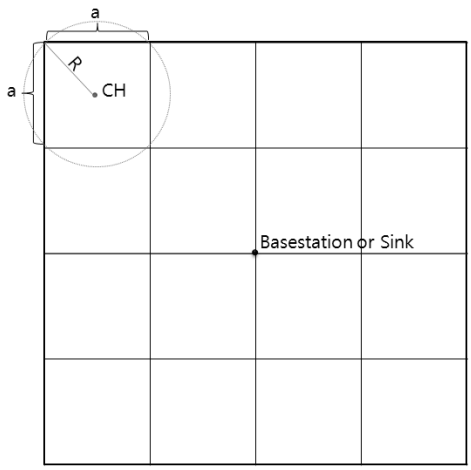
III. 네트워크 모델

3.1 가 정

제안하는 방법은 다음과 같은 사항을 가정한다. 센서 노드들이 초기에 필드에 위치하여 네트워크를 이룰 때에는 공격을 받지 않는다. 모든 노드는 한번 필드에 deployment된 후 고정되어 있다. Base station으로부터 one-hop 거리 밖에 위치한 모든 노드는 multi-hop 기반 통신을 한다. 클러스터 형성 시 클러스터 헤드는 one-hop거리의 노드들과 클러스터를 형성한다. 한 클러스터에 속한 노드는 클러스터 헤드 및 클러스터 내의 노드와 통신한다.

3.2 네트워크 구조

[그림 1]에 의하면 필드는 노드가 배치된 이후 이 노드들에 의해 클러스터를 형성한다. 이 클러스터는 인접 클러스터와의 노드 중복 현상을 고려하지 않은 형태인 정사각형 구조로 고려되었다. 또한, 본 연구에서는 필드에 배치되는 모든 노드는 골고루 분포된다고 가정하였다. 각 클러스터에 존재하는 노드의 평균 개수를 N_c개라 하고, 생성되는 클러스터의 한 변의 길이를 a, 노드의 전파 도달 거리는 R로 가정하고 $R \geq a$이다. 이 R이내에 존재하는 평균 노드의 수가 m_R이라고 가정하면, R내에 위치하는 노드의 수는 클러스터 헤드 노드를 포함한 개수인m_R+1개가 된다. 아래의 [표 1]은 제안하는 방법에서 사용되는 표기법을 나타낸다.



[그림 1] 제안하는 기법의 네트워크 구조

이것으로부터 네트워크 내부의 센서 노드의 밀도를 계산하면 노드의 밀도는 다음의 식 (1)과 같다.

$$N_d = \frac{(m_R+1)}{\pi R^2} \tag{1}$$

이 식으로부터 한 개의 클러스터에 위치한 노드의 개수는 다음의 식 (2)로 나타낼 수 있다.

$$N_c = N_d a^2 = \frac{(m_R+1)a^2}{\pi R^2} \tag{2}$$

3.3 공격 유형

위와 같은 계층적 클러스터 센서 네트워크에서 가능한 라우팅 공격 유형을 보면 다음과 같다.

Selective forwarding - 공격 노드가 특정 메시지의 전송을 거부하거나 삭제하는 공격이다. 이 공격은 특정 노드로의 전달이나 데이터를 거부함으로써 노드들의 통신을 단절시키거나 BS 으로 수집되는 정보의 신뢰성을 저하시킨다.

HELLO flood attack - 노드들의 경로 설정 단계에서 멀리 있는 공격자가 강한 강도의 HELLO 패

[표 1] 표기법

Symbol	Definition
ID_i	노드의 ID
N_i	센서 식별자
C_i	클러스터 식별자
r	선정된 임의의 값
R	노드의 전파도달 거리
a	클러스터 한 변의 길이
m_R	노드 전파도달거리 R 이내에 존재하는 평균 노드 수
k	노드에 할당된 키의 개수
N_d	네트워크내 센서 노드의 밀도

킷을 보냄으로써 일반 노드들의 경로 설정 시 공격 노드가 라우팅에 참여를 시도하는 형태의 공격이며 센서 노드들의 라우팅을 혼란시킨다.

Sybil attack - 공격 노드가 많은 수의 노드 ID를 가지고 이를 공격에 사용하는 방법이다. 이 공격은 정상 노드가 공격 노드인 것으로, 또는 공격 노드가 정상 노드인 것으로 가장할 수 있으며 라우팅 경로를 변경하여 공격 노드가 라우팅 경로에 포함되게 할 수 있다.

IV. 제안 방법

위와 같은 유형의 공격은 비밀키 공유와 인증을 통해 대응이 가능하며 제안하는 기법은 이변수 다항식을 이용한 pair-wise key를 생성하는 키 선분배 기법이며 키의 추출은 키 풀에서 생성된 키를 노드에 할당하는 형식이다. 이 기법은 크게 키 사전 키 배포 단계, 공유키 설정 단계, 경로키 생성의 3단계로 이루어진다.

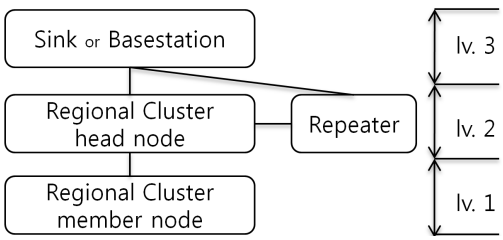
또한 계층적 클러스터 네트워크 구조[21]에 의하면 노드는 그 역할에 따라 3가지 레벨로 구분이 가능하다. 다음의 [그림 2]는 노드의 역할에 따라 3가지 레벨로 구분된 ARCS 기법의 네크워크 구조를 나타낸다.

각 레벨에 요구되는 키는 다음과 같다.

level 1에서 사용되는 키의 요구사항 - 사전에 분배된 키 셋을 이용해 확률적인 링크를 구성한다. 가장 기본이 되는 키이다. 클러스터 내의 멤버 노드에서 사용한다.

level 2에서 사용되는 키의 요구사항 - level 1의 키와는 다른 키를 상위 레벨로부터 받아 사용한다. level 2가 된 노드는 BS의 인증 절차를 거쳐 level 2로 동작하게 된다. CH 및 리피터 노드에서 사용한다.

level 3에서 사용되는 키의 요구사항 - 모든 키를 알고 있으며 키를 만들 수 있다. BS 및 Sink에서 사용한다.



[그림 2] ARCS의 네트워크 구조

4.1 사전 키 배포 단계

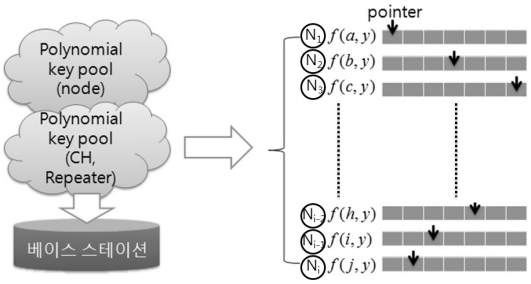
BS이 생성하는 t차 이변 다항식 pool의 크기가 P라고 가정하고, 노드에 임의로 할당되는 키의 개수는 k라고 가정하자. 제안하는 방법에서 base station은 두 개의 키 풀을 생성하여 유지하며, 각각 일반 노드와 상위 노드의 키 설정에 사용한다. 그리고 이 키는 중복해서 사용되지 않는다. 이렇게 사용하는 키를 구분하면 일반 노드에서 노출되는 키로 인해 상위 레벨의 노드가 포획되는 문제를 완화하는 효과가 있다. 이 base station은 소수q에 대한 유한체F_q 상에서 임의의 t차 이변 다항식을 다음의 식 (3)과 같이 생성하며 이 식은 $f(x,y)=f(y,x)$을 만족한다.

$$f(x,y)=\sum_{i,j=0}^{t} a_{ij}x^i y^j \tag{3}$$

이 k개의 키를 이용하여 모든 노드들은 공유키를 설정하여 인접하는 노드들 사이에 연결을 한다. 제안하는 방법에서 level 1의 모든 노드가 시도하는 연결은 기존의 다항식 풀 기반 방법과 같은 확률 기반 연결이며, level 2에서 이루어지는 CH 및 repeater의 연결은 BS의 제어에 의한 키 분배를 이용한 직접 연결이다. CH와 repeater는 데이터 모음과 중계의 역할을 수행하므로 네트워크에서 중요도가 높아 확률적인 연결은 고려되지 않았다. 두개의 키 셋업 중 확률 연결이 이루어지는 level 1에서 두 개의 이웃하는 노드 사이에 최소한 1개의 키를 공유하는 확률을 라고 정의하면 이는 다음의 식 (4)에 의해 계산할 수 있다.

$$p'=1-\frac{((P-k)!)^2}{(P-2k)!P!}\simeq\frac{(1-k/P)^{2(P-k+0.5)}}{(1-2k/P)^{(P-k+0.5)}},\quad 0\le p'\le 1 \tag{4}$$

또한 각 노드에 할당된 개의 키는 임의로 생성된 포인터와 연결되어 있다. 이 포인터는 시간을 입력값으로 한 의사난수함수의 결과값에 의해 매 라운드 마다 이동하여 다른 키를 가리킨다. 각 노드별 k개의 키와 포인터 위치는 BS가 생성하여 배포하는 것으로서 BS는 사전에 모든 정보를 알고 있으며, ARCS기법의 사전 정의에 의해 전체 네트워크는 시간적으로 동기화되어 있으므로 BS는 매 라운드마다 바뀌는 노드의 포인터 위치를 알고 있다. BS는 이 포인터 정보를 이용하여 CH가 되고자 하는 노드의 인증을 수행한다. 아래



〔그림 3〕 BS에서 노드에 임의로 할당된 키와 키 포인터

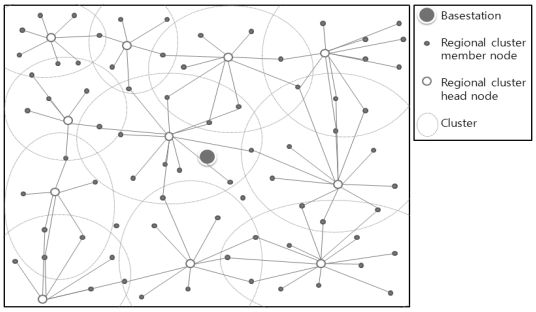
〔그림 3〕은 BS가 키 풀에서 노드에게 임의로 할당한 k개의 키와 포인터를 나타낸다.

4.2 공유키 및 경로키 설정 단계

제안하는 방법은 계층적 클러스터링 기법 중 ARCT〔21〕와 ARCS 방법을 기초로 한 키 분배 및 공유이므로 ARCT, ARCS의 클러스터 생성 절차에 맞추어 키를 분배한다. 다음의 〔그림 4〕 는 ARCS 기법의 클러스터 생성 절차를 나타낸다. ARCT와 ARCS 는 2단계 클러스터링을 통해 네트워크에서 발생하는 데이터 중복을 배제한 클러스터링 기법이다. 이 기법은 1단계에서는 인접한 노드들과 중복하여 수집하는 데이터를 배제하기 위해 특정 지역을 대표하는 동작 노드를 노드에 할당된 노드 동작지연시간을 이용한 경쟁조건에 의해 선별한다. 2단계에서는 지역 대표 동작 노드로부터 수집되는 데이터를 취합하여 전송하는 CH를 선정하고 CH간 연결을 돕는 repeater를 선정하여 네트워크를 구성한다.

```
CH_region  : regional cluster head node
Repeater   : relay node
N_region   : regional cluster member node
N_normal   : normal node before network setup
N_operation: operation node before clustering
N_sleep    : sleep node

Initialize :
    1. generate( random_delay time )
       /by normal nodes

Main Processing:
  /clustering process by normal nodes
    1.if(nodes weighted value > 0)
    2. decrease weighted value by 1 point
    3.end if
    4.Calculate available time slot period by
      weighted value
    5.delay time <- generate( available time
      slot)
    6.wait for delay time or until receiving {any
      advertisement message}
    7.if(delay time_Expired)
    8. if(nodeID == N_normal)
         become N_operation
         broadcast( the Advertisement
                Message {nodeID,
                sensing value, position})
    9. elseif(nodeID == N_normal && receiving
         {any advertisement message})
    10. if( receive the Advertisement
          Message{sensing value} ==
                        sensing value )
          become Nsleep
    11. else
          become N_operation
          broadcast( the Advertisement
                Message{nodeID, sensing
                    value, position})
    12. end if
    13.end if
    14.else
          wait for delay time or until
          receiving {any advertisement
                        message}
    15.end if

    16.if(nodeID == N_operation)
          increase weighted value by 1 point
          delay time
           <- generate(random_delay time)
    17. wait for delay time or until
        receiving {any advertisement
                        message}
    18.if(delay time_Expired)
    19. if( nodeID == N_operation)
          become CH_region
          increase weighted value
                        by 2 points
          broadcast(the Advertisement
            Message {NodeID, position})
    20. else
          cancel the delay time
    21. end if
    22.else
    23.if(receive the Advertisement Message)
          cancel the delay time
          become N_region
     else
          wait for delay Time or until
          receiving {any advertisement
                        Message}
    24.end if
    25.end if
    26.if( nodeID == N_region )
    27.if( # of neighbor CH_region))2&&
            # of neighbor CH_region<6)
    29.  become repeater
    30.  broadcast( the Advertisement
         Message {NodeID, position} )
    31.end if
    32.end if

CH_region
    1.broadcast( the Advertisement Message
      {nodeID, sensing value, position} )
    2.accept( join Message )
    3.compare stored sensor data with sensed
      event whether it same or not
    4.aggregate sensing data
    5.transmit_data_to_Sink (sensing value,
      nodeID, position)

N_region
    1.join to cluster( CHnodeID, nodeID,
      position )
    2.operate as an region cluster member node
    3.compare stored sensor data with sensed
      event whether it same or not

Repeater
    1.join to cluster( CHnodeID, nodeID,
      position )
    2.operate same as an regional cluster head
      node with data relay only
    3.compare stored sensor data with sensed
      event whether it same or not
    4.relay data
```

〔그림 4〕 ARCS의 클러스터링 의사코드

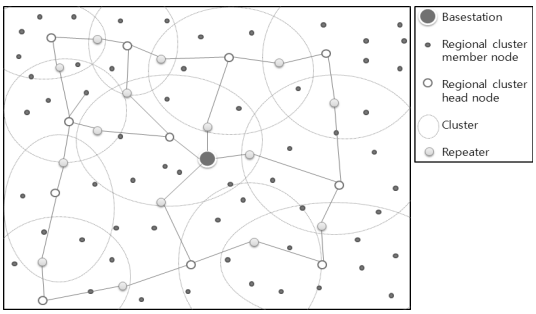


〔그림 5〕 클러스터 구성

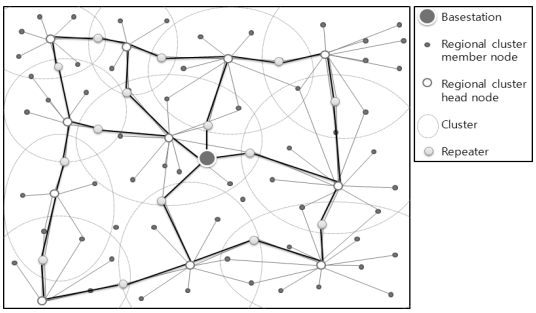
다음의 〔그림 5〕는 네트워크의 클러스터 구성 절차를 나타낸다. 클러스터 구성 단계에서 네트워크의 모든 멤버 노드는 자신이 보유하는 개의 키 중 인접 노드와 공유하는 키를 이용하여 노드의 ID를 이용해 인접 노드와 pair-wise key를 생성한다.

아래의 〔그림 6〕은 CH노드와 Repeater 노드의 선정과 키의 분배를 나타낸다. CH와 Repeater 노드는 자신의 키를 이용하여 BS에 클러스터 내 노드들의 공유키와 CH와 Repeater 간 멀티홉 통신을 위한 키를 요청하며, BS는 인증절차를 통해 키를 분배한다.

아래의 〔그림 7〕은 BS에 의해 분배받은 키를 공유하여 구성한 네트워크를 나타낸다. BS에 의한 인증



〔그림 6〕 CH와 Repeater의 선정



〔그림 7〕 네트워크의 키 공유

절차를 마치고 키를 분배받은 CH는 자신이 분배받은 클러스터 내 공유키를 이용해 자신의 클러스터에 포함된 멤버노드와 통신한다.

ARCT기법의 클러스터 구성 절차에 따라, 자신에게 할당된 동작지연시간의 값이 만료되어 CH가 되고자 하는 노드는 자신이 CH임을 자신의 전송반경 이내에 위치한 인접 노드에 알리며, 이 신호를 수신한 인접한 곳에 위치한 노드들 중 level 1단계의 공유키를 발견한 노드와 발견하지 못한 노드 모두 CH가 되기를 포기하고 CH의 멤버노드가 되기 위한 대기상태로 들어가며, 이후 BS의 인증을 마친 CH가 멤버노드에 클러스터 내에서 사용할 클러스터 공유키를 전달하면 멤버노드는 이 키를 공유하여 클러스터 내 멤버 노드로 동작하게 된다. 이 때 level 1단계의 공유키를 소유하는 멤버노드들은 CH와의 공유키를 이용하여 클러스터 내 공유키를 받으며, 공유키를 소유하지 못한 멤버노드는 인접한 멤버노드와 경로키 설정을 통해 클러스터내 공유키를 받아 CH와 키를 설정하게 된다.

- level 1

클러스터를 구성하기 위해, 네트워크의 노드들은 주어진 영역에서 상호 공유키를 설정하는 과정을 거쳐 클러스터를 구성한다. 이 클러스터는 해당 라운드만 유지되며 매 라운드마다 변경되므로 주기적인 클러스터 재설정이 필요하다. 이때 노드들 사이에 반복적인 공유키 설정이 필요하게 된다.

(1) 클러스터를 설정하는 과정에서 CH가 되고자 하는 노드는 자신이 소유하고 있는 k개의 키 부분정보를 포함한 패킷을 자신의 전송 반경 내에 위치한 인접 노드들에게 브로드 캐스트 한다.

(2) 인접 노드들 중 공통의 키를 소유한 노드들은 자신이 CH가 되려던 시도를 포기하고 CH의 BS인증 후 클러스터 내 공유키를 전송받을 때까지 대기한다.

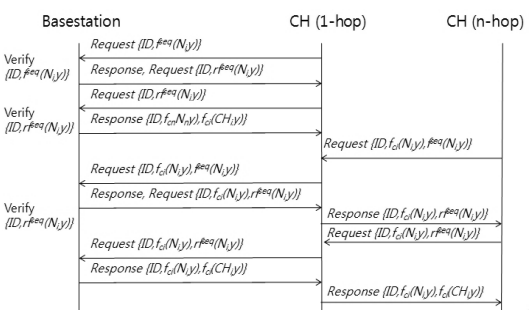
(3) 공통의 키를 소유하지 못한 노드들 또한 대기한다. 그러나 공격자에 의한 공격일 수 있으므로 이를 구분하기 위해 클러스터 내 공유키와 경로키 설정이 되기까지 대기시간을 더 연장한다. 클러스터 내 공유키와 경로키 설정이 이루어지지 않을 시 다시 CH가 되기 위한 타이머를 동작한다.

(4) 특정 클러스터의 멤버노드가 된 노드들은 이

후 CH의 인증절차를 통해 클러스터 내 공유 키를 받아 클러스터 내 노드들의 통신에 사용한다. pair-wise를 이루고자 하는 임의의 두 노드N_i, N_j는 각 클러스터별로 할당된 다항식에서 생성된 polynomial share $f_{Ci}(N_i,y)$와 $f_{Ci}(Nj,y)$를 가지고 있다. 이 각각의 polynomial share에 상대 노드의 ID를 y값에 입력하여 $f_{Ci}(Ni,Nj)$와 $f_{Ci}(Nj,Ni)$를 생성할 수 있으며 $f_{Ci}(Ni,Nj)=f_{Ci}(Nj,Ni)$이므로 동일 클러스터에 속한 노드이며 pair-wise key를 생성하게 된다.

- level 2

CH로 선정된 노드는 자신이 소유한 k개의 키들 중 포인터가 위치하지 않은 k-1개의 키들 중 임의의 키와 키의 순서번호 $f^{seq}(N_iy)$와 자신의 ID를 이용하여 BS과 통신을 시도한다. ARCS의 경우 리피터로 선정된 노드도 동일한 절차로 동작하며, 이는 통신 도중 키의 유출이 발생할 경우 포인터의 위치를 숨기기 위한 것이다. BS은 해당 노드와 키 순서번호를 검사하고 노드의 검증을 위해 임의의 키 순서번호에 위치한 $rf^{seq}(N_iy)$키를 요청한다. CH에 의한 임의의 키 전송과 키 재검증이 종료된 후 BS은 앞의 식으로 생성된 다항식 pool에서 임의의 클러스터 센서노드$CH_i(N_n)$에 대해 클러스터 헤드 CH_n에 분배되는 다항식 $f_{Cn}N_ny$, 클러스터 헤드간 pair-wise 형성을 위해 다항식에 클러스터 헤드의ID를 입력하여 생성한 $f_{ci}(CH_iy)$를 각 클러스터 헤드에 분배한다. 클러스터 헤드는 클러스터 내 pair-wise key 형성을 위해 BS에게 받은 다항식 $f_{Ci}(x,y)$을 사용하여 polynomial share $f_{Ci}(\ni,y)$를 생성한 후 노드에 분배한다. 또한



〔그림 8〕 BS에 의한 CH 인증 절차

클러스터와 헤드 사이에 pair-wise key형성을 위해 base station으로부터 받은 polynomial share를 인접 클러스터 헤드와 교환하여 pair-wise key를 생성한다. 아래의 〔그림 8〕은 BS과 1홉 거리 이내에 위치한 CH, BS과 1홉 거리 밖에 위치한 CH의 BS에 의한 인증 절차를 나타낸 것이다.

- level 3

BS은 하위 레벨 1,2의 노드들과 인증을 통한 안정된 네트워크를 구성하며, 레벨 2의 모든 노드는 네트워크의 안정된 동작을 위해 BS의 인증이 꼭 필요하다. 또한, 클러스터 내부에서 사용하는 클러스터 내 공유 키와 클러스터 헤드 노드간 멀티홉 통신을 위한 클러스터 헤드 노드 간 공유 키를 생성하여 분배하는 역할을 한다.

(1) 노드의 삽입

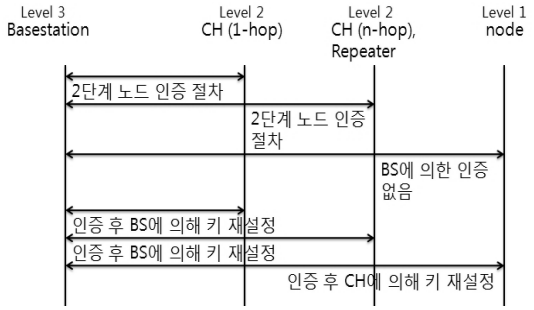
새로운 노드의 삽입시, 새로운 노드 또한 BS로부터 k개의 키와 포인터를 부여받는다. 이 키에 의해 인접 노드와 클러스터를 형성 시 키를 설정한다.

(2) 노드의 삭제

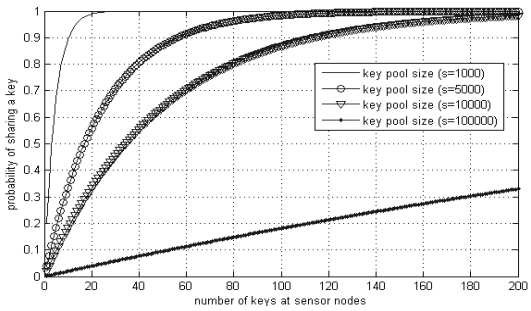
노드의 경우, 외부 공격에 의한 노드의 손실이 감지되면 해당 노드가 보유한 k개의 키 정보는 폐기해야 하므로 BS에 의해 전체 네트워크의 노드에 해당 키의 폐기를 요청하는 패킷을 브로드캐스트 하며 폐기 요청을 수신한 모든 노드는 해당 키를 리스트에서 삭제한다.

4.3 노드 인증 단계

계층적 센서 네트워크에서 노드의 인증은 일반 노드에게는 적용되지 않는다. 일반 노드는 최하위 계층으로서 내 외부로부터의 공격에 취약하며 이 노드들을 모두 인증하기 위해서는 상당한 자원의 소모가 필요하고 노드의 숫자에 비례해 요구 시간 및 자원이 증가하므로 사실상 불가능하다. 상위레벨의 CH 노드는 클러스터 단위의 데이터 수집자 역할을 하며 데이터 중계의 역할을 담당한다. 따라서 상대적으로 높은 보안 안전성을 요구하며 그 숫자도 일반 노드에 비해 상당히 적다. 그러므로 안전한 데이터 취합과 전송을 위해 CH 노드 레벨부터 BS의 인증이 필요하다. 아래 〔그림 9〕 는 계층적 센서 네트워크의 일반적인 레벨 구분과 인증 및 키 재설정 과정을 나타내며 CH는 〔그림 8〕의 2단계 인증 과정을 거친다.



〔그림 9〕 네트워크 레벨 구분과 키 분배 및 인증 절차



〔그림 10〕 확률기반에서 노드간 1개의 키를 공유할 확률

V. 성능 평가

본 장에서는 제안하는 기법을 Matlab을 이용하여 관련연구의 키 분배 기법과 비교, 분석하였다. 실험환경은 아래의 〔표 2〕와 같다. 라운드는 3프레임으로 구성되며 LEACH와 동일한 조건을 적용하였다.

TEEN과 APTEEN에서 사용되는 임계값 전송 확률은 계절별 기온 데이터에 따라 H_{th}=-3부터 3까지, S_{th}=0.2를 적용하였으며, APTEEN의 고정 전송 횟수는 3라운드마다 1회의 전송을 적용하였고 클러스터 헤드 노드의 수는 5%를 적용하였다. 제안하는 키 분배 방법은 동적 클러스터 모델을 고려하여 기존의 정적 모델과 비교에 무리가 있으므로 단일 round에서의 키 분배를 고려하여 클러스터가 고정된 상태에서의 노드간 연결도, 키 유도 방식, 최대 노출키 수(키 노출에 따른 견고성), 키 노출 피해범위, 키의 갱신 오버헤드, 노드에 저장되는 키의 메모리 오버헤드, 노드 포획에 대한 안전성에 대해 동일 조건을 주어 비교에 용이하도록 하였다.

〔표 2〕 시뮬레이션 파라메터

Item	Value
전자 에너지	$E_{elec}=50nJ/bit$
증폭 에너지 (free space model)	$E_{fs}=10pJ/bit/m^2$
증폭 에너지 (multipath model)	$E_{mp}=0.0013pJ/bit/m^4$
Scheduling 에너지	$E_{schedule}=5nJ/bit/signal$
데이터 병합 에너지	$E_{da}=5nJ/bit/signal$
데이터 크기	$l=1000bit$
전체 노드 수	$N=1000$
네트워크 면적 한 변의 길이	$M=200m$

5.1 노드간 연결도

확률기반 키 분배 기법들은 〔그림 10〕에서 보이는 바와 같이 키 풀에서 임의로 선택된 서브키 셋을 노드들에게 분배하는 기법을 사용하므로 전체 네트워크에 분포된 모든 노드들에 대해 완벽한 연결을 보장할 수 없다.

5.2 오버헤드

● 노드의 키 저장 오버헤드

확률기반 키 분배 기법에서 메모리 오버헤드 C는 s'를 노드에 할당되는 subset의 크기로 가정하면 다음의 식 $C=s'(t+1)\log_2 q$과 같다.

● 키의 갱신 오버헤드

동일한 다항식을 사용하여 polynomial share를 생성한 노드들이 해당된다.

● 노드의 키 계산 오버헤드

클러스터를 구성하는 센서 노드의 수를 클러스터에 할당된 t차 이변 다항식의 차수를 넘지 않도록 제한한다면 이웃 노드의 수를 최대 $t-1$개까지 제한할 수 있으므로 작은 오버헤드를 가진다.

5.3 키 견고성

임의의 t차 이변 다항식을 사용한 키 생성 및 분배 방법을 사용하는 모든 방법들은 노드의 ID를 이용하여 polynomial share를 생성하고 이 polynomial share에 상대 노드의 ID를 입력하여 pair-wise key를 생성한다. 이러한 기법은 t차 이변 다항식의 차수 t개 까지는 노드가 노출되어도 다항식이 노출되지 않으며 t+1개가 노출되었을 때 다항식이 노출된다.

5.4 키 노출 피해범위

동일한 키를 가지고 있는 노드들은 동일한 다항식을 사용하므로 다항식의 노출 피해범위에 해당된다.

5.5 노드 포획에 대한 안전성

앞의 조건에 의해 t차 이변 다항식의 차수 t개 까지는 노드가 노출되어도 다항식이 노출되지 않으며 t+1개가 노출되었을 때 다항식이 노출된다.

한 개의 클러스터에 위치한 노드의 개수 가 다음과 같을 때 $N_c = N_d a^2 = \frac{(m+1)a^2}{\pi R^2}$ 이므로,

특정 클러스터에 위치하며 다항식을 공유할 센서 노드의 수 N_s는 전송 범위를 기본 단위로 놓았을 때 공유하는 polynomial의 개수에 대해 공유하는 클러스터를 입력한 아래의 식 (5)로 나타낼 수 있으며 의 N_s수를 t개까지 제한하면 다항식의 노출시 사용되는 다항식에 대한 안전성을 갖는다.

$$N_s = \frac{C_s(m+1)a^2}{\pi} \qquad < (t+1) \tag{5}$$

공격자에 의해서 노출되는 네트워크 상의 센서 노드의 비율을 p_c라고 가정하자. 이것은 각각의 센서 노드가 노출될 확률 p_c를 가지고 있는 것을 의미한다. 그러므로 특정한 클러스터에서 같은 다항식을 공유하는 센서 중 i개 센서가 노출될 확률은 다음의 식(6)과 같다.

$$P_c(i) = \frac{N_s!}{(N_s - i)!i!} p_c^i (1-p_c)^{N_s - i} \tag{6}$$

따라서 이 클러스터에 할당된 다항식이 노출된 확률은 전체에서 노출된 노드에 할당된 다항식을 제하므로 다음의 식 (7)과 같다.

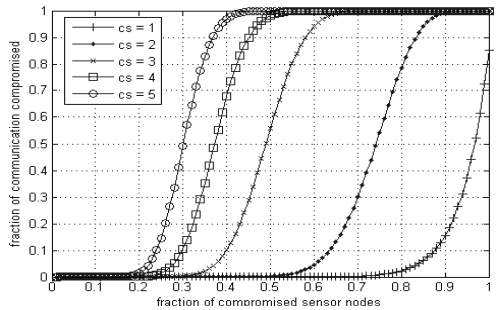
$$P_c = 1 - \sum_{i=0}^{t} P_c(i) \tag{7}$$

다음의 〔그림 9〕는 포획된 노드의 비율과 노출된 키의 비율에 대한 관계를 나타낸다.

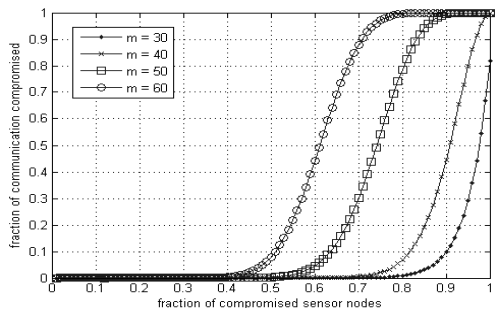
〔그림 11〕의 는 클러스터의 크기를 나타내며, C_s는 다항식을 공유하는 클러스터의 개수를, m은 노드의 수를 나타낸다. 위의 그래프에서 우리는 다항식을 공유하는 클러스터가 적을수록, 노드의 수가 적을수록, 클러스터의 크기가 작을수록 더 견고함을 알 수 있다. 특히 (a)의 공유하는 클러스터에 따른 견고성의 변화 그래프는 인접 셀과 동일 다항식을 공유하는 기존의 셀 기반 기법들에 취약점이 된다. 제안하는 기법은 BS로부터 받은 다항식을 인접노드와 키 공유에 사용하므로 공유하는 클러스터에 대해 키 노출위험을 감소시킬 수 있다.

5.6 취약한 공격에 대한 저항성

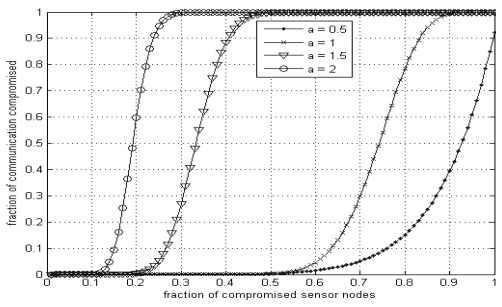
Selective forwarding - Selective forwarding



(a) a=1, m=50



(b) a=1, C_s=2



(c) m=50, C_s=2

〔그림 11〕 포획된 노드와 노출된 키의 관계

을 위해 공격 노드가 발생하는 조건을 고려하면, 일반 노드의 경우 베이스 스테이션의 인증을 거치지 않으므로 발생 가능하며 이때 공격 가능한 범위는 클러스터 내부가 될 수 있다. 그러나 이때에도 베이스 스테이션의 인증을 받는 클러스터 헤드 노드의 인증을 거쳐야 하기 때문에 노드의 모든 키와 포인터 정보가 노출되지 않는다면 해당 공격은 불가능하며, 발생할 경우에도 단일 클러스터 영역 내부로 제한된다.

HELLO flood attack - 네트워크 노드의 경쟁기반 셋업에서 HELLO flood attack 이 발생할 경우 유출된 키와 동일 정보를 공유하는 네트워크의 모든 노드는 sleep 모드로 전환하여 네트워크에 참여하지 않는다. 또한, 다항식 기반 키를 이용하므로 t+1개의 키가 노출되지 않는다면 공격으로부터 안전하게 된다. 네트워크 셋업 이후는 베이스 스테이션의 인증을 거치므로 사실상 불가능하다.

Sybil attack - 셋업 구간에서 공격이 발생할 경우, 네크워크 셋업이 노드의 시간 경쟁에 기초하므로 공격이 제한된다. 또한 베이스 스테이션의 인증을 받은 클러스터 헤드 노드의 인증 절차가 있으므로 공격이 불가능하다.

〔표 3〕 제안하는 방법의 안전성 및 효율 비교

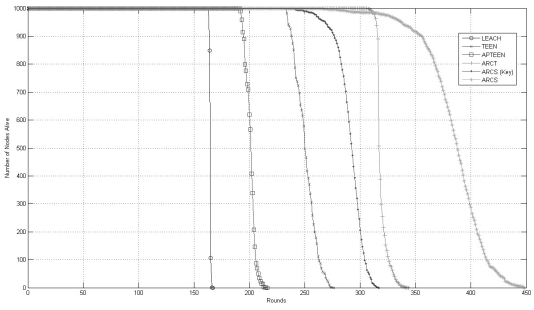
항목	Random [5]	Pool[9]	Grid [9]	Location [12]	Location [13]	Proposed
키설정 확률	0.99	0.99	1	1	1	0.99
키유도 방식	키	t	t	t	t	t
최대 노출키 수	1	t+1	t+1	t+1	t+1	t+1
키노출 피해범위	동일키	동일 다항식	동일 다항식	5셀	8셀	동일 다항식
키갱신 오버헤드	동일키	동일 다항식	동일 다항식	5셀	8셀	동일 다항식
노드저장 오버헤드	random	random	2	5	8	random
키 계산 오버헤드	없음	이웃 노드수	이웃 노드수	이웃 노드수	이웃 노드수	이웃 노드수(클러스터 내부 한정)
BS인증	최초 1회	최초 1회	최초 1회	최초 1회	최초 1회	최초 1회,+ 라운드 1회

5.7 네크워크 수명에 미치는 영향

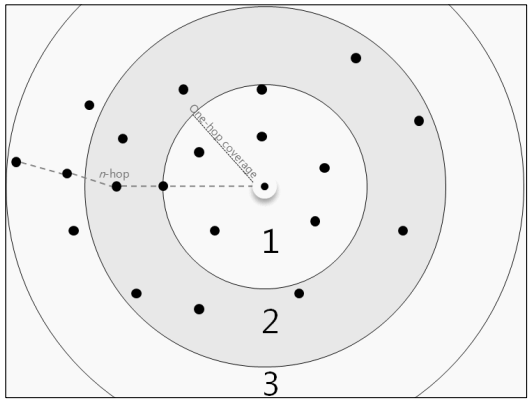
아래의 〔그림 12〕에 의하면 ARCS(key)로 표기한 제안하는 키 관리 및 인증 기법은 ARCS에 적용했을 경우 키 관리 기법을 적용하지 않은 ARCT 기법에 약간 못 미치는 네트워크 수명을 나타낸다. 이는 베이스 스테이션에 의한 노드의 인증 절차가 포함되어 있기 때문으로 보인다. 그러나 현재까지 제안된 클러스터링 기법들과 비교하여 볼 때, 제안하는 방법은 높은 수준의 네트워크 수명을 유지함을 알 수 있다.

5.8 영역별 소비 에너지

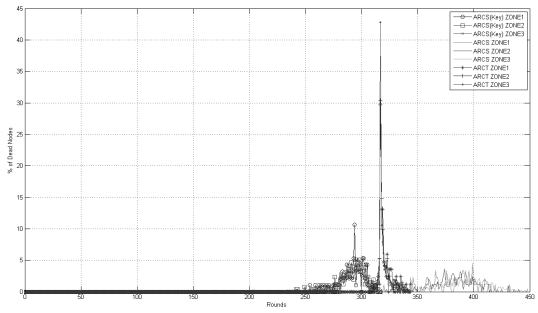
멀티 홉 기반 네트워크에서 전체 네트워크의 수명은 싱크 노드와 1홉 거리로 인접하는 노드들의 수명에 의해 결정된다. 이를 감안하여 싱크 노드와 인접한 노드와 그렇지 않은 노드들과의 영역별 에너지 소비 비율을 측정하기 위해 아래의 〔그림 13〕과 같이 영역을 분할하였다. 에너지 홀 문제는 싱크와 1-hop 거리 이내로 인접한 노드들에게서 주로 발생한다. 따라서 아



〔그림 12〕 제안하는 방법의 네트워크 수명 비교 그래프



〔그림 13〕 에너지 소비 측정을 위한 네트워크 영역 분할



〔그림 14〕 영역별 사망노드 발생 비율 비교

래의 그림에서 1영역에 해당하는 부분의 에너지 소비율을 다른 영역의 에너지 소비율과 비교해 보면 네트워크의 영역별 에너지 소비율을 알 수 있다.

위의 〔그림 14〕에 의하면 제안하는 방법은 특정 라운드에서 발생한 10%대의 사망노드 발생률을 제외한 노드 사망의 평균값이 키 관리 기법을 적용하지 않은 ARCT에 비해 완만한 경사도를 그리며 낮은 비율의 사망노드 발생률을 보임을 알 수 있다. 이는 네트워크의 연결도의 급격한 저하를 막아 네트워크가 분할됨을 지연시키는 역할을 한다. ARCT는 네트워크의 긴 수명에 비해 네트워크의 분할이 발생할 여지가 높아 후반부에 안정적인 네트워크 유지를 기대하기 어렵다. 그러므로 부하 분산이 이루어진 ARCS에 제안하는 키 관리 기법을 적용하는데 큰 문제가 없으며 이전의 기법보다 높은 네트워크 안정성을 보임을 알 수 있다.

VI. 성능 평가

본 논문에서는 계층적 클러스터를 기반으로 한 센서네트워크의 키 분배 방법에 대해 제안하였다. 무선 센서 네트워크에서 에너지 효율과 보안은 개별적으로 생각할 수 없다. 따라서 위와 같은 클러스터 네트워크의 키 분배 방법을 제안하게 되었다.

이 논문의 핵심 아이디어는 t차 2변 다항식의 polynomial share를 이용한 키 선분배 기법으로 클러스터 네트워크의 주기적인 노드의 연결을 쉽게 이루고, 여기에 신뢰할만한 BS에 의한 CH의 인증을 매 라운드마다 반복함으로써 안정적인 클러스터의 유지가 가능하게 되었으며, 각 클러스터에 사용하는 개별 키를 할당함으로써 클러스터 내 보안이 향상되었다. 또한 CH간 멀티홉 전송에 사용되는 키를 별개로 지정하여 멀티홉 전송시 발생할 수 있는 외부 공격에 대한 보안성을 향상시켰다.

제안하는 방법은 기존의 그리드 기반 키 분배 방법이나 위치 기반 키 분배 방법, 고정 클러스터 기반 키 분배 방법들을 고려하면 〔표 3〕과 같이 에너지 보존이나 클러스터 내 보안의 향상에 있어 상대적으로 우수함을 알 수 있다. 제안하는 방법은 다른 기법과 마찬가지로 매 라운드 이동시 클러스터 형성 및 키 분배에 따른 오버헤드가 존재한다. 그러나 오버헤드를 고려하더라도 기존의 키 관리를 고려하지 않은 라우팅 기법들에 비해 높은 에너지 소비 호율을 보이는 것을 알 수 있다. 차후 연구에서는 이러한 부분들을 고려하여 더욱 개선된 효율과 안정성을 보이는 기법을 제안하고자 한다.

참고문헌

〔1〕 Ronald Watro, Derrick Kong, Sue F. Cuti, Charles Gardiner, Charles Lynn, and Peter Kruus, "TinyPK: Securing Sensor Networks with Public Key Technology," Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks, pp. 59-64, Oct. 2004.

〔2〕 David Carman, Peter Kruus, and Brian Matt, "Constraints and Approaches for Distributed Sensor Network Security," NAI Labs, The Security Research Division Network Associates, Inc. 3060 Washington Road (Rt. 97) Glenwood, MD 21738-9745, Sep. 2000.

〔3〕 Adrian Perrig, John Stankovic, and David Wagner, "Security in Wireless Sensor Networks," Communications of the ACM SPECIAL ISSUE: Wireless sensor networks, vol. 47, no. 6, pp. 53-57, Jun. 2004.

〔4〕 Ning Hu, Randy K. Smith, and Phillip G. Bradford, "Security for Fixed Sensor Networks," Proceedings of the 42nd annual Southeast regional conference, pp. 212-213, 2004.

〔5〕 Donggang Liu and Peng Ning, Security for Wireless Sensor Networks: advances in Information Security, 1st Ed., Sprin-

ger, pp. 1-6 , Nov. 2007.
[6] Laurent Eschenauer and Virgil D. Gligor, "A key-management scheme for distributed sensor networks," Proceedings of the 9th ACM Conference on Computer and Communications Security, pp. 41-47, Nov. 2002.
[7] Haowen Chan, Adrian Perrig, and Dawn Song, "Random Key Predistribution Schemes for Sensor Networks," IEEE Symposium on Security and Privacy, pp. 197-213, May 2003.
[8] Carlo Blundo, Alfredo De Santis, Amir Herzberg, Shay Kutten, Ugo Vaccaro, and Moti Yung, "Perfectly-secure key distribution for dynamic conferences," Proceedings of the 12th Annual International Cryptology Conference on Advances in Cryptology, pp. 471-486, Aug. 1992.
[9] Donggang Liu and Peng Ning, "Establishing pair-wise Keys in Distributed Sensor Networks," Proceedings of the 10th ACM Conference on Computer and Communications Security, pp. 52-61, Oct. 2003.
[10] Wenliang Du, Jing Deng, Yunghsiang S. Han, and Pramod K. Varshney, "A key Predistribution Scheme for Sensor Networks Using Deployment Knowledge," IEEE Transactions on Dependable and Secure Computing, vol. 3, no. 1, pp. 62-77, Jan. 2006.
[11] Roberto Di Pietro, Luigi V. Mancini, and Alessando Mei, "Random Key Assignment for Secure Wireless Sensor Networks," Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks, pp. 62-71, Oct. 2003.
[12] Donggang Liu and Peng Ning, "Location-Based pair-wise Key Establishments for Relatively Static Sensor Networks," Proceedings of the first ACM Workshop on the Security of Ad-Hoc and Sensor Networks, pp. 72-82, Oct. 2003.
[13] Ngo Trong Canh, Tran Van Phuong, Young-Koo Lee, Sungyoung Lee, and Heejo Lee, "A Location-aware Key Predistribution Scheme for Distributed Wireless Sensor Networks," Proceedings of the 15th IEEE International Conference on, pp. 188-193, Nov. 2007.
[14] Wendi B. Heinzelman, Anantha P.Chandrakasan, and Hari Balakrishnan, "An Application-Specific Protocol Architecture for Wireless Microsensor Networks," IEEE Transactions on Wireless Communications, vol.1, no.4, pp. 660-670, Oct. 2002.
[15] Ossama Younis and Sonia Fahmy, "Distributed Clustering in Ad-hoc Sensor Networks: A Hybrid, Energy-Efficient Approach," Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies, vol. 1, pp.1-12, Mar. 2004.
[16] Siva D. Muruganathan, Daniel C.F. Ma, Rolly I. Bhasin, and Abraham O. Fapojuwo, "A centralized energy-efficient routing protocol for wireless sensor networks," IEEE Communications Magazine, vol. 43, no. 3, pp. s8-13, Mar. 2005.
[17] M. Rajiullah, and S. Shimamoto, "An Energy-Aware Periodical Data Gathering Protocol Using Deterministic Clustering in Wireless Sensor Networks (WSN)," Proceedings of Wireless Communications and Networking Conference, pp. 3014-3018, Mar. 2007.
[18] Arati. Manjeshwar and Dharma P. Agrawal. "TEEN: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," In 1st International Workshop on Parallel and Distributed Computing Issues in Wireless Networks and Mobile Computing, pp. 2009-2015, Apr. 2001.
[19] Arati Manjeshwar and Dharma P. Agarwal, "APTEEN: A Hybrid Protocol for Efficient Routing and Comprehensive

Information Retrieval in Wireless Sensor Networks," Proceedings of Parallel and Distributed Processing Symposium, Proceedings International, IPDPS, pp. 195-202, Apr. 2002.

〔20〕 Dongmin Choi, Sangman Moh, Ilyong Chung, "Variable Area Routing Protocol in WSNs: A Hybrid, Energy-Efficient Approach," IEEE International Conference on High Performance Computing and Communications,(HPCC), pp. 397-403, Sept. 2008.

〔21〕 Choi Dong-Min, Moh Sang-Man, Chung Il-Yong, "Regional Clustering Scheme in Densely Deployed Wireless Sensor Networks for Weather Monitoring Systems," IEEE International Conference on High Performance Computing and Communications,(HPCC), pp. 497-502, Sept. 2010.

〔22〕 Chris Karlof and David Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," IEEE International Workshop on Sensor Network Protocols and Applications, pp. 113-127, May 2003.

〈著者紹介〉

최 동 민 (Dongmin Choi) 정회원
2003년 2월: 경희대학교 공과대학 졸업
2007년 8월: 조선대학교 정보컴퓨터교육 석사
2010년 2월: 조선대학교 컴퓨터공학과 박사
2010년~현재: 조선대학교 컴퓨터공학과 박사후연구원
〈관심분야〉 네크워크 보안, 센서 네트워크, 모바일 애드혹 네트워크, 정보 윤리

심 검 (Jian Shen) 학생회원
2007년 2월: 난징대학교 공과대학 졸업
2009년 2월: 조선대학교 컴퓨터공학과 석사
2009년 3월~현재: 조선대학교 컴퓨터공학과 박사과정
〈관심분야〉 컴퓨터 네트워크, 보안 시스템, 모바일 애드혹 네트워크, 센서 네트워크

정 일 용 (Ilyong Chung) 종신회원
1983년 2월: 한양대학교 공과대학 졸업
1987년 2월: City University of New York 전산학과 석사
1991년 2월: City University of New York 전산학과 박사
1991년~1994년: 한국전자통신연구소 선임연구원
1994년~현재: 조선대학교 컴퓨터공학부 교수
〈관심분야〉 네트워크 보안, 분산시스템 관리, 코딩이론, 병렬 알고리즘, 애드혹 네트워크