무선 센서 네트워크에서 안전하고 에너지 효율적인 클러스터 헤더 선출 기법*

김진묵** · 이풍호*** · 유황빈****

요 약

센서 네트워크는 다양한 환경에 배치되어 환경요소 감시 및 군사적으로 유용한 정보를 제공하는데 사용될 수 있다는 특징을 가지고 있지만, 여러 가지 보안상의 취약점을 갖고 있는 단점이 있다. 따라서 이러한 센서 네트워크의 안전성을 위해서는 반드시 보안 서비스가 요구되며, 센서 네트워크 노드간의 안전한 통신을 위해 보다 안전하고 효과적인 노드 관리 기법이 요구된다. 본 논문에서는 센서 네트워크에서의 센서 노드의 보안성이 요구되는 환경 및 그룹 키 관리 기법에 적합한 효과적인 CH 및 클러스터링 기법을 제안한다. 먼저 각각의 노드들은 매 라운드 설정단계에서 BS와의 통신을 통하여 잔류 전력 및 암호 키를 이용한 인증 메시지를 전송하고 BS는 유효인증비율 및 잔류전력량을 반영하여 이 값들이 높은 노드를 CH로 선발한다. 이후 BS는 매 라운드 마다 이전라운드의 유효인증비율을 반영/누적 하여 적은 양의 에너지 소비로 안전한 클러스터 노드를 선발할 수 있는 기법을 제안한다.

A Cluster-Header Selecting Method for more Secure and Energy-Efficient in Wireless Sensor Network

Jin Mook Kim** · Pung Ho Lee*** · Hwang Bin Ryou****

ABSTRACT

Distributed wireless sensor network in various environment have characteristic that is surveillance of environment-element and offering usefully military information but there is shortcoming that have some secure risks. Therefore secure service must be required for this sensor network safety. More safe and effective techniques of node administration are required for safe communication between each node. This paper proposes effective cluster-header and clustering techniques in suitable administration techniques of group-key on sensor network. In this paper, first each node transmit residual electric power and authentication message to BS (Base-Station). BS reflects “Validity Authentication Rate” and residual electric power. And it selects node that is more than these regularity values by cluster header. After BS broadcasts information about cluster header in safety and it transmits making a list of information about cluster member node to cluster header. Also, Every rounds it reflects and accumulates “Validity Authentication Rate” of former round. Finally, BS can select more secure cluster header.

Key words : Sensor Network, Clustering, Group Key

---

* 이 논문은 2006년도 광운대학교 교내연구비에 의해 연구되었음.
** 선문대학교 컴퓨터정보학부
*** 광운대학교 컴퓨터과학과
**** 광운대학교 컴퓨터소프트웨어학과

1. 서 론

센서 네트워크는 인간이 접근하기 어려운 극악의 조건을 가진 위치나 재난 구조와 같은 응용분야에 적용될 수 있다는 특징을 가지므로 센서 네트워크를 구성하는 센서 노드들은 무작위로 배치될 수 있다. 그러므로 센서 네트워크 프로토콜은 자가 구성 능력을 가지며, 센서 노드들의 자체적인 통신을 통하여 서로 상호 협력하여 망을 구성한다. 센서 네트워크는 센서 노드들이 배치된 센서 필드와 외부 통신망을 연결하는 베이스 스테이션(BS : Base-Station)으로 구성된다. 사용자 들은 BS를 통하여 제어신호 및 질의전달을 할 수 있으며, 센서 노드로부터 수집된 데이터를 BS를 통하여 제공받을 수 있다. 그러나 센서 노드의 경우 통신범위가 극히 제한되어 있다는 특징을 가지며, 이 때문에 센서 노드의 데이터가 BS까지 도달하지 못하는 경우도 있다. 때문에 hop-to-hop 방식으로 통신을 하여 최종 목적지인 BS까지 도달하게 한다.

센서 네트워크의 경우 인접한 노드의 유사한 데이터를 중복으로 전송하여 에너지 낭비를 유발 할 수 있는데, 이러한 문제점을 최소화하기 위하여 “데이터 모음”이 필요하다는 특성을 고려할 때, 클러스터링 기반의 계층적 라우팅 기법이 센서 네트워크에서 효율적이라는 장점을 가진다[2-4]. 즉, 일정한 구간별로 로컬 클러스터를 형성하고, 이 클러스터에서 수집된 데이터를 클러스터 헤더(CH : Cluster Header)가 BS로 전송한다. 이러한 클러스터링 기법의 경우 중복성을 최대한 배제하기 때문에 노드의 수명 및 BS 데이터 관리면에서도 효율적이며, 또한 보안적인 관점에서도 클러스터링 기반의 그룹 키 기법으로 확장하여 지역적 보안성 및 인증 위임과 같은 이점을 얻을 수 있다는 장점을 얻을 수 있다.

대표적인 클러스터링 기반의 그룹핑 기법에는 센서 노드들간의 자율적인 클러스터링으로 이루어지는 LEACH[5, 6]와 BS에서 센서 노드들의 정보를 수집하여 일정한 조건에 따라 CH를 결정하여 클러스터가 구성되는 LEACH-C[7, 8]가 있다. LEACH와 LEACH-C는 일정한 주기별로 CH를 교체하여 센서 노드들이 균등하게 에너지 소비를 할 수 있다는 장점이 있다. 그러나 LEACH와 LEACH-C의 경우 보안요구에 적합한 프로토콜이 아니므로 외부의 악의적인 공격자에 의해서 센서 노드들의 데이터가 노출되거나 CH 선정 기준 값인 에너지 값을 Middle Attack, Delay Attack, Replay Attack등을 통해 위조/변조 하여 라우팅 공격을 할 수 있다는 문제점을 가지고 있다[9].

본 논문에서는 이러한 외부의 공격자가 LEACH-C의 보안적 취약성을 이용한 라우팅 공격 및 데이터 도청과 같은 악의적인 행위의 시도를 방지하기 위하여 초기 라운드 설정 시 BS에서는 센서 노드의 잔류 에너지 값뿐만 아니라 일정한 시간동안 전송된 인증 메시지에 대한 유효인증비율을 함께 적용하여 보다 안전하고 효율적으로 CH를 선정하고 클러스터를 유지 할 수 있는 기법을 제안한다. 또한 제안된 기법은 센서 네트워크에서의 지역적 보안성을 극대화하기 위한 그룹 키 기법과 확장하여 사용할 수 있도록 되어있다.

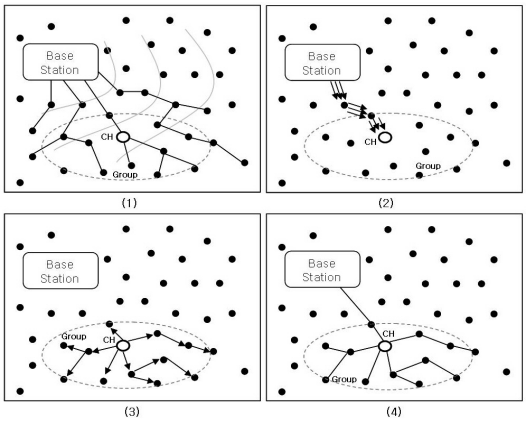
2. 관련 연구

클러스터링 기반의 라우팅 기법은 센서 필드에 배치된 다수의 센서 노드들을 작은 클러스터라는 단위로 나누어지고, 각각의 클러스터에는 CH가 존재하여 클러스터 멤버로부터 데이터를 수집하여 BS이나 상위 CH로 전송하는 역할을 수행한다. 이와 같은 클러스터링 기법은 센서 노드들에게 많은 이점을 가져오므로 다양한 기법이 연구되었으며, 정보보안을 고려하지 않은 대표적인 클러스터링 기법으로는 LEACH, LEACH-C, TEEN, BCDCP, SEIC 등이 있다.

이 기법은 기존의 유선 네트워크 시스템 환경과

마찬가지로 여러 보안적으로 취약한 문제점들을 내포하고 있을 뿐만 아니라, 센서 네트워크를 구성하는 노드들이 무선채널을 사용 및 노드들의 자체적인 저장 공간 및 연산능력이 부족한 관계로 유선 네트워크 환경에서의 보안요소들을 그대로 사용할 수 없으며, 이에 대한 해결책 또한 매우 부족한 실정이다. 아직까지 센서 네트워크 기술에 대한 연구가 진행되고 있지만, 차후 실질적으로 센서 네트워크를 실생활에 도입하고자 할 때 이러한 보안문제가 해결되지 못한다면 프라이버시 침해 문제 및 이를 이용한 범죄와 같은 큰 문제점을 유발할 수 있다.

그 중에서 데이터 패킷 위/변조 등을 통한 라우팅 공격과 도청과 같은 문제를 해결하기 위해서는 보안의 기초적인 해결책이 될 수 있는 BS와 노드들 간의 인증을 확인 할 수 있는 알고리즘과 사전에 기밀성 유지를 위한 암호 키를 활용하는 기법에 대하여 연구가 필요하다[10].



(그림 1) 클러스터 기반 그룹키 관리기법의 예

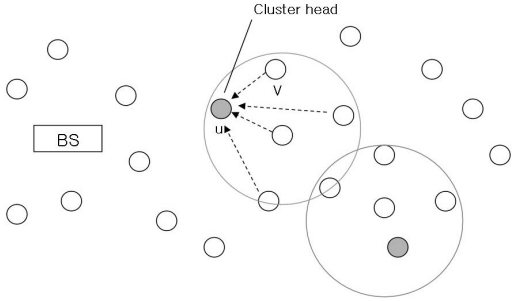
Jing Deng, Richard Han와 Shivakant Mishra [11]에 의하여 제안된 클러스터링 기반의 노드 관리 및 그룹 키 관리기법에서는 BS가 센서 노드의 관리를 CH가 수행하도록 하며 각각의 클러스터 멤버에 대한 공용 키인 그룹 키를 통해 안전한 통신을 수행할 수 있다는 특징을 가지고 있다. (그림 1)의 이 기법은 각 CH를 통해 BS로부터 효율적으로 키를 분배할 수 있으며 BS와 CH로부터의 메시지를 각 센서 노드가 인증할 수 있을 뿐 아니라, 각 센서로부터 전달된 메시지를 상위레벨에서 효과적으로 인증할 수 있는 방안을 제시하였다. 그러나 이 기법의 경우 센서 노드보다 연산능력이 뛰어난 CH가 이미 존재하여 있거나 LEACH와 같은 CH 선정 기법을 통하여 CH 역할을 하는 CH가 이미 선정되었다고 가정하고 있다. 기존의 클러스터링 기반의 라우팅 기법을 확장한 즉, 안전한 그룹관리 및 그룹 키 관리를 위한 그룹핑 기법에 대한 연구가 매우 부족하며, 서브키 생성에 사용될 정보가 평문상태로 존재하므로 악의적인 공격자가 이 정보를 이용할 수 있다는 보안적 문제점이 존재한다.

따라서 이와 같이 센서 노드들을 그룹으로 묶어 지역성 보안성을 유도하는 센서 노드 및 키 관리 기법을 사용한다 하더라도 그룹핑을 위해 사전에 수행되는 클러스터링 과정에 보안요소가 부재한 상태라면, 악의적인 공격자에 의한 보안적 위협에 노출 될 수밖에 없다. 때문에 센서 네트워크에서의 클러스터링 라우팅의 방해 공격을 방지하기 위하여 암/복호 및 인증 기법을 적용한 클러스터 기반의 라우팅 기법이 제안되었으며, 대표적으로 Kun-Won Jang이 제안한 LEAP/LEACH 기법[1]을 예로 들 수 있다.

이 기법은 센서 네트워크에서 키 관리기법인 LEAP[12]을 클러스터 기반의 라우팅 기법인 LEACH에 적용한 것으로 외부의 악의적인 공격자가 라우팅 데이터의 위/변조 등으로 라우팅 공격 및 도청을 방지하는 것을 목적으로 두고 있다. 먼저 각각의 센서 노드들은 사전에 배치되기 전 BS으로부터 고유 ID값과 함께 일종의 비밀 및 인증 키 값인 initial Key를 제공받는다

각각의 노드들은 (그림 2)와 같이 BS으로부터 제공받은 initial Key와 자신의 ID값을 통하여 자

신의 Individual Key를 생성할 수 있으며, 이 키는 BS와 노드 간의 데이터 기밀성 및 Node-to-Node 간의 공통된 키 쌍을 생성하는데 사용된다[13]. 이 기법의 경우 모든 키가 initial Key로부터 유도되며, 키 간에 상하관계가 명확하게 존재하므로 CH 선별 메시지의 기밀성을 위해 사용되는 클러스터 키는 일정 수 이상 노드들과의 인증작업이 아니면 얻을 수 없다는 특징을 가진다. 즉, BS로부터 제공된 initial Key 없이는 CH 선별에 관련된 데이터를 도청하거나 위/변조 하여 라우팅 공격을 시도할 수 있는 확률이 매우 어렵게 된다. 그러나 모드 노드들은 동일한 initial Key를 가지므로 이 키 값이 악의적인 공격자에게 노출될 경우 모든 노드들이 공격의 위험에 빠질 뿐만 아니라, 클러스터 키를 안전하게 공유하기 위해서는 총 s개의 키 쌍을 저장하기 위한 추가적인 공간이 요구된다. 뿐만 아니라 데이터가 암호화 되어 있다 하더라도 악의적인 공격자가 이 데이터를 임시적으로 저장해 두었다가 공격에 재사용 할 수 있는 “Reply attack”을 시도 할 수 있다는 단점이 존재한다.



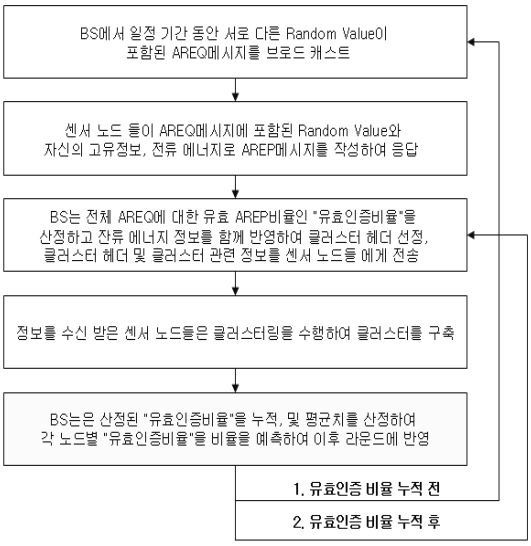
(그림 2) LEAP를 사용한 LEACH 기법

3. 제안 모델

기존의 클러스터링 기법은 CH 노드 선정 시 각 노드의 잔류 에너지 값을 기준으로 두기 때문에, 이러한 잔류 전력 데이터의 위/변조 및 페킷 수정 공격에 대하여 매우 취약한 구조를 가지고 있다. 따라서 본 장에서는 이러한 보안적 문제점을 해결하고 기존의 프로토콜과 비교하여 센서 노드의 부하를 감소시킬 수 있는 모델을 제안한다.

3.1 제안기법 개요

본 논문에서 제안하는 클러스터 헤더 선출 기법의 전체적인 모델의 구조는 (그림 3)과 같다.



(그림 3) 제안 기법의 전체적인 모델 구조

3.2 제안기법의 동작과정

3.2.1 가정사항

모든 센서 노드들은 배치 전에 BS로부터 서로 다른 BS-to-Node Pair-wise Key $K_{Pair}{}^{i}$와 MAC을 생성하기 위해 $Key_{MAC}{}^{A}$라는 값을 가진다. 이때 키 쌍과 $Key_{MAC}{}^{A}$값은 노드와 BS간에 공유를 하고 있으며 외부로 노출되지 않는다. 또한 BS는 자체적으로 보안이 되어 있으며 충분한 연산능력을 갖추고 있다고 가정하며 본 논문에서 사용되는 기호의 설명은 <표 1>과 같다.

3.2.2 노드인증 및 인증 값 수집

먼저 BS는 배치된 센서 노드들에 대한 인증작업을 위하여 일정시간동안 랜덤하게 생성된 서로 다른 n개의 값들을 AREQ 메시지에 포함시켜 브로드캐스트 한다.

$$R\_Value^i = Random\_Value\_Generator()$$
$$BS \rightarrow^* : AREQ^i \mid R\_Value^i \quad (i = 0, \cdots, n)$$

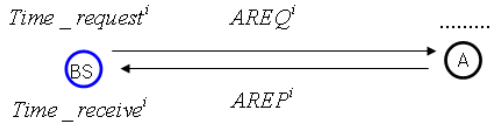
이때 BS는 메시지 송신시 시간정보를 측정하여 저장하며 이 시간정보는 "유효인증비율" 계산을 위해 사용되는 $Time\_stamp$ 생성에 반영된다. BS의 AREQ 메시지를 수신 받은 센서 노드들은 AREP 메시지를 작성하여 응답하게 된다. 이때 임의의 센서 노드 A는 자신의 잔류 에너지 값을 측정하며 에너지 값에 대한 MAC 생성을 위하여 i번째 AREQ 메시지에 포함된 R_Value^i값과 MAC Key 값인 $Key_{MAC}{}^A$그리고 노드 A가 측정한 잔류 에너지값을 기반으로 연산 후 One-way Hash함수를 거쳐 잔류전력 값에 대한 MAC을 생성한다.

$$Hash((Power \oplus R\_Value^i) \oplus Key_{Mac}{}^A)$$
$$= Hash(S_A^i)$$
$$= MAC_A^i \ (i = 0, \cdots, n)$$

센서 노드 A는 측정된 잔류 에너지 값과 MAC 값을 BS와 공유된 Pair-wise Key인 $K_{Pair}{}^i$로 암호화하여 AREP 메시지를 작성한 후 BS로 전송하여 응답한다.

$$M_i = EK(K_{Pair}{}^A,\ Power_A \mid MAC_A^i)$$
$$Node_i \rightarrow BS : AREP \mid M_i$$

BS는 n개 만큼의 AREP 메시지에 대한 총 m개의$(0 \le m \le n)$ AREP 메시지를 수신 받아 확인한다. 즉 키 쌍으로 복호화 후 얻어진 MAC값을 자체적으로 소유하고 있는 해당 센서 노드에 대한 값 $Key_{MAC}{}^A$, 잔류전력 값을 사용하여 MAC을 생성하여 센서 노드가 전송한 MAC과 비교하여 무결성을 체크한다.



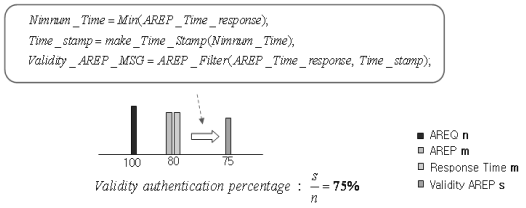
$$\textbf{Time\_receive}^i - \textbf{Time\_request}^i = \textbf{Time\_response}^i$$

(그림 4) 메시지에 대한 응답시간 측정

메시지에 대한 응답 시간 내에 정상적으로 무결성 체크가 완료 되었다면 (그림 4)와 같이 AREP 메시지 확인 시간인 $Time_request$과 AREQ 메시지 송신 시간 값인 $Time_receive$와의 차를 구하여 응답시간 값 $Time_response$를 계산한 후 해당 AREP 메시지의 확인 유무와 함께 리스트로 작성하여 저장한다.

3.2.3 유효인증비율 측정

BS는 n개의 AREQ 메시지에 대한 m개의 AREP 메시지 리스트 중 s개의 유효한 인증 메시지를 얻어내기 위하여 $Time_stamp$를 사용한다. 먼저 총 m개의 AREP 메시지와 이에 대한 $Time_response$로 구성된 $AREP_Time_response$리스트에 포함된 값들 중 가장 적은 $Time\_response$ 값을 기반으로 $Time\_stamp$ 값을 생성한다.



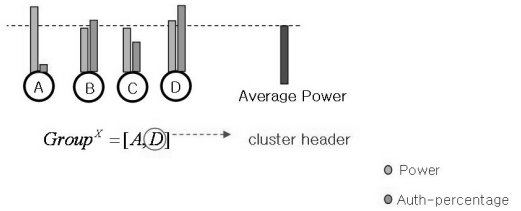
(그림 5) 제안기법의 유효인증비율 측정

만일, $AREP_Time_response$리스트의 존재하는 $Time_response$값들 중에서 $Time_stamp$를 초과하는 값이

있다면 *AREP_Time_response*리스트에서 해당 AREP 메시지와 함께 삭제가 되며, 이 작업은 악의적인 공격자가 다른 노드의 AREP 메시지를 저장, 차후 재사용 하는 Replay 방지와 고의적으로 지연된 Delay 메시지를 무시하기 위해서이다. 단, Delay 공격은 일반적인 암호화 기법으로 발견하거나 막아낼 수 없다. 따라서 본 기법에서 제안된 *Time_stamp*를 통한 인증기법의 경우 Delay Attack를 최대한 회피하는 것을 목적으로 하고 있다. BS는 (그림 5)와 같이 전체 n개의 AREQ 메시지에 대한 총 s개의 유효한 AREP 메시지의 비율을 계산, 각각 노드들에 대한 유효인증비율을 계산하여 저장한다. 즉, 경로가 불안정하거나 경로에 공격자가 있는 센서 노드들은 전체적으로 낮은 유효인증비율을 가지게 된다.

3.2.4 유효인증비율을 반영한 CH 선출

노드의 유효인증비율을 측정 및 저장한 BS는 각 센서 노드의 AREP 메시지에 포함된 잔류 에너지 값들로부터, 센서 노드 전체의 평균 잔류 에너지 값을 계산한다. 이때 BS는 평균치 이상의 센서 노드들을 (그림 6)와 같이 CH 선정 후보 그룹인 $Group^X$에 등록시킨다.



(그림 6) 클러스터 헤더 선출 S는

$Group^X$생성 이후 BS는 $Group^X$에 속하는 센서 노드의 유효인증비율을 반영하여 CH를 선정한다. 즉, 가장 높은 인증비율을 가진 센서 노드를 CH로 선정하며, 센서 필드가 크거나 배치된 센서 노드들이 많다면 필요한 개수만큼 유효인증비율을 기준점으로 오름차순 정렬하여 CH로 선출한다. 예를 들어 (그림 6)에서 노드 A는 높은 에너지 값을 가지지만, 낮은 유효인증비율을 가지므로 CH에서 제외되게 된다.

3.2.5 CH 공표 및 클러스터 구축

BS는 CH 선정 후, 센서 노드들에게 CH 선정 정보를 암호화하여 브로드캐스트 한다. 이때, BS는 암호화를 위한 임시 키 K_T를 생성한 후, 선정된 CH에 대한 데이터를 암호화하여 브로드캐스트 한다.

$$BS \rightarrow^{*} : EK(K_T, Node^{D}_{\mathrm{CH}})$$

센서 노드들은 암호화된 클러스터 공표 메시지를 받게 된다. 이때 이 메시지는 암호문이므로 암호화에 사용된 임시 키 없이는 그 내용을 확인하거나 수정할 수 없다. 이후 BS는 임의의 일정시간 경과 후 암호화에 사용된 임시 키 K_T를 브로드캐스트 하여 노드들에게 공개한다.

$$BS \rightarrow^{*} : K_T$$

키를 수신 받은 센서 노드들은 암호화된 CH 선출 관련정보를 확인할 수 있다. 이렇게 안전하게 CH 관련 정보를 획득하게된 센서 노드들은 자신의 이웃노드의 정보들과 BS로부터 수신 받은 CH의 정보를 통하여 자신이 속한 클러스터와 CH들을 알 수 있으며, 이후부터 센서 노드들은 해당 CH에게 데이터를 전송하게 된다. 센서 노드들은 자신의 이웃노드의 정보들과 BS로부터 수신 받은 CH의 정보를 통하여 자신이 속한 클러스터와 CH들을 알 수 있으며, 이후부터 센서 노드들은 해당 CH에게 데이터를 전송하게 된다.

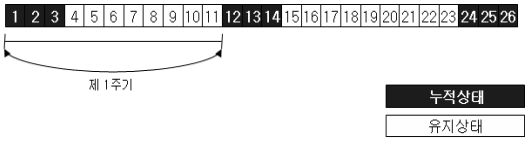
3.2.6 데이터 누적을 통한 유효인증비율 추정

유효인증비율 측정 시 BS에서는 총 n회의 AREQ 메시지를 전송하며 센서 노드들은 이 AREQ

메시지에 대한 n회 만큼의 AREP 메시지를 전송해야 한다. 이러한 특성 때문에 센서 노드의 과도한 에너지 소모가 유발 될 수 있다. 또한 악의적인 공격자가 직/간접적으로 관여할 수 있는 트래픽은 극히 제한되어 있다고 보기 때문에 매 라운드 마다 이러한 인증작업을 할 필요는 없다. 따라서 본 기법에서는 측정된 유효인증비율을 CH 선정 기준에 반영하되, 매 라운드 마다 누적된 유효인증비율 정보를 기반으로 각 노드들의 평균 유효인증비율을 추정하도록 한다. 먼저 BS은 일정한 라운드 동안 누적된 유효인증비율에 대한 평균 값을 계산한다. 다음 라운드부터 BS은 노드의 잔류 에너지 값을 요청하기 위한 최소한의 AREQ 메시지만을 브로드 캐스트하며, 평균 유효인증비율 값을 유효 인증비율로 대체하여 높은 안전성과 잔류 에너지를 소유한 센서 노드를 CH로 선정한다.

3.2.7 평균 유효인증비율 사용주기

센서 네트워크에서의 악의적인 공격자는 불규칙한 주기 혹은 시간에 네트워크에 개입하여 악의적인 행동을 수행 할 수 있고, 센서 노드 특정상 트래픽이 불안정할 수도 있다. 따라서 평균 유효인증비율을 통하여 유효인증비율을 예측하는 것은 오차를 유발할 수 있다. 이러한 오차가 누적되어 악영향이 미치는 것을 방지하기 위하여 3.2.8과정을 주기적으로 반복하여 동기화 시킬 필요가 있다. 동기화를 위해 제안 시스템은 “누적상태”와 “유지상태”로 전환을 반복하게 된다.



(그림 7) 데이터 누적 및 사용주기

즉, (그림 7)과 같이 “누적기간”에서는 매 라운드마다 각각의 노드에 대한 유효인증비율을 측정 및 누적하며 이후 “유지기간”에서는 누적된 유효인증비율의 평균값을 노드의 유효인증비율을 대체하여 CH 선정 기준에 사용한다. 즉 “유지기간”에서는 따로 유효인증비율을 측정하기 위한 작업을 요구하지 않는다. 이렇게 일정기간은 유효인증비율 측정 및 누적을 수행하고, 다시 일정기간 동안은 누적된 데이터를 기준으로 평균값을 계산 및 사용함으로써 과도한 인증작업으로 인한 에너지 소모를 최소화 할 수 있다. 물론 배치된 노드의 수, 네트워크 의 크기, 트래픽, 공격자의 수와 공격의 강도 같은 요소들은 시나리오마다 다를 수 있으므로 불규칙한 네트워크 환경에 따른 “누적상태”와 “유지기간”의 간격을 달리 할 필요가 있다.

4. 실험 평가

제안된 기법에 대한 실험 및 분석은 팬티엄 4 1GB RAM의 데스크 탑 환경에서 CygWin상에 인스톨된 TinyOS-1.x를 사용하였으며, 사용언어는 TinyOS에서 기본적으로 제공하는 NesC를 사용하였다. 그리고 제안된 기법에 대한 실험용 시뮬레이터로는 TOSSIM을, 또 이러한 실험과정을 알기 쉽게 GUI로 출력하기 위하여 TinyViz를 사용하였다. 또한, 시뮬레이션 시 아래와 같은 조건을 반영하여, 실제 센서 노드와 유사한 환경을 가지도록 했다.

ATmega 128L 칩셋기반의 가상 MICA 노드
노드 25, 50, 75, 100, 125개의 센서 네트워크
50m x 50m 면적의 센서 필드
센서 노드가 통신 가능한 범위는 반경 10m
Delay Time은 100m/s
적, 황, 녹 LED를 ON/OFF하여 표시

또한, 보안모듈이 적용된 LEAP/LEACH와 제안된 기법의 경우 SPINS[26]에서의 보안모듈 사용에 따른 에너지 소모비율을 참조하여, 메시지 전송

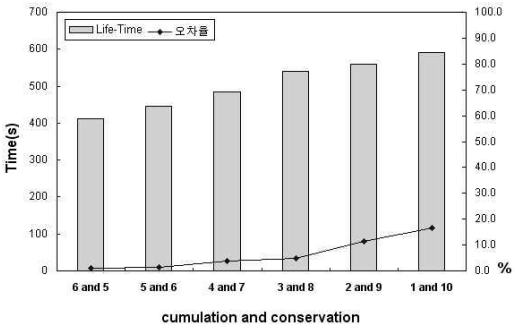
시 센서 노드에 대한 페널티를 주도록 하였다.

4.1 실험환경 및 실험과정

제안된 기법에 대한 실험 및 분석은 팬티엄 4 1GB RAM의 데스크 탑 환경에서 CygWin상에 인스톨된 TinyOS-1.x를 사용하였으며, 사용언어는 TinyOS에서 기본적으로 제공하는 NesC를 사용하였다. 그리고 제안된 기법에 대한 실험용 시뮬레이터로는 TOSSIM을, 또 이러한 실험과정을 알기 쉽게 GUI로 출력하기 위하여 TinyViz를 사용하였다.

4.2 실험결과

4.2.1 설정된 누적상태와 유지상태의 비율 설정

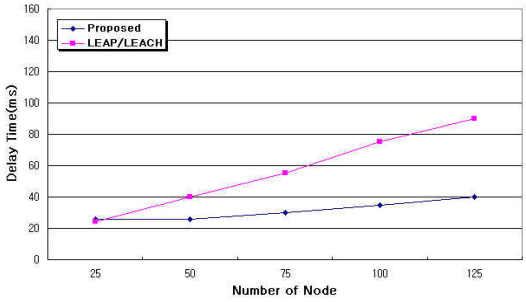


(그림 8) "누적상태와 유지상태"에 대한 비교

효과적인 실험을 위해 제안기법의 누적상태와 유지상태의 비율을 임으로 설정 및 실험하여 비교하였다. "누적상태와 유지상태"와 같은 형식으로 설정하였으며, 실험 결과는 (그림 8)과 같다. 이 실험에서 비교대상이 된 값은 네트워크의 생존시간과 유효인증비율 예측 시 나타날 수 있는 오차율로 전체 주기를 차지하는 누적상태가 적을수록 오차가 증가하고, 네트워크의 생존시간이 감소하는 것을 알 수 있다. 가장 이상적인 상태는 "3 and 8"이 되며, 이 설정 값은 제안 기법의 실험에 대한 매개변수로 사용된다.

4.2.2 노드간의 인증작업 시 노드 지연시간

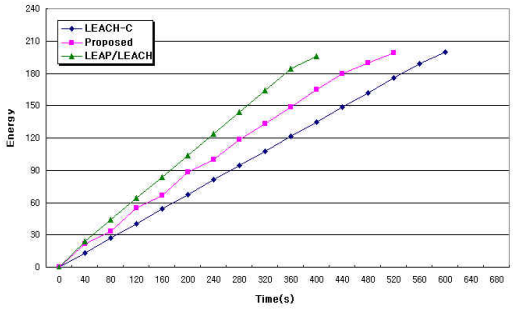
LEAP/LEACH와 제안기법에서 클러스터링 및 그룹핑 작업 시 추가적으로 수행하게 되는 인증작업에 대한 지연시간을 비교하였으며, (그림 9)와 같다. 단, 메시지 전송에 대한 지연사항은 제외하였으며, 인증작업 시 센서 노드 내부에의 암/복호화 혹은 인증확인 작업으로 인한 지연시간을 나타낸 것이다.



(그림 9) 노드 증가에 따른 인증 지연시간 비교

4.2.3 노드에서의 전력 사용량

(그림 10)는 100개의 노드를 배치한 후, 40초 간격으로 노드들이 소모한 전력을 그래프로 나타낸 것이다.



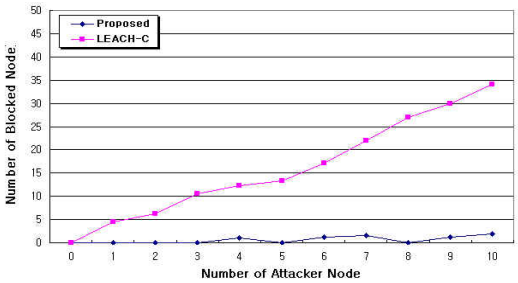
(그림 10) 노드에서의 전력 소모량 비교

LEAP/LEACH의 경우 잦은 암/복호화 작업 및 인증작업으로 인해 추가적인 메시지를 전송해야 하므로 전력소모가 매우 심한 것을 알 수 있다. 반면,

제안된 기법은 초기 40초 구간에서는 LEAP/LEACH와 전력소모가 유사한 것처럼 보이나, 점차 그 차이가 두드러지는 것을 알 수 있으며, 기존의 기법에서 약 15~17%의 전력소비감소를 볼 수 있었다. LEACH-C보다 많은 양의 전력을 소비하지만, 보통 보안모듈을 사용할 경우 그렇지 않은 노드에 비하여 추가적인 전력소모를 가져온다.

4.2.4 Sybil attack시 공격에 노출된 노드의 수

보안모듈이 없는 LEACH-C와 제안기법에 대하여 센서 공격을 수행하여, 보안모듈 부재로 인한 노드의 취약성과 보안모듈이 존재할 경우 이를 얼마나 방지할 수 있는지에 대한 실험결과를 (그림 11)과 같이 그래프로 나타내었다.



(그림 11) 보안공격에 의해 차단된 노드의 수

자체적인 인증 및 암호화 모듈이 존재하지 않는 LEACH-C의 경우 공격자가 수에 비례하여 차단된 노드의 수가 기하급수적으로 증가하는 것을 볼 수 있다. 반면 제안기법의 경우 노드의 인증을 고려하고 있으므로 공격자의 공격시도가 실패로 끝나는 것을 알 수 있다. 예상과 달리 3% 미만의 노드들이 BS로 부터 차단되고 있는 것을 볼 수 있는데, 이는 공격자가 전송하는 다량의 공격 메시지로 인한 트래픽 과부하가 주된 원인으로 추측하고 있다.

4.2.5 센서 네트워크의 보안공격에 대한 대응

<표 2>는 센서 네트워크에서의 대표적인 보안공격을 간단히 정리한 도표로 나태난 것으로 공격의 형태에 따라 “Routing related”, “Data forwarding related”, “Physical related”로 나눌 수 있으며, LEACH-C, LEAP/LEACH, 제안기법에 대한 보안공격 대응여부를 정리한 것이다.

〈표 2〉 보안공격에 대한 대응 여부 비교

Attack Types		LEACH-C	LEAP/LEACH	Proposed
Routing related	Hello attack	×	○	○
	Bogus routing info, attack	△	○	○
	Sybil attack	×	○	○
Data forwarding related	Message delay attack	×	×	△
	Message alteration attack	×	○	○
	Message replay attack	×	○	○
Physical related	Byzantine attack	×	×	×

4.3 보안분석

이 부분에서는 제안된 기법에 대한 간단한 보안분석을 기술하도록 하였다. 암/복호화 알고리즘과 같은 기본적인 보안 요소들은 현재 존재하는 SPINS, TinySec[28] 표준에 적합하도록 설계하여 기존의 보안 프로토콜과의 호환성을 최대화 하였다. 대표적으로 RC5 암호화 알고리즘과 CBC-Mode로 생성되는 MAC이 그것이다.

4.3.1 데이터의 기밀성

본 논문에서 제안된 기법의 경우 기밀성을 유지를 위해 RC5 암호화 알고리즘을 사용하기 때문에 전송되는 데이터의 기밀성을 충분히 가질 수 있다.

4.3.2 노드의 신원 인증

각 노드와 BS는 상호간의 인증을 위해 MAC을 사용한다. 이때 MAC은 BS-to-Node간의 MAC생성용 키 값인 Auth_Value값과 초기 BS의 AREQ 메시지에 포함된 Random_value값과 일련의 연산과정을 거친 후, Hash 함수 중 하나인 MD5 암고리즘을 통하여 생성된다. 이때, Auth_Value는 BS-to-Node간에 사전에 공유하고 있으며, 이 값은 외부로 직접 노출되지 않는다.

4.3.3 데이터의 무결성

RC5 알고리즘을 CBC-Mode로 사용하여 생성한 MAC으로 무결성을 보장한다. 이때 CBC-MAC은 위에서 신원인증에 사용되는 MAC과는 다른 의미이다. 데이터 무결성에 대한 메시지 인증(MAC)을 의미한다. CBC-Mode의 경우 공격자로 하여금 평문데이터를 추측하기 매우 어렵다는 특징을 가진다. 따라서 공격자는 데이터 위조 및 변조 공격 시 이러한 CBC-MAC의 특성을 고려해야만 한다.

4.3.4 데이터의 시간적 유효성

제안기법은 기밀성, 인증, 무결성 외에 Time_Stamp를 고려한 인증을 추가적으로 도입하였다. 즉, 정당한 인증 메시지라도 일정시간을 초과한다면, 그 인증메시지를 무효화 시키며, 이 기법은 기존의 유선 네트워크에서의 보안기법을 센서 네트워크에 적용한 것이다. 그러나 센서 네트워크의 경우 유선 네트워크와 달리 여러 가지 변수가 존재하므로 이 부분을 위한 알고리즘에 대하여 추가적인 연구가 필요할 것으로 예상된다.

5. 결 론

본 논문에서는 센서 네트워크에서의 클러스터링 및 그룹핑 기법인 LEACH에서 보안적인 취약점을 개선한 LEAP/LEACH에 대하여 간단히 기술하였고, 기존의 보안 클러스터링 기법에서 CH 선정 및 클러스터링 작업시 보안모듈을 통한 인증 및 확인 절차 작업으로 인해 노드들이 많은 양의 전력을 소모한다는 문제점을 제시하였다. 센서 네트워크 모델에서 에너지를 가장 많이 소모하는 부분은 바로 데이터의 송/수신 부분이라고 할 수 있기 때문에 Node-to-Node간의 1 : 1 인증을 필요로 하는 기존의 기법은 센서 네트워크에서 비효율적인 구조를 가지고 있었다고 할 수 있다. 따라서 본 논문에서는 이 문제점을 해결하기 위하여 BS-to-Node간의 인증작업을 수행하되, BS에서 노드와의 인증작업을 통하여 안정적인 노드들을 확보하고, 가장 안전하다고 판단되는 노드를 CH로 선정 및 클러스터링 작업을 수행하도록 하였다. 물론, 노드의 생존성을 위해 LEACH-C기법과 같이 노드의 잔류 에너지 값을 함께 고려하도록 하였으며, BS의 CH 선정 이후 메시지 전송 작업은 임시 키를 이용한 암/복호화 작업을 병행하여 사용함으로써 공격자가 메시지를 함부로 위/변조 할 수 없게 하였다. 이 일정 라운드 동안은 유효인증비율을 측정 및 CH 선정기준에 반영하며 이후부터는 그 동안 누적된 유효인증비율에 대한 평균값을 산정 및 유효인증비율을 추측하여 사용함으로써 유효인증비율 측정으로 인한 전력소모를 최소화 시키도록 하였다. 시뮬레이션을 통해 실험한 결과 기존의 클러스터링 기법에서 부족한 기밀성과 무결성 및 인증문제를 해결하였으며 기존의 보안 클러스터링 기법은 LEAP/LEACH에 비해 노드의 전력소모량을 줄일 수 있었다. 또한 기존의 그룹 키 기법에 그대로 적용할 수 있어 기존기법과의 호환성을 극대화 하였다.

참 고 문 헌

[1] Kun-Won Jang, Woo-sik Jung, Dong-kyu

Shin, and Moon-Seog Jun, “Design of Secure Clustering Routing Protocol using SNEP and μTESLA on Sensor Network Communication”, IJCSNS International Journal of Computer Science and Network Security, Vol. 6 No. 1B, January 2006.

[2] L. Krishnamachari, D. Estrin, and S. Wicker, “The Impact of Data Aggregation in Wireless Sensor Networks”, Distrituted Computing System Workshops, 200. Proc.

[3] S. Lindsey, C. S. Raghavendra, and K. Sivalingam, “Data Gathering in Sensor Networks using the Energy * Delay Metric”, Proc. of IPDPS Workshop on Issues in Wireless Networks and Mobile Computing, pp. 2001-2008, April 2001.

[4] H. O. Tan and I. Korperglu, “Power Effcient Data Gathering and Aggregation in Wireless Sensor Networks”, ACM SIGMOD, Vol. 32, Issue 4, pp. 66-71, 2003.

[5] K. Dasgupta, K. Kalpakis, and P. Namjoshi, “An Effcient Clustering-based Heuristic for Data Gathering and Aggregation in Sensor Networks”, Wireless Communication and Networking, pp. 1948-1953, Mar. 2003.

[6] W. Heinzelman, A. Chandrkasan, and H. Balakrishnan, “Energy-Effcient routing protocols for wireless microsensor networks”, in Proc. 22rd Hawaii Int. Conf. System Sciences (HICSS), Maui, HI, Jan. 2000.

[7] W. Heinzelman, “Aoolication-specific protocol architrctures for wireless networks”, Ph.D. dissertstion, Mass Inst. Technol., Cambridge, 2000.

[8] W. R. Heinzelman, A. Chandarkasan, and H. Balakrishnan, “An Application-specific Protocol architrctures for Wireless Microsensor Networks”, in IEEE Transactons on Wireless Commnication, October 2002.

[9] Kui Ren, Wenjing Lou, Moran, P. J. “A Proactive Data Security Framework for Mission-Critical Sensor Networks”, Department of ECE, Worcester Polytechnic Institute, Worcester MA 01609.

[10] D. W. Carman, P. S. Kruus, and B. J. Matt “Constraints and approaches for distributed sensor network security”, Technical report, NAI Labs, 2000.

[11] J. Deng, R. Han, and S. Mishra, “Security Support for In-Network Processing in Wireless Sensor Networks”, Proc. of the 1st ACM Workshop on the Security of Ad Hoc and Sensor Networks(SASN), 2003.

[12] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, “LEAP : Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks”, Proc. of the 10th ACM Conference on Computer and Communication Security (CCS), 2003.

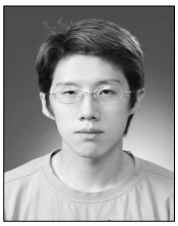
[13] O. Goldreich, S. Goldwasser, and S. Micali, How to Construct Random Functions. Journal of the ACM, Vol. 33, No. 4, pp. 210-217, 1986.

[14] 홍성식, 유황빈, “원형 좌표계를 이용한 센서 네트워크 키관리 기법”, 정보・보안논문지, 제6권, 제2호, 2006.

[15] http://www.distributed.net/rc5/.

김 진 묵

1998년 배재대학교 컴퓨터과학과(이학사)
2000년 배재대학교 컴퓨터공학과(공학석사)
2006년 광운대학교 컴퓨터과학과(공학박사)
2006년~현재 선문대학교 컴퓨터정보학부 연구교수



이 풍 호

2005년 학점은행 컴퓨터공학 (공학사)
2007년 광운대학교 컴퓨터과학과(공학석사)

유 황 빈

1968년 인하대학교 전자공학과 (학사)
1975년 연세대학교 전자공학과 (공학석사)
1984년 경희대학교 전자공학과 (공학박사)
1981년～현재 광운대학교 컴퓨터소프트웨어학과 교수