산업기술연구(강원대학교 산업기술연구소 논문집), 제25권 B호, 2005.
Journal of Industrial Technology, Kangwon Natl. Univ., Korea, No. 25 B, 2005.

교량감시를 위한 센서 네트워크 보안프로토콜

A Sensor Network Security Protocol for Monitoring the State of Bridge

임 화 정* 전 진 순** 이 헌 길***
Lim, Hwa-Jung Jeon, Jin-Soon Lee, Heon-Guil

Abstract

The wireless sensor network consists of a number of sensor nodes which have physical constraints. Each sensor node senses surrounding environments and sends the sensed information to Sink. The inherent vulnerability in security of the sensor nodes has promoted the needs for the lightweight security protocol.

In this paper, we propose a non-hierarchical sensor network and a security protocol that is suitable for monitoring the man-made objects such as bridges. Furthermore, we present the efficient way of setting the routing path by storing IDs, MAC(message authentication code) and the location information of the nodes, and taking advantage of the two node states, Sleep and Awake. This also will result in the reduced energy consuming rate.

키워드 : *센서 네트워크, 경량화된 보안 프로토콜, 에너지 소모율*
Keywords : *sensor network, lightweight security protocol, energy consuming rate*

1. 서론

무선 센서 네트워크는 분산 컴퓨터와 임베디드 시스템의 새로운 연구영역이다[1].

디지털회로기술의 개선으로 자료처리와 무선통신이 가능한 단일 칩으로 구성된 센서가 등장하였다. 소형 배터리로 작동하는 센서노드는 언제 어디서나 저가로 실생활에 배치할 수 있고, 분산된 센서 네트워크를 구축하여 주변의 환경에 대해서 정보를 수집하고 그 결과를 편하게 모니터링 할 수 있어, 군사 목적이나 일상생활 전반에 활용되고 있다[2].

특히 센서는 위험한 지역이나 접근이 힘든 지역에 값싼 비용으로 감시 체제를 구축할 수 있어 교량의 상태를 감지하고 위험요소를 바로 발견해서 안전성을 유지하는 등의 감시 장치에 많이 이용된다.

그러나 적은 메모리, 배터리 용량의 제한, 컴퓨팅 성능의 제약 등 제한적인 하드웨어 자원을 가지고 있는 센서들은 센서 정보의 도청이나 비정상적인 패킷의 유통, 메시지의 재사용 등 데이터 위·변조 문제와 네트워크 전체를 마비시킬 수 있는 서비스 거부 공격(Denial of Service)등 각종 물리적인 공격에 쉽게 노출된다[3]. 반면 일반적인 센서 노드와 달리 교량의 안전성 및 환경을 감시하는 센서 네트워크의 경우 센서 노드가 고정될 수 있는 특성이 있기 때문에 이에 맞는 보안 기술이 요구된다.

본 논문에서는 일반적인 센서 네트워크와 달리

* 강원대학교 정보통신공학과 박사과정
** 강원대학교 정보통신공학과 석사과정
*** 강원대학교 전기전자정보통신공학부 교수, 공학박사

교량용과 같이 센서의 위치가 변하지 않고, 한 곳에 고정된 센서 네트워크의 보안요구사항을 분석하고 이를 만족하기 위한 보안 프로토콜을 제시한다.

본 논문의 2장과 3장에서는 센서 네트워크의 특징과 보안요구사항을 알아보고 현재 센서 네트워크의 보안기법동향에 대해 살펴본다. 4장에서는 교량환경에 요구되는 보안기법에 대해 살펴보고, 효율적인 보안기법 및 라우팅 프로토콜을 제시한다. 5장에서는 제안방식의 성능을 비교분석하고, 6장에서 결론을 맺는다.

2. 센서 네트워크의 특징 및 보안 요구사항

센서 네트워크는 제한적인 하드웨어 자원을 가지고 있는 대량의 센서 노드들이 좁은 영역에 조밀하게 분포한다[4].

하나의 센서 노드가 통신하는 노드 수가 하나가 아닌 다대다 통신인 그물망 통신으로 이뤄지는 센서 네트워크는 브로드캐스트 통신 방식을 사용하기 때문에 주위의 노드들이 믿을 수 있는 상태인지에 대한 판단이 어렵고, 통신 반경이 짧아 통신 시 노드들의 동작이 항상 성공적이지 못하다는 특징을 지닌다.

따라서, 센서 정보를 목적지까지 전달하기 위한 경로 설정이나 유지를 위한 노드 간의 상호 인증과 제한된 센서 자원을 이용하여 인증과 암호화에 사용될 암호 키 관리의 문제가 주요 이슈 중의 하나이다[5].

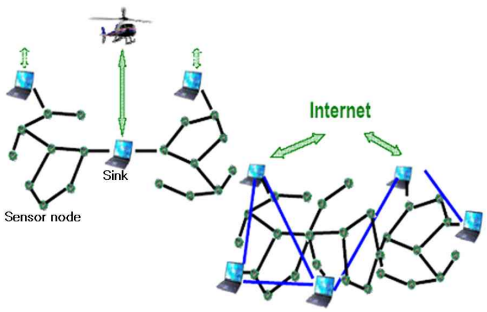

그림 1 센서 네트워크 구조

그림 1은 센서 네트워크 구조를 표현한 것으로 센서 네트워크는 그림과 같이 성능이 좋은 Sink와 자원의 제약을 지닌 센서 노드들로 구성되어있다.

Sink는 각 센서 노드들로부터 수집된 여러 정보를 Internet과 같은 통신망을 이용하여 송수신한다.

이때, 각 센서와 Sink 사이에 통신은 주로 무선으로 이뤄지기 때문에 보안문제가 대두되게 되었다. 문제는 센서 노드의 물리적인 제약성 때문에 데이터의 기밀성(Confidential), 데이터의 인증(Authentication), 데이터의 무결성(Integrity), 데이터의 참신성(Freshness)등 보안 요구사항을 지원하기 위한 센서 네트워크에 맞는 경량화된 보안 기법이 요구되고 있다[6].

센서 네트워크는 이러한 보안 요구사항을 수용하기에 물리적 제약성이 크다. 따라서 센서 네트워크를 위한 다양한 암호 및 인증 기법들이 제안되었다. 또한, 센서와 센서, 센서와 Sink 간에 사용될 안전한 데이터 및 패킷 전달을 위한 키를 공유하게 되었고, 이를 위한 키 관리기법들도 제안되었다.

이외에도 센서 네트워크의 센서 노드들은 이탈 및 고장 등으로 인한 서비스 거부공격(DOS)에 강한 구조뿐만 아니라, 사용자의 위치정보와 센서 노드의 집합정보에 대한 암호 기능을 제공하여 외부 공격에 대비하여 센서 노드의 노출을 방지하는 등의 다양한 보안 기능을 필요로 하게 되었다.

3. 센서네트워크의 보안기법 동향

3.1 인증기법

센서 네트워크에서 인증은 보안을 위한 가장 기본적인 단계로서, 멀티 캐스트 통신에서 각 패킷 인증에 주로 사용되는 스킴은 TESLA(Timed Efficient Stream Loss-tolerant Authentication)이다[7,8]. TESLA는 지연 키 노출 방법을 사용하여 각 패킷의 인증을 수행한다. 인증키는 단방향 키 체인(one-way key chain)을 사용하여 시간의 역방향으로 계산되므로 중간에서 임의로 생성할 수 없다. 이 방식은 패킷 손실에 강한 반면, 송·수신자간에 시간 동기화(time synchronization)가 필요하다.

센서 네트워크의 인증 메커니즘 중 하나인 SPINS(Security Protocols for Sensor Networks)는 센서 노드들이 Sink와 공유하는 하나의 마스터 키를 사전에 분배하는 방식을 이용한다[6].

SPINS는 데이터의 기밀성을 제공하기 위한 SNEP(Secure Network Encryption Protocol) 구조와 브로드캐스트되는 데이터의 인증을 제공하기 위한 μTESLA 스킴으로 구성된다.

3.2 키 관리기법

키 관리 기법으로는 Sink와 클러스터 구조를 중심으로 중간에 aggregator 노드를 두는 것을 기본 구조로 하는 그룹 키 관리 기법[9]과 일부 노드의 노출이 근접한 이웃 노드까지 노출시키는 위협을 최소화하기 위한 LEAP(Localized Encryption and Authentication Protocol)이 있다[10].

3.3 보안을 위한 센서 네트워크의 구조

센서 네트워크의 보안을 위해 제안된 여러 방식의 네트워크 구조를 살펴보면, 첫째, Sink를 보안상의 제약사항을 갖지 않는 특수한 노드로 설정하는 일반적인 방식과 달리 Sink에 대한 보안 강화를 위해 다중 Sink를 두는 네트워크 구조가 제시되었다[11]. 둘째, 센서 네트워크의 특성을 고려하여 비용, 공간 및 에너지 절약, 시간 효율성 등을 고려하여 네트워크를 관리영역과 비 관리 영역으로 분리하여 구성하는 분산된 네트워크 구조 및 키 관리 구조가 있다[12]. 셋째, 센서 노드의 레벨을 기반으로 하여 계층화된 구조를 정의하고 이웃의 수와 계층 클러스터에서의 레벨을 이용하여 에너지 효율을 높이는 동시에 최단 거리 통신을 가능하도록 하는 방안을 제시하는 방법(SRPSN) 등이 있다[13].

이 중 레벨 기반 계층화 구조방식은 타이머와 GPS 수신기를 가지고 이동성이 희박한 센서 노드들로 구성되며, 모든 센서 노드들에 대해 각각의 대칭키를 갖는 Sink 노드가 있음을 가정한다.

라우팅 방식은 Sink 노드가 네트워크 토폴로지를 파악한 후 그룹 키를 생성, 각 센서 노드에게 암호화하여 전송한다.

그룹 키 생성에 Multiparty Diffie-Hellman 프로토콜[14]을 응용, 각 센서 노드가 말단 노드로부터 상위 노드로 자신의 부분키를 내놓으면 부모 노드가 이를 취합하고 다시 부모 노드들이 내놓은 부분키를 그 상단에서 취합함으로써 그룹의 가장 상단의 노드가 전체 그룹 키를 최종적으로 확정하고 이를 암호화한 다음 각 센서 노드에게 보내는 방법을 취한다.

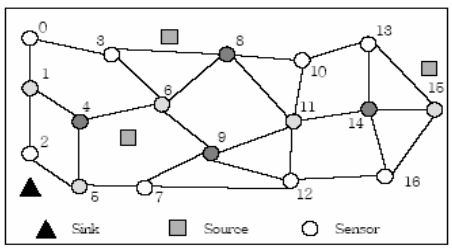

그림 2 레벨 기반 계층적 라우팅 프로토콜

그림 2에서 각 센서는 배치된 후 자신의 ID와 NBR(이웃의 수)을 브로드캐스트하여 주변에서 가장 높은 NBR을 가진 센서가 클러스터 헤드가 된다. 일반 센서, 클러스터 헤드, 두 개 이상의 클러스터 헤드를 연결하는 root순으로 레벨 1,2,3으로 점차 높아지며, 노드의 색깔이 진해질수록 레벨이 높은 센서를 의미한다.

이러한 계층적 구조는 네트워크 트래픽을 줄여 센서들의 자원을 절약할 수 있으며, 악의적인 노드에 의한 공격이나 센서의 고장으로 인해 정보가 중간에 잃어버리는 것을 방지할 수 있지만, 상단의 노드가 Sink와 멀리 떨어져 있을 경우, 가까이 있는 센서로부터 정보가 바로 전송되지 않고 우회하여 갈 수 있다. 또한, GPS 수신기는 파워나 메모리의 제약이 있는 센서노드에게는 부담스럽기 때문에 실제 환경에서는 적용하기 어렵다.

4. 교량 환경에 적용 가능한 보안기법 제안

교량 감시용 센서 네트워크는 센서가 교량에 고정되어 센서의 이동이 없기 때문에 다음과 같은 장점을 지니게 된다. 첫째, 이동에 따른 배터리 소모가 줄어든다. 둘째, 위치 파악을 위한 GPS장치가 필요 없고, 위치 정보를 통해 최단거리의 안정적인 보안을 제공할 수 있다. GPS장치 동작을 위한 에너지 소모가 없고, 설치 위치를 유지보수가 용이한 곳에 위치시켜 위험 노출정도가 다른 센서들에 비해 적다. 따라서 센서의 배터리 수명이 일반 GPS를 사용하는 센서보다 길기 때문에 보다 강력한 보안기술 및 키 관리 기법을 수용할 수 있다.

그림 3 교량의 모습

본 논문에서는 그림 3의 구조와 같은 인공구조물인 교량 감시용 센서 네트워크를 위한 보안 프로토콜을 제시한다.

교량은 크게 상부구조와 하부구조로 구성된다. 상부구조는 차량의 하중을 직접 지지하는 부분으로 상판 바닥틀, 상판을 지지하며 상부구조에 작용하는 모든 하중을 지점에 전달하는 역할을 하는 주형, 하중 저항 및 분배의 역할을 하는 브레이싱, 상부구조와 하부구조를 연결하는 구조부분으로써의 교량받침으로 나뉜다. 이외 부수적으로 신축이음장치 및 방호 울타리 등이 설치된다.

교대와 교각의 총칭을 하부구조라 하며, 지상에 적립한 부분을 구체, 지반에 적립하는 부분을 기초라고 한다. 기초 부분은 지반에 따라 말뚝기초, 우물통 기초 등으로 설치된다[15].

그림 4 교량의 점검로

위에서 알 수 있듯이, 교량받침은 교량의 거의 모든 하중 저항과 하중의 분배를 담당하는 중추적인 역할을 하는 곳으로 일반적인 교량보수 역시 그림 4와 같이 이곳에 집중된다. 센서 노드 역시 상판과 교량 받침 사이의 틈에 위치하는 것이 센서 노드의 부식률 저하와 보수에 적절하다[16].

즉. 교량 감시용 센서 네트워크에서는 그림 3과 같은 구조의 교량에 설치되는 최적의 네트워크 토폴로지와 센서 노드 수를 제안하여 보다 빠르고 안정된 보안 라우팅 프로토콜 기법을 제시한다.

또한, 인증 기법, MAC(message authentication code)[17], 키 관리 기법은 기존의 기법들을 그대로 수용하거나 수정하여 사용한다.

4.1 인증기법

교량 감시용 센서 네트워크에서 인증 기법은 SPINS 인증 키 생성 및 유지가 Sink에 집중 되는 것을 분산시키기 위해 3계층 방식을 응용한 TESLA 인증 방식을 수정하여 사용한다[17].

교량 감시용 센서 네트워크에서는 노드가 고정되어 초기 인증서 발급 이후 인증서 재발급이 필요 없다. 즉, TESLA 방식에서와 같이 TTP(Trusted Third Party)로부터 발행된 초기 인증서와 새로 장착된 노드와 응용 간의 공유키만을 설립하는 2계층 방식을 사용한다.

인증서 설정 및 사용단계는 다음과 같다.

첫째, 새로 가입 또는 설치되는 노드의 인증을 받기위해 TTP로부터 발급받은 초기 인증서(iCert)를 제출한다. 둘째, 새로 가입한 노드와 애플리케이션 간의 공유 키를 설립한다. 먼저, 공유 키 설립을 위해 제출한 초기 인증서의 유효성을 판별하고, 애플리케이션과 Sink, 애플리케이션과 센서 노드 사이에 공유키를 설립한 후 데이터의 근원지 인증 등의 서비스를 제공한다.

4.2 키 관리기법

제안하는 교량 구조와 같은 고정된 센서 네트워크에서는 센서 노드의 위치정보 및 ID, MAC 정보를 사전에 센서 노드에 장착함으로써 효율적인 키 관리 기법을 제시한다.

본 논문에서는 제안하는 방식에서는 LEAP의 키 관리 프로토콜을 사용하여 개인 키, 그룹 키, Pairwise key, Cluster key 등 네 가지 키를 생성한다.

먼저, 네트워크상의 모든 노드와 공유하는 그룹 키와 각 센서 노드가 Sink 노드와 공유하는 개인 키는 사전에 센서 노드에 분배한다.

이웃한 센서 노드와 공유하는 키 즉, Pairwise key는 경로 설정단계에서 노드에 저장되어 있는 MAC과 ID 정보를 이용하여 LEAP와 같은 방식으로 생성한다.

모든 이웃노드와 공유하는 Cluster key는 랜덤 키 K를 생성하고 생성된 키를 각각의 이웃노드와의 Pairwise key로 암호화하여 전달한다.

4.3 교량감시를 위한 센서 네트워크의 구조 및 보안 라우팅 프로토콜

교량에 설치되는 센서 노드들은 그림 5와 같은 네트워크 토폴로지로 구성된다.

교량상판과 교량받침사이의 틈에 7개가 기본으로 설치된다. 아래 교량하부의 교각과 우물통 부분의 센서 노드는 방수처리를 하여 교각이 물에 잠겼을 경우나 교각 또는 우물통의 진동 등을 별도로 감지하여 교량 하부를 감시하도록 한다.

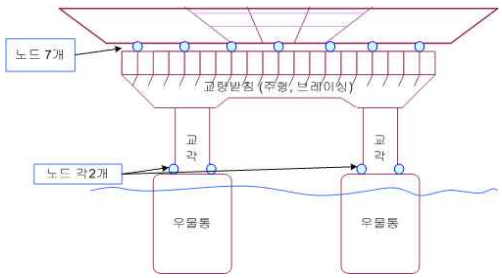

그림 5 교량의 센서 노드의 위치

위 그림 5의 센서 노드의 위치는 실제 교량에 적용할 경우를 가정하여 설정하였다.

그림 5에서 상부구조의 노드 7개 중 가운데 있는 노드를 다른 노드들로의 접근성을 고려하여

Sink로 정하였으며, 각 교각마다 같은 구조의 독립적인 센서 네트워크를 설치하여 교량의 상태를 감시한다. 단, 한 교각내의 센서 노드는 교각에 설치된 Sink와 통신 가능함을 가정한다.

교각에 설치되는 센서 노드들은 설치 전에 센서 ID, MAC, 위치정보 입력이외에 일정한 크기 이상의 자극에 의해서 Awake 상태로 전환되어 Sink로 감지한 정보를 전송하도록 하고, 그 이외의 경우에는 Sleep 상태를 유지하도록 하여 에너지 소모를 최소한으로 줄일 수 있도록 설정한다.

제안하는 방식은 이러한 특성을 고려하여 교량과 같은 인공 구조물을 위한 센서 노드와 네트워크에 대하여 다음과 같은 가정을 한다.

첫째, 각 센서 노드들은 MAC과 고유의 ID를 가지고 있으며, 각 노드에 데이터로 장착된다.

둘째, 센서 노드들은 이동성이 거의 없기 때문에 최초 설치 위치는 Sink에 저장된 후 별도의 업데이트를 하지 않는다. 따라서 GPS 같은 위치추적 장치를 필요치 않는다.

셋째, Sink는 센서 노드의 상태 즉, Sleep 상태인지 Awake 상태인지를 파악하기 위한 센서 노드로의 브로드캐스트가 가능한 반면, 각 센서 노드는 주변 노드로의 브로드캐스트가 불가능하다.

위와 같은 가정 하에 센서 네트워크의 라우팅 프로토콜은 각 센서노드의 Sleep 또는 Awake 상태를 판별하여 보안 경로를 설정하고, 설정된 경로로 보안 데이터를 안전하게 전송할 수 있도록 설정된 경로의 보안을 유지하는 것으로 이루어진다.

4.3.1 보안 경로 설정 프로토콜

센서 네트워크에서의 경로 설정 프로토콜방식은 통신 가능한 노드들을 찾기 위한 경로 요청메시지와 응답 메시지 그리고, 장애가 발생할 경우 대처할 수 있는 오류 메시지와 경로 대체경로 찾기 등으로 진행된다.

보안 경로 설정 프로토콜은 이와 유사한 방식으로 진행되나 Sink가 보안 경로 요청 메시지를 보내고 센서 노드들로부터 오는 요청 메시지를 다시 한 번 되돌려 보내 센서 노드의 앞뒤 경로를 파악할 수 있도록 하여 노드들 간의 인증이 가능하도록 하였다.

제안하는 방식의 보안 경로 설정 프로토콜은 보안 경로 요청, 보안 경로 전송, 보안 경로 유지 등 총 3단계로 이루어진다.

(1) 보안 경로 요청단계

각 센서 노드의 응답가능 여부를 호출하는 보안 경로요청(SRREQ: Secure Route Request)단계에서는 먼저 Sink 노드는 모든 센서 노드로 경로 요청 메시지를 브로드캐스트한다. Sink 노드는 센서 노드가 일정 크기 이상의 자극에 의해서 Sleep 상태에서 Awake 상태로 전환되므로, 센서 노드의 현재 상태가 Awake 상태인 센서 노드만을 파악하여 새로운 경로를 구축하기 위한 메시지를 보낸다.

보안 경로요청 단계의 메시지 구성은 다음과 같다.

(a) 경로요청 메시지(**Sink → SensorNode**)

$$\begin{cases} ID_{source}, ID_{\sin k}, ID_{SRREQ}, E_{key}(Rnum), \\ MAC(ID_{source}, ID_{\sin k}, ID_{SRREQ}, E_{key}(Rnum), Key) \end{cases}$$

(b) 경로요청 응답메시지(**SensorNode → Sink**)

$$\begin{cases} ID_{this}, ID_{pre}, ID_{source}, ID_{\sin k}, ID_{SRREQ}, E_{key}(Rnum), \\ MAC(ID_{source}, ID_{\sin k}, ID_{SRREQ}, E_{key}(Rnum), Key) \end{cases}$$

(a)의 경로 요청 메시지는 Source ID(ID_{source})와 Sink ID(ID_{sink}), 보안경로 요청 ID(ID_{SRREQ}), 임의의 숫자($Rnum$)로 암호화한 메시지와 메시지 인증코드 MAC으로 구성된다.

보안 경로요청 메시지를 받은 센서 노드는 (b)와같이 초기의 메시지에 자기 자신의 ID(ID_{this}), 이전 노드의 ID(ID_{pre})를 추가하여 Sink 노드의 MAC과 함께 경로요청 응답메시지를 구성하여 전송한다.

Awake 상태인 각 노드들로부터 경로요청 응답메시지를 받은 Sink 노드는 각 노드의 ID와 ID_{SRREQ}의 카운트를 보고 현재 깨어있는 노드의 수와 위치를 파악하여 경로를 설정한다.

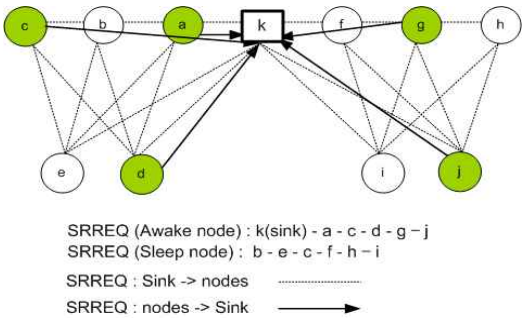

그림 6 보안경로 요청절차

그림 6에서 Sink 노드 k는 전체 센서 노드로 경로요청 메시지를 브로드캐스트하여 Awake 상태의 노드로부터 자신과 자신의 이웃 노드정보를 수집한다. 예를 들어, 노드 ***c***는 ***k***의 경로요청 메시지를 받고, 자신의 이웃 노드 중에서 ***b, e***가 Sleep 상태

이므로, 노드 ***d***를 다음 노드로 정해서 경로 ***c-d***를 Sink 노드로 보낸다.

(2) 보안 경로 전송단계

각 센서 노드의 앞뒤 노드 확인 및 센서 노드간의 보안 키 구축을 위해 보안 경로 전송 단계를 실행한다.

보안 경로전송 메시지 구성은 다음과 같다.

(c) 경로전송 메시지(**Sink → SensorNode**)

$$\begin{cases} ID_{this}, ID_{pre}, ID_{source}, ID_{\sin k}, ID_{SRREQ}, E_{key}(Rnum) \\ MAC(ID_{source}, ID_{\sin k}, ID_{SRREQ}, E_{key}(Rnum), Key) \end{cases}$$

(d) 경로전송 응답메시지(**SensorNode → Sink**)

$$\begin{cases} ID_{this}, ID_{next}, ID_{source}, ID_{\sin k}, ID_{SRREQ}, \\ MAC(ID_{source}, ID_{\sin k}, ID_{SRREQ}, Rnum, Key) \end{cases}$$

(1)단계의 경로요청 응답메시지(b)를 각 노드로부터 받은 Sink 노드는 경로요청 응답메시지(b)를 경로전송 메시지(c)의 형태로 구성하여 각 센서 노드에 브로드캐스트한다.

브로드캐스트된 경로전송 메시지(c)를 받은 각 노드는 메시지내의 이전 노드의 ID(ID_{Pre})가 자기 자신이면 (d)의 경로전송 응답메시지와 같이 자기 자신을 ID_{this}로, 경로전송 메시지(c)의 ID_{this}를 다음 노드의 ID(ID_{next})로 수정하여 자기 자신의 앞 뒤 노드를 경로 정보에 업데이트 한 후 경로전송 응답메시지(d)를 Sink로 보낸다.

Sink는 경로전송 응답메시지(d)와 경로요청 응답메시지(b)를 이용하여 경로를 구축한다.

즉, Awake 상태의 노드들을 찾아 그림 7과 같이 현재 경로를 수정한다. 이러한 방법을 통해 센서 노드들 간의 이웃노드와의 키 공유 및 인증을 함으로써 보다 안전한 경로구축을 할 수 있다.

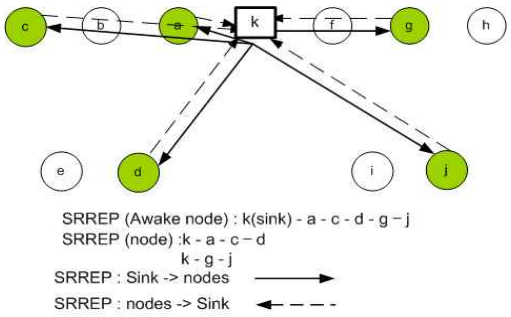

그림 7 보안 경로 전송절차

그림 7에서 Awake 상태의 노드 **a**, **c**, **d**, **g**, **j**는 Sink로부터 전송된 메시지를 이용해 자신과 이웃한 다음 노드 ID_{next}를 찾아 경로를 업데이트한다. 예를 들어, 노드 **g**의 다음 노드ID_{next}가 초기 설정에서 노드 **h**였지만, **h**가 Sleep 상태이고. 노드 **j**가 자신의 이전 노드 IDpre를 노드 **g**라고 했다면, 노드 **g**는 자신의 다음 노드가 **j**임을 알고 경로를 **k-g-j**로 수정할 수 있다.

(3) 보안 경로 유지단계

Awake 상태의 노드들로 경로를 구축하고 구축된 경로로 데이터나 패킷이 안전하게 전송될 수 있도록 경로를 유지하기 위해 각 노드는 데이터나 패킷을 전송할 때, 전송이 실패할 경우 Sink 노드로 보안 경로 에러(SRERR: Secure Route Error) 메시지를 보내어 경로 재구축 또는 다른 경로를 이용하여 우회하여 보낼 수 있도록 한다.

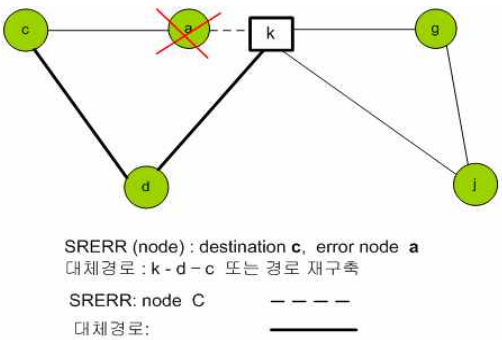

그림 8 경로 재구축 절차

그림 8에서처럼 노드 ***a***가 Sleep 상태이거나 또는 다른 이유에 의해서 데이터를 전송하지 못할 경우, 데이터를 전송하는 노드 ***c***는 일정시간 동안 a로부터 ACK 메시지를 받지 못했을 때, Sink로 보안 경로 에러메시지를 보내고, Sink는 다른 대체 경로의 노드 ***d***를 통해서 목적지 노드 ***c***로의 경로 정보를 보내주거나, 경로를 재구축한다.

4.3.2 안전한 데이터 보내기

데이터를 보낼 때, Sink 노드만이 각 노드들의 고유 ID를 알고 있으므로 각 노드의 ID와 MAC과 함께 데이터를 암호화하여 보낸다.

즉, 각 센서 노드에서 Sink로 보내는 데이터 메시지의 구성은 다음과 같다.

$$\begin{cases} ID_{this}, ID_{next}, [ID_{source}, R_{number}, E_{Key}(data)], \\ MAC[ID_{source}, R_{number}, E_{Key}(data), Key]) \end{cases}$$

각 센서 노드가 Sink로 data를 전송할 때, 자신의 ID_{this}와 다음 노드의 ID_{next}와 암호화된 data와 ID_{source}와 임의의 수를 생성하여, 노드의 MAC 정보와 함께 전송한다.

5. 분석 및 실험

제안하는 교량과 같은 인공구조물을 위한 무선 센서 네트워크는 센서 노드의 설치단계 이전에 노드의 위치를 미리 설정하여 센서 노드에 입력할 수 있다. 또한, 노드 간의 통신이 가능하도록 통신 범위 내에서 일정한 간격으로 설치할 수 있다.

따라서 GPS 같은 위치 파악을 위한 추가적인 장비 없이 초기에 센서 노드에 입력하는 방식만으로 센서 노드의 위치를 파악하여 제어할 수 있다.

본 실험에서는 노드의 ID와 MAC은 센서 노드에 기본적인 정보를 입력할 당시에 함께 입력한다는 가정 하에 위에 대한 사항을 배제하고 순수 노드의 Sleep과 Awake 확률에 따른 경로 생성확률과 에너지 소모율을 앞서 제안된 레벨 기반 계층적 라우팅 프로토콜 SRPSN([13]에서 제안된 라우팅 프로토콜과 비교 분석한다.

5.1 경로 생성확률

(1) SRPSN(Secure Routing Protocol in Sensor Network)

기존의 레벨 기반 계층적 라우팅 프로토콜의 토폴로지는 그림 9와 같이 생성된다.

레벨 기반 계층적 라우팅 프로토콜(SRPSN)은 센서 노드 16개일 경우(Sink까지 17개), 2계층 레벨로 이뤄지며, 각 노드는 상위 클러스터 노드를 통해서만 Sink 노드로 통신할 수 있다. 따라서 생성되는 경로의 경우의 가지 수는 아래 표 1과 같다.

(2) 제안하는 프로토콜(BSRPSN: Bridge SRPSN)

제안하는 방식의 라우팅 프로토콜은 레벨 기반의 계층적 센서노드를 구성하는 대신 각 센서 노드의 위치 파악이 가능한, 평면적인 토폴로지를 구성하였다. 또한 각 센서 노드들의 파워를 대등하게 설정하여 비대칭적인 센서 파워를 고려할 시 발생되는 비용을 절약 할 수 있도록 가정하였다.

이러한 가정을 통하여 그림 10과 같은 교량의 라우팅 프로토콜을 생성하였다.

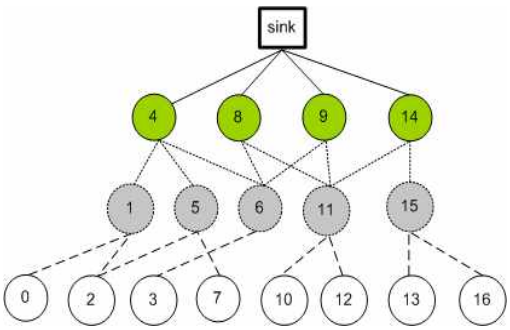

그림 9 SRPSN(레벨기반 계층적 라우팅 프로토콜)

그림 10의 센서 노드의 수는 Sink 노드 K를 포함하여 총 11개의 노드로 구성하였다. 각 센서 노드의 위치는 편의상, 교량의 모양에 의해 구성하였으며, 생성 가능한 라우팅 경로의 수는 표 1과 같다.

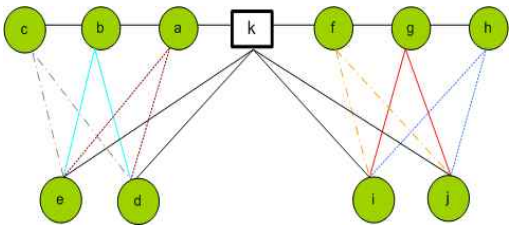

그림 10 BRPSN(교량의 라우팅 프로토콜)

표 1은 각 라우팅 프로토콜의 Hop수에 따른 생성될 수 있는 경로의 가지 수를 계산한 표이다.

표에서도 알 수 있듯이. 계층적 라우팅 프로토콜은 불필요한 에너지 소모를 줄이기 위해 설정한 계층이 가까운 거리 또는 하위 노드와 Sink 노드 간의 직접 통신을 배제함으로써 제안된 방식(BSRPSN)에 비해 생성될 수 있는 경로의 가지 수가 현저히 적음을 알 수 있다.

표 1 경로 수

hop수	SRPSN 경로 수	BSRPSN 경로 수
1	4	14
2	20	84
3	160	420

그림 11은 표 1을 그래프로 표현한 것으로 평균 3배정도의 경로 수 차이를 보이고 있다는 것을 알 수 있다.

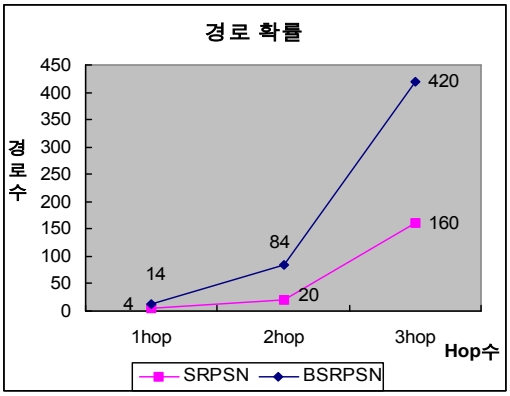

그림 11 Hop수에 따른 경로확률

5.2 에너지 소모율

제안하는 프로토콜의 에너지 소모율은 다음과 같은 이유로 기존의 **SRPSN**(Secure Routing Protocol in Sensor Network) 방식보다 뛰어난 에너지 효율성을 갖는 것을 알 수 있다.

첫째, 현재 실험용 테스트로 많이 쓰이고 있는 MICAz MOTE의 CPU 성능이 2.4GHz이고, 최대 10m 내외의 노드간의 통신이 가능하다[18]. 따라서 한 홉 또는 2~3홉 내에 경로를 설정할 수 있기 때문에 굳이 계층적인 구조를 사용할 필요가 없으며, 상위 계층의 노드들이 Sink 노드와 통신하기 위해 소모하는 에너지를 줄일 수 있다.

둘째, 센서 노드가 고정되어 있어 노드의 위치를 임의로 설정할 수 있으며, 설정 시 위치정보나 노드의 고유 ID 등을 프로그램으로 장착할 수 있기 때문에 별도의 GPS 장치가 필요 없다. 현재까지 개발된 초소형 GPS 수신기 칩셋은 3.3V, 최대 전류 1400mA/h로 작동 시 1시간에서 1시간 30분 정도 사용할 수 있으며, 최대 사용시간은 약 11시간 정도이다[19]. 따라서 최소 전력소비량은 약 420mW이다. 이는 표 2와 같이 센서노드가 전체 동작하는데 소비되는 전력 36mW의 12배에 달한다. 셋째, 노드의 휴면과 활동 상태에 따라 활동 상태의 노드들로 경로를 구축함으로써 센서 노드의 불필요한 전력 소모를 줄일 수 있으며, 노드의 생명주기를 일정하게 유지할 수 있다.

동작 모드	전류(mA)	전력(mW)
ATMega128L, 전체 동작	12 (7.37MHz)	36
ATMega128L, Sleep	0.010	0.03
Radio, receive	19.7	59.1
Radio, transmit(1mW, power)	17	51
Radio, sleep	0.001	0.003
Serial flash memory, write	15	45
Serial flash memory, read	4	12
Serial flash memory, sleep	0.002	0.006

표 2 MICAz의 전류 및 전력 요구량

위와 같이 제안 프로토콜의 배터리 소모율이 현저히 줄어들고, 따라서 부가적으로 위치를 찾기 위해 낭비되는 시간과 비용을 절약할 수 있다.

센서 노드는 1.5V의 건전지 2개 즉, 3V로 약 2000mA/h의 배터리 용량을 가지며, 센서 노드의 생명유지에 필요한 최소한의 에너지만을 소모한다면 약 12개월간의 수명을 보장한다[18].

표 3은 표 2를 참조하여 제안 프로토콜과 SRPSN의 경로 구축시 에너지 소모율을 비교한 것이다.

총에너지 (2000mA/h * 3V = 6000mW/h)

BSRPSN		SRPSN	
초기 상태	36	초기상태	36
Sink RREQ	36	Sink GPS 위치 수신	1400
SN RREQ(S)	51		
Sink RREQ(R)	59.1		
경로정보갱신	45		
SN RREP(S)	51		
Sink RREP(R)	59.1		
경로정보갱신	45	정보갱신	45
Total	**382.2**	**Total**	**4281**

표 3 보안 경로 생성시 에너지소모율

위 표에서 제안된 BSRPSN 프로토콜 방식으로 경로를 구축하는 것이 GPS 수신기를 이용하는 것에 비해 약 11배의 에너지소모 감소율을 보이고 있음을 알 수 있다. 아래 그림 12은 표 3을 그래프로 나타낸 것으로 두 프로토콜의 에너지 소모율을 보여주고 있다.

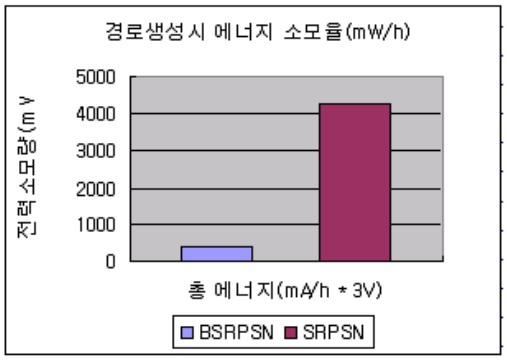

그림 12 보안 경로 생성시 에너지 소모율

6. 결 론

센서 네트워크는 상당히 다양한 분야에 응용되고 있으며, 교량 감시 또한 센서 네트워크가 응용되는 하나의 영역임을 안다.

본고에서는 센서 노드의 이동성을 가정하는 일반적인 센서 네트워크의 경우와 달리 고정된 센서들로 이루어진 센서 네트워크의 경우에 요구되는 보안기법이 서로 다를 수 있다는 것에 초점을 두었다.

인공 구조물의 경우 센서 노드 자체에 초기에 기본적인 프로그램을 설치하는 단계에서 고유한 ID 및 위치정보를 미리 설계하여 프로그램화 하여 넣을 경우 다음과 같은 이익을 얻을 수 있다.

첫째, 센서 노드가 비 계층적이기 때문에 센서 노드가 상위 계층일 수로 센서 노드의 성능이나 기능을 다르게 설정하는 레벨 기반의 계층적 프로토콜과 달리 센서 노드의 성능을 일정하게 설정할 수 있다. 이렇듯 센서 노드의 성능차이를 고려하지 않는다는 것은 센서 노드의 구입비용 및 생명 주기가 비슷하다는 것을 의미한다.

둘째, 경로 생성의 수가 월등히 많다는 것은 대체 경로의 수가 있을 가능성이 높다는 것으로, 데이터 전송률도 높을 것으로 추측할 수 있다.

앞으로 우리가 해야 할 과제는 시뮬레이션을 통해 센서 네트워크에 적용, 성능분석을 통하여 레벨 기반 센서 네트워크 보안구조와 비교하여 성능향상 정도를 측정하고 보다 나은 기술에 대해 생각해 보는 것이다.

참 고 문 헌

[1] I.F. Akyildiz,W. Su, Y. Sankarasubramaniam. and E. Cyirci., "Wireless sensor networks: A survey." In *Computer Networks*, volume 38(4), pages 393422, 2002.

[2] T. Nieberg, S. Dulman, P. Havinga, L.v. Hoesel, and J.Wu. "Collaborative algorithms for communication in wireless sensor networks." In T. Basten, M. Geilen, and H. de Groot, editors, *Ambient Intelligence: Impact on Embedded Systems Design*, pages 271294.Kluwer Acad. Publishers, 2003.

[3] Tieyan Li, "Security Map of Sensor Network," http://www.i2r.a-star.edu.sg/icsd/SecureSensor/papers/security-map.pdf,Aug. 2004.

[4] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, *Wireless sensor networks*: a survey Computer Networks 38 (2002) 393422, December 2001.

[5] http://dutetvg.et.tudelft.nl/~alex/CFP/

[6] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar, "SPINS: Security Protocols for Sensor Networks," Proc. of the 7th ACM/IEEE International Conference on MobiCom, 2001.

[7] http://www.ietf.org/internet-drafts/draft-ietf-msec-tesla-spec-00.txt draft-ietf-msec-tesla-intro-01.txt

[8] Jean-Pierre Avognon, Zhi Tang Li, "New Multicast Technology Survey and Security Concerns," *Information Technology Journal 3 (1)*:, 95-105, 2004.

[9] 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.

[10] 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.

[11] J. Deng, R. Han, and S. Mishra, "Enhancing Base Station Security in Wireless Sensor Networks," Technical Report CU-CS-951-03, Department of Computer Science, University ofColorado, Apr. 2003.

[12] Yee Wei Law, Ricardo Corin, Sandro Etalle, and Pieter H. Hartel, "A Formally Verified Decentralized Key Management Architecture for Wireless Sensor Networks," Proc. of PWC' 03, Sep. 2003.

[13] Malik Tubaishat, Jian Yin, Biswajit Panja, and Sanjay Madria, "A Secure Hierarchical

Model for Sensor Network,"Proc. of SIGMOD, Mar. 2004.
[14] Jean-Franc¸ois Raymond, Anton Stiglic, "Security Issues in the Diffie-Hellman Key Agreement Protocol", Zero-Knowledge Systems, Inc. December 19, 2000.
[15] Mathias Bohge and Wade Trappe, "An Authentication Framework for Hierarchical Ad Hoc Sensor Networks," Proc. of WiSE' 03, 2003.
[16] http://www.britec.co.kr/index/index.php
[17] h. Krawczyk, M. Bellare, and R. Canetti. HMAC: "Keyed-Hashing for Message Authentication," Internet RFC 2104, February 1997.