情報保護學會論文誌
第15券 第2號, 2005. 4

이동 싱크를 가진 무선 센서 네트워크의 안전한 라우팅 기법*

김 태 균,[1†] 김 상 진,[2] 오 희 국,[1‡] 이 익 섭,[3] 유 동 영[3]
[1]한양대학교, [2]한국기술교육대학교, [3]한국정보보호진흥원

A Secure Routing Scheme for Wireless Sensor Networks with a Mobile Sink*

Taekyun Kim,[1†] Sangjin Kim,[2] Heekuck Oh,[1‡] Ik-Seob Lee,[3] Dongyoung Yoo[3]
[1]Hanyang University, [2]Korea University of Technology and Education,
[3]Korea Information Security Agency

요 약

센서 네트워크에서 기존의 안전한 라우팅 방식은 고정된 싱크(sink)를 가정하였다. 그러나 실제 센서 네트워크가 활용되는 많은 분야에서 싱크는 사람이나 차량에 의해 이동되는 경우가 많다. 싱크의 이동은 감지된 데이터를 전달하기 위한 라우팅 경로의 재구성, 싱크의 위치 노출, 안전한 액세스 포인트 노드의 선택과 같은 기존의 연구에서 고려하지 않은 추가적인 문제점을 발생시킨다. 본 논문에서는 양방향 해쉬 체인과 그리드(grid) 형태의 위임 노드(delegation node)를 이용하여 위의 문제점을 해결하는 기법을 제안한다. 요청-응답 프로토콜과 이벤트 유도 프로토콜로 구성된 이 기법은 싱크의 이동에 따른 라우팅 경로를 안전하게 재구성해주고, 싱크의 위치 정보가 노출되지 않도록 보호해준다. 성능면에서 제안하는 기법은 경로를 저장하여 이용하는 라우팅 방식보다 통신 횟수가 적어 자원을 절약할 수 있다. 본 논문은 제안한 시스템의 안전성 분석과 시뮬레이션을 통한 성능평가 결과를 보여준다.

ABSTRACT

Previous secure routing protocols for wireless sensor networks assume that a sink is static. In many cases, however, a sink operated by man or vehicle is moving. A mobile sink creates a lot of technical problems such as reconfiguration of routing path, exposure of sink location, and selection of secure access point node, which are not considered by many previous researches. In this paper, we propose a new secure routing scheme for solving such problems using bi-directional hash chain and delegation nodes of grid structure. This scheme provides a secure routing path and prevents attacker from recognizing the location of a mobile sink in sensor networks. This new method reduces the resource requirements compared to the cashed routing schemes. Simulation results also show that the system is secure and efficient enough.

Keywords : *Sensor networks, Secure routing, Mobile sink*

접수일 : 2004년 12월 6일 ; 채택일 : 2005년 4월 8일
* 본 연구는 한국정보보호진흥원의 "홈 네트워크 표준보안 프레임워크 개발" 연구 결과의 일부분입니다.
† 주저자 : tkkim@cse.hanyang.ac.kr
‡ 교신저자 : hkoh@cse.hanyang.ac.kr

Ⅰ. 서 론

최근 무선 통신 분야에서 중요한 연구 분야로 떠오르고 있는 무선 센서 네트워크는 환경 및 생태감시, 군사작전, 인텔리전스 빌딩, 홈 네트워크 등 많은 분야에서 활용되고 있다. 군사용의 경우 센서 노드가 적 군사 지역에 설치되어 적군이나 적 차량의 이동을 감지하거나 감시할 수 있다. 집이나 사무실에서는 노약자의 건강이나 침입자에 대한 정보를 감지를 할 수 있다. 이런 감지된 정보는 공격자로부터 보호되어야 하며 수신자에게 안전하게 전달되어야 한다. 센서 네트워크의 안전한 라우팅 방법에 대한 대부분의 연구는 싱크(sink)가 이동하지 않는 환경을 가정하였다. 하지만 실제 센서 네트워크를 이용하는 많은 분야에서는 싱크가 이동하는 경우가 적지 않다.[1] 예를 들어 센서 네트워크가 가장 많이 활용되는 군사용의 경우 전장에서 싱크가 감지된 정보를 수집하면서 사람 또는 차량에 의해 이동하는 경우가 대부분이다. 이렇게 싱크가 이동할 경우 기존 연구에서 고려되지 않았던 다음과 같은 추가적인 문제점이 발생한다.

첫째, 싱크는 언제든지 이동할 수 있어 요청(request) 메시지를 보낸 후 이에 대한 응답(response) 메시지가 오기 전에 처음 요청 메시지를 수신했던 액세스 포인트 노드(access point node)와 통신이 되지 않는 위치로 이동할 수 있다. 고정된 싱크의 경우 응답 메시지가 액세스 포인트 노드까지만 오면 싱크까지 전달이 가능하나 이동 싱크의 경우 감지된 데이터가 액세스 포인트 노드까지 오더라도 싱크에게 제대로 전달할 수가 없는 상황이 발생한다. 이를 방지하기 위해 싱크가 이동한 경우 감지된 데이터 전달을 위한 추가적인 경로를 재구성해 주어야 한다.

둘째, 싱크의 이동 때문에 센서 노드들은 고정된 라우팅 경로를 이용하여 정보를 전달할 수가 없으므로 싱크의 이동에 따라 그 위치를 센서 노드들에게 알려주어야 한다. 하지만 감지된 정보를 싱크에 전달하기 위해 이동하는 싱크의 위치를 전체 네트워크에 알리는 것은 자원절약적인 측면뿐만 아니라 보안적인 측면에서도 좋지 않다. 예를 들어 센서 노드에게 전달되는 싱크 위치 정보를 통해 공격자가 싱크의 위치를 파악할 수 있다면 실제 전장에서 적의 위치나 이동 경로를 파악하기 위해 설치한 센서 네트워크가 오히려 아군의 위치를 노출시키는 위험한 결과를 초래할 수 있다. 그러므로 센서 네트워크의 안전한 이용을 위해 싱크의 위치를 숨기는 기법이 필요하다.

셋째, 요청-응답 메시지가 전달되는 과정 중에 메시지안의 라우팅 정보에 의해 네트워크의 센서 노드의 토폴로지(topology)에 대한 정보가 쉽게 노출될 수가 있다. 각 센서 노드가 노출시키는 이웃노드의 위치 정보를 최소화하여 전체 네트워크의 토폴로지가 노출되는 것을 방지하는 기법이 필요하다.

넷째, 처음 요청 메시지를 전달하는 액세스 포인트 노드뿐만 아니라 싱크가 이동할 때 선택하는 새로운 액세스 포인트 노드가 안전하지 않으면 송수신 데이터의 안전성을 보장할 수가 없다. 그러므로 안전한 액세스 포인트 노드를 선택하는 방법과 올바르게 선택된 노드인지를 확인할 수 있는 인증 방법이 필요하다.

이와 같은 문제점을 해결하기 위해 싱크가 이동하는 환경에서 안전하게 통신할 수 있는 라우팅 기법이 필요하다. 먼저 센서 네트워크와 유사한 기존의 네트워크에서 적용 가능한 방법이 있는지 라우팅 방법들을 살펴보면 다음과 같다. 모든 노드들이 이동하는 MANET(Mobile Ad-hoc Network)에서는 일반적으로 이전에 저장된 경로를 이용하고, 이를 이용할 수 없는 경우에는 경로를 재탐색하는 방법을 사용하고 있다. 그러나 센서 네트워크의 경우 일반 센서 노드가 이동하는 경우는 거의 없고 주로 싱크가 이동하기 때문에 싱크를 제외한 일반 노드의 위치 변화가 거의 없다. 그러므로 MANET의 라우팅 방법인 저장된 경로를 재사용하거나 경로를 재탐색하는 방법은 비용이 많이 들어 자원이 지극히 한정된 센서 네트워크에는 적절하지 않은 방법이다. 셀룰러 시스템의 경우 센서 네트워크와 달리 유선으로 베이스 스테이션 백본(base station backbone)이 구성된 하부구조 기반의 시스템(infrastructure-based system)으로 자원 절약보다는 QoS(Quality of Service)와 통신대역폭의 효율적인 사용에 초점을 맞추고 있다. 또한 이동 노드를 인증하기 위한 정보를 이동 스위칭 센터(mobile switching center)를 통해 데이터베이스 센터(database center)로부터 받아 확인하기 때문에 센서 네트워크에 적용하기에는 적절하지 않다. 그러므로 싱크가 이동하는 환경에 대해 안전하게 통신할 수 있는 새로운 라우팅 기법에 대한 제안이 필요하다.

본 논문에서는 앞에서 언급한 네 가지 문제를 해결하기 위해 양방향 해쉬 체인과 그리드(grid) 형태

의 위임 노드(delegation node)를 이용하여 안전하게 통신할 수 있는 새로운 라우팅 기법을 제안한다. 요청-응답 프로토콜과 이벤트 유도(event-driven) 프로토콜로 구성된 이 기법은 싱크의 이동에 따른 라우팅 경로를 안전하게 재구성해주고, 싱크의 위치 정보가 노출되지 않도록 보호해준다. 요청-응답 프로토콜에서는 싱크와 이웃 노드의 위치가 노출되지 않도록 하였고, 비밀키와 양방향 해쉬 체인을 이용하여 메시지와 싱크에 대한 신속한 인증 기능을 제공하여 이웃노드의 자원을 소비시키는 공격 가능성을 줄였다. 이벤트 유도 프로토콜에서는 그리드 형태의 위임 노드와 요청-응답 프로토콜을 기초로 싱크의 위치를 숨기면서도 통신 횟수를 줄여 전력자원의 소비를 감소시켰다. 본 논문의 나머지 부분은 다음과 같이 구성된다. 2장에서는 기존에 제시된 관련 연구들에 대해서 살펴보고, 3장에서는 제안하는 시스템에 대한 개요를 살펴본다. 4장에서는 양방향 해쉬 체인을 이용한 요청-응답 프로토콜을 제안하고, 이 프로토콜을 기초로 5장에서는 그리드 형태의 위임 노드를 이용한 이벤트 유도 프로토콜을 제안한다. 6장에서는 제안한 시스템에 대한 시뮬레이션 결과와 프로토콜의 안전성을 분석하고 기존 시스템과 차이점을 비교한다. 마지막으로 7장에서는 결론 및 향후 과제에 대하여 언급한다.

Ⅱ. 관련 연구

센서 네트워크는 기존의 유사한 네트워크와 환경적인 차이점을 가지고 있어 기존 네트워크의 라우팅 기법이 바로 적용될 수 없다. 셀룰러 시스템은 유선의 베이스 스테이션 백본이 미리 구성되어 있는 시스템으로 이동 노드는 가장 가까운 베이스 스테이션과 한번의 홉(one hop)만으로 통신을 한다. 또한 베이스 스테이션에는 거의 무제한으로 전력이 공급되고 이동 노드도 배터리를 충전할 수 있기 때문에 통신 프로토콜이 자원절약보다는 우수한 통신 품질과 대역폭의 효과적인 사용에 중점을 두고 있다. 그리고 베이스 스테이션이 이동 노드에 대한 인증 정보를 데이터베이스 센터로부터 받기 때문에 센서 네트워크에 적용하기에는 적절하지 않다.

MANET은 배터리에 의해 전원이 공급되지만 사용자에 의해 언제든지 충전될 수 있기 때문에 에너지 절약 차원보다는 서비스 품질에 더 큰 목적을 두고 있다. MANET는 대부분 베이스 스테이션과 같은 중앙제어기관(central controlling agent)을 가지고 있지 않아 이를 중심으로 한 라우팅 프로토콜이 거의 없다. 이와는 대조적으로 센서 네트워크는 노드 수나 분포밀도가 훨씬 높고 전력, 연산능력, 메모리와 같은 자원 제약 사항이 많아 기존의 라우팅 프로토콜을 그대로 사용하기에는 적절하지 않다. 안전한 라우팅 방법과 키 분배 방식 등 보안에 관한 연구는 센서 네트워크에서 중요한 부분으로 고려되어 많은 연구가 진행되고 있다. 이 가운데 본 논문에서 다룰 안전한 라우팅 기법과 관련된 기존 연구를 살펴보면 다음과 같다.

센서 네트워크 보안의 대표적인 연구로 Perrig 등[2]이 제안한 시스템인 SPINS에서는 싱크와 노드와의 안전한 통신을 위해 SNEP(Secure Network Encryption Protocol)와 μ-TESLA(Micro Timed Efficient Stream Loss-tolerant Authentication)라는 두 가지의 방법을 제안하였다. SNEP는 적은 오버헤더로 데이터의 기밀성과 최근성을 보장하고 두 노드 사이에 인증을 가능하게 해주는 기법이고 μ-TESLA는 대칭키만을 이용하여 인증된 브로드캐스트(authenticated broadcast)를 할 수 있도록 한 기법이다. 하지만 이 기법은 브로트캐스트 인증 시 시간 지연이 발생하기 때문에 거짓 메시지를 보내 전력을 소모시키는 공격이 가능하다.

Karlof 등[3]이 제시한 논문에서는 보안을 고려하지 않은 라우팅 프로토콜에서 발생할 수 있는 다양한 공격과 그에 대한 대처방법에 대해 언급하고 있다. 하지만 이 논문에서도 다양한 공격을 효율적으로 막기 위해서는 기존의 라우팅 프로토콜에 대한 보완보다는 안전한 라우팅 프로토콜을 새로 설계해야 한다고 제시하고 있다.

INSENS[4]에서는 다중 경로 라우팅, 플러딩(flooding)의 제한, 단 방향 해쉬 체인을 이용하여 공격자가 몇 개의 노드를 획득하더라도 견뎌낼 수 있는 시스템을 제안하였다. 하지만 라우팅 테이블을 생성하기 위한 경로를 검색할 때 노드 수에 비례하여 정보의 양이 늘어나 대규모 네트워크에 적합하지 않다.

Marti 등[5]과 Tanachaiwiwat 등[6]은 이웃 노드의 신뢰도를 관리하여 특정한 값 이하로 내려가면 신뢰할 수 없는 노드로 판단하고 경로상의 노드에서 제외시키는 방법을 제안하였다. 이 방법은 신뢰도를 사용하지 않는 것보다 재전송을 해야 하는 빈도가 낮기 때문에 자원이 절약될 수 있다. 본 논문에서도 액세스 포인트를 선택할 때 이 기법을 이용하여 안전한

노드를 선택한다.

LU 등[7,8]이 제안한 MANET 기반의 논문에서는 이동 가능한 싱크에 대한 언급을 하고 있지만 이를 계층적 구조에서 이동 가능한 노드의 특별한 형태로만 간주하여 싱크 중심으로 데이터가 전달되는 센서 네트워크의 특성을 제대로 고려하지 못하였다.

Gorlach 등[9], Capkun 등[10], Kong 등[11]은 유비쿼터스 환경 또는 모바일 애드혹 네트워크 환경에서 이동 노드의 위치를 노출시키지 않기 위한 연구를 하였다. 하지만 이 연구는 노드의 위치를 직접 숨기는 방법이 아니라 여러 개의 노드 중 어느 것이 추적하는 것인지를 모르게 하는 방법으로 센서 네트워크의 싱크 위치를 숨기는 기법으로 적절하지 않다.

Ⅲ. 제안하는 시스템: 개요

센서 네트워크의 라우팅 방법은 크게 네 가지로 나누어 볼 수 있다.[12] 먼저 싱크가 어떤 요청 메시지를 특정 지역의 센서 노드에게 보내면 이에 대해 센서 노드가 응답해주는 요청-응답(request-response) 방법, 미리 지정된 특정한 조건을 만족하면 센서 노드가 감지된 정보를 싱크에게 전달해주는 이벤트 유도(event-driven) 방법, 일정한 주기를 가지고 지속적으로 센서가 싱크에게 데이터를 보내주는 지속적인(continuous) 방법, 마지막으로 이러한 방법들이 하나의 센서 네트워크 안에 같이 있는 하이브리드(hybrid) 방법이 있다. 본 논문에서는 요청-응답 방법과 이벤트 유도 방법이 하나의 시스템 안에 같이 있는 하이브리드 라우팅 프로토콜을 제안한다.

제안하는 시스템의 요청-응답 프로토콜은 세 가지 단계로 나누어 볼 수 있다. 첫째, 싱크의 요청을 센서 노드에게 전달하고 감지된 데이터가 전달될 경로를 구성하는 단계. 둘째, 감지된 데이터를 소스로부터 싱크까지 전달하는 단계. 셋째, 이동하는 싱크에게 감지된 데이터 정보를 전달하기 위해 소스와 싱크 사이의 연결을 지원해주는 단계이다. 먼저 메시지가 전달되기 위해서는 라우팅 경로를 설정해 주어야 한다. 이를 위해 각 센서 노드들은 참조 노드(reference node)[13,14]를 이용하여 각자의 위치 정보를 싱크에게 전달하여 싱크가 전체 네트워크의 토폴로지를 구성할 수 있게 한다. 싱크는 Marit 등[5]과 Tanachaiwiwat 등[6]이 제안한 방식을 이용하여 자신의 이웃 노드 중 안전한 노드를 엑세스 포인트로 선택하여 요청 메시지를 전달한다. 싱크는 자신이 생성한 양방향 해쉬 체인과 각 센서 노드와 공유하고 있는 비밀키를 이용하여 전달되는 메시지를 보호하고 네트워크의 위치정보가 노출되지 않도록 한다. 요청 메시지가 전달된 액세스 포인트 노드와 통신이 불가능한 위치로 싱크가 이동하면 양방향 해쉬 체인을 이용하여 이전의 액세스 포인트 노드로부터 새로운 액세스 포인트 노드까지 안전하게 데이터가 전달될 수 있도록 한다.

제안하는 이벤트 유도 프로토콜은 네트워크를 그리드(grid) 형태로 나누고 위임 노드(delegation node)를 지정하여 싱크의 위치가 노출되는 것을 최소화하고 자원을 절약할 수 있는 방법이다. 이동 싱크는 가장 가까운 위임 노드까지 요청-응답 프로토콜을 이용하여 감지된 데이터가 전달될 수 있도록 경로를 설정하고 센서 노드는 이벤트가 발생하면 위임 노드에게 알려 싱크가 어떠한 위치에 있어도 데이터가 전달될 수 있도록 한다.

제안하는 프로토콜은 다음과 같은 가정을 한다.

센서 노드들은 자신의 위치정보를 알고 있다. Bulusu 등[13]과 Albowicz 등[14]이 제안한 방법을 이용하면 GPS(Global Positioning System)와 같은 부과적인 하드웨어 장치를 사용하지 않고도 자신의 위치를 파악할 수가 있다.

일반 센서 노드는 설치된 이후에는 이동하지 않지만 싱크는 센서 네트워크의 감지된 정보를 수집하면서 이동할 수 있다.

키 획득 공격에 대해 싱크는 안전하나 센서노드는 안전하지 않다.

싱크와 각 센서 노드사이에는 서로 비밀키를 공유하고 있다. 이 비밀키는 센서 노드를 설치하기 이전에 미리 각 노드에 저장해둔다.

이 논문이 제안하는 프로토콜에서는 다음과 같은 표기법을 사용한다.

A, B, C, D는 일반 센서 노드를 나타낸다.

S는 싱크, E는 감지된 정보를 보내는 센서 노드를 나타낸다.

K_A, K_B는 싱크와 일반 센서 노드(A, B) 사이의 비밀키를 나타낸다.

$MAC_{K_A}(Msg)$는 비밀키 K_A를 이용한 메시지(Msg) 인증 코드를 나타낸다.

$\{Msg\}_{K_A}$는 메시지(Msg)를 비밀키 K_A로 암호화한 것을 나타낸다.

$AP_0, AP_1, ..., AP_m$은 순차적인 액세스 포인트 노

드를 나타낸다.

ap_0, bp_0, a_0, b_0는 해쉬 체인을 생성하기 위한 임의의 랜덤(random) 값을 나타낸다.

ReqMsg는 요청 메시지, ResMsg는 감지된 응답 메시지를 나타낸다.

h는 해쉬 함수, TS는 타임 스탬프(time stamp)를 나타낸다.

Ⅳ. 요청-응답(request-response) 프로토콜

이 장에서는 싱크의 요청에 의해 센서 노드가 응답하는 요청-응답 프로토콜을 상세하게 기술한다. 이 프로토콜은 싱크가 원하는 정보를 얻기 위해 특정 지역의 센서 노드에게 명령을 전달하는 요청 프로토콜, 이에 대한 응답으로 감지된 정보를 싱크에게 안전하게 전달하기 위한 응답 프로토콜, 싱크가 요청 메시지를 보낸 후 액세스 포인트 노드와 통신할 수 없는 위치로 이동한 경우에도 응답 메시지를 전달하기 위한 이동 싱크 지원 프로토콜로 구성되어 있다.

4.1 요청(request) 프로토콜

각 센서 노드는 자신의 위치 정보와 이웃한 노드에 대한 정보를 수집하여 싱크에게 전달한다. 싱크는 Bulusu 등[13]과 Albowicz 등[14]이 제안한 방법처럼 각 센서 노드가 보낸 위치 정보를 이용하여 전체 네트워크에 대한 노드들의 토폴로지(topology)을 구성한다. 이 토폴로지 정보는 싱크가 특정 지역에 대한 정보를 얻고자 할 때 최적의 라우팅 경로를 구성할 수 있게 한다. 싱크는 통신 가능한 이웃 노드 중 하나를 액세스 포인트 노드로 선택한다. 노드의 선택은 Marti 등이 제안한 감시기법(watchdog)과 경로등급기법(pathrater)을 이용하여 안전하게 한다.

싱크는 특정 소스로부터 데이터를 얻고자할 때 요청 프로토콜을 수행한다. 이를 위해 싱크는 소스까지 최적의 경로를 생성하여 요청 메시지를 그 경로상의 노드를 통해 전달한다. 요청 메시지를 전달하는 과정에서 다음과 같은 공격이 가능할 수 있다.

i) 싱크로 위장하여 요청 메시지를 보내 이웃 노드의 전력을 소모시키는 공격: 요청 메시지에 대한 인증 서비스를 제공하지 않거나 μ-TESLA처럼 서비스를 제공하더라도 확인 할 수 있는 키가 공표(publish)되기 전까지 시간지연이 발생하는 경우, 공격자가 요청 메시지를 이웃 노드들에게 계속해서 보내 노드의 전력을 고갈시켜 정상적인 서비스를 할 수 없도록 할 수 있다.

ii) 거짓 노드를 중간에 추가하여 불필요한 경로로 돌아가게 하는 공격: 라우팅 테이블이 보호되지 않는다면 공격자가 경로를 변경하여 싱크가 설정한 최적의 경로대신 불필요하게 다른 노드를 통해 돌아가게 하는 공격을 할 수 있다.

iii) 블랙 홀(black hole), 선택적인 전송(selective forwarding)과 같이 메시지를 전달하지 않는 공격: 경로상의 노드 행위에 대한 감시가 이루어지지 않는다면 공격자 노드는 싱크가 보낸 요청 메시지가 소스에게 제대로 전달되지 못하도록 할 수 있다.

iv) 네트워크 내의 센서 노드나 싱크의 위치 정보 획득 공격: 요청 메시지 내의 라우팅 정보를 이용하여 센서 노드의 위치를 파악하면 공격자는 센서 노드의 키를 획득하거나 물리적인 공격을 가할 수 있다.

이러한 공격을 막기 위해 다음과 같은 요청 프로토콜을 제안한다.

단계1: 싱크는 사전에 양방향 해쉬 체인을 만든다.

$$h(a_0) = a_1, h(a_1) = a_2, ..., h(a_{n-1}) = a_n$$
$$h(b_0) = b_1, h(b_1) = b_2, ..., h(b_{n-1}) = b_n$$

$a_0, a_1, ..., a_n$은 요청 메시지를 전달할 때 MAC의 키로 사용되며, $b_0, b_1, ..., b_n$은 응답 메시지를 전달할 때 MAC의 키로 사용된다.

단계2: 싱크는 경로상의 노드들에게 전달해야 하는 양방향 해쉬 체인 값, 메시지를 전달해 주어야하는 이웃노드, 타임스탬프(time stamp)를 해당노드의 비밀키로 암호화하여 액세스 포인트 AP_0에게 전달한다. 이때 메시지의 인증과 무결성을 보장하기위해 MAC값을 붙여 보낸다.

$$S \rightarrow AP_0 : AP_0, \{a_n, b_1, B, TS\}_{K_{AP}},$$
$$\{a_{n-1}, b_2, C, TS\}_{K_B},$$
$$..., \{a_1, b_n, ReqMsg, TS\}_{K_L},$$

$MAC_{K_{AP_0}}(\{a_n, b_1, B, TS\}_{K_{AP_0}},$
$\{a_{n-1}, b_2, C, TS\}_{K_B},$
$..., \{a_1, b_n, ReqMsg, TS\}_{K_E})$

암호화된 메시지는 인증을 위한 두 개의 해쉬 체인 값, 메시지를 전달하여야 하는 다음 노드, 재전송(reply) 공격을 막기 위한 타임스탬프로 구성되어 있다. 메시지가 비밀키로 암호화되어 있기 때문에 싱크가 보낸 메시지임을 확인할 수 있다.

단계3: AP_0는 자신의 메시지 부분을 해독하여 양방향 해쉬 체인 값, 전달해야 하는 이웃노드를 알아낸 후 다음 전달 노드에게 나머지 부분과 MAC값을 전송한다.

$AP_0 \rightarrow B: B, \{a_{n-1}, b_2, C, TS\}_{K_B},$
$\{a_{n-2}, b_3, D, TS\}_{K_C}, ..., \{a_1, b_n, ReqMsg, TS\}_{K_E},$
$MAC_{a_n}(\{a_{n-1}, b_2, C, TS\}_{K_B},$
$\{a_{n-2}, b_3, D, TS\}_{K_C}, ..., \{a_1, b_n, ReqMsg, TS\}_{K_E})$

단계4: 중간 노드들도 자신의 메시지 부분을 해독하고 해쉬 체인 값, 이웃 노드를 알아낸 후 나머지 부분과 MAC 값을 다음 노드에게 전달하여 소스까지 메시지가 전달되도록 한다.

$B \rightarrow C: C, \{a_{n-2}, b_3, D, TS\}_{K_C}, ...,$
$\{a_1, b_n, ReqMsg, TS\}_{K_E},$
$MAC_{a_{n-1}}(\{a_{n-2}, b_3, D, TS\}_{K_C}, ...,$
$\{a_1, b_n, ReqMsg, TS\}_{K_E})$
$\vdots$
$D \rightarrow E: E, \{a_1, b_n, ReqMsg, TS\}_{K_E},$
$MAC_{a_2}(\{a_1, b_n, ReqMsg, TS\}_{K_E})$

다음 노드에 메시지를 전달할 때 해쉬 체인 값을 MAC의 키로 사용하여 그 결과 값을 전달한다. 다음 노드는 데이터를 해독하여 해쉬 체인 값을 얻고 이전 노드가 보낸 MAC값을 확인하여 정당한 메시지인지 확인한다.

단계5: 소스는 비밀키로 메시지를 해독하여 해쉬 체인 값을 얻고 요청이 무엇인지 파악한다. 해독된 해쉬 체인 값으로 MAC값을 확인한다.

요청 프로토콜에서 공격자는 센서 노드와 싱크사이의 비밀키를 알지 못하므로 싱크로 위장하여 거짓 메시지를 보내 이웃 노드의 자원을 소모시키는 공격을 할 수 없다. 경로상에 있는 노드는 해쉬 체인으로 서로 연결되어 있어서 공격자는 중간에 거짓 노드를 추가할 수 없다. 각 노드는 MAC값을 통해 이전 노드가 보낸 메시지인지를 바로 확인할 수 있다. 공격자가 노드를 획득해도 이웃 노드만이 노출되기 때문에 네트워크의 토폴로지 정보를 얻기가 어렵다. 또한 싱크의 위치는 액세스 포인트 노드만 알기 때문에 물리적 공격의 가능성이 적다. 다만 싱크의 위치와 라우팅 경로를 숨기기 위해 각 노드마다 전달해야 하는 정보가 달라 요청 메시지의 양이 커졌다.

4.2 응답(response) 프로토콜

요청 메시지를 수신한 소스는 정보를 감지하고 수집(aggregate)하여 요청 메시지를 보냈던 이웃 노드에게 데이터를 전달한다. 중간 노드도 요청 메시지를 보냈던 이웃 노드에게 전송하여 AP_0까지 전달한다. 응답 메시지를 전달하는 과정 중에 다음과 같은 공격이 가능할 수 있다.

i) 소스로 위장하여 응답 메시지를 보내 이웃 노드의 전력을 소모시키는 공격: 공격자가 소스인 것처럼 위장하여 거짓 응답 메시지를 보내 이웃 노드의 전력을 소모시키거나 싱크에게 거짓된 정보가 전달되도록 할 수 있다.

ii) 데이터의 내용 또는 위치 정보를 획득하는 공격: 응답 메시지를 도청하거나 경로 정보를 획득하여 센서 또는 싱크의 위치를 파악할 수 있다.

iii) 중간 노드가 잘못된 경로로 데이터를 전송하게 하는 공격: 중간 노드가 라우팅 경로에 임의의 노드를 넣거나 변경하여 데이터를 잘못된 경로로 전송되도록 하는 공격을 할 수 있다.

iv) 중간 노드가 응답 메시지의 내용을 위변조하는 공격: 중간 노드가 응답 메시지의 내용을 변경하거나 다른 내용으로 바꾸어 싱크에게 전달할 수 있다.

이러한 공격을 방지하기 위해 다음과 같은 응답 프로토콜을 제안한다.

단계1: 소스는 감지된 내용과 타임스탬프를 비밀키로 암호화하고 인증과 무결성을 보장하기 위해 MAC값을 붙여서 보낸다. 이때 MAC의 키는 해쉬 체인 값을 사용한다.

$E \rightarrow D$: D, $\{ ResMsg, TS \}_{K_E}$,
$MAC_{h_n}(\{ ResMsg, TS \}_{K_E})$

단계2: 중간 노드들도 해쉬 체인 값을 키로 사용하여 MAC값을 붙여 보낸다.

$D \rightarrow C$: C, $\{ ResMsg, TS \}_{K_E}$,
$MAC_{h_{n-1}}(\{ ResMsg, TS \}_{K_E})$
$C \rightarrow B$: B, $\{ ResMsg, TS \}_{K_E}$,
$MAC_{h_{n-2}}(\{ ResMsg, TS \}_{K_E})$
⋮

단계3: AP_0도 해쉬 체인 값을 키로 사용하여 MAC값을 붙여 싱크에게 보낸다.

$AP_0 \rightarrow S$: S, $\{ ResMsg, TS \}_{K_E}$,
$MAC_{h_1}(\{ ResMsg, TS \}_{K_E})$

단계4: 싱크는 비밀키로 메시지를 해독하여 응답 내용을 얻고 해쉬 체인 값으로 MAC값을 확인한다.

제안된 응답 프로토콜은 해쉬 체인으로 노드가 연결되어 있기 때문에 거짓된 노드를 추가할 수 없다. 또한 메시지를 바로 인증할 수 있어 거짓 메시지를 보내 전력을 소모시키는 공격을 차단시킨다. 노드는 자신의 이웃 노드만을 알고 싱크의 위치는 액세스 포인트 노드만 알기 때문에 센서 노드 공격으로 노출되는 위치 정보를 감소시켰다. 감지된 내용은 비밀키로 암호화되어 싱크만 해독할 수 있고 MAC값을 통해 무결성을 보장한다.

4.3 이동 싱크 지원 프로토콜

요청 메시지를 보낸 후 응답 메시지가 오기 전에 싱크가 액세스 포인트 노드와 통신이 불가능한 위치로 이동하면 응답 메시지를 못 받을 수 있다. 싱크가 이동하여도 소스로부터 온 응답 메시지를 받기 위해 그림 1과 같이 새로운 AP_1을 설정한다.

새로운 AP_1을 설정하고 응답 메시지가 소스에서 이동 싱크에게 전달되는 방법은 다음과 같다.

단계1: 싱크가 AP_0와 통신할 수 없는 위치로 이동하면 AP_0에게 응답 메시지가 오면 대기하라는 명령을 전달한다.

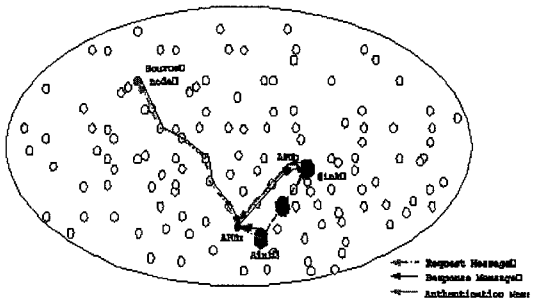


그림 1. 이동 싱크 지원 프로토콜

$S \rightarrow AP_0$: AP_0, $\{ Hold, TS \}_{K_{AP_0}}$,
$MAC_{K_{AP_0}}(Hold, TS)$

단계2: 새로운 AP_1을 선택하고 메시지 내용만 전송 명령으로 바꾸어 요청 프로토콜과 동일한 방법으로 AP_0에게 전달한다.

단계3: AP_0는 소스로부터 온 데이터를 중간 노드를 통해 응답 프로토콜과 동일한 방법으로 싱크까지 전달한다.

이동 싱크 지원 프로토콜은 근본적으로 요청-응답 프로토콜을 이용하기 때문에 앞에서 제시된 여러 공격을 차단시킨다. 해쉬 체인으로 노드가 연결되어 있기 때문에 거짓 노드를 추가할 수 없고 메시지를 즉시 인증할 수 있기 때문에 전력을 소모시키는 공격을 차단시켰다. 싱크와 센서 노드의 위치를 숨겨 이들에 대한 물리적 공격의 기회를 감소시켰다.

V. 이벤트 유도(Event-driven) 프로토콜

이 장에서는 센서 노드가 감지한 정보를 스스로 싱크에게 전달하는 이벤트 유도(event-driven) 프로토콜을 제안한다. 싱크가 고정되어 있으면 저장된 라우팅 경로를 이용하여 감지된 정보를 전송하면 되었다. 하지만 싱크가 이동하면 저장된 경로로 데이터를 전달할 수 없거나 경로를 추적하게 되면 그 길이가 길어지는 문제가 발생한다. 감지된 정보를 수신하기 위해 싱크의 위치를 전체 센서 네트워크에 알리는 방법은 자원의 소모가 많고 싱크의 위치가 공격자에게 쉽게 노출되는 문제점이 있다. SPIN[16]에서는 싱크의 위치를 노출시키지 않고 데이터를 전달할 수 있는 advertise-request-send 방식을 제안하였다. 이 방법은 센서 네트워크 내의 모든 노드를 싱크로 고려하여 모든 노드들에게 데이터를 전달하는 방

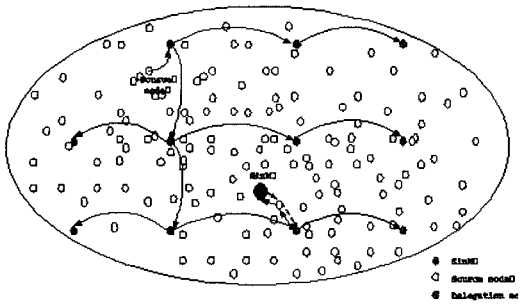


그림 2. 제안하는 이벤트 유도(event-driven) 프로토콜

법이다. 하지만 이 방법도 자원의 소비가 많은 문제점이 있다. 그래서 이 논문에서는 싱크의 위치를 숨기면서 자원의 소비를 줄일 수 있는 그림 2와 같은 방법을 제안한다.

제안하는 이벤트 유도 프로토콜은 센서 네트워크를 그리드(grid) 형태로 나누고 각 모서리마다 위임 노드(delegation node)를 지정한다. 센서 노드는 감지된 정보를 위임노드에게 전달하고 싱크는 위임 노드로부터 데이터를 전달받는 방법이다.

감지된 정보를 전달하기 위해 다음과 같은 이벤트 유도 프로토콜을 제안한다.

단계1: 싱크는 네트워크를 그리드 형태로 나누어 위임 노드를 선택하고 전체 네트워크에 알린다. 이때 위임 노드의 좌표를 알려주어 일반 노드가 자신의 가장 가까운 노드를 알 수 있도록 한다. K_{t0}는 μ-TESLA[12]에서 $t0$시간에 사용되는 인증키이다.

$$S \rightarrow *: DN_1, DN_2, ..., DN_n,$$
$$MAC_{K_{t0}}(DN_1, DN_2, ..., DN_n)$$

단계2: 싱크는 가장 가까운 위임 노드로부터 감지된 정보를 받기 위해 요청 프로토콜과 동일한 방법으로 위임 노드까지 메시지를 전달한다.

단계3: 이벤트가 발생하면 소스는 좌표 정보를 이용한 라우팅 프로토콜[17]을 이용하여 가장 가까운 위임 노드에게 전달하고 위임 노드는 다시 이웃한 위임 노드에게 전달하여 모든 위임 노드에게 전달되도록 한다.

$$E \rightarrow DN_{nearest}: \{SenMsg, TS\}_{K_E},$$
$$MAC_{K_E}(SenMsg, TS)$$
$$DN_{nearest} \rightarrow DNs: \{SenMsg, TS\}_{K_E},$$
$$MAC_{K_E}(SenMsg, TS)$$

전달되는 메시지는 소스의 비밀키로 암호화하고 MAC값을 붙여 기밀성과 무결성을 보장한다.

단계4: 싱크에서 가장 가까운 위임 노드는 응답 프로토콜과 동일한 방법으로 싱크까지 감지된 정보를 전달한다.

단계5: 싱크가 이동하여도 감지된 정보가 전달되도록 하기위해 이동 싱크 지원 프로토콜을 이용한다.

단계6: 싱크가 이동하여 가장 가까운 위임 노드가 바뀌면 새로운 위임 노드에게는 단계3의 등록 과정을 통해 데이터를 전달하고 이전의 위임 노드에게는 더 이상 데이터를 보내지 않도록 연결을 끊는다는 명령을 보낸다.

$$S \rightarrow DN_{old}: \{Disconnect, TS\}_{K_{DN_{old}}},$$
$$MAC_{K_{DN_{old}}}(Disconnect, TS)$$

제안된 이벤트 유도 방법은 싱크의 위치를 노출시키지 않으면서 자원을 절약할 수 있는 방법으로 앞에서 제안한 요청-응답 프로토콜을 사용하는 장점을 가지고 있다.

Ⅵ. 평가 및 분석

6.1 모의실험(Simulation)

모의실험을 위해 2000m×2000m의 크기에 200개의 센서 노드를 무작위로 설치하였다. 실험에 사용된 툴은 Visual C++로 가상의 필드에 200개의 노드를 랜덤하게 설치하고 C에서 제공하는 함수인 Rand() 함수를 이용하여 각각의 경우에 대해 100회의 시뮬레이션을 거쳐 이에 대한 평균값을 사용하였다. 그림 3에서는 제안한 요청-응답 프로토콜과 저장된 경로를 이용하는 프로토콜을 이용할 때 시간의 경과에 따른 통신량 변화를 비교하였다. 이 논문에서는 통신 비용의 척도로서 직접 통신 거리인 홉(hop)을 사용한다. 5m/초, 10m/초, 15m/초, 20m/초의 속도로 싱크가 이동하는 경우 저장된 라우팅 경로를 이용하는 방식은 시간이 지남에 따라 거쳐야하는 홉 수가 계속해서 증가하지만 제안한 요청-응답 프로토콜은 시간의 경과와 상관없이 거의 일정한 홉 수를 유지하고 있다. 그 이유는 저장된 경로를 이용하면 싱크가 이동함에 따라 거쳐야하는 노드의 수가 지속적으로 증가하기 때문에 시간이 지날수록 많은 홉을 거쳐 전달되지만, 제안된 요청-응답 프로토콜은 이동

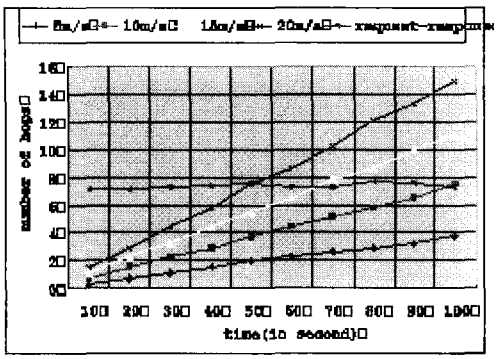


그림 3. 싱크의 이동 속도에 따른 통신횟수의 변화

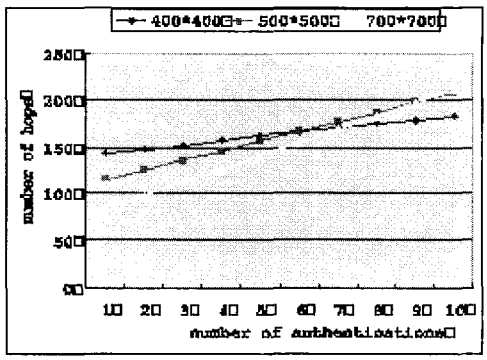


그림 4. 위임 노드간의 거리에 따른 통신횟수의 변화

속도나 시간의 경과에 상관없이 요청 메시지를 보낼 때마다 경로를 설정함으로 거의 일정한 홉 수로 싱크에게 데이터를 전달할 수 있기 때문이다. 시간이 경과하면 저장된 경로를 사용하는 방법보다 제안한 요청-응답 프로토콜이 효율적임을 보여준다.

제안한 이벤트 유도 프로토콜의 경우 위임 노드간의 거리에 따라 사용되는 자원의 양이 다르다. 그림 4는 그리드의 크기를 400m×400m, 500m×500m, 700m×700m로 하여 노드간의 거리에 따른 상대적인 통신비용을 실험한 결과이다. 위임 노드간의 거리가 멀수록 전달하여야 하는 위임 노드의 수가 적어지기 때문에 소스가 위임 노드에게 데이터를 전달하는 비용은 적게 든다. 하지만 싱크와 위임 노드사이의 거리도 멀어지기 때문에 싱크가 위임 노드에게 등록하기 위해 많은 노드를 거쳐야하므로 등록 횟수가 많아지면 거쳐야 하는 홉의 수가 많아짐을 보여준다.

6.2 비교 분석

요청 메시지는 각 센서 노드의 비밀키로 암호화되어 전달된다. 비밀키는 싱크와 해당 노드만이 알고 있어 거짓 메시지를 보내는 공격이 어렵다. 공격자가 어느 한 노드를 획득하더라고 하나의 키만 노출되고 이 키로 다른 노드를 공격할 수 없기 때문에 키 노출이 전체 네트워크에 미치는 영향이 적다. 공격자가 어느 하나의 노드를 획득하면 단지 그 이웃 노드만이 노출되므로 네트워크의 전체 토폴로지가 노출될 위험이 적다. 경로상에 있는 각 노드는 해쉬 체인 값으로 MAC값을 생성하여 전달하기 때문에 메시지를 수신한 노드는 그것이 정당한 메시지인지 바로 확인이 가능하여 거짓된 정보를 보내 이웃노드의 전력을 소비시키는 공격을 방지할 수 있다. 또한 공격자가 경로상의 노드를 획득하더라도 싱크의 위치를 알 수 없기 때문에 싱크에 대한 물리적 공격을 방지할 수 있다.

응답 메시지는 소스와 싱크의 비밀키로 암호화되고 MAC값이 같이 전송되기 때문에 기밀성과 무결성을 보장해줄 수 있다. 중간 노드도 해쉬 체인 값으로 MAC값을 생성하여 전달하므로 메시지에 대한 인증과 무결성을 확인할 수 있다. 이동 싱크에 대한 관리는 근본적으로 요청-응답 프로토콜을 이용하여 지속적으로 감지된 데이터를 안전하게 전달될 수 있도록 하였다.

이벤트 유도 프로토콜은 싱크의 위치를 노출시키지 않으면서 자원을 절약할 수 있는 방법으로 안전성이 검증된 요청-응답 프로토콜을 사용한다. 또한 일반 센서 노드가 브로드캐스트(broadcast)하는 것을 방지하여 이로 인한 공격의 범위와 가능성을 낮추었다.

표 1은 기존 시스템과 제안하는 시스템을 비교한 것이다. 제안하는 시스템은 이동 싱크의 특성을 고려하여 싱크의 위치추적 방지, 메시지에 대한 즉시 인증 기능을 제공한다. 기존의 시스템은 라우팅 경로를 설정하는 것에 초점을 두고 실제 데이터를 주고받는 순간에 경로의 변화에 대해서는 미흡하여 순간적으로 많은 변화가 있는 이동 싱크 환경에는 적합하지 않음을 보여준다.

Ⅶ. 결 론

센서 네트워크는 향후 많은 영역에서 사용될 것이며 안전한 라우팅 프로토콜에 대한 연구는 센서 네트워크의 사용 확대를 위해서 꼭 필요한 부분이다. 본 논문에서는 기존의 연구에서 미흡한 이동 싱크 환경에서 안전하게 데이터를 송수신할 수 있는 시스템을 제안하였다. 제안한 시스템은 싱크와 센서 노드의 위치가 노출되는 것을 최소화하고 양방향 해쉬 체인을

표 1. 제안하는 시스템과 기존 시스템의 비교

비교항목	Ariadne[15]	INSENS[4]	LU의 시스템[7,8]	제안하는 시스템
네트워크 환경	애드혹 네트워크	센서 네트워크	애드혹 네트워크	센서 네트워크
이동하는 싱크	고려하지 않음	고려하지 않음	이동하는 일반노드와 싱크를 동일하게 취급	이동하는 싱크의 특성을 고려
싱크 위치 추적 방지	위치 추적 가능	위치 추적 가능	위치 추적 가능	액세스 포인트 노드만 싱크 위치 파악 가능
메시지에 대한 인증	싱크 또는 소스에서만 인증 가능(지연이 발생)	싱크 또는 소스에서만 인증 가능(지연이 발생)	N/A	지연이 없는 인증이 가능

이용하여 메시지에 대해 바로 인증이 가능하다. 또한 이웃 노드의 전력 소모, 라우팅 경로 변경, 토폴로지 정보 획득 등의 공격을 차단시켜 데이터에 대한 안전성을 제공한다. 제안하는 시스템의 기술적인 특징으로는 요청-응답 프로토콜과 이벤트 유도 프로토콜이 하이브리드 형태로 존재하면서도 동일한 형태의 프로토콜을 사용하여 효율성을 추구하였다. 향후 과제로는 요청 메시지의 크기를 줄일 수 있는 방법과 여러 개의 싱크가 이동하거나 센서가 이동하는 환경에서 저비용의 안전한 라우팅 프로토콜에 관한 연구가 필요하다.

참 고 문 헌

[1] E. Howden, "Networked sensors for the objective force," In proceedings of SPIE 47th Annual Meeting, 2002.

[2] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, and D.E. Culler. "SPINS: Security Protocols for Sensor Networks," Wireless Networks Journal (WINET), vol. 8, no. 5, pp. 521-534, September 2002.

[3] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," First IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.

[4] J. Deng, R. Han, and S. Mishra, "INSENS: Intrusion-tolerant routing in wireless Sensor NetworkS," Technical Report CU CS-939-02, Department of Computer Science, University of Colorado, November 2002.

[5] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," In Proceedings of the Sixth annual ACM/IEEE International Conference on Mobile Computing and Networking, pp. 255-265, 2000.

[6] S. Tanachaiwiwat, P. Dave, R. Bhindwale, and A. Helmy, "Location-centric Isolation of Misbehavior and Trust Routing in Energy-constrained Sensor Networks," IEEE Workshop on Energy-Efficient Wireless Communications and Networks (EWCN), in conjunction with IEEE International Performance, Computing, and Communications Conference (IPCCC), April 2004.

[7] Y. Lu, W. Wang, and B. Bhargava, "Hierarchical Structure for Supporting Movable Base Stations in Wireless Networks," In Proceedings of IEEE International Conference on Telecommunication (ICT), Papeete, French Polynesia, Feb. 2003.

[8] Y. Lu, B. Bhargava, W. Wang, Y. Zhong, and X. Wu, "Secure Wireless Network with Movable Base Stations," In IEICE Transactions on Communications, IEICE/IEEE Joint Special Issue on Assurance Systems and Networks, Vol. E86-B, No. 10, pp. 2922-

2930, Oct. 2003.

[9] A. Gorlach, W. W. Terpstra, and A. Heinemann, "Survey on Location Privacy in Pervasive Computing," Proceedings of The First Workshop on Security and Privacy at the Conference on Pervasive Computing (SPPC), April 2004.

[10] S. Capkun, J. Hubaux, and M. Jakobsson, "Secure and Privacy-Preserving Communication in Hybrid Ad Hoc Networks," EPFL-IC Technical report IC/2004/10, Jan 2004

[11] J. Kong and X. Hong, "ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks," In Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing, pp291-302. ACM Press, 2003.

[12] S. Tilak , N. B. Abu-Ghazaleh , W. Heinzelman, "A taxonomy of wireless micro-sensor network models," ACM SIGMOBILE Mobile Computing and Communications Review, vol.6 no.2, pp. 28-36, April 2002.

[13] N. Bulusu, J. Heidemann, and D. Estrin, "GPS-less LowCost Outdoor Localization for Very Small Devices," IEEE Personal Communications Mag., Vol. 7, No. 5, pp. 28-34, Oct 2000.

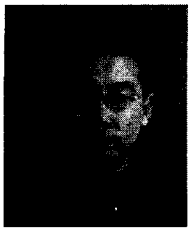
[14] J. Albowicz, A. Chen, and L. Zhang. "Recursive position estimation in sensor networks," In Proceedings of the International Conference on Network protocols (ICNP '01), pp. 35-41, November 2001. IEEE Computer Society.

[15] Y. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proceedings of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pp12-23, ACM, Atlanta, GA, September 2002.

[16] J. Kulik, W. R. Heinzelman, H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks," ACM Wireless Networks, vol. 8, no. 2-3, pp. 169-185, 2002.

[17] B. Karp, H. T. Kung, "GPSR: greedy perimeter stateless routing for wireless networks," Proceedings of the 6th annual international conference on Mobile computing and networking, p.243-254, August 06-11, 2000.

〈著者紹介〉



김 태 균 (Taekyun Kim) 학생회원
1996년 2월 : 부경대학교 전자공학과 졸업
1995년 12월~2000년 3월 : (주)현대전자 근무
2000년 3월~2003년 2월 : (주)안철수연구소 근무
2005년 2월 : 한양대학교 컴퓨터공학과(석사)
〈관심분야〉 센서네트워크 보안, 홈네트워크 보안

김 상 진 (Sangjin Kim) 종신회원
1995년 2월 : 한양대학교 전자계산학과(학사)
1997년 2월 : 한양대학교 전자계산학과(석사)
2002년 8월 : 한양대학교 전자계산학과(박사)
2003년 3월~현재 : 한국기술교육대학교 인터넷미디어공학부 조교수
〈관심분야〉 암호기술 응용
URL:http://infosec.kut.ac.kr/sangjin/

오 희 국 (Heekuck Oh) 종신회원
1983년 : 한양대학교 전자공학과(학사)
1989년 : 아이오와주립대학 전자계산학과(석사)
1992년 : 아이오와주립대학 전자계산학과(박사)
1993년~1994년 : 한국전자통신연구원 선임연구원
1995년 3월~현재 : 한양대학교 컴퓨터공학과 부교수
〈관심분야〉 암호프로토콜, 네트워크 보안
URL:http://infosec.hanyang.ac.kr/~hkoh/

이 익 섭 (Ik-Seob Lee)
2000년 2월 : 부경대학교 정보통신공학과 졸업
2002년 8월 : 부경대학교 정보통신공학과 석사
2002년 7월~현재 : 한국정보보호진흥원 근무
〈관심분야〉 정보보호, 홈네트워크, DWDM

유 동 영 (Dong-Young Yoo)
1997년 2월 : 숭실대학교 전자계산학과 졸업
2000년 2월 : 숭실대학교 컴퓨터학과 석사
2000년 12월~현재 : 한국정보보호진흥원 근무
〈관심분야〉 정보보호, 홈네트워크, 운영체제