情報保護學會論文誌
第17卷 第2號, 2007. 4

무선 센서 네트워크에서의 소스 위치 프라이버시

이 송 우,[1†] 박 영 훈,[1] 손 주 형,[1] 서 승 우,[1‡] 강 유,[2] 최 진 기,[2] 문 호 건[2]
[1]서울대학교 전기컴퓨터 공학부, [2]KT

Source-Location Privacy in Wireless Sensor Networks

Song-Woo Lee,[1†] Young-Hoon Park,[1] Ju-Hyung Son,[1] Seung-Woo Seo,[1‡]
Yu Kang,[2] Jin-Gi Choe,[2] Ho-Gun Moon[2]
[1]School of EECS at Seoul National University, [2]KT

요 약

본 논문에서는 센서 네트워크에서의 소스 위치 프라이버시를 제공하기 위한 방법을 제안하고 그 방법이 제공하는 익명성 정도를 분석하였다. 센서 네트워크에서의 소스 위치는 실제 센서의 지리적 위치이기 때문에 소스의 위치가 노출되지 않도록 보호하는 것이 매우 중요하다. 그러나 센서 네트워크에서는 내용 보호 및 인증에 관한 연구에 비해 소스 위치 프라이버시에 관한 연구는 아직 미흡하다. 더욱이 인터넷과 Ad-Hoc 네트워크에서 소스의 익명성을 제공하기 위한 기법들이 많이 제안되었지만, 이러한 기법들은 에너지 제한적인 센서 네트워크에 적합하지 않기 때문에 센서 네트워크의 특성에 맞는 익명성 제공 기법이 요구된다. 본 논문에서는 먼저 센서 네트워크에서 나타날 수 있는 Eavesdropper의 유형을 *Global Eavesdropper*와 *Compromising Eavesdropper*으로 정의하고, 이러한 Eavesdropper의 유형에 따라 소스의 익명성을 제공할 수 있는 새로운 기법을 제안하였다. 그리고 엔트로피 기반의 모델링 방법을 이용해 제안한 기법이 제공하는 익명성 정도를 분석하였다. 그 결과, 제안하는 기법을 사용할 경우가 그렇지 않은 경우 보다 소스의 익명성 정도가 높고, 센서의 전송 거리가 소스의 익명성 정도를 높이는데 중요한 요소임을 보였다.

ABSTRACT

This paper proposes a new scheme to provide the location privacy of sources in Wireless Sensor Networks (WSNs). Because the geographical location of a source sensor reveals contextual information on an 'event' in WSN, anonymizing the source location is an important issue. Despite abundant research efforts, however, about data confidentiality and authentication in WSN, privacy issues have not been researched well so far. Moreover, many schemes providing the anonymity of communication parties in Internet and Ad-hoc networks are not appropriate for WSN environments where sensors are very resource limited and messages are forwarded in a hop-by-hop manner through wireless channel. In this paper, we first categorize the type of eavesdroppers for WSN as Global Eavesdropper and Compromising Eavesdropper. Then we propose a novel scheme which provides the anonymity of a source according to the types of eavesdroppers. Furthermore, we analyze the degree of anonymity of WSN using the entropy-based modeling method. As a result, we show that the proposed scheme improves the degree of anonymity compared to a method without any provision of anonymity and also show that the transmission range plays a key role to hide the location of source sensors.

Keywords : *location privacy of source, Eavesdropper, anonymity of source, degree of anonymity, entropy*

Ⅰ. 서 론

저비용, 고성능의 센서 제작 기술의 발달로 주변 환경이나 중요 자산의 모니터링 등의 목적에 따라 다양한 센서 네트워크 애플리케이션이 널리 사용되고 있다. 이러한 센서 네트워크에서는 인터넷이나 애드 혹 네트워크에서와 같이 DoS 공격이나 정보 노출 등의 보안상 취약점을 갖고 있기 때문에 센서 네트워크에서도 보안상 취약점을 보완하기 위해 지금까지 많은 연구가 이루어져 왔다. 그러나 지금까지는 주로 암호화, 인증, 키 관리 등에 관한 연구가 주를 이루었고, 프라이버시에 대한 연구는 미흡한 편이다. 예를 들어 어떤 중요한 자산을 모니터링하는 경우, 센서의 모니터링을 통해 얻어진 정보는 제 3자에게 노출이 되어서는 안 되기 때문에 그 정보를 보호하기 위해 암호화와 같은 보안 장치를 사용할 것이다. 그러나 여기서 주목해야 할 것은 센서가 모니터링한 환경이나 자산 자체에 대한 정보, 즉 내용(Contents)도 중요할 수도 있지만, 그 정보를 전송한 소스의 위치(Source-location)가 더 중요할 수 있다는 것이다. 따라서 암호화를 통한 정보 보호 이외에 센서 네트워크의 특성에 맞는 소스 위치 노출 방지를 위한 추가적인 장치가 요구된다.

일반적으로, 인터넷과 같은 유선 네트워크에서는 송신자의 익명성을 보장하기 위해 여러 가지 방법이 제안되어 왔다. 첫 번째로 Chaum이 제안한 "Mix-net"[1]은 송신자의 익명성과 송신자와 수신자간의 비연결성을 제공해 주는 기법이다. Mix-net에서는 공개키 방식을 사용하는데, 송신자는 수신자의 ID와 중간에 있는 Mix 서버의 ID가 포함된 메시지를 각각의 공개키로 암호화하여 전송한다. 그러면 중간에 있는 Mix 서버는 자신의 비밀키로 메시지를 복호화 하여 다음 Mix 서버나 수신자에게 메시지를 전달하게 된다.

두 번째로 "Crowds"[2]는 AT&T에서 제안한 것으로 WWW 환경에서의 익명 통신을 위한 기법이다. 즉, 이 기술은 웹 서버에 접속하는 사용자의 익명성을 제공한다. Crowds에서는 사용자가 "Crowds"라는 익명의 사용자 그룹에 가입하게 되며, 사용자가 웹 서버에 접속하고자 할 경우 사용자가 보내는 "Request"는 그룹 내 멤버들 간의 무작위 경로를 통해 웹 서버에 전달된다.

에드 혹 네트워크에서는 [5][6]과 같이 익명 라우팅 기법들이 많이 제안되었다. 이러한 기법들은 무선 환경에서의 소스 위치 프라이버시 문제를 다루기는 했지만, Mix-net에서 사용한 방식과 유사하다. 즉, 연산 오버헤드가 많은 공개키 방식을 사용하기 때문에 이러한 기법들을 에너지 제한적인 센서 네트워크에 그대로 적용하기는 어렵다.

센서 네트워크에서도 소스 위치 프라이버시를 제공하기 위한 기법이 제안되었는데, 그 중 하나가 "Phantom Routing"[7]이다. 이 기법은 공격자는 싱크의 위치를 알고 있고 센서가 전송한 신호를 이용하여 그 센서의 위치를 추적할 수 있다고 가정하고, 소스가 싱크에게 메시지를 전송할 때 공격자가 소스의 위치를 추적하기 어렵게 하는 라우팅 기법으로 Random single-path routing과 Flooding (or Single-path routing) 방법을 혼합한 라우팅 기법이다. 이 기법은 무선 환경의 특성과 에너지 제한적인 센서 네트워크의 특성을 고려하였지만 몇 가지 단점이 있다. 첫째, 소스 위치 프라이버시 제공을 위해 메시지를 보낼 때 마다 라우팅 경로를 길게 하고 랜덤하게 변경함으로써 메시지 전달 시간이 많이 지연된다. 둘째, 싱크에 위치한 공격자가 싱크로 들어오는 신호를 이용하여 한 홉씩 단계적으로 소스의 위치를 추적하는 유형의 공격자만을 고려하였다.

본 논문에서는 센서 네트워크의 특성을 고려한 새로운 소스 익명성 제공 기법을 제시하였다. 제안한 기법은 일반적인 네트워크에서 제안된 기존의 기법들에 비해 비교적 간단하고, 익명성을 제공하기 위해 오버헤드가 많은 암호화 방식을 사용하지 않았기 때문에 센서 네트워크에 적합하다. [7]과 비교했을 때, 제안한 기법은 약간의 MAC 연산 오버헤드가 있긴 하지만 메시지 전달의 지연이 거의 발생하지 않는다. 그리고 [7]은 (경로 늘이기/ 변경하기 등) 기존 라우팅 알고리듬의 수정이 필요한 반면, 제안한 기법은 수정 없이도 기존의 어떤 라우팅 기법에도 적용할 수 있다. 또한 [7]에서는 하나의 공격자 유형만을 고려하여 분석하였지만, 본 논문에서는 공격자의 유형을 *Global Eavesdropper*와 *Compromising Eavesdropper*로 나누어 분석하였다. 제안한 기법은 소스의 ID를 숨기기 위해 소스의 ID를 사용하지 않고, 위장 ID와 MAC을 사용한다. 그리고 전송된 신호에 의해 소스 위치가 노출될 수 있는 무선 환경의 특성을 고려하여 소스 위치를 불명확하게 하기 위해

접수일: 2006년 10월 17일; 채택일: 2007년 1월 2일
* 본 연구는 (주)KT 및 ITRC 지원으로 수행하였습니다.
† 주저자, kma55@snu.ac.kr
‡ 교신저자, sseo@snu.ac.kr

동적인 전송 power 조절 방법을 사용한다. 또한, 수학적 분석을 통해 제안하는 기법이 제공하는 익명성 정도(Degree of Anonymity)를 정량화였고, 제안하는 기법을 사용할 경우 익명성 제공 기법을 사용하지 않았을 때보다 높은 익명성 정도를 제공함을 보였다.

본 논문의 다음과 같이 구성되어 있다. 2장에서는 네트워크 모델, 보안 가정, Eavesdropper 유형의 정의를 포함해 문제에 대한 정의를 설명하고, 3장에서는 센서 네트워크에서의 소스 익명성을 제공하기 위한 기법을 제안한다. 4장에서는 Eavesdropper의 유형에 따라 제안한 기법이 제공하는 소스 익명성 정도를 분석하고, 마지막으로 5장에서는 본 논문의 결론을 맺는다.

Ⅱ. 문제 정의

2.1 네트워크 모델

이 절에서는 본 논문에서 고려한 네트워크 모델에 대해 설명한다. 센서 네트워크는 수많은 동일한 센서로 이루어져 있고, 각 센서들은 고유의 ID를 갖고 있으며 에너지, 메모리, 연산 능력이 제한적이다. 〔그림 1〕과 같이 센서는 랜덤하게 뿌려지고, 센서는 전송 power를 동적으로 조절할 수 있다고 가정하였다. 또한 센서는 전송 거리 내에 있는 다른 센서들과 통신이 가능하고, 센싱 거리 내에 존재하는 신호를 감지할 수 있다. 이때 센싱 거리는 전송 거리 보다 p_s배 길다.

이 논문에서는 라우팅 기법을 다루지 않기 때문에 무선 센서 네트워크에서 제안되었던 많은 라우팅 기법들 중 (예, Flat Routing, Hierarchical Routing, Flooding, Single path Routing 등) Single-path Routing 기법을 (예, Directed diffusion[8], GBR[9], SPIN-PP[10]) 사용한다고 가정하였다.

2.2 보안가정

우리가 가정하고 있는 센서 네트워크는 end-to-end로 데이터의 기밀성과 신뢰성을 제공하고, 각 데이터를 익명의 형태로 한 홉씩 전달한다. 이를 위해, 모든 센서는 두 가지 종류의 보안키를 갖게 된다. 첫 번째 키는 싱크와 센서 i가 공유하고 있는 대칭키로써, 센서 i가 싱크에게 데이터를 보낼 때 이 키를 이용하여 암호화한다. 따라서 중간에 있는 센서들은 이 데이터를 복호화 할 수 없기 때문에 이 데이터는 노출되지 않는다.

두 번째 키는 센서 i와 그 이웃 센서들과 공유하고 있는 대칭키로써, 이 키를 이용하여 MAC를 생성할 수 있다[11]. 따라서 이 MAC를 통해 데이터의 신뢰성을 제공할 수 있을 뿐만 아니라 데이터 프레임에서 소스의 ID를 생략하더라도 수신하는 센서는 소스를 확인할 수 있다. 이에 대한 자세한 과정은 다음 장에서 설명한다.

또한 효율적으로 대칭키를 공유하기 위해 다음 몇 가지 방법들을 사용한다고 가정하였다. 싱크와 센서 간에 공유될 키는 센서를 배치하기 전에 미리 공유키를 저장하는 'key pre-deployment' 방법을 사용한다. 이 방법은 센서가 뿌려지기 전에 싱크가 n개의 랜덤한 키를 생성해서 각 센서에 분배하는 방법이다. 각 센서가 그 이웃 센서들과 키를 공유하기 위해서는 〔12〕〔13〕〔14〕와 같은 'pair-wise key establishment' 방법을 사용한다.

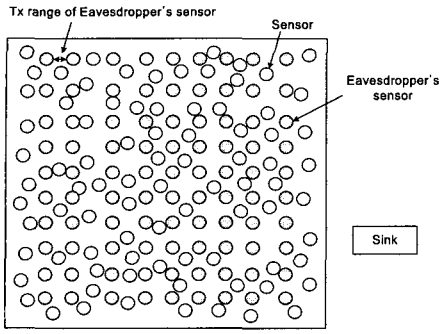
마지막으로 각 센서가 그 이웃을 확인하고 ID를 교환하는 과정과 싱크와 이웃들 간의 공유키를 교환하는 과정이 안전하게 이루어진다고 가정하였다.

2.3 Eavesdropper 유형

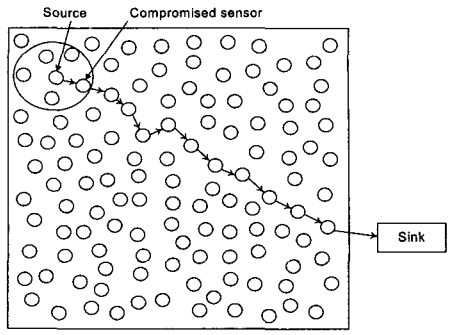
본 논문에서 정의하는 Eavesdropper는 데이터 자체보다는 데이터를 보낸 소스의 위치를 알아내려고 하는 공격자의 유형이다. Eavesdropper는 그가 침입한 사실이 발견되지 않도록 데이터를 조작하거나 데이터 전송을 방해하는 등의 악의적인 행동은 하지 않고, 전달되는 트래픽 데이터를 엿듣는 수동적 행동만 한다고 가정한다. 또한 Eavesdropper의 Resource가 충분하며 센서의 위치와 ID를 알고 있다고 가정하였다. 이 절에서는 센서 네트워크에서 소스 위치 프라이버시를 위협할 수 있는 두 가지 유형의 Eavesdropper에 대해 정의하였다. 첫 번째 유형은 네트워크 지역 내에서 발생하는 모든 신호를 감지할 수 있고, 그 신호를 이용하여 소스의 위치를 찾을 수 있는 *Global Eavesdropper*이다. 두 번째 유형은 네트워크 지역에 뿌려진 센서 중 일부 센서를 compromise하고 그 센서들을 이용하여 소스의 위치를 찾을 수 있는 *Compromising Eavesdropper*이다.

2.3.1 Global Eavesdropper

이 Eavesdropper는 네트워크 지역에서 발생하는 모든 신호를 감지하기 위해 네트워크 지역에 자신의 센서



〔그림 1 (a)〕 Global Eavesdropper



〔그림 1 (b)〕 compromising Eavesdropper

를 설치한다. 그리고 Eavesdropper는 자신이 배치한 센서에 의해 감지된 신호를 종합하여 최초의 신호 발생 위치와 전송 경로를 파악할 수 있다. 그러나 전송되는 데이터의 내용은 알 수 없다. Eavesdropper는 네트워크 전 지역의 모니터링이 가능하고, 최소한의 센서로 소스를 찾기 위해 그림 1과 같이 센서를 균일하게 배치한다고 가정하였다. 또한 Eavesdropper의 센서의 전송 및 센싱 거리는 일반 센서의 것과 동일하다고 가정하였다.

2.3.2 Compromising Eavesdropper

이 Eavesdropper는 네트워크 지역에 뿌려진 센서 중의 일부 센서를 compromise할 수 있다. 센서가 compromise되면 그 센서가 갖고 있는 2개의 pair-wise 키와 ID 정보가 노출되기 때문에 Eavesdropper는 compromise된 센서들이 수신하는 데이터를 통해서 소스의 위치를 알아낼 수 있다. 단, compromise된 센서가 전송 경로 상에 있으면서 소스와 이웃해 있을 때만 위치를 알아낼 수 있다. 그 센서가 전송 경로 상에 있지 않고 이웃하기만 한 경우에는 Eavesdropper는 소스가 갖고 있는 키와 동일한 pair-wise 키가 없어 소스의 ID를 알 수 없기 때문에 소스의 위치를 파악할 수 없다. 그 이유에 대해서는 다음 장에서 설명한다.

Ⅲ. 소스 익명성 제공 기법

이 장에서는 소스의 익명성을 제공하기 위한 기법에 대해 제안한다. 제안하는 기법은 다음 3 가지의 방법으로 구성되어 있다.

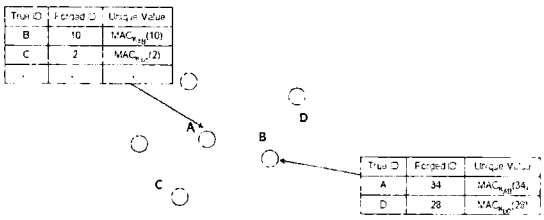
1) 위장 ID (Forged ID) 사용 (공통)
2) 데이터 프레임 수정 (Source ID 생략/ MAC 및 Unique value 사용) (공통)
3) 동적인 전송 power level 조절 (유형에 종속적)

1)과 2)는 Eavesdropper가 소스의 ID를 알아내는 등의 간단한 트래픽 분석만을 통해서 소스의 위치를 찾아내기 어렵도록하기 위한 방법이고, 3)은 Eavesdropper의 유형에 따라 동적으로 전송 power 레벨을 조절함으로써 Eavesdropper에게 혼란을 주기위한 방법이다.

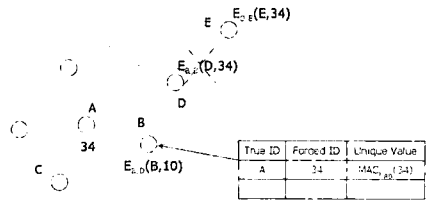
3.1 위장 ID (Forged ID) 사용

먼저 소스의 익명성 보장을 위해서 위장 ID를 사용한다. 위장 ID를 사용함으로써 Eavesdropper는 위장 ID를 아는 것만으로는 소스의 위치를 알 수 없다. 이러한 위장 ID는 각 센서에 의해 생성되며, 위장 ID가 생성되고 이웃 센서들 간에 교환되는 과정은 다음과 같다.

1) 최초 센서가 뿌려진 후, 각 센서는 특정 범위 [0, x] 내에서 임의의 숫자를 선택하여 그 숫자를 위장 ID로 사용한다.
2) 이웃 discovery 과정에서 이웃 센서들 간에 true ID와 위장 ID를 교환한다. 이때 ID들은 그들이 공유하고 있는 pair-wise 키로 암호화 된다.
3) 각 센서는 이웃 센서들과의 ID 교환 후 상대 센서의 위장 ID를 그 센서와 공유하고 있는 pair-wise 키로 MAC 연산하여 둘 만의 Unique value를 생성한다.
4) 각 센서는 ID 정보 및 Unique value를 〔그림 2〕와 같이 맵핑 테이블에 저장 / 유지한다.
5) 실제 ID/ 위장 ID 정보 교환 시 각 센서는 유지하고 있는 맵핑 테이블을 체크한다.
6) 만약 ID 정보 교환 시 맵핑 테이블을 체크하여 동일한 위장 ID 및 Unique value가 있으면 동일한



〔그림 2〕 True / Forged ID 교환



〔그림 3〕 위장 ID 교환 시 맵핑 테이블 검색

위장 ID를 보내온 센서에게 다른 위장 ID를 선택하도록 한 후 새로운 위장 ID를 다시 교환한다.

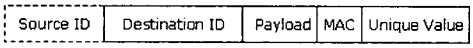
7) 위장 ID는 주기적으로 갱신된다.

예를 들어, 센서 A와 B가 이미 위장 ID를 교환하였다고 가정하자. 센서 D가 B에게 위장 ID로 센서 A와 동일한 '34'를 사용하겠다고 B에게 보내게 되면 B는 D에게 다른 위장 ID를 선택하도록 한 후 새로운 위장 ID를 교환하게 된다. 왜냐하면 B의 맵핑 테이블에는 이미 '34'라는 ID를 사용하는 센서 A가 있기 때문이다. 이러한 과정을 통해서 어느 한 센서를 기준으로 두 홉 이내의 이웃들은 동일한 위장 ID를 사용하지 않게 된다. 그러나 〔그림 3〕과 같이 그 이상의 홉에서는 동일한 위장 ID를 사용하는 센서가 있을 수 있다.

3.2 데이터 프레임 수정

이 절에서는 소스의 ID를 숨기기 위한 방법으로 데이터 프레임 수정을 제안한다. 그림 4(b)와 같이 데이터 전송 시 ID 필드에서는 Source ID를 생략하고 Destination ID만을 사용하고, CRC는 MAC (Message Authentication Code)으로 대체한다. 또한 통신하고 있는 이웃 센서만이 알고 있는 Unique value를 추가한다. 특히, Unique value는 Destination 센서만이 소스를 식별할 수 있게 하는 것으로 이를 통해서 Destination 센서는 일차적으로 소스를 신속하게 식별할 수 있게 된다.

〔그림 4 (a)〕 Original 데이터 프레임



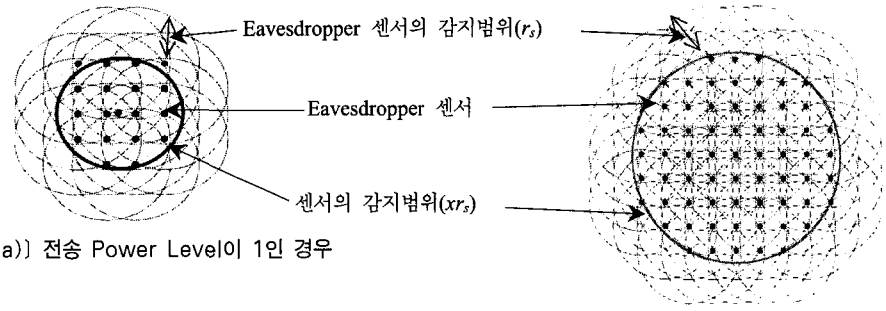
〔그림 4 (b)〕 수정된 데이터 프레임

데이터 전송 시 Source ID를 생략함으로써 Destination 센서만이 누가 소스인지 알 수 있게 되는데, 그 이유는 MAC을 확인하기 위해서는 소스와 동일한 키를 가지고 있어야 하기 때문이다. 즉, MAC 확인이 가능하다는 것은 누가 보낸 데이터인가를 알 수 있다는 것을 의미한다. 그리고 나머지 이웃 센서들은 소스가 누구인지를 알 수 없을 뿐만 아니라 Destination이 누구인지도 유추하기 어렵다. 따라서 위장 ID를 사용하고 〔그림 4〕와 같이 데이터 프레임을 수정함으로써 Eavesdropper가 소스를 찾아내는데 혼란을 줄 수 있다. 그러나 추가적인 MAC 연산 때문에 에너지 소모가 많을 것이라고 생각할 수 있다. 그렇지만 MAC 연산으로 인한 센서의 에너지 소모는 무시할 만하며, 이에 대해서는 4장에서 자세히 설명한다.

예를 들어, 〔그림 3〕에서 센서 A가 센서 B에게 데이터를 보낸다고 가정하자. 센서 A는 데이터 프레임에서 Source ID를 생략하고, 센서 B와 있는 pair-wise키로 MAC를 생성하여 데이터 프레임에 추가하여 데이터를 보낸다. 이 경우 센서 C도 이 데이터를 들을 수 있지만, 센서 C는 센서 A와 B가 공유하고 있는 pair-wise키를 가지고 있지 않기 때문에 소스가 센서 A인지 알 수가 없다. 따라서 통신을 하고 있는 센서 외 다른 센서들은 물론 Eavesdropper도 소스를 알아낼 수 없는 것이다. 그러나 Destination ID를 위장 ID가 아닌 true ID를 사용한다면 센서 B의 위치를 통해서 좀 더 쉽게 소스의 위치를 찾아낼 수 있을 것이다.

3.3 동적인 전송 Power 레벨 조절

이 절에서는 Eavesdropper의 유형에 따라 어떻게 전송 power 레벨을 조절해야 하는 지를 설명한다. Eavesdropper의 유형에 따라 전송 power level을 동적으로 조절함으로써 데이터 전송 시 소스의 익명성 정도를 높일 수 있다.



〔그림 5 (a)〕 전송 Power Level이 1인 경우

〔그림 5 (b)〕 전송 Power Level이 2인 경우

3.3.1 Global Eavesdropper의 경우

이 경우에는 소스의 전송 power 레벨을 어떻게 높이느냐가 중요하다. 즉, 소스가 첫 번째 홉에 위치한 이웃 센서에게 데이터를 전송할 때 전송 power 레벨을 높여야 한다. 그렇게 함으로써 〔그림 5 (b)〕와 같이 더 많은 수의 Eavesdropper 센서가 신호를 감지하도록 해 Eavesdropper가 소스의 위치를 유추하기 어렵게 할 수 있다. 다시 말해 Eavesdropper가 유추할 수 있는 지역의 범위를 넓게 함으로써 Eavesdropper가 소스라고 예측할 수 있는 센서의 수가 증가되어 소스의 익명성 정도를 높일 수 있게 되는 것이다. 하지만 전송 power 레벨을 높이는 것은 센서의 빠른 전력 소모를 유발하기 때문에 최적의 전송 power 레벨을 결정하는 것이 매우 중요하다.

3.3.2 Compromising Eavesdropper의 경우

이 경우에는 소스로부터 싱크까지의 평균 경로 길이에 따라 익명성의 정도가 결정 된다. 다시 말해, 평균 경로 길이가 길어질수록 소스의 익명성 정도가 높아지게 되므로 센서의 전송 power 레벨을 낮추는 것이 중요하다. 센서의 전송 power 레벨을 낮춤으로써, 즉 센서의 전송 거리를 짧게 하여 평균 경로 길이를 길게 함으로써 소스의 익명성 정도를 높일 수 있다. 평균 경로 길이를 늘임으로써 익명성의 정도가 높아지는 이유에 대해서는 다음 장에서 확인할 수 있다.

Ⅳ. 익명성 정도 분석

이 장에서는 제안한 기법의 성능에 대해 분석하였다. 성능 분석을 위해 성능을 익명성 정도 (Degree of Anonymity)로 정량화하였고, 제안한 기법이 소스 위치 프라이버시를 위한 어떠한 기법도 사용하지 않았을 때보다 높은 익명성 정도를 제공함을 보였다. 익명성 정도를 정량화하기 위해 〔3〕에서와 같이 엔트로피 관계식을 이용하였다.

$$H_X = -\sum_{k=1}^{n} p_k \log_2 p_k$$

p_k는 소스가 데이터를 전송하는 이벤트가 발생했을 때 Eavesdropper가 판단하기에 k번 째 센서가 소스일 확률을 의미하고, $\sum_{k=1}^{n} p_k = 1$이다. 엔트로피의 정의에 의해 익명성 정도는 다음과 같이 정의한다.

$$D(x) = \frac{H_X}{H_M}$$

H_M은 최대 엔트로피 값이며 위의 정의에 의해 $0 \le D(x) \le 1$임을 알 수 있다.

만약 Eavesdropper가 전체 센서 중에 누가 소스인지 전혀 알 수 없을 경우 즉, 모든 센서가 소스일 확률이 동일할 경우 엔트로피 값이 최대가 되며 또한 익명성 정도가 가장 높다고 할 수 있다.

4.1 Global Eavesdropper

Global Eavesdropper의 경우 최대 엔트로피 값 H_M은 식 (1)과 같다. H_M은 모든 센서가 소스일 확률이 동일한 경우의 엔트로피 값이며, 네트워크 지역 내에 신호가 없는 경우 Eavesdropper는 모든 센서를 잠정적인 소스로 생각하게 되므로 그 때의 엔트로피 값이 최대가 된다.

$$H_M = -\sum_{k=1}^{n} \frac{1}{n} log_2 \frac{1}{n} = \log_2 n \qquad (1)$$

〔표 1〕 분석 파라미터

Parameter	Definition
n	total number of sensors
r_0	initial transmission range
x	transmission power level
r	transmission range ($=xr_0$)
p_s	factor of sensing range (p_s=2.2 for IEEE 802.11)
r_s	sensing range ($=p_s r$)
$A(x)$	total area that Eavesdropper's sensor can observe
e	density of sensors (n/total network area)
c	number of compromised sensors
L	average path length between senor and sink, when tx range of sensor is r

H_X는 이벤트가 발생한 이후의 엔트로피 값으로 소스에 의해 신호가 발생한 이후에는 식 (2)와 같이 엔트로피 값이 변화한다.

$$H_X = -\sum_{k=1}^{\rho A(x)} \frac{1}{\rho A(x)} log_2 \frac{1}{\rho A(x)} = \log_2 \rho A(x) \quad (2)$$

왜냐하면 데이터를 전송하게 되면 Eavesdropper의 센서가 그 신호를 감지하여 소스의 위치를 유추할 수 있는 지역의 범위가 변화하기 때문이다. 즉, 신호를 감지한 Eavesdropper의 센서가 감지할 수 있는 범위 내에 있는 센서가 소스일 확률이 더 높아지게 되고, 그 외의 지역에 있는 센서는 소스일 확률은 '0'이 되는 것이다. 그리고 제안한 기법을 사용함으로써 Eavesdropper 센서의 감지 범위 내에 있는 센서들이 소스일 확률은 모두 동일하게 된다.

Eavesdropper의 센서에 의해 감지된 범위 내에 있는 각각의 센서가 소스일 확률에 대해 생각해 보자. Eavesdropper는 센서의 위장 ID를 알지 못하기 때문에, 신호를 감지한 것만으로 소스의 정확한 위치를 찾아낼 수 없다. 그러나 Eavesdropper는 소스가 있다고 생각할 수 있는 범위는 좁힐 수 있다. 따라서 감지된 범위 내에 있는 각각의 센서가 소스일 확률이 '$1/e\,A(x)$' 으로 동일하다고 말할 수 있다. 즉, Eavesdropper는 감지 범위 내에 있는 센서 중에 하나가 소스일 것이라 판단하게 된다. 〔그림 5〕에서와 같이 신호가 발생된 이후 초기의 최대 엔트로피 값과 변화된 엔트로피 값의 비율로 익명성 정도 $D(x)$를 구할 수 있다. 그리고 Eavesdropper의 센서가 감지한 범위의 면적 $A(x)$는 다음과 같이 근사하여 구할 수 있다.

$$A(x) \approx \pi(xr_s + r_s)^2$$

따라서 다음과 같이 익명성 정도 $D(x)$를 얻을 수 있다.

$$D(x) = \frac{\log_2(\rho A(x))}{\log_2 n} = \frac{\log_2(\rho\pi(xr_s + r_s)^2)}{\log_2 n} \quad (3)$$

식 (3)에서 보듯이 소스의 익명성 정도는 전송 거리 r이 증가할수록 커짐을 알 수 있다.

4.1.1 최적의 전송 거리 결정

전송 거리 r을 증가시키면 익명성 정도도 높아지지만, 3장에서도 언급했듯이 전송 거리 r이 증가하게 되면 센서의 전력 소모량도 증가하기 때문에 최적의 r을 결정하는 것이 중요하다. 이러한 문제를 해결하기 위해 최적의 전송 거리를 구하기 위한 식을 아래와 같이 정의했다. 이득은 익명성 정도에 비례하고 손실(전력소모)은 전송 거리의 제곱에 비례한다고 가정하였다. $B(x)$는 전송 거리 증가로 인한 손실과 익명성 정도의 증가로 인한 이득과의 차(net benefit)를 의미한다.

$$B(x) = \alpha D(x) - \beta(r_0 x)^2 = \alpha \frac{\log_2(\rho\pi(xr_s + r_s)^2)}{\log_2 n} - \beta(r_0 x)^2$$

B(x)의 최대값을 얻기 위해서는 $\frac{d}{dx}B(x) = 0$을 만족하는 x를 구하면 된다.

$$\frac{d}{dx}B(x) = \frac{d}{dx}\left(\alpha \frac{\ln(\rho\pi(p_s r_0 x)^2(x+1)^2}{\ln n} - \beta(r_0 x)^2\right) = \frac{2\alpha}{\ln n}\left(\frac{1}{x} + \frac{1}{x+1}\right) - 2\beta r_0^2 x$$

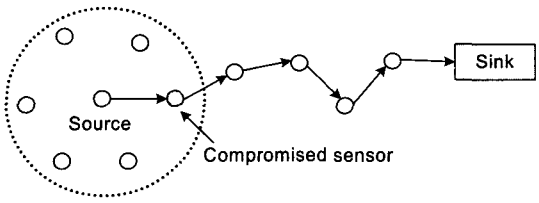
$\frac{d}{dx}B(x) = 0$로 놓으면, 다음과 같이 얻을 수 있다.

$$\frac{2x+1}{x(x+1)} = Cx, \quad where\ C = \frac{\beta r_0^2 \ln n}{\alpha}$$

위의 식을 정리하면 식 (4)와 같다.

$$Cx^3 + Cx^2 - 2x - 1 = 0 \quad (4)$$

식 (4)로부터 3 개의 근을 구할 수 있는데, 그 근이 모



〔그림 6〕 경로 상에 있으면서 소스의 바로 이웃한 센서가 compromise된 경우

두 실근인 경우와 2 개의 실근과 1 개의 허근인 경우로 나누어 볼 수 있다. 첫 번째의 경우에는 세 근의 합은 -1 이고 그 곱은 $\frac{1}{C}$이다. 이것은 세 개의 근이 하나의 양의 근과 두 개의 음의 근이라는 것을 의미한다. 두 번째의 경우, 식 (4)를 인수분해하면 $C(x^2+ux+v)(x-w)=0$이 되며 이때, u, v, w는 양의 상수이다. 이 경우에는 양의 근이 한 개만 존재하게 된다. 위의 두 가지 경우에서 보듯이, 어떠한 경우라도 식 (4)로부터는 양의 근 한 개만을 얻을 수 있다. 따라서 에너지 소모를 최소화하면서 익명성 정도를 높일 수 있는 최적의 전송 거리 r은 식 (4)를 이용하여 구할 수 있다.

4.2 Compromising Eavesdropper

전체 센서 중 c개가 Eavesdropper에 의해 compromise 되었다고 가정하자. 그러면 Eavesdropper는 자신이 *compromise*한 센서는 Anonymity set에서 배제시킬 수 있어 그 때의 최대 엔트로피 값은 식 (5)과 같이 구할 수 있다.

$$H_M=-\sum_{k=1}^{n-c}\frac{1}{n-c}log_2\frac{1}{n-c}=\log_2(n-c) \tag{5}$$

P_i를 Eavesdropper에 의해 결정되는 sensor i가 소스일 확률이라 하자. 그리고 편의를 위해 compromise된 센서들은 1부터 c까지로, 정상 센서는 $c+1$부터 n까지라고 가정한다. Eavesdropper는 $1\le i\le c$인 센서들에게는 확률 P_i를 '0'으로 놓을 것이다. 왜냐하면 compromise된 센서는 소스가 아닌 것이 확실하기 때문이다. 하지만 정상 센서들에게는 '0'이 아닌 확률값을 부여할 것이다. 〔그림 6〕과 같은 경우 Eavesdropper는 소스의 위 치를 알 수 있다. 따라서 Eavesdropper는 신호를 감지한 compromise된 센서의 바로 옆에 있는 이웃 중 하나의 센서에게는 높은 확률값을 부여할 것이다. 그 센서를 $c+1$이라고 하면 그 확률값 P_{c+1}은

$$p_{c+1}=\frac{c/(n-1)}{1-\prod_{x=1}^{L-1}(1-\frac{c}{n-x})}$$

와 같이 구할 수 있다. 이것은 compromise된 센서가 경로 상에 하나 이상 존재하면서 그 센서가 소스에 바로 이웃할 확률을 의미한다.

최종적으로, Eavesdropper는 나머지 정상 센서들에 대한 정보는 알 수 없기 때문에 그 센서들에게는 식 (6)과 같이 모두 동일한 확률값을 부여할 것이다.

$$p_i=\frac{1-p_{c+1}}{n-c-1},\quad c+1<i\le n \tag{6}$$

따라서 Eavesdropper가 일부 센서들을 compromise하고 소스가 신호를 보낸 이후 네트워크의 엔트로피를 구하면 식 (7)과 같다.

$$H_X=p_{c+1}\log_2(p_{c+1})+(1-p_{c+1})\log_2\left[\frac{n-c-1}{1-p_{c+1}}\right] \tag{7}$$

식 (5)와 (7)을 통해서 소스의 익명성 정도를 구할 수 있다.

4.2.1 최적의 전송 거리 결정

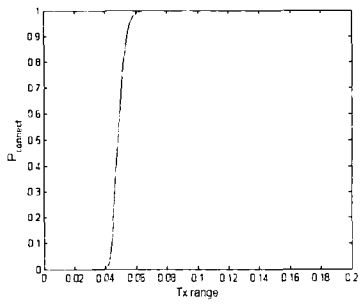
Compromising Eavesdropper의 경우 식 (7)에서 보듯이 소스의 익명성 정도는 전송 거리 r을 감소시켜 평균 경로 길이를 길게 하면 높아짐을 알 수 있다. 하지만 소스의 익명성 정도를 높이기 위해 센서의 전송 거리를 계속 줄여 threshold값 이하로 내려가게 되면 〔그림 7〕과 같이 네트워크의 연결이 급격하게 끊어질 수 있다. 따라서 네트워크의 연결성을 고려하여 최적의 r을 결정하는 것이 중요하다. 즉, 네트워크의 연결성을 보장하면서 최대의 익명성 정도를 얻을 수 있는 센서의 전송 거리 r을 결정해야 한다. 이를 위해 센서의 전송 거리 r에 따른 평균 경로 길이 및 네트워크의 연결성 변화와 식 (5)와 (7)을 통해 구한 소스의 익명성 정도를 함께 고려하여 최적의 전송 거리 r을 결정할 수 있다.

$$\begin{aligned}P_c&=\Pr(networks\ is\ connected)\\&=\lim_{N\to\infty}\Pr(N\pi r^2-\ln N\le\alpha)=e^{-e^{-\alpha}}\end{aligned} \tag{8}$$

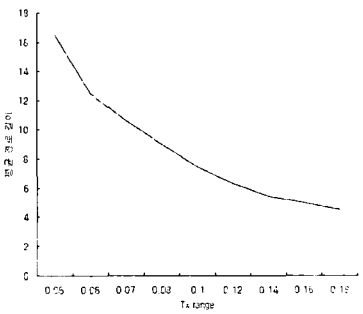
식 (8)에서 N은 네트워크 내 전체 노드 수이고, r은

〔표 2〕 패킷 전송 시 총 소모 에너지

Parameter	Energy (mAH)	Increase	Note
current TinyOS	0.000160	-	
TinySec-Auth	0.000163	2%	only MAC
TinySec-AE	0.000166	4%	MAC+Data Encryption



〔그림 7〕 전송 거리에 따른 네트워크의 연결 확률 (N=1000)



〔그림 8〕 전송 거리에 따른 평균 경로 길이 변화 (N=1000, 1km×1km)

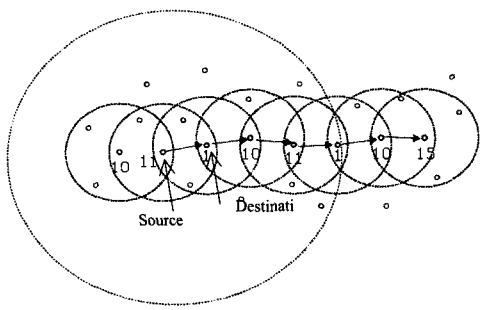
노드 수가 N일 때의 전송 거리이다.

〔그림 7〕은 기존에 연구되었던 *Random Geometric Graph*[16]에서 제시된 식 (8)을 이용하여 도식하였다.

〔그림 8〕은 센서의 전송 거리 r에 따른 평균 경로 길이를 나타낸 것으로 전송 거리 r이 짧을수록 평균 경로 길이는 길어짐을 볼 수 있다.

4.3 MAC 연산 오버헤드 분석

이 절에서는 MAC을 사용함에 따른 연산 오버헤드에 대해 분석한다. 〔표 2〕에서[15] 보듯이 MAC 연산을 한 번 하는데 소모되는 에너지는 3×10^{-6}mAH으로 매우 적다고 할 수 있다. 따라서 MAC 연산 자체의 오버헤드는 무 시할 만하다 할 수 있다. 각 센서의 MAC 연산 오버



〔그림 9〕 동일한 위장 ID 사용으로 불필요한 MAC 연산이 일어나는 경우 (소스로부터 4홉 떨어진 위장 ID가 '1'인 센서)

헤드에 대한 분석을 위해 두 가지의 경우 즉, 센서가 네트워크에 뿌려진 후 네이버를 discovery하는 경우와 실제 통신을 하는 경우 나누어 볼 수 있다.

첫 번째, 센서가 네트워크 지역에 뿌려진 이후 이웃을 discovery하는 경우이다. 이 경우에는 서로의 true ID와 위장 ID를 교환하게 되는데, 각 센서는 상대 센서의 위장 ID를 받은 후 그 센서와 공유하고 있는 pair-wise 키를 이용해 MAC 연산을 한 후 Unique value를 생성하여 맵핑 테이블에 저장한다. 따라서 이 과정에서 각 센서는 one-hop 네이버의 수만큼 MAC연산을 하게 된다.

<초기 MAC 연산 오버헤드 = 3×10^{-6}mAH (MAC 연산 시 소모에너지) × D (one-hop 네이버의 수)>

두 번째, 실제로 두 센서 간에 통신이 이루어지는 경우이다. 이 경우에는 데이터 프레임에 있는 MAC을 확인하기 위해 한 번만 MAC 연산을 하면 되기 때문에 MAC 연산 오버헤드는 매우 적다. 하지만 Global Eavesdropper의 경우 전송 power 레벨을 높여 전송하게 되면 〔그림 9〕와 같이 Destination 센서의 위장 ID와 동일한 ID를 사용하는 센서가 불필요하게 MAC 연산을 하게 되는 경우가 발생될 수 있다. 그러나 이러한 경우가 발생될 확률은 매우 낮으며, 이를 분석하면 다음과 같다.

〔그림 9〕에서 작은 원의 반지름을 r, 큰 원의 반지름

표 3. 네트워크 환경

Parameter	Value
network area	2km×2km
density (ρ)	320 sensors/km^2
Initial transmission range (r_0)	100m

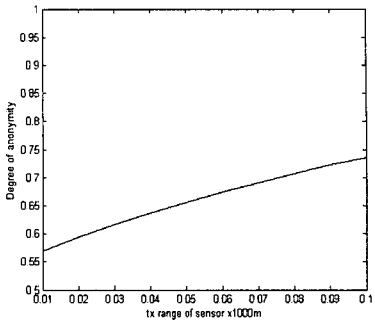
이 작은 원의 반지름의 x배라고 하고, 센서의 밀도를 ρ라고 하자. 그러면 큰 원 안에 존재하는 센서의 개수는 $\pi\rho x^2 r^2$ 개가 된다. Destination ID 필드는 2 바이트이기 때문에 각 센서가 생성할 수 있는 위장 ID의 수는 $2^{16}=65536$개 이다. 큰 원 안에 Destination 센서의 위장 ID와 동일한 ID를 갖는 센서가 하나도 없을 확률이 $(1-\frac{1}{2^{16}})^{\pi\rho x^2 r^2}$이므로 ID가 같은 센서가 적어도 하나 존재할 확률은 $1-(1-\frac{1}{2^{16}})^{\pi\rho x^2 r^2}$이다. 그리고 $1-(1-\frac{1}{2^{16}})^{\pi\rho x^2 r^2} < \frac{\pi\rho x^2 r^2}{2^{16}}$ 이므로 Destination의 위장 ID와 동일한 ID가 없을 확률은 $\frac{\pi\rho x^2 r^2}{2^{16}}$을 넘지 않는다는 것을 알 수 있다. 예를 들어 $\pi\rho r^2=10$이고 x=4일 때, $\frac{\pi\rho x^2 r^2}{2^{16}}=\frac{160}{65536}\ll 1\%$ 이므로 전송 거리를 4배 증가시키더라도 Destination 센서의 위장 ID와 같은 ID를 갖는 센서가 존재할 확률은 매우 낮아 불필요한 MAC 연산을 하게 되는 경우가 거의 발생되지 않는다.

결론적으로 네트워크를 구성하는 초기 단계 및 통신 과정에서 발생되는 MAC 연산 오버헤드는 매우 적기 때문에 MAC 연산으로 인한 오버헤드는 무시할 만하다.

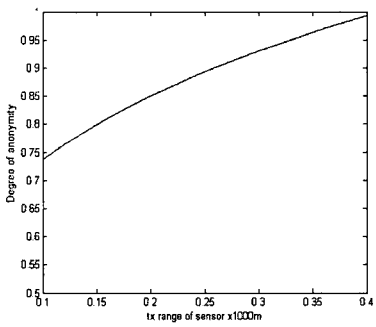
4.4 분석 결과

4.4.1 Global Eavesdropper

전송 거리 r에 따른 익명성 정도의 변화를 보이기 위해 네트워크 환경을 〔표 3〕과 같이 가정하였다. 그림 10은 제안한 기법을 사용했을 때 센서의 전송 거리에 따른 소스의 익명성 정도를 보여주고 있다. Phantom Routing의 경우에는 센서의 ID가 노출이 되기 때문에 전송 거리와 관계없이 익명성 정도는 항상 '0'이다. 〔그림 10〕에서 보듯이 전송 거리가 증가함에 따라 익명성 정도는 높아지며, 전송 거리를 초기 전송 거리 r_0보다 짧게 할 경우에는 익명성 정도를 최대 0.75이상으로 제



〔그림 10 (a)〕 전송 거리 $r \le r_0$



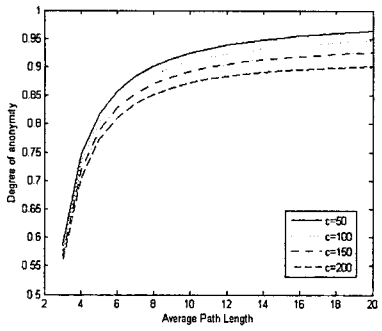
〔그림 10 (b)〕 전송 거리 $r \ge r_0$

공할 수 없다는 것을 알 수 있다. 따라서 높은 익명성 정도를 제공해야 한다면 에너지 소모를 줄이기 위해 전송 거리를 짧게 하는 것은 좋지 않다고 말할 수 있다.

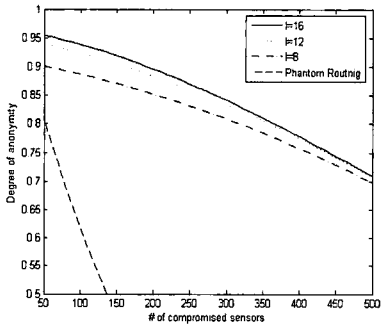
예를 들어, 전송 거리를 100m에서 400m로 증가시켰을 경우 소스의 익명성 정도는 약 35%가 높아지는데, 이는 최초 소스가 데이터를 전송하는 경우 Eavesdropper가 소스라고 예측할 수 있는 센서의 개수가 150여개에서 900여개로 증가하여 Eavesdropper가 소스를 알아낼 확률이 현저히 낮아짐을 의미한다.

4.4.2 Compromising Eavesdropper

〔그림 11 (a)〕는 compromise된 센서 수에 따른 소스의 익명성 정도의 변화를 보여주고 있다. 그림에서 보듯이 compromise된 센서 수가 증가함에 따라 익명성 정도는 낮아짐을 알 수 있다. 또한 Phantom Routing을 사용할 때보다 훨씬 높은 익명성 정도를 제공함을 보여주고 있다. Phantom Routing의 경우에는 전송 경로와 상관없이 compromise된 센서가 소스와 이웃해 있기만 하면 소스의 위치를 파악할 수 있기 때문에 익명성 정도



〔그림 11 (b)〕 평균 경로 길이에 따른 익명성 정도 변화



〔그림 11 (a)〕 노출된 센서 수에 따른 익명성 정도 변화 (l: 평균 경로 길이)

는 평균 경로 길이가 아닌 평균 Degree와 관계가 있다.

〔그림 11 (b)〕는 평균 경로 길이에 따른 소스의 익명성 정도를 나타내고 있다. 이 그림을 통해 평균 경로 길이가 증가함에 따라 익명성 정도도 높아짐을 알 수 있다. 초기에는 평균 경로 길이가 길어질수록 익명성 정도가 급격히 높아지나 경로 길이가 15이상에서는 익명성 정도가 한 값에 수렴되는 것을 볼 수 있다. 그리고 앞에서 언급한 네트워크의 연결성을 고려할 경우 최적의 전송 거리 r을 얻을 수 있다.

V. 결 론

본 논문에서는 센서 네트워크의 특성을 고려하여 소스 위치 프라이버시를 제공하기 위한 새로운 기법을 제시하였다. 이를 위해 센서 네트워크에서 소스 위치 프라이버시를 침해할 수 있는 Eavesdropper의 유형을 *Global Eavesdropper*와 *Compromising Eavesdropper*로 나누어 정의하였고, Eavesdropper의 각 유형에 따른 소스의 익명성을 제공하기 위한 기법을 제시하였다. 그리고 엔트로피 기반의 모델링 방법을 통해 센서 네트워크에서의 익명성 정도를 수학적으로 분석하고 정량화하였다. 그 결과 제안하는 기법이 높은 익명성을 제공함을 확인하였고, 센서의 전송 거리가 소스의 익명성 제공에 중요한 요소임을 보였다.

참고문헌

〔1〕 D. Chaum, "Untraceable Electronic Mail Return Addresses and Digital Pseudonyms," *Communication of the ACM*, 24, pp. 84-88, Feb. 1981.

〔2〕 Michael K. Reiter, Aviel D. Rubin, "Anonymity for Web Transactions," *ACM Transaction on information and system security*, 1998.

〔3〕 Claudia Diax, Stefaan Seys, Joris Claessens and Bart Preneel, "Towards Measuring Anonymity," *Appeared in Proceedings of .PET*, April 2002.

〔4〕 Andrei Serjantov, "On the Anonymity of Anonymity Systems," *Dissertation for the degree of Doctor of Philosophy in University of Cambridge*, March 2004.

〔5〕 Jiejun Kong, Xiaoyan Hong, "ANODR-ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks," *In MobiHoc*, 2003.

〔6〕 Azzedine Boukerche, Khalil El-Khatib, Li Xu and Larry Korba, "SDAR-A: Secure Distributed Anonymous Routing Protocol for Wireless Ad Hoc Networks," *Proceeding of the 29th Annual IEEE international Conference on Local Computer Networks*, 2004.

〔7〕 Pandurang Kamat, Yanyong Zhang, Wade Trappe and Celal Ozturk, "Enhancing Source-Location Privacy in Sensor Network Routing," *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems*, 2005.

〔8〕 C. Intanagonwiwat, R.Govindan, and D. Estrin,

"Directed Diffusion-a Scalable and Robust Communication Paradigm for Sensor Networks," *Proceedings of ACM MoBiCom*, pp. 56-67, 2000.

[9] C. Schurgers and M.B. Srivastava, "Energy Efficient Routing in Wireless Sensor Networks," *Proceedings of MILCOM*, 2001.

[10] J. Kulik, W.R. Heinzelman, and H. balakrishnan, "Negotiation-Based Protocols for Disseminating Information in Wireless Sensor Networks," *IEEE Wireless Networks*, 18, pp. 169-185, 2002.

[11] Mihir Bellare, Ran Canetti, and Hugo Krawczyk, "HMAC-Keyed-Hashing for Message Authentication," *Internet Engineering Task Force RFC2104,* 1997.

[12] 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, 2002. .

[13] Haowen Chan, Adrian Perrig, and Dawn Song, "Random Key Predistribution Schemes for Sensor Networks," *Proceedings of the 24th IEEE Symposium on Security and Privacy*, pp. 197-215, 2003.

[14] Sencun Zhu, Sanjeev Setia, and Sushil Jajodia, "LEAP-Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," *Proceedings of the 10th ACM Conference on Computer and Communication Security*, pp. 62-72, 2003.

[15] Chris Karlof, Naveen Sastry and David Wagner, "TinySec-A Link Layer Security Architecture for Wireless Sensor Networks," *Proceedings of the ACM Conference on Embedded Networked Sensor Systems*, 2004.

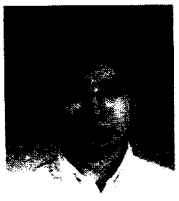
[16] Matthew D. Penrose, Random Geometric Graphs, *Oxford Univ. Pressr*, 2003.

[17] Pajek, website : http://vlado.fmf.uni-lj.si/pub/networks/pajek/

〈著者紹介〉

이 송 우 (Song-Woo Lee) 정회원

1999년 2월: 육군사관학교 무기공학과 졸업
2005년 3월~2007년 2월 : 서울대학교 전기컴퓨터공학부 석사
<관심분야> 무선 센서네트워크, 프라이버시 보호, 통신공학

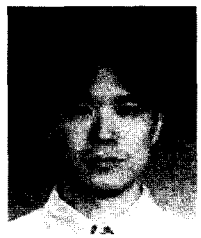


박 영 훈 (Young-Hoon Park) 학생회원

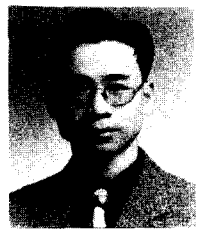
2006년 2월: 서울대학교 전기공학부 졸업
2006년 3월~현재: 서울대학교 전기컴퓨터공학부 석사과정
<관심분야> 프라이버시 보호, 네트워크 보안

손 주 형 (Ju-Hyung Son) 정회원
2001년 2월: 연세대학교 전기공학부 졸업
2003년 2월: 서울대학교 전기컴퓨터공학부 석사
2003년 3월~현재: 서울대학교 전기컴퓨터공학부 박사과정
<관심분야> 무선 센서네트워크 보안, 보안 키 관리

서 승 우 (Seung-Woo Seo) 정회원
1987년 2월: 서울대학교 전기공학과 졸업
1989년 2월: 서울대학교 전기공학과 석사
1993년 12월: 미국 펜실베니아 주립대학 전기공학 박사
1993년~1994년: 미국 펜실베니아 주립대학 전산기공학과 조교수
1994년~1996년: 미국 프린스톤대학 전기공학 poem 연구소



강 유 (Yu Kang) 준회원
2003년 2월: 서울대학교 컴퓨터공학과 졸업
2004년~현재: KT 정보보호단 기술개발 1부
<관심분야> 모의해킹, 위험분석, 컴퓨터 포렌식



최 진 기 (Jin-Gi Choe) 준회원
1998년 2월: 숭실대학교 전자공학과 졸업
1999년~2004년: KT 차세대 통신망 연구소 보안기술연구실
2005년: 충남대학교 정보통신공학과 석사
2005년~현재: KT 정보보호단 기술개발 1부
<관심분야> 위험분석, 네트워크 보안

문 호 건 (Ho-Kun Moon) 정회원
1985년 2월: 숭실대학교 전자공학과 졸업
1987년: 중앙대학교 전자공학과 석사
2005년: 부산대학교 전자공학과 박사
1987년~2004년: KT 차세대 통신망 연구소 보안기술연구실장
2005년~2006년: KT 정보보호단 기술개발 1부장