휴면 소오스들이 존재하는 환경의 센서 네트워크를 위한 위치 보호 강화 라우팅

(Location Privacy Enhanced Routing for Sensor Networks in the Presence of Dormant Sources)

양 기 원 † 임 화 정 †† 차 영 환 †††
(Gi-Won Yang) (Hwa-Jung Lim) (Yeonghwan Tscha)

요 약 전장에서 군 작전을 지원하거나 희귀 동물을 모니터링 하는 센서 네트워크에서는 전송 정보의 보안뿐만 아니라 그러한 관심 대상(asset)들의 위치를 적이나 악의적 추적으로부터 보호할 수 있어야 한다. 본 논문에서는 위치가 보호되어야 할 대상에 근접한 센서 노드들 즉, 휴면(dormant) 소오스들이 존재하는 환경에서, 활동 소오스(즉, 메시지 발생 노드)의 위치 보호를 강화하는 라우팅 프로토콜 GSLP (GPSR-based Source-Location Privacy)를 제안한다. GSLP는 단순하면서도 scalable한 라우팅 기법인 GPSR(greedy perimeter stateless routing)을 확장하여, 확률적으로 임의의 이웃 노드를 메시지 전달 노드로 선정하여 경로의 다양성을 제고하면서 퍼리미터(perimeter) 라우팅을 적용하여 휴면 소오스 노드들을 우회하도록 함으로써 안전 기간(safety period)으로 정의되는 활동 소오스의 위치 보호 능력이 강화되도록 하였다. 휴면 소오스들의 수가 전체 노드의 1.0%에 이르기까지 시뮬레이션을 수행한 결과, 기존의 대표적인 소오스 위치 보호 프로토콜인 PR-SP(Phantom Routing, Single Path)의 안전 기간은 휴면 소오스 노드들이 증가에 따라 급속히 감소하나 제안된 GSLP는 휴면 소오스 노드들의 수와 거의 무관하게 높은 안전 기간을 제공하면서도 평균 전달 지연(delivery latency)은 도착지와의 최단 거리의 약 두 배 이내에 머무는 것으로 확인되었다.

키워드 : 센서 네트워크, 소오스 위치 보호 라우팅

Abstract Sensor networks deployed in battlefields to support military operations or deployed in natural habitats to monitor the rare wildlifes must take account of protection of the location of valuable assets(i.e., soldiers or wildlifes) from an adversary or malicious tracing as well as the security of messages in transit. In this paper we propose a routing protocol GSLP(GPSR-based Source-Location Privacy) that is capable of enhancing the location privacy of an active source node(i.e., message-originating node) in the presence of multiple dormant sources(i.e., nodes lying nearby an asset whose location needs to be secured). Extended is a simple, yet scalable, routing scheme GPSR(greedy perimeter stateless routing) to select randomly a next-hop node with a certain probability for randomizing paths and to perform perimeter routing for detouring dormant sources so that the privacy strength of the active source, defined as safety period, keeps enhanced. The simulation results obtained by increasing the number of dormant sources up to 1.0% of the total number of nodes show that GSLP yields increased and nearly invariant safety periods, while those of PR-SP(Phantom Routing, Single

· 이 논문은 2007년도 정부(교육인적자원부, 현 교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2007-521-D00409). 연구 지원을 해준 관계당국과, 시뮬레이션 S/W 개발과 실험에 도움을 준 박상주, 차철환, 서경인, 신성 군에게 감사드린다.
· 이 논문은 2008 한국컴퓨터종합학술대회에서 '휴면 소오스들이 존재하는 환경에서의 위치보호 라우팅'의 제목으로 발표된 논문을 확장한 것임.

† 학생회원 : 한국정보통신대학교 공학부
giwonej@hotmail.com
†† 학생회원 : 강원대학교 컴퓨터정보통신공학과
lim1108@hanmail.net
††† 정 회 원 : 상지대학교 컴퓨터정보공학부 교수
yhtscha@sangji.ac.kr
(Corresponding author임)

논문접수 : 2008년 4월 17일
심사완료 : 2008년 10월 17일

정보과학회논문지: 정보통신 제36권 제1호(2009.2)

Path), a notable existing protocol for source-location privacy, rapidly drop off as the number of dormant sources increases. It turns out that delivery latencies of GSLP are roughly less than two-fold of the shortest path length between the active source and the destination.

Key words : sensor networks, routing for source-location privacy

1. 서 론

무선 통신 자체가 갖는 전송 신호의 노출 문제와 센서 관련 장비의 대중화 및 옥외 설치되는 환경적 특수성이 가중되기도 하는 센서 네트워크에서는 제한된 컴퓨팅 능력으로 한정된 에너지를 사용하여야 하므로 보안 문제를 해결하기가 매우 어렵다[1]. 암호화 기법을 이용하여 전송 정보의 내용을 보호하는 전통적 의미의 보안도 중요하지만, 통신 노드들의 위치나 트래픽의 양이나 종류 등과 같은 문맥 정보(contextual information) 보호도 응용에 따라 매우 중요하다. 예를 들어, 전장에서 임무 수행중인 병력이나 탱크 등과 같은 이동체를 지원하거나 희귀 동물의 활동을 감시하는 응용 등에서는 암호화된 메시지를 이용하는 것과 관계없이 송신 장치의 위치가 적이나 밀렵꾼 등에 노출되는 경우 그 피해는 심각할 수 있다.

본 논문에서는 기지국 또는 싱크로 메시지를 전송하는 활동 소오스의 위치를 지역 도청자(local eavesdropper)인 적으로부터 보호하기 위한 새로운 라우팅 기법을 제안한다.[1] 기지국은 센서 네트워크의 중심이 되는 노드로서 각종 노드에서 전송되는 정보들이 집중되며, 외부 서버나 네트워크에 연결되는 장비로써 그 존재가 쉽게 노출되거나 탐지될 수 있다[2]. 따라서 기지국으로 정보를 전송하는 소오스 노드의 위치 보호가 무엇보다도 우선되어야 한다.

센서 네트워크에 있어서 라우팅 차원에서의 소오스 노드의 위치 보호에 관한 연구는 미국 Rutgers 대학 WINLAB의 W. Trappe 교수팀에 의해 PR(Phantom Routing)이 제시되면서부터 매우 활발해졌다[3]. PR은 관리 보호 대상이나 특정 이벤트를 감지한 소오스 노드가 수집된 정보를 기지국으로 전송하는 과정에서, 기지국 근처나 경로 상에 머물고 있는 추적자가 도착하는 메시지의 신호를 따라 거슬러 올라가, 소오스의 위치를 파악하려는 역방향 홉 단위 이동 공격에 대응하기 위해 고안되었다. 라우팅 초반에는 일정 거리(예, 20 홉) 이상을 무작위로 선정된 방향으로 이동한 뒤(directed random walk 과정), 나머지 후반은 기지국으로 메시지를 전달하는 라우팅 과정으로 최단거리 라우팅을 수행하는 PR-SP(single path)와 브로드 캐스팅을 수행하는 PR-B(broadcast)가 있다. 후속 연구[4]에서는 위치 보호 모델을 정의하고, 소오스 노드가 이동하는 경우와 일정 위치에서 추적자가 메시지를 기다리는 시간이 제한된 경우에서의 PR의 성능을 다루었다. 라우팅 차원에서의 소오스 위치 보호에 관한 문제를 도출하고 대안과 함께 평가 기준을 정립하였다는 점에서 매우 고무적이다. 하지만, 임의의 이동 거리를 길게 할수록 안전 기간은 늘어나지만 이에 비례하여 메시지 전달이 과도하게 지연 되는 문제점이 있다.

PR에서 임의의 방향으로의 이동 과정에서 선택되는 노드들의 방향이 서로 상쇄되지 않고 소오스로부터 멀리 전개되도록 하는 방안[5]과 소오스와 싱크 양쪽으로부터 PR을 동시에 이용하여 경로를 설정하고 메시지를 전송하는 방법[6] 등, 후속 연구 결과들이 제시되었다. 또한, 설정 경로를 중간에 다른 경로와 겹치게 하여 추적에 혼선을 야기하도록 한 연구[7]도 제시되었다. 하지만 모두 활동 소오스 노드만을 고려하였고 안전 기간을 늘리기 위해 긴 경로를 사용하는 경우에 발생하는 전달 지연 문제에 대한 대안을 제시하지 않았다.

안전 기간을 길게 하되 전달 지연을 단축하기 위한 방안으로는 CEM(Cyclic Entrapment Method)가 있다[8]. 최단 거리 알고리즘에 의해 설정되는 경로 상의 노드에 특정 길이(예, 15홉) 이상의 루프 경로를 덧붙여서, 전송되는 메시지가 원래의 최단 경로뿐만이 아니라 루프를 선회하도록 하여 추적에 혼선을 주도록 한다. 전송 지연을 단축할 수 있지만 공격자가 GPS 또는 자신이 추적한 노드의 좌표 값을 기억하는 경우 루프를 반복하지 않을 수 있다. 또한, 경로로 이용되는 노드는 극히 일부이나 모든 노드가 네트워크 초기화시 일정 길이 이상의 루프를 미리 설정하여야 하기에 메시지들이 과중하게 발생된다. 최소 길이가 k 이상인 경로를 설정하는 k-최장 경로(k-longest path) 문제가 NP-complete임을 고려할 때 루프 구성 시간 역시 부담이 된다. 아울러, 추적자가 루프에 연결된 노드에 근접할 때 속임수 메시지가 루프로부터 발생되어야 추적자를 루프 안으로 유인할 수 있다. 문제는 일반 소형 노드에 추적자의 접근을 판단하는 효과적인 메커니즘을 어떻게 구현하여 넣을 것인가이다. 결국, CEM의 핵심인 루프 활용은 그

1) "위치를 보호한다"는 것은 "위치를 100% 노출시키지 않는다"는 의미보다는 "안전 기간(safety period)으로 정의되는, 즉 위치가 노출되기 전까지 관련 소오스가 얼마나 많은 메시지를 전송할 수 있는가"란 다소 우회적인 의미로 해석된다[3,4,8,9].

실효성에 문제가 있다.

한편, 메시지의 최종 도착지 노드나 기지국의 위치를 보호하기 위한 연구도 진행되었다. 기지국으로 향하는 트래픽들이 만나는 aggregator 노드의 주변에 머무는 공격자가 트래픽 수집과 분석을 통해 기지국의 위치를 파악하려는 공격에 대응하는 DEFP(Differential Enforced Fractal Protocol)가 있다[2]. 이 기법은 경로 상의 노드로 하여금 속임수용 메시지를 트리 형태로 분기 발생하고(fractal propagation 과정), 임의의 이동을 일정 확률로 수행하여 이용 경로의 무작위화(randomization)를 유도한다. 또한, 트래픽 유형, 정보량, 발생 주기 등과 같은 정보를 보호하기 위한 기법들을 종합적으로 연구하였는데, 속임수(fake) 메시지를 발생하는 기법이나 무작위 이동 등은 후속 연구들에서 많이 이용되고 있다.

LPR[9]은 PR-SP과는 반대로, 소오스의 위치가 노출된 경우 도착지 노드의 위치를 보호 수준을 높이기 위한 라우팅 기법이다. 각 노드는 자신의 이웃 노드들을 도착지 노드와 가까운 노드들의 집합(closer_list)과 같거나 먼 노드들의 집합(further_list)으로 정의하고 일정 확률로 이 둘 중에서 임의의 한 노드들 다음-홉 노드로 선정한다. 따라서 further_list로부터 선정될 확률을 증가시킴에 따라 길이가 긴 경로의 설정이 가능하기 때문에 추적자로 하여금 도착지의 위치 파악까지 많은 시간을 소비하도록 하게 할 수 있다. 하지만, 전달 지연이 과도해지게 되며, 메시지 전달 방향과 추적 방향이 같으므로 라우팅 과정에서 속임수 메시지를 발생하여 추적자로 하여금 실제 경로로의 진행을 어렵게 하는 기능이 필요하다.

보안 위협(threat)에 관해서는 여러 곳에 추적자(감시자)를 배치하고 정보를 수집 분석하는 전역(global eavesdropper) 모델[4,6,10] 또는, 일반 노드와 동일한 신호 수신 능력을 가지고 발생 신호에 따른 홉 단위 추적을 수행하는 지역 도청자 모델[3,4,9]이 있다. 트래픽 분석에 의한 트래픽 속성(량, 경로 패턴, 정보 유형 등)을 파악하려는 공격에 대응하기 위한 연구[11]나 정보 이론적 측면에서의 익명성 통신 연구[2] 등도 있다. 하지만, 본 논문의 주제인 지역 도청에 대응하는 라우팅 프로토콜 차원에서의 소오스 위치 보호와는 거리가 있다. 보다 자세한 관련 연구 및 본 연구의 확장에 대해서는 [12]에 나와 있다. 한편, 센서 네트워크에 관한 최신 연구들에 관해서는 [13]에서 자세히 다루고 있다. 본 논문의 기여 부분은 다음과 같다.

- 휴면(dormant) 소오스들이 존재하는 환경을 처음으로 고려하였다. 관련 연구[3,4,8]에서 소오스 노드로 정의하는 즉, 기지국으로 정보를 전송 중인 노드를 활동(active) 소오스 노드로 재 정의하는 한편, 정보 전송은 하고 있지 않지만 추적자가 일정 거리 이내로 접근하면 그 위치가 탄로 나는 어떤 보호 대상에 인접한 노드를 휴면 소오스 노드라고 정의하고 위치 보호 대상으로 고려하였다.[2] 이에, 휴면 소오스들이 존재하는 환경에서의 위치 보호 라우팅 문제를 제기 하고 그 대안을 제시하였다.
- 위치 기반(position-based) 라우팅이 가능하고 단순하면서도 구현이 용이하여 대규모 네트워크로의 적용이 가능한 GPSR(Greedy Perimeter Stateless Routing)[14]을 확장하여 소오스 위치 보호 기능을 갖는 GSLP(GPSR-based Source-Location Privacy)을 제안하였다. 최단 거리 라우팅을 지향하는 탐욕적 송출(greedy forwarding)외에 특정 확률로 일정 거리(홉)를 무작위로 전개하는 과정을 추가하는 한편, 퍼리미터(perimeter) 라우팅 기법을 이용하여 휴면 소오스 노드들을 우회하도록 하였다. 이로 인해 위치 보호 수준을 일정하게 유지하면서도 긴 경로를 이용하는 경우 발생되는 전달 지연을 가능한 억제하도록 하였다.

제안한 GSLP를 검증하기 위해 시뮬레이션에서는 평균 차수(degree)가 8인 노드 50,000개로 구성되는 네트워크 토폴로지 100개를 생성하여 측정하였다. 소오스 노드들의 수는 전체 노드의 0.2%에서부터 1%까지, 그리고 메시지를 전송하는 액티브 소오스 노드와 기지국 간의 거리(홉 수)는 30에서부터 100까지를 고려하였다. 평가를 위해 안전 기간과 메시지 전달 지연을 측정하였고, 비교 대상으로는 가장 대표적인 소오스 위치 보호 라우팅 기법인 PR-SP[3,4]를 선정하였다. PR-SP는 휴면 소오스들을 라우팅에서 고려하고 있지 않지만, 휴면 소오스들이 존재하는 환경에서의 활동 소오스의 위치를 어느 정도 보호할 수 있으며 본 연구 결과의 상대적 비교를 위함이다. 시뮬레이션 결과, GSLP의 평균 전달 지연(사용 경로의 평균 길이로 정의됨)은 활동 소오스와 기지국 사이의 홉 수에 두 배를 크게 넘지 않는 것으로 나타났다. 안전 기간은 소오스 노드의 수가 증가할 수록 그리고 활동 소오스 노드와 기지국간의 거리가 길어질수록 PR-SP에 비해 최고 11배까지 늘어났다. 특히, PR-SP의 안전 기간이 휴면 소오스들의 수의 증가에 따라 급격히 줄어드는 것과 대조적으로 GSLP는 휴면 소오스들의 수에 거의 무관하게 일정 수준의 안전 기간을 유지하였다.

본 논문의 구성은 다음과 같다. 다음 장에서는 연구를

2) 관리(또는 보호) 대상을 인지하자마자 무조건 기지국으로 정보를 전송하는 응용도 있을 수 있지만, 보호 대상에 대한 지역적 모니터링이나 수집 데이타의 압축과 같은 내부적인 이벤트를 처리 중인 소오스 노드를 표현하기 위해 "휴면 소오스 노드"의 개념을 도입한다. 예를 들어, 전장에 투입된 병력이나 탱크 등은 기지국과의 통신과 관계없이 그 위치가 공격자나 추적자에게 노출되지 말아야 되며, 라우팅 차원에서는 이들의 위치를 보호할 메커니즘을 강구할 필요가 있다.

위해 가정된 사항과 추적자 모델을 설명한다. 3장에서는 제안하는 소오스 위치 보호 라우팅 기법 GSLP를 설명하고, 평균 지연 시간을 분석한다. 4장에서는 시뮬레이션을 위해 설정된 파라미터들을 소개하고 측정된 안전 기간과 전달 지연에 대해 논한다. 본 논문은 5장의 결론으로 끝을 맺는다.

2. 네트워크 및 공격자 모델

2.1 네트워크 모델

네트워크 내에는 N 개의 센서 노드들과 하나의 기지국 b가 존재하며, 모든 노드는 자신의 위치(즉, 좌표 값)와 b의 좌표 값을 알고 있다. 전송 중에 어떠한 오류나 문제도 발생하지 않으며, 노드들 간에 주고받는 모든 메시지는 암호화되어 있어 공격자가 해독할 수 없다. 하지만 공격자에게 b의 위치가 노출되어 있다고 가정한다[3,4,9]. 센서 노드들이 모니터링 해야 할 보호 대상(asset)들의 수는 N에 비해 극히 적으며, 이들의 발현은 간헐적이라고 가정한다. 보호 대상의 발현을 감지한 센서 노드들은 기지국으로 메시지를 전달하는 활동(active) 소오스가 되거나 아니면 보호 대상에 대한 지역적 모니터링이나 보호 대상을 추적자로부터 보호하기 위한 경계 지역(alert zone)을 설정하고 대기 상태에 머무는 휴면(dormant) 소오스 노드가 된다고 가정한다. 즉, 보호 대상의 존재를 감지한 노드들은 기지국 b로의 메시지 전송에 앞서서 자신으로부터 거리가 $\beta(>r)$(r: 노드의 감지 거리 또는 신호 도달 거리)이내인 영역에 존재하는 노드들에게 보호 대상이 근처에 존재하므로 메시지 전송 과정에서 해당 영역을 우회할 것을 나타내는 경계 지역(alert zone)을 설정함을 가정한다.[3)]

한편, 문제의 단순성을 고려하여 전체 노드 수 N에 비해 보호 대상들의 수는 매우 적으며 네트워크 내에 산재되어 분포하여 동일한 센서 노드의 감지 범위 내에 하나 이상 존재하지 않는다고 가정한다. 즉, 보호 대상과 대응되는 센서 노드 즉, 휴면 소오스는 일대일 관계이다. 이에, 해당 보호 대상이 공격자에게 노출 되었다는 것은 곧 대응 소오스의 위치가 발각되었다는 것을 의미한다(이의 역도 마찬가지이다. 임의의 보호 대상과 대응되는 선서와의 거리는 언제나 r 이내이다).

2.2 공격자 모델

유사연구[3,4,8,9]에서와 같이 지역 도청자를 가정한다. 공격자는 각종 장비(예, 스펙트럼 분석기, 지향성 안테나, GPS 등등)들을 갖추고 있어 신호 방향, 세기, 도착각 등을 측정하여 어느 노드로부터 신호가 발생했는지 정확히 인지 할 수 있다. 즉, 공격자가 머물고 있는 노드에 메시지가 도착되면 이 신호를 인지하여 해당 메시지를 전송한 노드로 이동한다. 추격은 언제나 먼저 도착하는 신호를 따라 이동하고, 여러 신호가 동시에 발생하는 경우에만 임의로 선택한다. 추적 과정에서 경유하는 노드에서는 거의 무한정으로(현실적으로는 시뮬레이션을 위해 한정된 시간까지) 다음 신호가 발생할 때까지 기다리는 patient 모델을 고려한다.[4)]

어떤 소오스가 존재하는 곳으로부터 반지름이 α인 원내로 공격자가 진입하면 그 소오스의 위치는 탄로 난 것으로 간주한다. 이때의 영역을 노출 영역(disclosure area) 또는 포획 거리(capture distance)라고 한다[3,4]. α는 공격자의 추적 능력이나 보호 대상이 어떤 것인가 등에 따라 다양하게 정의된다. 예를 들면 사람의 시각 거리나 사용 장비의 신호 감지 거리 등이 될 수 있다. 위치 추적자의 공격은 완전한 수동 공격으로 방해용 메시지나 신호를 발생하지 않는다. 공격자는 과거 추적된 경로들에 대한 좌표 값을 기억하고 있어서, 이전 노드로의 이동이나 기지국으로의 복귀가 가능하다. 하지만 추적자의 추적 속도는 메시지의 이동 속도보다 빠르지 않으며, 홉 단위의 역 추적을 행하므로 발생 신호보다 앞서서 이동하지 않는다고 가정한다. 한편, 위에서 정의된 경계 지역의 범위를 나타내는 변수 β와 포획 거리 α에 대해 $\beta>\alpha$가 성립하며, 경계 지역 내의 보호 대상이나 소오스는 추적자가 α 이내로 접근하지 않는 한 안전하다.

2.3 평가 항목

라우팅 프로토콜의 소오스 위치 보호 능력과 성능을 평가하기 위해 다음 요소를 측정한다.

- 안전 기간(safety period) : 어떠한 소오스 노드의 위치도 추적자에게 노출되지 않는 동안에 활동 소오스 s가 기지국(최종 도착지) b로 전송한 메시지의 수
- 전달 지연(average latency): 활동 소오스 노드 s가 b로 성공적으로 전달한 메시지들이 경유한 경로의 평균 길이(홉)

안전 기간은 라우팅 프로토콜의 위치 보호 능력을 나타내는 척도로 W. Trappe[3]에 의해 처음 도입된 이후 거의 모든 관련 연구에서 사용하고 있다[4,8,9]. 안전 기간이 길면 길수록 높은 위치 보호 수준을 의미한다. 일반적으로 동일 경로에 연속적으로 메시지를 보내는 경우 추적의 용이성을 제공한다는 전제 하에서 메시지마다 다른 경로를 설정한다. 그런데 동일한 안전 기간에 대해서도 서로 다른 길이의 경로들이 사용될 수 있으므로 안전 기간이 길더라도 가능한 짧은 전달 지연을 갖

3) 예를 들면 geocasting[15]이나 scoped flooding[16] 등을 이용하여 경계 지역을 설정할 수 있다.

4) 추적자가 거쳐 가는 노드에서 일정 시간 동안만 대기하는 "cautious 모델"도 연구되었지만 "patient 모델"에 비해 추적 효과가 낮은 것으로 나타났다[4].

는 다수의 경로들이 사용되는 것이 좋다.

네트워크의 에너지(전력) 소비 정도나 라우팅 프로토콜의 비용을 평가하기 위해서는 단일 메시지를 전달하기 위해 발생되는 메시지들의 수를 고려하기도 한다. 그런데 본 연구에서 제안하는 GSLP나 비교되는 PR-SP 모두 속임수 메시지 등 추가적인 메시지의 발생 없이 전송 메시지만을 경로별로 전송하므로 경로별 평균 메시지 발생 수는 평균 전달 지연과 일치한다.[5] 이에 본 연구에서는 메시지 발생 비용을 고려하지 않는다.

3. 휴면 소오스를 고려한 위치 보호 라우팅

3.1 라우팅 기법

제안된 라우팅 기법 GSLP(GPSR-based Source-Location Privacy)에서는 메시지 전달을 위한 다음-홉(next-hop) 노드의 선정은 그림 1과 같이 네 개의 모드로 구분되어 이루어진다.[6] 모드간의 상태 천이를 유발하는 원인들에 대해서는 번호를 붙여 자세히 나타내었다.

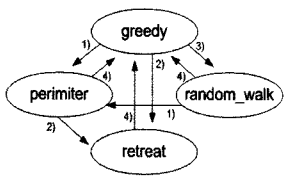


그림 1 GSLP의 다음 홉 노드 선정을 위한 운행 모드

- **greedy 모드**: 난수 $p(0<p<1)$를 생성하여 $p<p_{rw}$ $(0<p_{rw}<1)$이면 random_walk 모드로 전환하고 그렇지 않으면 GPSR[14]의 탐욕적 송출에 해당하는 기능을 수행한다. 즉, 확률 $(1-p_{rw})$로 목적지 b에 가장 근접한 이웃 노드를 다음 노드로 선정한다. 만일 이와 같은 조건으로 선정된 노드가 어떤 휴면 소오스가 설정한 경계 지역 내에 존재하는 것이라면 perimeter 모드로 이동한다. 소오스 위치 보호와 관련된 기존의 주요 연구[3,4,9]에서는 안전 기간을 늘리기 위해 긴 경로를 설정하는 원칙에 목표를 우선적으로 두었지만 본 연구에서는 greedy 모드를 도입하여 메시지 전달 지연을 억제하고자 한다.
- **random_walk 모드**: 메시지 전송 시 greedy 모드를 너무 많이 적용하면 동일 노드가 여러 경로에서 사용되게 되어 위치 보호 면에서 불리할 수 있다. 이에, 본 모드에서는 다양한 유형의 경로들이 가능한 중복되지 않고 설정될 수 있도록 하는 것이 목적이다. 다음 홉 노드로는 현재의 노드보다 목적지로의 거리를 증가시키지 않는 이웃 노드들 중 임의의 하나를 선정한다. 따라서 진행 방향의 뒤로 존재하는 노드들은 제외되게 되는데 이는 사용 경로의 과도한 길이 증가를 피하기 위함이다. 이 모드가 일단 진행되면 TTL에 해당하는 홉 수만큼 후속 다음 홉 노드들에 대해서도 연속적으로 random_walk 모드가 적용되도록 한다. 이를 위해 전송 메시지 내에 TTL 필드를 두어 나타낸다. 후속 노드에서는 그 값을 1씩 감소시키면서 수행하되, 0이 되면 random_walk 모드의 적용이 중지된다. 본 연구의 시뮬레이션에서는 p_{rw}을 0.05로 하였고, TTL는 활동 소오스와 도착지 노드간의 최단 거리의 [0.5%, 1%] 범위에서 활동 소오스로 하여금 선택하게 하였다(최소치 2). 이렇게 p_{rw} 값을 작게 한 이유는 고려되는 네트워크 내에 보호 대상들(즉, 휴면 소오스)들이 존재하므로 이들을 보호하기 위한 우회 경로의 설정으로 인해 자연스럽게 경로 길이가 증가되기 때문이다.
- **perimeter 모드**: GPSR에서 "국소 최대화(local maximum) 문제"[14,17,18]로 인해 발생되는 "라우팅 홀(routing hole)"를 피하기 위해 적용하는 퍼리미터 라우팅을 이용하여 설정된 경계 지역을 우회하여 다음 홉 노드를 선정 한다. 현재 노드에서 도착지로의 직선을 기준으로 시계 반대 방향으로 가장 가깝게 존재하는 노드를 다음 노드로 선정하는 오른손(right-hand) 규칙과 시계 방향으로 가장 가깝게 존재하는 노드를 다음 노드로 선정하는 왼손(left-hand) 규칙을 고려할 수 있다. 이들 중 어느 하나가 활동 소오스에 의해 전송 메시지마다 지정되게 되면 도착지에 이르기까지 만나는 모든 경계 지역에 대해 일괄되게 적용한다. 이를 위해 그림 2와 같은 메시지 형식에 Detour_Rule 필드를 둔다. 활동 소오스 노드는 이 필드 내에 전송되는 메시지마다 번갈아가며 서로 다른 규칙을 지정한다. 이는 활동 소오스에서 도착지 노드를 연결하는 가상의 직선을 고려 할 때, 왼쪽이나 오른쪽 어느 한 영역으로만 경로가 치우쳐서 설정되지 않도록 하기 위한 것이다. 네트워크 내의 휴면 소오스 노드들의 수가 증가할수록 perimeter 모드로의 동작은 빈번해지고 경로 길이는 증가된다. 일단 경계 지역을 지나 최단 거리 라우팅이 가능해지면 greedy 모드로 환원된다.
- **retreat 모드**: 위의 세 모드로 더 이상의 경로 전개가 불가능하여 이전의 노드로 다시 되돌아가는 과정이다. 일단 이전의 노드로 되돌아가면 다시 greedy 모드로 전환되어 앞서 방문하였던 이웃 노드를 제외한 나머지 이웃 노드들을 대상으로 다음 노드를 선정한다.[7]

5) 경계 지역을 설정하는 비용은 사용자 메시지를 전달하는 라우팅 비용과 달리 초기화 비용으로 정의된다. 다른 연구[3,4,8]에서 처럼 본 연구에서 라우팅 프로토콜의 성능 평가에 이러한 초기화 비용은 포함하지 않는다.

6) 편의상 본 논문에서는 "다음-홉 노드" 대신 "다음 노드"를 사용하기도 하며, "라우팅"과 "다음-홉 선정"을 구분하지 않고 동의의 의미로 사용한다.

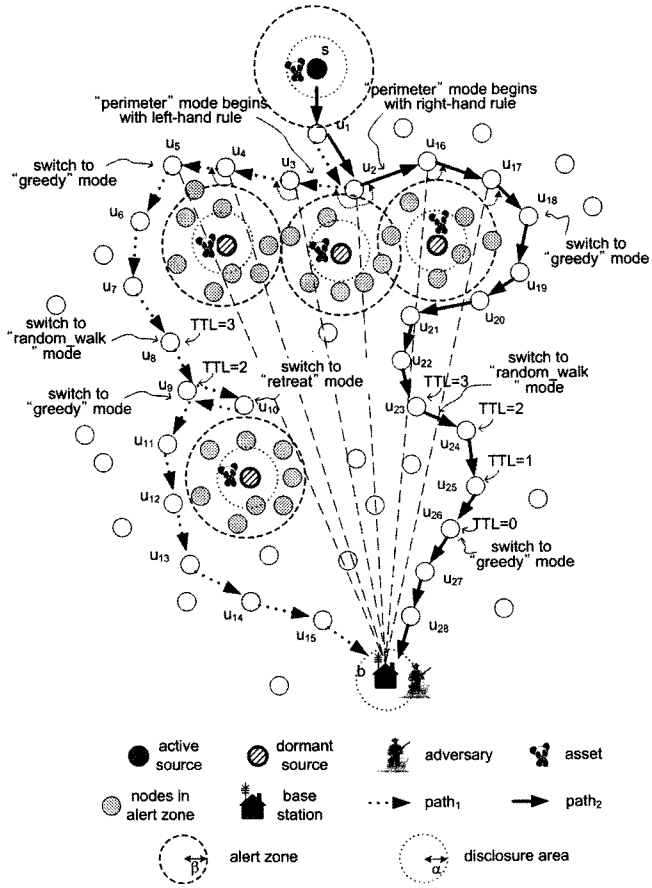


그림 3 GSLP의 동작 예

Coordinate_of_Destination		
Coordinate_of_Source		
Mode	TTL	Detour_Rule
Send_Sequence_Number		
Size_of_User_Data		
User_Data		

그림 2 GSLP 메시지 형식과 필드

GSLP의 메시지 형식은 그림 2와 같다. Coordinate_of_Destination은 도착지 노드의 좌표 값을, Coordinate_of_Source은 활동 소오스 노드의 좌표 값을 나타낸다. Mode는 GSLP의 추후 확장을 위해 정의된 것인데, 현재로는 random_walk 모드에 의한 다음-홉 선정 여부를 나타내며, TTL 필드 값이 0보다 큰 경우에만 적용되도록 하고 있다. Detour_Rule은 perimeter 모드에서 다음 노드를 설정할 규칙으로 left-hand 또는 right-hand를 나타낸. Send_Sequence_Number는 전송 메시지의 순번을 Size_of_User_Data는 사용 정보 길이를, 그리고 User_Data는 전송되는 사용자 정보를 나타낸다.

그림 3은 GSLP의 동작 과정을 보여주는 예이다. 보호 관리 대상으로 판다 곰을 들었는데, 이들이 존재하는 곳으로부터 가장 가까운 센서 노드들이 활동 소오스 s 외에 네 개의 휴면 소오스로 경계 지역을 설정한 경우를 가정하였다. 처음에, s로부터 두 개의 메시지가 전송되었다는 가정에서 이용된 경로 $path_1$과 $path_2$를 보였다. s에서 greedy 모드로 다음 노드 u_1이, 그리고 u_1에서도 greedy 모드로 u_2가 선정되었다. u_2에서 경계 지역을 만나서 perimeter 모드로 전환되어 $path_1$은 왼손 규칙에 따라, $path_2$는 오른손 규칙에 의거하여 경계 지역들을 우회하였다. 이는 s에 의해 전송 메시지 내의 Detouring_Rule 필드에 번갈아 가며 규칙을 배정하기

7) 본 연구에서는 소오스 위치 보호 라우팅 문제에만 집중한다. 라우팅 홀 문제와 이에 대한 보다 나은 해결책이나 평면(planar) 그래프 등으로의 변환 등은 관련 문헌[17-19]에 나와 있다.

```
// Node u that received message M from r, do followings.
// Let variable Mode keep node u's current mode.
// Assume that, initially, u is in greedy mode, i.e, Mode=greedy

1. case 1(Mode == greedy)
   1.1 if (M.Coordinate_of_Destination == L(u))
         accept M and exit; // the destination
   1.2 if (∃ v∈N(u) such that
         M.Coordinate_of_Destination == L(v))
         send M to v and exit; // to the destination
   1.3 if (Mode≠retreat) // set the predecessor node
         Predecessor^s_u = r;
   1.4 if (M.TTL==0 and p≤p_tw for generated random number
       p and given p_tw) { // switch to random_walk mode
         M.TTL=c; // c is a predefined constant
         Mode=random_walk and go to step 3.2;
       }
   1.5 if (∃ v∈N(u) such that (|L(v)-L(b)|<|L(u)-L(b)|) {
       if (v∉AZ(w) for any w) { // greedy mode
           send M to v and exit;
       } else { // go to perimeter mode
           Mode == perimeter and go to step 2.2;
       }
     }
2. case 2(Mode == perimeter)
   2.1 if (∃ v∈N(u) such that (|L(v)-L(b)|<|L(u)-L(b)|)
         and (v∉AZ(w) for any w) { // back to greedy mode
           Mode=greedy, send M to v, and exit;
       }
   // perimeter routing
   2.2 choose v∈N(u) such that v is the first node,
       counterclockwise if M.Detoruing_Rule = left_hand_rule
       or clockwise otherwise, about u from the line ub;
       if (v≠ Predecessor^s_u) { // perimeter mode
         Mode=perimeter;
         send M to v and exit;
       } else {
         Mode=retreat; // switch to retreat mode
         send M to Predecessor^s_u and exit;
       }
3. case 3(Mode == random_walk)
   3.1 x=M.TTL; // let x be a local variable
       x=x-1;
       if (x==0) { // return to greedy mode
         Mode=greedy and go to step 1;
       }
       M.TTL=x; //
   3.2 if (∃ arbitrary v∈N(u) such that (|L(v)-L(b)|<|L(u)-L(b)|)
         ∧ v∉AZ(w) for any w) )
         send M to v and exit; // random_walk mode
       else // switch to perimeter mode
         go to step 2.2;
4. case 4(Mode == retreat)
   N(u) = N(u) - {r}; // avoid cyclic forwarding
   Mode=greedy;
   go to step 1; // back to greedy mode
```

그림 4 GSLP의 다음 홉 노드 선정 과정(전달 노드)

때문인데, 한 가지 규칙만을 적용하면 특정 영역으로 경로가 편중되기 때문이다.

또한, 경로를 구성하는 노드들을 어느 정도 무작위화하기 위해 random_walk 모드가 적용되었다. $path_1$의 경우 u_8에서부터 TTL=3 즉, 3-홉 동안에 현재 노드보다 목적지 b로의 경로 길이가 늘어나지 않는 한 임의의 방향으로 이동하였다(최단 경로를 선정하는 것이 아님). 그런데, u_{10}에 이르러 더 이상 고려할 이웃이 존재하지 않아 retreat 모드로 전환되었고, u_9으로 되돌아와 greedy 모드에서 u_{11}을 선택하였다. 한편, $path_2$에서는 u_{23}에서부터 u_{26}에까지 3-홉만큼 무작위로 이웃 노드가 선정되었다. 이렇게 함으로써 목적지로의 홉 수를 크게 증가시키지 않으면서도 중복해서 동일 노드를 메시지 전달 노드로 선정하는 경우를 줄인다.

이상 설명한 GSLP의 다음 홉 노드 선정 절차를 나타내면 그림 4와 같다. 그림에서는 지면을 줄이기 위해 메시지를 수신한 중간 노드 u에서의 절차만을 보였다. 변수 Mode는 u에서의 다음-홉 선정을 위한 모드를 나타낸다. 기타 사용된 기호는 다음과 같다. s는 소오스(근원지) 노드, b는 기지국(도착지) 노드, M은 전송 메시지이다. M 내의 특정 필드 z를 지칭하기 위해서는 M.z와 같은 형식을 사용한다. 노드 u에 이웃한 노드들의 집합은 N(u)로 표기한다. u의 좌표 값 (x_u,y_u)을 L(u)로 간단히 표현하며, 두 노드 u와 v 사이의 거리를 |L(u)-L(v)|로 나타낸다. ∧는 논리적 연산자 'and', ∃는 '존재한다(there exists)'를 의미한다. $\overline{ub}$는 두 점 u와 b를 연결하는 직선 선분이다. 마지막으로 AZ(p)는 임의의 소오스 노드 p에 의해 설정된 경계 지역 안에 존재하는 노드들의 집합을 나타낸다.

3.2 경로 길이 분석

GSLP에 의해 활동 소오스 s에서 전송된 메시지가 목적지 b에 도착하기까지 경유하는 경로의 길이(즉, 홉 수)를 계산하도록 한다. 길이는 s와 b사이의 최단 경로의 길이에 비해 상대적으로 몇 배가 되는 지로 표현된다.

편의상 그림 4에서와 같이 다음 홉 노드를 선정하는데 있어 greedy 모드가 수행될 확률을 p_g, random_walk 모드가 수행될 확률을 p_{rw-c}, perimeter 모드가 수행될 확률을 p_p, 마지막으로 retreat 모드가 수행될 확률을 p_r이라고 하자. 단, $p_g+p_{rw-c}+p_p+p_r=1$이며, p_{rw-c}는 그림 4에서 greedy 모드에서 random_walk 모드로 전환할 확률 p_{rw}에 대해 $p_{rw-c} \le p_{rw}$이다. 왜냐하면 random_walk 모드로 전환된다고 해서 모두 random walk를 수행하는 것이 아니라 perimeter 모드로 다시 천이할 수 있기 때문이다.

정리: 제안된 GSLP에 의해 설정되는 경로는 최단 경로의 길이에 비해 $\frac{1}{2p_g-1}$배 더 긴 홉 수로 구성된다 (단, $1/2<p_g<1$).

증명: 활동 소오스 s에서 도착지 b까지의 최단 경로의 길이는 d-홉이라고 하고, E(k)를 s로부터 k-홉 이동한 후 그 곳에서 b로의 최단 경로의 홉 수를 나타내자 (k>0). 그러면 맨 처음에는 s에서 아직 움직이지 않았으므로 E(0)=d이다. 이후, 1-홉 이동 한 후에는 $E(1) = E(0)-p_g+(1-p_g) = E(0)+(1-2p_g)$가 성립할 것이다. 왜냐하면 확률 p_g만큼 b에 최단 거리가 되면서, 확률 $(1-p_g)$만큼은 비최단(non-shortest) 거리가 되기 때문이다. 즉, $E(0)=d$, $E(1)=E(0)+(1-2p_g)$, $E(2)=E(1)+(1-2p_g)$, …, $E(k)=$

$E(k-1)+(1-2p_g)d$ 인 관계식들이 성립한다. 고로, 정리하면 $E(k)=d+k(1-2p_g)$를 얻는다. 그런데 k-홉 이동 후 도착지 b에 다 달았다면 $E(k)=0$이므로, 곧 $d=k(2p_f-1)$가 성립된다. 이어서, 우리가 구하는 이동 홉 수 즉, 경로의 길이 k는 다음과 같다.

$$k=\frac{d}{2p_g-1}$$

다시말해, 최단 경로의 길이 d보다 GSLP는 $\frac{1}{2p_g-1}$ 배의 더 큰 경로를 이용한다. 여기서 $2p_g-1>0$ 즉, $1/2<p_g\leq 1$인 조건을 언제나 만족하여야 전송 메시지가 도착지 b에 도착(수렴)한다. 그렇지 않다면 전송 메시지는 계속해서 네트워크 내의 다른 노드로 발산하여 다음-홉을 선정하는 절차가 반복될 것이다. □

예를 들어 $p_g=0.7$이면 $1/(2\cdot 0.7-1) = 1/0.4 = 2.5$이므로 최단 경로보다 2.5배 긴 경로를 사용하여 메시지를 전달할 수 있다. 여기서, 앞서의 연구들[2,4-9]과 같이 단순히 안전 기간만을 늘리기 위해 긴 경로만을 구성하길 원한다면 가능한 p_g값을 1/2에 가깝게 설정하면 된다. 또는, 최단 거리에 비해 몇 배 더 긴 경로를 원하는지를 결정하고 이를 위한 p_g값을 선정할 수도 있다. 하지만 경로 길이가 길어짐으로 인한 과도한 지연 문제를 완화시키고, 또한 메시지 전달 과정 중에 만나게 되는 보호 대상들을 우회하면서 자연적으로 경로 길이가 증가됨을 고려할 때 지나치게 p_g값을 너무 작게 하는 것은 좋은 방법은 아니다. 그리고 이러한 값은 보호 대상이 하나일 때는 설정된 대로 적용이 가능하지만, 보호 대상이 여러 개인 경우에는 경계 지역들이 다수 존재하여 이들에 따른 퍼리미터 라우팅이 빈번히 수행되어 설정된 값의 영향이 줄어들게 된다.

한편, 위의 정리에서 주어진 식은 k의 상한치임에 유의할 필요가 있다. 왜냐하면 random_walk 모드에서도 목적지로의 최단 거리에 해당하는 이웃 노드가 선정될 수 있는데 이를 극히 작다고 가정하여 무시하고, greedy 모드 외의 다른 모드에서 선정되는 다음 홉 노드는 모두 도착지로의 비최단 경로로 이어진다고 가정하였기 때문이다. 위에서 언급된 확률 변수 p_{rw-s}나 random_walk 모드에서 사용하는 TTL는 설정 가능한 값이지만 p_g, p_{rw-c}, p_p와 p_r 등은 실제로는 네트워크 내의 휴면 소오스들(또는 보호 대상들)의 수와 이들의 분포 패턴 등에 따라 다르게 되는 것들이기에 $p_{rw}\approx p_{rw-c}$을 가정하여 근사적인 경로를 추정할 수 있다.

4. 평 가

4.1 환경 설정

아직까지 센서 네트워크에서의 위치 보호와 관련된 성능이나 보호 수준 등을 측정하는 공개된 전용 시뮬레이션 소프트웨어가 없는 이유로 인해 다른 연구들[2-5,8,9]과 마찬가지로 자체적으로 만들었다. Java로 개발된 시뮬레이터는 물리 층이나 MAC(Medium-Access Control) 층의 기능을 포함하지 않는 GSLP와 PR-SP의 라우팅 기능만을 포함하고 있다. 트래픽은 관련 연구들[3,4,8,9]과 마찬가지로 low-duty cycle 모델을 가정하여 s로부터 전송된 메시지가 기지국 b에 도착한 후에 다음 메시지가 발생하도록 하였다. 휴면 소오스들을 무작위로 균등하게 분포되도록 하되 활동 소오스로부터 6r 이내에는 존재하지 않음을 가정 하였다. 시뮬레이션 결과는 평균 차수가 8인 노드 50,000로 구성되는 토포로지 100개를 생성하고 얻어진 값들에 대해 평균을 취하였다. 사용된 주요 파라미터들은 표 1과 같다.

그림 5에 시뮬레이션 동안에 GSLP에 의해 생성된 경로와 공격자에 의한 위치 추적 과정의 스크린 샷을 나타내었다. 공격자의 이동 경로는 굵은 원으로 나타내었고, 일반 메시지 전달 경로는 가는 실선으로 나타내었다. 공격자가 활동 소오스의 위치를 찾기까지 총 538개의 경로가 설정되었고(즉, 안전 기간이 538) 휴면 소오스들은 경계 지역을 우회하는 기능에 의해 모두 보호되다가 최종적으로 활동 소오스의 위치가 노출되면서 메

표 1 파라미터 설정 값

파라메타		값 또는 범위
노드 수, N		50,000
노드의 평균 차수		8
활동 소오스 s와 기지국 b 간의 홉 수, h_{s-b}		30, 40, …, 100
소오스 노드 수, N_s		N의 0.2%, 0.4%, …, 1%
생성 토폴로지 수		100
GSLP	random walk 확률, p_{rw}	0.05
	random walk 홉 수, TTL	h_{s-b}의 [5%, 10%] 중 임의로 선택 (최소값 2)
	경계 지역 반지름, β	2r (r은 전송 거리)
	노출 영역 반지름, α	r
PR-SP	임의의 이동 거리	h_{s-b}의 [25%, 50%]에서 임의로 선택

시지 전송이 종료되었다. 활동 소오스 s와 기지국 b을 잇는 가상의 직선을 고려할 때 경로들이 좌우로 거의 고르게 설정되었음을 볼 수 있다. 따라서 어느 한 쪽으로 추적자가 유도되면 다른 한쪽으로 전송되는 메시지는 추적의 위험 없이 안전하게 전달될 수 있다. 또한, 설정 경로는 "앞뒤 이동(back-and-forth movement)" 이나 "zigzag" 이동 등을 포함하고 있지 않아 추적자의 의심을 낮추는 장점이 있는 데, 이는 대표적인 기존 연구들[3-6,9,11]의 단점과는 다른 것이다. 휴면 소오스 노드들의 수(= 보호 대상자들의 수) N_s는 전체 노드 수 N의 0.6%에 불과한 경우지만 많은 경계 지역들(포획 영역을 포함하여)로 채워져 있음을 알 수 있다. 실제로, N_s가 N의 1% 이상인 경우, 경계 지역을 우회하는 기능이 없는 PR-SP에 의한 경로 설정은 거의 불가능하였다. 또한 기존 연구[2-6,8,9,11]에서는 단지 하나의 보호 대상만을 고려한 점, 그리고 보호 대상의 수는 네트워크 내의 노드 수에 비해 일반적으로 굉장히 작다는 점을 고려하여 N의 1%일 때까지만 고려하였다.

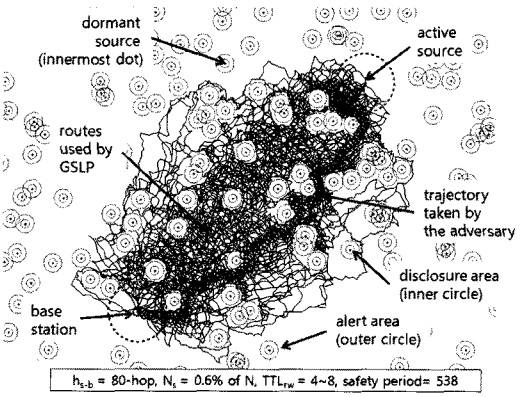


그림 5 위치 추적 과정 스크린 샷

4.2 안전 기간

시뮬레이션을 통해 얻어진 GSLP와 PR-SP의 안전 기간을 나타내면 그림 6과 같다. 각각의 경우를 구분하기 위해 그림의 우측에 적용된 라우팅 프로토콜 이름과 그 때의 활동 소오스 s와 기지국 b간의 홉 수 h_{s-b}를 괄호 안에 넣었다. 가장 큰 특징은 GSLP는 N_s의 증가에 관계없이 거의 일정한 수준의 안전 기간을 유지하나, PR-SP는 소오스 노드 수의 증가에 따라 급속히 감소한다는 것이다. GSLP는 경계 지역을 우회하면서 휴면 소오스들의 위치를 보호하는 능력이 있지만 PR-SP는 이러한 기능이 없기 때문에 N_s의 증가에 따라 경계 지역은 많아짐에 따라 노출 영역에 진입하는 경우가 더 많아져 안전 기간이 빨리 종료될 수밖에 없기 때문이다.

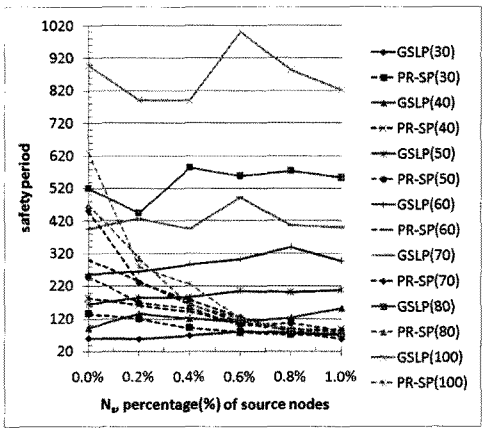


그림 6 GSLP와 PR-SP의 안전 기간 비교

둘째로, GSLP의 안전 기간은 h_{s-b}가 증가할수록 비례하여 늘어나므로 대규모 네트워크에 적합하다. 또한 h_{s-b}>60이며 N_s>0.3%인 모든 경우에서 PR-SP보다 월등히 높은 안전 기간을 제공한다. 하지만 PR-SP은 h_{s-b}를 늘리더라도 N_s의 증가에 더 민감하여(경계 지역을 우회하는 기능이 없으므로) 낮은 안전 기간을 보였다. 셋째로, GSLP의 경우 h_{s-b}>70에 대해 N_s값에 정비례하지 않으며 안전 기간의 격차가 다소 벌어진다. 이는 설정되는 경계 지역들의 모양들이 임의의적이긴 하지만 때로는 클러스터링될 수 있고 그러한 경우의 우회하는 거리는 h_{s-b}가 클수록 더 안전 길이를 길게하기 때문인 것으로 해석된다. 넷째로, PR-SP는 N_s가 N의 1%에 다다른 경우에 h_{s-b}에 관계없이 모두 70~90 범위의 낮은 안전 기간으로 수렴하는 특성을 보였다(이 역시 경계 지역을 우회하는 기능이 없기 때문).

한편, N_s이 0에 가까우며 상대적으로 작은 h_{s-b}에 대해서는 PR-SP가 GSLP보다 더 높은 안전 기간을 제공하였다. 그 이유는 다음과 같이 설명된다. GSLP에서는 경계 지역을 우회하는 경우나 퇴각하는 경우를 제외하고는 언제나 도착지에 가까운 방향으로 이동한다. 하지만, PR-SP에서는 일정 거리[8]를 임의의 방향으로 이동한 후에 최단 거리 라우팅을 실시하므로 h_{s-b}가 상대적으로 짧거나 N_s도 상대적으로 작은 경우에는 경계 지역을 만나지 않으면서 GSLP보다 더 긴 경로를 설정할 수 있어 안전 기간이 증가된다. GSLP에서의 이러한 문제는 p_{rw}와 TTL을 늘려 개선할 수 있다. 하지만 이번 실험에서는 대규모 센서 네트워크에서의 휴면 소오스 노드들의 증가에 따른 안전 기간과 전달 지연을 평가하는

8) 본 시뮬레이션에서는 표 1에 나타나듯이 메시지 전송 시마다 random walk의 길이를 h_{s-b}의 [25%, 50%]의 범위에서 임의로 선택하도록 하였는데 이는 값을 고정시키는 경우보다 PR에 매우 유리한 조건이다.

것에 목적을 두었기에 추후 연구로 미루었다[12].

4.3 전달 지연

그림 7에 평균 전달 지연(즉, 사용 경로의 평균 홉 수)을 나타내었는데, 두 프로토콜에서 모두 활동 소오스 s와 기지국 b 사이의 거리 h_{s-b}가 늘어남에 따라 전달 지연도 비례하여 늘어났다. 하지만, PR-SP의 경우에는 휴면 소오스들의 증가와 거의 무관하게 h_{s-b}에만 비례하는 전달 지연을 보여주었다. PR-SP는 휴면 소오스의 존재와 관계없이 경로를 설정하므로 경계 지역을 만나지 않고 성공적으로 메시지를 전달한 경우의 경로들만이 안전 기간을 증가시키기 때문에 N_s의 값보다는 h_{s-b}의 값에 영향을 받았기 때문이다.

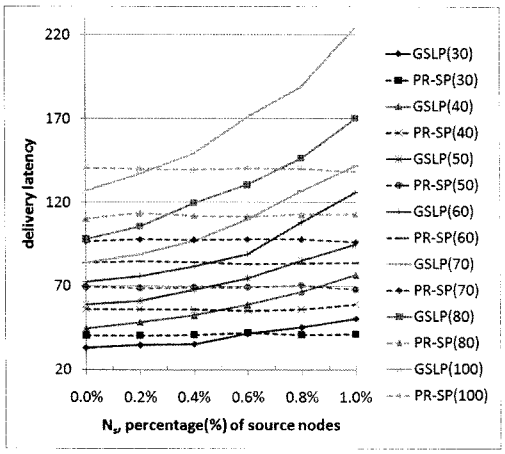


그림 7 GSLP와 PR-SP의 전달 지연 비교

4.4 종합 검토

그림 6과 그림 7을 종합하여 보면, GSLP의 전체적인 지연 폭은 안전 기간의 증가에 비해 상대적으로 높지 않다고 할 수 있다. 예를 들어, GSLP는 PR-SP에 비해 안전 기간을 최대인 약 11배(=822/71) 이상 증가시킨 경우에도(그림 7에서 h_{s-b}=100, N_s가 N의 1% 즉, 500개일 때) 전달 지연은 PR-SP에 비해 1.6(=224/138)배 이상 증가하지 않았다. 즉, 증가된 안전 기간에 비해 전달 지연의 증가는 매우 낮다. 이러한 특징은 perimeter 모드나 retreat 모드를 제외하고는 언제나 도착지로 가까운 노드를 다음 홉 노드로 이용하기 때문에 안전 기간이 증가하더라도 전달 지연은 어느 정도 억제되고 있는 것으로 해석된다. 또한 GSLP의 전달 지연은 h_{s-b}>80일 때 약 2배를 크게 넘지 않았고, 나머지에 대해서는 2배에 크게 미치지 않았다.

결론적으로 제안된 GSLP는 기지국(도착지)과의 거리가 비교적 먼 대규모 센서 네트워크에서 휴면 소오스 노드들이 존재하는 경우 과도한 메시지 전달 지연을 초래하지 않으면서 일정 수준의 안정적 안전 기간을 활동 소오스에게 제공한다고 평가할 수 있다. 기존의 대표적인 소오스 위치보호 라우팅 기법인 PR-SP과 제안된 GSLP를 간추려 비교하면 표 2와 같다.

5. 결 론

본 논문에서는 메시지 전송은 진행하고 있지 않지만 위치가 보호되어야 할 대상과 근접한 휴면 소오스 노드들을 고려한 환경에서의 소오스 노드의 위치 보호를 강화하기 위한 라우팅 기법 GSLP(GPSR-based Source-Location Privacy)를 제안하였다. 기본적으로 위치 기반 라우팅이 가능한 GPSR을 이용하되 메시지 전송 노드로 하여금 확률적으로 목적지로의 길이를 증가시키지 않는 노드들 중의 어느 하나를 임의로 선정하도록 하였다. 또한, 퍼리미터 라우팅을 이용하여 휴면 소오스 노드들을 우회하며, 왼손 규칙과 오른손 규칙을 번갈아 사용하도

표 2 기존의 대표적 방법 PR-SP와 제안된 GSLP의 비교

구분 \ 방법	PR-SP[3,4]	GSLP
개요	라우팅 전반부는 임의의 곳으로 이동한 후, 목적지로 라우팅 하는 두 과정으로 구성	탐욕적 송출, 임의의 이동 및 퍼리미터 라우팅 등을 혼합 적용하는 단일 과정의 라우팅
특징	보호 대상이 하나만 존재하는 경우의 소오스 위치 보호 라우팅	보호 대상이 여러 개 존재하는 경우의 소오스 위치 보호 라우팅
장점	· 비교적 짧은 거리의 통신에서 소오스의 위치 보호에 유리 · 프로토콜이 간단	· 비교적 먼 거리의 통신에 있어 소오스 위치 보호에 유리 · 경로길이 대비 안전기간이 우수 · 경로의 모양이 앞뒤 또는 좌우로 오실레이션(oscillation)할 가능성이 낮아 추적자의 의심을 저감시킴
단점	· 보호 대상이 다수 존재하는 환경에서 낮은 안전기간을 제공 · 지연시간 대비 안전기간이 낮음 · 경로 전개 시 앞뒤 또는 좌우로 오실레이션이 발생하여 추적자로 하여금 의심을 살 수 있음	· 짧은 거리의 통신 시 소오스의 위치 보호 능력이 낮음 · 프로토콜이 상대적으로 복잡

록 하여 설정 경로들이 특정 영역에 쏠리지 않고 무작위화 되면서 보호 대상들의 위치가 추적과정에서 노출되지 않도록 하였다. 그밖에 메시지 전달과정에서는 탐욕적 송출을 수행하도록 하여 경계 지역을 우회하거나 임의의 이동을 통해 길어지는 경로 길이를 어느 정도 상쇄하도록 하여 전달 지연을 억제하도록 하였다. 시뮬레이션을 통해 휴면 소오스 노드들의 수가 전체 노드의 1.0% 이하인 모든 경우에서 제안된 GSLP는 평균 전송 지연은 소오스와 기지국 간의 홉 수의 두 배 정도를 크게 벗어나지 않으면서도 기존의 PR-SP와 같은 방법과 달리 휴면 소오스들의 수의 증가에 무관하게 상대적으로 높은 소오스 위치 보호 능력(안전 기간)을 일정하게 유지하였다. 제안된 GSLP는 대규모 센서 네트워크에서 휴면 소오스 노드들이 존재하는 경우 일정 수준의 안정적 안전 기간을 활동 소오스 노드에 제공하는 방안이라 할 수 있다.

추후 연구로 활동 소오스와 기지국 간의 거리가 짧은 경우에 안전 기간을 늘리기 위한 적합한 TTL과 p_{rw}를 결정하는 것이다. 가장 간단한 방법으로는 이들의 값을 늘리는 것이지만 이는 경로 길이를 또한 증가시키므로 적절한 절충이 필요할 것이다. 활동 소오스 수를 여러 개로 확장한 경우의 안전 기간과 전달 지연 등에 관한 연구 그리고 활동 소오스가 이동하는 경우, 기지국을 여러 개 존재하는 경우 등을 고려한 확장이 필요하다.

참 고 문 헌

[1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, Vol.1, pp.293-315, 2003.

[2] J. Deng, R. Han, and S. Mishra, "Countermeasures against traffic analysis attacks in wireless sensor networks," *Proc. of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp.113-126, 2005.

[3] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," *Proc. of the 2nd ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN'04)*, pp.88-93, 2004.

[4] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor network routing," *Proc. of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS'05)*, pp.599-608, 2005.

[5] L. Zhang, "A self-adjusting directed random walk approach for enhancing source-location privacy in sensor network routing," *Proc. of the ACM International Wireless Communication and Mobile Computing Conference(IWCMC'06)*, pp.33-38, 2006.

[6] Y. Xi, L. Schwiebert, and W. Shi, "Preserving source location privacy in monitoring-based wireless sensor networks," *Proc. of the 2nd International Workshop on Security in Systems and Networks(SSN'06)*, pp.25-29, 2006.

[7] B. Hoh and M. Gruteser, "Protecting location privacy through path confusion," *Proc. of the 1st International Conference on Security and Privacy for Emerging Areas in Communications Networks*, pp.194-205, 2005.

[8] Y. Ouyang, Z. Le, G. Chen, and J. Ford, "Entrapping adversaries for source protection in sensor networks," *Proc. of the 7th IEEE International Symposium on a Word of Wireless, Mobile and Multimedia Networks(WoWMoM'06)*, pp.23-32, 2006.

[9] Y. Jian, S. Chen, Z. Zhang, L. Zhang, "Protecting receiver-location privacy in wireless sensor networks," *Proc. of the 26th IEEE Conference on Computer Communications(INFOCOM'07)*, pp.1955-1963, 2007.

[10] K. Mehta, D. Lie, and M. Wright, "Location privacy in sensor networks against a global eavesdropper," *Proc. of the 15th IEEE International Conference on Network Protocols(INCP'07)*, 2007 (Session VIII, #4).

[11] P. Kamat, W. Xu, W. Trappe, and Y. Zhang, "Temporal privacy in wireless sensor networks," *Proc. of the 27th IEEE International Conference on Distribute Computing Systems(ICDCS'07)*, pp.23, 2007.

[12] Y. Tscha, "Routing for enhancing source-location privacy against packet-tracing in wireless sensor networks of multiple assets," (*submitted for possible publication, available on request*), 2008.

[13] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, Vol.52, Issue12, 2008, pp.2292-2330.

[14] B. Karp and H.-T. Kung, "Greedy perimeter stateless routing for wireless networks," *Proc. of the 6th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'00)*, pp.243-254, 2000.

[15] Y.-B. Ko, and N. Vaidya, "Geocasting in mobile ad hoc networks: location-based multicast algorithms," *Proc. of 2nd IEEE Workshop on Mobile Computing Systems and Applications(WMCSA99)*, pp.101-110, 1999

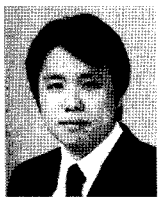
[16] K. Obraczka, K. Viswanath, and G. Tsudik, "Flooding for reliable multicast in multi-hop ad hoc networks," *Wireless Networks*, Vol.7, 2001, pp.627-634

[17] Z. Jiang, J. Ma, W. Low, and J. Wu, "An information model for geographic greedy forwarding in wireless ad-hoc sensor networks," *to appear in the 27th IEEE Conference on Computer Communications(INFOCOM'08)*, 2008.

[18] N. Asmed, S. Kanhere, and S. Jha, "The holes

problems in wireless sensor networks: a survey," *ACM SIGMOBILE Mobile Computing and Communication Review*, Vol.9, No.2, pp.4-18, 2005.

[19] H. Frey and I. Stojmenovic, "On delivery guarantees of face and combined greedy-face routing in ad hoc and sensor networks," Proc. of the 12th Annual ACM/IEEE International Conference on Mobile Computing and Networking(MobiCom'06), pp.390-401, 2006.



양 기 원

2008년 상지대학교 컴퓨터정보공학부(학사). 2008년~현재, 한국정보통신대학교 석사과정. 관심분야는 센서 네트워크, 차세대 인터넷 기술, P2P 응용, 인터넷 보안

임 화 정

1999년 상지대학교 행정학과(학사). 2003년 상지대학교 컴퓨터정보공학과(석사) 2009년 강원대학교 컴퓨터정보통신공학과(박사). 2003년~현재 상지대학교 컴퓨터정보공학부 강사. 2007년~현재 상지대학교 전자정부학과 강사. 2007년~현재 한림성심대학교 인터넷비즈니스과 강사. 관심분야는 센서 네트워크, 유비쿼터스 시스템 및 보안

차 영 환

1983년 인하대학교 전자계산학과(학사) 1985년 한국과학기술원(KAIST) 전산학과(석사). 1993년 인하대학교 대학원 전자계산학과(박사). 1985년~1990년 한국전자통신연구원(ETRI), 선임연구원. 1986년~1987년, 미국 NIST 객원 과학자. 2004년~2005년, 터어키 Boğaziçi 대학교 객원 교수. 1994년 3월~현재, 상지대학교 컴퓨터정보공학부 교수. 관심분야는 네트워크 구조, 통신 프로토콜, 네트워크 보안