

## 휴면 소오스들이 존재하는 환경에서의 위치 보호 라우팅

양기원<sup>○</sup> 신성 김다영 박상주 임화정<sup>▲</sup> 차영환<sup>▲</sup>  
 상지대학교 컴퓨터정보공학부 <sup>▲</sup>강원대학교 컴퓨터정보통신공학과  
<sup>○</sup>giwonej@hotmail.com <sup>▲</sup>lim1108@hanmail.net <sup>▲</sup>yhtscha@sangji.ac.kr

### Routing for Location Privacy in the Presence of Dormant Sources

G. Yang<sup>○</sup> S. Shin D. Kim S. Park H. Lim Y. Tscha  
 School of CIC Engineering/Sangji Univ. <sup>▲</sup>Dep't of CSE/Kangwon Univ.

전장에서 임무 수행중인 병력이나 탱크 등을 지원하거나 보호 동물의 활동을 모니터링 하는 센서 네트워크에서는 전송 정보뿐만 아니라 그러한 대상들의 위치를 악의적 추적자로부터 보호할 수 있어야 한다. 본 논문에서는 활동 소오스 노드처럼 메시지 전송은 진행하고 있지 않지만 위치가 보호되어야 할 대상과 근접한 휴면(dormant) 소오스 노드들을 고려한 소오스 위치 보호 라우팅 기법 GSLP(GPSR-based Source-Location Privacy)를 제안한다. GSLP는 알고리즘의 간결성과 신장성(scalability)이 뛰어난 GPSR(greedy perimeter stateless routing)을 확장하여 메시지 전달 노드를 선정할 때 일정 확률로 임의의 이웃 노드를 선택하는 한편, perimeter 라우팅을 적용하여 소오스 노드들을 우회하도록 하여 위치를 보호하도록 하였다. 시뮬레이션 결과, 기존의 대표적인 소오스 위치 보호 라우팅 프로토콜인 PR-SP(Phantom Routing-Single Path)에 비해 GSLP는 휴면 소오스 노드들의 수에 거의 관계없이 높은 안전 기간(전송 메시지 수)을 일정하게 제공하면서도 전달 지연(경로의 평균 홉(hop) 수)은 도착지와 의 최단 홉 수의 약 두 배 이내에 머물러 대규모 센서 네트워크에서의 소오스의 위치를 보호하기 위한 방안으로 적합한 것으로 평가되었다.

#### 1. 서 론

대규모의 다양한 응용들을 지원하는 센서 네트워크에서는 적시의 데이터 수집과 제어를 위한 효율성 높은 실시간 통신 기능이 필수적이다. 하지만 무선 통신 자체가 갖는 전송 신호의 노출 문제, 관련 장비의 포편화 및 소형화, 그리고 설치 공간이 대부분 옥외라는 특징 등은 제한된 컴퓨팅 능력으로 한정된 에너지를 사용하여야 하는 센서 네트워크에서의 보안 문제 역시 매우 중요하다[1]. 암호화 기법을 이용하여 전송 정보의 내용을 보호하는 전통적 의미의 보안도 필요하지만 통신 노드들의 위치나 트래픽의 양이나 유형 등과 같은 문맥 정보(contextual information)의 보호도 응용에 따라 매우 중요하다. 예를 들어, 전장에서 임무 수행중인 병력이나 탱크 등을 지원하거나 희귀 동물의 활동을 감시하는 응용에서는 전송 메시지가 암호화 되어 있다 하더라도 송신자의 위치가 적이나 밀렵꾼 등에 노출되게 되면 그 피해는 심각할 수 있다.

본 논문에서는 기지국으로 메시지를 전송하는 활동 소오스의 위치를 local eavesdropper로부터 보호하기 위한 라우팅 방안을 제안한다. 기지국은 센서 네트워크의 중심이 되는 노드로서 각종 노드에서 발생한 트래픽이 집중화 되고 외부 서버나 네트워크에 연결되는 장비이므로 그 위치가 쉽게 탐지될 수 있다[2]. 따라서 기지국의 상대방인 소오스 노드의 위치 보호가 무엇보다도 우선되어야 한다. 본 논문의 기여 부분은 다음과 같다.

- 휴면(dormant) 소오스 노드들이 존재하는 환경을 고려하였다. 다른 연구[3]에서 소오스 노드로 일컫던 즉, 기지국으로 정보를 전송 중인 노드를 활동(active) 소오스 노드로 정의하는 반면, 정보 전송은 하고 있지 않지만 추적자가 일정 거리 이내에 근접하면 그 위치가 탄로 나는 보호 대상에 인접한 노드를 휴면(dormant) 소오스 노드라고 정의하였다).
- 라우팅 프로토콜로는 위치 기반 라우팅이 가능하고 구현이 용이하여 대규모 네트워크로의 적용이 가능한 GPSR(Greedy Perimeter Stateless Routing)[4]을 확장하여 사용하였다. 최단 거리 라우팅을 지향하는 greedy forwarding과 확률적으로 일정 홉 거리를 무작위로 전계하는 임의의 이동 과정을 적용하는 한편, 휴면 소오스 노드들은 perimeter 라우팅 기법을 이용하여 우회하도록 하였다. 이로 인해 위치 보호 수준을 높이도록 하면서도 긴 경로를 이용하는 경우 발생하는 전달 지연을 가능한 억제하도록 하였다.

#### 2. 휴면 소오스를 고려한 위치 보호 라우팅

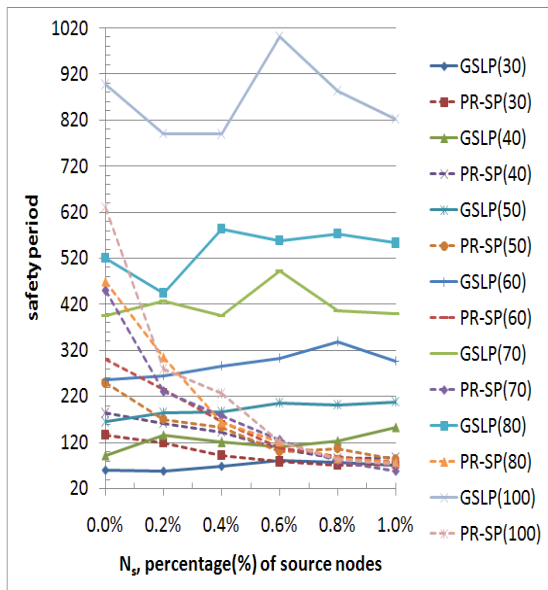
네트워크에는 하나의 기지국이 존재하며 공격자에게 그 위치가 노출되어 있다고 가정한다. 보호 대상의 발현을 감지한 노드들은 기지국으로의 메시지 전송에 앞서 자신으로부터 거리  $\beta$  ( $\beta > r$ ,  $r$ :신호 전송 거리) 이내의 노드들에게 보호 대상이 근처에 존재하므로 메시지 전송 과정에서 해당 영역을 우회할 것을 나타내는 경계 지역(alert zone)을 설정한다. 제안된 라우팅 기법 GSLP(GPSR-based Source-Location Privacy)에서는 다음과 같이 4개의 서로 다른 모드로 메시지 전달을 위한 다음-홉(next-hop) 노드를 선정한다.

1) 관리 또는 보호 대상을 인지하고 지역적 모니터링이나 내부적인 이벤트를 처리 중인 노드를 표현하기 위해 "휴면 소오스"의 개념을 도입한다. 예를 들어, 전장에 투입된 병력이나 탱크 등은 기지국과의 통신과 관계없이 그 위치가 공격자나 추적자에게 탄로 나지 말아야 되는 물체이다. 이러한 응용의 센서 네트워크에서는 라우팅 차원에서 이들의 위치를 보호할 메커니즘을 강구할 필요가 있다.

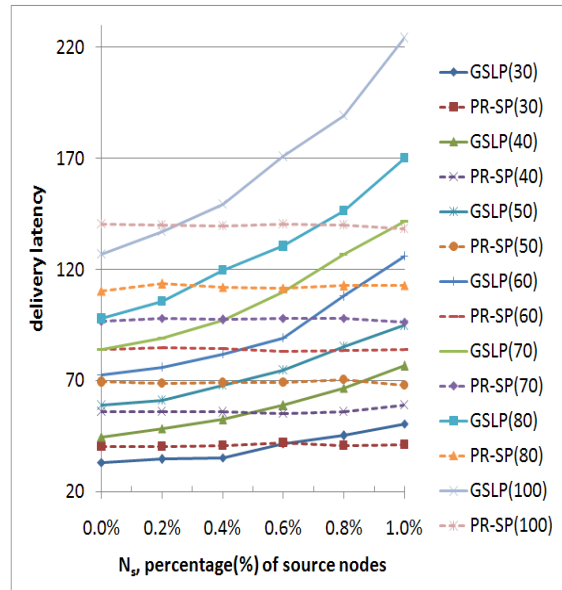
- Greedy 모드: Greedy forwarding에 해당하며 도착지로의 메시지 전달 지연을 억제한다.
- Perimeter 모드: GPSR [4]의 perimeter 라우팅을 이용하여 경계 지역을 우회하여 소오스의 위치를 보호한다. right-hand와 left-hand 규칙을 경로별로 번갈아 사용하여 경로들이 특정 영역으로만 설정되지 않게 한다.
- Random\_walk 모드: greedy 모드에서는 확률  $p_{rw}$ 로 임의의 이웃 노드를 다음 노드로 선정한다( $0 < p_{rw} < 1$ ). 이 모드가 진행되면  $TTL_{rw}$  홉 수만큼 반복하여 다양한 노드들이 여러 경로에 이용되게 한다.
- Retreat 모드: 더 이상의 경로 전개가 불가피하여 이전의 노드로 다시 되돌아가 greedy 모드로 환원된다.

### 3. 위치 보호 수준 및 성능 평가

제안 프로토콜의 평가를 위해서는 안전 기간(활동 소오스의 위치가 발각되기 전까지 전송한 메시지 수)과 메시지 전달 지연(경로의 평균 홉 수)을 측정하였고, 대표적인 소오스 위치 보호 라우팅 기법인 PR-SP(Phantom Routing, Single Path) [3]과 비교하였다. 시뮬레이션에서는 평균 차수(degree)가 8인 노드 50,000개로 구성되는 네트워크 토폴로지 100개를 생성하여 사용하였다. 소오스 노드 수  $N_s$ 는 전체 노드의 0.2%에서부터 1%까지, 그리고 메시지를 전송하는 액티브 소오스 노드와 기지국 간의 거리(홉 수)  $h_{s-b}$ 는 30에서부터 100까지를 고려하였다. 제한한 GSLP의 안전 기간은  $N_s$ 가 증가할 수 록 그리고  $h_{s-b}$ 가 길어질 수 록 PR-SP에 비해 최고 11배까지 늘어났다(그림 1). GSLP에서는 휴면 소오스들의 수에 거의 무관하게 일정 수준의 안전 기간을 유지하였는데, 경계 지역을 우회하면서 휴면 소오스들의 위치를 보호하는 능력이 있지만 PR-SP는 이러한 기능이 없기 때문에  $N_s$ 의 증가에 따라 경계 지역은 많아져 이에 진입하는 경우가 늘어나 안전 기간이 조기에 종료되었다. 전달 지연의 경우, GSLP의 모든 경우는  $h_{s-b}$ 가 늘어남에 따라 비례하여 늘어났다(그림 2). 하지만, PR-SP의 경우에는 휴면 소오스들의 증가와 거의 무관하게  $h_{s-b}$ 에만 비례하였다. PR-SP는 휴면 소오스의 존재와 관계없이 경로를 설정하므로 경계 지역을 만나지 않고 성공적으로 메시지를 전달한 경로들만이 안전 기간을 증가시키기 때문에  $N_s$ 의 값보다는  $h_{s-b}$ 의 값에만 영향을 받았기 때문이다. 하지만, GSLP의 평균 전달 지연은 활동 소오스와 기지국 사이의 홉 수에 2배를 크게 넘지 않아 안전 기간의 증가 비율에 훨씬 못 미쳤다. GSLP는 기지국(도착지)과의 거리가 비교적 먼 대규모 센서 네트워크에서 휴면 소오스 노드들이 존재하는 경우 일정 수준의 안정적 안전 기간을 활동 소오스에 제공하는 라우팅 방안이라고 결론 내릴 수 있다.



[그림 1] 안전 기간(전달 메시지 수) 비교



[그림 2] 전달 지연(평균 경로 홉 수) 비교

### 참 고 문 헌

- [1] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," *Ad Hoc Networks*, Vol.1, 2003, pp.293-315.
- [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*, 2005, pp.113-126.
- [3] P. Kamat, Y. Zhang, W. Trappe, and C.I. Ozturk, "Enhancing source-location privacy in sensor network routing," *Proc. of the 25th IEEE International Conference on Distributed Computing Systems(ICDCS'05)*, 2005, pp.599-608.
- [4] 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)*, 2000, pp. 243-254.

이 논문은 2007년도 정부(교육인적자원부, 현 교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2007-521-D00409)