# 무선 센서 네트워크에서의 통신 근원지 및 도착지 은닉(제2부) : 프로토콜 평가

차영환*

# Concealing Communication Source and Destination in Wireless Sensor Networks (Part I) : Protocol Evaluation

Yeong-Hwan Tscha*

요 약

대규모 무선 센서 네트워크에 있어서 광역도청에 대응하여 통신 근원지와 도착지의 위치기밀을 유지하기 위해서는 흔히 과다한 더미패킷들이 발생된다. 앞서의 연구에서는 데이터패킷 전송 동안에 근원지와 도착지를 포함하는 일정 범위 내의 노드들만이 빈 타임-슬롯마다 더미패킷을 발생하도록 하는 위치보안 라우팅 프로토콜 ELPR(End-node Location Privacy Routing)을 제안하였다. 이 논문에서는 고정된 보안성을 갖는 PCM(Periodic Collection Method)에 비해 ELPR은 다양한 위치보안 수준을 제공함을 보였다. 시뮬레이션을 통해 ELPR은 노드들의 수나 데이터패킷들이 많은 경우, PCM보다 발생 패킷 수에 있어서 경제성 있는 위치보안이 가능함을 확인하였다.

ABSTRACT

In large-scale wireless sensor networks, tremendous amount of dummy packets is usually accompanied by keeping location privacy of the communication source and destination against global eavesdropping. In our earlier work we designed a location privacy routing protocol, ELPR(End-node Location Privacy Routing) in which the generation of dummy packets at each idle time-slot while transferring data packets are restricted to only the nodes within certain areas of encompassing the source and destination, respectively. In this paper, it is given that ELPR provides various degrees of location privacy while PCM(Periodic Collection Method) allows the only fixed level. Simulation results show that as the number of nodes or data packets increases ELPR permits in terms of the number of generated packets more cost-effective location privacy than PCM.

키워드

Global eavesdropping, Location privacy of source and destination, Protocol design and evaluation
광역도청, 근원지 및 도착지 위치기밀, 프로토콜 설계 및 평가

## Ⅰ. 서 론

희귀동물의 위치를 추적하거나 전장에서 작전 중인 병력 또는 이동체의 위치를 모니터링 하는 무선 센서 네트워크 응용 등에서는 보호 대상들의 위치보안(location privacy)이 내용보안 못지않게 중요하다[1]. 만약 밀렵꾼이나 적에게 이들의 위치가 노출되는 경우 생존의 위협을 받게 될 것이다. 정보를 생성하는

* 상지대학교 컴퓨터정보공학부(yhtscha@sangji.ac.kr)
접수일자 : 2012. 11. 25 심사(수정)일자 : 2013. 02. 20 게재확정일자 : 2013. 03. 22

노드(node)인 근원지(source)나 생성 정보의 최종 수신 노드인 도착지(destination) 즉, 기지국(basestation)의 위치기밀을 라우팅 차원에서 유지하기 위한 지금까지의 연구들은 공격자의 신호감지 능력이 일반 노드가 패킷(packet)을 송수신 할 때, 감지할 수 있는 최대거리와 동일한 지역도청(local eavesdropping)을 대상으로 하였다[2],[3]. 즉, 공격자는 패킷이 전송될 때마다 발생하는 신호를 감지하고 이를 따라 추적함으로써 근원지나 도착지의 위치를 찾아내는 수동적 지역도청에 의한 위치추적자였다. 보다 일반적인 경우에 대한 연구의 필요성은 물론, 무선 및 도청 관련기술의 발전에 따라 감시대상을 네트워크 전체로 확대한 광역도청(global eavesdropping)을 고려하는 경우에는 보다 강력한 위치보안기능을 제공하는 라우팅 프로토콜이 요구된다[4].

PCM(Periodic Collection Method)[4]는 광역도청에 대응하여 가장 높은 위치보안성을 제공한다. 네트워크 내의 모든 노드들은 일정 시각마다 패킷을 발행하는데, 전송할 데이터가 있는 노드는 데이터패킷을 전송한다. 데이터패킷을 수신한 경우에는 이를 이웃 노드로 전파한다. 다만 데이터 패킷을 수신하지 않았거나 전송할 데이터가 없는 노드는 데이터패킷과 동일한 크기의 더미패킷(dummy packet) 즉, 수신자도 지정되어 있지 않으며 패킷 내용도 의미 없는 정보로 채워져 단지 데이터패킷이 전송되는 것과 같은 신호를 발생시키는 패킷을 전송하여 도청자가 근원지나 도착지를 찾는데 혼선을 갖도록 한다. 이러한 과정이 매 타임-슬롯(time-slot)마다 반복 수행됨에 따라 근원지에서 발행한 패킷은 결국 도착지에 이르게 되는데, 이 동안에 근원지나 도착지가 다른 노드와 구별이 되지 않으므로 그들의 위치보안이 유지된다.

선행 연구[5]에서는 ELPR(End-node Location Privacy Routing)이라는 라우팅 기법을 제안하였다. 특징으로는 데이터패킷 전송 동안에 근원지와 도착지를 포함하는 각기 원(disk) 모양의 위치보호구역(location privacy zone)내의 노드들과 보호구역 밖의 데이터패킷 전송경로 상의 노드들만 데이터패킷 또는 더미패킷을 발행한다. 보호구역의 크기를 필요에 따라 증감할 수 있기 때문에 패킷 발생비용을 감축할 수 있음은 물론, 원하는 수준의 근원지나 도착지의 위치보호가 가능하다.

이 연구에서는 위치보안성과 통신비용(즉, 위치보안을 위해 네트워크 내에서 발생되는 모든 패킷들의 수)을 평가 척도로 하여 ELPR과 경쟁 프로토콜 PCM을 비교한다. 엔트로피(entropy) 개념에 따른 위치보안성 분석에서는 고정된 보안성을 갖는 PCM에 비해 ELPR이 다양한 위치보안 수준을 설정할 수 있는 융통성이 있다. 통신비용의 경우 네트워크 내의 노드들의 수나 전송 데이터패킷이 많을수록 ELPR이 PCM보다 경제성 있는 통신비용으로 근원지와 도착지의 위치 기밀을 제공한다. ELPR의 이해를 위한 좀 더 자세한 내용은 참고문헌 [5]에, 광역도청에 의한 위치추적에 관한 일반사항 및 PCM은 참고문헌 [4]에 나와 있다. 도착지는 기지국을 지칭하여 네트워크에 오직 하나만 존재하나, 근원지는 여러 개 존재함을 가정한다.

다음 장에서는 ELPR의 사용 패킷들과 이들을 이용한 동작절차를 소개한다. 3장에서는 ELPR과 경쟁 프로토콜 PCM과의 보안성을 분석한다. 4장에서는 통신비용을 산출한 후, 시뮬레이션을 통한 통신비용을 상호 비교한다. 5장에서 이 연구의 결론을 맺는다.

## II. ELPR 동작과정

### 1) 사용 패킷

ELPR의 동작은 위치보호구역을 설정하는 초기화단계와 데이터를 전송하는 데이터 전송단계로 구성된다. 이 과정에서 사용하는 패킷들의 종류와 용도는 표 1과 같다. 초기화단계에서 사용하는 패킷은 HL(Hello), FP(Flood PZ), PZ(Privacy Zone) 등이며, FR(Flood RR), RR(Receive Ready), FD(Flood DT), DT(Data)는 데이터 전송단계에서 사용된다. F로 시작하는 FP, FR 및 FD는 근원지나 도착지가 자신의 프락시에게 자신을 대신해서 어떠한 역할을 수행해 줄 것을 요청할 때 사용되는 패킷들이며, 발행자로부터 δ-홉 이내의 노드들로만 플러딩(flooding)이 국한된다. DT는 근원지프락시에서 도착지프락시로의 단일 경로 상으로 전달되는 데이터패킷이다. 그 밖의 PZ와 RR은 네트워크 전체로 플러딩 즉, 브로드캐스트 되는 패킷이다.

HL은 프로토콜의 시작과 함께 모든 노드가 자신으로부터 δ-홉 이내의 이웃 노드들에게 자신의 존재를

알리는 용도 외에, 보호구역 내의 노드가 전송할 데이터패킷이 없을 경우에도 발행되는 더미패킷이다. 모든 패킷은 그 용도가 서로 다르나 물리적인 길이가 동일하게 패딩(padding)되어 전달되며, 내용은 적절한 암호화 기법에 의해 기밀이 유지되어 외부 도청자가 내용을 구분해 낼 수 없다고 가정한다[2]-[5].

표 1. ELPR의 패킷과 용도
Table 1. ELPR packets and their usages

| 패킷유형 | 발행자 | 수신자 | 용도 |
|---|---|---|---|
| HL(Hello) | 모든 노드 | 발행자로부터 δ-홉 이내의 노드 | 자신의 존재를 알림. 더미패킷으로도 사용됨 |
| FP(Flood PZ) | 근원지 및 도착지 | 발행자의 프락시 | 위치보호영역이 설정된 것을 알리도록 요청 |
| PZ(Privacy Zone) | 근원지 및 도착지 프락시 | 모든 노드 | 설정된 위치보호영역을 알림 |
| FR(Flood RR) | 도착지 | 발행자의 프락시 | 기지국이 데이터 수신이 가능함을 알리도록 요청 |
| RR(Receive Ready) | 도착지 프락시 | 모든 노드 | 기지국이 데이터 수신이 가능함을 알림 |
| FD(Flood DT) | 근원지 | 발행자의 프락시 | 데이터를 전송할 것을 요청 |
| DT(Data) | 근원지 프락시 | 도착지 | 데이터 패킷 |

### 2) 초기화 단계

ELPR은 초기화단계와 데이터 전송단계를 하나의 세션(session)으로 하여 주기적으로 반복한다. 세션의 동작과정을 설명하기 위해 편의상 근원지를 s 도착지를 d, 근원지의 프락시를 x, 도착지의 프락시를 y라 한다. 그리고 s의 주변에 있는 임의의 노드 z, d의 주변에는 임의의 노드 t를 고려한다.

초기화단계는 그림 1과 같이 모든 노드들이 자신의 존재를 알리는 패킷 HL을 발행하는 것으로 시작된다. HL의 수신범위는 발행자로 부터 δ-홉 이내로 제한되는 데, 이 값은 사전에 설정되거나 또는 기지국(즉, 도착지)가 후속 세션에서 사용할 값을 데이터 전송단계에서 브로드캐스트(broadcast)를 통해 동적으로 알려줄 수도 있다. 전송할 데이터가 있는 근원지 s나 데이터를 수신할 도착지 d는 HL을 수신할 때마다 자신과 HL을 발행한 노드와의 거리 k(>0)가 $0<i_1<i_2<\delta$인 임의의 두 정수 $i_1$와 $i_2$에 대해 $i_1<k<i_2$인 노드이면 일단 프락시 후보로 정한다. 여기서, $i_1$과 $i_2$는 근원지나 도착지로 부터 너무 가깝거나 또는 너무 먼 거리에 위치한 노드가 프락시로 설정되는 것을 방지하기 위해 고려된 파라미터들이다.

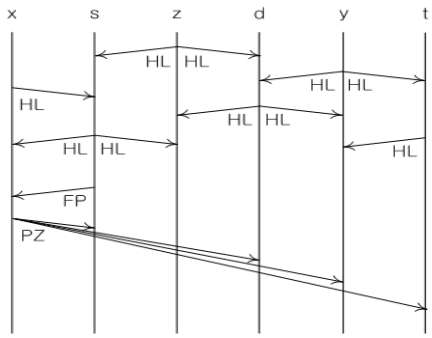



그림 1. 초기화단계
Fig. 1 Initialization phase

일단 프락시 후보가 정해진 뒤에는 위의 조건을 만족하는 또 다른 노드로부터 HL이 수신될 때마다 확률 $p_{proxy}(0<p_{proxy}<1)$로 기존의 것을 대체한다. 일정기간이 경과된 후 최종적으로 남은 것이 프락시가 된다. 자신의 프락시를 갖게 된 근원지 s는 자신의 프락시 x를 통해 자신의 위치보호구역을 네트워크 내의 노드들로 알려줄 것을 요청한다. 이 때 사용되는 것이 FP이며, 이를 수신한 근원지 프락시 x는 PZ를 만들어 브로드캐스트 한다. PZ 내에는 중계 노드를 거칠 때마다 홉 수를 더해주는 필드가 있기 때문에[5], PZ를 수신한 노드는 자신과 PZ를 발행한 근원지프락시와의 거리가 몇 홉인지 알 수 있다. 아울러, PZ를 수신하므로 써 자신이 PZ가 알려준 근원지보호구역에 속하는지 확인도 가능하다.

초기화단계 동안에 모든 노드는 HL을 한번만 발행하는 것이 아니라 FP나 PZ을 발행 또는 중계하지 않는 타임-슬롯에서는 HL을 더미패킷 용도로 지속적으로 발행한다(여기서, 발행(generation)은 해당 패킷의 생성과 이의 전송을 뜻하는 의미이다). 따라서 초기화과정에서는 근원지나 도착지의 위치기밀이 유지된다.

### 3) 데이터 전송단계

데이터 전송단계에서는 크게 두 가지 기능이 수행된다. 첫째, 기지국인 도착지가 데이터를 수신할 준비가 되면 초기화단계에서 정했던 자신의 프락시를 통해 자신의 위치보호구역과 프락시를 네트워크 내의

노드들에게 알린다.

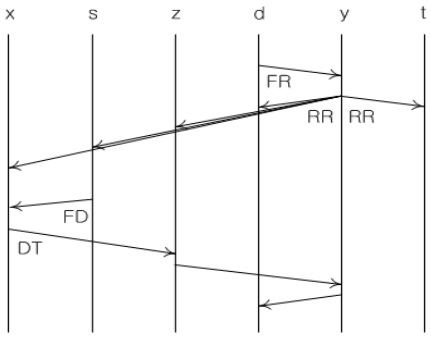



그림 2. 데이터 전송단계 과정
Fig. 2 Data transfer phase

그림 2에서 도착지 d는 자신이 설정한 프락시 y로 하여금 이러한 기능을 수행하기 위해 FR을 발행하였다. FR을 수신한 y는 RR을 생성 브로드캐스트 함으로써 d가 데이터 수신이 가능하다는 것과 도착지보호구역을 알려준다. 그러면 RR을 수신한 각 노드는 도착지 d, 도착지 프락시 y 그리고 향후 y로 데이터패킷을 전송할 때 사용할 자신의 다음-홉(next-hop) 노드를 알게 된다. 여기서, 도착지 프락시 y로 패킷을 전달하기 위한 최단경로상의 다음-홉 노드는 RR을 처음으로 자신에게 전달 해준 이웃 노드이다. 왜냐하면 RR은 브로드캐스트 되기 때문에 자신에게 가장 먼저 RR을 전해준 이웃 노드가 RR을 발행한 도착지 프락시 y로 가는 최단경로상의 노드이기 때문이다[5]. 또한 RR을 수신한 각 노드는 자신과 y간의 거리(즉, 홉 수)를 알기 때문에 그 거리가 δ를 넘으면 도착지 위치보호구역 밖에, 그렇지 않으면 그 내부에 존재하는 것임을 판단할 수 있다. 이로써 자신이 어떠한 보호구역에도 속하지 않는 노드들은 RR을 수신한 이후부터는 더미패킷 HL의 발행을 중지하고 단지 패킷 수신만 가능한 휴면상태(sleeping state)로 전환한다. 이로써 위치보호구역 내에 속하는 노드만 매 타임-슬롯마다 패킷을 발행하게 된다.

둘째로는 근원지 노드 s가 데이터패킷을 발행하는 것이다. 이를 위해서 FD내에 전송 데이터를 넣은 후 δ-홉 이내로 제한된 플러딩을 수행한다. 이때 보호구역내의 다른 노드들은 더미패킷을 발행하므로 근원지의 위치는 노출되지 않으며, 단지 패킷을 발행하는 보호구역내에 근원지가 존재한다는 것만 드러날 뿐이다. FD를 수신한 근원지프락시 x는 자신과 도착지프락시 y 간의 최단경로(RR을 수신할 때 설정된)를 이용하여 데이터패킷 DT를 전달한다. 단, DT에서는 도착지프락시 y로 가기 위한 다음-홉 필드에 수신 노드가 반드시 지정되어야 한다. 따라서 위치보호구역 밖에 존재하며 휴면상태에서 패킷을 수신한 노드 z는 다시 활동 상태로 복귀하여 자신의 다음-홉 노드로 DT를 전달하여야 한다. 근원지프락시 x로부터 도착지프락시 y에 이르기까지 DT를 전달하는 경로는 단일 경로이다. 이러한 경로상의 노드들 중 위치보호구역밖에 존재하는 노드들은 전달할 DT가 없는 타임-슬롯에서 더미패킷을 발행할 필요는 없다.

## III. 위치보안성

광역도청에 대하여 근원지나 도착지의 위치를 노출시키지 않기 위해서는 데이터 전송에 직접관련이 없는 일정한 노드들로 하여금 더미패킷들을 발행하도록 하는 것이 필요하다. 이는 근원지나 도착지를 다른 노드들로 부터 구별해내지 못하게 의도된 것이다. 따라서 근원지나 도착지를 공격자가 찾아낼 확률이 곧 근원지나 공격자의 위치보안성에 직결되므로 위치보안성은 엔트로피(entropy) 정의를 이용하여 평가한다[4]. 즉, 근원지나 도착지의 위치가 발생될 확률을 p라고 하면 그 위치보안성은 $\log_2(1/p)$로 정의한다. 예컨대, 위치보안성이 10이라면 $2^{10}$ = 1024이므로 근원지나 도착지가 발견될 확률은 1/1024임을 뜻한다. 일반적으로 위치보안성은 p가 작을 수록 높아진다.

PCM의 경우 N개의 노드들이 존재하는 네트워크에 있어서 모든 노드가 항상 매 타임-슬롯마다 패킷을 생성하므로 근원지나 도착지를 찾아낼 확률은 1/N이다. ELPR의 위치보안성을 분석하기 위해서는 반지름이 δ인 원 모양의 위치보호영역 내의 노드들의 수를 구하여야한다. 이를 위해 노드들의 밀도가 충분히 크며 네트워크 역시 위치보호구역처럼 원의 형태임을 가정한다.

성질 1 : N개의 노드들이 원의 형태로 형성되어있는 무선 네트워크에서의 ELPR이 제공하는 위치보안

성은 $\log_2 N - 2\log_2(1/\rho)$이다. 단, $0<\rho<1$이다.

증명: 네트워크 전체를 R-홉을 반지름으로 하는 원으로 간주하고, 모든 위치보호구역은 반지름이 δ-홉인 원들로 고려하자. 관련 연구[2],[4],[7]에서와 같이 전체 노드들의 수 N에 비해 위치보호가 필요한 노드들(즉, 근원지들과 도착지)의 수는 극히 적고 네트워크 내에 고루 편재되어 있어 위치보호구역들이 서로 겹치지 않는다고 가정한다. 네트워크 내의 노드들의 수 N에 대해 하나의 보호구역 내에는 $(S_{privacy_zone}/S_{network})N$개의 노드들이 존재한다. 여기서, $S_{Privacy_Zone}$은 하나의 위치보호구역 면적을, $S_{network}$는 네트워크 전체면적을 나타낸다. $S_{privacy\_zone} = \pi\delta^2$, $S_{network} = \pi R^2$이며 1-홉을 단위길이 1에 대응시키면 $(S_{privacy_zone}/S_{network})N = (\delta/R)^2N = (\rho R/R)^2N = \rho^2N$이 된다. 여기서, $\rho=\delta/R$로 표현되는 네트워크 반지름 R에 대한 위치보호구역 반지름의 비율을 나타내며 $0<\rho<1$이다. 고로 원 모양의 위치보호구역 내에 존재하는 근원지나 도착지가 발견될 확률은 $1/(\rho^2N)$이므로, 위치보안성은 $\log_2(\rho^2N) = \log_2 N + 2\log_2\rho = \log_2 N - 2\log_2(1/\rho)$이다.

그림 3은 N=500, 1000, ..., 4000에 대해 ρ의 값을 달리하는 경우에 대한 PCM과 ELPR의 위치보안성을 비교한 것이다. ELPR의 장점은 원하는 위치보안 수준을 위해 ρ을 조정할 수 있다는 것이다. 예를 들어 N=2000일 때 위치보안성 7을 겨냥한다면 ρ=0.2이면 충분할 것이다. 이렇게 ρ를 설정할 수 있다는 것은 통신비용 즉, 네트워크 내의 노드들이 발생하는 패킷들의 수 역시 조정할 수 있어 보안성과 통신비용을 사용자가 모두 사전에 조율할 수 있다. 반면에 PCM의 보안성은 네트워크 내의 노드들의 수 N에만 의존하여 고정적이다.

성질 2 : 반지름이 R인 원의 형태의 네트워크에 있어서 ELPR을 이용하는 경우 상호 겹치지 않는 위치보호구역의 최대 수 $k=1/\rho^2$이다.

증명 : $S_{privacy_zone}=\pi\delta^2$이고, $S_{network}=\pi R^2$이므로, k개의 위치보호구역들이 서로 겹치지 않고 전체 네트워크에 존재할 수 있는 최대 수 k는 $k\le(\pi R^2/\pi\delta^2)$을 만족해야 한다. 여기서, $\delta=\rho R(0<\rho<1)$이므로, $k\le 1/\rho^2$이다.

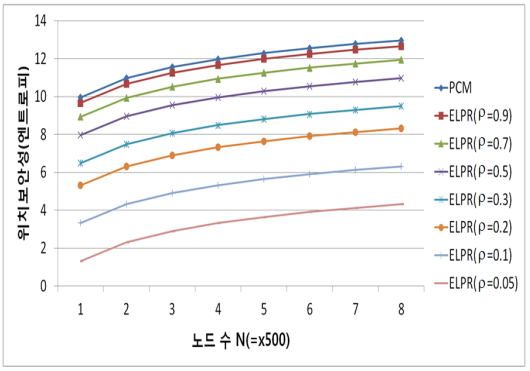



그림 3. 위치보안성 비교
Fig. 3 Comparison of location privacy levels

성질 1에 따른 위치보안성이 결정되면, 성질 2를 이용하여 주어진 네트워크 내에 위치보호구역 수 즉, 위치보호가 필요한 근원지들과 도착지의 전체 수 k를 구할 수 있다. 예를 들어 N=2000인 네트워크에 대해 7 이상인 위치보안성을 고려한다면 $\rho\ge0.2$이면 되므로 $1/(0.2)^2 = 25$이다. 그런데, k는 최소 2이므로(하나의 근원지와 하나의 도착지가 있는 경우), $2\le k\le25$를 만족하는 범위에서 k를 선정하면 된다. 역으로 k가 주어진 경우에는 성질 2를 이용하여 ρ를 결정하고 성질 1에 따라 원하는 위치보안성을 결정할 수 있다.

## Ⅳ. 통신비용

통신비용은 위치보안 라우팅 과정에서 발행되는 모든 종류의 패킷들의 총 수이다. 데이터패킷 수가 $n_{data}$개일 때, 이를 모두 전송하는 동안 수반되는 더미패킷들의 수는 물론, 프로토콜 자체 내에서 제어용으로 사용하는 패킷들의 수도 고려한 것이다. 반지름이 R-홉인 원의 형태인 네트워크를 가정하면 임의의 두 노드 간의 최단경로길이 중 가장 큰 값 즉, 지름(diameter) D=2R이다. 이는 하나의 패킷을 네트워크 내의 임의의 노드에게 전달되기 위하여 최대 2R만큼의 타임-슬롯이 필요함을 의미한다. PCM에서는 모든 노드들이 매 타임-슬롯마다 패킷을 발행하므로 $n_{data}$개의 데이터패킷들이 전송되기 위해서는 모두 $n_{data}\cdot D\cdot N = 2R\cdot n_{data}\cdot N$개의 패킷들이 발생한다.

성질 3 : 반지름이 R인 원의 형태의 네트워크에서

ELPR을 이용하여 $n_{data}$개의 데이터패킷을 전송하는 경우 최대 $k(2RN+N\rho^2n_{data}+2Rn_{data})+N\rho R-2Rn_{data}$ 개의 패킷이 발생한다. 단, k는 네트워크 내의 위치보호구역들의 수이다.

증명: ELPR의 초기화단계에서 위치보호구역 설정에 $N\cdot\delta$ 그리고 (k-1)개의 근원지들이 자신들의 보호구역을 통보하는데 $N\cdot k-1\cdot D$ 등 모두 $N(\delta+ k-1\cdot D)$ 개의 제어용 패킷들이 발행된다(그림 1참조). 그림 2를 참조하여 데이터 전송단계에서 발생하는 패킷들을 구해 본다. 데이터 전송단계의 맨 처음에서 도착지가 자신의 보호구역을 알리는 동안에 $N\cdot D$만큼의 패킷들이 발행된다. 그리고 $n_{data}$개의 데이터패킷들을 k-1개의 근원지들이 각기 보내는 동안 k개의 보호구역들에서 모두 $k(\rho^2N)n_{data}$개의 패킷들이 발생되고, k-1개의 근원지들로부터 하나의 도착지로 가는 k-1개의 경로상의 노드들로부터 $k-1\cdot D\cdot n_{data}$개의 데이터패킷들이 또한 발생한다. 따라서 이들을 모두 합해 D=2R을 고려하면 통신비용은 $N(\delta+kD) + k(\rho^2N)n_{data} + k-1\cdot D\cdot n_{data} = k(2RN + \rho^2Nn_{data} + 2Rn_{data}) + N\rho R - 2Rn_{data}$로 주어진다.

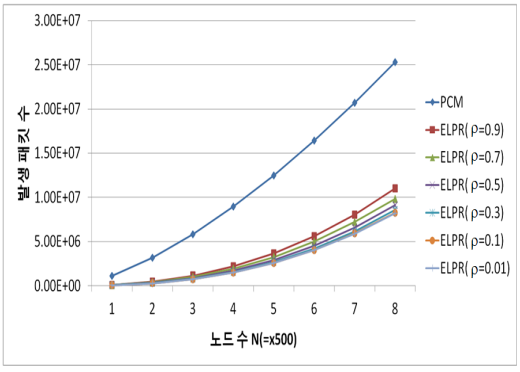
통신비용을 구하기 위해서 관련 연구들[6],[7],[8]에서 사용된 시뮬레이션 도구를 사용하여 PCM과 ELPR의 라우팅기능을 수행하는 과정에서 발생하는 패킷들의 수를 측정하였다. 동작과정에서 혼잡이나 전송오류 등은 발생하지 않음을 가정하고, low-duty cycle 모델을 가정하여[2],[3],[4] 발행된 패킷이 의도된 도착지에 도착한 후에야 다음 패킷이 발생하도록 하였다. 네트워크는 원의 형태로 노드들을 무작위로 균등하게 분포되도록 배치하되, 노드들의 평균 차수(degree)는 8로, 네트워크 지름 D(=2R)는 $\sqrt{N}$ 으로 설정하였다. 모든 시뮬레이션의 실행은 무작위로 생성된 토폴로지 100개에 대해 얻어진 값들에 대해 평균을 취하였다. 네트워크의 고려된 변수는 네트워크 내의 노드 수 N, 데이터패킷 수 $n_{data}$, 위치보호구역 수(다시 말해, 위치보호가 필요한 노드들의 수로 근원지들의 수 k-1에 도착지 수 하나를 더한 것) k, 네트워크 반지름대비 위치보호구역 반지름 비율 $\rho(=\delta/R)$ 등이다. N에 비하여 k의 수는 상대적으로 극히 작고 네트워크 내에 고르게 편재되어 있음을 가정하여 모든 시뮬레이션에서는 위치보호구역은 겹치지 않는 경우만을 고려하였다. 그리고 k값의 변화에 따른 통신비용을 평가하는 경우를 제외하고는 위치기밀성은 7을 유지하도록 하였다.

그림 4에 N과 ρ의 변화에 따른 통신비용을 나타내었는데 N이 증가할 수 록 PCM에 비해 ELPR의 통신비용이 크게 절약되는 경향을 보였다. 이는 PCM은 언제나 N개의 모든 노드가 패킷발행에 관여하지만, ELPR은 초기화단계에서만 모든 노드가 타임-슬롯마다 패킷을 발행할 뿐, 데이터전송 단계에서는 k개의 위치보호구역내의 노드들과 위치보호구역간을 연결하는 k-1개의 경로상의 노드들만 패킷을 발행하기 때문이다. 그리고 동일한 N에 대해서는 ρ가 작을수록 보호구역내에 존재하는 노드 수는 적어져 통신비용이 감소하였다.

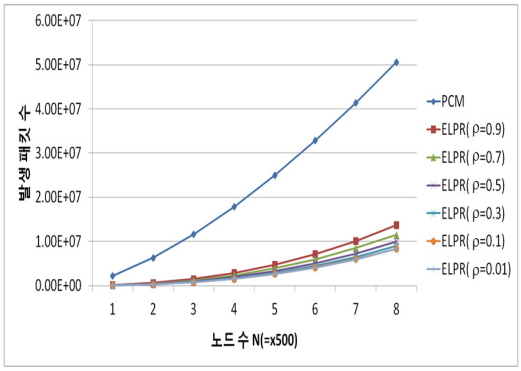
PCM이나 ELPR 모두 $n_{data}$가 증가할수록 N과 ρ이 고정되더라도 통신비용이 늘어나는 경향을 보였지만, N이 클수록 PCM에 대한 ELPR의 통신비용은 더 많이 감축되는 것을 확인하였다. 즉, 그림 c)에서의 ELPR의 PCM에 대한 통신비용 감소 정도는 b)에서의 감소 정도보다 N이 클수록 더 컸으며, 마찬가지로 b)에서의 감소 정도는 a)에서 보다 더 컸다.

k와 통신비용과의 관계는 그림 6에 나타냈다. PCM은 k와 무관하기에 고정된 통신비용을 보이지만, ELPR은 k가 증가함에 따라 보호구역 내의 노드들의 수가 증가하므로 통신비용도 늘어났다. 같은 k에 대해서도 ρ이 클수록 보호구역 내의 노드들의 수가 더 많아져 ELPR의 통신비용이 또한 상승하였다.

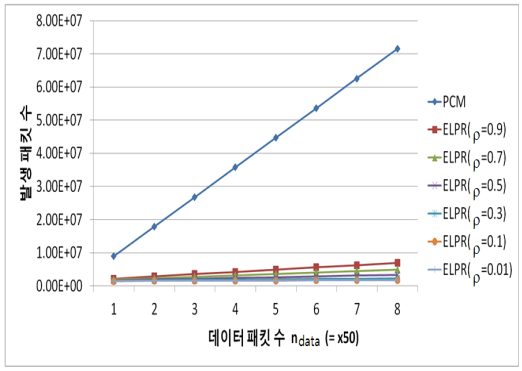
결론적으로 성질 2에 의해 주어진 k에 대해 N이 클수록 ELPR은 PCM에 비해 더 작은 통신비용으로 위치보안을 제공한다.



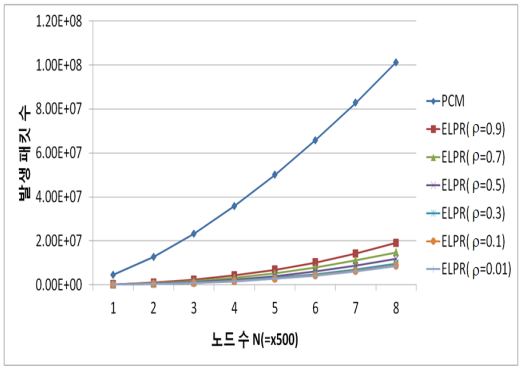

a) $n_{data}$=50




b) $n_{data}$=100

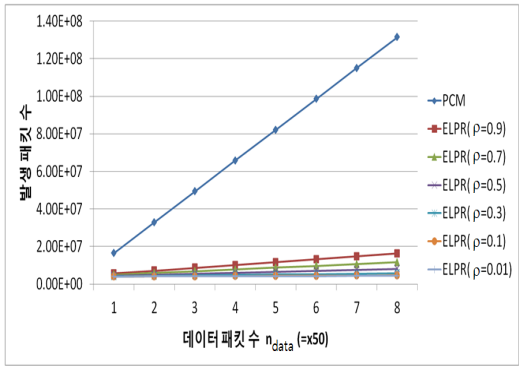



b) N=2000



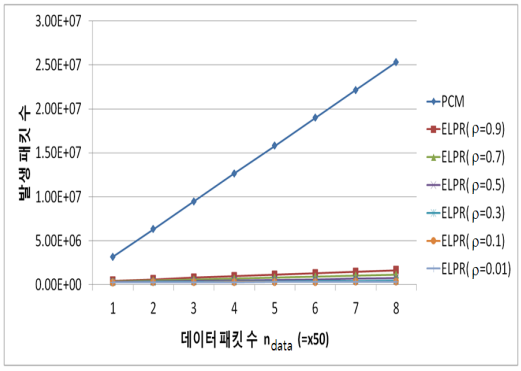

c) $n_{data}$=200

그림 4. 노드 수에 따른 통신비용(k=N/250)
Fig. 4 Communications costs VS. number of nodes(k=N/250)

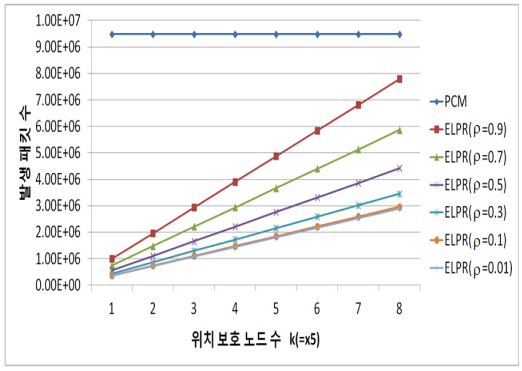



c) N=3000

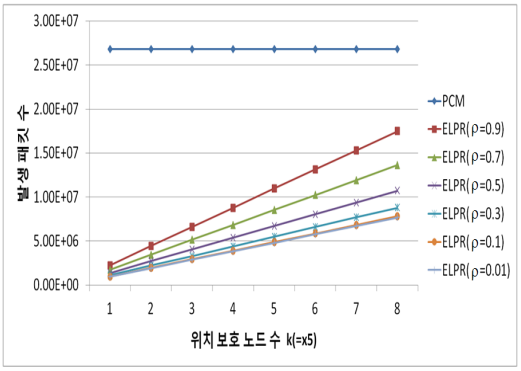
그림 5. 데이터패킷 수에 따른 통신비용(k=N/250)
Fig. 5 Communications costs VS. number of data packets(k=N/250)



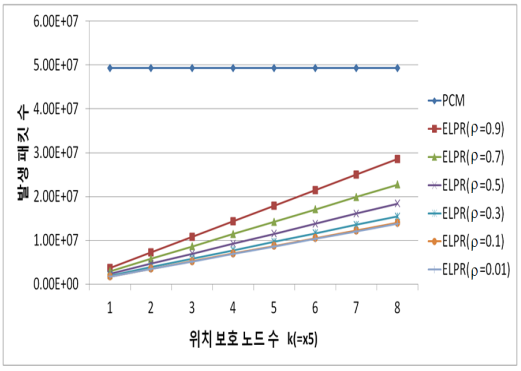

a) N=1000




a) N=1000




b) N=2000




c) N=3000

그림 6. 위치보호노드 수에 따른 통신비용($n_{data}$=100)
Fig. 6 Communications costs VS. number of nodes requiring location privacy($n_{data}$=100)

## V. 결 론

이 논문에서는 광역도청에 의해 통신 경로상의 근원지와 도착지의 위치를 파악하려는 공격에 대응하기 위해 선행 연구에서 제안한 라우팅 프로토콜 ELPR을 경쟁 프로토콜 PCM과 비교 평가하였다. 위치보안성은 엔트로피 정의를 이용하여 분석하였고, 통신비용은 시뮬레이션을 통하여 동작 중에 발생되는 패킷들의 수를 산출하여 평가하였다. 고정된 위치보안성은 제공하는 PCM과 달리 ELPR에서는 위치보안이 요구되는 근원지들과 도착지의 수를 고려하여 적합한 위치보안성을 결정할 수 있다. 이러한 조건하에서 노드들의 수가 클 수 록 그리고 전송 데이터의 수가 많을 수 록 ELPR은 PCM에 비해 상대적으로 적은 통신비용으로 설정된 위치보안성을 제공할 수 있음을 확인하였다. ELPR의 가장 큰 제약점은 위치보호 노드들(즉 근원지와 도착지)의 수 k가 매우 큰 경우 즉, k=O(N)에 대해 PCM보다 통신비용이 증가한다는 것이다. 이와 같은 경우에 대해서 효과적인 통신비용으로 원하는 수준의 위치보안성을 제공하는 새로운 접근방안이 연구되어져야 할 것이다. 아울러, 근원지나 도착지의 물리적 이동이 허용된 경우, 위치보호구역들이 서로 겹치는 경우, 도착지가 하나가 아닌 여러 개 존재하는 경우 등에 대한 확장 연구들도 필요하다.

미래의 네트워크 보안 인프라를 구축하기 위한 표준화된 플랫폼[8]에 연계하는 것도 흥미로운 향후 연구가 될 것이다. 기타 군사적 목적의 특수용도의 통신링크[[9]와 클라이언트 컴퓨팅 분야[10]에서의 위치보안 응용과 효과적 보안키[11]을 이용한 내용보안 등과의 접목도 주요한 과제이다.

**감사의 글**

본 논문은 2011년도 상지대학교 연구년 지원에 의한 것임을 밝힙니다.

## 참고 문헌

[1] N. Li, N. Zhang, S.-K. Das, and B. Thuraisingham, "Privacy preservation in wireless sensor networks : a state-of-the-art survey", Ad Hoc networks, Vol. 7, pp. 1501-1514, 2009.

[2] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor networking routing", Proc. of ICDCS'05, pp. 1-10, 2005.

[3] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, "Protecting receiver-location privacy in wireless sensor networks", Proc. of INFOCOM'07, pp. 1955-1963, 2007.

[4] K. Mehta, D. Liu, and M. Wright, "Protecting location privacy in sensor networks against a global eavesdropper", IEEE Transaction on Mobile Computing, Vol. 11, No. 2, pp. 320-336, 2012.

[5] 차영환, "무선 센서 네트워크에서의 통신 근원지 및 도착지 은닉: 제1부, 프로토콜 설계", 한국전자통신학회논문지, 8권, 2호, pp. 218-225. 2013.

[6] Yeonghwan Tscha, "Routing for enhancing source-location privacy in wireless sensor networks of multiple assets", Journal of Communications and Networks, Vol. 11, No. 6, pp. 589-598, 2009.
[7] H. Chen and W. Lou, "From nowhere to somewhere : protecting end-to-end privacy in wireless sensor networks", Proc. of IPCCC'10, pp. 1-8, 2010.
[8] 양기원, 임화정, 차영환, "휴면 소오스들이 존재하는 환경의 센서 네트워크를 위한 위치 보호 강화 라우팅", 정보과학회논문지 : 정보통신, 36권, 1호, pp. 12-23, 2009.
[7] 이철승, "MANET 기반의 MD5 보안 라우팅에 관한 연구", 한국전자통신학회논문지, 7권, 4호, pp. 797~804, 2012.
[8] 서우석, 박재표, 전문석, "네트워크 보안 인프라 구성을 위한 표준화된 플랫폼 디자인 방법론에 관한 연구", 한국전자통신학회논문지, 7권, 1호, pp. 203~211, 2012.
[9] 정상래, 신현식, "NCW 및 전술데이터링크 기술 개발 현황분석", 한국전자통신학회논문지, 7권, 5호, pp. 991~998, 2012.
[10] 차병래, 김대규, 김남호, 최세일, 김종원, "클라우드 컴퓨팅 기반 스트리밍 미디어의 검색 가능 이미지 암호 시스템 설계", 한국전자통신학회논문지, 7권, 4호, pp. 811~819, 2012.
[11] 정우열, 이선근, "근접 통신망의 보안성 향상을 위한 자기키 생성 알고리즘에 관한 연구", 7권, 5호, pp. 1027~1032, 2012.

## 저자 소개

**차영환(Yeong-Hwan Tscha)**

1983년 인하대학교 전자계산학과 졸업(이학사)
1985년 한국과학기술원 전산학과 졸업(공학석사)
1993년 인하대학교 대학원 전자계산학과졸업(이학박사)
1985년~1990년 한국전자통신연구원 선임연구원
1986년 NIST(미국) 방문과학자
2004년, 2011년 Boğaziçi 대학교(터키) 방문교수
1994년~현재 상지대학교 컴퓨터정보공학부 교수
※ 관심분야 : 네트워크 구조, 통신 프로토콜, 네트워크 보안