센서 네트워크에서 낮은 전달 지연으로 근원지 위치 기밀을 강화하는 라우팅

종신회원 차 영 환*

Routing for Enhancing Source-Location Privacy with Low Delivery Latency in Sensor Networks

Yeonghwan Tscha* *Lifelong Member*

요 약

센서 네트워크에 있어서 정보 전송 노드인 근원지의 위치를 악의적 추적자로부터 보호하기 위해 길이가 긴 경로를 통해 단일 메시지를 전송하는 라우팅에서는 전달 지연이 길어지는 단점이 있다. 본 논문에서는 전송 메시지가 사전에 주어진 경우, 근원지 위치를 보호하면서 최소 비용의 단일 경로를 이용하여 이들을 목적지로 전달하는 문제는 NP-complete 임을 보인다. 이러한 양 극단의 절충 방안이라 할 수 있는 경로 당 ω개의 메시지들을 전송하도록 하여 근원지의 위치 보호 능력을 높이면서도 전달 지연을 저감시키는 라우팅 프로토콜 GSLP-ω (GPSR-based Source Location Privacy with crew size ω)를 제안한다. 평가 기준으로는 목적지와의 최단 경로의 홉 수를 기준으로 정규 안전 기간(NSP: Normalized Safety Period)과 정규 전달 지연(NDL: Normalized Delivery Latency)을 고려한다. 평균 차수(degree)가 8인 노드 50,000개로 구성되는 네트워크 토폴로지 100개를 생성하여 측정한 결과 제안된 GSLP-ω는 GSLP-ω의 초기 버전인 GSLP와 기존의 대표적인 근원지 위치 보호 라우팅 프로토콜인 PR-SP(Phantom Routing - Single Path)보다 더 높은 안전 기간을 보였다. 전달 지연에서는 GSLP-ω가 PR-SP보다 높으나 GSLP 보다는 낮은 것으로 나타났다.

Key Words : Sensor networks, Source-location privacy routing, Safety period, Delivery latency

ABSTRACT

Most of routing schemes that protect the source's location from a malicious attacker usually make use of a path of a long length per message for the sake of lengthening the safety period. The biggest problem to such approaches is taking a very long latency in transferring messages to the destination. In this paper we show the problem to find the least-cost single path that is enough to keep the source-location always secure from the attacker, provided that it is used for the delivery of a set of messages given in priori, is NP-complete. Consequently we propose a routing protocol GSLP-w(GPSR-based Source-Location Privacy with crew size ω) that is a trade-off between two extreme approaches. The advantage of GSLP-ω lies in its enhanced safety period for the source and its lowered delivery latency in messaging. We consider NSP(Normalized Sefety Period) and NDL(Normalized Delivery Latency), measured in terms of the least number of hops to the destination, to achieve tangible interpretation of the results. We ran a simulation to confirm our claim by generating 100 topologies of 50,000 nodes with the average number of neighbors being 8. The results show that GSLP-ω provides more enhanced NSP compared to other protocols GSLP, an earlier version of GSLP-ω, and PR-SP(Phantom Routing - Single Path), the most notable existing protocol for the source-location privacy, and less NDL than that of GSLP but more than that of PR-SP.

※ 이 논문은 2007년도 정부(교육과학기술부)의 재원으로 한국학술진흥재단의 지원을 받아 수행된 연구임(KRF-2007-521-D00409)
* 상지대학교 컴퓨터정보공학부(yhtscha@sangji.ac.kr)(° : 교신저자)
논문번호 : KICS2008-04-191, 접수일자 : 2008년 4월 28일, 최종논문접수일자 : 2008년 7월 24일

I. 서 론

무선 통신 기술의 발전과 센서 기술의 확대 보급으로 인해 센서 장치들을 유기적으로 연결하여 대이터를 수집하고 제어하는 다양한 응용 분야의 센서 네트워크들이 연구 개발 되고 있다. 일반적으로 네트워크 노드로 불리는 센서 장치는 한정된 컴퓨팅 능력과 자원을 갖는데, 설치 환경으로부터 발생한 특정 이벤트나 수집 데이터를 다중-홉(*multi-hop*) 형태의 경로를 이용하여 기지국(base station)으로 전달하는 정보의 근원지(source) 역할을 수행한다. 역으로는 기지국으로부터의 정보를 수신하여(주로 제어 정보) 설치 환경의 관련 대상이나 장치의 제어 등에 적용한다.

센서 네트워크의 성공적 운용을 위해서는 적기의 데이터 수집과 제어가 가능하도록 효율적인 실시간 통신 기능이 확보되어야 한다. 하지만 무선 통신 자체가 갖는 전송 신호의 노출 문제, 센서 관련 장비의 표준화, 그리고 네트워크 설치 공간이 대부분 옥외라는 점에서 센서 네트워크의 보안 문제를 간과할 수 없다[1]. 특히, 암호화 기법에 의존하여 전송 정보의 내용을 보호하는 기술만으로는 성공적인 보안 체계를 유지할 수 없는 응용들이 있다. 예를 들어 전장에서 작전 중인 병력이나 탱크 등과 같은 이동체를 지원하거나 희귀 동물의 활동을 모니터링하는 센서 네트워크에서는 전송 메시지가 암호화되어 있어 그 내용에 대한 기밀이 유지된다 하더라도, 정보 전송의 근원지에 해당하는 노드의 위치가 적이나 밀렵꾼 등에 노출되는 경우 병력이나 장비의 손실 또는 보호 동물의 생존에 심각한 위협을 주게 된다. 이와 같은 이유로 인해 최근 정보 생성 노드의 위치나 트래픽의 양, 종류, 송수신 분포 유형 등과 같은 문맥 정보(contextual information)를 보호하기 위한 연구들이 주목을 받게 되었다[2-10].

센서 네트워크에서의 위치 보호[1]와 관련된 라우팅 분야에는 정보의 송신자에 해당하는 근원지 노드의 위치를 보호하기 위한 연구[2,4,6,7,9,11]와 메시지의 최종 도착지의 위치를 보호하는 연구[3,8]가 있다. 그리고 정보 이론적 측면에서 송수신자를 모두 보호하는 익명성 통신과 완전한 위치 보호에 관한 연구[10] 등도 있다. 센서 네트워크에서의 다양한 보안 문제들 특히, 라우팅에 관련된 제반 이슈와 대책들은 Karlof-Wagner의 논문에 잘 나와 있다[1].

본 논문과 관련된 센서 네트워크에 있어서 메시지 전송 노드인 근원지의 위치를 보호하기 위한 라우팅에서는 안전 기간을 늘이기 위해 길이가 긴 경로를 이용하면서 경로 당 하나의 메시지를 전송하여 공격자의 연이은 추적을 단절시키려는 접근방식을 따르고 있다[2,4,6,7,9,11]. 이러한 방법들의 최대 단점으로는 메시지 전달 지연이 지나치게 늘어나는 것이다. 이와 달리 또 다른 극단의 관점에서는 하나의 경로를 통해 모든 메시지들을 전송하는 방안을 고려할 수 있다. 전송 메시지 수가 사전에 알려져 있는 경우, 근원지 위치를 보호하면서 최소 비용의 단일 경로를 이용하여 이들을 도착지로 보내도록 하는 것이다. 본 논문에서는 이러한 문제는 최적 해결을 위해계산 량이 엄청나게 요구되는 NP-complete임을 보인다. 그리고 이러한 양 극단의 절충이라 할 수 있는 경로 당 ω개의 메시지들을 전송하도록 하여 근원지의 위치 보호 능력을 높이면서도 전달 지연을 낮추는 라우팅 프로토콜 GSLP-ω (GPSR-based Source Location Privacy with crew size ω)를 제안한다.

제안 프로토콜의 평가를 위해서 비교 대상으로는 PR-SP(Phantom Routing-Single Path)[2,4]와 저자에 의해 선행 연구로 제안된 GSLP[2]를 선정하였다. PR-SP가 휴면(dormant) 근원지[3]들이 존재하는 환경에서의 라우팅을 고려하지 않았기에 비교 자체가 불공평할 수도 있으나 이러한 환경에서 어느 정도의 위치 보호 능력을 발휘하면서도 기존의 가장 대표적인 근원지 위치 보호 라우팅 기법이기 때문이다. GSLP는 휴면 근원지들이 존재하는 경우를 고려한 최초의 라우팅 방안이기 때문이다. 제안 프로토콜의 검증을 위한 시뮬레이션에서는 평균 차수(degree)가 8인 노드 50,000개로 구성되는 네트워크 토폴로지 100개를 생성하여 사용하고 얻어진 결과값의 평균을 취하였다. 근원지 노드 수는 전체 노드

1) 위치 보호(location privacy 또는 location protection)란 센서 네트워크에서의 모니터링이나 관측 대상 즉, 전장 터의 병력이나 희귀 동물과 같은 보호 대상(asset) 또는 이와 가장 근접한 센서 노드의 위치 정보를 보호한다는 것을 의미하며 본 논문에서는 이를 구분하지 않는다.

2) GSLP는 본 논문에서 제안하는 GSLP-ω에서 ω=1인 프로토콜이다. 약어 GPSR-based Source Location Privacy에서 GPSR은 Karp와 Kung이 제안한 위치 기반 라우팅 프로토콜인 Greedy Perimeter Stateless Routing[12]을 나타낸다.

3) 휴면 근원지란 "활동(active) 근원지"처럼 메시지를 전송하고 있지는 않으나 위치 보호가 필요한 대상과 인접한 노드이다. 이러한 용어는 단일 근원지만을 고려하던 종래의 연구들[2,4,6,9]과 달리 동일 저자에 의한 연구[11]에서 처음으로 도입되었다.

의 0.0%에서부터 1%까지 0.2%의 간격으로 그리고 메시지를 전송하는 활동 근원지와 기지국 간의 거리(홉 수)는 30에서부터 80까지 10홉의 간격으로 고려하였다.

본 논문의 구성은 다음과 같다. 다음 장에서는 추적 모델을 설명하고 단일 경로를 이용한 근원지 위치 보호 라우팅 문제를 살펴본다. III 장은 본 연구를 위해 가정된 사항을 소개하고, 제안하는 근원지 위치 보호 라우팅 프로토콜을 설명한 후, 지연 시간을 분석한다. 성능 평가는 IV장에서 다루는데 시뮬레이션을 위해 설정된 파라미터들을 소개하고 측정된 정규 안전 기간(NSP)과 정규 전달 기간(NDL)을 분석 검토한다. V장의 결론으로 논문의 끝을 맺는다.

Ⅱ. 단일 경로를 이용한 근원지 위치 보호 라우팅

2.1 추적자 모델

공격자는 지역 도청자(local eavesdropper)로서 각종 장비(예, 스펙트럼 분석기, 지향성 안테나, GPS 등)를 갖추고 있기 때문에 신호 방향, 세기, 도착각 등을 측정하여 어느 노드로부터 신호가 발생했는지 정확히 인지 할 수 있다고 가정한다[2,4,9,10]. 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 모델[4]을 고려한다. 어떤 근원지가 존재하는 곳으로부터 반지름이 α인 원 내로 공격자가 진입하면 그 근원지의 위치는 탄로 난 것으로 간주한다. 이때의 영역을 노출 영역(disclosure area), α를 포획 거리(capture distance)라고 한다. 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. 한편, 네트워크 내에서 노드들 간에 주고받는 모든 메시지는 암호화되어 있어 공격자가 해독할 수 없지만, 근원지 노드 s에서 전송된 메시지의 목적지인 기지국 b의 위치는 공격자에게 노출되어 있다고 가정한다[2,4,9,11].

2.2 단일 경로를 이용한 라우팅

단일 경로를 이용하여 주어진 메시지들을 최소의 비용으로 근원지의 위치가 노출되지 않고 보내는 문제는 다음과 같은 특성을 갖는다.

정리: 어떤 노드 s가 목적지 또는 기지국 b로 전송할 메시지 T개를 가지고 있다고 가정하자. 추적자 a가 현재 b에 머물고 있을 때 2.1과 같은 모델의 추적자로부터 s의 위치를 완전히 보호하면서 T개의 메시지를 최소 홉 수의 경로를 이용 전송하는 문제는 NP-complete이다.

증명: 일반성을 잃지 않고 네트워크 내의 노드 수 N이 충분히 커서 $T<N$이라 가정하자. s가 b로 설정한 경로의 홉 수(길이)를 L이라고 하면 전송 메시지 수 T 및 포획 거리 α에 대해 $L-T>\lfloor \alpha/r \rfloor$인 관계가 성립해야 s의 위치가 발각되지 않는다. 여기서 r은 신호 전달 거리이고, $\lfloor x \rfloor$는 x보다 같거나 큰 정수 중 가장 작은 수를 나타낸다. 즉, $\lfloor \alpha/r \rfloor$는 포획 거리 α를 홉 수로 변환 한 값이다. 이에, s가 b로 홉 수가 $T+\lfloor \alpha/r \rfloor$인 경로를 사용하여 T개의 메시지를 연속적으로 전송하면 최단 거리이면서도 추적자로부터 s는 포획 거리 α에 대응되는 홉 수 $\lfloor \alpha/r \rfloor$ 이상 떨어져 있을 수 있어 안전하다. 그런데 일반적으로 길이가 최소 k 또는 그 이상인 경로를 찾는 "k-th longest path" 문제는 이미 NP-complete이다[17]. 주어진 문제에서 $k=T+\lfloor \alpha/r \rfloor$로 놓음으로서 본 정리는 성립한다. □

위 정리의 의미는 단일 경로를 이용하여 최소 비용으로 주어진 메시지들을 전송하기 위한 알고리즘은 엄청난 계산 량이 소요되기 때문에 근사해나 변형된 문제로의 해법을 찾는 것이 유리하다는 것이다. 한편, 위의 정리에서 추적자 a가 기지국 b가 아닌 임의의 노드에 위치하고 있을 경우에도 마찬가지로 NP-complete임을 유사한 방법으로 증명할 수 있다. 이에 본 연구에서는 근원지 위치 보호와 관련된 다음과 같은 접근방법을 고려한다.

- 경로당 하나의 메시지를 전송하면서 여러 개의 경로들을 이용하는 방안과 하나의 경로로 모든 메시지를 전송하는 두 극단의 접근방안을 피하고 "crew size ω"로 정의되는 경로당 전송 메시지 수 ω를 고려하면서 동시에 여러 개의 경로를 이용하는 방안을 통해 높은 안전 기간을 제공하면서도 낮은 전달 지연이 가능한 방안을 모색한다.

- 근원지 s의 위치 보호 수준을 평가하는 안전 기간과 성능을 나타내는 전달 지연을 s와 도착지 b 사이의 최단 홉 수 $h_{s,b}$에 관한 값으로 나타내어 근원지로 하여금 위치 보호와 전달 지연을 고려한 메시지 전송 정책을 마련할 수 있게 한다. 즉, 근원지는 전송할 메시지 수가 주어진 경우 이들을 연속해서 보낼 것 인지 아니면, 일정 개수를 보낸 후 충분한 휴지(idle) 시간을 갖는 과정을 반복할 것인지 등을 고려할 수 있다. 그리고 보다 높은 근원지의 위치 보안성을 유지하기 위해서는 사전에 교환되는 메시지 수에 대한 제한을 두는 전략적 대안도 검토할 수 있다.

Ⅲ. 제안 프로토콜 GSLP-ω

3.1 가정 사항

네트워크 내에는 N 개의 센서 노드들과 하나의 기지국 b가 존재하며, 모든 노드는 자신의 위치(즉, 좌표)와 b의 좌표 그리고 이웃 노드들의 좌표를 알고 있다고 가정한다. 보호 대상을 감지한 센서 노드는 먼저 경계 지역(alert zone)을 설정하고 보호 대상에 대한 지역적 모니터링이나 휴지 상태에 머무는 휴면 근원지(dormant source) 노드가 된다. 즉, 보호 대상의 존재를 감지한 노드들은 기지국 b로의 메시지 전송에 앞서서 자신으로부터 거리가 β(>r) 이내인 영역에 존재하는 노드들에게 보호 대상이 근처에 존재하므로 메시지 전송 과정에서 해당 영역을 우회할 것을 나타내는 경계 지역을 설정한다 (수신 지역을 한정짓는 지역 플러딩(local flooding) 기법[15] 등을 이용).

그림 1에 휴면 근원지에 의한 경계 지역 설정과 노출 영역과의 관계를 나타내었다. 여기서 보호 대상은 판다 곰이며, 이에 가장 근접한 노드가 휴면 근원지가 되어 경계 지역을 설정하였다. 만일 메시지 전달 과정에서 추적자가 발생 신호를 따라 경계 지역을 넘어 노출 영역 이내로 들어오는 경우 휴면 근원지의 위치는 노출되고 따라서 보호 대상 역시 그 위치가 탄로 나게 된다.

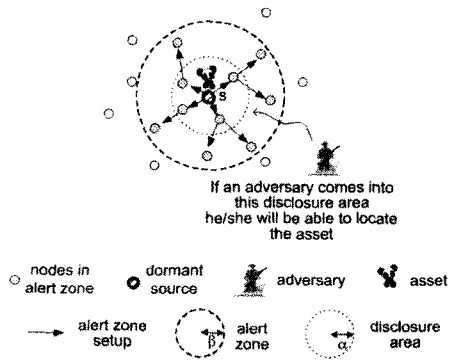


그림 1. 경계 지역 설정과 노출 영역

본 논문에서는 보호 대상마다는 하나의 대응되는 센서 노드를 가정한다. 즉, 보호 대상과 대응되는 휴면 근원지는 일대일 관계이다. 따라서 보호 대상과 대응되는 노드의 좌표는 허용된 오차의 범위 내에서 충분히 가까워 "근원지의 위치 보호가 곧 보호 대상의 위치 보호와 일치 한다"고 가정한다.

3.2 메시지 전달 노드 선정

제안된 라우팅 기법 GSLP-ω에서는 ω개의 메시지가 동일 경로를 이용하므로 맨 처음 메시지에 대해 다음과 같이 다음-홉(next-hop) 노드 즉, 메시지 전달 노드를 선정하고 라우팅 테이블에 관련 정보를 저장한다.

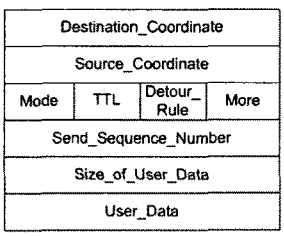
- **greedy** 모드: 어떤 난수(random number) $p(0<p_{rw}<1)$를 생성, 주어진 $p_{rw}(0<p_{rw}<1)$에 대해 $p<p_{rw}$이면 random_walk 모드로 진입한다. 그렇지 않으면(즉, $(1-p_{rw})$의 확률로) greedy forwarding[12]을 수행하여 목적지에 가장 근접한 이웃 노드를 다음 노드로 선정한다. 선정된 노드가 어떤 휴면 근원지가 설정한 경계 지역 내의 노드라면 perimeter 모드로 진입한다. greedy 모드의 도입은 메시지 전달 지연을 억제한다.
- **random_walk** 모드: 현재의 노드와 비교해서 목적지로의 거리를 증가시키지 않는 이웃 노드 중 임의의 하나를 선정한다. 일단, 이 모드가 진행되면 TTL_{rw}에 해당하는 홉 수만큼 후속 노드에서도 random_walk 모드가 적용된다. 만일 적용 과정에서 경계 지역 내의 노드가 선정되면 이를 우회하기 위해 perimeter 모드로 전환된다. random_walk 모드는 다양한 노드들이 서로 다른 경로들에서 사용되도록 해준다.
- **perimeter** 모드: GPSR[12]에서 라우팅 hole문제를 해결하기 위해 적용하였던 perimeter 라우팅을 이용하여 경계 지역 내에 존재하지 않는 노드들 전달 노드로 선정하여 경계 지역을 우회한다. 현재의 노드에서 도착지로의 직선을 기준으로 시계 반대 방향으로 존재하는 노드를 다음 노드로 선정하는 right-hand 규칙과 시계 방향으로 존재하는 노드를 다음 노드로 선정하는 left-hand

규칙이 고려된다. 일단 규칙이 정해지면 전송 메시지가 도착지에 이르기까지 만나는 모든 경계 지역에 대해 일관되게 적용한다. 활동 근원지에 의해 두 규칙을 번갈아가며 지정함으로써 어느 한 쪽으로만 경로가 치우치지 않게 한다. 일단 경계 지역을 지나 최단 거리 라우팅이 가능해지면 greedy 모드로 환원된다. 근원지 노드들의 수가 증가함에 따라 우회하여야 할 경계 지역도 늘어나, 자연적으로 경로 길이도 길어진다.

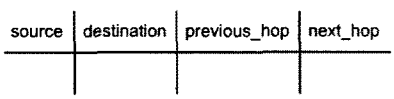
- **retreat** 모드: 경로 전개가 불가능하여 현재 노드에서 이전의 노드로 수신 메시지를 다시 되돌려주는 backtracking 과정이다. 일단 전송한 메시지를 다시 되돌려 받으면 해당 노드를 제외한 나머지 이웃 노드들을 대상으로 다음 노드를 다시 선정한다.[4)]0

3.3 메시지 형식 및 절차

메시지의 형식은 그림 2의 (a)와 같다. Destination_Coordinate는 도착지 노드의 좌표를, Source_Coordinate은 활동 근원지의 좌표이다. Mode 필드는 메시지 전달 선정하는 방법인 greedy(0), perimeter(1), random_walk(2), retreat(3) 중 어느 하나를 나타낸다. TTL 필드는 random_walk 모드로 계속해서 적용할 홉 수를 나타낸다. 적용 시 마다 1씩 감소되어 0이 되면 greedy 모드로 복귀한다. Detour_Rule 필드는 perimeter 모드에서 메시지 전달 노드를 설정하는 left-hand(0) 규칙 또는 right-hand(1) 규칙을 나타낸다. 이는 활동 근원지에서 결정한다.



(a) 메시지 형식



(b) 라우팅 테이블

그림 2. 메시지 형식과 라우팅 테이블

More 필드는 동일 경로를 이용하는 메시지가 더 남아 있는지를 알려준다. 즉, 후속 메시지가 있을 때는 follow(1) 그리고 맨 마지막 메시지 인 경우는 last(0)이다. 한편, 맨 처음 메시지의 경우에는 경로 설정을(즉, 메시지 전달 노드를 선정) 하여야 한다.(More 필드 값이 first(2)인 경우이다) 경로 정보를 나타내는 라우팅 테이블의 구조는 그림 2의 (b)와 같다. 테이블 내에는 근원지 노드 및 도착지 노드를 나타내는 source와 destination 항목, 메시지를 전달해준 노드를 나타내는 previous_hop, 그리고 선정된 메시지 전달 노드를 나타내는 next-hop 필드가 있다. previous_hop은 메시지 전달 노드 선정에서 retreat 모드에 의한 이전 노드로 수신된 메시지를 되돌려줄 때 이용된다. 설정된 경로는 more 필드가 last(0)인 메시지를 보낸 후 삭제된다. 한편, Send_Sequence_Number는 전송 메시지의 순번을, Size_of_User_Data는 사용 정보 길이를, 그리고 User_Data는 전송되는 사용자 정보를 나타낸다.

활동 근원지 s에서 사용하는 변수는 다음과 같다. TTL_{rw}는 random_walk 모드 내에서 이동할 홉 수를 나타내는데 활동 근원지 s에서 목적지 b까지의 최단 홉 수 $h_{s\text{-}b}$의 [5%, 10%] 범위에서 임의로 선정되며 최소치는 2이다. ω는 crew size 즉, 동일 경로

```
1. select a certain random number ω
   from [h_s-b/4, (3h_s-b)/4] and do as follows.

  for (i=0; to ω-1; i++)
  {
    1.1 // message packaging
      M.Destination_Coordinate = L(b);
      M.Source_Coordinate = L(s);
      M.TTL = TTL_rw;
      Detour_Rule_s = Detour_Rule_s   ; // toggling
      M.Detour_Rule = Detour_Rule_s;

      if (i==0) M.More =2; // 1st crew
      else if (i==w-1) M.More = 0; // last crew
      else M.More = 1; // otherwise

      M.Send_Sequence_Number = SSN_s++;
      M.Size_of_User_Data = Size_of_User_Data_s;
      M.User_Data = User_Data_s;
    1.2 // message forwarding
      if (M.More==2) { // 1st message
         choose the next-hop node v as stated in Section
         3.2, fill out the routing table and send M to v;
      } else {
         forward M to the node pointed by next_hop
         field of the routing table; }
  }
2. go to step 1 if there exist more messages or delete
   the route information in the routing table;
```

그림 3. 활동 근원지의 수행 절차

4) 본 연구에서는 근원지 위치 보호 라우팅 문제에만 집중한다. 라우팅 hole 문제와 이에 대한 보다 나은 해결책 등은 관련 문헌[13,14]에 나와 있다.

```
1. if ( M.Destination_Coordinate == L(u) ) {
      accept M; // the destination
      if (M.More == 0 )
        delete the route information in the routing table;
      exit;
   }
2. if ( M.More != 2 ) { // already being used
      forward M to the node pointed by next_hop field
      of the routing table;
      if (M.More == 0 )
        delete the route information in the routing table;
      exit;
   }
// create route as it is M.More == 2
3. select the next-hop node as stated in Section 3.2 and
   exit;
```

그림 4. 전달 노드에서의 수행 절차

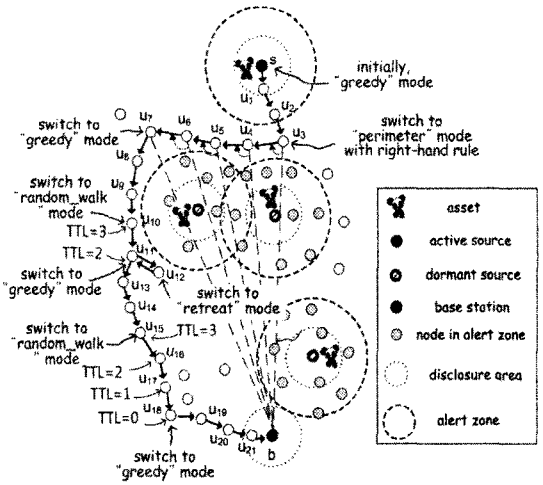


그림 5. GSLP-ω에서의 경로 설정 예

를 이용하는 메시지들의 수로 $[h_{s\text{-}b}/4, (3h_{s\text{-}b})/4]$인 범위에서 역시 무작위로 선정된다. $Detour_Rule_s$은 perimeter 모드에서 적용할 규칙으로 left-hand(0)규칙과 right-hand(1) 규칙이 번갈아가며 지정된다.(이를 $\overline{Detour_{Rule_s}}$로 표시하였다) 그 밖에 SSN_s은 전송 메시지의 순서번호(초기치 0)를 $User_Data_s$는 전송되는 사용자 정보를 나타낸다. 수행 과정은 그림 3과 같다. 그림에서 L(v)는 노드 v의 좌표 값 (v_x,v_y)을 나타낸다.

중간에 전송 메시지 M을 수신한 노드 r에서는 다음 홉 노드를 선정하는 경우와 이미 생성된 라우팅 테이블 내의 정보를 이용 단순히 전달하는 경우로 나뉜다. 전자는 M.More == first(2)일 때이다. 후자는 M.More == last(0) 또는 follow(1)인 경우이다. 단, M.More는 메시지 M내의 More 필드를 나타낸다. 그림 4의 단계 1에서 2까지는 단순 전달 과정이며, 처음 도착한 메시지에 대한 전달 노드를 선정하는 과정은 단계 3부터이다. 이는 3.2에서 상세히 설명하였다.

그림 5는 GSLP-ω의 동작 과정을 보여주는 예이다. 활동 근원지 s에서부터 u_3까지 greedy 모드로 도착지인 기지국 b와 가까운 이웃 노드들을 다음-홉 노드로 선정하였다. u_3에서부터는 목적지에 가까운 노드가 경계 지역 내에 속하는 것들이어서 right-hand 규칙에 의해 시계 반대 방향으로 위치한 이웃 노드 u_4, u_5, u_6, u_7이 차례로 정해졌다. u_7에서는 목적지 b에 가까운 노드 u_8이 경계 지역에 속하지 않아 선정되었다. 한편, u_{10}에서 TTL_{rw}=3으로 시작된 random_walk는 u_{12}가 더 이상 목적지로의 경로를 설정할 수 없어 retreat 모드로 전환되고 u_{11}로 되돌아와 greedy 모드로 u_{13}가 선정되었다. 이후 도착지까지 random_walk 모드와 greedy 모드가 경로가 설정에 적용되었다. 메시지 전달 노드를 선정하는 4가지 모드의 상대적인 적용 빈도와 p_{rw}와 TTL_{rw} 등의 주요 파라미터들의 값에 따라 경로의 길이와 모양이 다양해진다.

3.4 전달 지연(경로 길이) 분석

GSLP-ω에 의해 근원지 s를 출발한 메시지 M이 목적지 b에 도착하기까지 경유하는 경로의 평균 홉 수를 직관적 방법으로 구한다. 편의상, 노드들의 밀도가 충분히 높아서 retreat 모드나 라우팅 hole 등으로 인한 경로 구성이 불가능한 경우는 발생하지 않는다고 가정한다.

활동 근원지 s에서 목적지 b에 이르기까지 메시지 M이 경유한 경로의 길이가 k 홉이라고 하자. 이 중 random_walk 모드로는 k_1 홉을 이동하였고, perimeter 모드로는 k_2 홉만큼, 그리고 그 외의 greedy 모드로는 k_3 홉을 이동하였다고 하자. 즉, $k=k_1+k_2+k_3$로, $k_1=k\cdot p_p$ $k_2=k\cdot p_{rw}$, $k_3=k\cdot p_g$ 이며, $p_p+p_{rw}+p_g = 1$이다. 그런데 perimeter 모드에서 선정되는 메시지 전달 노드는 최단 경로를 보장하지 않으며 최악의 경우 s에서 b로의 방향과 정 반대 방향에 위치하고 있는 노드들이 선정될 수 있다. random_walk 모드에서 선정되는 노드는 목적지로의 길이(홉 수가 아님)를 증가시키지 않는 위치의 임의의 노드가 선정될 수 있다. 그리고 greedy 모드에서는 언제나 목적지 b로의 최단 경로를 선정한다. 이에 $p_p+p_{rw}<0.5$이고 $p_g>0.5$이어야 s로부터 출발한 메시지는 목적지 b에 도착할 수 있다. 따라서 k가

최대 일 경우는 $p_{rw}\approx 0$ 즉, $p_p\approx 0.5$ 이며, s에서 perimeter 모드로 b와의 정반대 방향으로 k_1 홉을 이동하고, 이후 greedy 모드로 (k_1+d) 홉으로 b에 도착하는 경우이다. 즉, $k = k_1+k_2+k_3 \approx k_1+k_3 = k_1+(k_1+d) = 2k_1+d$이다. 그런데 $p_g=1$인 경우 $k=k_3=d$이다. 즉, $p_{rw}<0.5$이므로 $k_1<d/2$이며, $k\leq 2k_1+d<2(d/2)+d$ $(=2d)$이다. 고로 경로의 홉 수 k에 대해 $d\leq k<2d$이므로 산술적으로 $k=1.5d$이다. GSLP-ω에 의해 설정되는 경로는 최단 경로보다 약 1.5배의 긴 경로를 이용한다.

Ⅳ. 성능 평가

4.1 실험 환경 설정

소오스 위치 보호 라우팅 프로토콜의 위치 보호 수준과 성능 평가를 위한 공개된 범용 시뮬레이션 패키지가 없기 때문에 시뮬레이션 소프트웨어는 Java로 자체 제작하였다. 물리 계층이나 데이터-링크 계층의 기능은 포함하지 않고 시뮬레이션 대상 프로토콜(PR-SP, GSLP, GSLP-ω)들의 라우팅 알고리즘만을 구현하였다. 타 연구들[2,4,10,11]과 마찬가지로 low-duty cycle 모델을 가정하여 s로부터 전송된 메시지가 기지국 b에 도착한 후에 다음 메시지가 발생하도록 하였다. 휴면 근원지들을 무작위로 균등하게 분포되도록 하되 활동 근원지로부터 6r 이내에는 존재하지 않음을 가정하였다(r은 신호 도달 거리). 시뮬레이션 결과는 평균 차수가 8인 노드 50,000로 구성되는 토폴로지 100개를 생성하고 얻어진 값들에 대해 평균을 취하였다. 사용된 주요 파라미터들은 표 1과 같다.

표 1. 시뮬레이션 파라미터

파라메타		값 또는 범위
전체 노드 수(N)		50,000
노드의 평균 차수		8
활동 근원지 s와 기지국 b 간의 최단 홉 수($h_{s\text{-}b}$)		30, 40, ..., 80
휴면 근원지 수(N_s)		N의 0.2%, 0.4%, ..., 1%
생성 토폴로지 수		100
GSLP-ω, GSLP	random_walk 확률(p_{rw})	0.05
	경로당 전송 메시지 수(ω)	$\{h_{s\text{-}b}/4, (3h_{s\text{-}b})/4\}$ 에서 무작위로 선정
	random_walk 적용 홉 수(TTL_{rw})	$h_{s\text{-}b}$의 {5%, 10%} 중 무작위로 선택(최소 2)
	경계 지역 반지름(β)	2r(r은 전송 거리)
	포획 거리(α)	r
PR-SP	임의의 이동 거리	$h_{s\text{-}b}$의 {25%, 50%}에서 무작위로 선택

4.2 실험 결과 및 분석

활동 근원지와 기지국 간의 최단 거리가 비교적 짧은 경우, 중간인 경우 및 긴 경우를 고려하기 위해 $h_{s\text{-}b}$=30, 50, 70일 때, 근원지 노드의 수 N_s가 전체 노드 N의 0.0%에서 1%까지 0.2% 간격으로 주어진 경우들에 대해 정규 안전 기간(NSP: Normalized Safety Period)과 정규 전달 지연(NDL: Normalized Delivery Latency)을 구하여 보았다. 결과는 그림 6과 같다. 범례에서 괄호 안의 숫자는 활동 근원지와 기지국 간의 최단 홉 수 $h_{s\text{-}b}$이다. 그리고 제안된 GSLP-ω의 결과는 점선으로 표시하였다. 예를 들어 GSLP-ω는 70 홉 떨어진 노드로 메시지 전달 시 상대방과의 홉 수의 약 4.5배(N_s가 0%일 때) 즉, 70×4.5=315개 에서 9배(N_s가 N의 1%일 때) 즉, 70×9=630개에 이르는 메시지들을 근원지의 위치를 보호하면서 보낼 수 있었다.

그림 6에 나타난 NSP 결과에 대해 다음과 같은 사항에 주목 할 수 있다. 먼저, 제안한 GSLP-ω와GSLP 모두 근원지 노드들의 수가 증가하더라도 전체적으로

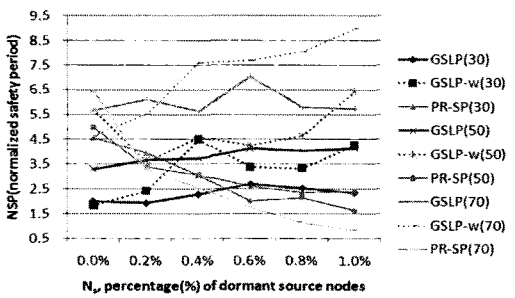


그림 6. 휴면 근원지 수에 따른 NSP 비교

안전 기간은 줄어들지도 않으면서 일정한 수준을 유지한다. 두 프로토콜 모두 경계 지역을 우회하는 기능을 갖고 있어 이러한 기능 없이 다른 휴면 근원지가 존재하는 노출 영역을 통과하여 그 위치를 노출시키는 PR-SP와 비교하여 명확히 대비된다. GSLP-ω는 GSLP에 비해 전체적으로 다소 더 높은 안전 기간을 나타냈고 ,N_s가 N의 0.8% 이상인 경우에 대해서 증가하는 추세를 보였다. 이는 휴면 근원지 노드들의 수가 증가하면서 경계 지역이 많아져 이들을 우회하는 빈도가 높아져 경로 길이가 증가하기 때문인 것으로 분석된다.

다음으로 $h_{s\text{-}b}$가 증가함에 따라 GSLP-ω와 GSLP 모두 안전 기간이 늘어나지만 PR-SP는 휴면 근원지들의 수 N_s가 전체 노드 수 N의 약 0.1% 이상을 넘으면서부터 심하게 줄어드는 경향을 보였다. 이 역시 PR-SP의 경우에는 $h_{s\text{-}b}$가 증가할수록 그리고 N_s가 증가할수록 근원지의 위치가 더 쉽게 노출되어 안전 길이가 줄어들기 때문이다. 그리고 PR-SP의 경우 N_s가 전체 노드 수 N의 약 0.7% 일 때부터 1이하로 낮아져 근원지의 위치가 노출되지 않고 전달되는 메시지 수가 기지국과의 최단 홉 수 $h_{s\text{-}b}$보다 적었다. 다만, PR-SP는 N_s가 N의 약 0.2%이하일 때 그리고 $h_{s\text{-}b}$가 짧을수록 GSLP와 GSLP-ω에 비해 높은 안전 기간으로 보였다. PR-SP에서는 일정 거리를 임의의 방향으로 이동한 후에 최단 거리 라우팅을 실시하므로 $h_{s\text{-}b}$가 상대적으로 짧거나 N_s가 적은 경우에는 경계 지역을 만나지 않아 안전 기간이 증가되기 때문이다.

한편, 다양한 N_s에 대한 NSP의 값들의 평균을 구하여 $h_{s\text{-}b}$의 변화에 따른 전체적인 추세를 나타내면 그림 7과 같다. GSLP-ω의 평균 NSP은 도착지와의 최단 홉 수 $h_{s\text{-}b}$에 관해 약 $0.1h_{s\text{-}b}$이고, GSLP는 $0.1h_{s\text{-}b}$-1이었다. 하지만 PR-SP는 3이하로 $h_{s\text{-}b}$와 무관하게 낮았다. 그림의 내용은 다음과 같이 활용될 수 있다. 어떤 도착지 노드 b로 메시지를 보내는 근원지 s가 GSLP-ω를 사용하면 b와의 최단 경로의 길이 $h_{s\text{-}b}$에 대하여 최대 약 $0.1h_{s\text{-}b}^2$ 개의 메시지들을 위치가 노출되기 전에까지 보낼 수 있다. 만일 $h_{s\text{-}b}$=75이면 $0.1(75)^2$ = 562.5개가 된다. 근원지 입장에서 전송할 메시지의 총 수 T가 주어졌다면 이들을 안전하게 보내기 위한 최소 비용의 단일 경로를 준비하기 보다는(II장에서 이는 NP-complete임을 보았다) 위의 값을 참조하여 이보다 훨씬 작은 개수들의 메시지들로 분할하여 놓고(예를 들면, 562.5는 평균값이므로, 약 반이하인 200개의 메시지들로 구성되는 G_1, G_2, ..., G_t 등 t개의 그룹으로

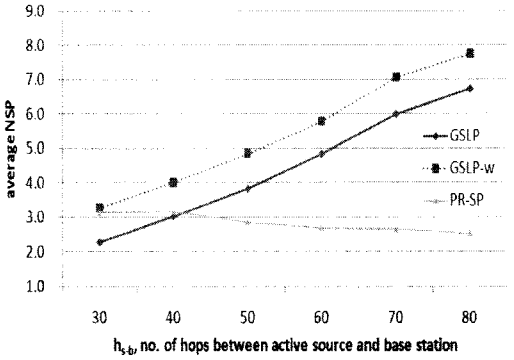


그림 7. 홉 수에 따른 평균 NSP 비교

나누어 놓고) 각각에 대해 GSLP-ω를 사용하여 보낸 후 상당히 큰 기간의 휴지(idle) 시간을 갖는 방안도 고려될 수 있다. 또한 근원지 노드가 사전에 메시지 수신측과의 거리를 고려하여 전송할 메시지 수를 전략적으로 특정 개수(예를 들면 위의 예에서, 100) 이하로 줄여서 통신하는 방안도 고려할 수 있다. 그리고 전송 정보의 압축이나 특수한 코딩 방안[16] 등을 접맥시켜 전송 정보량 자체를 줄일 수 도 있을 것이다.

다음으로는 정규화 전달 지연(NDL) 즉, 메시지 하나가 경유하는 경로의 평균 길이를 측정하였는데 결과는 그림 8과 같다. PR-SP는 휴면 근원지의 수에 관계없이 약 1.4에 밑도는 거의 일정한 전달 지연을 보였다. 이와 달리 GSLP-ω와 GSLP 모두 N_s의 증가에 따라 비례하여 늘어나는 추세를 나타냈고, 제안된 GSLP-ω는 GSLP에 비해 낮게 나타나 GSLP보다 전달 지연을 감축하는 효과가 있음을 보였다. PR-SP의 경우 휴면 근원지 노드들을 고려하지 않고 경로를 설정하다가 위치가 노출이 되면 안전 기간이 종료된다. 이에 경계 지역을 만나지 않고 성공적으로 메시지를 전달한

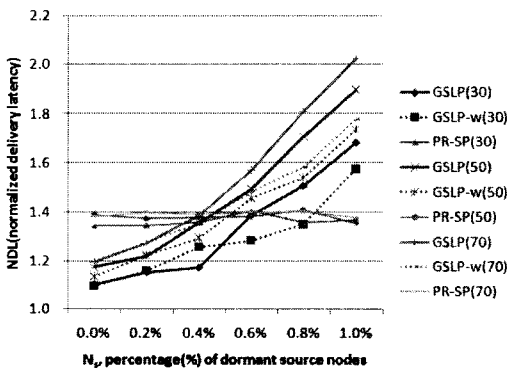


그림 8. 휴면 근원지 수에 따른 NDL 비교

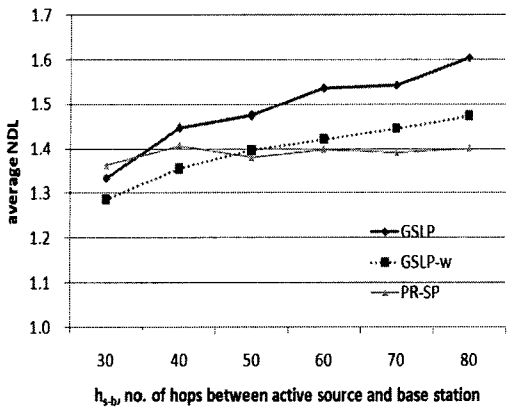


그림 9. 홉 수에 따른 평균 NDL 비교

경우의 경로들만이 전달 지연 측정에 고려되기 때문에 h_{s-b}의 값에만 영향을 받는 것으로 보인다. 하지만 경계 지역을 우회하는 GSLP-ω는 N_s의 증가에 따라 경로 길이가 증가되게 되고 따라서 전달 지연도 증가하였다.

GSLP-ω의 경우에는 경로당 $[h_{s-b}/4,(3h_{s-b})/4]$인 범위에서 무작위로 선정된 수에 해당하는 수만큼의 메시지들을 보내므로 경로당 하나의 메시지를 보내는 GSLP 보다 평균적으로 사용한 경로 길이가 짧았다. 따라서 전달 지연이 GSLP보다 낮았다. 이러한 특성은 N_s가 증가할수록 더 차이를 보였다. 흥미롭게도 GSLP-ω의 전달 지연은 h_{s-b}의 2배 이내를 나타내 3.4절의 이론적 분석결과의 상한치($2h_{s-b}$)와 평균치($1.5h_{s-b}$)와 나름대로 잘 일치하였다. 실험에서는 backtracking이 발생하더라도 도착지로 메시지를 전달하는 경로에 포함시켰기 때문에 전체적으로는 이론 치보다 다소 증가한 것으로 보인다. 그림 9는 N_s에 따른 NDL들의 평균을 구하여 기지국과의 홉 수 h_{s-b}에 따라 나타낸 것이다. GSLP-ω는 전체적으로 1.5이하(평균 1.40)로 3.4절의 분석과 유사한 결과를 보였다. 한편, GSLP는 1.6이하(평균 1.49)로 그리고 PR-SP는 1.40이하(평균 1.39)로 측정되었다.

종합하면 제안된 GSLP-ω는 기지국(목적지)과의 거리가 비교적 길며 휴면 근원지 노드들이 존재하는 대규모 센서 네트워크에서 일정 수준의 안전 기간을 제공하면서도 상대적으로 낮은 전달 지연으로 제공하는 프로토콜이라고 평가된다.

V. 결 론

본 논문에서는 휴면 근원지들이 존재하는 대규모 센서 네트워크에 있어서 근원지 위치 기밀을 강화하면서 메시지 전달 지연을 줄일 수 있는 라우팅 방안으로 GSLP-ω를 제안하였다. 이 프로토콜은 경로 당 하나의 메시지를 전송하면서 근원지 위치를 보호하는 경우의 전달 지연이 길어지는 단점과 최소 비용의 단일 경로를 이용하여 모든 메시지를 보내는 문제가 NP-complete임을 고려하여 경로당 일정 범위에서 무작위로 선정되는 ω개의 메시지를 전송하는 방안을 제시하였다. 시뮬레이션을 통한 측정한 결과 GSLP-ω가 다른 비교 프로토콜보다 전달 지연 대비 안전 기간이 가장 높아 낮은 전달지연으로 높은 안전 기간을 제공할 수 있음을 보여주었다.

추가 연구로 ω 값의 설정에 관한 보다 다양한 실험이 진행되고 있다. 또한, 활동 근원지 수와 기지국의 수를 여러 개로 확장한 경우 그리고 근원지가 이동하는 경우의 안전 기간과 전달 지연 등에 관한 연구 등도 계획 중이다. 이밖에 다양한 지능형 추적자 모델의 연구도 기대된다.

참 고 문 헌

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

[2] 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.

[3] 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.

[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] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[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] 휴먼 소오스들이 존재하는 환경에서의 센서 네트워크를 위한 위치 보호 강화 라우팅(심사 중), 2008.

[12] 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.

[13] 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.

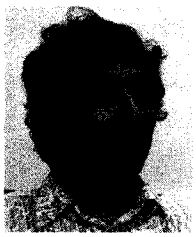
[14] N. Ahmed, S. Kanhere, and S. Jha, "The hole problem in wireless sensor networks: a survey," *ACM SIGMOBILE Mobile Computing and Communications Review*, Vol.9, No.2, 2005, pp.4-18.

[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)*, 1999, pp. 101-110.

[16] N. Kimura and S. Latifi, "A survey on data compression in wireless sensor networks," *Proc. of the International Conference of Information Technology: Coding and Computing(ITCC'05)*, Vol.2, pp.8-13, 2005.

[17] M. Garey and D. Johnson, *Computer and Intractability: a guide to the theory of NP-completeness*, W.H. Freeman and Company, San Francisco, 1979.

차 영 환 (Yeonghwan Tscha) 종신회원



1983년 2월 인하대학교 전자계산학과 졸업

1985년 2월 한국과학기술원 전산학과 석사

1993년 2월 인하대학교 전자계산학과 박사

1985년 3월~1990년 2월 한국전자통신연구원 선임연구원

1994년 3월~현재 상지대학교 컴퓨터정보공학부 교수

<관심분야> 네트워크 구조, 통신 프로토콜, 네트워크 보안