무선 센서 네트워크에서의 도착지 위치 기밀을 강화하는 라우팅

차영환*

On Routing for Enhancing Destination-Location Privacy in Wireless Sensor Networks

Yeonghwan Tscha*

이 논문은 2009년도 상지대학교 교내 연구비 지원에 의한 것임

요 약

이 논문에서는 패킷 추적 과정에서 획득한 위치 정보를 이용하여 추적 노드를 결정하는 방안을 고려한다. 한편, 추적에 대응하는 라우팅 전략으로는 위치 보호가 필요한 노드들과 근접하지 않은 노드들로 라우팅 경로를 구성하고, 가능한 경로 궤적이 지그-재그나 앞뒤로 이동하지 않도록 한다. 시뮬레이션을 통해 추적 성공률이 매우 향상됨을 확인 하였고, 제안된 라우팅 기법은 다수의 보호 대상들이 존재하는 환경에서 더 많은 패킷들을 전달하면서도, 추적자로 하여금 더 많은 거리를 이동하도록 유인함을 알 수 있었다.

ABSTRACT

In this paper we consider methods for selecting the next tracing node that take advantage of the history of traced positions during the packet-tracing. In the meantime, the proposed routing strategy that counters the tracing is to design the routing path is such a way that nodes on it are not close to the nodes whose location privacy is needed and zigzag or back-and-forth movements hardly take place. In simulations, the ratios of successful tracing were largely improved. It was shown that our routing scheme allows more data packets to be delivered to the destination while, enticing the tracer to move more long distances in the presence of multiple assets.

키워드

도착지-위치 보호 라우팅, 지역 도청에 의한 위치 추적, 무선 센서 네트워크, 위치 기반 라우팅

Key word

Routing for Destination-location Privacy, Local Eavesdropping Based Tracing, Wireless Sensor Networks, Position(Location)-aware Routing

* 상지대학교 (yhtscha@sangji.ac.kr)

접수일자 : 2010. 02. 25
심사완료일자 : 2010. 03. 29

I. 서 론

센서 네트워크에서는 패킷 또는 메시지가 전송될 때마다 발생하는 신호를 감지하여 특정 노드의 위치를 추적하는 지역 도청(local eavesdropping)에 의한 위협으로부터 노드의 위치를 보호하기 위한 라우팅 기법들이 요구된다[1]. 이들은 크게 정보 발생의 근원지(source)의 위치를 보호하기 위한 방안들[3-7]과 정보의 최종 도착지(destination)의 위치를 보호하는 방안들[8,9]로 구분된다. 여기서, 지역 도청이란 공격자를 기준으로 전송 신호를 감지할 수 있는 일정 거리 r 이내에서 패킷 전송 시 발생되는 신호들을 감지하는 능력이다. 근원지 보호 라우팅에서는 전송 패킷에 대한 역방향의 추적에 대응하기 위해 서로 다른 여러 개의 경로들을 사용하여 패킷들을 전송한다. 도착지 보호 라우팅에서는 데이터 패킷 전송 방향과 추적 방향이 일치함을 고려하여 전송 중에 속임수(fake)용 거짓 패킷들을 데이터 패킷과 함께 발생시켜 추적에 혼돈을 주거나 따돌리게 된다.

이 논문과 관련된 위치 기반 라우팅이 가능한 무선 센서 네트워크에서의 도착지 보호와 관련된 라우팅 방안들의 단점은 다음과 같다. 첫째, 추적 모델이 단순하다. 도청을 위해 머물고 있는 현재 노드에서 가장 먼저 전송 신호를 발생시킨 노드로 추적을 이동하거나[3,4] 또는 현재의 노드와 바로 직전에 추적한 노드를 지나는 직선으로부터 가장 가깝게 존재하는 노드로 이동한다[9]. 둘째로, 라우팅에서 설정되는 경로의 궤적이 좌우 또는 전후로 자주 위치를 바꾸는 형태를 취하기 때문에 추적자를 따돌리기 위한 유인 과정이 쉽게 노출될 수 있고, 정보 전달 경로의 길이가 또한 증가된다.

이 연구에서는 위와 같은 문제점들을 개선하여 먼저 지역 도청에 의한 패킷 추적 과정에서 얻어진 노드들의 위치(좌표)들을 이용하여 추적 노드를 보다 정확하게 선정하는 추적 모델을 제안한다. 도착지 노드의 위치 파악을 위한 패킷 추적에 대응하기 위해 제안된 라우팅 방법으로는 근원지 위치 기밀을 강화하기 위해 선행 연구[5,6]에서 제안되었던 접근방안을 확장하여, 패킷 전달 과정에서 속임수용 패킷들을 확률적으로 발생하도록 하여 추적에 혼선을 야기한다. 한편, 경로 구성에는 전후 또는 좌우로 다음-홉 노드들을 선정하지 않게 하여 경로 길이의 증가를 막고 추적자로 하여금 유인 의혹을 낮추도록 한다.

II. 위치 추적

지역 도청에 의한 패킷 추적을 통해 근원지나 도착지의 위치를 파악하고자하는 공격(추적) 모델로 가장 많이 이용되는 것은 가장 먼저 전송 신호를 발생시킨 이웃 노드를 다음의 추적 노드로 선정하는 것이다[3]. 하지만, 추적 과정에 얻어진 노드들의 위치 정보를 활용하지 않는다는 문제점이 있다. 이 논문에서는 다음과 같은 두 가지 모델을 제안한다.

2.1 EL(Earliest and Latest Points) 모델

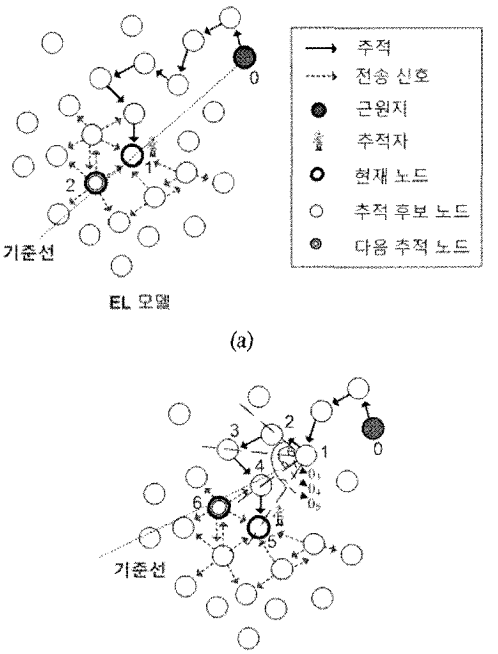


그림 1. 제안된 추적 모델
(a) EL 모델 (b) AA 모델
Fig. 1 The proposed tracing models
(a) EL model (b) AA model

최초의 추적 위치와 현재의 위치를 연결하는 직선 선분에 가장 가까우면서 현재의 위치에서 후진 방향으로 존재하지 않는 노드로 추적을 이동하는 모델이다. 여기서 후진방향이란 추적이 가장 오래전에 이루어졌던 좌표(즉, 현재 기억되어 있는 추적 위치 중 가장 앞서서 이루어진 위치)에 가까움을 의미한다. 예를 들어, 그림 1 a)에서 추적이 근원지 0에서 시작되었고 현재 머무는 노드가 1로 이들의 좌표 $L_0(=(x_0,y_0))$와 $L_1(=(x_1,y_1))$을 지나는 기준선에 대해 노드 1의 이웃 노드들은 모두 5개이지만, 노드 2가 기준선에 가장 가까우면서도 현재의 위치에서 가장 비-후진 방향에 위치하므로 다음의 추적 노드로 선정된다. 여기서, 추적자는 다음 추적 노드를 선정하기 전에 일정 시간 동안 이웃한 노드들로부터 발생하는 신호들을 수집하기 위해 대기함을 가정한다. EL 모델에서는 최초의 추적 위치와 가장 최근의 위치만을 기억하면 된다.

2.2 AA(Average Angle among k points) 모델

이 방법에서는 추적 과정에서 가장 최근에 방문한 k개의 노드들의 좌표 $L_1, L_2, ..., L_k$에 대해 L_1에서 L_2를 연결하는 직선을 우선 기준선으로 결정한다. 그리고 L_1에서 각각의 L_i(단, $L_i=(x_i,y_i)$, i=3, 4, .., k)를 연결하는 직선이 교차하면서 만드는 k-2개의 각 $\Theta_3, \Theta_4, ..., \Theta_k$들로부터 산술 평균 각을 구한 후, 이러한 평균 각을 지나는 직선과 가장 편차가 적으며 현재 위치에서 후진방향에 존재하지 않는 노드를 선정한다. 단, L1는 가장 먼저 추적한 위치 그리고 L_k는 가장 나중에 추적한 즉, 현재 추적자가 머물고 있는 노드의 위치이다. 그림 1 b)는 방문 노드가 1, 2, 3, 4, 5인 경우 다음 추적 노드로 6을 선정한 예이다.

Ⅲ. 제안된 도착지 보호 라우팅

3.1 다음-홉 선정

제안된 라우팅 기법은 매 패킷 전송 시마다 그림 2와 같이 greedy, random_walk, perimeter 등 세 가지 방식에 의해 다음-홉 노드를 선정한다. greedy 모드는 목적지로의 가장 가까운 이웃 노드를 선택하여 목적지로 다가가게 한다. random_walk 모드는 현재보다 목적지에 더 가까운 이웃 노드들 중 임의의 노드를 선정하여 경로 모양의 임의성을 높인다. 그리고 perimeter 모드에서는 목적지와 현재 노드들 중심으로 시계 방향(또는 반시계 방향)으로 존재하면서 위치 보호 대상과 일정 홉(hop) 이웃하지 않는 노드를 다음-홉 노드로 선정하여 위치 보호가 필요한 노드들을 우회하게 한다. 마지막으로, fake 모드는 데이터 패킷과 동일한 크기의 속임수용 거짓 패킷들을 생성하여 추적자로 하여금 실제 데이터 패킷이 전송된 이웃 노드를 찾아내기 어렵게 만든다. 한편, 선정 노드가 존재하지 않거나 이웃한 노드가 이미 모두 고려된 노드들이라면 retreat 모드에 의해 앞서의 노드로 되돌아가게 된다. 제안된 라우팅 기법은 GPSR(Greedy Perimeter Stateless Routing)[10]을 기반으로 random_walk 모드와 fake 모드를 추가 도입하여 도착지 위치 기밀을 보호하기 위해 설계되었기에 GDLP(GPSR-based Destination Location Privacy)로 칭한다.

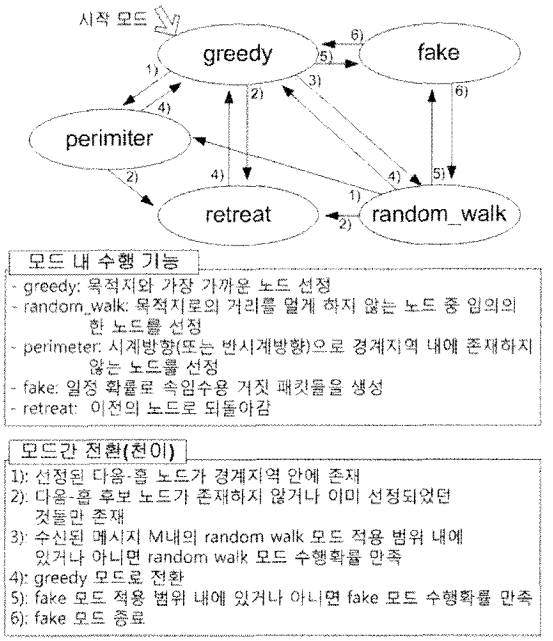


그림 2. 제안된 다음-홉 선정 기법
Fig. 2 The proposed next-hop selection scheme

GDLP에서의 모드간 전환은 다음과 같다. 초기 모드는 greedy이며, 수신 패킷 내에 random_walk 모드의 적용 여부를 나타내는 필드(TTL_{rw})의 값이 0보다 크면 계속해서 random_walk 모드로 이전하여 다음-홉 노드를 선정한다. 그렇지 않으면 greedy 모드에서 목적지에 가장 가

까운 이웃 노드들 다음-홉 노드들 선정한다. 그리고 선정된 노드가 경계 지역 내에 속하는 노드라면 perimeter 모드로 다시 천이 한다. 그렇지 않고 greedy 모드에 남아 있는 경우에는 임의의 변수 p의 값(0<p<1)을 무작위로 생성한 후, 그 값이 속임수 패킷을 수행할 확률 p_{fake}보다 작으면 데이터 패킷의 전송과 함께 속임수 패킷들을 생성한다. 이러한 속임수 패킷들의 생성은 random_walk 모드에서도 동일하게 적용된다. 한편, perimeter 모드에서는 목적지와 현재 노드들 중심으로 시계 방향 또는 반시계 방향 중 어느 방향으로 다음 홉 노드들 선정할 지는 근원지 노드에 의해 전송되는 패킷 내에 명시된다. 사용되는 패킷의 형식과 일반적인 사항은 [5,6]에 자세히 나와 있다.

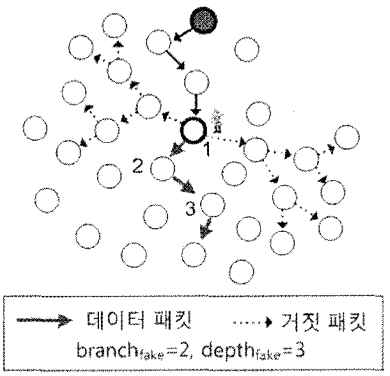


그림 3. 속임수용 거짓 패킷의 생성 예
Fig. 3 Example of fake packets generation

3.2 속임수용 거짓 패킷의 생성

fake 모드에서는 몇 개의 노드들이 거짓 패킷을 생성할지를 나타내는 변수 $branch_{fake}$와 이러한 과정이 몇 개의 홉에 걸쳐 지속적으로 반복되는지를 나타내는 변수 $depth_{fake}$에 의해 속임수용 패킷들의 생성량이 결정된다. 예를 들면, 그림 3의 현재 노드 1에서 fake 모드가 수행되어 이웃한 두 개의 노드가 지정된 후, 이들로부터 각기 두 개의 노드가 선정되고 다시 이와 같은 과정을 한 번 더 반복하여 총 $branch_{fake}(branch_{fake}^{depth}fake\text{-}1) = 2(2^3\text{-}1) = 14$ 개의 거짓 패킷들이 생성되었다(점선으로 나타낸 화살표 방향의 노드들을 주목). 여기서, 데이터 패킷은 거짓 패킷과 별도로 노드 2와 3을 거쳐 전달되고 있다. 일반적으로 변수 $branch_{fake}$와 $depth_{fake}$의 값이 증가하면 생성되는 속임수용 거짓 패킷들의 수는 지수적으로 (exponentially) 늘어나 추적자가 실제 데이터 패킷을 추적하기도 그 만큼 어렵게 된다.

Ⅳ. 평 가

4.1 시뮬레이션 설정

대규모 센서 네트워크에서의 라우팅 차원에서의 위치 보호 능력의 평가에 집중하기 위해 관련 연구들[3-9]처럼 물리 계층이나 MAC(Medium-Access Control) 계층의 기능은 포함하지 않고 라우팅 기능만을 Java 언어로 구현하여 사용하였다. 평가 프로토콜은 제안한 GDLP와 기존의 가장 우수한 도착지 보호 능력을 보여주는 LPR[9]이며, 추적 성공률, 안전 기간, 경로 길이, 추적(이동)거리 및 총 패킷 발생량 등에 대해 평가하였다. 시뮬레이션에 사용된 주요 파라미터의 설정 값은 표 1과 같다.

표 1. 파라메타 설정
Table. 1 Configuration of Major Parameters

파라메타		값 또는 범위
노드 수		50,000
노드의 평균 차수		8
h_{s-b}		30, 50, 70
N_s		N의 0.4%, 0.6%, 1.2%
생성 토폴로지 수		100
도착지로의 메시지 전송 수		1000
추적 모델		FS, RS, EL, AA
GDLP	P_{tx}	0.05
	TTL_{tx}	h_{s-b}의 [5%, 10%] 중 임의 선택(최소 2)
	β	2r (r은 전송 거리)
	α	r (=1)
	P_{fake}	0.20
	$Branch_{fake}$, $Depth_{fake}$	2, 3
LPR	P_{closer}, $P_{further}$	0.875, 0.125
	P_{fake}	0.20
	$Branch_{fake}$, $Depth_{fake}$	1, 7

시뮬레이션에서는 100개의 서로 다른 네트워크 토포롤지들을 생성하여 실행하였고, 측정치의 최고 10개와 최저 10개를 제외한 나머지의 값들에 대해 산술 평균을 내었다. 추적 능력을 비교하기 위해 고려된 추적 모델은 FS(First Signal), RS(Random Selection), EL(Earliest and

Latest Points) 및 AA(Average Angle among K-point) 등이다. 속임수용 거짓 패킷을 생성할 확률 P_{fake}은 GDLP와 LPR 모두 0.2로 하고, 거짓 패킷의 생성 범위와 규모는 표1에서와 같이 프로토콜별로 달리하였다. 추적 모델 AA에서는 9개 이상의 추적 위치들을 이용하면 유사한 추적 성공률에 나타내었기에 k=9인 경우만을 고려하였다.

4.2 결과 및 평가

활동 근원지와 도착지간의 최단 거리가 50-홉 즉, $h_{s\text{-}b}$=50이며 휴면 근원지는 없는(N_s=0)인 경우에 대해 제안된 라우팅 기법 GDLP를 대상으로 위치 추적 모델 FS, RS, EL 및 AA의 추적 성공률을 비교하였다(그림 4). 단, 여기서는 속임수용 거짓 패킷을 생성할 확률 p_{fake}=0.1과 0.2일 두 가지 경우에 대한 결과를 나타내었다. 전체적으로 EL과 AA가 다른 모델에 비해 크게 우수한 추적 성공률을 보였고, 관련 연구들에서 고려되었던 FS는 RS보다도 낮은 추적 능력을 보였다.

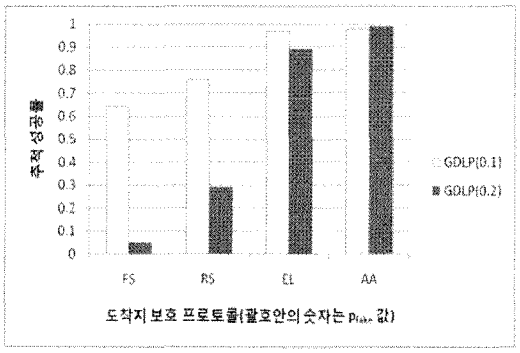
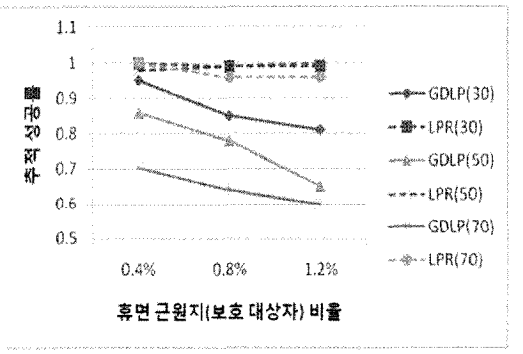
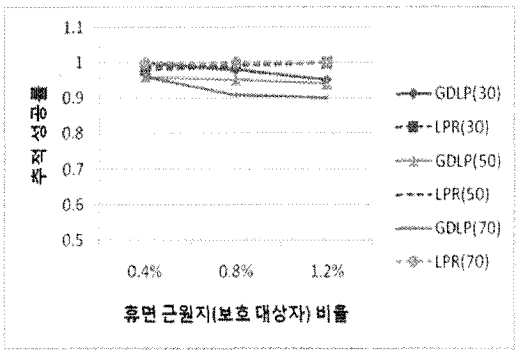


그림 4. 추적 성공률 비교
Fig. 4 Comparison of trace success ratios

그림 5는 통신 거리 $h_{s\text{-}b}$와 휴면 근원지 수 N_s의 변화에 따른 EL과 AA의 추적 성공률이다. 휴면 근원지 수가 증가함에 따라 GDLP의 경우 추적 성공률을 낮추는 효과가 있었지만, LPR의 경우에는 거의 100%에 가깝게 도착지 추적을 허용하였다. Ns의 증가에 따라 GDLP는 경계 지역이 더 많아져 이들을 우회하는 과정에서 경로 선정이 불규칙하게 되어 추적 성공률을 다소 낮추는 효과가 있다. 하지만, LPR의 경우에는 경계 지역을 우회하는 기능이 없기 때문에 추적 중 다른 보호 대상의 위치가 노출되어 추적 성공률을 낮추는 효과가 거의 나타나지 않았다.



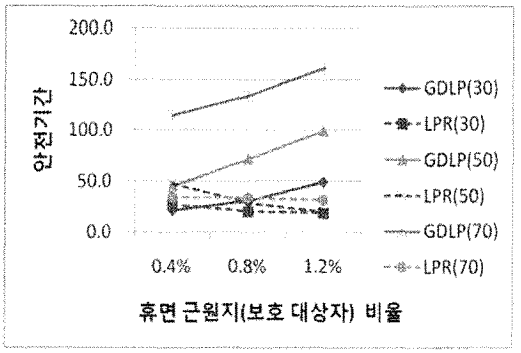
(a)



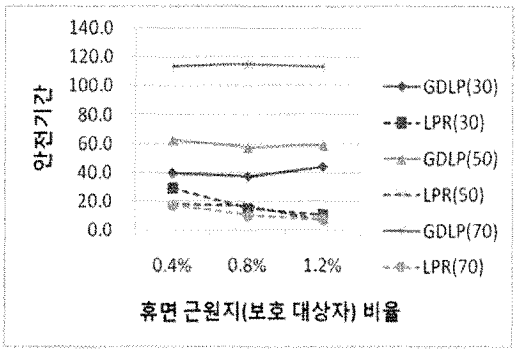
(b)

그림 5. 추적 성공률
(a) EL 모델 적용 (b) AA 모델 적용
Fig. 5 Comparison of trace success ratios
(a) Under EL model (b) Under AA model

안전 기간에 대해서, LPR은 N_s의 증가와 함께 GDLP와 커다란 차이를 보이며 감소하였다(그림 6). GDLP는 EL 모델에 대해서는 N_s의 증가와 함께 안전 기간도 증가하였지만 AA 모델에서는 큰 차이가 없었다. 이는 AA에서는 최근의 9개의 위치만을 분석하여 다음 추적 노드를 선정하므로 거짓 패킷들의 발생과 거의 무관하게 다음-홉이 결정되기 때문이다. 그리고 GDLP에서는 통신 거리가 멀수록 안전 기간도 커졌지만 LPR에서는 차이가 거의 없었다. 왜냐하면 LPR은 경계 지역을 우회하여 라우팅 과정에서의 위치 보호가 필요한 노드들의 위치를 지켜주지 못하였기 때문이다.

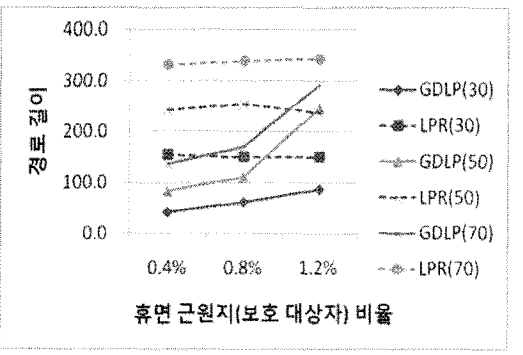


(a)

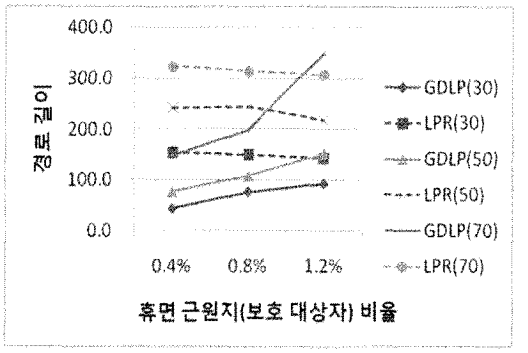


(b)

그림 6. 안전 기간
(a) EL 모델 적용 (b) AA 모델 적용
Fig. 6 Comparison of safety periods
(a) Under EL model (b) Under AA model



(a)

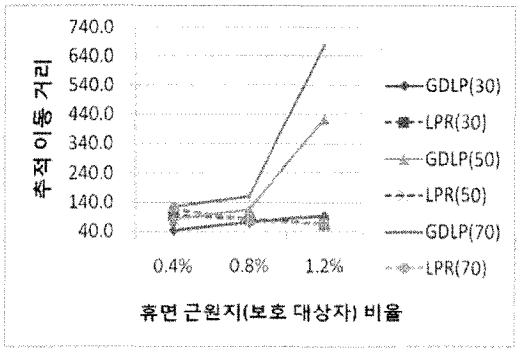


(b)

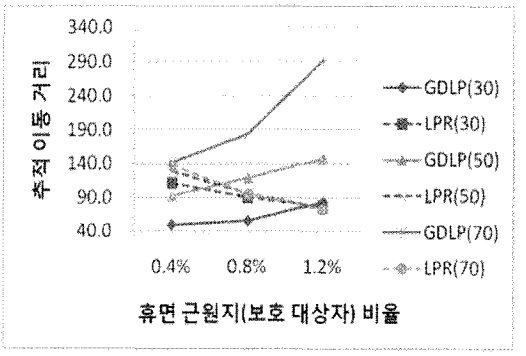
그림 7. 경로 길이
(a) EL 모델 적용 (b) AA 모델 적용
Fig. 7 Comparison of path lengths
(a) Under EL model (b) AA model

다음으로 위치 추적자가 목적지를 발견하기까지 성공적으로 전송한 데이터 패킷이 사용한 경로들의 평균 길이(홉 수)를 측정하였다. 이는 전달 패킷의 지연시간을 간접적으로 측정하기 위한 것이다. 전체적으로 LPR의 사용 경로의 길이가 GDLP보다 매우 길게 나타나 경로가 더 길었다(그림 7). 이는 LPR은 확률 $p_{further}$(실험에서는 이 값은 0.125로 설정되었다)만큼 현재 노드보다 목적지로 더 멀어지는 이웃 노드를 다음-홉 노드로 결정하였기 때문이다. GDLP의 경우에는 N_s가 0.8%를 넘어서면서부터 경로 길이가 급격히 증가하였는데 이는 보호 대상자의 증가에 따라 이들을 우회하는 perimeter 라우팅이 빈번해지면서 경로 길이가 급속히 늘어나기 때문이다.

위치 추적자가 목적지를 발견하기까지 이동한 홉 수인 이동 거리는 그 값이 클 수 록 공격자를 효과적으로 유인하여 공격자의 전원 소모를 유발하거나 이동에 따른 시간 지연을 유발하는 정도를 나타내는 지표이다. 따라서 이 값이 클수록 좋은 라우팅 전략이라 할 수 있다. GDLP가 LPR보다 위치 추적자로 하여금 더 많은 거리를 이동하도록 유인한 것으로 나타났고, N_s가 0.8%를 넘어서면서부터 더욱 증가함으로 보였다(그림 8). 하지만, LPR은 라우팅 과정에서 추적자에게 휴면 근원지의 위치를 노출시킴으로 인해 조기에 라우팅이 종료 되어 N_s가 증가할 수 록 공격자의 추적 이동 거리가 감소함을 보였다.

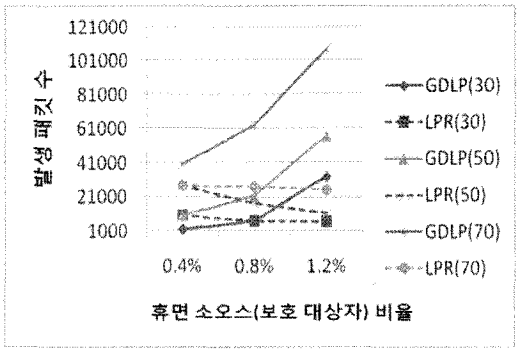


(a)

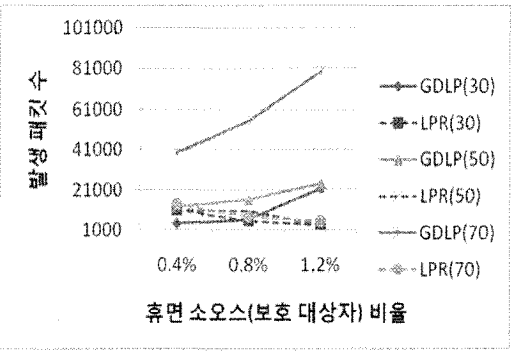


(b)

그림 8. 추적 이동 거리
(a) EL 모델 적용 (b) AA 모델 적용
Fig. 8 Comparison of tracing movements
(a) Under EL model (b) Under AA model



(a)



(b)

그림 9. 패킷 발생 수
(a) EL 모델 적용 (b) AA 모델 적용
Fig. 9 Comparison of generated packets
(a) Under EL model (b) Under AA model

마지막으로 활동 근원지에서 목적지로 데이터 패킷들을 성공적으로 전송하는 과정에서(즉, 안전 기간 내에) 속임수용 거짓 패킷을 포함한 전체적으로 발생한 패킷들의 수를 측정하였다. 그림 9에 나타나듯이 N_s가 증가함에 따라 GDLP를 사용하므로 써 발생하는 패킷들의 수가 LPR의 경우에 비해 크게 증가하였다. GDLP는 통신 거리가 멀수록 전체적으로 통신비용도 더 높아졌는데 이는 통신거리가 길 수 록 거짓 패킷들의 발생 수도 더 증가하였기 때문이다. 반면에, LPR은 라우팅 과정에서 휴면 근원지들을 우회하지 못하고 중간에 추적자에게 휴면 근원지의 위치를 노출시 조기에 라우팅이 종료되므로 인해 패킷의 발생량이 적었다.

V. 결 론

이 논문에서는 종래의 추적 모델과 달리 추적 과정에서 얻어진 좌표들을 이용하는 추적 모델로 EL과 AA를 제안하였다. 그리고 위치 보호가 필요한 대상들이 다수 존재하는 환경에서 도착지 추적을 어렵게 하는 라우팅 기법 GDLP를 제안하였다. 시뮬레이션을 통해 AA와 EL 모두 기존의 RS이나 FS보다 매우 높은 추적 성공률을 나타냄을 확인하였다. 특히, AA는 속임수 패킷의 발생과 무관하게 거의 일정하게 우수한 추적 성공률을 보였다. GDLP는 현재까지 가장 우수한 도착지 보호 능력을 제공하고 있는 것으로 알려진 LPR에 비해 보다 많은 데이

터 패킷을 전달하였다. GDLP는 추적자에 대해 지그-재그나 앞뒤로 움직이는 형태를 반복하지 않고도 더 많은 거리를 이동하도록 할 수 있음이 관찰되었다.

추후 연구로, 생성되는 속임수용 거짓 패킷의 수를 더 적게 발생하면서도 높은 안전 기간을 확보하는 방법이 요구된다. 또한 추적 과정에서 발생 신호들을 수집하기 위해 소요되는 대기 시간을 고려할 필요가 있다. 그리고 MAC 계층 프로토콜의 동작 특성과 라우팅 과정의 큐잉 분석이나 손실 또는 지연 등과 같은 동적 요소의 고찰을 위해 NS-2와 같은 공인된 시뮬레이션 도구를 이용한 후속 연구가 기대된다.

참고문헌

[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, Issue. 8, pp.1501-1514, 2009.

[2] J. Yick, B. Mukherjee, and D. Ghosal, "Wireless sensor network survey," *Computer Networks*, Vol. 52, No.12, pp.2292-2330, 2008.

[3] C. Ozturk, Y. Zhang, and W. Trappe, "Source-location privacy in energy-constrained sensor network routing," *Proc. of the 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 ICDCS'05*, pp.599-608, 2005.

[5] 양기원, 임 화정, 차 영환 "휴면 소오스들이 존재하는 환경의 센서 네트워크를 위한 위치 보호 강화 라우팅" 한국정보과학회논문지: 정보통신, 제36권, 제1호, pp.12-23, 2009.

[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, Dec., pp.589-598, 2009.

[7] Y. Ouyang, Z. Le, G. Chen, and J. Ford, "Entrapping adversaries for source protection in sensor networks," *Proc. of the WoWMoM'06*, pp.23-32, 2006.

[8] 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.

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

[10] B. Karp and H.-T. Kung, "Greedy perimeter stateless routing for wireless networks," *Proc. of the MobiCom'00*, pp.243-254, 2000.

저자소개

차영환(Yeonghwan Tscha)

1983년 인하대 전산계산학과 (학사)
1985년 KAIST 전산학과(석사)
1993년 인하대학교 대학원(박사)
1985~2000년: 한국전자통신연구원 선임연구원
1986~1987년: 미국 NIST 객원과학자
2004~2005년: 터어키 보스포러스대학 객원교수
1994~현재: 상지대학교 컴퓨터정보공학부교수
※관심 분야: 네트워크 구조, 통신 프로토콜, 네트워크 보안