Regular paper
Journal of the KIECS. pp. 861-868, vol. 11, no. 9, Sep. 30 2016, t. 77, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2016.11.9.861

센서 네트워크에서 위치 기밀 수준에 따른 더미 메시지 생성

차영환*

Generation of Dummy Messages Depending Upon the Location Privacy Level in Sensor Networks

Yeong-Hwan Tscha*

요 약

센서 네트워크에서 광역 도청에 대응하여 기지국이나 근원지들의 위치 기밀을 유지하기 위해서는 일반적으로 더미 메시지들을 발행해야한다. 이 논문에서는 기지국과 근원지들 간에 통신 경로를 확보하는 한편, 요구되는 기밀 수준을 고려하여 일정 수의 노드들을 아무런 활동도 하지 않는 휴면 상태로 전환하도록 하여 전체 더미 메시지들의 발생을 줄이는 방법을 제안한다. 시뮬레이션을 통해 기지국과 근원지들 간의 경로 설정 성공률과 그들의 위치 기밀 수준을 검증한다.

ABSTRACT

Dummy messages are usually generated for faking in preserving the location privacy of a sink or source against the global eavesdropping in wireless networks. In this paper, we propose a new method in which a certain number of nodes determined by considering the required privacy level are made to transit to the dormant state doing nothing so that the total number of dummy messages is reduced, while the paths from the sink to the sources are ensured. Through simulation we verify the success ratio of path establishments between the sink and a set of sources and the location privacy level of them.

키워드

Dummy Message, Global Eavesdropping, Location Privacy in Sensor Networks, Protocol Design
더미 메시지, 광역 도청, 센서 네트워크, 위치 기밀, 프로토콜 설계

Ⅰ. 서 론

무선 네트워크에서는 메시지 전송 시마다 일정 세기의 전파 신호가 방사된다. 이러한 신호들을 포착하면 메시지가 생성된 근원지(source)로부터 메시지를 중계하는 중간의 노드들을 거쳐 최종 도착지(destination) 즉, 기지국(sink 또는 basestation)에 이르는 일련의 노드들의 위치를 파악하여 해킹이나 파괴 등은 물론, 노드들 간의 통신 관계, 시간, 정보량 등을 파악하는데 활용될 수 있다[1-2]. 더욱이 네트워크 전역에 걸친 수동적 광역도청(passive global eavesdropping)은 통신 노드들 사이에 어떠한 방해나

* 교신저자 : 상지대학교 컴퓨터정보공학부
• 접 수 일 : 2016. 08. 29
• 수정완료일 : 2016. 09. 13
• 게재확정일 : 2016. 09. 24
• Received : Aug. 29, 2016, Revised : Sep. 13, 2016, Accepted : Sep. 24, 2016
• Corresponding Author : Yeong-Hwan Tscha
Dept of Computer Science and Engineering, Sangji University
Email : yhtscha@sangji.ac.kr

개입 없이 수행되므로 탐지가 어렵다.

이에 대응하는 무선 센서 네트워크를 위한 대표적인 데이터 전송 기법에는 PCM(: Periodic Collection Method)이 있다[3]. 모든 노드들이 매 시각마다 데이터 메시지 또는 동일한 길이의 의미 없는 더미(dummy) 메시지 중 어느 하나를 반드시 전송하게 함으로써 마치 모든 노드가 통신하는 것처럼 보이게 한다. 노드들의 신호 발생 밀도가 일정하므로 기지국이나 근원지들의 위치 기밀 수준을 최고로 유지할 수 있다. 하지만 매 시각 메시지를 발행해야 하므로 배터리를 사용하는 노드들의 전력소모가 과중하게 된다.

또 다른 연구[4]에서는 모바일 기지국을 수용하는 센서 네트워크에 있어서 근원지들을 포함한 일정 지역 내의 노드들에 한해서만 PCM과 같이 동작하도록 제한함으로써 그 밖의 노드들의 더미 메시지 발행을 억제하고 전원 절약을 도모하였다. 하지만 데이터 발생에 관한 패턴이 미리 알려져 있지 않거나 근원지들이 네트워크 전역에 걸쳐 고르게 산재되어 있을 때에는 그 효과를 기대할 수 없다.

이 논문에서는 이러한 제약점이 없이 일반적인 무선 네트워크에 적용 가능하면서 과중한 더미 메시지의 발행을 억제하는 방법을 제안한다. 네트워크 내의 각 노드는 확률 변수를 생성하여 자신이 데이터 전송 단계에서 아무런 활동을 하지 않고 휴면(dormant) 상태로 남아 있을 지를 결정한다. 이 때 확률 변수의 기준치(threshold)는 기지국이나 근원지들의 위치 기밀 수준을 반영하여 결정된다.

한편, 확률적 브로드캐스팅을 이용한 더미 메시지 감축을 언급한 연구[5]가 있었지만 확률과 위치 기밀 유지 수준과의 관계를 제시하지 않았고, 기지국과 근원지들 간의 경로 단절 문제도 다루지 않았다. 또한 확률적 브로드캐스팅에서는 휴면 노드란 개념 없이 각 노드가 전송 메시지가 있을 때마다 확률에 따라 전송 여부를 결정하므로 노드들의 신호 밀도가 균등하지 않을 수 있다.

연구와 관련된 용어 및 수동적 광역 도청 공격자 모델 등에 관해서는 유사 연구들[3-5]을 따른다. 전송 정보는 내용의 기밀성을 유지하기 위해서는 적절한 암호 체계[6-8]을 사용함을 가정한다.

다음 장에서는 제안된 접근 방식과 이를 수행하기 위해 사용되는 메시지들 및 동작 절차를 기술한다. Ⅲ장에서는 시뮬레이션을 통해 제안 방식의 타당성을 검증한다. 연구의 결론은 Ⅳ 장에서 언급한다.

Ⅱ. 제안 방식

2.1 접근 방법

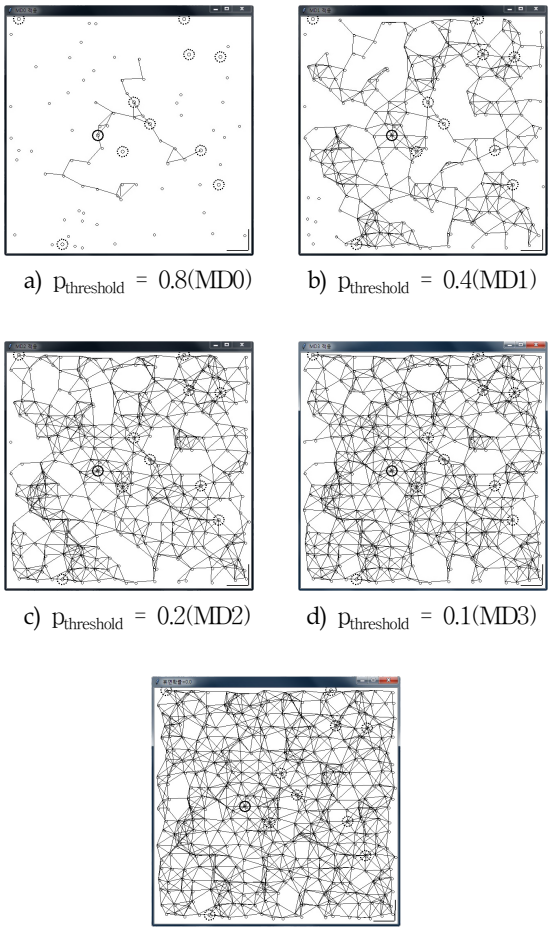
기지국이나 근원지들은 데이터 메시지의 수신이나 발송을 위해 데이터 전송 과정에서 활성 상태를 유지해야 한다. 하지만 기지국과 근원지들 사이의 경로 상의 노드들과 더미 메시지들을 발행하여 기지국과 근원지들의 위치 기밀 유지에 기여할 일정한 노드들 외에는 굳이 활동 상태를 유지하며 더미 메시지를 양산할 필요가 없다. 이러한 노드들을 비활동적인 휴면 상태에 머물게 함으로써 일정 수의 더미 메시지들의 발생을 예방할 수 있다.

기지국이나 근원지가 아닌 노드들은 초기의 휴지(idle) 상태에서 확률 변수 $p_{dormant}$를 생성하여 기준치 $p_{threshold}$에 대해 $p_{dormant} \leq p_{threshold}$ 이면 준 휴면(semi-dormant) 상태로, 그렇지 않으면 준 활성(semi-active) 상태로 전환한다(단, $0 < p_{dormant}, p_{threshold} < 1$). 여기서 준 휴면 상태와 준 활성 상태가 필요한 이유는 기지국과 근원지들 간의 데이터 전송을 위한 경로가 확보되었는지 확인하는 과정을 위해서이다. 경로가 존재하지 않는 경우, 준 휴면 상태의 노드들 중 일부는 준 활성 상태로 바뀌어 경로 설정에 참여한다. 경로가 확정된 후에 준 휴면 상태의 노드들은 휴면 상태로 남아 아무런 활동도 하지 않고, 그 외의 노드들은 활성 상태로 전환하여 데이터 전송 단계를 맞이한다.

2.2 배수적 감소(MD: Multiple Decrease)

경로 단절 문제를 해결하기 위해 $p_{threshold}$ 값을 배수적 감소(MD: Multiple Decrease) 형태로 조정한다. 즉, 기지국은 근원지와의 사이에 경로가 존재하지 않으면 준 휴면 상태의 노드들로 하여금 $p_{threshold}$ 값을 그 이전의 반으로 줄이는 $p_{threshold} = p_{threshold}/2$를 수행하고, $p_{dormant} \leq p_{threshold}$이면 준 휴면 상태를 유지하되 그렇지 않으면 준 활성 상태로 전환하도록 요청한다. 이러한 과정은 최대 3번으로 제한하는데 $p_{threshold}$ 값이 0.8과 같이 크더라도 3번에 걸친 배수적 감소를 적용

하면 0.4, 0.2, 0.1로 급격히 감축 되어 그 효과가 미미해지기 때문이다. 이러한 재조정 후에도 경로 설정에 실패하면 맨 마지막으로 모든 노드를 활성 상태로 전환하여 데이터 전송용 경로가 확보되도록 한다.



a) $p_{threshold}$ = 0.8(MD0) b) $p_{threshold}$ = 0.4(MD1)

c) $p_{threshold}$ = 0.2(MD2) d) $p_{threshold}$ = 0.1(MD3)

e) $p_{threshold}$ = 0.0

그림 1. 배수적 감소(MD) 적용 효과
Fig. 1 Effects by applying MD

그림 1에 400개의 노드들로 형성되는 네트워크에 있어서, 하나의 기지국(그림 a)에서 짙은 색 바깥 원이 더 있는 노드)과 10개의 근원지들(그림 a)에서 점선의 바깥원이 더 있는 노드)을 무작위로 생성하고, 배수적 감소 적용에 따른 기지국과 근원지간의 경로의 연결 여부와 준 활성 노드들의 밀도를 상대적으로 비교해 볼 수 있게 나타내었다. 각 그림의 하단 우측 모서리에는 무선 셀의 반지름 길이를 x-축과 y-축으로 표시하여 참고가 되게 하였다.

a)는 $p_{threshold}$ = 0.8로 배수적 감소가 적용되기 전(MD0) 준 활성 노드가 80개일 때이다. 즉 1-$p_{threshold}$ = 0.2이므로 400개의 노드들 중 20%에 해당하는 80개가 무작위로 선정되어 준 활성 상태인 경우이다. 기지국은 3개의 근원지들과 연결되어 있고 나머지 7개와는 단절되어 있다. b)는 배수적 감소 1차(MD1) 적용에 의해 $p_{threshold}$ = 0.4로 반감된 후로, 좌측 최상단의 하나의 근원지만을 제외하고 나머지 근원지들은 기지국과 연결되어 있다. c)와 d)는 배수적 감소 2차(MD2)와 3차(MD3)를 적용하여 $p_{threshold}$ = 0.2와 $p_{threshold}$ = 0.1인 경우이다. e)는 $p_{threshold}$ = 0.0으로 모든 노드가 활성화된 PCM[3]과 같은 모습이다. 만일 기지국과 근원지들 사이에 데이터 전송용 경로가 모두 존재하는 c)와 d)에서 그림에 보이는 준 활성 노드들이 모두 활성화되고 나머지들은 휴면 상태가 되어 더 이상 활동하지 않는다고 하자. 그러면 e)에 비해 더미 메시지 발생을 줄이면서도 기지국이나 근원지들의 위치 기밀을 일정 수준 유지할 수 있다. 이것이 이번 연구의 핵심이다.

표 1. 사용 메시지들과 용도
Table 1. Messages and their usages

messages	usage	originator	destination	major fields
PP (Path Prove)	prove the path between each source-sink	sink	sources	source_list: a list of all sources
PC (Path Confirm)	confirm the path from a source to the sink	source	sink	-
MD (Multiplicative Decrease)	ask to make more semi-active nodes	sink	semi-dormant nodes	round: number of MD trials
PE (all Paths established)	inform all paths established	sink	all nodes	-

2.3 메시지 및 동작 과정

제안된 방식에서 사용되는 메시지들은 표 1에 나타내었다. 모든 노드가 동기화 되어 일정한 타임 슬롯(time slot)마다 메시지를 전송함을 가정하고, 제안 방

법의 동작 과정을 기지국, 근원지 및 그 밖의 노드들로 구분하여 기술하면 그림 2, 3, 4와 같다.

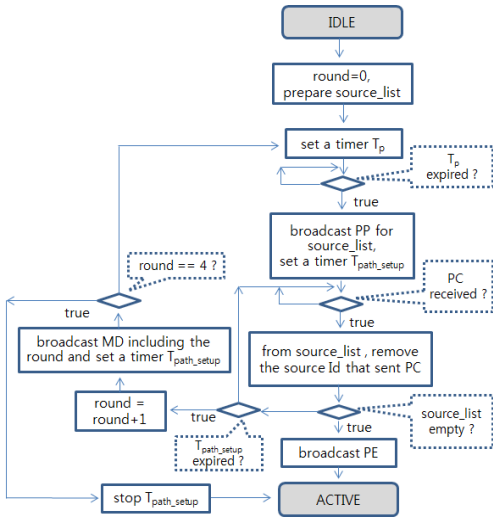


그림 2. 휴면 노드 설정을 위한 기지국의 절차
Fig. 2 Procedure for a sink to set up dormant nodes

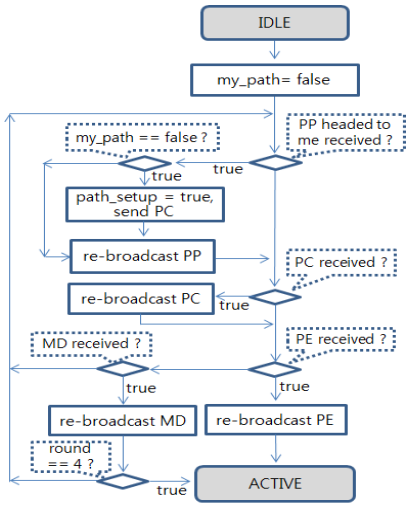


그림 3. 휴면 노드 설정을 위한 근원지의 절차
Fig. 3 Procedure for a source to set up dormant nodes

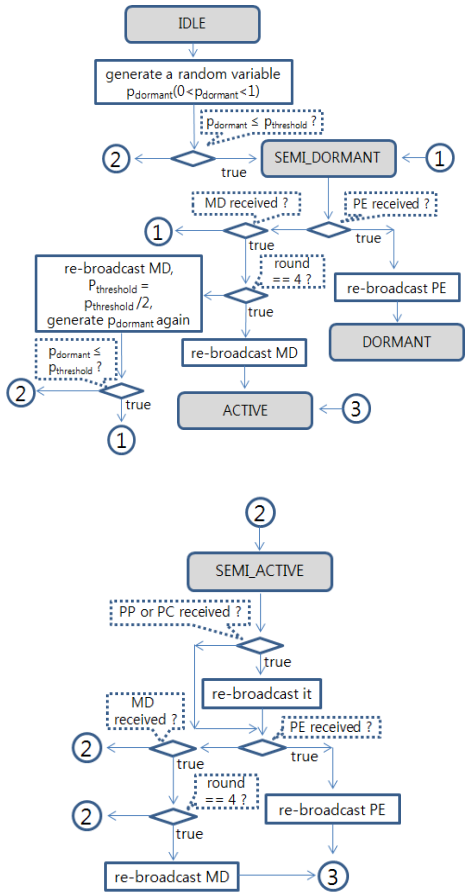


그림 4. 휴면 노드 설정을 위한 기타 노드들의 절차
Fig. 4 Procedure for others to set up dormant nodes

준 휴면 상태의 노드들은 기지국과 근원지들 간에 경로 존재를 확인하기 위해 교환하는 메시지인 PP(Path Prove)나 PC(Path Confirm)에는 관여하지 않는다. 배수적 감소를 알리는 메시지 MD(Multiple Decrease)와 경로 설정이 모두 확인됨을 알리는 메시지 PE(all Paths Established)에 대해서만 반응한다.

시작과 함께 근원지들과 기지국외의 모든 노드는 $p_{dormant}$를 생성하고 자신을 준 휴면 또는 준 활성 노드로 결정하게 된다. 그림 2와 같이 기지국은 이러한 결정에 소요되는 시간 T_p가 경과되면, source_list내의 근원지들과의 사이에 준 활성 노드들로 형성되는 경로가 존재하는 지를 확인하기 위해 메시지 PP를 전송한다. PP를 수신한 각각의 근원지는 그림 3과 같이

경로 확인에 응답하는 메시지 PC를 전송한다. 기지국은 PP 전송 후, T_{path_setup} 기간 내에 모든 근원지로부터 PC가 오지 않으면 배수적 감소의 이행을 요구하는 메시지 MD를 전송한다. 이어서 T_p 경과 후, PP를 재발송하여 경로 존재여부를 확인하게 된다. 모든 근원지들로부터 PC가 도착하면 모든 노드들에게 PE 메시지를 전송하여 준 휴면 상태의 노드는 휴면 상태로, 준 활성 상태의 노드는 활성 상태로 확정한다. 만일 3회까지 반복된 배수적 감소 적용 후에도 경로 검증에 실패하면 모든 준 휴면 상태의 노드들을 활성 상태로 전환하는 마지막 메시지 MD가 기지국에서 발송된다. 최종적으로 활성 상태의 노드들만이 PCM[3]과 같은 방법으로 데이터를 전송하게 된다.

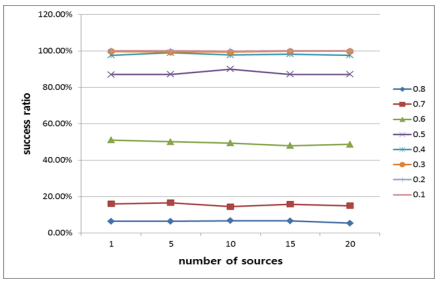
III. 평 가

3.1 시뮬레이션 설정

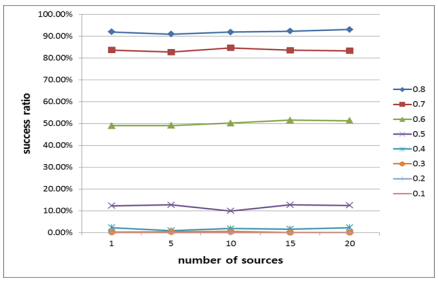
제안 방식의 유용성을 검증하기 위해 시뮬레이션에서 표 2와 같이 주요 파라미터들의 값을 설정하였다. 시뮬레이션 S/W는 파이썬 3.5.1 언어로 구현하여 다음과 같은 두 가지 항목을 측정하였다. 즉, 배수적 감소 적용에 따른 경로 설정의 성공 비율과 경로 설정과 휴면 노드들이 결정된 후의 데이터 전송 단계에서 기지국이나 근원지의 위치 기밀 정도이다. 모든 결과는 300개의 무작위로 생성된 네트워크 토폴로지들에 대해 얻어진 것들에 대해 평균을 취하였다.

표 2. 시뮬레이션을 위한 주요 파라미터 설정
Table 2. Major parameters for simulation

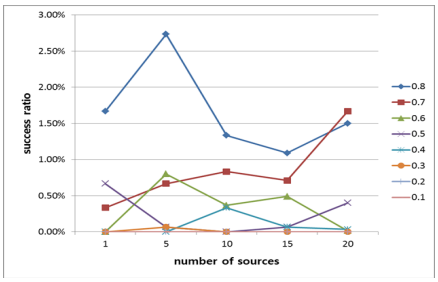
parameters	values
area	600 x 600 (㎡)
radio radius	54(m)
no. of nodes	400
no. of sources	1, 5, 10, 15, 20
avg node degree	8.78
thresholds of $p_{dormant}$	0.1 thru 0.8 with interval 0.1
no. of topologies	300



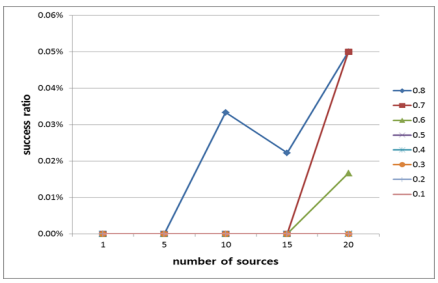
a) MD0



b) MD1



c) MD2



d) MD3

그림 5. 경로 설정 성공률
Fig. 5 Success ratio of connection setups

3.2 시뮬레이션 결과

먼저 $p_{threshold}$가 0.8. 0.7, 0.6., 0.4, 0.3, 0.2 및 0.1일 경우, 근원지들의 수를 1, 5, 10, 15, 20으로 늘리면서 배수적 감소에 따른 기지국과 근원지들 간의 설정된 경로들의 비율을 측정하였다. 그림 5는 배수적 감소가 적용되기 전(MD0)의 경로 성공률과 1차(MD1), 2차(MD2), 3차(MD3)에 이어진 배수적 감소를 적용한 후의 성공률이다.

a)에 나타나듯이 $p_{threshold}$ 가 작을수록 경로 설정의 성공률은 높았고, $p_{threshold}$가 크더라도 b)에서 나타나듯이 배수적 감소를 적용 한 후에는 대부분 성공적이었다. 즉, 1차 적용 후 경로의 97.0% 이상까지 확보되어 c)에서는 나머지 약 3%미만에 대해서, 그리고 2차까지 적용한 후에는 99.95%가 완료되어 나머지 0.05%에 대해 d)와 같이 확보되었다. MD3까지 이르게 된 것은 MD0에서 $p_{threshold} \geq 0.7$인 경우였다. MD0에서 즉, 처음에 $p_{threshold} \leq 0.5$이면 적어도 MD2까지면 모든 경로가 확보되었다. 흥미롭게도 근원지들의 수가 증가하더라도 경로 설정율과는 거의 무관할 정도로 미미하여(c)와 d) 참조) 배수적 감소에 의한 $p_{threshold}$ 값 변화가 사실상 경로 설정 여부를 결정짓는 것으로 나타났다.

기지국이나 근원지의 위치 기밀 수준을 측정하기 위해 근원지들의 수 g와 네트워크 내의 전체 노드들의 수 N 및 임의의 노드가 휴면 노드가 될 확률 $p_{dormant}$를 고려하자. PCM에서 도청자가 근원지나 도착지 어느 하나를 선택할 확률 $p_{PCM} = (g+1)/N$ 이다. 제안된 방식(편의상 MD라 하자)에서 $p_{dormant} \leq p_{threshold}$ 이고 네트워크 내의 활성 노드 수는 $N \bullet (1-p_{threshold})$ 이므로 근원지나 기지국 어느 하나가 무작위로 선택될 확률 $p_{MD} = (g+1)/(N \bullet (1-p_{threshold}))$이다. 위치 기밀 수준은 이러한 확률의 엔트로피(entropy)로 정의되어[3]. 어떤 노드의 위치 기밀 수준이 k(>0)라면 그 노드의 위치가 밝혀질 확률이 $1/2^k$임을 뜻한다. 따라서 PCM의 위치 기밀 수준 $L_{PCM} = -\log_2 p_{PCM} = \log_2 N - \log_2(g+1)$로, 제안 방법의 위치 기밀 수준 $L_{MD} = -\log_2 p_{MD} = \log_2 N + \log_2(1-p_{threshold}) - \log_2(g+1)$로 주어진다. 일반적으로 제안 방식은 $\log_2(1-p_{threshold})$ 만큼 PCM보다 낮은 위치 기밀 수준을 제공하며 $p_{threshold} = 0$일 때는 동일하게 된다. 제안 방식에서 더미 메시지의 발생 규모를 결정하는 $p_{threshold}$는 N, g 및 L_{MD}이 주어진 경우 다음과 같은 식을 얻는다.

$$p_{threshold} = 1-[(g+1)2^{L_{MD}}/N] \quad (1)$$

그림 6에 서로 다른 $p_{threshold}$에 대한 근원지나 기지국의 위치 기밀 보호 수준을 나타내었다. 이는 표2와 같은 조건으로 시뮬레이션을 실시하고 기지국과 근원지들 사이에 성공적으로 경로가 존재할 때에 측정된 값들이다. 일반적으로 근원지들의 수가 증가함에 따라 위치 기밀 수준은 낮아진다. $p_{threshold} \rightarrow 0$일수록 제안 방법은 PCM에 가까운 기밀 수준을 보여준다. MD0에서 $p_{threshold}=0.3$ 또는 0.2로 시작하면, PCM에 매우 근접한 위치 기밀을 제공하면서 1차적인 배수적 감소만으로도 기지국과 근원지들 간의 경로를 확보하고, 전체 노드의 30% 또는 20% 정도를 휴면화 하여 더미 메시지의 발생을 그 만큼 줄일 수 있어 권장할만하다고 할 수 있다.

식 (1)에서 전체 노드 수 N=400과 근원지들의 수 g=5에 대해, 원하는 기지국이나 근원지의 위치 기밀 수준 $L_{MD}=5$라고 하면 $p_{threshold} \leq 0.52$이어야 하는데 이는 그림 6에서도 바로 확인된다. 만일 같은 조건에서 근원지들의 수가 15이상이라면 이러한 기밀 수준은 달성할 수 없음도 알 수 있다. 이처럼 제안된 접근 방식을 이용하면 근원지들의 수와 원하는 위치 기밀 유지 가능 여부와 유지 가능 시, 이에 부합하는 $p_{threshold}$를 결정할 수 있어 PCM에 비해 더미 메시지들을 줄일 수 있다.

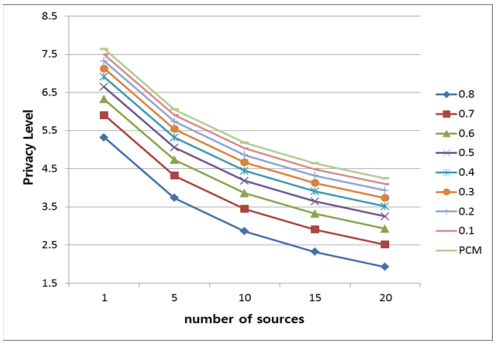


그림 6 근원지나 기지국의 위치 기밀 수준
Fig. 6 Location privacy level of a source or sink

Ⅳ. 결 론

이 논문에서는 센서 네트워크에 있어서 근원지와 기지국 사이의 경로를 확보해주면서 일부 노드들을 휴면화함으로써 데이터 전송 과정에서의 더미 메시지 발생을 감축하는 방법을 제시하였다. 제안된 방법을 따르면 기지국이나 근원지들에 대해 기대하는 위치 기밀의 성취 여부를 미리 알 수 있고 해당 위치 기밀을 유지하는데 합당한 휴면 노드들의 수를 결정할 수 있어 과중한 더미 메시지의 발생을방지할 수 있다. 제안 방법에서 $p_{threshold}$ = 0인 경우가 PCM[3]에 해당되므로 제안 방법이 보다 일반적이라 할 수 있다. 또한, 기지국과 근원지들 간에 다수의 경로들을 제공하므로 인해(그림 1 c)와 d) 참조) 데이터 전송 시의 장애나 오류 극복에 유리하다 할 수 있다.

후속 연구로, 근원지들의 수가 미리 알려져 있지 않은 상황에서 비동기적인 형태로 데이터 세션을 진행하는 경우를 위한 효과적인 휴면 노드 설정 방법을 연구 중에 있다.

References

[1] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, “Enhancing source-location privacy in sensor networking routing,” *In Proc. of Int. Conf. on Distributed Computing System 2005*, Columbus, Ohio, USA, June 6-9, 2005, pp.1-10.

[2] Y. Jian, S. Chen, Z. Zhang, and L. Zhang, “Protecting receiver-location privacy in wireless sensor networks,” In *Proc. of IEEE (INFOCOM) Int. Conf. on Computer Communications 2007*, Anchorage, Alaska, USA, May 6-12, 2007, pp. 1955-1963.

[3] K. Mehta, D. Liu, and M. Wright, “Protecting location privacy in sensor networks against a global eavesdropper,” *IEEE Trans. Mobile Computing*, vol. 11, no. 2, Feb. 2012, pp. 320-336.

[4] Y. Tscha, “Concealing communication paths in wireless sensor networks,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 13, no. 1, 2014, pp. 115-130.

[5] Yi Ouyang, Zhengyi Le, Donggang Liu, James Ford, and Fillia Makedon, “Source location privacy against laptop-class attacks in sensor networks,” In *Proc. of ACM 4th Int. Conf. on Security and Privacy in Communication Networks*, Istanbul, Turkey, September 22-25, 2008, pp. 5-14.

[6] M. Yon and Y. Him, “A study on hierarchical communication method for energy efficiency in sensor network environment,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 9, no. 8, 2014, pp. 889-897.

[7] K. Kim, B. Kim, S. Bae, and D. Kim, “An improved message broadcast scheme over wireless sensor networks,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 5, no. 6, 2010, pp. 588-594.

[8] C. See, “A Study on MD5 Security Routing based on MANET,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 7, no. 4, 2012, pp. 797-804.

저자 소개

차영환(Yeong-Hwan Tscha)

‘83년 인하대 전자계산학과 학사
‘85년 KAIST 전산학과 석사
‘93년 인하대 대학원 박사

‘85년 ~ ’90년 ETRI 선임연구원
‘86년 미국 NIST 객원 연구원
‘04년, ’11년 터키 Boğaziçi 대학교 객원 교수
‘94년 ~ 현재 상지대학교 컴퓨터정보공학부 교수
※ 관심분야 : 네트워킹, 통신 프로토콜, 통신 보안