Regular paper http://dx.doi.org/10.13067/JKIECS.2014.9.12.1353

무선 센서 네트워크에서의 통신 경로 은닉

차영환*

Concealing Communication Paths in Wireless Sensor Networks

Yeong-Hwan Tscha*

요 약

무선 센서 네트워크에 대한 전역 도청에 대응하여 통신 경로 상의 노드들을 은닉하기 위해서는 네트워크 전반에 걸쳐 수많은 속임수용 더미 패킷들이 발행되어야한다. 이 논문에서는 모바일 싱크(기지국)와 근원지들을 포함하는 일정 크기의 원 형태 내에 존재하는 노드들로 국한되는 플러딩 기반의 데이터 전송 프로토콜을 제안하여 노드들의 위치 기밀을 유지하고 생성되는 더미 패킷들의 수를 감축하고자 한다. 플러딩 크기는 보안 수준과 통신 비용을 고려하여 결정할 수 있다. 제안 프로토콜을 설계하고 주요 특성을 검증한다.

ABSTRACT

Tremendous amount of dummy packets are generally generated for faking over a wireless sensor network so as to keep the location privacy of nodes on the communication paths against the global eavesdropping. In this paper, a scoped-flooding protocol is designed for transferring data between each source and mobile sink(aka, basestation) where, the only nodes within the scope are allowed to issue dummy packets at every idle time so that the location privacy of the nodes on the paths is kept and the amount of dummy packets is reduced to the extend of the flooding scope. The size of the flooding diameter can be taken into consideration of the privacy level and the communication cost. We design a detailed specification of the protocol and verify several properties.

키워드

Global Eavesdropping, Location privacy of Communication Nodes, Protocol Design and Verification
광역도청, 통신 노드의 위치기밀, 프로토콜 설계 및 검증

Ⅰ. 서 론

무선 네트워크에서는 데이터의 전송 시 대기 중으로의 전파 신호 발생이 불가피하다. 발생되는 신호들을 포착하면 데이터가 발생한 노드(근원지, source)로부터 데이터를 중계 전송하는 중간 노드들은 물론 데이터의 최종 노드(도착지, destination)들의 위치를 알 수 있다[1-2]. 통신 과정에 직접적 방해나 관여 없이 무선 네트워크 전역에 걸친 이러한 수동적 광역도청(passive global eavesdropping)에 대응하는 저비용의 데이터 전송 프로토콜을 제안하는 것이 이 연구의 목적이다.

광역도청에 의한 통신 경로상의 노드들의 위치 파악 공격에 대응하는 데이터 전송 기법으로는 최근에 발표된 PCM(Periodic Collection Method)이 거의 유일하다[3]. PCM은 네트워크 내의 모든 노드들이 매

* 교신저자(corresponding author) : 상지대학교 컴퓨터정보공학부(yhtscha@sangji.ac.kr)
접수일자 : 2014. 09. 30 심사(수정)일자 : 2014. 11. 21 게재확정일자 : 2014. 12. 15

시각마다 데이터 패킷이나 또는 내용이 의미없는 신호발생용 더미(dummy) 패킷 둘 중의 하나를 반드시 발행하여야 하므로 보안성은 매우 높으나 과중한 통신 비용을 유발하여 규모가 큰 네트워크에서는 실용적이 않다.

무선 센서 네트워크는 응용 분야에 따라 데이터의 발생과 수집의 범위가 네트워크 전반에 걸쳐 일어나지 않고 시각을 달리하면서 국소적인 범위로 국한되는 경우가 있다. 예를 들어 희귀 동물의 생태를 모니터링 하는 응용에서는 동물들의 거주지와 이동경로 등이 특정지역으로 한정되어 있고, 계절과 주야에 따라 일정한 패턴을 갖는다. 군사 작전에 이용되는 네트워크의 경우에도 활동 범위가 일정한 물리적 공간에 제한되고 데이터의 발생도 일정 공간 범위내의 노드들이 주를 이룬다. 이러한 응용에서는 그림 1과 같이 데이터 발생에 대한 패턴 정보를 사전에 알고 있는 이동성이 보장되는 모바일 싱크(mobile sink)를 투입하여 운용한다면 통신 경로를 보호하기 위해 네트워크 전반에 걸쳐 속임수용 패킷 즉, 더미 패킷들을 발생할 필요 없이 보안 수준에 따라 현재 활동 중인 노드들을 포함하여 일정 지역 내의 노드들에 한해 통신을 제한함으로써 위치 보안 유지와 통신 비용 감축을 도모할 수 있을 것이다.

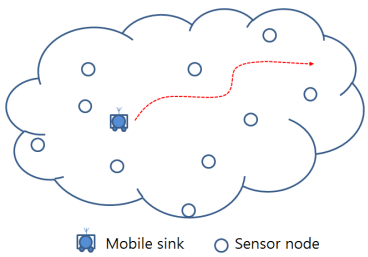

그림 1. 모바일 싱크를 수용하는 센서 네트워크
Fig. 1 A sensor network deploying a mobile sink

이 논문에서는 이와 같이 모바일 싱크를 수용하는 센서 네트워크에서 데이터의 발생과 이의 수집에 관여하는 근원지들이 일정 지역에 편재되는 즉, 클러스터링 되는 경우를 대상으로 근원지들과 모바일 싱크의 위치 그리고 이들 사이의 데이터가 전송되는 경로상의 노드들의 위치를 광역 도청자로부터 보호하기 위한 데이터 전송 기법을 제안한다. 연구와 관련된 가정이나 용어 및 수동적 광역도청 공격자 등에 관해서는 관련 연구들[4],[6]을 따른다. 아울러 전송 정보는 기밀성을 위해 참고문헌[5]과 같은 적절한 암호화체계를 사용한다고 가정한다.

다음 장에서는 제안 프로토콜의 접근방식과 사용 패킷들과 동작 절차를 소개한다. 제 Ⅲ 장에서는 제안 프로토콜이 제공하는 보안성 정도와 발생되는 패킷들의 수 즉, 통신비용을 분석한다. 연구의 결론과 향후 연구에 대해서는 제 Ⅳ 장에서 기술한다.

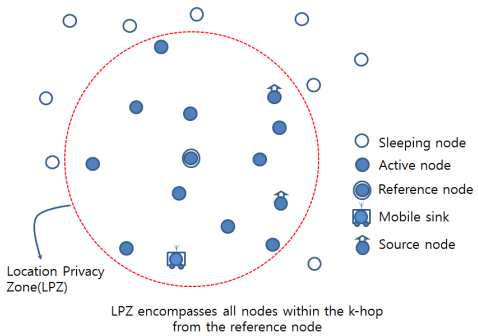

그림 2. 기준 노드에 의한 위치보호구역(LPZ) 설정
Fig. 2 Location-privacy zone(LPZ) setup by the reference node

Ⅱ. 제안 프로토콜

2.1 접근방법

모바일 싱크는 사전에 어느 지역의 어느 부근에 데이터 전송이 예정된 근원지들이 존재하는지 알고 있는 상황에서, 기준 노드(reference node)라고 불리는 노드에 의해 위치보호구역(LPZ: Location-Privacy Zone)의 설정을 알리는 패킷이 발행될 때까지 대기한다. 기준 노드는 선행 연구[6]에서 근원지 프락시나 도착지 프락시를 선정하는 방법 등을 이용하여 동적으로 선정될 수 있고, 미리 그 역할이 지정되어 있을 수도 있다. 이 연구에서는 후자의 경우를 가정한다. 기준 노드는 그 위치가 알려져도 무관한 노드로 LPZ의 중심에 위치한다.

모든 노드들이 초기 ACTIVE(활동) 모드에 있는 상황에서 그림 2에서 나타내듯이 기준 노드는 자신으로부터 k-홉(hop)에 이르는 노드들에 대해 LPZ가 설정됨을 알리게 된다. 그러면 LPZ 내의 노드는 매 슬

롯마다 패킷을 보내어야 하고, 이는 LPZ가 해제될 때까지 지속된다. 그러므로 이 구역 내의 모든 노드는 데이터 전송이 종료될 때까지 매 타임 슬롯마다 패킷들을 전송함으로써 외부의 신호발생 관찰자 즉, 도청자로 하여금 어느 것이 근원지이고 기지국이고 데이터 경로 상의 노드인지 명확히 선별하여 낼 수 없도록 한다.

LPZ의 크기를 나타내는 k는 일련의 근원지 들을 모두 포함할 만큼 충분히 크고 모바일 싱크도 포함할 수 있어야 한다. LPZ 밖의 노드들은 휴면 모드인 SLEEP로 전환된다.

2.2 프로토콜 패킷 및 절차

제안 프로토콜에서 사용되는 패킷들의 종류와 이들이 누구에 의해 생성되고 어떤 노드를 위한 것인지 표 1에 나타내었다. 또한 각 패킷의 주요 필드들과 그 의미는 표 2와 같다. 전송 패킷의 순서나 흐름 제어 또는 오류 제어 등과 같은 것을 위한 필드는 논의의 편의성을 위해 생략하였다.

패킷들은 Packet_Type 필드 값(예를 들면 1, 2, 3, 4)으로 구분된다. 전파 신호만을 발생하는 DUMMY (이 논문에서는 표 1에 의한 dummy 패킷은 DUMMY로 표기하고 그렇지 않은 일반적인 경우는 dummy로 구분한다)를 제외하고 해당 패킷을 처음으로 생성한 노드의 id는 Origin에 기억된다. 모든 패킷들은 동일한 길이로 패딩(padding)되어 전송되기 때문에 모두 동일한 시간동안 전송 신호가 지속되어 도청자는 발생 신호만으로 패킷을 구분할 수 없다.

LPZ을 설정하기 위해 기준 노드에 의해 LPZA(LPZ Advertizement)가 플러딩 되는데, 초기에 Hop_Count=0으로 설정되어 중간 노드를 거칠 때마다 1씩 증가하여 Hop_Limit에 다다를 때까지 전파된다. Hop_Limit은 위치 보안 수준과 통신 비용을 고려한 일정한 값 k(>0)로 정해져 전달된다.

패킷 DATA는 LPZ내의 근원지들의 집합 V^{LPZ}_{source}에 대하여, $t \in V^{LPZ}_{source}$인 노드 t의해 발생된다. 전송 데이터의 크기를 알려주는 Data_Length 필드가 존재하고, 전송 Data가 끝이면 More 필드는 0으로, 아니면 1로 설정된다. 주의할 점은 DATA 내에는 도착지를 나타내는 필드가 없다. 모바일 싱크만이 자신의 이웃 노드로부터 수신되는 DATA를 수신하도록 하는 것으로 충분하다.

DUMMY는 전송할 패킷이 없는 노드가 즉, 빈(empty) 타임 슬롯에서 발행하는 패킷으로 수신자나 내용 필드도 존재하지 않고, 수신에 따른 처리도 불필요하다. 도청자에게 모든 노드가 매 타임 슬롯마다 패킷을 전송한다는 것을 의도적으로 보여주기 위한 것이다. 한편, Sequence_Number 필드는 DUMMY를 제외한 모든 패킷에 있는데 수신자가 중복수신 여부를 가릴 때 사용한다.

표 1. 사용 패킷의 종류와 용도
Table 1. Packets and their usages

Comments / Type	Purpose	Originator	Recipient
LPZA(LPZ Advertizement)	LPZ setup	reference node	all nodes in LPZ
DATA(Data)	data transfer	source node	mobile sink
DUMMY(Dummy)	signal propagation	all nodes in LPZ	-
LPZW(LPZ Withdrawal)	LPZ release	reference node	all nodes in LPZ

표 2. 사용 패킷의 필드와 의미
Table 2. Packet fields and their semantics

Field / Purpose / Packet	Type	Origin	Sequence_ Number	Hop_ Limit	Data_ Length
	packet identification	originator identification	packet number	flooding scope	data length
LPZA	√	√	√	√	
DATA	√	√	√		√
DUMMY	√				
LPZW	√	√	√	√	

Field / Purpose / Packet	Data	Hop_Count	More	Padding
	user data	distance from reference node	succeeding data indication	length alignment (if necessary)
LPZA		√		√
DATA	√		√	√
DUMMY				√
LPZW		√		√

LPZW(LPZ Withdrawal)는 데이터 전송 단계가 종료됨을 알려준다. 이는 기준 노드에 의해서 생성되며 마지막 근원지로부터의 DATA 패킷내의 More 필드 값이 0일 때 발행된다.

프로토콜의 동작 절차를 나타내면 그림 3과 같다. 절차 내의 사용된 기호 V^{LPZ}_{node}는 LPZ 내에 존재하는 노드들의 집합을, N(v)는 노드 v의 이웃한 노드들의 집합을, V_{node}는 네트워크 내의 모든 노드들의 집합을 나타낸다. 모든 노드는 초기 ACTIVE 모드에서 시작

하고 LPZ외의 노드는 휴면 모드인 SLEEP로 전환된다. 노드 A가 노드 B에서 패킷 Π를 전송하는 과정은 "A→B: Π"의 형식으로 표기하고, 이해가 용이하도록 절차적 고급언어 형태로 기술하였다. 부연 실명이 요하는 몇몇 과정은 다음과 같다.

줄 번호 3은 LPZ 내의 모든 노드가 ACTIVE 모드에서 빈 타임 슬롯 즉, 전송할 LPZA, DATA나 LPZW가 없는 경우 DUMMY를 발행함을 기술한 것이다. 다만, 네트워크의 기지국인 모바일 싱크 M_SINK는 이 과정을 수행하지 않도록 하여 패킷 전송 시 발생 신호를 원천적으로 방지한다.

```
<LPZ Setup>
1. REF → N(REF) : LPZA where Hop_Limit=k(>0), Hop_Count=0;
2. for any v(≠M_SINK) that received non-duplicated LPZA,
   2.1 if (Hop_Count>Hop_Limit) goto SLEEP mode and exit;
   2.2 else {
         Hop_Count = Hop_Count + 1;
         v → N(v) : LPZA; // propagate LPZA
       }
3. for any u ∈ {V^LPZ_node - M_SINK}, // u ∈ {V^LPZ_node - M_SINK},
     if (the time slot is idle) u → N(u): DUMMY;

<Data Transfer>
4. For any s∈V^LPZ_source, if (there exists data to send)
     s → N(s): DATA // More=0 for the last otherwise, More=1;
5. For any v∈V^LPZ_node that received non-redundant DATA
   5.1 if (v is M_SINK) accept DATA; // the destination
   5.2 else v → N(v) : DATA; // propagate DATA
6. if this is the last DATA from the last source,
     REF → N(REF) : LPZW;

<LPZ Release>
7. for any v ∈ {V^LPZ_node - M_SINK} that received non-redundant LPZW,
   7.1 if (Hop_Count < Hop_Limit) {
         Hop_Count=Hop_Count+1;
         v → N(v) : LPZW; // propagate LPZW
         goto SLEEP mode and exit;
       }
   7.2 else
         goto SLEEP mode and exit;
```

그림 3. 범위제한 플러딩에 기반을 둔 데이터 전송
Fig. 3 Scoped flooding based data transfer

줄 번호 4는 근원지가 DATA를 생성하여 전송하는 과정이다. 줄번호 5에는 모바일 싱크만 데이터 패킷을 수신하고 그렇지 않은 노드들은 이를 플러딩한다. 그리고 마지막 DATA가 수신되면 기준 노드는 위치보호구역을 해제하는 LPZW를 발행하고, 이를 수신하는 노드는 바로 SLEEP 모드로 전환된다(줄 번호 7). 주의할 점은 DATA는 LPZA 내의 모든 노드들로 플러딩 된다는 것이다. 즉, 근원지와 모바일 싱크 간에 특정 경로 하나가 선정되는 것이 아니다. 이로 인해 발생 신호만을 통해 데이터 통신 경로 상의 특정 노드를 찾아내어 파괴 등과 같은 적극적 공격을 시도하는 경우에 노드 선정의 어려움을 야기하고 투입되는 시간과 노력을 소모하도록 유도한다.

III. 분석 및 평가

이 장에서는 제안 프오토콜의 보안성과 통신 비용에 대해 분석하고 평가한다. 평가 항목과 방법 및 비교 등은 관련 연구[4],[6]를 따른다.

3.1 일반 성질

그림 3의 프로토콜은 다음을 만족한다.

성질 1. LPZA를 수신하고부터 LPZW를 수신하기까지 모든 $v \in \{V^{LPZ}_{node} - M_SINK\}$는 빈 타임 슬롯마다 DUMMY를 발행한다(단, M_SINK는 모바일 싱크임).

성질 2. M_SINK는 어떠한 패킷도 전송하지 않는다. 즉, M_SINK로부터는 어떠한 전송 신호도 발생되지 않는다.

성질 3. LPZ 내의 M_SINK와 근원지 사이에 경로가 존재하는 한, DATA 패킷은 전달된다.

성질 1은 그림 3의 줄 번호 3의 과정이, 줄번호 7에 해당하는 경우가 발생할 동안 빈 타임 슬롯마다 수행되므로 성립한다. 모바일 싱크 M_SINK는 줄번호 5와 같이 패킷 DATA를 수신할 뿐 DUMMY 조차 발행하지 않고, 다른 어떠한 패킷도 중계하지도 않으므로 성질 2가 성립한다. 성질 3은 플러딩을 사용하면 근원지와 도착지가 네트워크에 연결되어 있는 한 패킷은 전달될 수 있다는 점에서 성립한다.

3.2 위치보안성

성질 4. 그림 3의 제안 프로토콜이 제공하는 모바일 싱크 M_SINK의 위치보안성은 무한대이다.

증명: 성질 2에 의해 M_SINK는 어떠한 패킷 전송도 하지 않으므로 전파신호를 발생하]시키지 않는다. 따라서 발생 전파의 탐지에 의해서는 그 존재를 확인할 수 없으므로 이 성질은 참이다.

네트워크 내에 존재하는 근원지들의 수 $|V^{LPZ}_{source}| > 0$인 경우에 있어서, 하나의 근원지가 갖는 위치보안성은 다음과 같이 PCM방식[4]에 대한 비율로 정의한다. 즉, PCM 방식에서 하나의 근원지가 선택될 확률을 p_1, 제안된 방식에서 하나의 근원지가 선택될 확률을 p_2라 하면, 제안된 방식에서의 근원지의 위치보안성은 $\log_2(p_2/p_1)$로 정의한다(단, $p_2 \geq p_1$).

성질 5. 위치보호구역 내의 근원지의 위치보안성은 PCM 방식에 비해 $\log_2(1/\rho^2)$배 낮다. 단, $\rho = k/R$이고, k는 LPZ의 반지름, R은 네트워크의 반지름으로 $k \leq R$이다.

증명: 위치보호구역 내의 임의의 근원지 v가 선택될 확률은 $|V^{LPZ}_{source}|/|V^{LPZ}_{node}|$이다. 그런데 S_{LPZ}은 하나의 위치보호구역 면적을, $S_{network}$는 네트워크 전체의 면적을 나타내고, 1-홉을 단위길이 1에 대응시키면 $S_{privacy\_zone} = \pi\delta^2$, $S_{network} = \pi R^2$이므로 $|V^{LPZ}_{node}| = (S_{privacy_zone}/S_{network})N = (\delta/R)^2N = (\rho R/R)^2N = \rho^2N$이다. 여기서, $\rho=\delta/R$로 표현되는 네트워크 반지름 R에 대한 LPZ 반지름의 비율로 $0<\rho<1$이다. 따라서 네트워크 내에 ω개의 근원지가 있다면 PCM에서 하나의 근원지가 발생할 확률은 ω/N 이고 제안 프로토콜을 이용하면 $\omega/(\rho^2N)$이므로 이들의 비는 $(\omega/(\rho^2N))/(\omega/N) = 1/\rho^2$이다. 고로 PCM 대비 제안 프로토콜의 위치보안성 수준은 $\log_2(1/\rho^2)$이다.

3.3 통신 비용

성질 6. PCM의 통신 비용 대비 제안 프로토콜의 통신 비용은 ρ^3이다.

증명: PCM은 N개의 모든 노드가 n_{data}개의 데이터를 전송하는 타임 슬롯 동안 DUMMY나 DATA 둘 중, 어느 한 패킷을 반드시 전송해야한다. 그런데 네트워크의 지름은 2R이므로 임의의 한 패킷이 모든 노드에게 전달되려면 최대 2R개의 타임 슬롯이 소요된다. 고로 n_{data}개의 데이터를 전송하기 위해 $2R \cdot n_{data} \cdot N$개의 패킷들이 발생한다. 제안 프로토콜은 LPZ 설정을 위해 각기 $|V^{LPZ}_{node}| \cdot k$개의 LPZA 또는 DUMMY, 해제를 위해서는 $|V^{LPZ}_{node}| \cdot k$개의 LPZW 또는 DUMMY가 발생한다. 그리고 하나의 DATA를 전송하기 위해서는 위치보호구역 지름 최대 2k만큼의 지연이 요구되므로 n_{data}개의 데이터를 전송할 때 $n_{data} \cdot 2k \cdot |V^{LPZ}_{node}|$개 즉, $2k \cdot |V^{LPZ}_{node}|(1+n_{data})$개가 발생한다. 여기서 $n_{data} \gg 1$임을 고려하면 제안프로토콜에서 발생하는 패킷들의 총 수는 $2k \cdot |V^{LPZ}_{node}| \cdot n_{data}$이다. 그런데 $|V^{LPZ}_{node}| = (\pi k^2/\pi R^2) \cdot N = \rho^2N$이므로(단, $\rho=k/R$), PCM에 의한 발생 패킷 수에 대한 제안 프로토콜에서 발생하는 패킷들의 비는 $(n_{data} \cdot 2k \cdot \rho^2N)/(2R \cdot n_{data} \cdot N) = (k\rho^2)/R = \rho^3$이다.

표 3. PCM 방식 대비 성능
Table 3. Comparison with PCM method

Evaluation Criteria \ Parameter		Ratio ρ of LPZ radius k to network radius R(aka. ρ=k/R)					
		1/2 (k=R/2)	1/3 (k=R/3)	1/4 (k=R/4)	1/5 (k=R/5)	1/6 (k=R/6)	1/7 (k=R/7)
Privacy	$\log_2(1/\rho^2)$	2	3.17	4	4.6439	5.17	5.6147
	$(1/\rho^2)\cdot100(\%)$	25%	11.1111%	6.25%	4%	2.7778%	2.0408%
Cost	ρ^3	0.125	0.0370	0.0156	0.008	0.00046	0.0029
	$\rho^3\cdot100(\%)$	12.5%	3.7037%	1.5625%	0.8%	0.463%	0.2915%

표 3에 성질 5와 성질 6에 따른 기존의 프로토콜 PCM과 제안된 프로토콜의 위치보안성과 통신 비용 비교에 대한 수치적 값을 보였다. LPZ의 반경 k가 네트워크 반경 R의 단지 1/2 또는 1/3 정도만 되어 전체 노드의 25%나 11%만 활동하는 상황에서 통신 비용은 각기 12.5%와 3.7% 정도의 매우 낮은 비용으로 통신 경로의 은닉을 도모할 수 있다. 이러한 파라미터 k는 전체 노드 수 N이 큰 대규모 네트워크에서 특히 바람직하다. 왜냐하면 LPZ의 지름이 작아도 그 내부에 많은 수의 노드들이 존재하여 무작위로 어느 한 노드를 선정 시 그 것이 근원지나 모바일 싱크일 확률이 낮아지기 때문이다. 따라서 노드의 밀도를 고려하여 k를 정하면 된다. 아울러 제안 프로토콜은 모바일 싱크는 단지 패킷 수신 기능만을 수행하도록 함으로써 어떠한 패킷의 발행에도 관여하지 않아 수동적 도청자에게 그 존재를 노출하지 않는다.

Ⅳ. 결 론

이 논문에서 제안한 원 형태의 위치보호구역(LPZ) 설정에 의한 통신 경로 은닉 프로토콜은 모바일 싱크의 위치 기밀성을 무한대로 유지한다. 그리고 기존의 방식 PCM에 비해 LPZ의 반경이 네트워크 반경의 1/2과 1/3 정도만 되어도 12.5%와 3.7% 정도의 통신

비용으로도 통신 경로를 은닉할 수 있는 장점을 제공한다.

이러한 접근방법에 있어서 공격자 관점에서 수동적 공격을 탈피하여 최소한의 노드들을 파괴하며 통신 경로를 두절시키기 위한 최적 공격 알고리즘에 대해 연구 중에 있다. 확장 연구로는 센서 네트워크의 에너지 절약 방안[7]이나 브로드캐스트 비용의 축소 방안[8] 등과 연계한 통신 경로 은닉을 고려하고 있다.

감사의 글

본 논문은 2012년도 상지대학교 교내 연구비 지원에 의한 것임을 밝힙니다.

References

[1] P. Kamat, Y. Zhang, W. Trappe, and C. Ozturk, "Enhancing source-location privacy in sensor networking routing," In *Proc. of The 25th Int. Conf. on Distributed Computing Systems,* Columbus, OH, Apr. 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 26th Annual IEEE Conf. on Computer Communications IEEE INFOCOM 2007,* Anchorage, AK, May 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] E. Ngai and I. Rodhe, "On providing location privacy for mobile sinks in wireless sensor networks," *Wireless Networks,* vol. 19, no. 1, 2013, pp. 115-130.

[5] C.-S. Lee, "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.

[6] Y. Tscha, "Concealing communication source and destination in wireless sensor networks(Part I): Protocol Design," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 8, no. 2, 2013, pp. 219-226.

[7] M.-Y. Son and Y.-H. Kim, "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.

[8] 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.

저자 소개

차영환(Yeong-Hwan Tscha)

1983년 인하대 전자계산학과 학사
1985년 KAIST 전산학과 석사
1993년 인하대 대학원 박사
1985년～1990년 ETRI 선임연구원
1986년 NIST(NBS) 방문과학자
2004년, 2011년 터키 Boğaziçi 대학교 방문교수
1994년～현재 상지대학교 컴퓨터정보공학부 교수
※ 관심분야 : 네트워킹, 통신 프로토콜, 통신 보안