

# USNs 에서 노드 위치정보 보호기법

임화정\*, 이헌길\*

\*강원대학교 컴퓨터공학과

e-mail : {hjlim, hglee}@kangwon.ac.kr

## A Mutual Expose Prevention Scheme of Node Location in USNs

Hwa-Jung Lim\*, Heon-Guil Lee\*

\* Dept. of Computer Engineering, Kangwon National University

### 요 약

유비쿼터스 센서 네트워크(Ubiquitous Sensor Networks: USNs)환경은 주변 공간의 상황을 인식할 수 있고, 인식한 상황을 바탕으로 적절한 시기에 필요한 정보를 올바른 사용자나 사용자 장치에게 제공해주는 지능적인 환경을 제공한다. 이러한 환경에서 사용자의 위치정보는 매우 중요한 요소로 부각되고 있으며, 위치정보 측정을 위해 GPS(Global Positioning System)같은 위치 측정 시스템들이 개발되고 있다. 하지만, 사용자의 위치정보를 측정하는 것은 다른 한편으로 사용자의 프라이버시를 침해 할 수도 있는 심각한 보안상의 문제점을 야기시킬 수 있다. 본 논문에서는 CBS(Covert Base Station)을 이용하여 베이스스테이션만이 노드의 위치를 파악할 수 있도록 하여, 노드 및 노드 주변의 다른 어떤 노드에게도 위치가 노출되지 않도록 하기 위한 기법을 제시한다.

### 1. 서론

최근 들어서 유비쿼터스 센서 네트워크(Ubiquitous Sensor Networks: USNs)에 관한 연구가 활발히 진행되고 있다[1].

유비쿼터스 센서 네트워크환경은 주변 공간의 상황을 인식할 수 있고, 인식한 상황을 바탕으로 적절한 시기에 필요한 정보를 올바른 사용자나 사용자 장치에 제공해주는 지능적인 환경을 제공한다[2].

이러한 환경은 주변 사물과 환경에 통신장치가 탑재된 초소형의 지능화된 임베디드(Embedded) 컴퓨터가 내재되어 상호 네트워크를 구성함으로써 가능해진다. 즉, 사용자가 멀리 떨어져 있더라도, 원하는 장소나 시간에 따른 사물 및 주변 환경의 변화를 인식하거나 추적하여 상황 인식적이고 특화된 정보 서비스를 제공할 수 있음을 의미하는 것이다[3]. 따라서 이러한 환경에서 사용자 혹은 사용자 장치의 물리적인 위치와 조건 및 그 변화하는 정도 역시 인식할 수 있어야 한다. 따라서 사용자의 위치정보는 매우 중요한 요소로 부각되고 있다[4,5].

사용자의 위치정보를 획득할 수 있는 대표적인 시스템으로는 GPS(Global Positioning System)와 이동통신

망을 이용한 위치측정 시스템을 들 수 있다[6,7].

그러나 장치의 가격이 매우 중요한 요소인 유비쿼터스 컴퓨팅 환경에서 비교적 고가인 GPS 장비는 적합하지 않다. 이상과 같은 관점에서 GPS 를 대체할 수 있는 새로운 위치 측정 시스템에 대한 필요성이 대두고 있으며, 이에 따라 저가의 위치 시스템에 관한 연구가 활발하게 진행되고 있다[8].

문제는 이러한 저가의 위치 측정 시스템들은 가격이 저렴하다는 장점은 있으나, 사용자의 정보가 외부에 유출될 가능성이 GPS 보다 높다는 단점이 있다.

사용자에게 편의를 제공하고자 획득되는 위치정보는 사용자의 프라이버시에 속하며 사용자가 원하는 목적 이외에 용도로 사용되면 안될 것이다. 따라서 센서 네트워크를 이용하여 위치를 측정하는 시스템에서 위치정보의 유출을 막기 위해서는 위치를 측정하는 센서 노드들에 대한 보안뿐만 아니라 위치를 측정하는 메커니즘에도 보안을 적용해야 한다[9,10,11,12].

본 논문에서는 삼각측량법을 이용하는 위치측정 시스템에 CBS(Covert Base Station)개념을 도입하여 위치 측정을 위해 노드들이 발생시키는 전파나 사운드에 접근이 가능하더라도 인증된 베이스스테이션(BS)만이 사용자의 정확한 위치를 파악할 수 있도록 하고 사용

자나 제 3 자가 위치정보를 변경할 경우 이를 검증하고 방지하는 방안을 제안하고자 한다.

본 연구 2 장의 관련연구에서는 위치 측정 기술 및 위치 인식 시스템에 대해 살펴보고, 3 장에서 제안 시스템 및 공격 모델에 대해서 묘사하기로 한다. 4 장에서는 CBS 를 이용한 인프라스트럭처 기반 노드 기반에서의 노드 위치보호 메커니즘에 대해 설명한 후 결론에서 논문의 적용 분야 및 향후 연구방향에 대하여 설명하도록 한다.

## 2. 위치 측정 기술 및 시스템

위치측정 기술은 측정방식에 따라 삼각측량, 장면 분석, 근접방식 등으로 분류하거나, GPS 와 같은 위치를 측정할 수 있는 하드웨어적 인프라가 있는지 여부에 의해 분류할 수 있다.

삼각측량법은 기준점까지의 거리를 측정하는 거리 측정 방식과 기준점으로부터 떨어져있는 각도를 이용하는 각도 측정 방식으로 나누어 볼 수 있다[8,13].

이러한 위치인식 기술을 각 시스템 별로 분류한 것이 <표 1>과 같이 매크로 위치인식 시스템과 마이크로 위치인식 시스템 그리고, 센서 네트워크와 같이 무선이동 노드들의 위치를 인식하는 Ad-Hoc 위치인식 시스템으로 나눌 수 있다[14].

<표 1> 위치인식 시스템 분류

매크로 위치인식 시스템	마이크로 위치인식 시스템	Ad-hoc 위치인식 시스템
◎ GPS	◎ Infrared	◎ Centroid
◎ Infra of Mobile Communication	◎ Ultrasonic	◎ APIT
◎ Hybrid	◎ RF Signal	◎ DV-Hop, DV-Distance
	◎ UWB	
	◎ Scene Analysis	

측정된 거리로부터 삼각측량법을 이용하는 위치 계산하는 시스템의 대표적인 예인 GPS 는 AOA(Angle of Arrival), TOA(Time Of Arrival), TDOA(Time Difference of Arrival) 등의 방식을 사용하여 위치를 계산한다[15].

반면에 인프라가 없는 유비쿼터스 센서 네트워크 환경에서는 레퍼런스 노드와 RF 의 연결성 기반으로 위치인식을 수행하는 Centroid 기법과 이동 노드에서 무선으로 연결 가능한 레퍼런스 노드들로 삼각형을 형성하고, 이동 노드가 그 삼각형 내부에 있는지 여부를 계산하여 이동 노드가 내부에 있는 삼각형들이 겹치는 영역의 중심점을 이동 노드의 위치로 인식하는 APIT(Approximation Point-In-Triangulation)기법 그리고 DV(Disrance Vector)라우팅 알고리즘의 hop-by-hop 라우팅 정보전송 방법과 GPS 의 삼각측정원리를 이용한 위치계산 방법을 조합하여 사용하는 DV-Hop, DV-Distance 기법 등이 있다[16,17,18].

## 3. 제안 모델

### 3.1 시스템 모델

제안된 시스템은 노드와 상호 신뢰 관계인 베이스 스테이션(BS)과 여러 개의 CBS(Covert Base Station)들로 구성된다.

제안된 시스템에서의 노드는 CBS 의 위치를 모르며 자기자신의 정확한 위치도 알지 못한다.

CBS 는 노드의 위치를 알 수 없지만, 자신의 위치 정보를 알고 있고, 노드로부터 전송되는 신호로 거리 계산을 할 수 있다. 또한 CBS 는 베이스스테이션과 암호화된 키를 공유하고 있고 이를 이용해 정보를 주고받는다. 따라서 베이스스테이션은 노드로부터의 정보와 CBS 로부터 수집된 CBS 와 노드와의 거리정보 및 CBS 의 위치정보를 토대로 노드의 위치를 파악할 수 있다.

반면에 노드나 CBS 는 거리정보만으로 노드의 위치를 계산할 수 없으므로 노드의 위치는 BS 이외에는 노출되지 않는다.

### 3.2 공격모델

우리는 내부(Internal)와 외부(External) 두 가지의 공격모델을 제시한다[19].

첫 번째, 내부로부터의 공격에는 인증된 노드(CBS, 노드)들이 오작동 또는 감염되었을 경우를 말한다.

두 번째, 외부로부터의 공격에는 인증되지 않은 노드(주변노드, 악의적인 노드)들이 노드의 RF 비컨 신호를 엿들음으로써 노드의 위치를 계산할 수 가 있다.

## 4. CBS 를 이용한 노드 위치보호 기법

센서네트워크를 이용하는 위치인식 시스템은 크게 노드 센트로이드(Node Centroid)방식과 인프라스트럭처 센트로이드(Infrastructure Centroid)방식으로 분류할 수 있다[20].

각각의 경우에 노드 위치 보호기법은 다음과 같다.

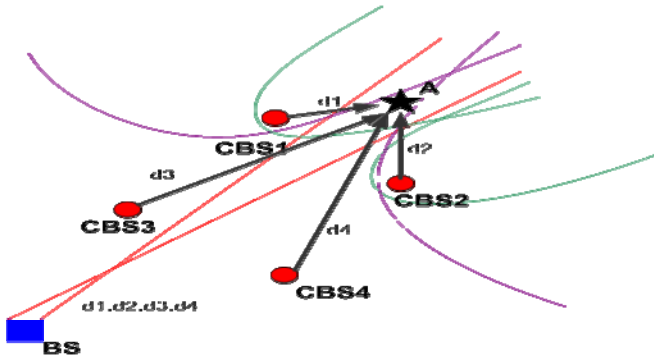
### 4.1. 노드 센트릭 기반

노드 센트로이드(Node Centroid)방식에서는 노드의 위치를 찾기 위해 인프라스트럭처를 구성하는 노드들이 사운드나 전파를 발생시키며 위치 측정 대상 노드가 이 정보들을 수집하여 거리 정보를 계산하고 이를 이용하여 자신의 위치를 계산하는 방식이다.

노드 센트릭 방식을 이용할 경우 위치를 계산하는 사용자가 위치정보를 변경할 수 있으며 위치정보가 제 3 자에게 유출되거나 변경될 수도 있다.

이를 방지하기 위해 첫째, 사용자의 위치는 BS 만 이 계산 가능하도록 한다. 둘째, 위치 계산을 위해 필요한 인프라스트럭처 노드들의 정확한 위치 정보가 사용자를 포함한 외부에 유출되는 것을 방지하기 위해 CBS 개념을 도입하였다.

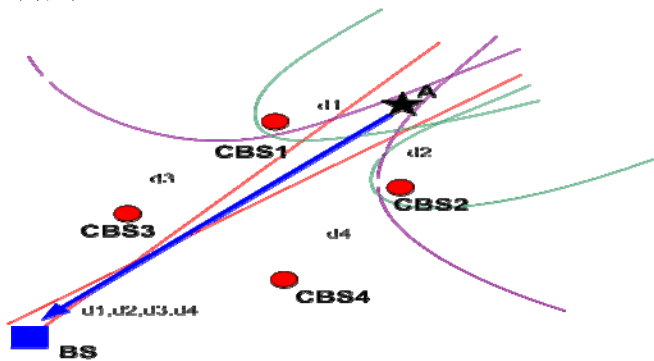
제안된 기법은 그림 1~3 에서와 같은 방식으로 동작한다.



(그림 1) Node Centroid Step1

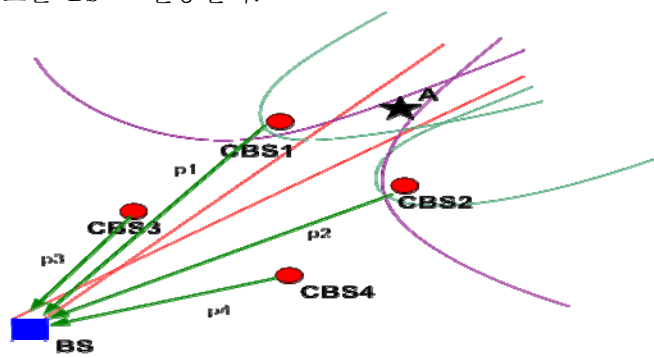
첫 번째, 그림 1 은 기본 노드 센트릭 기법에서처럼 CBS 들이 위치측정을 위해 사운드나 전파를 발생시키고 위치측정 대상노드 A 가 이 정보를 수집하여 각 CBS 와 A 노드 자신과의 거리  $d_1 \sim d_4$  를 계산한다.

이때, CBS 의 정확한 위치는 CBS 자신과 BS 만이 알기 때문에 사용자(노드 A)나 제 3 자는 CBS 와 노드 사이의 거리정보만으로는 노드의 정확한 위치파악이 어렵다.



(그림 2) Node Centroid Step2

두 번째 단계인 그림 2 에서 노드는 수집된 거리정보를 BS 로 전송한다.



(그림 3) Node Centroid Step3

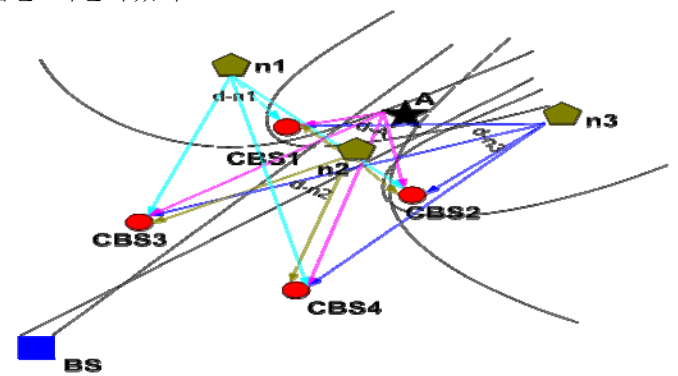
마지막 그림 3 에서 CBS 는 자신들의 위치정보를 암호화 하여 BS 로 전송하고, BS 는 이들 정보를 수집하여 노드 A 의 위치를 계산한다. 만약 노드 A 나 제 3 자가 전송되는 CBS 의 위치정보를 수집하더라도 암호화 되어있어 A 노드나 제 3 자는 A 의 정확한 위치를 알 수 없다.

#### 4.2. 인프라스트럭처 기반

인프라스트럭처 센트로이드(Infrastructure Centroid)방식은 위치 측정 대상노드가 전파나 사운드를 발생시키고 인프라스트럭처를 구성하는 노드들이 이 정보를 수집하여 거리정보를 계산하고 이를 이용하여 해당 노드의 위치를 계산하는 방식이다.

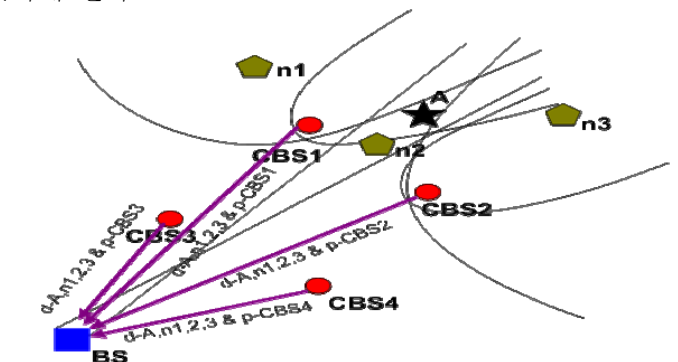
이 방법을 사용할 경우, 위치측정 대상노드가 발생하는 전파나 사운드를 제 3 자가 접근할 수 있으며 이를 이용하여 노드의 위치를 파악할 수 있다.

본 논문에서는 제 3 자가 해당 노드의 위치를 파악하는 것을 방지하기 위하여 다음 그림 4~5 와 같은 방법을 제안하였다.



(그림 4) Infrastructure Centroid Step1

먼저 그림 4 에서 대상노드 A 가 전파나 사운드를 발생시킬 때, BS 나 CBS 들이 명령을 내려 임의의 지역에 위치한 터미 노드들도 대상노드와 동일한 전파나 사운드를 발생시킨다. 따라서 네트워크 상에 전파나 사운드가 중복적으로 발생 다수의 거리정보가 생성 된다. 이때 대상노드와 터미 노드들은 발생시키는 전파(패킷)에 자신들의 정보를 암호화하여 저장함으로써 BS 만 판독 가능하게 하여 이 정보를 수신하는 것만으로는 어떠한 노드가 전파를 발생시켰는지 알지 못하게 한다.



(그림 5) Infrastructure Centroid Step2

그림 5 에서는 CBS 들은 암호화되어 전송된 정보들을 수집하여 거리를 계산하고 이를 암호화된 정보와 함께 BS 으로 전송하면 BS 는 암호화된 정보를 복호화하여 노드 정보와 거리정보를 매칭시켜 위치를 찾

는다. 이때 각 노드들이 전송한 정보는 BS 만이 판독 가능하므로 BS 만이 거리정보와 노드정보를 매칭시킬 수 있으며 노드 A 의 정확한 위치를 파악할 수 있다.

이러한 방법을 통해서 우리는 노드 A 의 위치를 BS 이외에 노출시키지 않음으로써 노드 A 의 위치정보에 대한 보안을 유지할 수 있다.

다시 말해 우리는 노드 A 의 프라이버시를 침해하지 않고 베이스스테이션이 노드 A 의 위치를 파악할 수 있도록 할 수 있다.

## 5. 결론

본 논문에서 대상노드 A 의 위치가 노출되는 것을 방지함으로써 프라이버시를 침해하지 않는 방법에 대해 제안하였다. 반면에, BS 에서는 노드의 위치를 파악할 수 있도록 하였다.

제안 방법에서 우리는 노드 센트로이드와 인프라스트럭처 센트로이드에서의 대상 노드의 위치 노출방지 기법에 대한 아이디어를 제시하였다.

제안 방법은 특정한 대상 위치를 지속적으로 파악해야 하나, 대상의 정보가 외부로 유출되거나 당사자가 수정하면 안 되는 경우 즉, 현재 이슈화되고 있는 범죠평자 감시시스템에 적용해 볼 수 있을 것이다.

앞으로의 연구에서는 앞서 제시 방법의 분석과 더불어 실내 및 실외 등 다양한 환경에 적용했을 경우에 대해 분석 및 시뮬레이션 할 것이다.

## 참고문헌

- [1] <http://forum.rfid-usn.or.kr>
- [2] G. Chen and D. Kotz, "A Survey of Context-Aware Mobile Computing Research," Dartmouth Computer Science Tech Report TR2000-381, 2000.
- [3] B. Schilit, N. Adams, and R. Want, "Context-aware computing applications," Proc. of IEEE Workshop on Mobile Computing Systems and Applications, pp. 85-90, December 1994.
- [4] M. Satyanarayanan, "Pervasive computing: vision and challenges," IEEE Personal Communications, pp.10-17, Aug. 2001.
- [5] Dey, A. K., "Understanding and Using Context," Personal and Ubiquitous Computing Journal, Vol. 5(1), pp.4-7, 2001.
- [6] I. Getting, "The Global Positioning System," IEEE Spectrum. vol.30, no.12, pp.36-47, December 1993.
- [7] GPS, <http://boom.x-y.net/>
- [8] Jeffrey Hightower, and Gaetano Borriello, "A Survey and Taxonomy of Location Systems for Ubiquitous Computing," Technical Report UW-CSE 01-08-03, University of Washington, Aug. 2001.
- [9] M. G. Kuhn, "An Asymmetric Security Mechanism for Navigation Signals," In Proceedings of the Information Hiding Workshop, 2004.
- [10] S. Capkun and J.-P. Hubaux, "Secure positioning of wireless devices with application to sensor networks," In Proceedings of InfoCom, 2005.
- [11] L.Lazos, S. Capkun, and R. Poovendran. "ROPE: Robust Position Estimation in Wireless Sensor Networks," In Proceedings of IPSN, 2005.
- [12] Z. Li, W. Trappe, Y. Zhang, and B. Nath., "Robust Statistical Methods for Securing Wireless Localization in Sensor Networks," In Proceedings of the International Conference on Information Processing in Sensor Networks (IPSN), 2005.
- [13] J.Hightower and G. Borriello. "Location systems for ubiquitous computing," IEEE Computer, 34(8):57-66, Aug 2001.
- [14] 김재호, 김영섭, 박옥선, 김성희, "유비쿼터스 위치기반 서비스 및 위치인식시스템 연구동향," ETRI 주간기술동향 통권 1127 호, 2003 년 12 월.
- [15] Andreas Savvides, Chih-Chieh Han, and Mani B. Strivastava, "Daynamic Fine-grained localization in ad-hoc Networks of sensors," in Proceedings of the 7th annual ACM/IEEE international conference on mobile computing and networking (mobicom), Rome, Italy, 2001, pp. 166-179.
- [16] N. Bulusu, J. Heidemann and D. Estrin, "GPS-less Low Cost Outdoor Localization for Very Small Devices," IEEE Personal Communications Magazine, 7(5):28-34, October 2000.
- [17] Tian He, Chengdu Huang, B. M. Blum, John A. Stankovic, and Tarek F. Abdelzaher, "Range-Free Localization Schemes in Large Scale Sensor Networks," CS-TR-2003-06. Submit to MobiCom 2003.
- [18] D. Niculescu and B. Nath, "DV Based Positioning in Ad hoc Networks," In Journal of Telecommunication Systems, 2003.
- [19] C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," in IEEE SPNA, 2003.
- [20] djan Capkun, Mario Cagalj, Mani Srivastava [CapkunCS:06] "Secure Localization With Hidden and Mobile Base Stations," IEEE Infocom 2006, Barcelona, 23-29 Apr 2006.