USNs에서 키 노출 방지를 위한 쓰레시홀드 암호화 기법

임화정° 이헌길
강원대학교 컴퓨터공학과
{hjlim°, hglee}@kangwon.ac.kr

Threshold Cryptography Scheme for Mutual Exposed Key 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 있고 위치측정기술도 개발되고 있다. 하지만, 사용자의 위치정보를 측정하는 것은 다른 한편으로 사용자의 프라이버시를 침해할 수도 있는 심각한 보안상의 문제점을 야기시킬 수 있다. 본 논문에서는 CBS(Covert Base Station)을 이용하여 베이스스테이션만이 노드의 위치를 파악할 수 있도록 하고, 위치를 파악하는 동안 노드 및 노드 주변의 다른 어떤 노드에게도 위치가 노출되지 않도록 하기 위한 (n, t+1) 쓰레시홀드 암호화 기법을 제시한다.

1. 서 론

최근 활발히 연구가 진행되고 있는 유비쿼터스 센서 네트워크(Ubiquitous Sensor Networks: USNs)는 주변 공간의 상황을 인식할 수 있고, 인식한 상황을 바탕으로 적절한 시기에 필요한 정보를 올바른 사용자나 사용자 장치에 제공해주는 지능적인 환경을 제공한다[1,2,3].

따라서 사용자 혹은 사용자 장치의 물리적인 위치와 조건 및 그 변화 정도 역시 인식할 수 있어야 하므로 사용자의 위치정보는 매우 중요한 요소로 부각되고 있다[4,5].

사용자의 위치정보를 획득할 수 있는 대표적인 시스템으로는 GPS(Global Positioning System)와 이동통신망을 이용한 위치측정 시스템을 들 수 있다[6,7].

그러나 장치의 가격이 매우 중요한 요소인 유비쿼터스 컴퓨팅 환경에서 비교적 고가인 GPS장비는 적합하지 않기 때문에 저가의 새로운 위치 측정 시스템에 대한 관한 연구가 활발하게 진행되고 있다[8].

문제는 저가의 위치 측정 시스템들은 가격이 저렴한 반면에, 사용자의 정보가 외부에 유출될 가능성이 GPS보다 높다는 단점을 갖고 있다는 것이다[7,8].

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 사용자의정화간 위치를 파악할 수 있도록 하고 사용자나 제3자가 위치정보를 변경할 경우 이를 검증하고 방지하는 방안 및 BS가 노드의 위치를 파악하는 동안 N개의 CBS들 중 t개까지 노출되어도 노드의 위치를 찾을 수 있는 (n, t+1) 쓰레시홀드 기법을 제안하고자 한다.

본 연구 2장에서 위치 측정 기술 및 위치 인식 시스템에 대해 살펴보고, 3장에서 제안 시스템 모델에 대해서 묘사하기로 한다. 4장에서는 CBS를 이용한 인프라스트럭쳐 기반 및 노드 기반에서의 노드 위치보호 메커니즘 및 레퍼런스 노드의 노출에도 보안을 유지할 수 있는 (n, t+1) 쓰레시홀드 기법에 대해 설명한 후 결론에서 논문의 적용분야 및 향후 연구방향에 대하여 설명하도록 한다.

2. 위치 측정기술 및 시스템

위치측정 기술은 측정방식에 따라 삼각측량, 장면분석, 근접방식 등으로 분류하거나, GPS와 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].

3. 제안 모델

3.1 시스템 모델

제안시스템은 노드와 상호 신뢰 관계인 베이스스테이션(BS)과 N개의 CBS(Covert Base Station)들로 구성된다.

제안된 시스템에서의 노드는 CBS의 위치를 모르며 자기 자신의 정확한 위치도 알지 못한다.

CBS는 노드의 위치를 알 수 없지만, 자신의 위치정보를 알고 있고, 노드로부터 전송되는 신호로 거리계산을 할 수 있다. 또한 CBS는 베이스스테이션과 암호화된 키를 공유하고 있고 이를 이용해 정보를 주고받는다.

베이스스테이션은 노드로부터의 정보와 CBS로부터 수집된 CBS와 노드와의 거리정보 및 CBS의 위치정보를 토대로 노드의 위치를 파악할 수 있다. 반면에 노드나 CBS는 거리정보만으로 노드의 위치를 계산할 수 없으므로 노드의 위치는 BS이외에는 노출되지 않는다.

4. 제안된 노드 위치보호 기법

센서네트워크를 이용하는 위치인식 시스템은 크게 노드 센트로이드(Node Centroid)방식과 인프라스트럭쳐 센트로이드(Infrastructure Centroid)방식으로 분류할 수 있다[14].

각각의 경우에 노드 위치 보호기법은 다음과 같다.

4.1 노드 센트릭 기반

노드 센트로이드(Node Centroid)방식에서는 노드의 위치를 찾기 위해 인프라스트럭쳐를 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 제3 자에게 유출되거나 변경될 수도 있다.

이를 방지하기 위해 첫째, 사용자의 위치는 BS만이 계산 가능하도록 한다. 둘째, 위치 계산을 위해 필요한 인프라스트럭쳐 노드들의 정확한 위치 정보가 사용자를 포함한 외부에 유출되는 것을 방지하기 위해 CBS개념을 도입하였다. 제안된 기법은 그림 1과같이 동작한다.

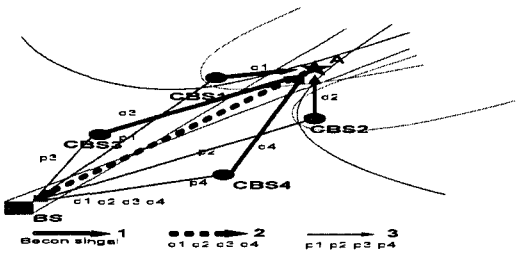

그림 1 Node Centroid

그림1의 과정1은 기본 노드 센트릭 기법에서처럼 CBS들이 위치측정을 위해 사운드나 전파를 발생시키고 위치측정 대상노드A가 이 정보를 수집하여 각CBS와 A노드 자신과의 거리d1~d4를 계산한다.

과정 2에서 노드A는 수집된 거리정보를 BS로 전송한다.

과정 3에서 CBS는 자신들의 위치정보를 암호화 하여 BS로 전송하고, BS는 이들 정보를 수집하여 노드A의 위치를 계산한다. 만약 노드A나 제3자가 전송되는 CBS의 위치정보를 수집하더라도 암호화 되어있어 A노드나 제3자는 A의 정확한 위치를 알 수 없다.

4.2 인프라스트럭쳐 기반

인프라스트럭쳐 센트로이드(Infrastructure Centroid)방식은 위치 측정 대상노드가 전파나 사운드를 발생시키고 인프라 스트럭쳐를 구성하는 노드들이 이 정보를 수집하여 거리정보를 계산하고 이를 이용하여 해당 노드의 위치를 계산하는 방식이다. 이 방법을 사용할 경우, 위치측정 대상노드가 발생하는 전파나 사운드를 제3자가 접근 할 수 있으며 이를 이용하여 노드의 위치를 파악할 수 있다.

본 논문에서는 제3자가 해당 노드의 위치를 파악하는 것을 방지하기 위하여 다음 그림 4~5와 같은 방법을 제안하였다.

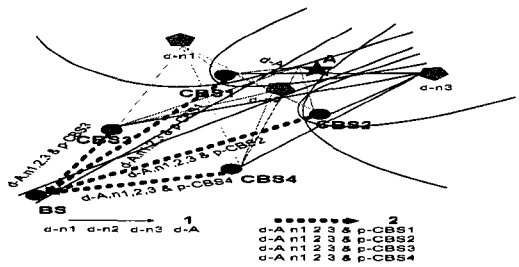

그림 2 Infrastructure Centroid

그림2의 과정 1은 대상노드A가 전파나 사운드를 발생시킬 때, BS나 CBS들이 명령을 내려 임의의 지역에 위치한 더미 노드들도 대상노드와 동일한 전파나 사운드를 발생시킨다. 따라서 네트워크 상에 전파나 사운드가 중복적으로 발생 다수의 거리정보가 생성 된다. 이때 대상노드와 더미 노드들은 발생시키는 전파(패킷)에 자신들의 정보를 암호화하여 저장함으로써 BS만 판독 가능하게 하여 이 정보를 수신하는 것만으로는 어떠한 노드가 전파를 발생시켰는지 알지 못하게 한다.

과정 2에서는 CBS들은 암호화되어 전송된 정보들을 수집하여 거리를 계산하고 이를 암호화된 정보와 함께 BS으로 전송하면 BS는 암호화된 정보를 복호화하여 노드 정보와 거리정보를 매칭시켜 위치를 찾는다. 이때 각 노드들이 전송한 정보는 BS만이 판독 가능하므로 BS만이 거리정보와 노드정보를 매칭시킬 수 있으며 노드A의 정확한 위치를 파악할 수 있다.

이러한 방법을 통해서 우리는 노드 A의 위치를 BS이외에 노출시키지 않음으로써 노드A의 위치정보에 대한 보안을 유지할 수 있다. 다시 말해 우리는 노드 A의 프라이버시를 침해하지 않고 베이스스테이션이 노드A의 위치를 파악할 수 있도록 할 수 있다.

4.3 (n, t+1)쓰레시홀드 기법

Shamir[15]가 비밀 공유 기법을 제안한 이후, 쓰레시홀드 암호화 시스템은 발전하였다. 쓰레시홀드 암호화기법은 공개키와 비밀키 쌍을 이용하는데, 공개 키는 한 개만 존재하는 반면에 비밀키는 n개의 노드로 이루어진 그룹에 의해 비밀정보가 일부분씩 공유된다. 비밀키는 쓰레시홀드 값 t이하의 노드는 원문을 복구해 내지 못하고 t+1 이상의 노드가 모여야만 비밀키를 얻어낼 수 있는 암호화 시스템이다[16]. 또한 Pedersen은 신뢰할 수 있는 노드(trusted party)가 없는 쓰레시홀드 암호화 시스템을 제안하였다[17].

이 기법은 주로 공개키 기반에 적용되나, 센서네트워크는 특성상 특정 관리자에 의해 배치된 센서 노드들로 네트워크가 구성된다. 따라서 초기 노드 배치할 때 초기 키를 분배하여 배치하면 $(n,t+1)$쓰레시 홀드 기법을 적용할 수 있다.

4.3.1 키 생성 프로토콜

하나의 수신자 그룹에 속해 있는 각각의 수신자는 임의의 비밀정보 $Si \in Zq$ 와 임의의 문자열 Ri를 생성한다.

Ri에서 $C(Ri,Si) \in \{0,1\}$ 을 생성하고 $hi = g^{Si}$ 를 생성하여 브로드캐스트한다. 이때 대표수신자(Quorum)는 $\prod hi$ 를 구하여 그룹에 대한 공개키 생성한다.

여기서 각각의 수신자는 자신이 생성한 비밀정보 Si와 Ri를 생성할 수 있다.

원문을 얻기 위한 비밀키 생성프로토콜에서 각각의 사용자는 임의의 $t+1$차 방정식을 만든다.

$f_1(z) = f_{i0} + f_{iZ}Z + \Lambda + f_{ik} + f_{ik-1}Z^{k-1} \bmod, f_{i0} = Si$

생성된 $f_1(z)$로부터 $f_1(j) = S_{ij}$를 생성하여 각각의 j 노드에게 안전한 채널을 통해 전송한다. 각 수신자는 $S_i = \sum S_{ji}$ 를 구하여 $x = \sum S_i$ 인 비밀키를 생성한다.

4.3.2 키 재 생성

$(n,t+1)$쓰레시홀드 암호화시스템은 초기 키를 가지고 키를 재 생성할 수 있다. 따라서 첫째, 네트워크의 안전도를 증가시킬 수 있고 둘째, 수신자 그룹에 새로운 노드의 진입이나 탈퇴가 없는 경우 주기적 키 재생성을 통해 새로운 그룹키를 생성하여 기밀성과 무결성을 보장할 수 있다.

4. 결론

본 논문에서 대상노드A의 위치가 노출되는 것을 방지함으로써 프라이버시를 침해하지 않는 방법과 더불어 BS에서는 노드의 위치를 파악할 수 있도록 하였다.

제안 방법에서 우리는 노드 센트로이드와 인프라스트럭쳐 센트로이드에서의 대상 노드의 위치 노출방지기법 및 레퍼런스 노드의 노출에도 노드의 위치를 측정할 수 있는 방법에 대한 아이디어를 제시하였다.

이중 노드 센트로이드 방식은 특정한 대상 위치를 지속적으로 파악해야 하나, 대상의 정보가 외부로 유출되거나 당사자가 수정하면 안 되는 경우 즉, 현재 이슈화되고 있는 범죄자 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] djan Capkun, Mario Cagalj, Mani Srivastava [CapkunCS:06] " Secure Localization With Hidden and Mobile Base Stations," IEEE Infocom 2006, Barcelona, 23-29 Apr 2006.

[15] Adi Shamir, " How to share a secret," Communications of the ACM, Vol.22(1979, pp.612-613.

[16] L. Zhou, Z.Hass, " Securing ad hoc networks," IEEE Network, 1999.

[17] T. P Pedersen, :" A Threshold Cryptosystem without a Trusted Party," In Advances in Cryptology-Eurocrypt ' 91, pages 522-526, 1991.