무선 센서 네트워크에서 위치 정보를 이용한 키 생성 기법

최여민, 채미연, 송주석
연세대학교 컴퓨터과학과

Location-Based Key Generation Scheme in Wireless Sensor Networks

Yeomin Choi, Mee Youn Chae, Jooseok Song
Department of Computer Science, Yonsei University

요 약

센서 네트워크는 다양한 환경에서 사용되고 있으나 지금까지 제시된 센서 네트워크의 보안 기법은 센서 네트워크가 사용되는 다양한 환경에서 모두 적용하기에는 한계가 있다. 이 논문에서는 센서 노드의 위치 정보를 이용할 수 있는 특정 환경에서 사용할 수 있는 키 생성 기법을 제시한다.

I. 서론

센서 네트워크는 전 세계적으로 환경 및 생태 감시, 군사 작전, 인텔리전스 빌딩 등 많은 분야에서 활용되고 있다.[1]

이렇게 여러 분야에서 활용되고 있는 만큼 센서 네트워크를 통해 오가는 정보들에 대한 보안 위협이 중요한 문제가 되었으며, 특히 센서 노드들의 경우는 여러 제약 사항을 가지고 있기 때문에 이런 제약을 극복하기 위한 다양한 보안 기법들이 발표되었다. 그러나 현재까지 발표된 대부분의 기법들은 센서 네트워크가 사용되는 다양한 환경에 대한 고려가 되어있지 않기 때문에 실제로 사용되는 환경에 그대로 적용하는 데에는 많은 어려움이 따른다. 따라서 본 논문에서는 센서 노드의 위치 정보를 알 수 있다는 특정 환경 하에서 사용할 수 있는 보안 기법을 제시하려고 한다.

본 논문은 다음과 같이 구성된다. II 에서는 본 논문과 관련된 pair-wise 키 분배 기법에 대한 연구를 소개하고, III에서는 본 논문에서 제시하는 기법을 소개하며, IV에서는 보안 및 성능 측면에서 분석을, V에서 마무리한다.

본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 육성·지원사업의 연구결과로 수행되었음

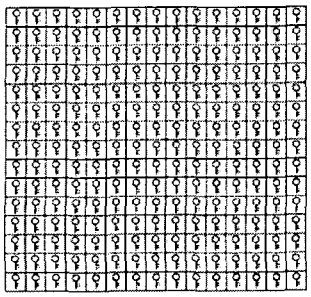
II. 관련 연구

2.1 LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks.

LEAP[2]은 센서 노드가 포획되어 메모리의 정보가 유출될 시간을 가정하고, 노드가 공격당하기 전에 하나의 그룹 키를 사용하여 세션 키를 교환하고 그룹 키를 삭제하는 방법을 사용한다. 그룹 키가 삭제된 이후에는 임의의 센서 노드가 공격당해도 전체 그룹 키는 삭제되었기 때문에 공격자는 네트워크 전체에서 사용되는 키를 알 수 없다.

2.2 Probability Density Function of Node Deployment

Ito와 Ohta 등의 연구[3]는 센서 노드가 위치할 수 있는 지역들을 분할하여 [그림 1]과 같은 Key-Position Map을 구성하여 지역에 따라 할당된 Key를 가지게 고안되었다. 이 기법에서



〔그림 1〕 Key-position Map

는 최종적인 센서 노드의 위치를 알 수 없기 때문에 센서 노드가 뿌려지고, 통신할 수 있는 범위 내에 있는 지역 키를 다음과 같이 Random하게 생성한다.

1. 센서 노드가 뿌려질 수 있는 범위 내에서 점 P를 구한다.
2. 점 P에서 통신할 수 있는 점 Q를 구한다.
3. 구해진 점 Q의 위치에 해당하는 지역에 해당하는 Key를 생성하여 센서 노드에 저장한다.
4. m개의 Key가 생성될 때까지 이 작업을 반복한다.

두 노드 사이에 통신을 할 때에는 이렇게 만들어진 지역 키들 중 서로 공유하고 있는 키를 이용해서 통신한다.

이 기법의 단점으로는 지역 키를 만드는 범위가 실제로 센서가 통신할 수 있는 범위보다 크며, 센서가 여러 위치에서 뿌려질 경우에 다른 위치에서 뿌려진 센서들과 통신할 수 있는 확률이 적어지게 되는 것과 또 센서들을 뿌리려고 하는 곳의 지형 등이 복잡할 경우 센서들이 뿌려질 수 있는 위치에 대한 계산이 복잡해지게 된다.

III. 제안하는 기법

3.1 센서 네트워크의 발전 방향 및 가정

본 논문에서 고려하는 센서 네트워크는 다음과 같은 센서 네트워크에 사용되는 센서 노드들은 앞으로 기술이 발전하면서 다음과 같은 경향을 가지게 될 것으로 전망된다.

- 에너지 효율성: 센서 노드들은 제한적인 배터리의 전원만을 사용하기 때문에 에너지를 효율적으로 사용해야 한다. 앞으로 기술이 발전함에 따라 같은 Processing Power를 이용하기 위한 소비 전력은 계속적으로 감소할 것으로 기대되지만, 데이터 송수신에 필요한 전력은 어느 한계 이하로 내려갈 수 없기 때문에 데이터 송수신을 최소화 하는 것이 중요할 것이다.

- 센서 위치 인식: 센서 노드의 위치 정보를 정확히 알게 될수록 센서 네트워크를 통해 얻은 정보의 해상력이 증대될 것이다. 센서 네트워크가 다양한 분야에 활용될수록 이러한 요구가 많아질 것이며, 센서 노드들이 자신들의 위치를 쉽게 알 수 있는 방법이 필요할 것이다.

따라서 본 논문에서 고려하는 센서 네트워크는 다음과 같은 가정을 만족한다.

- 센서 네트워크를 통해 센싱하려는 범위는 광범위하며, 센서 노드는 한 번 뿌려진 이후 이동하지 않는다.
- 센서 노드는 자신의 위치를 쉽게 알 수 있다.
- 처음 Network Setup을 수행하는 동안에는 공격을 받을 확률이 거의 없다.

3.2 제안하는 기법

본 논문에서는 위 가정 및 발전 방향에 맞추어 센서 네트워크의 데이터 수집 범위가 광범위하며, 센서 노드들이 자신의 위치를 쉽게 알 수 있다고 가정했을 때, Ito 등의 연구[3]를 발전시켜서 센서 노드들의 위치 정보를 기반으로 한 키 생성 기법을 제시하려 한다.

3.2.1 표기법 (Notation)

본 논문에서 표기하는 용어들에 대한 설명은 다음과 같다.

- K_M : 센서 노드가 초기 상태에 가지고 있는 마스터 키. 마스터 키와 센서의 위치 정보를 이용해서 실제로 사용되는 키를 생성한다.
- N : 센서 네트워크를 통해 정보를 얻으려는 하는 지역의 총 수
- n : 센서 노드가 통신 가능한 영역 내에 위치하는 지역의 수
- m : 센서 노드가 가지는 지역 키의 수
- L : 센서 노드의 위치
- X || Y : X와 Y를 결합한 메시지

- F(x) : x를 이용해서 키를 생성하는 함수
- K : 두 센서 노드간의 통신에 사용되는 pair-key
- KID : 키 K의 ID

3.2.2 제안하는 기법

먼저 센서 네트워크의 정보 수집 대상이 되는 지역을 [그림 1]에서와 같이 Key-position Map으로 나눈다. 이후 Master Key K_M을 뿌리려는 센서 노드에 모두 저장한 후에 센서 노드들을 뿌려준다.

센서 노드들이 뿌려진 이후, Network Setup에서는 다음 과정을 통해 센서 노드들의 지역 키를 설정한다.

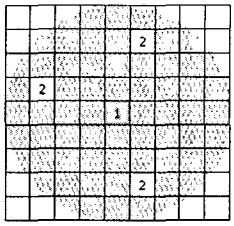
1. 자신의 위치에 해당하는 지역 키를 가진다.
   $K_0 = F(K_M \| L), KID_0 = L$
2. 통신 가능한 영역 내에 있는 위치 L_i를 랜덤하게 생성한 후에 해당 지역에 해당하는 지역 키를 가진다.
   $K_i = F(KM \| L_i), KID_i = L_i$
3. 2번 동작을 가지고 있는 Key의 개수가 총 m개가 될 때까지 반복한다.
4. 마스터 키 K_M을 삭제한다.

이 방법을 통해 센서 노드가 가지는 지역 키의 예는 [그림 2]와 같다.

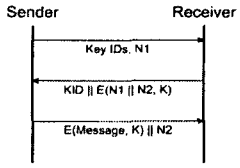
센서 노드는 이렇게 생성된 지역 키를 이용해서 다른 노드들과 통신하게 되며, 다른 노드와 직접 연결을 할 수 있는 경우의 연결 및 인증 과정은 다음과 같다.

1. Sender에서 Receiver에게 자신이 가지고 있는 키들의 ID들을 포함한 HELLO 메시지를 보낸다.
2. Receiver에는 Sender가 가진 키의 ID들을 보고, 공통적으로 가진 키를 선택한다.
3. Receiver는 선택된 키의 ID와 함께 해당 키로 암호화한 연결 수락 메시지를 보낸다.
4. Sender는 Receiver가 보낸 키의 ID를 이용해서 Receiver의 연결 수락 메시지를 복호화한 인증정보와 해당 키로 암호화한 실제 메시지를 보낸다.

위 과정에서 Sender와 Receiver 간에 오가는 정보를 나타낸 것이 [그림 3]이며, 이 과정을 통해 두 노드들은 서로의 통신에 필요한 공유 키를 알 수 있게 된다.



[그림 2] 센서가 최종적으로 가지는 지역 키의 예.



[그림 3] 두 센서 노드들이 직접 연결되어 통신할 때 전달되는 메시지.

IV. 분석

4.1 보안 공격

센서 네트워크에서 발생할 수 있는 다음과 같은 보안 문제들에 대해서 본 논문에서 제시한 기법의 안정성을 평가하였다.

4.1.1 도청 및 스파이 노드 추가

공격자는 센서 네트워크에서 오가는 모든 정보를 볼 수 있다고 가정할 때, 본 논문에서 제시된 기법은 마스터 키나 실제 사용되는 키를 직접 전송하지 않기 때문에 공격자가 전송에 사용되는 키를 알기 힘들며, 스파이 역할을 할 노드를 센서 네트워크에 추가했다고 하더라도 키를 알 수 없기 때문에 다른 센서 노드들과의 통신도 불가능하다.

4.1.2 물리적인 포획

Network Setup이 끝나기 전에 센서 노드가 포획된다면 공격자가 K_M을 알아낼 수 있기 때문에 이를 통해 센서 네트워크에서 사용되는 모든 지역 키를 알아낼 수 있다. 그러나 LEAP[2]에서도 분석되었듯이 Network Setup은 빠른 시간 내에 종료되며, 실제로 공격자가 물리적인 포획을 통해 K_M을 알아내는 것은 매우 어렵다.

공격자가 실제 동작중인 센서 노드를 직접 포획하여 센서 노드에서 가지고 있는 정보를 알아내는 공격이다. 이 공격을 통해 공격자는 한 개의 센서 노드를 포획하였을 경우 m개의 지역 키를 알아낼 수 있지만, 이런 지역 키들을 통해 마스터 키를 알아내는 것은 매우 어려우며, 전체 통신에서 사용되는 N개의 키들 중 m개의 키만을 알아냈을 뿐이며, 이 키들을 사용하는 센서도 되는 범위도 해당 지역을 통신 범위 내에 두고 있는 노드들뿐이다. 여기에서 센

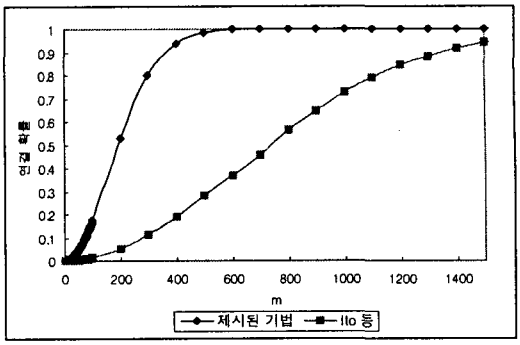
서 노드가 가지는 키의 개수를 늘리면 센서 노드들 사이의 연결성은 좋아지지만, 센서 노드가 포획 당했을 때 정보 유출 확률 또한 늘어난다.

4.2 비교 분석

본 논문에서 제시한 기법을 Ito 등의 연구[3]에서 제시된 기법과 비교 시뮬레이션을 통해 분석하였다. 분석에 사용된 가정 및 변수는 다음과 같다.

- Key-position Map이 구성되는 지역들은 정사각형의 2차원 영역이다.
- 센서는 한 곳에서만 뿌려진다.
- 센서가 뿌려질 수 있는 범위의 반지름 위에 있는 지역의 수는 100 개이며, 이 범위 내에 있는 총 지역의 수는 약 $100^2 \times \pi$ 개이다.
- 센서가 통신할 수 있는 범위의 반지름 위에 있는 지역의 수는 500 개이며, 이 범위 내에 있는 총 지역의 수는 약 $500^2 \times \pi$ 개다.
- 센서 노드가 가지는 키의 개수를 변화시키면서 1만번씩 시뮬레이션 하였다.

시뮬레이션 결과 [그림 4]의 결과를 얻을 수 있었다. 이 결과를 분석해보면 같은 확률로 키를 공유하는 경우 본 논문에서 제시한 기법이 더 좋은 것을 볼 수 있다. 이는 본 논문에서 제시한 기법은 실제 통신 가능한 영역만을 대상으로 해서 지역 키를 생성하기 때문에 지역 키의 후보가 될 수 있는 범위가 Ito 등의 연구[3]에서 제시된 기법보다 더 작기 때문이다. 또한 [3]의 단점으로 제시했던 다른 곳에서 뿌려진 인접한 노드와의 통신 문제에 대해서도 더 좋은 결과를 보여줄 것으로 보이며, 센서 노드의 실제 위치를 기반으로 하기 때문에 센서 노드가 뿌려지는 곳의 지형이 복잡해도 이용할 수 있다.



[그림 4] 시뮬레이션 결과

V. 결론

본 논문에서 제시된 기법은 실제로 인접된 노드에서 가지고 있을 확률이 높은 키들만을 생성하기 때문에 이웃 노드들과의 연결성이 높으며, 공격자에 의해 지역 키가 유출되어도 다른 지역의 노드들은 영향을 받지 않는다. 그러나 센서 노드가 이동성을 가지고 있거나 위치 정보를 알 수 없는 경우에는 사용할 수 없다는 한계가 있다.

VI. 앞으로 계획

본 논문에서 제시된 기법은 센서 노드가 이동성을 갖지 못한다는 것을 가정하고 있다. 센서 노드가 이동성을 가지는 경우에 사용할 수 있는 보안 기법을 연구해야 할 것이다.

[참고문헌]

[1] Seyit A. Çamtepe and Bülent Yener, "Key distribution mechanisms for wireless sensor networks: a survey" Rensselaer Polytechnic Institute, Computer Science Department, Tech. Rep. 05-07, Mar. 2005.

[2] S. Zhu, S. Setia and S. Jajodia. "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks." To appear in the 10th ACM Conference on Computer and Communications Security '03, Washington D.C., Oct. 2003.

[3] Takashi Ito, Hidenori Ohta, Nori Matsuda, and Takeshi Yoneda, "A key pre-distribution scheme for secure sensor networks using probability density function of node deployment" Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks '05, Nov. 2005