PIKE를 이용한 센서네트워크에서의 키 합의 프로토콜†

양연형*, 이필중*

*포항공과대학교 전자전기공학과

Key Establishment Protocol in a Sensor Network Using PIKE

Yeon Hyeong YANG*, Pil Joong LEE*

*Department of Electronic and Electrical Engineering, POSTECH

요 약

무선 센서 네트워크는 미래의 유비쿼터스 컴퓨팅에서 핵심적인 역할을 할 것으로 알려져 있으며, 그에 따라 센서 네트워크에서의 안전한 통신도 중요한 문제로 떠오르고 있다. 이러한 센서 네트워크에서의 안전한 통신을 위해서는 각 센서 노드 사이에서의 안전한 키 관리 프로토콜이 필수적이다. [1]에서는 기존에 제안된 key-predistribution 방식보다 효율적인 키 합의 프로토콜을 제안했다. 그런데, [1]에서 제안된 PIKE 프로토콜에서 각 센서 노드 사이의 통신에 대한 가정을 현실적으로 바꾸면 보다 효율적인 프로토콜을 얻을 수 있다. 네트워크의 전체 센서 노드의 수를 n이라고 했을 때, [1]에서 제안된 프로토콜에서 각 센서 노드의 메모리 소요량은 $O(\sqrt{n})$이나, 본 논문에서는 키 합의 매개 노드의 수와 메모리 소요량 사이의 trade-off 관계를 보이고 최적의 프로토콜을 구성하는 방법에 대해 논의한다.

I. 서론

무선 센서 네트워크는 미래의 유비쿼터스 컴퓨팅 환경에서 핵심적인 역할을 할 것으로 알려져 있으며 그 관심이 증대되고 있다. 이러한 관심의 증대와 더불어 센서 네트워크에서 안전한 통신이 중요한 문제로 떠오르고 있다. 이 문제는 결국, 각 노드 사이의 비밀키를 어떻게 관리할 것인가 하는 문제로 귀결된다.

일반적으로 두 객체 사이에서의 비밀키 공유를 위해서는 공개키에 기반한 키 공유 프로토콜을 사용할 수 있으나, 센서 노드와 같이 열악한 환경에서는 그러한 프로토콜의 사용이 부정적인 평가를 받고 있다.

센서 노드와 같이 통신능력이 제한되어 있으며, 전력이나 메모리, 계산능력이 떨어지는 장치들에서는 키 분배 센터와 같은 중앙집중식 관리체계를 생각할 수 있다[6, 7]. 그러나 이러한 방식은 키 분배 센터에 부하가 집중되고, 다이나믹 라우팅을 사용하는 네트워크에서는 분배 센터 주변의 노드들에 과중한 통신이 이루어진다. 또한 이러한 방식은 키 분배 센터가 집중적인 공격 대상이 되고, 일단 키 분배 센터가 공격되고 나면 전체 네트워크의 비밀 통신이 위협받게 된다.

다른 방식으로는 모든 노드가 사전에 상호 비밀키를 배포받는 방식이 있으나[2, 3], 이 방식은 네트워크의 크기가 클 경우 각 노드의 메모리 부담도 같이 커지게 된다. 이러한 부담을 줄이기 위해서 random key predistribution[2, 3, 4, 5] 방식이 제안되었다. 그러나 이러한 방식을 사용하더라도 안전한 네트워크를 만들기 위해서는 각 노드 사이의 통신량이 $O(n)$으로 증가하게 된다.

이런 문제점을 개선하기 위해서 Chan과

† 본 연구는 정보통신부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업, BK21 사업의 연구결과로 수행되었음.

Perrig에 의해서 PIKE 프로토콜이 제안되었다 [1]. 이 프로토콜에서는 각 노드의 메모리 요구량과 통신 요구량이 모두 $O(\sqrt{n})$으로 줄어들게 된다.

II. PIKE 프로토콜

이 절에서는 기본적인 PIKE 프로토콜을 설명한다. 본 논문에서 n은 네트워크에서 전체 노드의 수를 나타낸다.

1. 키 사전 배포 단계

각 노드는 $O(\sqrt{n})$개의 다른 노드들과 각각 키를 사전 공유한다. 각 노드들 사이에 공유되는 pairwise key는 각 노드의 쌍마다 유일하도록 한다. 이때, 전체 노드의 수 n이 perfect square라고 가정하면 각 노드는 $2(\sqrt{n}-1)$개의 노드와 키를 공유하게 된다. 각 노드에 (x,y) 형태의 ID를 부여하게 되면, 노드 (x,y)는 $0 \le i,j \le \sqrt{n}-1$인 i,j에 대하여 (i,y), (x,j)를 ID로 갖는 노드들과 키를 공유한다. 예를 들어 그림 1에서 노드 (1,1)은 (0,1)부터 (9,1)까지의 9개의 노드, (1,0)부터 (1,9)까지의 9개의 노드와 비밀키를 사전 공유한다.

2. 공유키 확인 단계

각 노드마다 $2(\sqrt{n}-1)$개의 키를 사전 배포한 후에 각 노드는 실제 설치된다. 설치된 이후에 임의의 노드와 비밀 통신을 하고자 할 경우 공유키 확인 단계를 먼저 거친다. 이 단계에서는 통신하려는 노드와 사전에 배포된 pairwise키를 가지고 있는지를 확인하는 단계이다. 노드 (x,y)가 노드 (a,b)와 비밀 통신을 하고자 할때 $x=a$, 혹은 $y=b$의 관계가 만족할 때는 사전에 공유된 키가 있으므로 그 키를 사용해 비밀통신을 한다.

3. 키 매개 단계

사전에 공유된 키가 없는 경우에는 매개 노드를 이용해 키 공유를 수행한다. 위의 키 사전 배포 단계에서 설명한 것과 같은 방식을 사용할 경우, 임의의 노드 A와 B에 대해서 A, B 모두와 키를 사전에 공유하고 있는 노드 C가

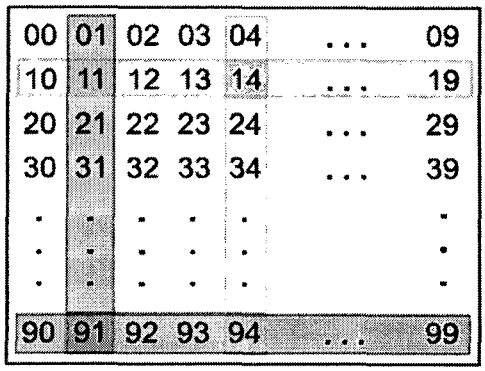

그림 1. 키의 사전 공유 관계도

반드시 존재하게 된다. 예를 들어, 그림 1의 경우, 노드 (1,1)이 노드 (9,4)와 키 공유를 수행해야 할 경우 노드 (9,1)은 (1,1)과도 키를 사전 공유하고 있고 노드 (9,4)와도 키를 사전 공유하고 있게 된다.

노드 A와 B가 매개 노드 C를 통해서 키를 공유하는 과정은 다음과 같다.

$A \rightarrow C: E_{K_{AC}}\{A,B,K_{AB}\}, \mathrm{MAC}_{K_{AC}}(E_{K_{AC}}\{A,B,K_{AB}\})$

$C \rightarrow B: E_{K_{BC}}\{A,B,K_{AB}\}, \mathrm{MAC}_{K_{BC}}(E_{K_{BC}}\{A,B,K_{AB}\})$

$B \rightarrow A: E_{K_{AB}}\{A,B,N_B\}, \mathrm{MAC}_{K_{AB}}(E_{K_{AB}}\{A,B,N_B\})$

4. 노드의 설치 순서

위의 키 매개 단계에서 키 매개가 실패 없이 이루어지기 위해서는 전체 네트워크의 노드들이 모두 설치되었다는 가정이 필요하다. 그러나, 전체 n개의 노드를 한꺼번에 설치한 후 더 이상 추가되는 노드가 없는 것을 가정하기보다는, n보다 작은 수의 노드를 설치한 후 나중에 노드를 더 추가할 수 있도록 하는 것이 현실적이다. 이 경우에는 어느 노드를 먼저 설치할 것이냐가 중요한 문제가 된다. [1]에서는 노드 (0,0)부터 (0,1), (0,2)의 순서로 차례대로 설치한 후에, (0,9) 이후에는 (1,0), (1,1), (1,2), ... 의 순서로 설치하도록 규정하고 있다. 이렇게 할 경우에는 전체 n개의 노드가 모두 설치되지 않더라도 임의의 두 노드와 모두 키를 공유하고 있는 매개 노드를 결정할 수 있다.

III. PIKE 프로토콜의 통신 모델

기본적인 PIKE 프로토콜은 임의의 두 노드가 최대 하나의 매개 노드만을 경유하여 공유키를 생성하도록 하고 있다. 그러나 키의 사전 공유 관계도에서 가까운 노드들일 수록 실제로 설치되었을 때도 가까울 가능성이 커지게 된다. 반대로 말하면, 실제 설치된 이후에 이웃에 있는 노드들은 키 사전 공유 관계도에서도 가까운 위치에 있을 가능성이 크게 된다. 이 경우에 하나의 노드가 $2(\sqrt{n}-1)$개의 노드와 키를 공유하지 않고 그보다 가까운 노드들과만 키를 사전 공유해도 이웃 노드들끼리 키를 공유할 때는 문제가 발생할 가능성이 적게 된다.

또한, 가까운 노드들일 수록 보다 빈번한 통신을 하게 된다는 것도 자연스러운 현상이 된다. 다시 말하면, 설치된 장소가 먼 노드들끼리 비밀 통신을 하는 빈도는 더 낮다고 가정할 수 있다.

IV. 개선된 PIKE 프로토콜

1. 키 사전 배포 단계

$\sqrt{n}=2km$의 관계를 만족하는 정수 k,m이 존재한다고 가정한다. 하나의 노드는 키 공유 관계도에서 같은 열에 존재하는 $2m$개의 노드들, 같은 행에 존재하는 $2m$개의 노드와 공유한다. 이 때 하나의 노드가 키를 사전에 공유하는 노드의 수는 $4m$이 된다. 노드의 ID가 (x,y)라고 할 때, 이 노드는 $-m \leq i,j \leq m$를 만족하는 i,j에 대하여, $(x+i \bmod \sqrt{n}, y)$의 노드들, $(x, y+j \bmod \sqrt{n})$의 노드들과 키를 사전 공유한다.

2. 공유키 확인 단계

공유키 확인 단계는 기본적으로 PIKE 프로토콜과 같으나, 노드 사이의 가로축의 거리와 세로축의 거리가 m 이하인 경우에 사전 공유키가 있다는 것만 다르다.

3. 키 매개 단계

키 매개 단계도 기본적으로 PIKE 프로토콜과 같으나, 노드 사이의 거리가 먼 때는 여러 개의 매개 노드가 필요 할 수 있다는 것만 다르다. 그러나 이것은 무시할 수 없는 차이가 된다.

노드 사이의 가로축과 세로축의 거리가 m 이하인 경우에는 PIKE 프로토콜과 같은 방식으로 하나의 매개 노드를 이용해서 키를 공유한다. 이때 노드 (x,y)에 대해서 $|x-a|<m$, $|y-b|<m$을 만족하는 노드 (a,b)들로 이루어지는 정사각형을 편의상 직접통신범위라고 정의한다. 실제로는 최대 하나의 매개 노드만을 이용해서 키를 공유할 수 있는 범위이다.

노드 A, B 사이의 거리가 $2m$보다 작은 경우에는 두 노드의 직접 통신 범위가 겹치는 곳에 존재하는 노드 C를 우선 선정한다. 이 노드 C는 노드 A와 B와 최대 하나의 매개 노드를 사용하여 키를 공유할 수 있으므로, 노드 A와 B는 최대 3개의 매개 노드를 사용하여 키를 공유할 수 있다.

이보다 먼 거리에 있는 노드들 사이에는 더 많은 매개 노드가 사용될 수 있다. 이러한 방식을 사용하면 키 공유 관계도에서 먼 거리에 있는 노드들은 많은 수의 매개 노드를 거쳐야만 키를 공유할 수 있다는 문제점이 있으나, 3절에서 살펴보았듯이 이러한 경우는 적게 발생할 것이라고 예상할 수 있다.

4. 노드의 설치 순서

PIKE 프로토콜에서는 키 관계도에서 한 개의 행에 해당하는 노드들부터 설치했으나, 개선된 프로토콜에서는 보다 세심한 주의가 필요하다.

키 공유 관계도를 $2k \times 2k$개의 블록들로 나눈다. 각각의 블록들은 $0 \leq X, Y \leq 2k-1$인 X, Y에 대하여 (X, Y)라고 이름 붙인다. 이때, 블록 (0,0)에 있는 노드들을 먼저 설치하고, 그 다음은 블록 (0,0)에서 나선형으로 블록들을 설치한다. 각 블록 내에서는 PIKE 프로토콜에서와 같은 방식으로 노드들을 설치한다.

이렇게 하면 임의의 두 노드에 대해서 몇 개의 매개노드를 사용하든 비밀키를 공유할 수 있게 된다. 그러나 3절의 가정을 적용하면 이

경우에 가까운 블록들끼리는 더 적은 수의 매개 노드를 사용하여 키를 공유할 수 있으며 대부분의 경우는 여기에 해당할 것이다.

V. 비교

PIKE 프로토콜에서는 각각의 노드가 $2(\sqrt{n}-1)$개의 노드와 키를 사전 공유해야 했다. 개선된 프로토콜에서 $k=2$라고 가정했을 때, 각각의 노드는 $\sqrt{n}$ 개의 키를 사전 공유한다. PIKE 프로토콜에서는 공유키를 생성하기 위해서 최대 한 개의 매개노드가 사용되지만, 개선된 프로토콜에서는 최대 3개의 매개노드가 사용된다. 참고로, $k=1$일 경우는 기존의 PIKE 프로토콜과 같다. 파라미터 k로 trade-off 관계를 조절할 수 있다.

VI. 결론

본 논문에서는 센서네트워크에서의 효율적인 키 합의 프로토콜을 위해 기존에 제안되었던 PIKE 프로토콜을 개선하는 방안을 살펴보았다. 전체 노드의 수가 n일 때, 기존의 PIKE 프로토콜은 각 노드가 $2(\sqrt{n}-1)$개의 키를 사전 공유하고 있어야 했으나, 개선된 프로토콜에서는 $\sqrt{n}=2km$일 때 $4m$개의 키를 사전공유한다.

[참고문헌]

[1] H. Chan and A. Perrig, PIKE: Peer Intermediaries for Key Establishment in Sensor Networks, IEEE Infocom 2005.

[2] H. Chan, A. Perrig, and D. Song, Random Key Predistribution Schemes for Sensor Networks, IEEE Symposium on Security and Privacy, 2003.

[3] L. Eschenauer and V. Gligor. A Key-management Scheme for Distributed Sensor Networks. In Proceedings of the 9th ACM Conference on Computer and Communication Security, pages 41-47, November 2002.

[4] W. Du, J. Deng, Y. Han, and P. Varshney. A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks. In Proceedings of the Tenth ACM Conference on Computer and Communications Security (CCS 2003), pages 42-51, October 2003.

[5] D. Liu and P. Ning. Establishing Pairwise Keys in Distributed Sensor Networks. In Proceedings of the Tenth ACM Conference on Computer and Communications Security (CCS 2003), pages 52 - 61, October 2003.

[6] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J. D. Tygar. SPINS: Security Protocols for Sensor Networks. In Seventh Annual International Conference on Mobile Computing and Networks (MobiCom 2001), pages 189-199, July 2001.

[7] J. Steiner, C. Neuman, and J. Schiller. Kerberos: An Authentication Service for Open Network Systems. In Usenix Winter Conference, pages 191 - 202, January 1988.