악의적 노드 탐지를 위한 Random Key Predistribution 기반의 센서 네트워크 키 관리 기법

박한*, 송주석*
*연세대학교 컴퓨터과학과
e-mail : {ipuris, jssong}@emerald.yonsei.ac.kr

Sensor Network Key Management Scheme for Detecting Malicious Node Based on Random Key Predistribution

Han Park*, JooSeok Song*
*Dept. of Computer Science, Yonsei University

요 약

센서 네트워크는 유비쿼터스 컴퓨팅에서 핵심적인 역할을 담당하는 기반 네트워크이다. 그 때문에 센서 네트워크로부터 제공되는 정보는 신뢰할 수 있어야 한다. 하지만 센서 자체의 여러 가지 한계로 인해 보안의 핵심 요소인 키 관리에는 많은 어려움이 존재한다. 이 논문에서는 Random Key Predistribution 기법에 기반하여 악의적인 노드를 탐지하지 못하는 기존의 한계점을 분석하고, 이를 해결하기 위한 새로운 키 관리 기법을 제안한다.

1. 서론

센서 네트워크에서의 키 관리는 제한된 메모리와 프로세싱 파워, 전력 등 센서의 다양한 제약사항으로 인해 연구가 어려우며, 이 때문에 다양한 키 관리 기법이 제안되어 왔다.

이 논문에서는 센서 노드의 통신 범위가 좁은 지역으로 제한된다는 점을 이용하여 가까운 범위에 존재하는 센서 노드들 간에 키 풀 매트릭스에서의 키 인덱스로부터 가중치를 얻고, 통신을 원하는 두 노드가 각각 계산한 해당 후보키의 가중치 값을 비교한다. 이를 통해 Eshenauer 와 Gligor 가 제안한 Random Key Predistribution Scheme[1]에서 노드 캡춰나 노드 복제에 의한 악의적 노드 탐지가 불가능한 보안 취약성을 개선하는 방법을 제안한다.

2. Random Key Predistribution 의 취약성 분석

2.1 기본 Scheme

Random Key Predistribution Scheme 의 Phase 는 아래와 같다.

Initialization Phase: 센서 노드가 배포되기 전에 전체 가능한 키 공간(Key Space)에서 임의의 키를 뽑아낸다. 이렇게 뽑아낸 키 풀(Key Pool) S 에 있는 키 중에서 m 개를 또다시 임의로 골라 센서 노드에 저장한다. 이렇게 저장된 키 셋을 키 링(Key Ring)이라고 한다.

Key-Setup Phase: 위의 센서가 배포되고 난 후에 실행된다. 각각의 센서는 통신 범위 내에 존재하는 또 다른 센서를 찾아 두 센서가 각각 가지고 있는 m 개의 키 링에서 공통되는 키를 찾아낸다. 이렇게 찾아낸 키는 두 노드 간의 공유키로 사용된다.

2.2 기본 Scheme 의 취약성 분석

기본 Scheme 은 다음과 같이 크게 두 가지 보안 취약성을 가진다.

첫 번째는 노드 캡춰(Node Capture)에 의한 위협이다. 작동중인 노드가 캡춰될 경우, 그 노드가 가진 키 링이 공격자에게 노출되게 되며 공격자는 그 키 링을 이용해 네트워크에 침투할 수 있게 된다. 또한 일정 수 이상의 노드가 캡춰당하면 전체 키 풀이 알려지게 되어 전체 네트워크가 위험해진다.

두 번째는 노드 복제(Node Replication)에 의한 위협이다. 똑같은 노드를 여러 개 복제 혹은 개조하여 공격자가 공격할 경우 여전히 같은 키 링을 가지게 되므로 기본 Scheme 은 이를 탐지해낼 수 없다.

위에서 지적한 두 가지 취약성은 모두 키 링이 한 번 공개되어 버리면 그 키를 악용하는 공격자를 탐지하는 것이 불가능하다는 점에서 기인한다. 전체 키 풀에서 임의의 키 링을 선택함으로써 키 링이 노출되더라도 전체 네트워크가 위협받는 상황은 피할 수 있으나, 미리 설정된 키 링만을 이용해 네트워킹을 하므로 키가 노출되었을 시의 취약성을 해결하지는 못한다.

3. 가정

제안하는 기법은 아래와 같은 가정을 전제한다.

1) 한번 배포된 노드는 그 위치가 거의 변하지 않는다.

이 논문은 2008 년도 정부(과학기술부)의 재원으로 한국과학재단의 지원을 받아 수행된 연구임(No. R01-2006-000-10614-0).

2) 공격자는 노드 캡춰 혹은 노드 복제를 통해 얻은 소수의 키 링만을 공격에 사용할 수 있다.

4. 제안하는 기법

이 기법은 센서 노드가 짧은 통신거리를 가지는 특징을 이용한다.

[그림 1]에서 볼 수 있듯이, 노드 A 가 노드 B 와 통신을 하려고 한다면 이 두 노드는 서로 지역적으로 가까운 노드이며, 각각의 노드는 그 지역에 존재하는 또다른 노드와도 동시에 통신할 수 있는 상황일 가능성이 매우 높다.

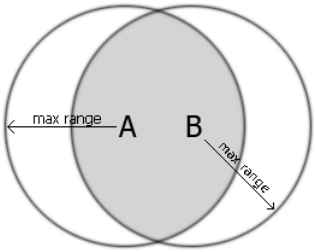

그림 1. 두 노드의 지역적 연관성

악의적인 노드를 탐지하기 위해 가중치(Weight) 라는 개념이 필요하다. [그림 1]의 노드 A 와 B 의 통신 범위에 동시에 포함되는 노드들(회색 영역에 존재하는 노드)은 네트워크의 초기 구성 시에 자신의 키 링에 포함된 키들의 인덱스를 해당 노드에 제공한다. 노드 A 와 B 는 각각 주위의 노드로부터 받은 키들의 인덱스로부터 자신이 가진 키의 가중치 w 를 계산한다. 계산 방법은 아래와 같다.

$$w(r) = \sum_{i=1}^{n} \max(k(R - d_i), 0)$$

Notation
n: 주위의 노드로부터 받은 키 인덱스의 수
R: 키 풀에서 가중치의 유효거리
k: 가중치의 변화비율을 나타내는 상수값
d_i: 주위의 노드에게 받은 키와 자신의 후보키간의 키 풀 매트릭스 상 거리

이를 그림으로 나타내면 아래와 같다.

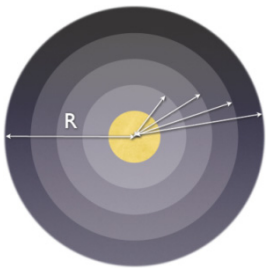

그림 2. 키 풀 매트릭스 상에서 키 인덱스에 따른 가중치와 유효거리 R

즉, A 와 B 가 가진 모든 키 링에 존재하는 키들은 그 키가 위치한 키 풀 매트릭스에서의 인덱스에 의해 가중치가 결정된다.

Random Key Predistribution Scheme 에 따라 두 노드 A 와 B 사이에는 공통의 키가 하나 이상 존재한다. 노드 B 에게 통신을 요청한 노드 A 는 그 공통의 키를 후보키로써 노드 B 에게 그 인덱스와 자신이 계산한 가중치 값을 평문 형태로 전송한다. 노드 B 는 그 인덱스에 따른 가중치 값을 자신이 계산한 가중치 값과 비교하게 되는데, 노드 A 와 B 는 지역적으로 가까운 거리에 있기 때문에 거의 비슷한 값을 가져야만 한다.

만약 노드 A 가 보낸 가중치 값이 노드 B 가 계산한 가중치 값과 차이가 클 경우, 즉 미리 설정한 Error Boundary 보다 큰 오차가 생길 경우, 이는 노드 A 가 지역적으로 멀리 떨어진 곳에서 가중치를 계산했다는 의미이고, 이는 노드 캡춰 혹은 노드 복제를 당한 악의적 노드라 판명 가능하다.

이렇게 악의적 노드를 판명한 이후에는 해당 키 인덱스를 더 이상 유효하지 않은 키로써 전체 네트워크에 브로드캐스트하여 추가적인 네트워크 피해를 막는다.

5. 결론

이 논문에서 제안하는 기법은 센서가 지역적으로 좁은 범위에서만 통신이 가능하다는 점을 이용하여 노드 캡춰 혹은 노드 복제를 통해 악의적인 목적을 가진 노드가 침입하는 것을 탐지해 낼 수 있다는 장점이 있으며, 가중치의 연산이 단순하여 센서의 낮은 프로세싱 파워나 메모리에서도 무리 없이 작동할 수 있다는 장점이 있다.

하지만 이 기법의 가장 큰 한계는 노드 추가(Node Addition)과 노드 복제로 인한 악의적 노드의 공격을 구분해 낼 방법이 모호하다는 점이다. 최초 배포 후 초기 네트워크를 구성에 참여했던 노드의 경우 네트워크와 단절되었다가 다시 연결하는 경우에 아무런 문제가 없지만, 초기 네트워크 구성에 참여하지 못했던 노드인 경우, 혹은 추후에 노드를 추가적으로 배포했을 경우에는 정상 노드를 악의적인 노드와 구분할 수 없다.

참고문헌

[1] Laurent Eschenauer and Virgil D. Gligor, “A Key-Management Scheme for Distributed Sensor Networks”, Proceedings of the 9th ACM Conference on Computer and Communication Security, pages 41-47. November 2002.

[2] Haowen Chan, Adrian Perrig, Dawn Song, “Random Key Predistribution Schemes for Sensor Networks”, IEEE Symposium on Security and Privacy, 2003.