센서네트워크의 랜덤 키 설정 기법에 관한 연구

신수연[0], 권태경
세종대학교, 정보보호 & 컴퓨터 네트워크 연구실
shinsy80@hotmail.com[0], tkwon@sejong.ac.kr

A Study on Random Key Establishment Schemes for Sensor Networks

Sooyeon Shin[0], Taekyong Kwon
Information Security & Computer Network Lab. Sejong University

요 약

센서 노드의 자원 제약성 때문에 센서네트워크에서 키 설정 하는 것은 어렵다. 특히 기존에 제안된 공개키 암호 방식 키 설정 기법은 센서 네트워크에 적용이 불가능하며 이를 해결하기 위한 대칭키 암호 방식을 이용한 키 설정 기법들이 제안되어왔다. 대칭키 암호 방식을 이용한 여러 가지 키 설정 기법 중 랜덤-키 사전분배 기법[2]과 랜덤 Pair-wise 키 사전 분배기법[1]에 대해 알아보고 문제점을 지적한다.

1. 서 론

센서 네트워크는 수십, 수천 개의 센서 노드와 수개의 Base station으로 구성되어있다. 센서 노드는 컴퓨팅 파워, 메모리 등 자원이 제약적이기 때문에 센서 네트워크에서 기존 유선 PC환경에서 사용하는 정보보호 서비스를 제공하는 것은 어려운 일이다. 정보보호 서비스에서 우선적으로 고려해야 할 사항은 암호 키를 설정하는 것이다. 지난 수십 년 동안 다양한 키 관리 프로토콜이 제안되었지만 센서 노드의 자원 제약성 때문에 기존 유선 PC 환경에서 사용하던 공개키 암호 방식의 키 관리 프로토콜이 적용 될 수는 없었다. 지금까지의 연구 결과 중 이 문제에 대한 해결책으로 모든 센서 노드가 단일 암호 키를 사용하는 것, 랜덤-키 사전 분배, Pair-wise 키와 랜덤 Pair-wise 키 사용 등이 있다. 공개키 암호 방식에 반해 센서네트워크에 적용이 가능하고 안전성도 증가시켰지만 이 프로토콜들 또한 문제점을 가지고 있다. 본 논문에서는 이들에 대하여 비교하고 각각의 문제점에 대해 알아본다.

2. 관련 연구

지난 수십 년간 다양한 효율적인 키 관리 프로토콜이 제안되었지만 이들의 대부분은 공개키 암호 방식을 사용한다. 공개키 암호 방식은 연산 량이 많아 배터리를 사용하고 메모리가 적은 센서 노드에 적용하기에는 적합하지 않다. 이에 대한 해결책은 대칭키 암호 방식을 사용하는 것이다. 대칭키 암호 방식을 사용한 가장 기본적인 프로토콜은 센서네트워크를 구성하고 있는 모든 센서 노드가 단일키를 사용하는 것이었다. 그러나 하나의 노드로부터 단일키가 노출이 될 경우 센서 네트워크 전체의 정보를 노출시키는 문제가 있다. Pair-wise 키를 사용하여 이 문제를 해결하였지만 각각의 노드가 $n-1$개의 키를 메모리에 저장하고 있어야 하므로 자원제약이 많은 센서 노드에겐 적합하지 않고 전체적으로 $n*(n-1)/2$개의 키가 필요하므로 확장성이 떨어진다. 이 외에도 센서네트워크에 공개키 암호 방식을 적용했을 때의 문제점과 단일키를 사용했을 때의 문제점을 해결한 연구들로는 Laurent Eschenauer와 Virgil D. Gligor가 제안한 랜덤-키 사전 분배[2]와 이를 보안시킨 Haowen Chan, Adrian Perrig와 Dawn Song가 제안한 랜덤 Pair-wise 키 사전분배가 있다.

3. 센서네트워크의 랜덤 키 설정 기법

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

센서네트워크 키 설정을 위한 대표적인 프로토콜로는 랜덤-키 사전분배 프로토콜과 랜덤 Pair-wise 키 사전분배 프로토콜이 있다. 이 프로토콜들은 랜덤 그래프 $G(n,p)$을 기반으로 한다. 여기서 n은 센서 네트워크를 구성하는 노드의 수이고, p은 어떤 두 노드 사이에 링크가 존재할 확률을 의미한다. 만약 $p=0$인 경우는 랜덤 그래프에서는 연결된 것이 하나도 없음을 의미하고, 센서 네트워크에서는 연결된 노드가 하나도 없음을 의미한다. 만약 $p=1$인 경우는 랜덤 그래프 전체가 연결되었음을 의미한다. Erdős와 Rényi[3]는 monotone 속성에 관하여 매우 큰 랜덤 그래프에서 속성이 "nonexistenct"에서 "certainly true"로 이동하는 p의 값이 존재함을 보였다. Eschenauer와 Gligor[1]은 네트워크 사이즈 n에서 키 설정 동안 노드가 확립할 안전한 링크의 수 d를 계산했다.

$$d=\left(\frac{n-1}{n}\right)(\ln(n)-\ln(-\ln(c)))$$

키 설정 동안 노드가 확립할 안전한 링크의 수가 적어도 d일 때, 어떤 노드가 성공적으로 키 설정으로 할 확률 p 즉, 어떤 두 노드 사이에 링크가 존재할 확률은 다음과 같다.

$p=\frac{d}{n'}$. (n': 노드의 통신 범위 내에 존재하는 인접한 노드의 기대 값)

3.1 랜덤-키 사전 분배

랜덤-키 사전분배(Random-key Predistribution)는 단일키를 사용한 키 설정과 Pair-wise 키를 사용한 키 설정 방법의 문제점을 보안하기 위해 제안되었다. 랜덤-키 사전분배 프로토콜은 초기화와 키 설정 두 부분으로 구성되어있다.

3.1.1 초기화

센서 노드가 배치되기 전의 과정으로 모든 가능한 키들의 공간에서 매우 큰 대칭키 풀을 랜덤하게 선택하고 여기서 일정한 개수의 키를 랜덤하게 선택하여 각 센서 노드의 키 링에 저장한다. 대칭키 풀에 있는 모든 키는 유일한 ID를 가지며 키와 함께 키에 대한 ID도 노드의 키 링에 저장된다. 그림 1은 초기화 과정을 보여준다.

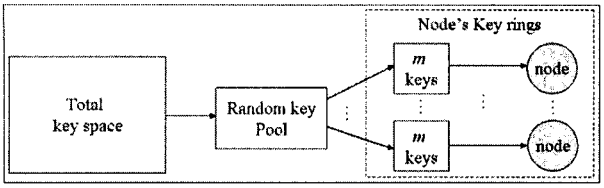

그림 2. 초기화 과정

3.1.2 키 설정

센서 노드들이 배치된 후 키 설정 과정이 수행된다. 각각의 센서 노드는 자신의 키 링에 있는 키의 ID를 브로드캐스트 한다. 인접한 노드는 브로드캐스트 된 ID와 자신의 키 링의 ID와 비교하여 상대방과 같은 공통키를 소유하고 있는지 판단한다. 만약 동일한 키가 자신의 키 링에 있다면 Challenge Response 프로토콜을 통해 세션 키를 설정한다. 만약 키 링에 공통키가 없다면 세션 키를 설정한 인접 노드를 통하여 경로키를 설정한다. 예를 들어, 그림 2의 경우 노드 B와 노드 C는 공통키를 가지고 있지 않아 노드 A를 이용하여 경로키를 설정한다.

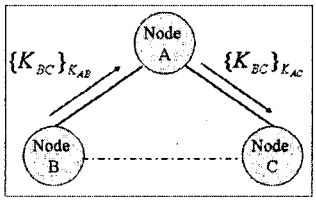

그림 3. 경로키 설정 과정

3.2 랜덤 Pair-wise 키 사전 분배

Haowen Chan, Adrian Perrig와 Dawn Song은 랜덤 키 사전분배의 결점을 보안하기 위해 q-합성수 랜덤 키 사전분배 스킴과 multipath 키 강화 스킴을 제안하였다. 더 나아가 노드 간 상호인증을 제공하고 안전성도 강화시킨 랜덤 Pair-wise 키 사전분배 스킴을 제안하였다[1].

3.2.1 q-합성수 랜덤 키 사전분배 스킴

q-합성수 랜덤 키 사전분배 스킴은 3.1의 랜덤 키 사전분배 프로토콜의 결점을 보안하기 위해 제안된 스킴으로 공통키를 하나 이상인 q개를 사용한다는 점 외에는 랜덤 키 사전분배 프로토콜과 동일하다. 노드는 인접한 노드의 브로드캐스트를 통해 q개의 공통키를 찾은 다음 그 q개의 키를 이용하여 새로운 세션 키 $K=hash(k_1||k_2||\ldots||k_q)$를 생성한다.

3.2.2 Multipath 키 강화 스킴

Multipath 키 강화 스킴 또한 랜덤 키 사전분배 프로토콜의 결점을 보안하기 위해 제안되었다. 노드는 기본적인 세션 키 설정 후 독립적인 경로를 통하여 세션 키를 강화한다. 그림 3에서 노드 B와 노드 C는 세션 키 K_{BC}를 강화하기 위하여 독립적인 두 경로, 노드 A를 통한 경로와 노드 D를 통한 경로를 이용한다. 노드 B는 키와 같은 길이를 갖는 ν_1과 ν_2을 랜덤하게 선택한 다음 독립적인 두 경로를 통해 노드 C에게 보낸다. 노드 C는 두 랜덤한 값을 받은 후 새로운 세션 키 $k' = k \oplus \nu_1 \oplus \nu_2 \oplus \ldots \oplus \nu_j$ (j: 독립적인 경로의 수)가 생성된다.

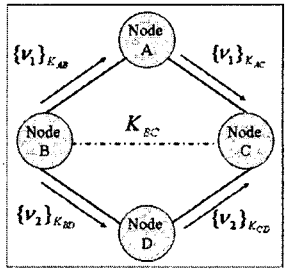

그림 4. Multipath 키 강화

3.2.4 랜덤 Pair-wise 키 스킴

랜덤 Pair-wise 키 스킴은 Pair-wise 스킴의 단점을 보안한다. 노드 간 상호 인증, 노드 캡쳐에 대한 완벽한 회복력을 가지고, base station 없이도 손상된 노드를 감지하여 취소할 수 있는 기능 등 센서네트워크에서 중요한 정보보호 서비스를 제공한다. 랜덤 Pair-wise 키 스킴은 배치되기 전의 초기화 과정과 배치된 후의 키 설정 과정으로 나뉜다. 초기화 과정은 센서 네트워크를 구성하는 센서 노드의 수가 n이라고 할 때, n개의 유일한 노드 ID를 생성하고, 각각의 노드는 랜덤하게 선택한 m개의 노드 ID를 갖는다. 생성된 각각의 노드 쌍에 대해서 Pair-wise 키를 생성하고 각각의 노드 키 링에 저장한다. 키 설정 과정은 우선 각각의 노드가 자신의 ID를 인접한 노드들에게 브로드캐스트 하고, 이 브로드캐스트를 통해 인접한 노드들은 자신의 키 링과 비교하여 같은 ID를 찾아낸다. 같은 ID를 가진 경우에는 cryptographic handshake를 통해 공통의 Pair-wise 키를 가지게 된다. 일치하는 ID가 없을 경우에는 링크를 생성하지 못한다.

4. 센서네트워크의 랜덤 키 설정 기법의 문제점

3장에서 설명한 프로토콜들은 센서 노드에 공개키 암호 방식을 적용하지 못하는 문제를 해결하고 단일키 사용 시의 문제점과 Pair-wise 키를 사용할 경우의 문제점도 해결하였다. 본 장에서는 랜덤-키 사전분배 프로토콜과 랜덤 Pair-wise 키 사전분배 프로토콜의 3가지 스킴의 장점과 단점을 비교하고 문제점을 지적한다.

4.1 랜덤-키 사전분배의 문제점

랜덤-키 사전분배는 키 풀에서 랜덤하게 m개의 키를 선택함으로 두 노드가 공통키로 사용하려는 키를 인접한 다른 노드가 가지고 있을 가능성이 있으므로 이 키를 이용하여 두 노드 사이의 트래픽을 도청할 수 있다. 예를 들어, 그림 2의 노드 A와 노드 B가 공통으로 사용하려는 키가 노드 C의 키 링에도 저장되어있다면 노드 C가 공격자에게 캡쳐 당했을 경우 공격자는 두 노드 A와 B 사이의 트래픽을 도청하여 정보를 얻어 낼 수 있다. 만약 키 풀의 크기가 작을 경우 하나의 키가 여러 노드의 키 링에 저장되어있을 가능성은 더 높아지고 공격자가 한 노드를 공격했을 경우 센서 네트워크 전체 중 큰 부분을 손상 시킬 수 있다.

4.2 랜덤 Pair-wise 키 사전분배의 문제점

랜덤 Pair-wise 키 사전분배의 q-합성수 랜덤 키 사전분배 스킴은 비록 랜덤-키 사전분배 프로토콜보다 안전성은 강화되었지만, 여전히 문제점을 가지고 있고 Multipath 키 강화 스킴과 랜덤 Pair-wise 키 스킴은 security은 증가하였지만 또 다른 문제점을 가지고 있다.

4.2.1 q-합성수 랜덤 키 사전분배 스킴의 문제점

랜덤-키 사전분배 프로토콜과 같이 인접한 노드의 키 링에 어떤 두 노드 사이의 q개의 키가 모두 저장되어 있다면 노드가 캡쳐 당

했을 경우 두 노드 사이의 트래픽은 안전하지 못하게 된다. 다른 한 가지 문제는 만약 어떤 두 노드가 인접해 있더라도 공통으로 가지는 키의 개수가 q이하라면 두 노드 사이의 링크는 생성되지 못한다.

4.2.2 Multipath 키 강화 스킴의 문제점

랜덤-키 사전분배 프로토콜의 문제점을 해결 할 수 는 있지만 독립적인 경로를 찾기 위한 오버헤드가 생기고 경로에 있는 중간 노드들을 전적으로 신뢰해야만 한다. 만약 경로들 중 어느 하나만 공격자에 의해 손상되면 키의 일부가 손상되는 것과 같다. 예를 들어, 그림 3의 경우 만약 노드 A, 노드 D 혹은 노드 A와 D가 공격자에 의해 캡쳐 당한다면 노드 B와 노드 C의 키와 트래픽은 안전하지 않다.

4.2.3 랜덤 Pair-wise 키 스킴의 문제점

랜덤 Pair-wise 키 스킴은 센서 네트워크에서 중요한 정보보호 서비스를 제공하지만 문제점이 있다. 만약 어떤 노드의 키 링에 인접한 노드와의 Pair-wise 키가 저장되어 있지 않은 경우에 랜덤-키 사전분배 프로토콜의 경로 키 설정이 불가능하므로 두 노드는 링크를 생성 할 수 없다. 경로키를 설정이 불가능하므로 만약 새로운 노드의 키 링에 인접한 노드와의 Pair-wise 키가 저장되어 있는 경우는 이를 이용하여 인접한 노드와 링크를 생성할 수 있지만 그렇지 못한 경우 새로운 노드를 추가하는 것이 불가능하게 된다. 비록 이 스킴에서는 전체 센서 네트워크의 연결성을 증가시키기 위해 범위 확장을 시도 하지만 이는 공격자들에게 DOS (Denial of Service) 공격을 시도할 수 있게 해주고 범위 확장은 오버헤드를 증가 시킨다.

4.3 키 사전분배 프로토콜의 비교

다음의 표 1은 프로토콜의 장점과 단점을 비교해 놓은 것이다. 이 중 Base station 없이 안전성 제공이 가능하다는 것은 센서 네트워크의 정보보호 서비스에서 중요한 부분이다. Base station은 센서 노드에 비해 컴퓨팅 파워와 메모리 등이 강력하고 외부와 연결시켜주는 게이트웨이 역할도 담당하며 센서 노드들이 자원 제약성 때문에 하지 못하는 일도 할 수 있다. 센서 네트워크에서 Base station은 하나 이상 존재 할 수 있으며 센서 노드는 전적으로 Base station을 신뢰한다. 하지만 Base station이 공격자에 의해 손상되면 센서 네트워크 전체가 손상되므로 큰 문제를 가지고 있다. 표 2에서는 키 사전분배 프로토콜을 하나의 노드가 가져야 하는 키의 개수와 노드에게 필요한 메모리의 크기를 통해 비교해 보았다. 표 2의 n은 센서 네트워크를 구성하는 센서 노드의 수, x는 키 하나의 사이즈, m은 노드의 키 링에 저장되어 있는 키의 수 ($m \ll n$), $path$는 키 설정이후 경로키의 수, d는 인접한 노드와 생성한 링크의 수이고 ran은 Multiple 경로 키 강화 스킴을 위해 랜덤한 값을 저장할 메모리의 크기를 나타낸다. 랜덤 Pair-wise 키 Erdős와 Rényi[3]는 전체 그래프가 높은 확률로 연결되는 가장 작은 p를 계산 가능하게 했다. 네트워크의 크기가 n일 때, 이 확률 p를 얻기 위해서 각각의 노드는 np개의 Pair-wise 키만 키 링에 저장하면 된다.

5. 결론

센서네트워크는 자원제약이 큰 센서 노드로 이루어져 있어 대칭키 암호 방식을 사용한 다양한 키 설정 기법이 제안되었다. 본 논문에서는 그 중 대표적인 4가지의 키 설정 기법에 대하여 연구하고 장점, 단점과 문제점에 대하여 알아보았다. 기법이 발전함에 따라 안전성은 증가 하였으나 여전히 문제점이 남아있고 후에 이 문제를 해결해 보고자 한다.

표 1. 키 사전분배 프로토콜의 장점과 단점
(BS: Base station)

	장점	단점
단일키	단일키 하나만 저장하면 됨.	단일키 깨지면 전체 네트워크 깨짐.
Pair-wise 키	BS 없이 안전성 제공, 노드 간 상호인증 제공.	센서 노드의 자원에 비해 너무 많은 키를 저장해야함.
랜덤-키 사전분배	인접한 노드와 링크 생성 가능.	어떤 두 노드 사이의 키를 다른 인접한 노드가 가질 수 있음.
q-합성수 랜덤 키 사전분배	랜덤-키 사전분배 프로토콜에 비해 안전성 증가, 적은 수의 노드가 캡쳐 당했을 경우 전체 네트워크에 미치는 영향 작음.	랜덤-키 사전분배 프로토콜과 같은 문제 가짐, 인접한 노드이더라도 q를 만족하지 못하면 링크 생성하지 못함.
Multipath 키 강화 스킴	랜덤-키 사전분배 문제 해결.	경로 찾기 위한 오버헤드, 중간노드 신뢰가 전제조건.
랜덤 Pair-wise 키 스킴	BS 없이 안전성 제공, 노드 간 상호인증 제공.	인접한 노드와의 Pair-wise 키가 키 링에 없을 경우 링크 생성 불가능, 인접한 노드와 Pair-wise 키가 없는 새로운 노드 추가 불가능.

표 2. 키 사전분배 프로토콜 비교

	키의 개수	메모리 크기
단일키	1	x
Pair-wise 키	$n-1$	$(n-1)\times x$
랜덤-키 사전분배	m	$(m+path)\times x$
q-합성수 랜덤 키 사전분배	m	$(m+path+d)\times x$
Multipath 키 강화 스킴	m	$(m+path+d)\times x+ran$
랜덤 Pair-wise 키 스킴	$m=np$	$m\times x$

참고 문헌

[1] H. Chan, A. Perrig and D. Song, "Random Key Predistribution Schemes for Sensor Networks," In Proceedings of the 2003 IEEE Symposium on F and Privacy, pages 197-215, May 2003

[2] L. Eschenauer and Virgil D. 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.

[3] J. Spencer, "The Strange Logic of Random Graphs," Algorithms and Combinatorics 22, Springer-Verlag 2000, ISBN 3-540-41654-4.