무선 센서 네트워크를 위한 계층적인 사전 키 분배 방법

김복순[0] 조기환 이행곤[1]
전북대학교 전자정보공학부, 한국과학기술정보연구원[1]
{buskim[0], ghcho}@dcs.chonbuk.ac.kr, hglee@kisti.re.kr[1]

A hierarchical key pre-distribution scheme for wireless sensor network

Bogsoon Kim[0], Gihwan Cho, Haenggon Lee[1]
Div. of Electronics Information, Chonbuk National University
Korea Institute of Science and Technology Information[1]

요 약

무선 센서 네트워크(WSN: Wireless Sensor Network) 환경에서 보안성을 확보하기 위하여, 센서 노드 간에 전송된 메시지를 암호화하고 인증하는 것이 중요하다. 암호화와 인증을 위해 사용되는 키는 통신 노드 사이에 합의되어야 한다. 그러나 자원의 제약성 때문에, 일반적인 네트워크에서 많이 사용되는 Diffie-Hellman이나 공개키 기반 키 협의 방법은 WSN 환경에 적합하지 않다. 많은 노드에 비밀키를 사전에 정적으로 분배하는 것은 대용량의 메모리와 계산 능력을 요구하고, 네트워크 환경이 커짐에 따라 이들의 요구량이 급증하기 때문이다. 따라서 이러한 사전키 분배 문제를 해결하기 위하여, 본 논문은 계층적인 사전 키 분배 방법을 제시한다. 제안된 방법은 기존 방법론과 비교하여 센서 노드간의 공유키가 존재할 가능성을 증가시켜, 통신 채널을 쉽게 형성할 수 있도록 하였다. 또한 외부 공격자의 위협에 대비하여 q-composite 이론을 적용하여, 보안성을 강화시켰다.

1. 서론

컴퓨터 기술과 통신의 최근 발전은 무선 센서 네트워크(WSN: Wireless Sensor Network)의 확대를 용이하게 하였다. 센서 네트워크는 대규모의 초소형 장치로 구성된 환경으로, 각 장치는 센서 노드로 불린다. 이들 센서 노드는 주로 밧데리로 전력을 공급받고, 통합 센서 장치로 구성되었으며, 데이터 처리 능력과 단거리 무선 통신이 가능하다. 예를 들면, SmartDust와 WINS가 센서 네트워크를 적용한 예이다[2].

WSN의 응용 분야는 군대 센싱과 추적, 환경 모니터링, 환자 감시 그리고 스마트 환경이다. 이중 센서 노드가 위험 지역에 설치된 경우, 보안성은 매주 중요하다. 예를 들면, 공격자는 쉽게 트래픽을 엿들을 수 있고, 주변 노드에게 잘못된 정보를 제공함으로써 네트워크 센서 노드로 흉내 낼 수도 있다. 그러므로 WSN에 보안성을 제공하려면, 통신이 암호화되고 인증되어야 한다. 이러한 문제는 센서 노드 간의 안정적인 통신을 위하여, 비밀키를 설정하도록 함으로써 해결가능하다[4].

이를 위하여 일반적으로 네트워크에서는 키 관리 방법에 대한 다양한 연구가 진행되어 왔다. 첫째, 신뢰된 인증 서버에 의하여 키를 분배받는 방법으로, 이는 센서 네트워크와 같이 구조적인 기반 구조가 없는 환경에서는 적용이 어렵다. 둘째, 공개키 인증서를 활용한 비대칭 암호화 방법으로, 한정된 계산력과 에너지로 구성된 센서 노드에서 Diffie-Hellman이나 RSA 방법을 적용하는 것은 바람직하지 않다. 마지막으로 사전 키 분배 방식은 센서 노드를 배치하기 전에 키 정보를 미리 저장하는 것으로, 모든 정보가 사전에 결정되어야 한다. 그러나 센서 노드의 설치는 임의적으로 이루어지므로, 이러한 많은 사전 지식을 보유하는 것은 어렵다. 따라서 본 논문은 WSN 환경에서 오프라인과 온라인을 이용한 계층적인 사전 키 분배 방법을 제안한다. 본 방법론은 과거의 랜덤 키 분배 방법론이나 확률적인 키 분배 방법론보다 계층적인 단계 적용을 통하여 키를 분배함으로써, 공유키의 존재 가능성을 좀더 높였다. 또한 공유키를 발견하고, 키 협의를 맺는 방법까지 제안함으로써, 완전한 센서 네트워크의 키 관리 방법을 제시한다. 이는 센서 노드간의 공유키의 존재 가능성을 높임으로써 고립된 노드의 수를 줄여 더 많은 정보를 획득 할 수 있도록 한다. 또한 q-composite 이론을 이용하여 필요한 키의 기준치를 통신 채널 설정의 파라미터로 사용함으로써, 보안성을 좀더 강화시켰다.

본 논문의 구성은 다음과 같다. 2절에서 센서 네트워크에서 키 분배를 위하여 지금까지 수행된 연구들을 살펴보고, 3장에서는 계층적인 키 분배 방법에 대한 개요와 통신 프로토콜을 살펴본다. 마지막으로 4장에서는 결론 및 고찰, 향후 과제를 제시하였다.

2. 관련 연구

최근 WSN을 위한 키 분배는 크게 기반 시스템을 활용하거나 사전 분배 방식을 고려하여 왔다.

2.1 제한된 센서 네트워크 환경을 위한 서브시스템 활용

서브 시스템간의 통신을 위하여 게이트웨이 역할을 하는 BS(Base Station)을 가정함으로써 키 분배와 키 관리가 용이한 WSN을 구현하는 것이다. BS는 워크스테이션과 유사한 성능을 갖는 신뢰된 센서 노드로서, 보안에 좀더 강한 환경을 구성할 수 있다. 또한 중앙의 BS가 시스템 전체를 통제함으로써, 서브시스템은 인증되고 기밀성있는 통신뿐만 아니라, 인증된 브로드캐스팅을 지원할 수 있다. [3,7]의 키 관리 방법은 정기적으로 대칭키를 갱신함으로써 키 관리가 가능하도록 하였다. 그러나 키 분배 전후의 비밀성이 보장되지 않는 단점이 있다. 또한

실제로 강력한 기능을 가진 BS가 존재하기도 어렵고, 대규모의 센서 네트워크 환경을 통제하는 것은 불가능하다. 따라서 본 논문에서는 BS의 역할을 줄이면서, 전체 센서 네트워크를 통제할 수 있는 방법론을 제안한다.

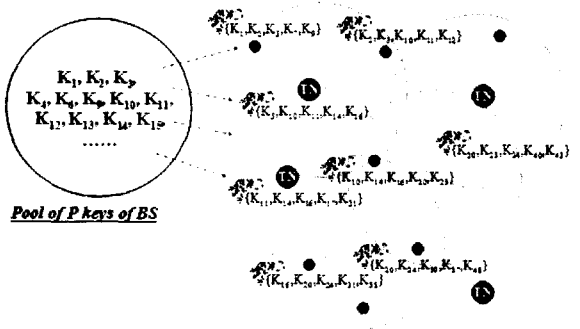
2.2 확률적인 키 분배[1,2,5]

확률적인 키 분배 방법과 랜덤 키 사전 분배 방법은 설치 전에, 각 센서 노드가 대규모 키 풀로부터 부분 키 집합을 받는 것이다. 센서 노드들이 통신을 하기 위하여, 임의의 두 노드는 그들의 키 집합 내에서 공통키를 찾고, 노드간 통신을 위한 공유키로 사용한다. 이들 방법에 q-composite 랜덤 키 사전 분배 방법을 적용하여 키 셋업에 대한 보안성을 강화한 방법론이 있다[2]. 그러나 이는 센서 네트워크 특성을 고려하지 않고, 확률적으로 랜덤하게 키를 분배하므로, 센서 노드간의 공유키가 존재하지 않을 가능성이 매우 높다. 또한 공유키가 존재하더라도, 공유키를 발견하는데 소용되는 시간과 에너지가 많아 에너지 효율적이지가 못하다. 이에 따라, 본 논문에서는 설치된 센서 노드들 사이에 공유하는 키가 가능한 많아지도록 하는 본 방법론을 제시한다.

3. 계층적인 키 분배 방법

3.1 시스템 구성 요소와 가정

계층적인 키 분배 방법인 적용되는 WSN는 크게 3가지 요소인, BS, TN(Target Node), SN(Sensor Node)로 구성되어 있다. BS는 모든 정보를 수집하여, 전달하는 게이트웨이 역할을 하는 것으로서 모든 부분 키 풀을 생성하여, TN에게 전달한다. TN은 BS로부터 전달받는 부분 키 풀을 이용하여 주변 영역에 존재하는 SN에게 임의적으로 키 체인을 생성하여 키를 분배한다. SN은 TN으로 받은 키 체인을 이용하여 주변 노드와 공유키를 발견하고, 경로를 설정한다.



[그림 1] 센서 네트워크 구성 환경

이와 같이 구성 요소간의 키를 분배하고 통신을 하기 위한 가정은 다음과 같다. 첫째, 센서들은 RF(Radio Frequencies)를 이용하여 통신하므로, 브로드캐스팅은 기본적인 통신 요소이다. 둘째, 각 센서들은 통신 범위 안에 존재하는 한정된 센서 노드들과 통신을 할 수 있고, 패킷은 멀티 홉을 거쳐서 목적지에 전달될 수 있다. 셋째, TN에게 제공하는 부분 키 풀은 오프라인으로 미리 설치한다. 넷째, TN의 통신 범위를 벗어나는 센서 노드간의 통신은 반드시 TN을 거쳐 이루어진다. 다섯째, 센서 네트워크는 ad-hoc만큼은 이동성이 크지 않으며, 한번 인증 받은 노드는 악의적인 공격을 하지 않는다. 여섯째, 통신 보안을 강화하기 위하여 BS는 대규모의 키 풀을 생성할 수 있고, 보유할 수 있다. 일곱째, BS는 각 TN을 제어하는 공유키 K_{BS_TN1}(TN 노드번호)와 TN이 통신 범위내의 센서 노드를 제어하는 공유키 K_{TN1_SN1}(SN 노드번호)가 존재한다. 각 SN은 자신이 어느 TN 그룹에 속하는지 알고 있다.

3.2 제안 방법론

3.2.1 BS의 키 풀 생성과 분배

TN이 설치될 위치를 정확하게 알고 있는 BS는 P개의 키 풀을 순서대로 생성한다. 이를 키를 k개씩 임의로 선택하여 각 노드에게 전송한다. 이때 두 노드 간에 공유키가 존재할 확률 Pr[E]는

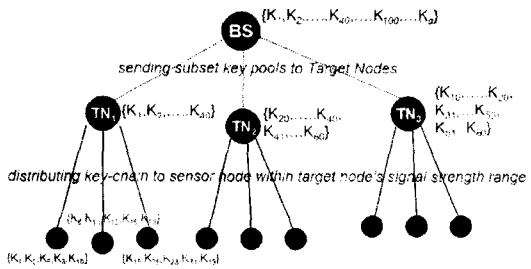
$$Pr[E] = 1 - Pr[\overline{E}] = 1 - \frac{(P-k)}{\binom{P}{k}}$$

이다. 그러나 각 노드가 공유키를 가질 확률이 키 풀의 크기가 커질수록 매우 작아지므로, TN이 설치될 위치와 RF의 범위에 따라 부분 키 풀을 TN에게 배분한다. 이때 TN이 받는 부분 키 풀은 BS가 소유한 전체 키 풀의 수보다는 작다. 즉 하나의 TN이 소유한 부분 키 풀의 크기를 P'하면, TN을 중심으로 센서 노드간의 공유키가 존재할 확률 Pr[E']는

$$Pr[E'] = 1 - Pr[\overline{E'}] = 1 - \frac{(P'-k)}{\binom{P'}{k}}$$

이다. 이때 확률 Pr[E']는 Pr[E]보다 크다($P' \le P$). 이는 좀더 작은 키 풀에서 동일한 수의 키 체인을 생성하는 것이 공유키의 존재 가능성을 높이기 때문이다.

[그림 2]는 BS가 생성한 전체 키 풀에서 부분 키 풀이 각 TN노드에 분배되고, TN이 무작위로 키 체인을 생성하여 TN의 통신 범위에 있는 센서 노드에 키를 분배하는 과정을 보여준다.

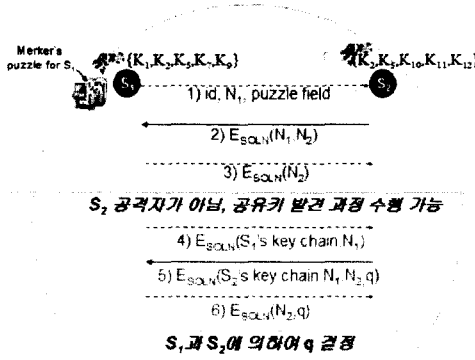


[그림 2] 계층적인 키 생성과 분배 과정

TN이 생성한 키 체인은 K_{TN1_SN1}{Key_chain}을 통하여 각 SN에 전달된다. 예를 들어, TN1이 SN1에게 제공하는 키 체인을 Key_chain_1이라하면, TN_1은 SN_1과 통신을 위한 비밀키 K_{TN1_SN1}으로 Key_chain_1을 암호화하여 전송한다{$K_{TN1\_SN1}(Key\_chain_1)$}. 이때 SN_1에게 전달된 Key_chain_1은 TN_1의 부분 키 풀에서 확률적으로 생성한 키의 집합이다. 전체 키 풀에서(P)에서 부분 키 풀을 생성하고(P'), 부분 키 풀에서 확률적으로 추출한 키 체인을 만들어 SN에 전달하므로, SN은 좀더 작은 키 풀의 키 체인을 받게 된다. 이는 각 노드간의 공유키의 존재 가능성을 높인다.

3.2.2 상호 인증을 통한 공유키 발견 과정

TN으로 수신한 키 체인을 이용하여 각 센서 노드는 공유키 발견을 시도한다. [그림 3]은 공유키 발견 과정을 단계별로 나타내낸다. 공유키를 발견하기 전에, 통신을 수행할 수 있는 노드임을 확인하기 위하여 S_1노드는 S_2에게 id, N_1, puzzle field[6]를 전송한다. 이를 수신한 S_2는 puzzle field에서 임의의 문제를 선택하여 해답을 얻으면{E_{SOLN}}, S_1이 보낸 N_1과 S_2의 N_2를 E_{SOLN}로 암호화하여 S1에 전송한다{$E_{SOLN}(N_1,N_2)$}. S_1은 S_2가 전송한 솔루션을 자신의 puzzle field에서 찾아, $E_{SOLN}(N_1,N_2)$을 복호화하고 S_1이 보낸 N_1값을 확인한다. 그리고 S_2에게 N_2를 E_{SOLN}으로 암호화하여 보낸다{$E_{SOLN}(N_2)$}. 이로써 키 체인의 공유키를 발견하기 이전에 두 노드간의 통신 채널 보안키로 E_{SOLN}을 사용함으로써, 노드를 상호 인증하였다. 상호 인증 후, S_1과 S_2는 자신의 키 체인을 E_{SOLN}으로 암호화하여 전송한다. 이때 S1의 키 체인을 수신한 S_2는 공유키의 숫자를 계산하여(q), $E_{SOLN}(S_2$'s key_chain,N_1,N_2,q)로 암호화하여 S_1에게 전송한다. S_1도 S_2의 키 체인을 전송 내용을 확인하여 q값을 확인한다. 이때 상호 확인하는 q값은 두 노드가 최소한 공유해야하는 키의 숫자로서, q의 값이 TN이 지정하는 기대치보다 작으면 통신 채널을 생성할 수 없다. 그러므로 계산된 q'는 항상 q'≥q이어야 한다.



[그림 3] 상호 인증과 공유키 발견 프로토콜

하나의 TN 범위 내에서 서로 겹치는 공유키의 수를 q, 키 체인의 키의 수를 k, 두개의 노드가 적어도 q개의 키를 공유할 확률을 |P'|, 두 개의 노드가 적어도 i개의 키를 공통으로 가질 확률을 P(i)는

$$P'(i)=\frac{\binom{|P|}{i}\binom{|P|-i}{2(k-i)}\binom{2(k-i)}{k-i}}{\binom{|P|}{i}^2}$$

이다. 또한 두 개의 노드가 충분한 키를 공유할 확률은 $P'_{connect}=1-(P(0)+P(2)+\cdots+P(q-1))$이다. $|P'|<|P|$이므로, $P'_{connect}$의 확률 계산 결과는 TN의 영역 구분 없이 키를 분배한 경우보다 더 높다. 따라서 고립된 노드의 숫자를 줄일 수고, 각 노드의 정보를 더 많이 수집 가능하다.

3.2.3 키 철회와 갱신

SN이 위험상태에 빠지거나 악의적인 노드가 특정키를 도용하고 있는 경우 노드의 키를 철회하는 것은 매우 중요하다. 키를 철회하기 위하여 TN은 범위 내의 SN에게 메시지를 보내어, 공유키 사용을 제한한다. 이러한 메시지를 받은 SN은 키 체인을 확인하여 키를 철회하고, 키 정에 키가 사용되는 경우는 키 협정을 취소한다. 키 협정이 취소된 노드는 과거에 얻은 공유키 정보의 사용 가능 여부를 이웃 노드에게 확인하여 키 협정을 다시 맺는다. 만약 공유키가 존재하지 않는 경우에는 공유 키 발견 단계부터 다시 시작한다.

노드의 존재하는 키의 라이프타임이 만료되면 키 갱신은 반드시 일어나야만 한다. 만약 키 갱신이 이루어지지 않으면, 타임아웃에 의한 비가용 키의 숫자가 점차 증가하여 키 협정이 어렵거나 불가능할 수 있다. 또한 TN이 지정하는 q의 지정 값을 얻지 못하여, 통신 채널 형성이 이루어지지 않는다. 그러므로 TN이 각 노드에 분배한 키 체인의 사용 가능한 키의 수가 특정 기준 이하로 감소하면, 다시 키 체인을 할당받도록 한다. 이는 고립된 노드의 존재를 막고, 악의적인 노드가 지속적으로 키 협정 관계를 유지하는 것을 예방한다.

4. 결론

본 논문에서는 무선 센서 네트워크 환경에서 키 분배 방법을 제안하였다. 전체 네트워크 환경에 분배되는 확률적이면서도 임의적인 방법론과 비교하여, 계층적으로 키 분배를 구성하였고, 수학적으로 본 제안 방법론이 공유키가 존재할 가능성이 더 높음을 증명하였다. 또한 가벼운 quiz field를 이용한 노드간의 상호 인증을 통하여, 공격자에게 모든 키 정보가 노출될 가능성을 줄였으며, q-composite에 의한 공유키의 숫자에 제한을 둠으로써 외부 공격자의 용이한 공격이 어렵게 하였다.

향후 연구 과제로는 TN의 통신 범위가 불규칙한 경우의 키 관리 방안과 이러한 환경에서 악의적인 노드를 탐지하는 방법을 찾는 것이 있다.

[참고 문헌]

[1] L. Echenauer and V. D. Gligor. "A Key-Management scheme for Distributed sensor networks," *In Proceedings of the 9th Computer Communication Security*, Nov. 2002, pp.41-47.

[2] H. Chan, A. Perrig, and D. Song. "Random key predistribution schemes for Sensor networks," *In IEEE Symposium on Research in Security and Privacy*, May. 2003, pp.197-213

[3] S. Basagni, K. Herrin, D. Bruschi, and E. Rosti. "Secure pebblenets," *In Proceedings of the 2001 ACM International Symposium on Mobile ad hoc networking & computing*, ACM Press, 2001, pp. 156-163.

[4] D. W. Carman, P. S. Kruus, and B. J. Matt. "Constraint and approaches for distributed sensor network security," *Technical Report#00-010, NAI Labs*, 2000.

[5] S. Zhu, S. Setia, and S. Jajodia, "A distributed group key management protocol for ad hoc networks," *Unpublished manuscript*, George Mason University, Dec. 2002.

[6] C.J. Mitchell, "Public key encryption using block ciphers," *Technical Report, RUUL-MA-2003-6*, London University, Sept. 2003.

[7] 김복순, 조기환, 이행곤, 박병연, "센서 네트워크에서 랜덤 키 체인을 활용한 단대단 키 협의 방안," 한국통신학회 추계종합학술발표논문집, 28, 2003. pp. 1-12