情報保護學會論文誌
第16卷 第2號, 2006. 4

소모형 센서 네트워크 환경에 적합한 키 관리 스킴*

김 용 호†, 이 화 성, 이 동 훈‡
고려대학교 정보보호 대학원

A Key Management Scheme for Commodity Sensor Networks*

Young Ho Kim†, Hwa Seong Lee, Dong Hoon Lee‡
Graduate School of Information Security, Korea University

요 약

신뢰할 수 있는 무선 센서 네트워크 통신을 위해, 무선 센서 노드들 사이의 보안 키들은 안전하게 설립되어야 한다. 최근에, Anderson, Chan, 그리고 Perrig들은 소모형 센서 네트워크 환경을 위한 보안 키 설립 스킴을 제안하였다. 그들은 공격 가능성이 적은 소모형 센서 네트워크 환경에 적합한 현실적인 공격 모델을 제안하였다. 그러나 제안된 스킴은 그들이 정의한 공격 모델에서 취약점을 가지고 있다. 본 논문에서는 그 취약점을 설명하고 개선된 스킴을 제안한다. 더불어, 우리가 제안한 스킴은 추가적인 통신비용을 요구하지 않으면서 센서 배치 전에 센서 노드가 잠재적인 키를 저장 할 필요도 없다.

ABSTRACT

To guarantee secure communication in wireless sensor networks, secret keys should be securely established between sensor nodes. Recently, a simple key distribution scheme has been proposed for pair-wise key establishment in sensor networks by Anderson, Chan, and Perrig. They defined a practical attack model for non-critical commodity sensor networks. Unfortunately, the scheme is vulnerable under their attack model. In this paper, we describe the vulnerability in their scheme and propose a modified one. Our scheme is secure under their attack model and the security of our scheme is proved. Furthermore, our scheme does not require additional communication overhead nor additional infrastructure to load potential keys into sensor nodes.

Keywords : *Security, Key Management, Wireless Sensor Networks*

Ⅰ. 서 론

무선 센서 네트워크는 향후 통신 영역에서 새로운 패러다임으로 인식되고 있다. 일반적인 센서 네트워크는 저비용의 작은 장치인 센서 노드들로 대규모 네트워크를 형성한다. 각 센서 노드는 감지 기능, 데이터 처리 기능, 그리고 통신 기능을 갖는 장치이다.[2,6]

무선 센서 네트워크 환경에서 신뢰할 수 있는 무선 통신을 위해, 센서 노드들 사이의 pair-wise key들은 안전하게 설립되어야 한다. 이 pair-wise key들은 인증과 기밀성 같은 보안 목적을 위해 사용된다. 그러나 센서 노드들의 자원 제약 때문에 공개키 방식과 같은 전통적인 방식들은 저비용의 센서 네트워크 환경에서는 부적합하다. 게다가, 일반적으로 센서 노드들은 임의의 위치에 배치되므로 이웃 노드들에 대한 정보를 사전에 결정할 수 없다. 이

접수일: 2005년 11월 16일; 채택일: 2006년 3월 31일
* 본 연구는 과학재단 특정기초연구(R01-2004-000-10704-0) 지원으로 수행되었음
† 주 저자 : optim@korea.ac.kr
‡ 교신저자 : donghlee@korea.ac.kr

제약 조건 때문에 대부분의 센서 키 스킴들은 센서 노드들을 배치하기 전에 센서 노드들에게 잠재적인 키들을 배당하는 방법을 사용한다. 그러나 이 방법은 대규모의 소모형 센서 네트워크 환경에서는 부담이 될 수 있다.

대부분의 센서 키 스킴들은 센서 배치 초기 단계에도 공격이 가능하다고 가정하고 있다. 이 가정은 매우 강한 가정이어서 간단하고 효율적인 키 스킴을 설계하는 것은 매우 어려운 문제이다. 이 가정에서의 공격자는 언제든지 노드를 포획할 수 있고 모든 통신을 도청할 수 있다. 그러나 모든 센서 네트워크 응용이 이런 공격 모델에 노출되는 것은 아니다. 소모형 센서 네트워크 응용들은 공격 가능성이 높은 고가의 센서 네트워크 응용들 보다 적은 보안 위험을 갖는다. 그러므로 현실적인 공격 레벨을 가정하고 효율적인 스킴을 설계하는 것은 매우 현명한 선택이다.

1.1 관련 연구들

센서 키 스킴을 설계할 때 가장 간단한 방법은 모든 센서 노드들이 하나의 single master key를 저장하고 그 키로 노드 사이의 pair-wise key를 설립하는 방식이다. 그러나 이 경우에 공격자는 하나의 센서 노드에서 공통된 키를 얻어 전체 네트워크의 pair-wise key들을 계산할 수 있다. 다른 극단적인 방법으로 노드를 배치하기 전에 각 노드마다 다른 모든 노드와의 pair-wise key들을 직접 저장하는 방식이 있다. 이 경우에 각 노드는 전체 센서 노드 수만큼 키를 저장해야 하기 때문에 매우 큰 메모리 공간을 요구한다. 그러므로 이 두 방법은 무선 센서 네트워크 환경에서 사용될 수 없다.

Perrig 등은 SPINS(security protocols for sensor networks)를 제안하였다.[13] SPINS에서, 각 센서 노드는 센서 노드의 배치 전에 베이스 스테이션과 사용할 공유키를 저장한다. 그리고 이웃 노드와 pair-wise key를 설립하기 위해 베이스 스테이션을 경유하게 된다. SPINS는 작은 메모리 공간을 요구하고, 노드 포획에 대한 강한 안전성을 보장한다. 그러나 전체 센서 노드 수가 많으면 베이스 스테이션 주위에 있는 센서 노드들의 집중적인 자원 손실이 발생할 수 있다. 그래서 SPINS는 대규모 무선센서네트워크 구성에는 적합하지 않다.

Eschenauer와 Gligor는 Random key pre-distribution 스킴을 제안하였다.[11] 이 기술은 베이스 스테이션을 경유하지 않고 이웃 노드 사이의 pair-wise key를 설정할 수 있기 때문에 대규모 센서 네트워크 구성에 적합하다. 그러나 많은 메모리 공간을 요구하고, 노드 포획(node capture)에 대해 낮은 안전성을 가지고 있다. 2003년, 2004년에 걸쳐 안전성이 개선된 기술들이 제안되고 있지만, 많은 수의 노드 포획에 대해서 보안 문제를 갖는다.[7,9,10,12]

Zhu등은 효율적인 키 관리 기법인 LEAP를 제안했다.[14] LEAP에서 모든 센서 노드는 배치 전에 전체 single master key를 저장해 둔다. 배치 후에 이웃 노드와 single master key에서 pair-wise key를 생성하고 전체 single master key를 안전하게 제거한다. LEAP은 매우 효율적인 기법이지만, LEAP에서는 초기 키 설립 동안 노드 포획에 의한 전체 single master key 노출이 어렵다고 가정하고 있다. 그러나 새로운 노드가 추가될 경우 추가되는 노드가 저장하고 있는 전체 single master key가 노출될 가능성은 초기에 배치되는 노드들 보다 높다. 왜냐하면, 초기 네트워크 형성 시점보다 새로운 노드가 추가되는 시점에는 공격자가 더욱 적극적인 공격을 할 수 있기 때문이다.

최근에, Anderson, Chan, 그리고 Perrig 들은 소모형 센서 네트워크 환경에 적합한 키 설립 스킴 (ACP 스킴)을 제안하였다.[1] 효율적인 스킴을 제작하기 위해 이 논문에서는 현실적인 공격 모델(ACP 공격 모델)을 정의하였다. ACP 공격 모델에서의 공격자는 초기 키 설립 동안 노드 포획과 같은 물리적인 공격과 전파 방해 같은 능동적인 공격을 수행할 능력이 없으며 전체 통신의 일부만 도청할 수 있다. 그러나 초기 키 설립 이후에는 모든 공격이 100% 가능하다. 추가적으로, 이 논문에서는 안전성을 약 20% 강화하는 Secrecy Amplification 방법을 제안하였다. 하지만 이 강화 방법은 ACP 공격 모델 하에서 취약점을 갖는다.

1.2 본 논문의 공헌

본 논문의 공헌은 다음과 같이 요약될 수 있다.

○ 안전성 개선 : 기본 ACP 스킴은 ACP 공격 모델에 대해서 높은 안전성을 갖는다. 그러나 그들의 키 설립 이후의 Secrecy Amplification 방

법은 ACP 공격 모델에 대하여 취약점을 갖고 추가적인 통신비용을 요구한다. 우리는 기본 ACP 스킴에 대해서 안전성이 개선된 스킴을 제안한다. 제안된 스킴은 ACP 공격 모델에 대한 기존의 취약점이 적용되지 않고, 추가적인 통신 비용도 요구하지 않는다.

- ○ 증명가능한 안전성 : 우리는 제안된 스킴의 안전성을 암호학적으로 증명하였다. 이 증명은 Bellare 등의 암호학적인 안전성 정의에 기반 한다.[3] 우리는 의사난수함수가 안전하다는 가정 하에 우리 스킴의 안전성을 증명한다.
- ○ 적은 비용과 대규모 네트워크 지원 : 우리 스킴은 대규모 네트워크 구성이 가능하다. 우리 스킴의 계산비용, 통신비용 그리고 저장비용은 전체 네트워크 크기에 의존하지 않는다. 게다가, 우리 스킴은 각 노드에게 잠재적인 키 저장을 요구하지 않기 때문에 센서 제작에서 추가적인 공정을 절약할 수 있다.

본 논문의 구성은 다음과 같다. 2장에서는 이 논문에서 사용하는 기호들을 설명하고 3장에서는 공격 모델을 정의한다. 4장에서는 ACP 스킴을 설명하고 취약점을 분석한다. 5장에서는 개선된 스킴을 설명하고 분석한다. 마지막으로 6장에서는 결론을 맺는다.

II. 기 호

표 1. 기호와 설명

기 호	설 명
n	전체 센서 네트워크 노드 수
d	한 노드의 통신 반경 내에 있는 이웃 노드들의 평균 수
R	각 노드의 통신 반경
W_i	손실 되지 않은 i 번째 화이트 노드 (정당한 노드)
B_i	공격자가 사전에 배치 해둔 i 번째 블랙 노드 (공격자의 노드)
|	Concatenation 연산자
$\oplus$	XOR 연산자
K_{ij}	W_i와 W_j가 공유한 pair-wise key
H(·)	단방향 해쉬 함수
E(K, ·)	키 K를 사용하는 대칭암호함수
F(K, ·)	키 K를 사용하는 의사난수함수

III. 공격 모델

센서 키 스킴 설계 시 고려하는 공격은 크게 노드 포획과 같이 노드로 물리적인 접근을 하여 비밀 정보나 비밀키를 직접 얻는 공격 방법과 공격자가 미리 배치한 몇 개의 블랙 노드들을 이용하여 노드들 간의 통신을 감시하고 분석하여 비밀 정보를 얻는 공격 방법이 있다. 실제로, 노드는 배치되자마자 짧은 시간 내에 키 설립을 완료하게 된다. 그러므로 초기 키 설립 동안에는 공격자가 배치 장소 및 시간에 대해 사전 정보가 없기 때문에 노드 포획을 통한 능동적 공격은 어렵다. 마찬가지로 통신 감시 역시 완벽하게 이뤄지기가 힘들다. 이런 현실적인 상황을 고려하여 제시된 공격 모델이 ACP 공격 모델이다.[1] 즉, 물리적 접근을 통한 능동적 공격은 키 설립 동안에는 없지만 키 설립 이후에는 가능하고 통신 감시 역시 키 설립 동안에는 일부분만(α%) 가능하며 키 설립 이후에는 100%의 통신 감시가 가능하다. 소모형 센서 네트워크 환경에서의 공격 모델은 [1]에서 다음과 같이 정의하였다.

표 2. ACP 공격 모델

	키 설립 동안	키 설립 후
물리적 접근, 능동적 공격	불가능	가능
통신 감시	α%	100%

실제로 ZigBee에서 초기 키 생성 시 이런 환경을 고려하고 있다. ZigBee에서는 일반 노드가 코디네이터(coordinator)와의 pair-wise key와 라우터(router)와의 pair-wise key를 생성하고 지속적으로 갱신해 나간다. 이 때, 초기 pair-wise key 생성 방식은 두 가지가 있다. 첫 번째 방식은 관리자가 각 노드의 pair-wise key를 노드에게 사전 저장하는 방식이고 두 번째 방식은 초기 노드 배치 후 싱크(sink)가 직접 pair-wise key를 broadcast하는 방식이다.[15] 즉, 실제로 ZigBee 네트워크 형성 시 키 설립 동안에는 노드 포획과 같은 능동적 공격과 통신 감시 역시 없다고 가정하고 있다.

소모형 센서들을 이용한 응용 분야는 보안 위험이 높은 센서 네트워크와는 다른 응용 분야이다. 업계와 기술 연구진들은 센서 네트워크가 일상생활과 산업 현장에서 널리 사용 될 것이라고 예측한다. 일부

어플리케이션은 공장 기계와 오염 수준 및 고속도로 교통량 등을 모니터링 하는데 사용 될 것이다.[8] 그리고 센서 네트워크는 화재지역을 발견하고 예방할 수 있다. 뿐만 아니라, 미리 광범위하게 배치된 노드들을 이용하여 멸종 위기에 처한 동물들의 유용한 정보를 동물학자에게 전송하는 방식으로 이런 동물들을 추적할 수도 있다. 또한 센서 네트워크는 홈 네트워크에서 중요한 요소로 사용 될 것이다. 왜냐하면 현재의 실내 온도나 습기를 측정할 수 있을 뿐 아니라 어떠한 예기치 않은 행동을 감지함으로써 도둑으로부터 주택을 보호할 수 있기 때문이다.

하지만 이러한 형태의 센서 네트워크를 공격하려는 시도나 위협은 위험한 환경에서의 센서 네트워크에 대한 공격에 비해서는 심각하지 않을 것이다. 하지만 이것은 소모형 센서 네트워크가 전혀 보안이 필요하지 않다는 것을 의미하지는 않는다. 노드들은 여전히 물리적 공격에 노출되어 있고 수집된 데이터는 공격자에 의해 도청도 가능하다. 또한 가짜 데이터가 센서 네트워크의 작동을 방해하기 위해 삽입될 지도 모른다. 이러한 공격의 위험성은 단순한 일시적 기능 저하에서부터 인간 생활을 위협하는 범위까지 다양할 것이다. 다시 말해, 요구되는 보안 레벨을 충족시키지 않는다면 센서 네트워크의 경제적 가치 또한 감소할 것이다.

만약 위험 환경에서 사용하는 보안 메커니즘만큼 소모형 센서 네트워크를 강화 한다면 어플리케이션의 사용이 감소할 것이다. 이렇듯 유용성과 보안 수준 사이의 trade-off는 항상 존재하기 마련이다. 그래서 센서 네트워크의 키 관리를 설계 시 적절한 보안 수준을 고려해야 한다.

Ⅳ. ACP 스킴[1]

이제 기본 ACP 스킴과 안전성을 개선한 Secrecy Amplification을 설명한다. 그 후, ACP 공격 모델 하에서 Secrecy Amplification의 취약점을 지적할 것이다.

(그림 1)에서 W_1, W_2 와 W_3은 화이트 노드들이고 서로 이웃 노드들이다. 왼쪽 원은 W_1의 통신 반경을 나타내고 오른쪽 원은 W_2의 통신 반경을 나타낸다. 편의상, 노드명과 노드 식별자(ID)는 동일하게 사용한다. 즉, 노드 W_1, W_2와 W_3의 노드 식별자 역시 W_1, W_2와 W_3으로 한다. B_1은 미리 배치된 블랙 노드이다. 이렇게 배치되었을 경우, W_3과 B_1은 W_1과 W_2의 모든 통신을 감지할 수 있지만 B_1은 W_3의 통신은 감지 할 수 없다.

4.1 기본 ACP 스킴

기본 ACP 스킴은 다음과 같이 두 단계로 이루어져 있다.

(1) 노드의 배치와 동시에 화이트 노드 W_1은 랜덤 값 K_1을 생성하여 브로드캐스트 하고 이웃 노드 W_2는 그 메시지를 획득한다.
(2) W_2는 임의의 pair-wise key로 K_{12}를 생성한 후 K_1을 사용하여 암호화 된 메시지 $E(K_1, W_2|K_{12})$를 브로드캐스트 한다. 결과적으로 두 노드 W_1과 W_2는 공통의 pair-wise key K_{12}를 공유하게 된다.

블랙 노드가 없는 지역에서는 W_1과 W_2간에 안전한 링크가 생성된다. 하지만 만약에 (그림 1)처럼 블랙 노드 B_1이 키 설립 동안 W_1과 W_2의 모든 메시지를 도청했다면 W_1과 W_2간에 pair-wise key는 손실되게 된다. [1]의 예제에서 알 수 있듯이, 화이트 노드 100개당 1개의 블랙 노드가 존재하고 d가 4라고 가정할 때, 손실된 링크는 대략 2.4%에

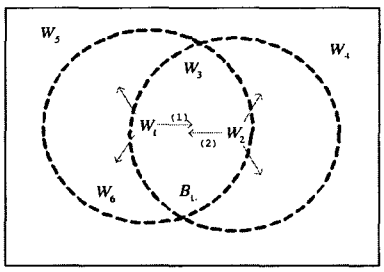


그림 1. 기본 ACP 스킴

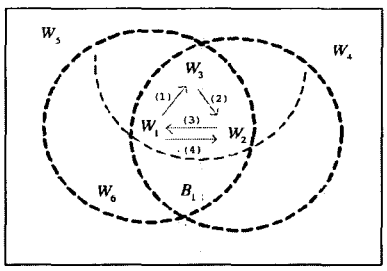


그림 2. Secrecy Amplification

불과하다.

4.2 Secrecy Amplification

두 이웃 노드 W_1과 W_2가 키 설립 후 pair-wise key K_{12}를 공유했다고 가정해 보자. 이 때, 두 노드는 공통의 이웃 노드 W_3를 사용하여 키의 안전성을 증대 시킬 수 있다. 기본 ACP 스킴 후 Secrecy Amplification은 네 단계로 이루어진다.

(1) W_1은 암호화 된 메시지 $E(K_{13}, W_1|W_2|N_1)$을 W_3에게 전송한다. 이 때 N_1은 W_1이 생성한 예측 불가능한 난수(Nonce)이고 K_{13}은 W_1과 W_3간에 공유된 pair-wise key이다.
(2) W_3은 전송 받은 메시지를 복호화 한 후 또 다른 암호문 $E(K_{23}, W_1|W_2|N_1)$를 W_2에게 전송한다. 이 때 K_{23}은 W_2와 W_3간의 pair-wise key이다. W_2는 암호문을 복호화 한 후 N_1을 얻게 된다. 그래서 W_1과 W_2는 공통의 난수 N_1을 가지게 되고 pair-wise key를 $K'_{12} = H(K_{12}|N_1)$로 갱신할 수 있다.
(3) 다음으로, pair-wise key를 confirmation (확인)하기 위해서 W_2는 자신이 생성한 난수 N_2를 사용하여 암호 메시지 $E(K'_{12}, N_1|N_2)$을 W_1에게 전송한다.
(4) 마지막으로, W_1은 암호 메시지 $E(K'_{12}, N_2)$를 W_2에게 전송하여 두 노드들은 갱신된 pair-wise key을 확인하게 된다.

공격자에 의해 미리 배치된 B_1이 W_1과 W_2의 공통 통신 반경에는 속하지만 W_3의 통신 반경 밖에 있다고 가정해 보자. 이 블랙 노드는 기본 ACP 스킴 동안에는 K_{12}는 알지만 K_{13}와 K_{23}는 알 수 없다. 그래서 Secrecy Amplification 동안에 공격자가 갱신된 키 K'_{12}를 계산 하는 것은 어렵다. 이런 차이 때문에 기본 ACP 스킴과 비교해서 Secrecy Amplification 과정 후에 전체 안전성이 약 20% 정도 개선된다.[1]

4.3 Secrecy Amplification의 취약점

B_1을 이용하여 K_{12}를 획득한 공격자가 K'_{12}를 알기 원한다고 가정해 보자. ACP 공격 모델에서 기본 ACP 스킴 이후 공격자는 모든 통신을 감시할 수 있고 노드들을 포획하여 메모리에 저장된 비밀 정보를 획득할 수도 있다. 그렇기 때문에, 공격자는 암호화된 메시지 $E(K_{13}, W_1|W_2|N_1)$를 모니터링 할 수 있고, W_3을 포획하여 K_{13}을 얻을 수도 있다. 그러므로 공격자는 $E(K_{13}, W_1|W_2|N_1)$와 K_{13}에서 난수 N_1을 알아 낼 수도 있고, K'_{12}를 계산 할 수 있다. 물론, W_1과 W_3가 일방향 함수를 사용하여 K_{13}를 $H(K_{13})$으로 갱신한다면 이런 공격에 대한 취약점을 개선할 수 있다. 그러나 이 방법은 추가적인 계산 과정을 요구하고, ACP 공격 모델에서, K_{13}이 $H(K_{13})$으로 갱신되기 전에 공격자는 K_{13}을 얻을 수 있기 때문에 ACP 공격 모델에서 Secrecy Amplification은 여전히 취약성을 갖는다.

V. 새로운 스킴

우리 스킴에서 보안 모델은 ACP 공격 모델과 같지만 기본 ACP 스킴 후에 이뤄지는 Secrecy Amplification의 취약점은 제거하였다. 또한 통신상의 추가적 비용 없이 안전성도 개선하였다. 게다가, 제안된 스킴은 암호학적으로 증명가능한 안전성을 갖는다.

5.1 개선된 스킴

우리 스킴은 다음과 같이 구성된다.

(1) 배치된 화이트 노드 W_1이 랜덤 키 K_1을 생성한 후 그것을 이웃 노드들에게 브로드캐스트 한다. 여기서 W_1과 W_2는 이웃 노드이고 W_3 역시 이들의 이웃 노드라고 가정하자.
(2) W_2는 랜덤 키 K_2를 생성한 후 암호화 된 메시지 $E(K_1, W_3|K_2)$를 브로드캐스트 한다.
(2)′ 유사하게 W_3 역시 랜덤 키 K_3을 생성한 후 $E(K_1, W_2|K_3)$을 브로드캐스트 한다. 여기에서 (2)와 (2)′는 서로 독립적이기 때문에 (2)와 (2)′의 두 메시지는 순서에 상관없이 전송될 수 있다.

이제 노드 W_1, W_2와 W_3은 K_2와 K_3을 획득 할 수 있다. 왜냐하면 세 노드 모두 K_1을 알고 있으므로 그들 사이의 모든 통신을 복호화 할 수 있기 때문이다. 두 노드 W_1과 W_2는 $K_{12}=F(K_3, F(K_2, K_1))$을 둘 사이의 pair-wise key로 사용하고 두 노드 W_1과

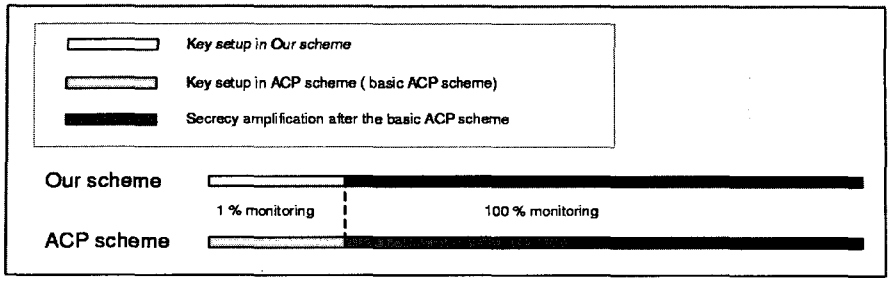


그림 3. pair-wise key 설립 단계

W_3은 $K_{13} = F(K_2, F(K_3, K_1))$을 그들의 pair-wise key로 사용한다. 키 설립 후 모든 노드들은 메모리에 저장된 K_1, K_2와 K_3을 완전하게 삭제한다.

Pair-wise key K_{12}를 얻을 수 있는 블랙 노드는 W_1, W_2와 W_3의 모든 통신 내용을 도청 할 수 있는 통신 영역 내에 위치해야만 한다. 이 안전성 조건은 기본 ACP 스킴 후 Secrecy Amplification에서 갱신된 키 K'_{12}를 획득하기 위한 조건과 같다. 그래서 우리 스킴의 안전성도 Secrecy Amplification와 같이 기본 ACP 스킴보다 20% 정도 개선된다.

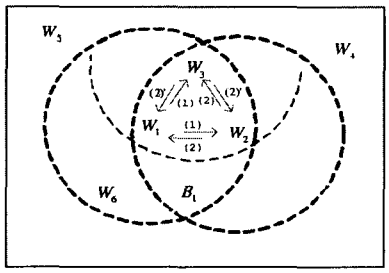


그림 4. 개선된 스킴

5.2 안전성 분석

제안된 스킴은 기본 ACP 스킴 후 Secrecy Amplification과 동일한 수준만큼 안전성을 개선하면서 Secrecy Amplification의 취약성은 적용되지 않는다. 또한 공격자가 K_{12}를 얻기 위해서는 키 설립 동안 W_1, W_2와 W_3 사이의 통신 내용을 도청해야만 한다. 하지만 기본 ACP 스킴에서는 공격자가 W_1과 W_2 사이의 통신 내용만 도청하면 K_{12}를 얻을 수 있다.

Secrecy Amplification은 기본 ACP 스킴 이후의 과정이기 때문에 통신 모니터링이 가능하다. 그러나 만약 공격자가 Secrecy Amplification 과정의 통신을 얻을 수 없다면 4.3에서 설명한 취약성을 피할 수 있다. 그러기 위해서는 Secrecy Amplification이 키 설립 시간에 포함되어야 한다. 이렇게 키 설립 시간을 정의하면 초기 키 설립 시간이 증가하게 된다. 각 공격모델에서 키 설립 동안 공격이 거의 없다는 가정을 사용하기 때문에 키 설립 시간이 최대한 적을수록 현실적인 공격 모델로 인정할 수 있다. 그러므로 Secrecy Amplification의 취약성을 피하기 위해 Secrecy Amplification 과정을 키 설립 시간에 포함시키는 것은 기존 보다 더욱 강한 가정이 된다. 반면 제안된 스킴은 기본 ACP 스킴과 비슷한 통신비용을 요구하기 때문에 기본 ACP 스킴과 비슷한 시간 내에 키를 생성 할 수 있다.

이제, Secrecy Amplification의 취약성 분석과 동일한 방법으로 제안된 스킴을 분석할 것이다. (그림 3) 같이 배치된 블랙 노드 B_1을 사용해서 초기 키 설립 과정에서 공격자가 K_1과 K_2를 획득했다고 가정해 보자. 또한, 공격자가 키 설립 후에 W_3을 포획하였다고 가정하자. 공격자는 포획한 노드로부터 K_{13}을 획득 할 수 있다. 이러한 시나리오에서 공격자는 직접적이든 간접적이든 계산을 통해 K_{12}를 획득하려고 시도할 것이다. 먼저, 만약에 공격자가 $K_{13}=F(K_2, F(K_3, K_1))$로부터 K_3을 계산해 낼 수 있다면, $F(K_3, F(K_2, K_1))$을 직접 계산하여 K_{12}를 획득 할 수 있다. 하지만 이것은 의사난수함수가 일방향 함수(one-way function)이기 때문에 불가능하다. 두 번째로, 만약에 K_1, K_2와 K_{13}만으로(K_3을 제외) K_{12}를 간접적으로 계산해 낼 수 있는 방법이 존재한다면 우리 스킴은 안전하지 않을 것이다. 이제 우리 스킴의 안전성을 증명할 것이다. 아래의 정리는 의사난수함수가 안전하다면 공격자가 K_1, K_2, K_{13}로부터 K_{12}를 계산하는 것이 어렵다는 것을 의미한다.

정의 1. 어떤 정수 $k,l,L \geq 0$에 대해 $F: \{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^L$를 어떤 함수의 집합이라 하자. 그때 어떤 구별자 A에 대해서 다음을 정의한다.

$$Adv_F^{prf}(A) := \Pr\left[f \xleftarrow{R} F: A^f = 1\right] - \Pr\left[f \xleftarrow{R} Rand^{l-L}: A^f = 1\right]$$

우리는 F의 advantage 인 $Adv_F^{prf}(\cdot,\cdot)$를 어떤 정수 $q, t \geq 0$에 대해 다음과 같이 정의한다.

$$Adv_F^{prf}(q,t) := \max_A\left\{Adv_F^{prf}(A)\right\}$$

이것은 최대 q 개의 질의를 하고, 최대 t 수행 시간이 가능한 구별자 A에 대한 최대값이다.

우리는 제안된 스킴(M)의 안전성을 정의한다. 키 설립 이후에 공격자는 모든 통신의 모니터링과 노드 포획 (chosen node capture attack, cna)을 할 수 있다. 이 공격자는 포획한 노드의 메모리에서 비밀 정보를 얻을 수 있다. 만약 공격자가 포획된 노드의 이웃노드가 아닌 포획하지 않은 노드의 pair-wise key를 적어도 하나 유도할 수 있으면 이 공격은 성공하게 된다.

정의 2. $F: \{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^L$를 어떤 함수의 집합이라 하자. 만약 아래 advantage가 파라미터 k에 대해 거의 0이면 제안된 스킴 M은 안전하다.

Experiment $\mathrm{EXP}_M^{cna}(B)$

$K_1, K_2, K_3 \xleftarrow{R} \{0,1\}^k$

Compute $K_{13} = F(K_2, F(K_3, K_1))$

$B \leftarrow K_1, K_2, K_{13}$

$\widehat{K_{12}} \leftarrow B$

If $F(K_3, F(K_2, K_1)) = \widehat{K_{12}}$
then return 1
else return 0

B의 advantage는 다음과 같이 정의된다.

$$Adv_M^{cna}(B) := \Pr\left[\mathrm{EXP}_M^{cna}(B) = 1\right]$$

제안된 스킴 M의 advantage는 어떤 정수 값 $t' \geq 0$에 대해서 다음과 같이 정의된다.

$$Adv_M^{cna}(t') := \max_B\left\{Adv_M^{cna}(B)\right\}$$

이 값은 수행시간이 최대 t'인 모든 공격자에 대한 최대 advantage 값이다.

정리 1. $F: \{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^L$ 를 어떤 함수의 집합이라 하자. 그때 제안된 스킴 M은 $q = 2$ 그리고 $t = t' + O(k)$ 인 정수 값들에 대해 다음을 만족한다.

$$Adv_M^{cna}(t') < Adv_F^{prf}(q,t) + \frac{1}{2^L}$$

증명) B가 M을 공격하는 공격자라고 가정하자. 우리는 F의 공격자 A_B를 아래와 같이 구성한다.

Distinguish A_f^B

$K_1, K_2 \xleftarrow{R} \{0,1\}^k$

$y \leftarrow f(K_1)$

Compute $K_{13} = F(K_2, y)$

Run attacker B

$B \leftarrow K_1, K_2, K_{13}$

$\widehat{K_{12}} \leftarrow B$

Compute $F(K_2, K_1)$

$z \leftarrow f(F(K_2, K_1))$

If $z = \widehat{K_{12}}$ then return 1 else return 0

여기서 A_B는 B를 내부 알고리즘으로 사용한다.

$$\Pr\left[f \xleftarrow{R} F: A_B^f = 1\right] \geq Adv_M^{cna}(B)$$

$$\Pr\left[f \xleftarrow{R} Rand^{l-L}: A_B^f = 1\right] = \frac{1}{2^L}$$

$$Adv_F^{prf}(A_B) \geq Adv_M^{cna}(B) - \frac{1}{2^L}$$

정의의 부등식은 아래와 같이 얻어진다.

$$Adv_M^{cna}(t') := \max_B\left\{Adv_M^{cna}(B)\right\}$$

$$\leq \max_B\{Adv_F^{prf}(A_B)\}+\frac{1}{2^L}$$
$$\leq \max_A\{Adv_F^{prf}(A)\}+\frac{1}{2^L}$$
$$= Adv_F^{prf}(q,t)+\frac{1}{2^L}$$

여기서 A_B는 오라클의 질의를 두 개 ($q=2$) 만들고 수행시간으로 $t=t'+O(k)$를 사용한다. ■

5.3 효율성 분석

통신비용은 기본 ACP 스킴과 동일하다. 뿐만 아니라, 기본 ACP 스킴 후에 Secrecy Amplification이 추가적인 통신비용을 요구한 반면에 우리 스킴은 이러한 추가적 통신비용 없이 안전성을 강화하였다. 기본 ACP 스킴과 비교해 볼 때, 우리 스킴은 각 노드마다 두 번의 의사난수함수를 더 사용한다. 의사난수함수의 기본적 개념은 블록 암호를 모델링하는 것이다. 즉, 의사난수함수 사용 시 드는 계산 비용은 대칭 암호 함수를 사용에 따르는 비용과 동일하다고 볼 수 있다. 두 번의 의사난수함수 연산은 우리 스킴이 암호학적으로 증명 가능한 안전성을 가지도록 설계하기 위해서 추가된 부분이다. 만약에 안전성 증명을 요구하지 않는다면 pair-wise key는 간단하게 $K_{12} = H(K_1|K_2|K_3)$로 사용할 수 있다.

우리 스킴에서 두 이웃 노드가 키를 설립하기 위해서는 두 번의 통신과 두 번의 의사난수함수 연산을 요구한다. 반면에 대표적인 Random key pre- distribution 스킴에서 두 이웃 노드가 키를 설립하기 위해서는 각 노드가 저장하고 있는 키 후보(50~200)만큼의 통신과 암호화 과정을 요구한다. 이 스킴은 노드 배치 초기에도 공격이 가능한 강한 공격 모델에 대해 확률적인 안전성[11]을 보장하지만 많은 통신 및 계산 비용을 요구하기 때문에 소모형 센서 네트워크 환경에는 부적합하다.

5.4 공통 이웃 노드

우리 스킴은 ACP 스킴과 같이 세 노드에 대해서 논의 하였지만, 여러 이웃 노드들에 대해서도 간단하게 고려할 수 있다. ACP 스킴처럼, 우리 스킴도 각 노드들이 배치되면 이웃 노드들을 감지한다는 가정을 갖는다. 배치된 노드는 이웃 노드 중 하나와 키 설립을 시도하고 공통된 이웃 노드들을 파악한다. 만약 공통된 이웃 노드가 두 개 이상 있으면 공통 이웃 노드들 중 ID값이 작은 노드를 선택하고 키 설립을 수행하다. 반면, 두 노드가 공통된 이웃 노드가 없을 경우는 $K_{12} = F(K_2, K_1)$를 pair-wise key로 사용하면 된다. 하지만 이럴 확률은 (1)의 계산을 통해 알 수 있듯이 매우 희박하다.

$$\Pr[\text{no common neighbor node}] = \left(1-\frac{2}{\pi}arctan\sqrt{8}+\frac{\sqrt{8}}{9\pi}\right)^{d-1} \quad (1)$$

두 이웃 노드 사이의 평균 거리는 다음과 같이 계산된다.

$$\int_0^R xf(x)dx = \int_0^R x\frac{2\pi x}{\pi R^2}dx = \frac{2}{3}R$$

그리고 두 이웃 노드 사이의 평균 공통 영역은 다음과 같이 계산된다.

$$Common range = 2(\arctan\sqrt{8}-\frac{\sqrt{8}}{9})R^2$$

그러므로 만약 각 노드가 d개의 이웃노드를 갖는다면 임의의 두 이웃 노드가 공통된 이웃 노드를 가지지 못할 확률은 다음과 같이 유도된다.

$$\Pr[\text{no common neighbor node}] = \left(1-\frac{Common range}{\pi R^2}\right)^{d-1}$$
$$= \left(1-\frac{2}{\pi}arctan\sqrt{8}+\frac{\sqrt{8}}{9\pi}\right)^{d-1} \blacksquare$$

여기서, 만약 d가 5일 때 공통 이웃 노드가 존재 하지 않을 확률은 0.03이 된다.

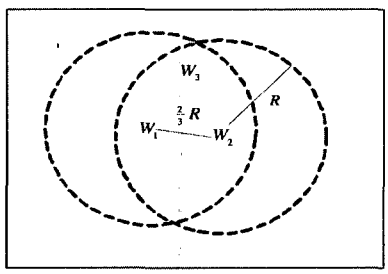


그림 5. 두 이웃 노드의 공통 영역 평균

Ⅵ. 결 론

우리는 ACP 공격 모델에서 취약성이 없는 개선된 스킴을 제안하였다.[1] 본 논문의 공헌은 다음과 같다. 첫째, 제안된 스킴은 기본 ACP 스킴에 비해 20% 정도 개선된 안전성을 갖는다. 둘째, 우리는 제안된 스킴의 안전성을 암호학적으로 증명하였다. 마지막으로, 제안된 스킴은 효율적이고 대규모 네트워크 구성이 가능하다. 비록 ACP 스킴과 마찬가지로 우리의 제안된 스킴도 새로운 노드 추가를 지원하지는 않지만, 소모형 센서 네트워크 환경이 새로운 노드를 추가를 고려하지 않기 때문에 문제가 되지 않는다. 제안된 스킴은 매우 효율적이고 현실적인 공격 모델을 고려하고 있기 때문에 실용적인 센서 네트워크 응용에서 다양하게 활용될 것이다.

참 고 문 헌

[1] R. Anderson, H. Chan, and A. Perrig, "Key Infection : Smart Trust for Smart Dust," In 12th IEEE International Conference on Network Protocols, pp.206-215, October 2004.

[2] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communications Magazine, Vol. 40, No. 8, pp. 102-114, August 2002.

[3] M. Bellare, J. Kilian, and P. Rogaway, "The security of the cipher block chaining message authentication code," Journal of Computer and System Sciences, Vol. 61, No. 3, pp. 362-399, December 2000.

[4] R. Blom, "An optimal class of symmetric key generation systems," In Proceedings of EUROCRYPT `84, LNCS Vol. 209, pp.335-338, 1985.

[5] C. Blundo, A. D. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," In Proceedings of CRYPTO `93, LNCS Vol. 740, pp. 471-486, 1993.

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

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

[8] H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," IEEE Computer, Vol.36, No.10, pp. 103-105, October 2003.

[9] W. Du, J. Deng, Y. S. Han, S. Chen, and P.K. Varshney, "A Key Management Scheme for Wireless Sensor Networks Using Deployment Knowledge," In Proceedings of the IEEE INFOCOM `04, pp. 586-597, March 2004.

[10] W. Du, J. Deng, Y. S. Han, P.K. Varshney, J. Katz, and A. Khalili, "A Pairwise Key Pre-distribution Scheme for Wireless Sensor Networks," ACM Transactions on Information and System Security, pp.228~258, August 2005.

[11] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," In Proceedings of the 9th ACM conference on Computer and communications security, pp.41-47, November 2002.

[12] D. Liu, P. Ning, and R. Li, "Establishing Pairwise Keys in Distributed Sensor Networks," ACM Transactions on Information and System Security, pp.41~77, February 2005.

[13] A. Perrig, R. Szewczyk, V. Wen, D. Cullar, and J. D. Tygar, "SPINS: Security protocols for sensor networks," In Proceedings of the 7th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking, pp.189-199, July 2001.

[14] S. Zhu, S. Setia, and S. Jajodia,

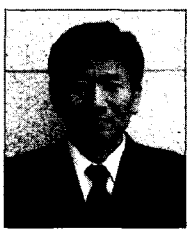
"LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," CCS'03, Washington, DC, USA. October 27-31, 2003.

[15] Zigbee Alliance, "Security Services Specification Revision 13", ZigBee Alliance Board of Directors, December 14th, 2004

〈著者紹介〉

김 용 호 (Kim, Young Ho) 정회원
2000년 2월 : 고려대학교 수학과 학사
2002년 2월 : 고려대학교 수학과 이학석사
2002년 3월~현재 : 고려대학교 정보보호대학원 박사과정
〈관심분야〉 정보보호 프로토콜, 암호이론, RFID/USN 보안 이론, 키 교환

이 화 성 (Lee, Hwa Seong) 학생회원
2003년 2월 : 안동대학교 멀티미디어 공학과 학사
2006년 2월 : 고려대학교 정보보호대학원 공학석사
2006년 3월~현재 : 고려대학교 정보보호대학원 박사과정
〈관심분야〉 무선센서네트워크 정보 보호 기술, 정보보호 이론, RFID 인증



이 동 훈 (Lee, Dong Hoon) 종신회원
1983년 8월 : 고려대학교 경제학사
1987년 12월 : Oklahoma University 전산학 석사
1992년 5월 : Oklahoma University 전산학 박사
1992년 8월 : 단국대학교 전자계산학과 전임강사
1993년 3월 ~ 1997년 2월 : 고려대학교 전산학과 조교수
1997년 3월 ~ 2001년 2월 : 고려대학교 전산학과 부교수
2001년 2월~현재 : 고려대학교 정보보호대학원 부교수
〈관심분야〉 암호프로토콜, 암호이론, USN 이론, 키 교환, 익명성 연구, PET 기술