무선 센서 네트워크 환경에서 확장성 있는 브로트캐스트 인증을 제공하기 위한 초기화 프로토콜†

김준완, 김용호, 이동훈*

*고려대학교 정보보호대학원

The Bootstrapping Scheme Providing Scalable Broadcast Authentication in Wireless Sensor Networks

Joon-Wan Kim, Yong-Ho Kim, Dong-Hoon Lee*

*Graduate School of Information Security, Korea University.

요 약

무선 센서네트워크에서의 브로드캐스트 인증은 중요한 문제이다. 이를 위해 μ-TESLA와 이를 개선한 멀티레벨 μ-TESLA 방법 등이 제안되었다. 이들 모두는 인증을 성공적으로 수행하기 위해 브로드캐스트 메시지를 보내고자 하는 당사자의 해시체인 commitment를 인증 받으려는 상대방에게 안전하게 전달해야만 했다. 하지만, 센서들이 랜덤하게 배치될 경우 각 노드는 인증을 위해 전체 노드 수만큼의 commitment를 저장해야만 하는 문제점을 지니고 있다. 이를 해결하기 위해 Chen 등은 브로드 캐스트 인증에 사용되는 해시 체인 commitment를 안전하고 효율적인 방법으로 전달하는 방안을 제안하였다. 그러나 불행이도 이들의 방법은 노드 추가가 원천적으로 불가능하고, 초기화 과정에서 부득이하게 참여하지 못한 노드를 구제할 방법이 전혀 없어 큰 비용 낭비를 초래한다. 뿐만 아니라 베이스 스테이션이 비밀 값을 재사용 할 경우 안전성에도 큰 문제가 발생한다. 제안하는 스킴은 멀티 세션을 적용하고 비밀 값에 대한 해시 체인을 구성하여 앞서 열거된 모든 문제점을 해결함으로써 안전하고 효율적인 commitment 전달 방법을 제시한다. 아울러 주고받는 메시지에 대한 무결성 검증을 제공한다.

I. 서론

최근 들어 무선 센서 네트워크에 대한 연구가 활발히 진행되고 있다. 센서 네트워크는 크게 베이스 스테이션과 노드로 구분되지만 더 세분하면 전력 공급 유무나 통신 반경 등의 능력에 따라 베이스 스테이션과 일반 노드 사이를 연결해 주는 싱크 노드 등이 추가되기도 한다. 하지만, 절대 다수를 차지하는 일반 센서 노드들은 여전히 저전력, 저능력, 저비용의 제약을 갖기 때문에 적정 보안 수준이나 서비스를 충족시키기는 어려운 실정이다.

그러나 설사, 이러한 제약조건이 있다하더라도 센서 환경에서의 인증은 반드시 필요한 요소 중 하나이다. 인증은 크게 개체 인증과 정보 인증으로 나눌 수 있는데, 전자는 베이스 스테이션과 노드 등이 정당한 구성원인지를 밝혀주며 후자는 수신된 정보가 위조되거나 변조되지 않았다는 것을 증명해 준다. 전통적인 환경에서 이 둘은 전자서명 스킴으로 한꺼번에 간단히 해결될 수 있었다. 하지만, 앞서 언급했듯이 센서 환경은 다르다. 다시 말해, 언급된 제약조건은 전통적인 전자서명 방식으로 인증문제를 해결하기 어렵게 만든다. 공개키 방식의 인증 시스템은 인증 시 센서노드에게 계산 부담을 가중시켜 전력 소모가 급격히 이루어지게 만들 수 있기 때문이다.

이러한 와중에 훨씬 빠르고 전력을 적게 소모하는 대칭키 방식으로 인증이 가능케 되도록 한 μ-TESLA가 제안되었다. 그것은 Perrig 등이 기존 인증 방식인 TESLA를 일부 수정하여 무선 센서 네트워크와 같은 소모형 네트워크에 적합하도록 만든 것이었다. 이후 센서 환경에서의 인증은 μ-TESLA이나 그와 유사한 방식으로 이루어져왔다. 즉, 시간 지연을 통한 대칭키 노출, 그리고 이를 이용한 MAC값의 확인 절차에 따라 사용자 인증과 메세지 인증을 동시에 가능하도록 만들었다[1].

1.1 연구 배경과 필요성

마이크로 테슬라의 이러한 공헌에도 불구하고 많은 취약점들이 발견되었다. 대표적인 예로서, 해시체인의 길이 문제, 베이스스테이션이 commitment를 노드들에게 유니캐스트함으로 발생하는 문제, 때문에 베이스 스테이션에서 노드로의 인증에만 용이 할 뿐 실질적으로 네트워크 내 임의의 구성원 간에, 이를테

† 본 연구는 2006년도 두뇌한국 21사업으로 수행되었음.

면 노드 대 노드 인증에는 제대로 사용할 수 없다는 점 등이 그것이다. 지난 몇 년간 이를 부분적으로 극복한 작업들이 진행되었다. Liu 등은 단일 해시 체인만을 사용하던 기존 마이크로 테슬라의 단점을 극복하기 위해 여러 개의 해시 체인을 계층적으로 엮은 멀티레벨 마이크로 테슬라 방식을 제안하였다[3]. 그들은 스킴을 제안하면서 commitment를 유니캐스트하지 않고 브로드 캐스트 하는 방식으로 바꾸었다. 이와 더불어 그들은 자신들이 제안한 스킴이 DoS 공격에 견딜 수 있는지도 다루었는데 멀티 해시 체인의 도입으로 인한 추가적인 부담을 극복한 근본적인 해결책은 제시하지 못하였다. 가장 주목할 만 한 점은, 마이크로 테슬라나 멀티레벨 마이크로 테슬라 모두 보내는측(sender)과 받는측(receiver)이 사실상 베이스 스테이션과 노드로 편중되었다는 점이다. 이는 심각한 문제인데 만일 보내는 측이 막강한 능력을 갖춘 베이스 스테이션이 아닌 일반 노드가 되었을 때 문제가 심화된다. 이 경우 제한된 센서 노드는 마이크로 테슬라나, 멀티레벨 마이크로 테슬라를 통해 인증하기 위해 받는 측에 자신의 해시 체인 commitment를 전달해야 한다. 바꿔 말하면 어떤 노드가 다른 누군가를 인증하려면 그의 해시 체인 commitment를 가지고 있어야만 한다는 것이다. 그런데, 특별한 경우를 제외하고서 대부분 센서 노드가 대량으로 랜덤하게 뿌려진다고 가정해보자. 그렇게 되면, 한 노드의 입장에서 봤을 때 주변 이웃 노드가 누가 될지 알 수 없으므로 임의의 노드를 인증하기 위해선 전체 노드 각각의 해시 체인 commitment를 미리 저장해야만 할 것이다. 전체 노드의 수 n 에 대해 n-1개의 commitment를 저장해야 하는 것이다[2]. 즉각 우리는 이것이 비효율적이라는 것을 알아차릴 수 있다. 결국, 센서 노드의 랜덤 배치와 메모리 제약을 배제하지 않고서, 베이스 스테이션과만이 아니라 노드들 간에도 마이크로 혹은 멀티레벨 마이크로 테슬라 방식의 인증이 효율적으로 이루어지게 하려면 특정 절차를 따르는 부트스트래핑 스킴이 필요하다는 결론에 이른다. Chen 등은 멀티캐스트 인증을 위해 센서 노드의 랜덤 배치와 메모리 제약을 감안한 부트스트래핑 스킴을 제안하였다. 그들의 방식에서는, 각 노드들이 배치된 뒤 누가 될지 모르는 이웃 노드를 인증하기 위해 각자 n-1개의 commitment를 저장하는 것이 아니라 단지 하나의 키만을 저장할 것이 요구된다. 그러나 불행히도 그들의 방식은 메모리 부담을 크게 줄이는 뚜렷한 장점을 가지게 되었지만 동시에 다음과 같은 두 가지 치명적인 단점도 지니게 되었다.

- 노드 추가 문제 등 확장성에 대한 고려 결여.
- 배치된 노드 중 예측 못한 문제로 인해 초반 부트스트래핑 프로토콜 단계에 참여하지 못하거나 뒤늦게 참여한 노드들은 브로드캐스트 인증 시스템에서 배제, 즉 사실상의 노드 손실과 그로 인한 비용 낭비를 초래.

1.2 본 논문의 공헌

우리는 센서 노드의 랜덤 배치와 성능상의 제약조건을 기본적으로 가정한 상태에서 다음 스킴을 제안한다.

- 브로드 캐스트 인증을 위해 수행하는 부트스트래핑 스킴에서 초반 참여에 아예 실패하거나 뒤늦게 참여한 노드들이 성공적으로 시스템에 참여할 수 있게 해주는 자가 치료(self-healing) 기능을 갖춘 멀티 세션 부트스트래핑 스킴을 제안한다.
- 또한 제안하는 스킴은 세션이 종료되더라도 새로운 노드를 얼마든지 추가할 수 있는 확장성을 지닌다.

II. 노드 간 인증 문제

노드 간 인증은 베이스스테이션과 노드 사이에 이루어지는 인증 방식보다 제약이 심하다. 때문에 보내는측과 받는측을 각각 베이스스테이션과 노드로 가정하고 이 둘 사이의 인증에 기준을 맞추어 인증 스킴을 설계한다면 노드와 노드 사이의 인증에 적용했을 때엔 매우 비효율적이거나 심지어 불가능해 질 수 있다. 본 논문에서 고려한 가정과 요구조건들은 다음과 같아.

-Node's Low Performance: 노드의 제반 능력은 베이스 스테이션이나 싱크 노드들에 비해 현저히 떨어짐을 가정함

-Broadcast Authentication: 브로드캐스트 인증에는 대칭키 방식의 MAC을 사용함 (간단히 μ-TESLA 이나 멀티레벨 μ-TESLA를 가정함)

-Random Deployment: 노드들은 이웃 노드에 대한 배치 정보를 사전에 알지 못한 채 배치됨

-Security & Efficiency: 설계될 스킴은 알려진 공격모델에 대해 안전하고 메모리 면이나 통신 면에서 효율적이어야 함

2.1 노드간 인증을 위한 부트스트래핑 스킴

Chen 등은 멀티캐스트 인증을 위해 센서 노드의 랜덤 배치와 메모리 제약을 감안한 부트스트래핑 스킴을 제안하였다[4]. 부트스트래핑 스킴은 크게 네 단계로 구분되어 있으며 마지막 단계가 끝나면 μ-TESLA와 같은 브로드캐스트 인증 스킴에게 권한을 넘겨준다. 우선 μ-TESLA와 마찬가지로 부트스트래핑 스킴에서도 베이스 스테이션과 노드 사이에 개략적인 시간 동기화기 필요하다. 첫째 단계인 초기화에서는 노드들에게 고유한 식별자(ID)가 부여되고 베이스 스테이션은 랜덤한 값으로 GMK를 선택한다. 그리고 나서 이 둘을 입력하여 얻은 하나의 해시값을 각 노드마다 고유키로서 저장한다. 초기화 과정이 끝나면 브로드캐스트 과정이 이어진다. 먼저 각 노드들은 배치된 다음 사전에 저장된 고유키로 자신들의 해시 체인 commitment를 암호화고 이를 식별자와 함께 이웃 노드들에게 브로드캐스트한다. 대기 단계를 거쳐 약속된 시간이 지나면 베이스 스테이션에

의해 공개된 정보를 이용하여 브로드캐스트단계에서 저장해 놓은 암호화된 데이터를 복호화하여 식별자를 확인 후 commitment를 수락할지 결정한다. 전 과정이 무사히 끝나면 정당한 commitment를 이용해 이웃 노드의 데이터를 인증할 수 있게 된다.

그러나 불행하게도 이들이 제안한 방법은 치명적인 결함이 있다. 우선, 실제 센서 환경을 고려해보면 새로운 노드를 추가해야만 하는 상황을 충분히 가정할 수 있는데 기존 스킴으로는 노드 추가가 사실상 불가능하다. 물론 베이스스테이션이 GMK를 재사용하여 노드를 추가할 수는 있다. 하지만 그렇게 되면 이미 노출된 GMK를 공격자가 도청하여 재사용하는 상황과 정당한 재사용이 구별불가능하게 되어 기존 노드들은 추가되는 노드를 신뢰할 수가 없게 된다. 신뢰할 수 없는 노드의 데이터를 마구잡이로 수용하게 되면 공격자의 악의적인 공격에 쉽게 노출될 수 있다. 또 한 가지 문제점은 초반에 기회를 놓친 노드들은 인증 과정에서 아예 배제되고 시스템에서 탈락하고 만다는 점이다. 이는 불필요한 비용 낭비를 초래한다. 이렇듯, 확장성이 낮고 GMK 재사용 시 시스템 안전에 문제가 발생하며, 초반 노드 손실을 복구할 수 없다는 점 등은 보다 개선된 부트스트래핑 스킴을 절실히 요구한다.

2.2 제안된 스킴의 개요

하나 뿐인 GMK에 대해 새롭게 해시 체인을 구성하고 부트스트래핑 단계에는 멀티 세션을 도입한다. 노드에 저장되는 정보를 세션에 맞도록 재구성하여 부트스트래핑 스킴에 뒤늦게 참여하거나 아예 참여하지 못한 노드들도 브로드캐스트 인증에 참여토록 한다. 제안된 스킴은 GMK재사용을 원천적으로 막고, 초반 탈락했던 노드나 새로운 노드가 참여할 경우 전체 시스템의 안전성을 약화시키지 않는다.

III. 확장성을 제공하는 새로운 부트스트래핑 스킴

3.1 멀티 세션을 이용한 초기화 스킴

제안하는 스킴은 크게 네 단계, 즉, 초기화 단계, 브로드 캐스팅 단계, 대기 단계, 비밀 값 공개 단계를 포함하며 노드 추가나 구제 작업 시 새로운 세션으로 이루어지는 재귀 단계가 더해진다. 먼저 초기화 단계에 베이스 스테이션은 각 센서 노드에 고유한 식별자를 부여하고, 자신이 임의로 선택한 GMK 값으로 길이 n의 해시 체인을 생성한다. GMK에 대한 commitment GMK_0와 노드 ID, 세션 번호에 대한 해시값을 계산하고 이것을 해당 노드에 각각 저장한다. 브로드 캐스팅 단계에서 모든 센서 노드들은 배치된 후, 초기화 단계에서 베이스스테이션으로부터 받은 해시 값을 비밀키로 사용하여 자신의 해시 체인 commitment와, ID, 세션번호를 암호화해 이를 이웃 노드들에게 브로드 캐스팅한다. 이 과정이 끝난 다음 설정된 시간만큼 대기 단계를 거치면 베이스 스테이션은 비밀 값, GMK에 대한 commitment 을 드디어 공개한다. 이제 노드들은 이 값을 이용하여 이전에 받아놓은 자신의 주변 노드들의 암호화된 값을 복호화 하여 그들을 인증할 수 있다.

이제 하나의 세션이 완료된 다음에 새로운 노드가 추가되는 상황을 고려해보자. 베이스 스테이션은 새롭게 추가하려는 노드에 대해 이전 i 번째 세션에서 사용한 GMK_i 대신, GMK_{i+1} 를 사용하여 초기화단계부터 비밀 값 공개 과정까지 비슷하게 수행한다. 각 노드들은 해시 체인을 이용하여 새로운 GMK_{i+1} 를 인증할 수 있다. 프로토콜의 자세한 모습은 다음 그림과 같다.

I. *초기화 단계* (베이스 스테이션)

- 각 노드에 대한 식별자 $ID_1, ID_2, \ldots, ID_s$를 생성하고 부여
- $GMK_n \in_R \{0,1\}^*$에 대한 해시 체인 형성

$$GMK_i = Hash(GMK_{i+1}) \quad (0 \le i \le n-1)$$

- 세션 번호 i에 대해 각 노드별 비밀 키를 계산한 다음 이를 각 노드에 저장

$$K_{ID_s} = Hash(GMK_0 \| ID_s \| i)$$

II. *브로드 캐스팅 단계*

평문 P를 비밀키 K를 이용하여 암호화 하는 것을 E(P,K)라고 했을 때, 각 노드는 자신의 고유한 비밀키 K_{ID_s}를 이용하여 다음의 암호화 과정을 수행한다.

$$E(FID_s \| ID_s \| i, K_{ID_s})$$

여기서, FID_s 는 각 노드가 마이크로 테슬라 등의 인증 방법을 사용하기 위해 전달하고자 하는 노드 자신의 해시 체인 commitment이고, i는 세션 번호이다. 각 노드는 이 값을 계산한 다음 이웃 노드들에게 브로드 캐스팅한다.

III. *대기 단계*

설정된 시간만큼 대기한다. (브로드 캐스팅이 완료될 만큼의 시간에 준함)

IV. *비밀 값 공개 단계*

베이스 스테이션

GMK_0 를 모든 노드들에게 브로드 캐스트 한다.

노드

자신과 이웃 노드의 ID, GMK_0를 이용하여 다음 값들을 계산할 수 있다.

$$K_{ID_s} = Hash(GMK_0 \| ID_s \| i)$$

또한 노드는 주변 노드들로부터 받은 값을 상대방의 ID를 이용하여 복호화한 다음 정당성을 확인할 수 있다.

$$D(E(FID_s \| ID_s \| i, K_{ID_s}), K_{ID_s})$$

정당한 것으로 확인되면 해당 노드의 FID_s 를 마이크로 테슬라 인증에 사용될 commitment로 받아들인다.

그림 1. i번째 세션에 대한 초기화 프로토콜

i번째이 끝난 후 노드 추가 시 다음 과정을 수행한다.

V. 노드 추가 단계

i+1번째 세션에 대해 다음 값을 계산 후 노드에 저장

$$K_{ID_s} = Hash(GMK_{i+1} \| ID_s \| i+1)$$

위의 II.브로드 캐스트 단계에서 노드는 다음과 같이 암호화 한 다음 추가노드 자격으로 자신이 배치된 위치에서 이미 인증 과정을 끝낸 주변노드들에게 다음을 브로드 캐스팅한다.

$$E(FID_s \| ID_s \| i+1 , K_{ID_s})$$

베이스 스테이션이 대기 단계 거친 후 GMK_{i+1}를 공개하면 추가된 노드의 이웃노드들은 추가된 노드들을 다음 값을 계산하여 인증할 수 있다.

$$K_{ID_s} = Hash(GMK_{i+1} \| ID_s \| i+1)$$

$$D\ (\ E(FID_s \| ID_s \| i+1 , K_{ID_s}),\ K_{ID_s})$$

정당성이 확인되면 FID_s를 신규 노드의 해시 체인 commitment로 받아들인다.

그림 2. i+1 번째 세션에서의 노드 추가

3.2 초기화 과정에서 배제된 노드 구제 방안

i번째 세션에서 모든 노드들에 대해 위 프로토콜의 I.초기화 단계에서 베이스 스테이션은 해시체인의 연속된 α개의 값

$$GMK_0, GMK_1, \ldots, GMK_{\alpha-1}$$

를 이용하여 α개 만큼의 비밀 키를 다음처럼 계산한 다음 각 노드에 저장한다.

$$K_{ID_s,0} = Hash(GMK_0 \| ID_s \| i+1)$$

$$K_{ID_s,1} = Hash(GMK_1 \| ID_s \| i+1)$$

...

$$K_{ID_s,\alpha} = Hash(GMK_{\alpha-1} \| ID_s \| i+1)$$

노드들은 배치된 후 먼저 $K_{ID_s,0}$를 이용하여 i번째 세션에 대한 초기화 스킴을 정상적으로 수행한다. 이 과정에서 발생한 낙오 노드는 $K_{ID_s,0}$대신 $K_{ID_s,1}$를 이용하여 II.브로드 캐스팅 단계를 수행하도록 한다. IV.비밀 값 공개단계에서 베이스 스테이션은 GMK_1를 공개한다. 이런 방법으로 i번째 세션에서 총 α번 노드 구제가 가능하다. 계속되는 i+1번째 세션에서는 베이스 스테이션이

$$GMK_\alpha, GMK_{\alpha+1}, \ldots, GMK_{2\alpha-1}$$

를 사용해 초기화 프로토콜을 진행할 것이다.

IV. 안전성 및 효율성 분석

i번째 세션에서 공격자는 단계 II에 브로드 캐스팅 되는 값 $K_{ID_s} = Hash(GMK_i \| ID_s \| i)$ 를 도청 한다 해도 GMK_i를 모르기 때문에, 새로운 정당한 해시 값을 만들지 못하고 따라서 베이스 스테이션이나 정당한 노드로 가장할 수 없다. 또한,

$$GMK_i = Hash(GMK_{i+1}) \quad (0 \le i \le n-1)$$

에서 공격자는 베이스 스테이션이 단계 IV에서 공개한 GMK_i를 알게 되더라도 해시 체인의 다음 값인 GMK_{i+1}을 계산할 수 없으므로 i+1번째에서도 여전히 정당한 노드나 베이스 스테이션으로 가장할 수 없다.

제안된 스킴은 베이스 스테이션의 경우 길이 n의 해시체인 연산과 노드 수만큼의 해시 값 계산을 부담한다. 노드 측면에서 살펴보면 대칭키 암호화 연산 1번, 해시와 대칭키 복호화 연산이 각각 이웃 노드 수만큼 필요하다.

V. 결론 및 향후 연구 방향

제안된 스킴은 센서네트워크 환경에서 인증을 위해 일반적으로 널리 사용되는 마이크로 테슬라와 같은 브로드캐스트 인증방법 등을 지원하기 위한 초기화 스킴으로서, 멀티 세션과 α개의 해시 체인 값을 이용한 노드 추가 및 자가 구제가 가능한 최초의 초기화 스킴이다. 노드 추가가 안전하고 효율적으로 이루어지며 초기화 과정에 참여하지 못한 노드를 간단히 구제하여 노드 손실로 인하 비용 낭비를 막는다. 세션에 사용된 비밀 값들이 암호학적 해시 체인으로 연결되어 이전 세션에서 들어난 비밀 값들이 다음 세션의 안전성에 영향을 미치지 않는다. 외부 공격자는 어떠한 세션에서도 정당한 노드나 베이스스테이션으로 위장하지 못한다.

[참고문헌]

[1] A. Perrig, R. Szewczyk, V. Wen, D. Culler, and J.D. Tygar. "SPINS: Security Protocols for Sensor Networks.", *Wireless Networks*, Vol. 8, pp. 521-534, Sept. 2002.

[2] H. Chen, A. Perrig, and D. Song, "Random key distribution schemes for sensor networks", in *Proc. IEEE Symposium on Security and Privacy*, pp. 197-215. May 2003.

[3] D. Liu and P. Ning, "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks.", in *Proc. Annual Network and Distributed System Security Symposium*(NDSS), pp. 263-276, Feb, 2003.

[4] W. Chen and Y. Chen, "A Bootstrapping Scheme for Inter-Sensor authentication within Sensor Networks.", in *IEEE Communication Letters*, Vol. 9, NO. 10, October, 2005.