# 센서 네트워크에서 ID기반 인증서를 이용한 Sybil 공격 탐지 기법 설계

정은희* · 이병관**

*강원대학교, **관동대학교

# A Design of Sybil Attack detection technique using ID-based certificate on Sensor network

Eunhee Jeong* · Byungkwan Lee**

*Kangwon National University, **Kwandong University

E-mail : *jeongeh@kangwon.ac.kr, **bklee@kwandong.ac.kr

## 요 약

본 논문에서는 센서 네트워크에서 ID 기반 인증서를 이용한 Sybil 공격 탐지 기법을 제안함으로 첫째, 효율적인 키 분배로 키 분배시 발생할 수 있는 Broadcast Storm 해결 방안을 제시하였다. 둘째, 키 체인 기법으로 센서 네트워크의 노드의 키를 생성하고, 주기적으로 변경하도록 설계함으로써 재전송 공격을 방지하였다. 셋째, 해시 함수를 사용하여 센서 노드의 신분을 인증함으로써, 센서 노드의 메모리 사용량을 극대화시켰으며, 통신 오버헤드를 줄였다. 끝으로, ID 기반 인증서를 통해 Sybil 공격을 탐지할 수 있도록 하였다. 따라서, 본 논문에서는 제안한 ID 기반 인증서를 이용한 Sybil 공격 탐지 기법은 센서 네트워크의 환경에서의 에너지 효율성과 안정성을 동시에 제공하였으며, 센서 네트워크를 통해 제공되는 정보를 신뢰할 수 있도록 하였다.

## ABSTRACT

This paper proposes a technique of sybil attack detection using an ID-based certificate on sensor network. First, it can solve the broadcast storm problem happening when keys are distributed to sensor nodes. Second, it prevents the replay attack by periodically generating and changing the keys of sensor nodes with Key-chain technique. Third, it authenticates sensor node's ID using hash function. So, it maximizes sensor node's memory usage, reduces communication overhead. Finally it detects Sybil attack through ID-based certificate. Therefore, the proposed technique of Sybil attack detection using ID-based certificate consider simultaneously energy efficiency and stability on sensor network environment, and can trust the provided information through sensor network

## 키워드

Sybil attack, ID기반 인증서, MHT(Merkle Hash Tree), 체인 키

## Ⅰ. 서 론

센서 네트워크는 초소형, 빈번한 데이터 이동, 제한적인 계산 및 저장 능력, 배터리 전력의 한계를 특징으로 갖는 센서 노드들로 구성되며, 센서 노드들의 잦은 토폴로지 변경과 노드 간 통신을 위해 브로트캐스트 방식을 사용하므로 센서 노드의 동작은 항상 보장되지 않는다. 특히, 센서 노드의 하드웨어적인 제약 및 무선 네트워크 특성으로 인한 Sinkhole, Wormhole 등 라우팅 공격에 취약하다. 따라서 센서 네트워크 환경에서 안전한 데이터 전송 및 개인 정보를 보호할 수 있는 해

결 방안이 필요하다[1].

현재, 공개키 기반 연구, 대칭키 기반의 기법, 사전 키 분배 방식 그리고, 노드 식별자(이하 ID) 기반 암호화 기법의 센서 네트워크에 대한 적용 방안이 연구되고 있다. 이 중에서 센서 네트워크의 노드 ID는 공개된 정보이기에 감청을 통해 쉽게 획득이 가능하다는 점에서 ID 기반 인증 기법은 Sybil Attack과 같은 ID 위장 공격에 취약점을 가지고 있다[2]. 그리고 센서 네트워크의 보안 기법 적용 시 가장 고려되어야 할 사항은 센서 노드의 컴퓨팅 성능이나 배터리 용량과 같은 하드웨어적 제약이다.

본 논문에서는 센서 네트워크를 MHT(Merkle Hash Tree)로 구성하고, 단방향 키 체인 기법으로 각 센서 노드의 키 값을 생성한 후, 센서 노드의 ID와 연접해 센서 네트워크 내에서만 통용되는 인증서를 생성한다. 그리고 이 인증서를 이용해 센서 노드를 검증함으로써 ID 위장공격인 Sybil 공격을 탐지하는 효율적인 Sybil 공격 탐지 기법을 설계하고자 한다.

## II. 관련연구

### 2.1 Merkle 해시 트리

Merkle 해시 트리(Merkle Hash Tree, 이하 MHT)는 해시 함수를 이용해 안전한 인증 기법을 구축하면서 1979년 Merkle에 의해 소개되었다[3]. 그림 1에서처럼, 네 개의 leaf 노드의 값은 $i=1,2,3,4$일 때 단방향 해시함수 $h()$을 이용한 데이터의 해시 값인 $h(n_1)$, $h(n_2)$ ,$h(n_3)$, $h(n_4)$이다. 그리고 내부 노드 A의 값은 자식 노드인 $h(n_1)$와 $h(n_2)$의 해시 값을 해시한 $h_a=h(h(n_1)\|h(n_2))$이며, 루트 노드의 값 또한 A와 B의 해시 값을 해시한 $h_r=h(h_a\|h_b)$이 된다. 이때 $h_r$는 아주 작은 양의 보조 인증 정보인 AAI(Auxiliary Authentication Information, 이하 AAI)의 결합으로, $n_1$, $n_2$, $n_3$, $n_4$의 데이터 값 중 일부분을 인증하기 위한 완전한 트리로 사용된다.

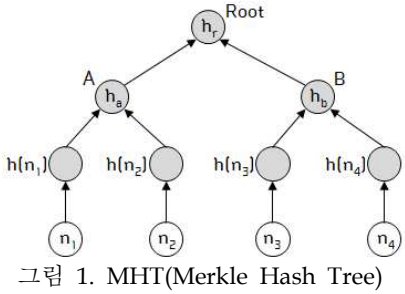


그림 1. MHT(Merkle Hash Tree)

본 논문에서는 센서 네트워크를 MHT 형태의 센서 네트워크로 모델링하여 각 센서 노드의 ID와 체인 키 기법으로 생성된 키 값을 이용해 각 센서 노드의 ID의 인증서를 생성하여 각 센서 노드의 신분을 인증함으로써 Sybil 공격을 탐지하고자 한다.

### 2.2 Sybil Attack

Sybil 공격은 한 노드가 자신의 식별자(identity)로 여러 개의 식별자를 네트워크에서 사용하는 것이다.

그림 2는 위치기반 라우팅 프로토콜에 대해 네트워크를 단절시키기 위한 Sybil 공격을 설명한 것이다. 예를 들어, 어떤 악의적인 노드 A가 A1, A2, A3 세 개의 식별자를 제시하는 경우, 이를 오인한 노드 B는 노드 C까지의 경로로 노드 A3을 선택하여 메시지를 전송한다. 그러나 노드 A3은 존재하지 않는 노드이므로 메시지는 실제로 C에게 전달되지 못하게 된다.

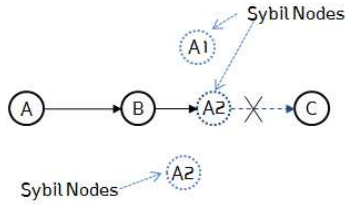


그림 2. 위치기반 라우팅 프로토콜에 대한 Sybil 공격의 개념

## III. Sybil 공격 탐지 기법 설계

본 논문의 센서 네트워크 구조는 MHT 형태로 설계하고, 센서 네트워크 구조 내의 각 노드들은 체인 키 생성 기법으로 각 노드의 키를 생성한 후, 체인 키와 각 노드의 ID, 부모노드 ID로 ID 기반 인증서를 생성한다. 그리고 이 인증서로 센서 노드의 신분을 확인함으로써 Sybil 공격을 탐지하고자 한다.

본 논문에서 설계하는 MHT 형태의 센서 네트워크 구조는 그림 3과 같다.

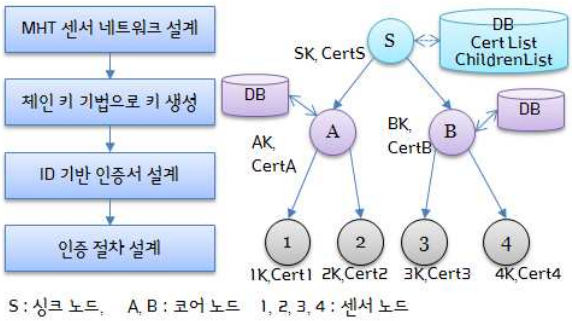


그림 3. 센서네트워크 설계 및 ID기반 인증서 설계 절차

### 3.1 키 설계

본 논문에서는 단방향 키 체인을 이용해 센서 네트워크의 각 노드에 대한 키 값을 생성한다. 이 키는 Seed 값 선정에 따라 각 노드의 키 값이 다르게 생성되므로, 주기적으로 Seed 값을 변경함으로써 키 값을 주기적으로 변경시킬 수 있도록 설계하여 키 값 노출에 대비한다.

싱크노드는 MHT 형태의 센서 네트워크의 모든 코어 노드와 센서 노드를 관리하는 매니저 역할을 담당하고, 각 노드의 키를 생성하도록 설계한다. 이때, 키 생성은 체인 키 기법을 사용하며, 키의 시작은 싱크노드로부터 시작된다.

[1 단계] 싱크노드는 체인 키의 초기값인 SEED값을 선정한 후, 해시 함수로 해시하여 첫 번째 체인키를 생성한다. 이 키는 싱크노드의 키가 된다.

[2 단계] 싱크노드는 자신의 자식노드인 코어 노드의 체인키를 생성한 후, 초기키(Initial Key, 이하 iK)로 암호화하여 코어 노드에 전달한다.

[3 단계] 코어노드는 자신의 자식노드인 센서 노드의 체인키를 생성한 후, 초기키 iK로 암호화하여 센서 노드에 전달한다.

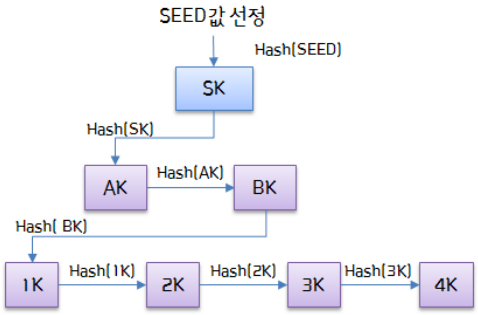


그림 4. 키 생성 절차

이렇게 생성된 각 노드의 체인키는 각 노드의 고유 ID와 연접하여 인증서를 생성하는데 사용된다.

### 3.2 ID 기반 인증서 설계

센서 노드는 ID와 키 값, 그리고 부모 노드의 ID를 결합해 인증서를 생성한다. 그리고 이 인증서를 이용해 Sybil 공격을 검출 하도록 설계하였다. ID 기반 인증서 생성 과정은 다음과 같으며, 그림 5는 각 노드의 키 값과 노드 ID, 부모 ID를 이용한 인증서 생성 과정을 설명한 것이다.

[1 단계] 싱크노드는 코어노드의 체인키를 생성하여 초기키 iK로 암호화하여 코어노드에 전송한다.

[2 단계] 코어노드는 iK로 복호화한 후, 부모노드인 싱크노드의 ID와 자신의 ID, 그리고 체인키를 연접하여 코어노드의 인증서를 생성한다.

[3 단계] 싱크노드 또한 자신의 ID, 자식노드인 코어노드의 ID, 그리고 코어노드의 체인키를 연접하여 코어노드의 인증서를 생성한 후, 싱크노드의 DB에 저장한다.

[4 단계] 코어노드는 자식노드인 센서노드의 체인키를 생성한 후, 초기키 iK로 암호화한 후 센서노드에 전달한다.

[5 단계] 센서노드는 초기키 iK로 암호화한 후, 부모노드인 코어노드의 ID, 자신의 ID, 그리고 자신의 체인키를 연접하여 센서노드의 인증서를 생성한다.

[6 단계] 코어노드는 자신의 ID, 자식노드인 센서노드의 ID, 그리고 자식노드의 체인키를 연접하여 센서노드의 인증서를 생성한 후, 그 인증서를 싱크 노드의 DB에 전달한다.

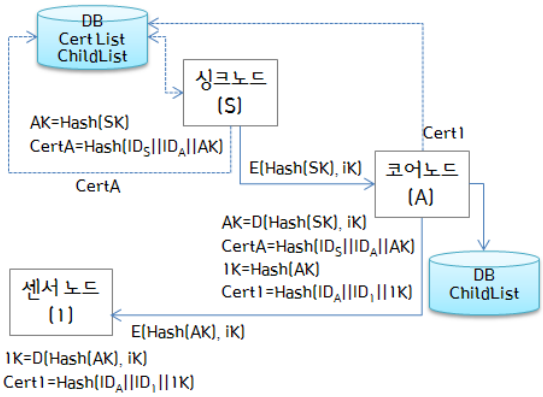


그림 5. 인증서 생성 흐름도

### 3.3 ID기반 인증서 검증 절차 설계

센서 네트워크를 구성하고 있는 센서 노드 1이 센서노드 2의 ID기반 인증서 검증 과정을 단계별로 살펴보면 다음과 같다.

[1 단계] 센서노드 1는 센서노드 2에 정보를 전송하기 전에 센서노드2의 신분확인을 요청한다.

[2 단계] 센서노드 2는 자신의 ID와 인증서인 Cert2, 부모노드 ID를 기본키 iK로 암호화하여 센서노드 1에 전송한다.

$$E(ID_2, ID_A, Cert2, iK)$$

[3 단계] 센서노드 1은 수신한 암호문을 기본키 iK로 복호화한 후, 센서노드 2의 ID와 인증서 Cert2를 부모 노드인 A에게 전달한다.

$$D(E(ID_2, ID_A, Cert2, iK),iK)$$

[4 단계] 부모노드 A는 센서노드 2가 자신의 자식노드인지를 확인한 후, 자신의 자식노드이면, 센서노드2의 인증서와 코어노드 A의 ID를 기본키 iK로 암호화하여 싱크노드 S에 전송한다.

$$E(ID_2, ID_A, Cert2, iK)$$

[5 단계] 싱크노드 S는 수신한 암호문을 기본키 iK로 복호화한 후, 코어노드 A가 자신의 자식노드인지를 확인하고, 자식노드이면 요청한 센서노드2의 신분을 확인한다. 그리고 그 결과를 코어노드 A에 전달한다.

$D(E(ID_2, ID_A, Cert2, iK),iK)$

[6 단계] 코어노드는 싱크노드로부터 수신한 메시지를 센서노드 1에게 전달한다.

## Ⅳ. 분석

### 4.1 보안 분석

센서 네트워크는 가짜 라우팅 정보를 제공하고, 라우팅 프로토콜을 조작함으로써 쉽게 라우팅 공격에 대한 위협을 받을 수 있다. 즉, 수신된 라우팅 메시지를 변경 또는 재전송하여 라우팅을 교란함으로써 라우팅 루프의 생성, 전송지연 등을 야기 시킬 수 있다.

본 논문에서 제안한 기법은 센서 네트워크의 소그룹을 형성하는 동안 안전하다는 가정 하에 이뤄지고, 메시지를 전송하기 전에 소그룹이 먼저 형성한 후에, 체인키 기법으로 키를 생성하므로 라우팅 공격은 아무런 효력을 발휘할 수 없다.

Sybil 공격과 같이 ID를 변경하여 메시지를 보낸다고 하더라도 체인키 기법으로 생성된 키 값과 각 노드 ID, 부모 노드 ID로 생성된 각 노드의 인증서로 센서 노드의 신분을 확인하거나, 자식노드인지를 검증한 후에 응답 메시지를 전송하기 때문에 Sybil 공격을 검출할 수 있다.

### 4.2 센서 노드의 오버헤드 분석

본 논문에서 제안하는 ID기반 인증서를 이용한 Sybil 공격 탐지 기법은 센서 노드에 해시 값 생성을 위한 해시 함수를 저장해야 한다. 일반적으로 SHA-1 해시 함수의 경우 코드 저장 공간은 410byte가 필요하다[5]. 이것은 센서 노드가 충분히 저장할 만한 공간이므로 센서 네트워크 메모리 사용량에 부담을 주지 않는다. 또한, 평균적으로 SHA-1 해시함수의 경우 128bit 스트링으로 해시하기 위해서 단지 2 msec 시간이 걸린다. 이는 센서 노드를 위한 16-bit single ship 마이크로프로세서 M16을 기반으로 계산한 것이다[5]. 이 결과로 보아 해시 함수를 사용하는 것이 센서 노드의 계산적 부담감을 거의 주지 않는 것을 알 수 있다.

## Ⅴ. 결 론

본 논문에서는 ID 기반 인증서를 이용한 Sybil 공격 탐지 기법을 설계하여 무선 센서 네트워크의 센서 노드의 제한점들을 다음과 같이 해결하였다.

첫째, 효율적인 키 분배를 위해 브로드캐스팅 메시지를 줄이기 위해, 센서 네트워크의 모든 노드에게 브로드캐스팅 하는 것이 아니라, 싱크 노드는 코어 노드에게만 기본키로 암호화하여 메시지를 전송하도록 하여 데이터 중복을 줄이고, 키 분배시 발생할 수 있는 Broadcast Storm 해결 방안을 제시하였다.

둘째, 키 분배에는 체인키 기법을 사용하여 센서 네트워크의 노드의 키를 생성하도록 하고, 이 키를 활용해 Sybil Node를 검출 할 수 있도록 설계하였다.

셋째, 센서 네트워크 내의 센서 노드의 신분을 인증하는데 해시 함수를 사용하여 센서 노드의 메모리 사용량과 계산에 대한 부담감을 줄여 메모리 사용량을 극대화 시켰다.

따라서, 본 논문에서는 제안한 기법은 해시 함수를 사용하여 센서 네트워크의 환경에서의 에너지 효율성과 안정성을 동시에 고려하였으며, ID 기반 인증서를 통해 센서 네트워크를 통해 제공되는 정보를 신뢰하고 동시에 개인의 프라이버시를 보장 받을 수 있도록 하였다.

## 참고문헌

[1] C. Karlof, D. Wagner, "Secure routing in wireless sensor networks : attacks and countermeasures", IEEE International Workshop on Sensor Network Protocol and Applications, 2003.

[2] 나상호, “센서네트워크를 위한 안전한 아이디 기반 위임인증 기법과 PMIPv6을 활용한 안전한 이동성 지원방안”, 경희대학교 일반대학원 석사논문, 2010

[3] R. Merkle, “protocols for public key cryptosystems,”in Proc. SP, Oakland, CA, Apr. 1980, pp. 122– 34.

[4] 권창영, 김경신, 원동호, "ID를 이용한 암호시스템 고찰", 통신정보보호학회지, 제4권 제1호, pp.20-29, 1994

[5] Qiang Huamg, Johnas Cukier, Hisashi Kobayashi, Bede Liu, and Jinyun Zhang, “Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks,” Workshop on Wireless Sensor Networks and Applications(WSNA), 2003

[6] 후엔누엔, 허의남, “무선 센서 네트워크를 위한 신뢰성 있는 2-모드 인증 프레임워크”, 인터넷정보학회논문지, 제10권 제3호, pp.51-60, 2009