# 사물인터넷을 위한 타임스탬프 기반 해시 체인 인증 기법

윤준호*, (교신저자)김현성*,**
*경일대학교, **말라위대학교
*yoonjunho62@gmail.com, **kim@kiu.ac.kr

# Hash Chain Authentication Scheme based on Timestamp over Internet of Things

Junho Yoon*, (Corresponding iuthor)Hyunsung Kim*,**
*Kyungil University, **University of Malawi

요 약

오늘날의 인터넷은 사물에서도 쓰일 정도로 발전했지만 그만큼 다양한 보안 및 프라이버시 위협의 노출도는 증가하였다. 본 논문에서는 Lee와 Lee가 제안한 사물인터넷을 위한 해시 체인 기반 센서 상호 인증 기법이 난수 생성기를 필요로 하는 문제점을 도출한다. 특히, 이를 해결하기 위한 타임스탬프 기반의 해시 체인 인증 기법을 제안한다. 보안 분석을 통해 본 논문에서 제안한 기법의 안전하고 사물인터넷 환경에 적합함을 보인다.

## Ⅰ. 서 론

사물인터넷은 점차 발전하여 오늘날에서는 주변에서도 쉽게 찾아볼 수 있다. 하지만 사물에도 인터넷이 연결되면서 동시에 여러 위협으로부터 그대로 노출되었다[1-3]. 이러한 위협을 줄이기 위해 사물인터넷에 대한 보안책이 마련되어야 한다. 최근 사물인터넷을 위한 여러 보안 기법들이 제안되고 있지만 본 논문에서는 논문 [4]에서 Lee와 Lee가 제안한 사물인터넷을 위한 해시 체인 기반 센서 상호 인증 기법의 개요를 설명하고 이를 보완한 타임스탬프 기반 해시 체인 인증 기법에 대해 제안하고 제안한 내용의 안정성 분석을 제시한다.

## Ⅱ. 해시 체인 기반 센서 상호 인증 기법 개요

Lee와 Lee는 사물인터넷을 위한 해시 체인 기반 센서 상호 인증 기법을 제안하였다[4]. 본 장에서는 Lee와 Lee가 제안한 인증 기법에 대해 소개한다. 그림 1에서 제시한 바와 같이 Lee와 Lee가 제안한 기법은 소형 센서를 기반으로 하는 사물인터넷 환경에서 S/KEY 프로토콜을 이용해 인증한다. 이 기법은 $BS$와 센서 노드 그리고 이들의 중간 역할을 하는 $MN$으로 구성된 총 세 네트워크 참여자가 있다. 해시 체인에서 $V_n$을 S/KEY로 사용하고 생성한 난수를 배타적 논리합 (Exclusive or)으로 추론한다. 하지만 이 기법엔 난수가 노출되면 챌린지가 쉽게 도출될 수 있는 취약점이 존재한다.

표 1. 기호 정의

| 기 호 | 의 미 |
|---|---|
| $ID_i$ | 센서 노드 $SN_i$의 식별자 |
| $h()$ | 안전한 해시 함수 |
| $E_k()$ | 키 $k$를 이용한 대칭키 암호 알고리즘 |
| $D_k()$ | 키 $k$를 이용한 대칭키 복호 알고리즘 |
| $K_i$ | 서버가 발급하는 $i$의 비밀키 |
| $SEED$ | 해시체인 초기 값 |
| $V_i$ | 해시체인의 $i$번째 해시값 |
| $T_i$ | $i$번째 시점의 타임 스탬프 |
| $\triangle T$ | 허용 가능한 네트워크 지연 시간 |
| $R_i$ | $i$번째 인증에서의 난수 |
| $N_i$ | $BS$에 저장되어 있는 $i$번째 해시값 |

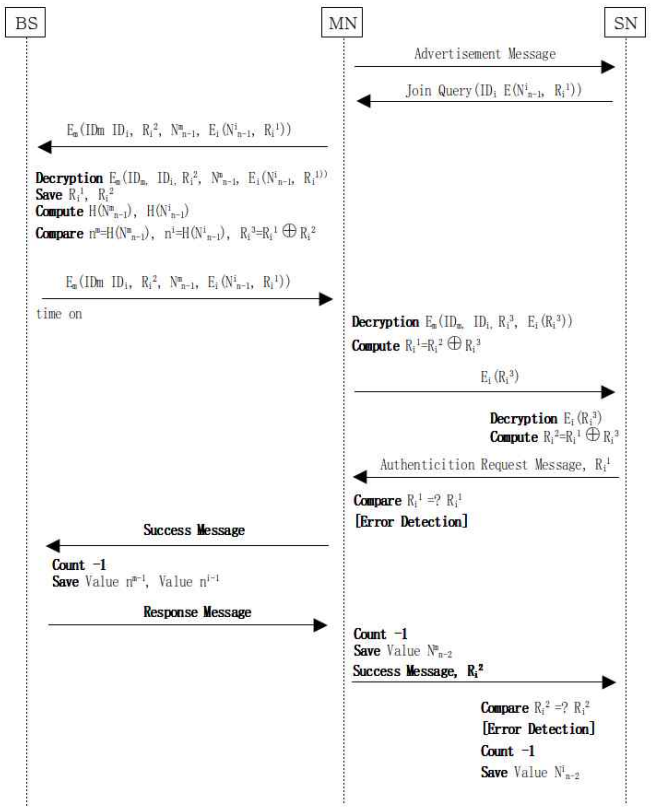


그림 1. Lee와 Lee의 인증 기법 [4]

## Ⅲ. 타임스탬프 기반 해시 체인 인증 기법

본 장에서는 타임스탬프를 기반으로 한 해시 체인 인증 기법을 제안한다. 네트워트 환경은 $BS$, 센서 노드 $SN_i$, 그리고 이들의 중간에서 통신을 중재하는 $MN$으로 구성된다. 제안한 기법은 등록 단계와 인증 단계로 구성된다. 표 1은 본 논문에서 사용하는 기호를 정의한다.

3.1 중간 노드 등록단계

중간 노드 $MN$이 네트워크에서 서비스를 제공받기 전에 $BS$를 통해 이 단계를 수행한다. 이 단계는 오프라인으로 진행된다.

단계 1: $BS$는 $MN$을 위한 식별자 $ID_m$와 비밀키 $K_m$을 선택한다.

단계 2: $BS$는 $K_m$과 $MN$의 서비스와 연계된 센서노드들 $SN$의 $ID_i$를 $MN$의 메모리에 저장한다. 또한, $BS$는 $ID_m$와 $K_m$을 자신의 데이터베이스에 저장한다. 마지막으로 $MN$과 시간을 동기화한다.

3.2 센서 노드 등록단계

센서 노드 $SN_i$가 배치되기 전에 $BS$는 이 단계를 진행한다. 이 단계는 오프라인으로 진행된다.

단계 1: $BS$는 $SN_i$를 위한 식별자 $ID_i$와 비밀키 $K_i$를 선택한다.

단계 2: $BS$는 $SN_i$의 인증 가능 횟수 $n$을 결정하고 해시체인의 초기 값 $SEED$를 생성한다. $V_1=h(SEED)$, $V_2=h(V_1)$, …, $V_i=h(V_{i-1})$, … $V_n=(V_{n-1})$ 연산을 통해 해시체인을 생성한다.

단계 3 : $BS$는 $K_i$와 $\{V_n, V_{n-1}, \cdots, V_1\}$으로 구성된 해시체인을 $SN_i$의 메모리에 저장한다. $BS$는 $\{ID_i, K_i, V_n\}$를 데이터베이스에 저장하고 $N_1=V_n$으로 설정한다. $SN_i$와 시간을 동기화한다.

3.3 인증단계

$SN_i$는 해시체인을 이용한 인증을 수행한다. 즉, $SN_i$는 $BS$와 $n$번의 인증 서비스를 제공받을 수 있다. 인증 과정은 그림 2와 같고 상세한 $SN_i$의 $i$번째 인증 과정은 다음과 같다.

단계 1: $SN_i$는 $MN$에게 인증 요청 메시지를 전송한다. $MN$은 메시지를 확인하고 정보 요청 메시지를 $SN_i$에게 전송한다.

단계 2: $SN_i$는 현재 타임스탬프 $T_{SN1}$와 세션 검증자 $V_{n-i}$를 이용하여 $C^S_{n-i}=E_i(V_{n-i}, T_{SN1})$를 계산하고, 인증 요청 메시지 $\{ID_i, C^S_{n-i}, T_{SN1}\}$를 $MN$에게 전송한다.

단계 3: $MN$는 자신의 타임스탬프 $T_{m1}$를 통해 $T_{m1}-T_{SN1} < \triangle T$ 가 성립하지 않으면 세션을 종료한다. 조건이 성립하면 $MN$은 $C^M_{n-i}=E_m(ID_i, C^S_{n-i}, T_{m1})$를 계산하고 $\{ID_m, C^M_{n-i}, T_{m1}\}$를 $BS$에게 전송한다.

단계 4: $BS$은 자신의 타임스탬프 $T_{b1}$를 통해 $T_{b1}-T_{m1} < \triangle T$ 가 성립하는지 확인한다. $BS$은 $K_m$를 이용하여 $\{ID_i, C^S_{n-i}, T_{m1}\}=D_m(C^M_{n-i})$를 계산하고, $ID_i$의 $K_i$를 이용하여 $\{V_{n-i}, T_{SN1}\}=D_i(C^S_{n-i})$를 계산한다. $BS$은 $h(V_{n-i})$를 연산하여 자신의 데이터베이스에 저장되어 있는 $N_i$와 일치하지 않으면 세션을 종료한다. 검증이 성공적이면 BS는 $N_i=V_{n-i}$를 계산한 후, 현재 타임스탬프 $T_{b2}$로 $C^B_{n-i}=E_m(E_i(T_{b2}))$을 연산하고 $\{ID_b, C^B_{n-i}, T_{b2}\}$를 $MN$에게 전송한다.

단계 5: $MN$는 자신의 타임스템프 $T_{m2}$를 통해 $T_{m2}-T_{b2} < \triangle T$ 를 체크하고 조건이 만족하지 않으면 세션을 종료한다. 조건이 성립하면 $C^M_{n-i}=E_i(T_{b2})=D_m(C^B_{n-i})$를 계산하여 $SN_i$에게 $\{ID_m, C^M_{n-i}, T_{m2}\}$을 전송한다.

단계 6: $SN_i$는 자신의 타임스템프 $T_{SN2}$를 통해 $T_{SN2}-T_{m2} < \triangle T$ 가 만족하지 않으면 세션을 종료한다. 조건이 성립하면 $SN_i$는 $T_{b2}=D_i(C^M_{n-i})$를 계산하고 계산한 $T_{b2}$와 전달받은 $T_{m2}$가 같은지 검증하고 검증이 실패하면 세션을 종료한다. 그렇지 않다면 인증 성공을 확인한다.

## IV. 보안성 분석

본 장에서는 제안한 인증 기법의 보안성 분석을 제시한다. 재전송 공격은 A가 B에게 메시지를 전송할 때 제 3자인 C가 메시지를 가로채 C가 A로 위장하여 B에게 메시지를 보내는 공격이다. 재전송 공격을 방지하기 위해 제안한 기법은 네트워크 참여자가 타임스탬프를 이용하였다. 특히, 대칭키 암호를 통해 적법한 키를 알고 있는 네트워크 참여자만 세션 신선성을 제공하는 데이터를 통한 값을 생성할 수 있고 이에 대한 응답 메시지를 생성할 수 있다. 특히, Lee와 Lee의 인증 기법에서는 난수 생성기를 통해 생성된 세션 난수가 노출될 경우 챌린지가 도출될 수 있는 취약점이 존재했다. 하지만 제안한 기법은 난수 생성기에 의존하지 않고, 사물인터넷 환경에 적합한 타임스탬프를 이용함으로서 다양한 사물인터넷 응용에 적용할 수 있을 것으로 기대된다.

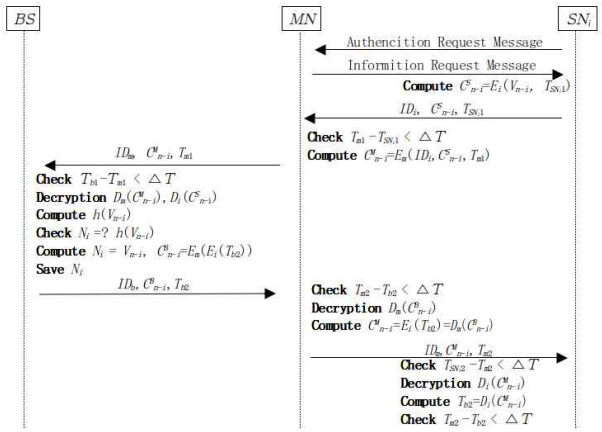


그림 2. 제안한 인증 기법의 인증단계

## V. 결론

본 논문은 사물인터넷을 위한 타임스탬프 기반의 해시 체인 기법을 제안하였다. 해시 체인을 이용함으로서 사물인터넷의 연산 오버헤드를 줄이고, 타임스탬프를 활용함으로서 세션의 신선성을 제시할 수 있어서 다양한 사물인터넷을 위한 보안의 기반 구조로 활용될 수 있을 것이다.

## ACKNOWLEDGMENT

This work was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

## 참 고 문 헌

[1] H. Kim, “Data Centric Security and Privacy Research Issues for Intelligent Internet of Things,” *ICSES Interdisiplinary Transactions on Cloud Computing, IoT, and Big Data*, pp. 1-2, 2017.

[2] B. Kapito, M. Nyirenda, H. Kim, “Privacy-Preserving Machine Authenticated Key Agreement for Internet of Things, International Journal of Computer Networks & Communications, vol. 13, no. 2, pp. 99-120, 2021.

[3] K. H. Han, S. H. Lee, “A Study on the Security Threats of IoT Devices Exposed in Search Engine”, *The Transactions of the Korean Institute of Electrical Engineers*, vol. 65, no. 1, pp. 128-134, 2016.

[4] G. H. Lee, J, S, Lee, “Mutual Authentication Method for Hash Chain Based Sensors in IoT Environment”, *Journal of the Korea Acadmia-Industrial cooperation Society*, vol. 19, no. 11, pp. 303-309, 2018.