https://doi.org/10.7236/JIIBC.2019.19.5.9
JIIBC 2019-5-2

M2M 통신 환경에서 해시 충돌을 이용한 그룹키 생성 및 교환 기법 연구

A Study on Group Key Generation and Exchange using Hash Collision in M2M Communication Environment

송준호[*], 김성수[**], 전문석[***]

Jun-Ho Song[*], Sung-Soo Kim[**], Moon-Seog Jun[***]

요 약 IoT 환경이 보편화됨에 따라 사람의 직접적인 개입 없이 물체와 물체 사이의 통신 환경을 구축하는 M2M 환경의 안전성이 중요시 되고 있다. 무선 통신 환경의 특성상 데이터 노출, 위조, 변조, 삭제 및 개인 정보 보호와 같은 다양한 측면에서 보안 위협에 노출 될 가능성이 존재하고, 안전한 통신 보안 기술이 중요한 요구 사항으로 다뤄진다. 본 논문에서는 해시충돌을 이용하여 기존 'M2M 통신 환경에서 트랩도어 충돌 해쉬을 이용한 그룹키 생성 및 교환 기법' 연구의 한계점을 확인하고, 스니핑 공격에 안전한 그룹간에 키를 생성하고 이를 세션 키와 교환하는 기법과 그룹 키 생성 후에 장치와 게이트웨이의 인증을 확인하는 메커니즘을 제안한다. 제안 된 방법은 충돌 메시지 및 충돌 해시의 특이성을 이용하여 그룹 통신 섹션의 위장 공격, 중간자 공격, 재전송 공격과 같은 공격 저항을 가지며, 해시충돌의 취약점에 대해 안전성을 증명하는 기법이다.

Abstract As the IoT environment becomes more popular, the safety of the M2M environment, which establishes the communication environment between objects and objects without human intervention, becomes important. Due to the nature of the wireless communication environment, there is a possibility of exposure to security threats in various aspects such as data exposure, falsification, tampering, deletion and privacy, and secure communication security technology is considered as an important requirement. In this paper, we propose a new method for group key generation and exchange using trap hash collision hash in existing 'M2M communication environment' using hash collision, And a mechanism for confirming the authentication of the device and the gateway after the group key is generated. The proposed method has attack resistance such as spoofing attack, meson attack, and retransmission attack in the group communication section by using the specificity of the collision message and collision hash, and is a technique for proving safety against vulnerability of hash collision.

Key Words : Group Key, IoT, M2M, Trapdoor Collision Hash

[*]정회원, 숭실대학교 일반대학원 컴퓨터학과(교신저자)
[**]정회원, 한국정보화진흥원 ICT문화융합본부 책임연구원
[***]정회원, 숭실대학교 일반대학원 컴퓨터학과
접수일자 2019년 8월 2일, 수정완료 2019년 9월 2일
게재확정일자 2019년 10월 4일

Received: 2 August, 2019 / Revised: 2 September, 2019 / Accepted: 4 October, 2019
[*]Corresponding Author: jhsong@soongsil.ac.kr
Dept. of Computer Science and Engineering, Soongsil University, Korea

Ⅰ. 서 론

M2M(Machine-to-Machine) 기술은 사물 간 정보를 수집하고 처리하는 지능형 인프라이다. 유무선 ICT 기술과 결합하여 물체, 환경, 사람 등 다양한 정보를 수집하여 활용한다. 이는 센서 네트워크에서 데이터를 수집, 처리 및 배포하는 서비스와 유사하며, 사람이 개입하지 않아도 장치 자체가 정보를 교환하고 교환한다는 점에서 과거 센서 네트워크 서비스에 비해 향상된 서비스를 제공한다.[1] 또한 LTE, WCDMA, GSM, W-LAN, 이동 통신 및 무선 인터넷, Zigbee 및 Bluetooth와 같은 저전력 통신 기술에도 적용되고 있으며, 다양한 서비스를 제공한다.[2] 그러나 중간자 공격과 재전송 공격과 같은 해킹 공격에 대한 대책이 부족하다.[3] 또한 서비스 환경에 따라 다양한 다양한 제조업체들의 장치가 연결되며 이들 사이의 신뢰성 또한 문제가 된다.[4]

본 논문에서는 다수의 M2M 장치와 oneM2M 환경의 보안을 위한 소수의 게이트웨이 사이에 그룹 키를 생성하는 세션 키 전송 프로토콜을 제안한다. 2 장에서는 기존 프로토콜의 배경과 문제점을 제안하고,[5] 3 장에서 개선 된 기법과 프로토콜을 제안하며 제안 된 프로토콜이 기존의 취약성에 대해 안전하다는 것을 보여준다.

Ⅱ. 관련 연구

본 장에서는 기존 M2M 통신 환경에서 해시 충돌을 이용한 그룹키 생성 및 교환 기법의 기반이 되는 트랩도어 충돌 해시와 기존 연구의 취약점에 대해 설명한다.

1. 트랩도어 충돌 해시

일반적으로 보안 프로토콜에 사용되는 해시 함수는 메시지의 오류 및 변조를 탐지하기 위해 무결성 및 디지털 서명과 함께 사용된다. 트랩도어 충돌 해시 기능은 메시지에 대한 서명이 유효한지 확인하며, 다른 각 서명은 증명할 수 없다.[6]

그러나, 트랩도어 충돌 해시 함수는 발신자와 수신자가 충돌을 발견 할 수 있으므로, 충돌 값을 모르는 다른 사용자는 동일한 트랩도어 충돌 해시 값을 계산할 수 없다.[7]

표 1은 트랩도어 충돌 해시 기능의 보안 요구 사항을 보여 주며 충돌 저항, 해시 결과 값의 무효화, 충돌 확인에 사용되는 비밀 키 숨김 및 비밀 키 노출과 관련이 없는 네 가지 보안 요구 사항을 충족해야 한다.[8]

표 1. 트랩도어 충돌 해시 보안 요구사항
Table 1. Trapdoor Collision Hash Security Requirement

Collision-resistance	There is no efficient algorithm that given only PK, L, m and r, (but not the secret key SK) can find a second pair m, r.
Semantic Security	The chameleon hash value C does not reveal anything about the possible message m that was hashed.
Message Hiding	Assume the recipient has computed a collision using the universal forgery algorithm. By showing the second pair(m', r') without the need to open the original message it may correspond to invalid request.
Key Exposure Freeness	If a recipient with public key PK has never computed a collision under label L, then given C=Hash(PK, L, m, r) there is no efficient algorithm that can find a collision. (a second pair m, r mapping to the same digest C).

각 송신자와 수신자는 사전에 큰 소수 p, g를 공유하고, 개인키 SK와 공개키 PK 쌍, 난수 m과 r을 Z_q^* 상에서 선택하여 이용한다. 트랩도어 충돌 해시 함수는 아래의 연산과정으로 동일한 해시 값을 계산한다.

큰 소수 g, p와 비밀키 x를 이용하여 공개키 y를 구한다.

$$y = g^x \bmod p \,(\text{단}, x \in Z_p^*) \tag{1}$$

초기 난수 m과 r을 생성하여, 식 (2)와 같이 트랩도어 충돌 해시값(C_y)을 계산한다.

$$C_y(m,r) = g^m y^r \bmod p \tag{2}$$

새로운 충돌 메시지 m'은 $C_y(m,r)$와 동일한 충돌 해시 값을 계산하기 위해서는, 새로운 난수 r'과 기존의 충돌 비밀키 $x \in Z_p^*$를 알고 있어야 계산이 가능하다. 동일한 충돌 해시 값을 계산하기 위한 충돌 메시지 m'을 계산한다.

$$m' = m + x(r - r') \tag{3}$$

새로운 충돌 해시값 $C_y(m',r')$는 (m',r')에 대한 충돌 해시값은 첫 난수 (m,r)쌍과 $m' \neq m$일 때, 두 쌍의 메시지와 난수로 생성되는 충돌 해시값은 동일함을 확인할 수 있다.

$$\begin{aligned} C_y(m',r') &= g^{m'} y^{r'} \bmod p \\ &= g^{m+x(r-r')} g^{xr'} \bmod p \\ &= g^m g^{xr} \bmod p \\ &= C_y(m,r) \end{aligned} \tag{4}$$

위와 같이 송수신간에 동일한 충돌 해시 값을 계산하지 못하는 경우 공격으로 간주할 수 있다. 또한 기존의 DSA(Digital Signature Algorithm), RSA와 같은 전통적 서명기법을 사용하므로 보안 프로토콜에 적용하기 쉽다. 하지만 트랩도어 충돌 해시함수는 스니핑 공격에 취약하다. 공격자가 송신자와 수신자 사이에서 m과 r을 획득하고, 이후에 전송되는 새로운 m'과 r'을 획득 한다면, (5)과 같이 비밀키 x를 계산할 수 있다.[9]

$$x = \frac{m - m'}{r - r'} \tag{5}$$

2. 트랩도어 충돌 해시를 이용한 그룹키 생성 및 교환

기존의 연구에서 제안한 그룹키 생성 및 키 교환 기법은 큰 소수 g, p를 이용하여 초기 난수 m과 r을 모든 디바이스로 분배해 충돌 메시지를 생성하고, 디바이스를 인증한다[5]. 이후 계산 가능한 트랩도어 충돌 해시를 이용하여 정상적인 디바이스임을 인증한다. 또한 이미 인증을 완료한 디바이스들은 이를 그룹키로 활용하여 보안 세션을 설립한다.

1) 기존 프로토콜의 파라미터

기존 프로토콜의 디바이스의 요약어는 표 2, 그룹키 생성 및 키교환 프로토콜에 사용하는 파라미터는 표 3과 같다.

표 2. 디바이스 요약어
Table 2. Device Abbreviation

Name	Description
IN	서비스 제공자
MN	게이트웨이(미들 노드)
ASN/ADN	M2M 디바이스

표 3. 트랩도어 충돌 해시 파라미터
Table 3. Trapdoor Collision Hash Parameter

Parameter	Description
g, p	큰 소수
x	비밀키
r_i	Z^*_p 상의 난수
m_i	충돌 메시지
y_i	충돌 해시 공개키
S	전자 서명
ID_i	식별 정보
C_{y_i}	트랩도어 충돌 해시
SK_i	그룹 세션키

2) 사전 단계

M2M 환경에서 정상적인 장치인 ASN/ADN, MN, IN은 EAP-TLS와 같은 기존 무선망의 인증방식으로 인증, 그룹키에 사용하는 값과 식별 정보를 사전에 동의하여 IN으로부터 MN과 ASN, ADN으로 공유한다.

3) 그룹키 생성 및 키 교환

MN_i은 IN으로부터 그룹간의 키로 사용할 최초 난수 m_i와 r_i를 수신한다. 그리고 자신의 비밀키 $x_{i_{mn_i}}$를 선택하고, 난수 $r_{mn_{i+1}}$을 생성하여 충돌 메시지 $m_{mn_{i+1}}$을 계산한다.

공개키 y_{mn_i}와 생성한 난수 $r_{mn_{i+1}}$, 충돌 메시지 $m_{mn_{i+1}}$을 이용하여, 트랩도어 충돌 해시값을 같이 미리 계산한다. 이는 각 ASN, ADN 노드들이 생성한 충돌 해시 값과 동일한 값인지 비교하기 위한 값이다. MN_i의 주변 노드들에 $x_{i_{mn_i}} r_{mn_{i+1}}$값과 생성한 충돌 메시지 $m_{mn_{i+1}}$을 전송한다. $x_{i_{mn_i}} r_{mn_{i+1}}$과 $m_{mn_{i+1}}$값을 수신한 노드들은 고유의 비밀키 $x_{i_{node_i}}$를 생성하고, 충돌 메시지 값을 계산하기 위한 난수 $r_{node_{i+1}}$값을 생성한다.

선택한 비밀키와 생성한 난수로 노드에서 동일한 충돌 해시값을 계산할 수 있는 충돌 메시지 $m_{node_{i+1}}$를 계산한다. 노드들은 자신의 ID_{node_i}와 $m_{node_{i+1}}$, $r_{node_{i+1}}$값을 서명하여 S_{node_i}를 생성하고 MN_i으로 전송한다. MN_i는 노드들로부터 전송받은 서명 S_{node_i}와 ID_{node_i} $m_{node_{i+1}}$, $r_{node_{i+1}}$를 저장한다.

서명에 대한 변조나 위조를 확인하기 위해 MN_i 자신의 식별정보 ID_{mn_i} 와 서명S_{mn_i}, 공개키 y_{mn_i} 그리고 노드로부터 받은 서명 S_{node_i}값을 해당 노드들에게 전송한다.

노드들은 MN_i로부터 전송받은 ID_{mn_i}, S_{mn_i}, y_{mn_i}를 저장하고, 자신의 공개키 y_{node_i}로 재전송 받은 서명 S_{node_i}가 변조되었는지 확인한다. 이상이 없을 경우 자신의 $m_{node_{i+1}}$, $r_{node_{i+1}}$로 트랩도어 충돌 해시 값 $C_{y_{node_i}}$을 계산하여 MN_i와 그룹키로 사용한다. 마지막으로 MN_i의 서명 S_{mn_i}와 자신의 공개키 y_{node_i}를 MN_i에게 전송한다.

MN_i는 수신한 각 노드의 공개키 y_{node_i}로 저장된 노드의 서명 S_{node_i}를 확인한다. 그리고 노드로부터 수신한

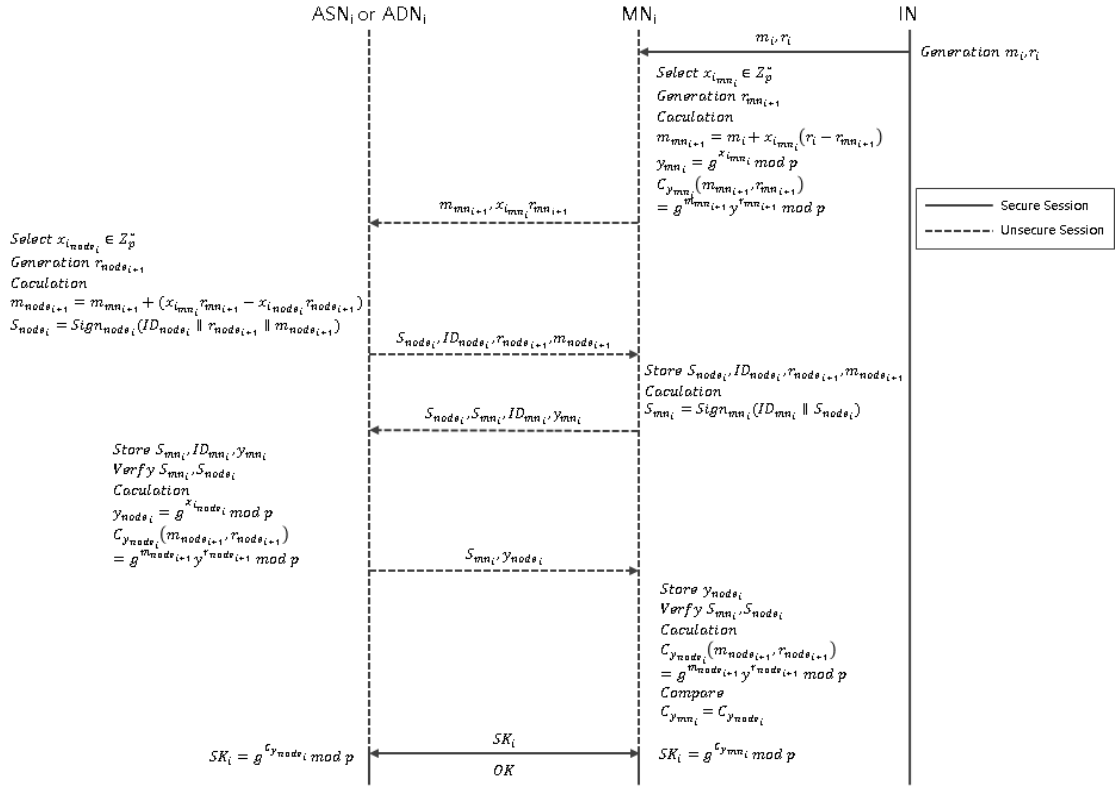

그림 1. 그룹키 생성 및 키 교환 기법[5]
Fig. 1. Group key generation and key exchange techniques[5]

$m_{node_{i+1}}$, $r_{node_{i+1}}$, y_{node_i}값으로 $C_{y_{node_i}}$를 계산하여, 자신이 계산한 트랩도어 충돌 해시값 $C_{y_{mn_i}}$와 같은지 확인한다.

정상적인 노드에서 생성한 값은 MN$_i$이 계산하는 트랩도어 충돌 해시 값과 같다. 확인된 트랩도어 충돌 해시 값으로 세션키 SK_i를 생성하여 그룹내에서 MN$_i$과 노드들이 정보를 주고받는 보안 세션키로 설정한다.

4) 프로토콜의 취약점

충돌 메시지를 생성하는 식(12)에서 비밀키 $x_{i_{node_i}}$를 제외한 값 중, $m_{mn_{i+1}}$과 $x_{i_{mn_i}} r_{mn_{i+1}}$는 그룹키 생성 절차 중 MN$_i$에서 수신 가능한 노드들에게 안전하지 않은 채널을 통해 전송하며, $m_{node_{i+1}}$, $r_{node_{i+1}}$는 그룹키 생성 절차 중 ASN, ADN 노드들에서 MN$_i$으로 안전하지 않은 채널을 통해 전송된다.

$$m_{node_{i+1}} = m_{mn_{i+1}} + (x_{i_{mn_i}} r_{mn_{i+1}} - x_{i_{node_i}} r_{node_{i+1}}) \quad (6)$$

이를 노출되지 않은 ASN, ADN 노드들의 비밀키 $x_{i_{node_i}}$에 대해 정리하면 식 (13)이 도출되고, 공격자는 스니핑을 통해 수집한 정보를 이용해 비밀키를 유추할 수 있다.

$$x_{i_{node_i}} = - \frac{m_{node_{i+1}} - m_{mn_{i+1}} - x_{i_{mn_i}} r_{mn_{i+1}}}{r_{node_{i+1}}} \quad (7)$$

Ⅲ. 제안 기법

제안하는 그룹키 생성 및 키 교환 기법은 큰 소수 g, p를 이용하여 초기 난수 m을 모든 디바이스로 분배하고, 순환부분군의 역원을 이용해 충돌값을 교환하여 초기 디바이스를 인증한다. 이후 계산 가능한 해시 충돌을 이용하여 정상적인 디바이스임을 인증한다. 또한 이미 인증을 완료한 디바이스들은 이를 그룹키로 활용하여 보안 세션을 수립하는 기법을 제안한다.

1) 가정 사항

서비스제공자(IN)와 모든 게이트웨이(MN), 디바이스(ASN/ADN)는 통신이 가능한 위치에 있고, 물리적인 공격에 안전한 신뢰성이 있는 컴퓨팅 환경이 보장되며, IN과 MN은 안전한 통신 회선이 구축되어 있다.

표 4. 해시 충돌 그룹키 파라미터
Table 4. Trapdoor Collision Hash Parameter

Parameter	Description
g, p	큰 소수
E	지수 역원
Pu, Pe	곱 교환키, 합 교환키
SR, MR	곱 교환값, 합 교환값
TK	충돌 비밀값
tx	충돌 생성자
tr	충돌 난수
x	비밀키
r_i	Z^*_p상의 난수
m_i	충돌 메시지
y_i	충돌 해시 공개키
S	전자 서명
ID_i	식별 정보
C_{y_i}	해시 충돌 값
SK_i	그룹 세션키

2) 프로토콜의 파라미터

프로토콜에서 표기하는 디바이스의 요약어는 기존 알고리즘과 동일하며, 제안하는 그룹키 생성 및 키교환프로토콜에서 사용하는 파라미터는 표 4와 같다.

3) 사전 단계

M2M 환경에서 정상적인 장치인 ASN/ADN, MN, IN은 EAP-TLS와 같은 기존 무선망의 인증방식으로 인증, 그룹키에 사용하는 값과 식별 정보를 사전에 동의하여 IN으로부터 MN과 ASN/ADN으로 공유한다.

4) 그룹키 생성 및 키 교환

MN_i은 IN으로터 그룹간의 키로 사용할 최초 난수 m_i, r_i과 비밀값 공유를 위한 비밀키쌍 E_{Pu}, E_{Pr}, E_{Pe}, E_{Pd}를 수신한다. m_i와 r_i을 수신한 MN_i은 비밀키 $x_{i_{mn_i}}$와 난수 $r_{mn_{i+1}}$을 생성하여 충돌 메시지 $m_{mn_{i+1}}$을 계산한다.

$$m_{mn_{i+1}} = m_i + x_{i_{mn_i}}(r_i - r_{mn_{i+1}}) \quad (8)$$

충돌 비밀값 공유를 위하여 비밀키쌍 S_{Pu}, S_{Pr}로 Pu를 생성하고, S_{Pe}, S_{Pd}로 Pe를 계산한다.

$$Pu \equiv g^{S_{Pu}} \bmod p$$
$$Pe \equiv g^{S_{Pe}} \bmod p \quad (9)$$

공개키 y_{mn_i}와 생성한 난수 $r_{mn_{i+1}}$, 충돌 메시지 $m_{mn_{i+1}}$, 을 이용하여, 해시 충돌 값을 미리 계산한다.

$$C_{y_{mn_i}}(m_{mn_{i+1}}, r_{mn_{i+1}}) = g^{m_{mn_{i+1}}} y^{r_{mn_{i+1}}} \bmod p \quad (10)$$

MN_i의 주변 노드들에게 $x_{i_{mn_i}} r_{mn_{i+1}}$값과, 충돌 메시지 $m_{mn_{i+1}}$을 전송한다. $x_{i_{mn_i}}$과 $m_{mn_{i+1}}$값을 수신한 노드들은 자신의 비밀키$x_{i_{node_i}}$와 충돌 난수 $tr_{node_{i+1}}$를 선택하고, 충돌 비밀값을 합의하기 위하여 SR_{EK}와 MR_{EK}을 계산하여 MN_i로 전송한다.

$$SR_{EK} \equiv Pu^{EK} \bmod p$$
$$MR_{EK} \equiv Pe^{EK} \times tr_{node_{i+1}} \bmod p \quad (11)$$

MNi는 전달받은 SR_{EK}와 MR_{EK}로 $tr_{node_{i+1}}$를 확인하고, TK를 생성할 수 있는 $tx_{node_{i+1}}$를 계산하여 ASN/ADN노드로 전송한다.

ASN/ADN노드는 생성한 $tr_{node_{i+1}}$값과 전달받은 $tx_{node_{i+1}}$, 선택한 비밀키 $x_{i_{node_i}}$와 생성한 난수$r_{node_{i+1}}$로 충돌 메시지 $m_{node_{i+1}}$을 계산한다.

$$m_{node_{i+1}} = m_{mn_{i+1}} + (tx_{node_{i+1}} tr_{node_{i+1}} - x_{i_{node_i}} r_{node_{i+1}}) \quad (12)$$

노드들은 자신의 ID_{node_i}와 $m_{node_{i+1}}$, $r_{node_{i+1}}$값을 서명하여 S_{node_i}를 생성하고 MN_i으로 전송한다. MN_i는 노드들로부터 전송받은 서명 S_{node_i}와 ID_{node_i} $m_{node_{i+1}}$, $r_{node_{i+1}}$를 저장한다.

서명에 대한 변조나 위조를 확인하기 위해 MN_i 자신의 식별정보 ID_{mn_i} 와 서명S_{mn_i}, 공개키 y_{mn_i} 그리고 노

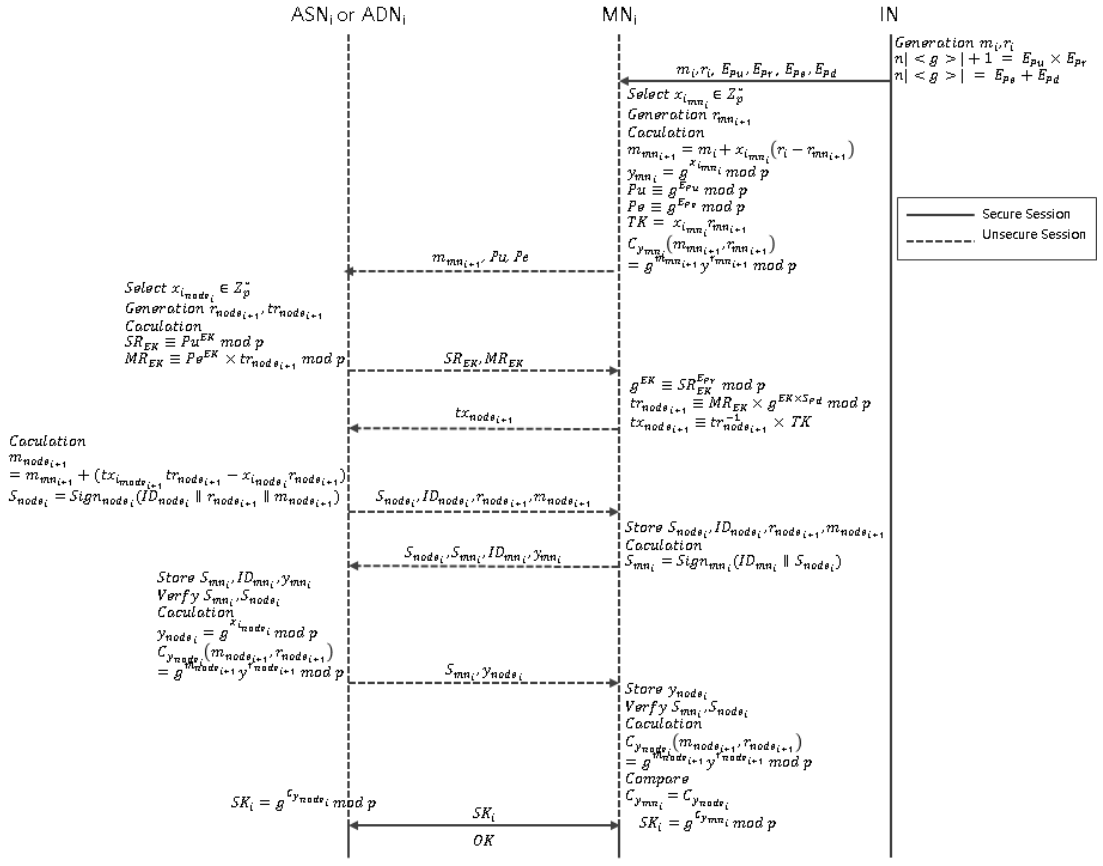

그림 2. M2M 통신 환경에서 해시충돌을 이용한 그룹키 생성 및 교환 기법
Fig. 2. Group key generation and exchange using hash collision in M2M communication environment

드로부터 받은 서명 S_{node_i}값을 해당 노드들에게 전송한다.

노드들은 MNi로부터 전송받은 ID_{mn_i}, S_{mn_i}, y_{mn_i}를 저장하고, 자신의 공개키 y_{node_i}로 재전송 받은 서명 S_{node_i}가 변조되었는지 확인한다. 이상이 없을 경우 자신의 $m_{node_{i+1}}$, $r_{node_{i+1}}$로 해시 충돌 값 $C_{y_{node_i}}$을 계산하여 MNi와 그룹키로 사용한다. 마지막으로 MNi의 서명 S_{mn_i}와 자신의 공개키 y_{node_i}를 MNi에게 전송한다.

$$C_{y_{mn_i}}(m_{mn_{i+1}}, r_{mn_{i+1}}) = g^{m_{mn_{i+1}}} y^{r_{mn_{i+1}}} \bmod p \quad (13)$$

MNi는 수신한 각 노드의 공개키 y_{node_i}로 저장된 노드의 서명 S_{node_i}를 확인한다. 그리고 노드로부터 수신한 $m_{node_{i+1}}$, $r_{node_{i+1}}$, y_{node_i}값으로 $C_{y_{node_i}}$를 계산하여, 자신이 계산한 해시 충돌 값 $C_{y_{mn_i}}$와 같은지 확인한다.

$$C_{y_{mn_i}}(m_{mn_{i+1}}, r_{mn_{i+1}}) = C_{y_{node_i}}(m_{node_{i+1}}, r_{node_{i+1}}) \quad (14)$$

정상적인 노드에서 생성한 값은 MNi이 계산하는 해시 충돌 값과 같다. 확인된 해시 충돌 값으로 세션키 SK_i를 생성하여 그룹내에서 MNi과 노드들이 정보를 주고받는 보안 세션키로 설정한다.

$$SK_i = g^{C_{y_{mn_i}}} \bmod p = g^{C_{y_{node_i}}} \bmod p \quad (15)$$

Ⅳ. 성능 분석

본 장에서는 작은 소수를 이용하여 제안하는 알고리즘의 동작을 검증하고, 알려진 공격으로부터의 안전성에 대해 증명한다.

표 5. 충돌 해시 파라미터 검증
Table 5. Collision Hash Parameter Verification

g	227		p	487		
m	70		r	150		
MN1						
x_{mn}	89	TK	12549	m'_{mn}	871	
y_{mn}	246	$C_{y_{mn}}$	137	SK	6	
Node1						
x_{node1}	71	r'_{node1}	179	tx_{node1}	228	m'_{node1}	711
y_{node1}	384	tr_{node1}	23	$C_{y_{node1}}$	137	SK	6
Node2							
x_{node2}	83	r'_{node2}	158	tx_{node2}	54	m'_{node2}	306
y_{node2}	246	tr_{node2}	43	$C_{y_{node2}}$	137	SK	6
Node3							
x_{node3}	43	r'_{node3}	298	tx_{node3}	61	m'_{node3}	606
y_{node3}	190	tr_{node3}	70	$C_{y_{node3}}$	137	SK	6
Node4							
x_{node4}	61	r'_{node4}	217	tx_{node4}	11	m'_{node4}	183
y_{node4}	10	tr_{node4}	34	$C_{y_{node4}}$	137	SK	6
Node5							
x_{node5}	19	r'_{node5}	691	tx_{node5}	312	m'_{node5}	291
y_{node5}	217	tr_{node5}	73	$C_{y_{node5}}$	137	SK	6

1. 제안 기법 검증

제안한 기법은 알고리즘의 각 파라미터에 표 6과 같이 값을 적용하여 1개의 게이트웨이와 5개의 노드들이 통신하는 시나리오로 검증하였다.

ASN/ADN 노드들은 MNi의 비밀키 x_{mn}와 연산한 TK, $m_{mn_{i+1}}$값의 수신을 시작으로 생성한 tr_{nodei}를 기반으로 $tx_{nodei+1}$를 받아 새로운 충돌 메시지m'_{nodei}를 계산하여 생성한다. ASN/ADN 노드들이 생성한 r'_{nodei}과 자신의 공개키 y_{nodei}로 충돌 해시 값 $C_{y_{nodei}}$ 을 계산하였다.

이를 Node1에 대해 계산해보면 소수인 밑수 227과 모듈로 487인 군에서, 그룹간의 키로 사용할 최초 난수로 m_i은 70, r_i은 150으로 정하고. 비밀값 공유를 위한 충돌 비밀키쌍으로 (61, 425)와 (12, 162)를 적용한다. MNi의 비밀키가 89, 난수가 141일 때 충돌 메시지는 871이 된다.

$$871 = 70 + 89(150 - 141) \tag{16}$$

충돌 비밀값 공유를 위한 비밀키쌍 중 합의 역원 암호화값 61 적용하여 61로 Pu 10을 생성하고, 곱의 역원 암호화값 12를 적용하여 Pe 130을 계산한다.

$$\begin{aligned} 10 &\equiv 227^{61} \bmod 487 \\ 130 &\equiv 227^{12} \bmod 487 \end{aligned} \tag{17}$$

공개키 246과 생성한 MNi의 난수 141과 충돌 메시지 871을 이용하여, 해시 충돌 값을 미리 계산한다.

$$137 = g^{871} y^{321} \bmod 487 \tag{18}$$

MNi의 주변 노드들에게 공개키의 지수 값 141과, 충돌 메시지 871을 전송한다. $x_{i_{mn_i}}$ 값 89과 $m_{mn_{i+1}}$값 871을 수신한 노드들은 자신의 비밀키$x_{i_{node_i}}$와 충돌 난수 $tr_{node_{i+1}}$를 선택하고, 충돌 비밀값을 합의하기 위하여 SR_{EK}와 MR_{EK}을 계산하여 MNi로 전송한다. 여기에서는 Node1을 기준으로 비밀키 71과 충돌 난수 228을 선택한다.

$$\begin{aligned} 223 &\equiv 10^{71} \bmod 487 \\ 236 &\equiv 130^{71} \times 228 \bmod 487 \end{aligned} \tag{19}$$

MNi는 전달받은 223과 236으로 tx_{node1}값 228을 확인하고, TK값을 생성할 수 있는 116를 계산하여 ASN/ADN노드로 전송한다.

ASN/ADN노드는 생성한 $tr_{node_{i+1}}$값 228과 전달받은 $tx_{node_{i+1}}$값 116, 선택한 비밀키 71와 생성한 난수 179로 충돌 메시지 711을 계산한다.

$$711 = 871 + (228 \times 116 - 71 \times 179) \tag{20}$$

노드들은 자신의 $m_{node_{i+1}}$값 711과 $r_{node_{i+1}}$값 179로 해시 충돌 값을 계산하여 MNi와 그룹키로 사용한다. 마지막으로 MNi의 서명 S_{mn_i}와 자신의 공개키 y_{node_i}를 MNi에게 전송한다.

$$\begin{aligned} &C_{y_{mn_i}}(m_{mn_{i+1}}, r_{mn_{i+1}}) \\ &= 137 = 227^{711} 384^{179} \bmod 487 \end{aligned} \tag{21}$$

MNi는 수신한 각 노드의 공개키 y_{node_i}로 저장된 노드의 서명 S_{node_i}를 확인한다. 그리고 노드로부터 수신한 $m_{node_{i+1}}$, $r_{node_{i+1}}$, y_{node_i}값으로 $C_{y_{node_i}}$를 계산하여, 자신이 계산한 해시 충돌 값 $C_{y_{mn_i}}$와 같은지 확인한다.

$$C_{y_{mn_i}}(871,321) = C_{y_{node_i}}(711,179) = 137 \quad (22)$$

노드에서 생성한 값은 MN_i이 계산하는 해시 충돌 값과 같다. 확인된 해시 충돌 값으로 세션키 SK_i를 생성하여 그룹내에서 MN_i과 노드들이 정보를 주고받는 보안 세션키로 설정한다.

$$6 = 227^{137} \bmod 487 = 227^{137} \bmod p \quad (23)$$

위와같이 표 5는 게이트웨이인 MN_i와 5개의 ASN/ADN 노드에서 모두 동일한 충돌 해시값을 계산하여 그룹키를 생성하며, 동일한 그룹 세션키 값을 나타낸다.

2. 안전성 분석

제안하는 기법의 안전성은 크게 그룹키 생성 및 교환 기법에 대한 안전성과 충돌 해시를 사용함으로써 나타날 수 있는 취약점으로 나눌 수 있다. 각 항목에서 안전성에 대해 분석한다.

가. 그룹키 생성 및 교환 기법의 안전성

제안하는 그룹키 생성 및 교환 기법은 큰 소수 g, p를 이용한 이산 대수 문제를 기반으로 하므로, 그룹 세션키 SK_i를 대상으로 그룹키인 해시 충돌 값 C_y을 구할 수 없다. 따라서, 알려진 재전송 공격, 중간자 공격, 위장 공격에 대해 안전성을 가진다.

나. 트랩도어 충돌해시 취약점의 저항성

(1) 비밀키 생성 메시지 탈취 공격

기존의 프로토콜에서 공격자는 비밀키에 대한 연산에서 필요한 정보를 안전하지 않은 채널을 통해 습득하여 유추가 가능하다. 제안하는 기법은 노출되는 공유 값 중 $x_{i_{mn_i}} r_{mn_{i+1}}$값을 노출되지 않는 tx_{node_i}와 $tr_{node_{i+1}}$ 값의 합의절차로 설계하여 전송값을 탈취하는 공격으로부터 안전하다.

$$x_{i_{node_i}} = - \frac{m_{node_{i+1}} - m_{mn_{i+1}} - x_{i_{mn_i}} r_{mn_{i+1}}}{r_{node_{i+1}}} \quad (24)$$

(2) 트랩도어 충돌 해시 비밀키 공격

기존의 충돌 해시 기법은 충돌 메시지 생성하기 위해 동일한 비밀키를 사용하기 때문에 전송되는 키 쌍 (m', r')과 (m'', r'')을 수집한다면, 다음 식과 같이 비밀키 x를 유추할 수 있다. 제안하는 기법은 MN_i으로 전송하는 $m_{node_{i+1}}$와 $r_{node_{i+1}}$이 노출되지 않으므로 식(17)과 같은 취약점을 가지지 않는다.

$$\begin{aligned} C_{y''}(m'', r'') &= C_{y'}(m', r') \\ g^{m''} g^{xr''} \bmod p &= g^{m'} g^{xr'} \bmod p \\ m'' + xr'' &= m' + xr' \\ x &= \frac{m' - m''}{r' - r''} \end{aligned} \quad (25)$$

또한 충돌 해시 값을 노출하지 않고, 노드들에서 새로운 $x_{i_{node_i}} \in Z_p^*$를 선택하여 새로운 충돌 메시지를 계산하고 생성하기 때문에 비밀키 $x_{i_{node_i}}$에 대한 공격은 어렵다.

$$x_{i_{node_i}} \neq \frac{m_{mn_{i+1}} - m_{node_{i+1}}}{x_{i_{mn_i}} r_{mn_{i+1}} - r_{node_{i+1}}} \quad (26)$$

V. 결 론

본 논문에서는 해시 충돌을 이용하여 M2M 환경에서 그룹키를 생성하여 세션 키를 합의함으로써 보안성을 제공하는 그룹 통신 기법을 제안하였다. 서비스 제공자로부터 초기 난수를 받되, 기존 프로토콜에서 노출되어 비밀값이 계산 가능했던 값들을 게이트웨이와의 비밀합의 절차로 보완하여, 안전한 방법으로 동일한 충돌 해시 값을 생성하여 정상적인 노드를 확인하였다. 또한 전송되는 정보들은 재전송 공격, 중간자 공격, 위장 공격, 비밀키 공격, 충돌 메시지 공격에 저항성을 가지는 것을 확인하였다.

제안한 기법은 해시 충돌을 이용한 알고리즘이 알려진 취약점에서 어떻게 안전성을 확보할 수 있는지를 보여주었으며, M2M 뿐만 아니라 해시 충돌값을 이용한 키합의가 적용될 수 있는 다양한 환경에서 필수 보안 요구사항을 충족시킬 수 있는 방법론을 제공할 수 있을 것으로 기대한다.

References

[1] Wen Quan JIN, Do Hyeun Kim, “Implemen tation and Experiment of CoAP Protocol Based on IoT for Verification of Interoperability” The Journal of The Institute of Internet Broadcasting and Communication(JIIBC), Vol 14, No 4, pp 7-12, Aug

2014, Retrieved from http://www.earticle.net/Article.aspx?sn=229038

[2] G. Lawton, "Machine-to-Machine technology ge ars up for growth" IEEE Computer Society, Vol 37, No 9, pp 12-15, Sep 2004. DOI: https://doi.org/10.1109/MC.2004.137

[3] KISA, "Internet Threat Trend things", Korea Internet & Security Agency, 2014.

[4] Jeongin Kim, Namhi Kan, "Secure Configuration Scheme of Pre-shared Key for Lightweight Devices in Internet of Things" The Journal of The Institute of Internet, Broadcasting and Communication(JIIBC), Vol 15, No 3, pp 1-6, Jun 2015, Retrieved from http://www.earticle.net/Article.aspx?sn=249122

[5] Sung-Soo Kim, Do-Hyeon Choi, Moon-Seog Jun, "Group Key Generation and Exchange Scheme using a Trapdoor Collision Hash in M2M Communications Environment", The journal of the Institute of Internet Broadcasting and Communication, Vol. 15, Issue 5, p. 9-17, 2015, Retrieved from http://www.earticle.net/Article.aspx?sn=256742

[6] KISA, "The Trend of Project related to Tech nology for Personal Information protection", Korea Internet and Security Agency, 2006.

[7] Krawczyk H., Rabin T., "Chameleon Hashing and Signatures" Proceedings of NDSS, pp 143-154, 2000, Retrieved from http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.50.3262

[8] Ateniese Giuseppe, De Medeiros Breno, "Iden tity-based chameleon hash and applications" Financial Cryptography. Springer Berlin Heidelberg, pp 164-180, 2004, DOI: https://doi.org/10.1007/978-3-540-27809-2_19

[9] G. Ateniese, and B. de Medeiros, "On the Key Exposure Problem in Chameleon Hashes", Proc. of the 4th Conference on Security in Communication Networks, LNCS 3352, Springer-Verlag, pp.165-179, 2004.9, DOI: https://doi.org/10.1007/978-3-540-30598-9_12

저 자 소 개

송 준 호(정회원)

- 2011년 : 학점은행제 컴퓨터공학 공학사
- 2012년 : 숭실대학교 컴퓨터학과 석사
- 2015년 ~ 현재 : 숭실대학교 컴퓨터학과 박사과정

- 주관심분야 : 정보보호, 네트워크 보안, 암호학

김 성 수(정회원)

- 2016년 : 숭실대학교 컴퓨터학과 박사
- 2014년 ~ 2016년 : 안양대학교 교양대학 겸임교수
- 2017년 ~ 현재 : 한국정보화진흥원 ICT융합본부 책임연구원

- 주관심분야 : 네트워크 보안, 인증 이론, 암호학

전 문 석(정회원)

- 1981년 2월 : 숭실대학교 전자계산학과 졸업
- 1986년 2월 : University of Maryland Computer Science 석사
- 1989년 2월 : University of Maryland Computer Science 박사
- 1991년 3월 ~ 현재 : 숭실대학교 컴퓨터학과 정교수

- 주관심분야 : 정보보호, 네트워크 보안, 암호학