Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.29, NO.1, Feb. 2019 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2019.29.1.17

안전한 6LoWPAN Neighbor Discovery 주소 등록 프로토콜*

한 상 우,† 박 창 섭‡
단국대학교

Secure 6LoWPAN Neighbor Discovery Address Registration Protocol*

Sang-woo Han,† Chang-seop Park‡
Dankook University

요 약

IEEE 802.15.4 기반의 6LoWPAN은 다양한 IoT (Internet of Things) 응용 프로그램을 위한 사실상의 표준 플랫폼이다. LoWPAN (Low-power Wireless Personal Area Network)을 부트 스트랩 하려면 각 디바이스는 고유한 IPv6 주소를 할당하기 위해 6LoWPAN-ND 주소 등록을 수행해야 한다. 적절한 보안 메커니즘이 없다면, 6LoWPAN-ND는 손상된 노드 공격을 포함한 다양한 보안 공격에 취약하다. 취약점에 대한 보완으로 몇 가지 보안 메커니즘이 제안되었지만 IEEE 802.15.4 hop-by-hop 보안에만 의존하기 때문에 취약점이 존재한다. 본 논문에서는 6LoWPAN-ND 주소 등록의 취약점 및 손상된 노드 공격 방지에 적합한 새로운 보안 메커니즘을 제안하고 분석한다. 또한 제안된 보안 메커니즘이 IETF (Internet Engineering Task Force) 표준과 호환되며 IETF 6lo WG에서 제안 된 메커니즘 보다 효율적임을 보인다.

ABSTRACT

6LoWPAN based on IEEE 802.15.4 is a realistic standard platform for various Internet of Things (IoT) applications. To bootstrap the LoWPAN (Low-power Wireless Personal Area Network), each device must perform 6LoWPAN-ND address registration to assign a unique IPv6 address. Without adequate security mechanisms, 6LoWPAN-ND is vulnerable to a variety of security attacks including corrupted node attacks. Several security mechanisms have been proposed as a supplement to the vulnerability, but the vulnerability exists because it relies solely on IEEE 802.15.4 hop-by-hop security. In this paper, we propose and analyze a vulnerability of 6LoWPAN-ND address registration and a new security mechanism suitable for preventing the attack of damaged node. It also shows that the proposed security mechanism is compatible with the Internet Engineering Task Force (IETF) standard and is more efficient than the mechanism proposed in the IETF 6 lo WG.

Keywords: 6LoWPAN, Neighbor Discovery, Address Registration

Received(10. 29. 2018), Modified(12. 13. 2018), Accepted(12. 13. 2018)
* 본 연구는 과학기술정보통신부 및 한국인터넷진흥원의 "고용 계약형 석사과정 지원사업"의 연구결과로 수행되었음. (과제번호 H2102-18-1001)
* 본 연구(논문)는 과학기술정보통신부 및 정보통신기획평가원의 SW컴퓨팅산업원천기술개발사업(GCS)의 연구결과로 수행되었음. (과제번호 IITP-2018-0-00640)
† 주저자, sangwoo1-17@naver.com
‡ 교신저자, csp0@dankook.ac.kr(Corresponding author)

I. 서 론

6LoWPAN[1, 2]은 IEEE 802.15.4와 같은 저전력의 손실이 많은 링크를 통해 IPv6 패킷을 전송할 수 있게 하는 IoT 네트워크 프로토콜이다. LoWPAN 내의 자원이 제약적인 디바이스는 6LBR (6LoWPAN Border Router)을 통해 IPv6 인터넷 호스트에 연결될 수 있다. 각 디바이스는 LoWPAN에 가입한 후, 고유한 IPv6 주소를 할당받기 위해 6LoWPAN-ND (6LoWPAN Neighbor Discovery) 프로토콜을 수행하여야 한다. LoWPAN에 참여하도록 승인된 각 디바이스는 보안 부트스트래핑 프로세스를 통해 생성된 암호화 키 재료를 기반으로 액세스 제어를 수행하고 6LoWPAN-ND 메시지를 보호한다.

현재, 6LoWPAN-ND 보안에 관한 연구는 EC (Elliptic Curve)암호화 또는 대칭키 암호화를 사용하여 두 디바이스 사이의 대칭키를 설정하는 데 중점을 두고 있다. 첫째, 두 디바이스 사이에 대칭키를 설정하기 위해 각 디바이스에 EC 공개키와 개인키 쌍이 설치된다[3, 4]. 또한, 두 개의 디바이스가 ECDH (Elliptic Curve Diffie Hellman) 키 교환을 수행할 수 있도록 LoWPAN의 각 디바이스에 ECQV (Elliptic Curve Qu-Vanstone) 인증서[5]를 발행할 수 있다[6, 7]. 계산 부하가 크다는 문제점이 있지만, ECQV 인증서와 해당 EC 개인키를 사용하여 디바이스에 대한 액세스 제어를 시행할 수 있다. 둘째, 하나 이상의 대칭키 또는 키 재료를 각 디바이스에 사전 로드하여 각 쌍이 적어도 하나의 대칭키를 공유할 수 있다[8, 9]. 그러나 여러 디바이스는 다중 홉 LoWPAN 환경에서 사용되므로, 각 디바이스에 상당한 메모리 공간이 사용되는 문제점이 존재한다. 셋째, 각 디바이스는 초기에 LoWPAN의 앵커 디바이스와 대칭키를 공유한다[10, 11]. 디바이스는 대칭키를 사용하여 LoWPAN에 가입하고 6LoWPAN 메시지를 보호한다. 하지만, [10, 11]에서 제안 된 보안 메커니즘은 단일 홉 LoWPAN에 대해서만 설계되었으며 [10]에서 보안 취약점이 발견되었다. IEEE 802.15.4 기반의 6LoWPAN이 IEEE 802.15.4 hop-by-hop 보안에 의해 보안이 유지되는 것으로 가정 한 몇 가지 연구가 제안 되었지만 인접한 디바이스 간의 대칭키 공유 방식을 지정하지 않거나 손상된 노드 공격 (Compromised Node Attack)은 고려하지 않고 있다.

본 논문에서는 첫째, 기존 연구의 문제점을 지적하고 둘째, 다중 홉 LoWPAN 환경에서 6LoWPAN-ND 주소를 안전하게 등록하기 위해 IETF 표준[12]과 호환되는 보안 메커니즘을 제안한다. 또한, IEEE 802.15.4 hop-by-hop 보안을 기반으로 제안된 보안 메커니즘은 손상된 노드 공격에 대해 탄력적으로 대응할 수 있다. 셋째로, 6LoWPAN-ND 주소 등록에 참여하는 두 개의 인접한 디바이스 사이의 대칭키를 동적으로 공유할 수 있고 6LoWPAN-ND 신호 메시지를 보호할 수 있는 Cross-Layer 키 관리 체계를 제시한다. 대칭키는 6LoWPAN-ND 주소 재등록 중에 보안성 향상을 위해 정기적으로 갱신된다. 따라서 IEEE 802.15.4 hop-by-hop 보안의 키 관리 문제 역시 해결할 수 있다.

본 논문은 다음과 같이 구성된다. 2장에서는 6LoWPAN-ND 주소 등록과 관련된 기존 연구에 대해서 설명하고 3장에서 6LoWPAN-ND 주소 등록을 위한 새로운 보안 메커니즘을 제안한다. 4장에서는 새로운 보안 메커니즘의 보안 분석을 수행하고 5장에서 성능 평가를 수행한다. 마지막으로 6장에서 결론을 맺는다.

II. 6LoWPAN-ND 기존 연구

2.1 6LoWPAN Neighbor Discovery

6LoWPAN 및 RPL 프로토콜을 지원하는 6LN (6LoWPAN Node)이 LoWPAN에 처음 배포되면 LoWPAN에 가입하기 위한 IEEE 802.15.4 Association 프로토콜과 IPv6 주소 구성을 위한 6LoWPAN Address Registration 프로토콜을 수행한다. 그 결과, 각 6LN은 LoWPAN 내에서 사용될 주소인 Link Local Address와 전역적으로 사용될 주소인 Global Unicast Address의 두 가지 유형의 IPv6 주소를 구성한다.

Fig. 1.에서, *RS* (Router Solicitation) 및 *RA* (Router Advertisement) 메시지는 6LN 과 중계 노드인 6LR (6LoWPAN Router) 사이에서 교환되며, 여기서 *RA* 메시지는 LoWPAN을 관리하는 *6LBR_info* (*Prefix*..)를 포함한다. *RA* 메시지를 수신할 때, 6LN은 자신의 Long MAC Address (*MAC64*) 또는 Short MAC Address (*MAC16*)에서 파생된 6LN의 인터페이스 식별자인 *IID*

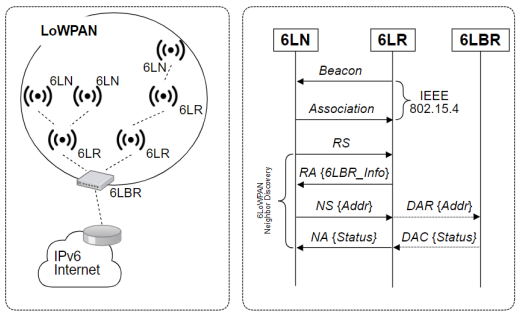

Fig. 1. 6LoWPAN neighbor discovery for address registration

(Interface ID)와 *6LBR_info*에 포함된 *Prefix*를 사용하여 고유한 Global Unicast Address 인 *GP = Prefix :: IID*를 구성할 수 있다. 생성된 *GP*의 고유성을 보장하고 6LBR에 등록하기 위해서는 Fig. 1.의 6LoWPAN-ND Address Registration Protocol[13]을 수행해야 한다. *GP*는 *MAC64* 기반으로 구성된 *GP64*이나 *MAC16* 기반으로 구성된 *GP16*이 사용될 수 있다.

6LN은 *Addr = (MAC64, GP16, LT)*를 생성하여 *NS* (Neighbor Solicitation) 메시지를 전송한다. 이 때, *MAC*64는 LoWPAN 내에서 6LN의 유일한 식별 값이 된다. *NS*를 수신한 6LR은 중복 주소 확인을 위한 *DAR* (Duplicate Address Request) 메시지를 통해 6LBR에게 *Addr*를 전달한다. 6LBR은 LoWPAN에 등록 된 모든 6LN의 (*MAC64, GP16, LT*) 항목을 유지하는 *DAD* (Duplicate Address Detection) 테이블을 사용하여 *GP16*이 중복 주소인지 여부를 확인할 수 있다. *LT*는 (*MAC64, GP16*)의 등록 수명 (Lifetime)을 나타내며, *LT* 가 유효할 때 까지 *DAD* 테이블에 항목이 유지된다. 6LBR은 중복 검사 중복검사 결과 (*Status*)를 *DAC* (Duplicate Address Confirmation) 메시지를 통해 6LR로 전송하고, 6LR은 *NA* (Neighbor Advertisement) 메시지를 통해 6LN에게 결과를 전달한다.

2.2 6LoWPAN 주소 등록 프로토콜 및 보안 요구사항

6LoWPAN-ND Address Registration Protocol[13]에서는 IEEE 802.15.4 hop-by-hop 보안이 6LoWPAN-ND 메시지 (*RS* / *RA* / *NS* / *NA* / *DAR* / *DAC*)의 무결성을 위해 사용된다고 가정한다. 이 가정은 접근제어 문제를 해결하기 위해 적용되었으며, 사전 공유키를 가진 6LN만이 LoWPAN에 가입할 수 있다는 것을 의미한다. 하지만, 일반적으로 6LN은 개방 환경에 배치되기 때문에, 6LN에 동일한 키 (그룹키)가 배포된 경우 손상된 노드 문제로 인한 키 유출 가능성을 배제할 수 없다[14].

손상된 노드 공격 (Compromised Node Attack)이 가능하다고 가정하면 6LoWPAN-ND 주소 등록에 대한 두 가지 유형의 공격이 가능하다. 하나는 합법적인 6LN 또는 6LR을 위장하여 공격하는 방법과 다른 하나는 6LoWPAN-ND 메시지의 변조 공격을 수행하는 방법이다. 두 가지 공격 모두 정상적인 주소 등록을 방해하는 리다이렉션 및 스푸핑 공격을 유도할 수 있다. *RS* 메시지를 제외하고 다른 다섯 개의 6LoWPAN-ND 메시지는 악의적인 변조로부터 보호되어야 한다. *RA* 메시지가 보호되지 않으면, *6LBR_Info*를 수정하여 6LN이 *GP16*의 생성을 방해하여 유효하지 않게 할 수 있다. 6LBR의 *DAD*

Table 1. Notation

Notation	Description
$6LN_j$	6LoWPAN nodes, $j = 1, 2, 3, \cdots$
$MAC16_j$	short (16-bit) MAC address of $6LN_j$
$MAC64_j$	long (64-bit) MAC address of $6LN_j$
$GP16_j$	global unicast address of $6LN_j$ derived from $MAC16_j$
LT_j	(registration) lifetime of $6LN_j$
$Addr_j$	$(MAC64_j, GP16_j, LT_j)$
Ctr_j	counter value maintained by $6LN_j$ and 6LBR
K_G	global key shared among all the 6LNs
K_j	device key pre-shared between $6LN_j$ and 6LBR
K_{ji}	link key shared between $6LN_j$ and $6LN_i$
$h(.)$	cryptographic hash function
$Auth_N(K_j)$	Authenticator generated by $6LN_j$
$Auth_B(K_{ji})$	Authenticator generated by 6LBR
$E_K(m)$	encryption of m with symmetric key K
$MIC(K)$	message-integrity code computed with a key K covering all preceding message fields

테이블에 (*MAC64, GP16, LT*)의 항목이 있다고 가정한다면, 공격자는 (*MAC64, GP16, 0*)을 포함하는 *NS* 메시지를 6LBR에게 전송하여 기존 항목의 등록이 취소되도록 유도하고 *GP16*이 다른 6LN에 할당될 수 있게 할 수 있다. Table 1.은 본 논문에서 사용된 표기법을 보여준다.

2.3 Lightweight SEND for 6LoWPAN-ND

Lightweight SEND (L-SEND)[15]는 LoWPAN 내부의 주소 도난 및 위장 공격으로부터 IPv6 주소의 소유자를 보호하기 위해 제안되었다. 6LN은 *6LBR_Info*로부터 구성된 *Addr* = (*MAC64, GP16, LT*)를 안전하게 등록하기 위해 EC 공개키 *PK*와 개인키 *PR*를 생성한다. 그 후, 생성된 *PK*를 사용하여 암호화 식별자 *CID* = *h*(*PK, param*)를 계산한다. *param*은 추가적인 공개 파라미터이고, 생성된 *CID*는 *MAC64*와 함께 6LN을 식별하기 위해 사용된다. 6LN은 6LBR에 *NS*{*Addr, CID*} 메시지를 전송한 뒤, 6LBR로부터 *Nonce*를 전송받는다. 6LN은 메시지의 무결성을 위하여 개인키 *PR*로 {*Addr, Nonce, PK*}에 ECDSA 서명 알고리즘을 사용하여 *Sig*를 생성한다. 그 후, *NS*{*Addr, Nonce, PK, Sig*} 메시지를 6LBR에 전송한다. *Sig*가 유효하고 *GP16*이 아직 할당되지 않은 경우, 주소 등록은 성공적으로 이루어진다.

L-SEND의 주요 목적은 주소가 6LBR에 등록된 뒤, *GP16*이 *DAD* 테이블에서 악의적으로 등록 취소되지 않도록 보호하는 것이다. L-SEND는 IEEE 802.15.4 hop-by-hop 보안을 사용하여 보안이 유지된다고 가정하였지만, 손상된 노드 공격 하에서의 L-SEND에는 몇 가지의 보안 약점이 존재한다. 첫째, 6LN이 LoWPAN에 가입한 뒤 IPv6 주소를 등록할 수 있다는 점에서 접근 제어 문제를 해결하지 못한다. 이로 인해 공격자는 *DAD* 테이블을 과부하시키기 위해 6LBR에 많은 IPv6 주소를 등록하는 공격을 수행할 수 있다. 둘째, *RA* 메시지의 무결성이 보장되지 않기 때문에 위조된 *6LBR_Info*를 사용하여 6LN의 주소 구성을 방해할 수 있다. 셋째, *Sig*를 계산하기 위한 ECDSA 알고리즘은 많은 계산 부담을 야기하므로, 공격자는 다량의 *NS*{*Addr, Nonce, PK, Sig*}메시지를 6LBR에 전송하여 계산량 부하를 야기할 수 있다. 넷째, L-SEND는 *NS* / *NA* 메시지의 추가적인 교환이 요구된다.

III. 6LoWPAN-ND를 위한 보안 메커니즘 제안

3.1 설계 원리 및 가정

각 6LN 디바이스는 manufacturing, deployment / commissioning, operational 단계로 구성된 라이프 사이클을 가지고 있다[16]. manufacturing 단계에서, 디바이스에 펌웨어 및 기본 매개 변수가 저장된다. 그 후, deployment / commissioning 단계에서 디바이스 식별 프로세스를 통하여 디바이스 식별자와 디바이스의 물리적 위치를 매칭 시킨다. 디바이스 식별자 - 물리적 위치 쌍은 네트워크 관리자의 데이터베이스에 저장되어 관리된다. 그 후, 디바이스의 전원이 켜지면 각 디바이스는 IEEE 802.15.4 연결과 6LoWPAN-ND 주소 등록을 통해 LoWPAN 가입을 수행한다.

6LoWPAN-ND 메시지를 보호하기 위해서는 deployment / commissioning 단계에서 각 6LN에 자격 증명을 사전 로드하여 보안 구성을 수행해야 한다. 제안된 보안 메커니즘의 수행을 위해 6LN과 6LBR 간에 사용 될 대칭키를 사전 배포한다. $S = \{6LN_j \mid j \in [1, n]\}$은 LoWPAN에 배치될 수 있는 n 개의 6LN 집합이다. K_j는 Fig. 2. (a)에 보이는 바와 같이 $6LN_j$와 6LBR 사이에 사전 공유된 대칭키 (디바이스 키라고 함)를 나타낸다. 하지만, 대칭키는 임의의 두 6LN 간에 사전 공유될 필요는 없다. 디바이스 키 및 디바이스 식별자 (K_j, $MAC64_j$)는 $6LN_j$가 LoWPAN 가입이 허가되었는지를 검증하는 데 이용된다. 6LN이 6LBR에서 다중 홉 거리에 있는 경우, 두 개의 인접한 6LN 사이에 추가적인 대칭키 (링크키라고 함)가 요구된다. 이 링크키는 6LoWPAN-ND 주소 등록 중에

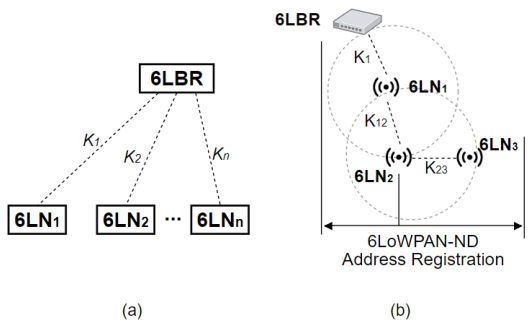

Fig. 2. Device Keys and Link keys

6LBR에 의해 생성되고 분배된다. 예를 들어, Fig. 2. (b)에서, 인가된 $6LN_3$이 $6LN_2$를 통해 LoWPAN에 가입한다면, $6LN_2$와 $6LN_3$ 사이에서 사용될 링크키 K_{23}이 생성된다. 링크키는 6LoWPAN-ND 주소 등록을 보호하는 데 사용될 뿐만 아니라 IEEE 802.15.4 hop-by-hop 보안에도 사용된다. 위 방안은 제안된 보안 메커니즘이 IEEE 802.15.4 hop-by-hop 보안의 키 관리 문제를 해결하는 방법으로 사용될 수 있다.

6LN에 대한 손상된 노드 공격은 6LBR을 제외하고 실현 가능하다고 가정한다. *RA, NS* 및 *NA* 메시지는 *Prefix,* $Addr_j$ 및 *Status* 정보의 무결성을 보장하기 위해 보호되어야 한다. *Prefix*와 *Status*는 6LBR에 의해 생성되고 $6LN_2$를 통해 $6LN_3$으로 전달된다. $6LN_2$가 중계 노드로서 작동하고 $6LN_3$와 6LBR간에 디바이스 키 K_3가 사전에 공유되어 있기 때문에 무결성 및 보안이 보장된다. 유사하게, $6LN_3$에 의해 생성된 $Addr_3$가 6LBR에 의해 최종적으로 처리되기 때문에, 디바이스 키 K_3로 보호될 수 있다.

기존의 *DAD* 테이블의 각 항목은 *MAC64, GP16, LT*로 구성된다. 제안된 Secure 6LoWPAN-ND 주소 등록의 경우, *DAD* 테이블에 *Ctr* 및 *K*를 포함하도록 확장되어 각 항목은 ($MAC64_j$, $GP16_j$, LT_j, Ctr_j, K_j)의 형식을 가진다. 여기서 Ctr_j는 6LoWPAN-ND 메시지의 신규성을 확인하기 위한 카운터 값이다. Fig. 3.과 같이 6LBR은 LoWPAN에 권한이 부여된 6LN ($\in S$)을 확인하기 위해 *DAD* 테이블의 초기 항목으로서 $MAC64_j$, K_j 쌍을 저장하고 있다. 예를 들어, $6LN_3 \in S$ 이라면 6LBR은 *DAD* 테이블의 ($MAC64_3$, K_3) 항목을 확인하여 $6LN_3$이 인가된 디바이스 인 것을 알 수 있다. $6LN_3$의 주소 등록에 성공하면 *DAD* 테이블은 ($MAC64_3$, $GP16_3$, LT_3, Ctr_3, K_3)의 항목으로 채워진다. $6LN_5 \in S$가 ($MAC64_5$, $GP16_5$, LT_5)로 주소 등록 프로토콜을 수행한다고 가정하고, $GP16_5$ = $GP16_3$ 이라면 $GP16_5$가 $6LN_3$에 의해 이미 사용되었기 때문에 주소 등록이 실패한다.

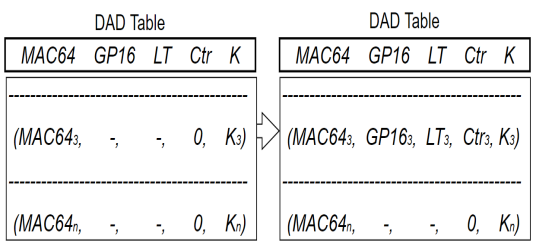

Fig. 3. Extend DAD Table

3.2 보안 주소 등록

$6LN_3$이 6LR (Fig. 2. (b)의 $6LN_2$)과 동일한 로컬 링크 상에 있다고 가정한다. Fig. 4.와 같이 $6LN_3$ 가 *RS* 메시지를 멀티캐스트로 전송하여 인접한 6LR로부터 *RA* 메시지를 요청할 때, $6LN_2$는 $6LN_3$에 *RA*{*6LBR_Info*} 메시지로 응답한다. $6LN_1$ 및 $6LN_2$는 6LBR과 $6LN_1$을 통해 LoWPAN에 가입한 상태라고 가정한다. 링크키 K_{12}는 $6LN_2$의 Secure 6LoWPAN-ND 주소 등록 과정에서 $6LN_1$ 및 $6LN_2$로 분배되고 아래에서 더 상세하게 다룬다.

$6LN_3$는 *6LBR_Info*의 *Prefix*를 기반으로 $GP16_3$을 구성하고 Ctr_3을 증가시킨다. 이것이 첫 번째 주소 등록이면 Ctr_3은 1로 설정된다. 그 후, $Addr_3$ = ($MAC64_3$, $GP16_3$, LT_3) 인 *NS*{$Addr_3$, Ctr_3, $Auth_N(K_3)$} 메시지를 $6LN_2$에 전송한다. K_3는 $6LN_3$과 6LBR 사이에 사전 공유된 디바이스 키다. 인증자 $Auth_N(K_3)$는 ($Addr_3$, Ctr_3, *6LBR_Info*)의 무결성을 위해 $Auth_N(K_3) = h(Addr_3 \,||\, Ctr_3 \,||\, 6LBR_Info \,||\, K_3)$로 계산된다. 인증자는 특히 $6LN_2$로부터 수신된 *6LBR_Info*가 유효한지 확인하는데 사용된다. Fig. 2.와 같이, $6LN_2$가 6LBR로부터 하나 이상의 홉 거리에 있다고 가정하면, $6LN_2$는 *DAR*{$Addr_3$, Ctr_3, $Auth_N(K_3)$} 메시지를 $6LN_1$을 통해 6LBR로 전송시키며, 여기서 *DAR* 메시지는 링크키 K_{12} 및 디바이스 키 K_1을 사용하여 IEEE 802.15.4 hop-by-hop 보안이 유지된다. 6LBR이 메시지를 수신하면 $6LN_3$에 의해 전송된 주소 등록 매개 변수에 대한 유효성 및 보안 검사를 수행한다.

첫째. 6LBR은 $MAC64_3$을 갖는 $6LN_3$가 *DAD* 테이블에 존재하는지 검색함으로써 $GP16_3$을 등록하도록 허가되었는지 확인한다 (Fig. 4. ①). *DAD* 테이블에 $MAC64_3$가 존재하지 않는다면 권한이 없는 6LN으로 분류한다. 이 경우, *DAR* 메시지를 무시하고 6LoWPAN-ND 주소 등록 과정을 중지한다. 둘째, 6LBR은 *DAD* 테이블에서 $6LN_3$의 *Ctr* 및 *K*를 사용하여 $Auth_N(K_3)$의 유효성을 확인한다 (Fig. 4. ②). 특히, Ctr_3이 최신인지 확인하고 *6LBR_Info*가 $GP16_3$을 구성하는 데 사용되는지 확인한다. 유효성 검사는 다음과 같이 확인할 수 있다.

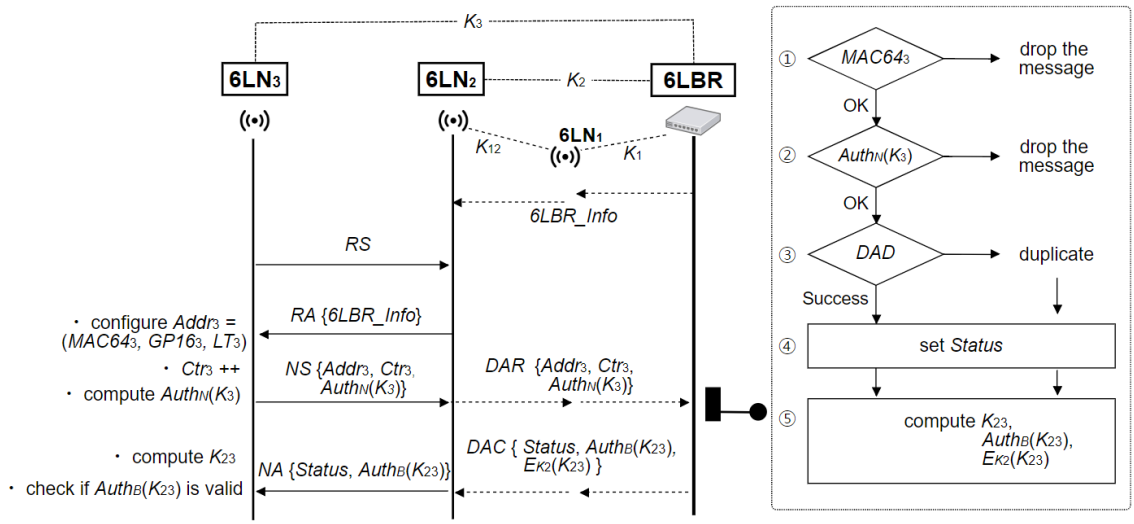

Fig. 4. Secure Address Registration

[Procedure for checking $Auth_N(K_3)$]

Given the received $\{Addr_3, Ctr_3, Auth_N(K_3)\}$ *and stored_6LBR_Info,*

- $(stored\_Ctr_3, stored\_K_3) \leftarrow$ *select* Ctr, K *from DAD Table where* $MAC64 = MAC64_3$;
- *compute* $Auth_N(stored\_K_3) = h(Addr_3 \| Ctr_3 \| stored\_6LBR\_Info \| stored\_K_3)$
- *If* $(Ctr_3 > stored\_Ctr_3)$ and $(Auth_N(K_3) = Auth_N(stored\_K_3))$, *then goto* ③; *else drop the message and stop*;

셋째, 6LBR은 *DAD* 테이블을 사용하여 $GP16_3$의 중복 여부를 확인한다 (Fig. 4. ③). 중복 여부 검사는 초기 주소 등록과 Life Time을 갱신하기 위한 주소 재등록에 따른 두 가지의 경우로 나누어진다. 첫 번째 경우, *DAD* 테이블 항목은 $(MAC64_3, _, _, 0, K_3)$이며 여기서 $6LN_3$의 $GP16_3$, LT_3 및 $Ctr_3 = 0$은 아직 등록되지 않은 상태이다. 6LBR은 $GP16_3$의 중복 여부를 확인한 후, *DAD* 테이블에 $GP16_3$, LT_3 및 Ctr_3을 추가시킨다. 두 번째 경우, *DAD* 테이블의 항목은 $(MAC64_3, GP16_3, LT_3', Ctr_3', K_3)$으로 $GP16_3$은 이미 등록되어 있는 상태이다. 따라서 6LBR은 $Ctr_3 > Ctr_3'$, $LT_3 > LT_3'$ 인 경우, *DAD* 테이블 항목을 (LT_3', Ctr_3')에서 (LT_3, Ctr_3)로 갱신한다.

[Procedure for duplicate address detection]

Given the received $\{Addr_3=(MAC64_3, GP16_3, LT_3)\}$

- *result* ← *select MAC64 from DAD Table where* $GP16 = GP16_3$;
- *If* (*result is null or* $MAC64_3$), *then insert* $(MAC64_3, GP16_3, LT_3, Ctr_3, K_3)$ *into DAD Table where* $MAC64 = MAC64_3$; *return* "*success*";

else return "*duplicate*";

중복 여부 검사의 결과에 따라 *Status*는 "success"또는 "duplicate"가 반환된다 (Fig. 4. ④). 이어서, $6LN_3$와 $6LN_2$ 사이의 링크키는 pseudo-random 함수인 *prf*(.)를 사용하여, $K_{23} = prf(K_3, Ctr_3 \| 6LN_3 \| 6LN_2 \| 6LBR)$로 계산된다. $6LN_3$은 링크키 K_{23}가 자신의 디바이스 키 K_3에서 파생되므로 스스로 계산할 수 있다. 6LBR은 $6LN_3$와 K_3을 공유하고 있으므로 링크키 K_{23}을 계산할 수 있다. 6LBR은 링크키를 공유하기 위해 인증자 $Auth_B(K_{23}) = h(Auth_N(K_3) \| Status \| K_{23})$ 및 암호화된 링크키 $E_{K2}(K_{23})$를 계산한다. 그런 다음, 6LBR은 6LR (Fig. 4.의 $6LN_1$)을 통해 $6LN_2$에 $DAC\{Status, Auth_B(K_{23}), E_{K2}(K_{23})\}$ 메시지를 전송한다. $6LN_2$는 링크키 K_{23}을 획득하고 $Auth_B(K_{23})$가 유효한지 여부를 검사한 후, $NA\{Status, Auth_B(K_{23})\}$ 메시지를 $6LN_3$로 전송한다. $6LN_3$은 $Auth_B(K_{23})$가 유

효하다면 6LoWPAN-ND 주소 등록의 결과를 승인한다.

IV. 보안 분석

4.1 접근 제어 및 인증

LoWPAN 가입을 허가받은 6LN 집합 (S)은 LoWPAN에 배치되기 전에 결정된다. 즉, 6LBR의 DAD 테이블은 $6LN_j \in S$에 대한 항목 ($MAC64_j$, _, _, 0, K_j)으로 초기화된다. Fig. 5.에서 $6LN_3$가 $6LN_2$를 통해 LoWPAN 가입을 시도 할 때, $6LN_2$는 $6LN_3$가 인가되었는지, $6LN_3$는 $6LN_2$가 정상 라우터임을 확인하기 위한 상호 인증이 필요하다. 하지만 이들 사이의 링크키가 할당되지 않았으므로 직접적인 인증을 수행할 수 없다. 때문에, 6LBR은 상호 인증을 지원하기 위한 인증 서버의 역할을 수행한다. 6LBR은 DAR 메시지의 $Auth_N(K_3)$에 대한 유효성을 판별하고, 유효하다면 $6LN_3$이 인가되었다고 판단한다. $6LN_2$는 K_{23}을 획득하고 DAC 메시지에서 $Auth_B(K_{23})$를 검증함으로써 6LBR 및 $6LN_3$을 인증한다. $6LN_3$는 $6LN_2$로부터 NA 메시지를 수신하고 $Auth_B(K_{23})$의 검증이 성공적일 때 6LBR 및 $6LN_2$를 인증한다. 이전 연구의 경우, 6LBR 인증이 지원되지 않기 때문에 몇 가지의 보안 취약점을 갖는다. 그러나 제안된 보안 메커니즘은 상호 인증을 통하여 보안 취약점을 해결하였다.

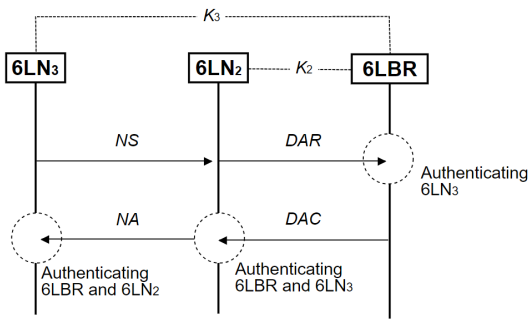

Fig. 5. Authentication of 6LNs

4.2 손상된 노드 공격

$6LN_2$가 손상되면, 공격자는 $6LN_2$를 통해 LoWPAN에 가입하기 위한 DoS 공격을 시도 하거나 $6LN_2$에게 전달되는 NS 메시지를 삭제할 수 있다. 하지만 제안된 보안 메커니즘은 인접한 6LN 간 각 링크에 고유한 링크키가 할당되어 있기 때문에 손상된 노드 공격은 LoWPAN의 다른 부분에 영향을 미치지 않는다. 또한, 링크키는 디바이스 키를 기반으로 한 해시 함수를 사용하여 파생되기 때문에, 공격자는 $6LN_2$에 속한 하위 6LN의 디바이스 키를 링크키로부터 도출할 수 없다. 예를 들어, 3개의 6LN ($6LN_3$, $6LN_4$ 및 $6LN_5$)이 $6LN_2$를 통해 LoWPAN에 가입하면 3개의 링크키 (K_{23}, K_{24} 및 K_{25})가 각 6LN과 손상된 $6LN_2$간에 공유된다. 그러나 손상된 $6LN_2$를 제어하는 공격자는 연결된 디바이스의 디바이스 키 (K_3, K_4 및 K_5)를 얻을 수 없다. 제안하는 보안 메커니즘은 디바이스 키 K_j를 기반으로 생성된 $Auth_N(K_j)$와 링크키 K_{ji}를 기반으로 생성된 $Auth_B(K_{ji})$의 두 인증자를 사용하여 디바이스 키를 보호하고 메시지의 무결성을 보장한다.

공격자는 손상된 $6LN_2$의 디바이스 키 K_2를 획득하여 합법적인 노드로 위장해 $6LN_2$를 통하여 LoWPAN에 가입하려는 6LN의 주소 구성을 방해할 수 있다. 하지만 RA 메시지에 포함된 $6LBR_Info$가 인증자 $Auth_N(K_j)$에 포함하여 계산되고, 공격자는 디바이스키 K_j를 알 수 없으므로 인증자 $Auth_N(K_j)$를 위조할 수 없다. 따라서 제안된 메커니즘은 손상된 노드 공격 하에서의 위조된 6LoWPAN 메시지 공격으로부터 안전하다. Replay 공격 또한 6LBR의 DAD 테이블 상의 Ctr_3을 사용하여 $Auth_N(K_3)$ 및 $Auth_B(K_{23})$에 대한 신규성 검증을 수행하여 방지할 수 있다. NA 메시지는 Ctr_3을 직접적으로 포함하지 않지만, $Auth_N(K_3) = h(Addr_3 \| Ctr_3 \| 6LBR_Info \| K_3)$이 $Auth_B(K_{23})$의 연산에 포함되므로 NA 메시지의 신규성이 보장될 수 있다.

4.3 Hop-by-Hop 링크키

인접한 두 개의 6LN 사이에 IEEE 802.15.4 보안을 적용하려면 미리 링크키가 설정되어 있어야 한다. 인가된 6LN 집합 ($= S$)을 감안할 때, 모든 6LN 쌍에서 각 링크키가 공유되도록 노드에 키 재료 세트를 사전 로드하는 것은 효율적이지 않다. 하지만 무선 센서 네트워크를 위한 키 사전 분배 방식 [8, 9]의 대부분은 이러한 접근 방식을 따른다. 그러나 LoWPAN 네트워크의 경우, Fig. 2.와 같이 링크키는 2개의 인접한 6LN 사이에서만 설정되어야

하며, 그 중 한 6LN은 다른 6LN을 통해 LoWPAN에 가입한다. 이 경우, 6LBR은 링크키 분배 센터 역할을 수행할 수 있다. 즉, IEEE 802.15.4 보안에 대한 링크키 설정은 6LoWPAN-ND 주소 등록 중에 수행된다. 제안된 링크키 설정 프로토콜의 특징은 등록 수명을 업데이트하기 위한 6LoWPAN-ND 주소 재등록이 수행될 때 링크키가 업데이트될 수 있다는 점이다. 예를 들어,Fig. 5에서, 링크키는 $K_{23} = prf(K_3, Ctr_3 \parallel 6LN_3 \parallel 6LN_2 \parallel 6LBR)$으로 Ctr_3을 기반으로 계산되며, 이는 Ctr_3 가 증가될 때 업데이트된다.

V. 성능 비교

5.1 IEEE 802.15.4 및 6LoWPAN-ND 메시지 형식

Fig. 6.은 6LoWPAN 주소 등록을 위한 IEEE 802.15.4 프레임 및 6LoWPAN-ND 메시지의 구조를 나타낸다. 여기서 6LoWPAN 메시지 (*NS, NA, DAR, DAC*)는 IEEE 802.15.4 프레임으로 캡슐화되며 프레임 크기는 127바이트로 제한된다. IEEE 802.15.4 MAC Header는 source / destination PAN identifier 및 source / destination MAC Address의 네 가지의 주소 지정 필드로 구분된다. 여기서 PAN 식별자 및 MAC 주소는 각각 2바이트 및 2/6바이트다. 모든 6LoWPAN 디바이스가 단일 PAN으로 구성된 LoWPAN에 속하고 Short MAC address (*MAC16*)가 사용된다고 가정하면 source PAN identifier는 생략할 수 있으므로 주소 필드는 6바이트 길이가 된다.

6LoWPAN-ND 메시지를 캡슐화하는 IEEE 802.15.4 프레임을 최적화하기 위해 IPHC Compression[1, 2]을 사용하여 IPv6 Header (40 바이트)를 압축할 수 있다. *NS / NA* 메시지에 대한 Dispatch Byte와 IPHC Byte를 가진 IPv6 Header는 메시지의 송신자와 수신자가 동일한 로컬 링크 (예 : Fig 3.(b)의 $6LN_2$와 $6LN_3$)에 위치하므로 최대 2바이트까지 줄일 수 있다. *DAR / DAC* 메시지에 대한 Dispatch Byte 및 IPHC Byte를 갖는 IPv6 Header는 최대 7바이트 (예 : Fig. 2.(b)의 $6LN_2$ 와 6LBR)까지 감소 될 수 있다. 따라서 IEEE 802.15.4 페이로드는 6LoWPAN 메시지를 위한 충분한 공간을 제공하며 몇 가지 옵션을 포함한다.

Fig. 6.의 점선으로 된 박스는 6LoWPAN-ND 메시지 옵션 (RFC 6775)[12] : SLLAO (Source Link-Layer Address Option) 및 ARO (Address Registration Option)을 나타낸다. Target Address와 Registered Address 필드는 $GP16_3$이 채워지고 EUI-64 필드는 $MAC64_3$가 채워진다. 본 논문에서 제안하는 안전한 6LoWPAN 주소 등록을 위해 보안 관련 옵션인 Authenticator 옵션과 Key Transport 옵션이

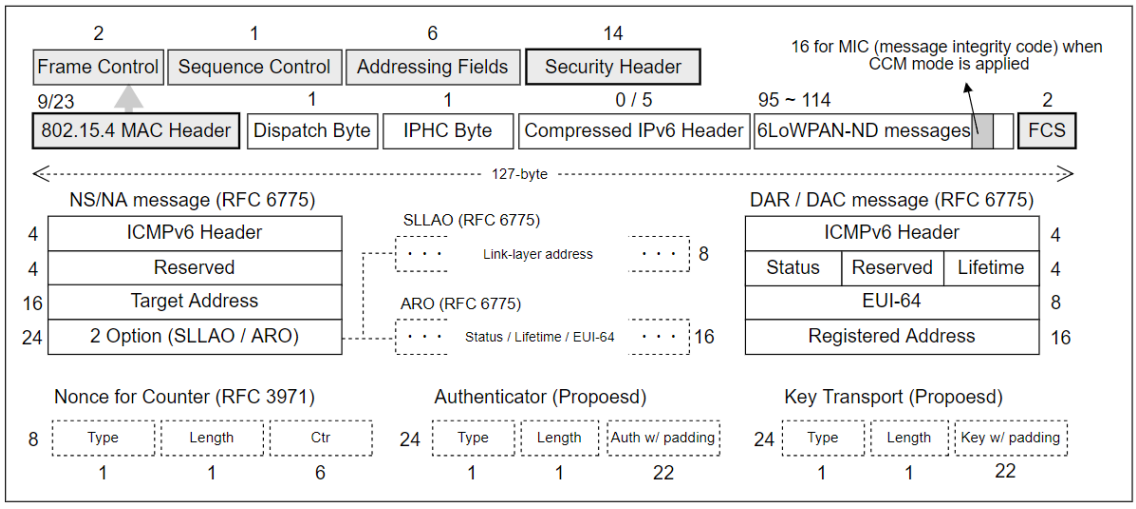

Fig. 6. IEEE 802.15.4 and 6LoWPAN-ND Message format

새로 정의되었다. Authenticator는 $Auth_N(K_3)$ / $Auth_B(K_{23})$를 전달하는 데 사용되고, Key Transport는 $E_{K2}(K_{23})$를 전달하는 데 사용된다. RFC 3971[17]의 *Nonce* 옵션은 Counter로 사용된다. 옵션의 길이는 8바이트의 배수여야 하므로 Authenticator 및 Key Transport 옵션에 패딩 작업을 수행한다.

5.2 보안 오버 헤드 비교

Table 2.는 기존의 6LoWPAN-ND 메시지[12], L-SEND 메시지[18], 제안된 6LoWPAN-ND 메시지의 크기를 보여준다. L-SEND의 경우, 6LoWPAN-ND 주소 등록을 위해 *NS* / *NA* / *DAR* / *DAC* 메시지는 각각 2회씩 교환된다. 기존의 6LoWPAN-ND[12]와 L-SEND[18]는 주소등록 과정에서 두 개의 인접한 6LN 사이에 링크키를 공유하는 방법을 지정하지 않고 IEEE 802.15.4 hop-by-hop 보안을 사용하여 보안이 유지된다고 가정한다. 제안된 방법에서는 IEEE 802.15.4 hop-by-hop 보안이 *NS* 및 *NA* 메시지에는 사용되지 않지만 *DAR* 및 *DAC* 메시지에는 사용된다.

Fig. 7.은 각각의 6LoWPAN-ND 메시지를 캡슐화하는 IEEE 802.15.4 프레임의 크기를 보여준다. IEEE 802.15.4 hop-by-hop 보안의 CCM (Counter-CBC-MAC) 모드가 적용될 때, 보안 Header를 포함하는 IEEE 802.15.4 Header / Trailer (25바이트)는 Dispatch Byte, IPHC Byte, Compressed IPv6 Header 및 6LoWPAN-ND 메시지에 대한 페이로드가 연결된다. 또한, 무결성을 위한 16바이트 크기의 MIC (Message Integrity Code)가 페이로드에 포함된다. 보안을 사용하지 않으면 Security Header가 없는 IEEE 802.15.4 Header / Trailer (11바이트)가 사용된다.

Table 2. Comparison of 6LoWPAN-ND message size

message type	RFC 6775	L-SEND (1st/2nd)	Proposed
NS	48	48 / 136	80
NA	48	56 / 48	72
DAR	32	48 / 136	64
DAC	32	48 / 48	80

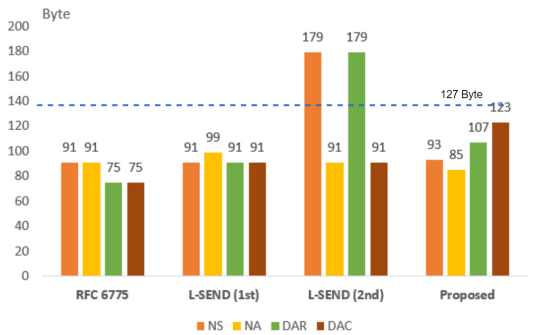

Fig. 7. Size of IEEE 802.15.4 frames encapsulating each of 6LoWPAN-ND messages (in bytes)

예를 들어 기존의 6LoWPAN-ND의 경우, IEEE 802.15.4 header 및 trailer 25바이트, Dispatch / IPHC / IPv6 Header 2바이트, *NS* 48바이트, MIC 16바이트로 총 91바이트의 크기를 갖는다. 반면에 제안된 방법은 IEEE 802.15.4 header 및 trailer 11바이트, Dispatch / IPHC / IPv6 header 2바이트, *NS* 80바이트로 총 93바이트의 크기를 갖는다. Fig. 7.을 보면 기존의 6LoWPAN-ND 의 경우, 네 개의 메시지 크기가 332바이트인데 반해 제안된 방법의 경우, 네 개의 메시지의 크기는 408바이트로 증가한다. 이를 보면 전체 프레임 크기가 약 22.8% 증가하며 RFC 6775의 보안을 유지하는 데 드는 암호화 비용을 초래시키는 것을 확인할 수 있다. 하지만 각 메시지의 크기가 IEEE 802.15.4 최대 프레임 크기인 127바이트를 초과하지 않기 때문에, 단편화가 필요한 L-SEND의 제 2 *NS* 및 *DAR* 메시지와 다르게 단편화에 대한 처리 지연은 발생하지 않는 것을 확인할 수 있다.

Table 3.은 *NS* / *NA* / *DAR* / *DAC* 메시지가 처리 될 때, 6LN, 6LR 및 6LBR에 필요한 암호화 작업을 보여준다. RFC 6775[12]의 경우, 6LN은 *NS* 및 *NA* 메시지를 처리하기 위해 AES 기반 *ccm* 작업을 2회 수행해야 한다. L-SEND의 경우, *NS* 및 *NA* 메시지가 두 번 교환되기 때문에 6LN은 4 *ccm*, 6LR은 8 *ccm* 작업이 필요하다. 또한, 6LN 및 6LBR 간 ECDSA 생성 및 검증에 대한 추가적인 연산이 필요하다. 제안된 방법에서는 6LN이 *NS* 메시지를 처리하기 위해 1 *hash* 연산이 필요하고, *NA* 메시지를 처리하기 위해서 1 *hash* 연산과 링크키

Table 3. Comparison of Cryptographic Operations

	RFC 6775	L-SEND	Proposed
6LN	2 *ccm*	4 *ccm* + 1 *EC* + 1 *hash*	2 *hash* + 1 *kg*
6LR	4 *ccm*	8 *ccm*	2 *ccm* + 1 *hash* + 1 *ctr*
6LBR	2 *ccm*	4 *ccm* + 1 *EC* + 1 *pr*	2 *ccm* + 2 *hash* + 1 *ctr* + 1 *kg*

- *ccm*: CCM operation for IEEE 802.15.4 hop-by-hop security
- *ctr*: AES-CTR operation for $E_{K_2}(K_{23})$
- *hash*: SHA-1 cryptographic hash operation for L-SEND's key hash, $Auth_N(.)$ and $Auth_B(.)$
- *EC*: elliptic curve DSA generation or verification
- *kg*: HMAC-SHA-1 operation for computing a link key K_{23}
- *pr*: pseudo-random number generation for *Nonce*

계산을 위한 1 *kg* 연산이 필요하다. 따라서 6LoWPAN-ND 주소 등록 중에 6LN을 처리하기 위해서 총 2 *hash* 와 1 *kg*의 연산이 필요하다.

본 연구의 실효성 검증 연구로서 Fig. 7.과 Table 3.을 바탕으로 Cooja 시뮬레이터의 Sky mote를 사용하여 6LoWPAN-ND 주소 등록 중에 6LN, 6LR 및 6LBR에 필요한 암호화 작업의 누적 처리 시간(밀리 초)을 측정했다. L-SEND는 ECDSA 생성 및 검증에 대한 암호화 연산이 필요하기 때문에 6LoWPAN-ND 주소 등록에 대한 처리 시간이 가장 길다. RFC 6775[12]와 비교할 때, 제안된 방식은 6LN 및 6LBR은 각각 1.6 times (39.7ms vs 65.9ms) 및 3.3 times (30.9ms vs 102.6ms)의 추가적인 처리 시간이 소요된다. 제안된 메커니즘은 처리 시간 측면에서 약 59%가 증가하였지만 IEEE 802.15.4 hop-by-hop 보안을 유지하면서 손상된 노드 공격과 같은 기존의 보안 취약점을 해결하였다.

VI. 결 론

본 논문에서는 6LoWPAN-ND 주소 등록과 관련된 보안 문제를 조사했다. 이전의 관련 연구에 보안 취약성이 있음을 발견하여 6LoWPAN-ND 주소 등록과 주소 등록 중에 수행할 수 있는 동적 링크키 분배 아키텍처를 보장하기 위한 보안 프레임 워크를 설계했다. 디바이스 수명주기의 deployment / commissioning 단계에서 각 인증 된 6LN의 디바이스 키가 6LBR에 사전 설치되어 있다고 가정하면, 인접한 두 6LN간에 링크키를 공유할 수 있으며 6LoWPAN-ND의 signaling 메시지를 적절하게 보호할 수 있다 . 따라서 제안된 보안 메커니즘은 IEEE 802.15.4 hop-by-hop 보안의 키 관리 문제를 해결한다. 제안된 보안 메커니즘에서 추가된 세 가지 보안 관련 옵션은 6LoWPAN-ND 표준과 호환된다. 향후, 연구를 위해 NFC, Bluetooth 및 WBAN을 통한 6LoWPAN과 같은 다른 플랫폼에 있는 보안 문제를 조사할 것이다.

References

[1] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks," IETF RFC 4944, Sep. 2007.

[2] J. Hui and P. Thubert, "Compression Format for IPv6 Datagrams over IEEE 802.15.4-based Networks," IETF RFC 6282, Sep. 2011.

[3] S. Misra, S. Goswam, C. Taneja, A. Mukerjee, and M. Obaidat, "A PKI Adapted Model for Secure Information Dissemination in Industrial Control and Automation 6LoWPANs," IEEE Access, vol. 3, pp. 875-889, 2015

[4] Y. Qiu and M. Ma, "A Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks," IEEE Trans. on Industrial Informatics, vol. 12, no. 6, pp. 2074-2085, Dec. 2016.

[5] Certicom Research, "SEC 4: Elliptic Curve Qu-Vanstone Implicit Certificate Scheme (ECQV)," Standard for Efficient Cryptography, Jan. 2013.

[6] P. Porambage, C. Schmitt, P. Kumar, A. Gurtov, and M. Ylianttila, "PAuthKey: A Pervasive Authentication Protocol and Key Establishment Scheme for Wireless Sensor

Networks in Distributed IoT Applications," International Journal of Distributed Sensor Networks, vol. 2014, Article ID 357430.

[7] C. S. Park, "A Secure and Efficient ECQV Implicit Certificate Issuance Protocol for the Internet of Things Applications," IEEE Sensors Journal, vol. 17, no. 7, pp. 2215-2223, Apr. 2017

[8] L. Eschenauer and V. Gligor, "A Key Management Scheme for Distributed Sensor Networks," in Proc. of 9th ACM conference on Computer and Communications Security (ACM-CCS), pp. 41-47, Washington D.C., U.S.A., Nov. 18-22, 2002.

[9] H. Chan, A. Perrig, and D. Song, "Random Key Pre-distribution Schemes for Sensor Networks", in Proc. of the IEEE Symposium on Security and Privacy, 2003, pp. 197-213, Washington D.C., U.S.A., May 11-14, 2003.

[10] L. Oliveira, J. Rodrigues, A. Sousa, and V. Denisov, "Network Admission Control Solution for 6LoWPAN Networks Based on Symmetric Key Mechanisms," IEEE Trans. on Industrial Informatics, vol. 12, no. 6, pp. 2186-2195, Dec. 2016.

[11] A. Esfahani, G. Mantas, R. Matischek, F. B. Saghezchi, J. Rodriguez, A. Bicaku, S. Maksuti, M. Tauber, C. Schmittner, and J. Bastos, "A Lightweight Authentication Mechanism for M2M Communications in Industrial IoT Environment," IEEE Internet of Things Journal, 2017.

[12] Z. Shelby, S. Chakrabarti, E. Nordmark, and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)," IETF RFC 6775, Nov. 2012.

[13] J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby, and C. Gomez, "IPv6 over Bluetooth Low Energy," IETF RFC 7668, Oct. 2015.

[14] L. Seitz, S. Gerdes, G. Selander, M. Mani, and S. Kumar, "Use Cases for Authentication and Authorization in Constrained Environments," IETF RFC 7744, Jan. 2016.

[15] M.A.M. Seliem, K.M.F. Elsayed, and A Kattab, "Optimized Neighbor Discovery for 6LoWPANs: Implementation and Performance Evaluation," Computer Communications, vol. 112, pp. 73-92, Nov. 2017.

[16] C. S. Park and J. H. Lee, "Security Bootstrapping for Secure Join and Binding on the IEEE 802.15.4-Based LoWPAN," IEEE Internet of Things Journal, vol. 4, no. 4, pp. 996-1005, May. 2017.

[17] J. Arkko, J. Kempf, B. Zill, and P. Nikander, "Secure Neighbor Discovery," IETF RFC 3971, Mar. 2005.

[18] P. Thubert, B. Sarikaya, and M. Sethi, "Address Protected Neighbor Discovery for Low-power and Lossy Networks," IETF 6lo WG Internet-Draft, draft-ietf-6lo-ap-nd-06, Feb. 2018.

〈저 자 소 개〉

한 상 우 (Sang-woo Han) 학생회원
2017년 2월: 단국대학교 컴퓨터과학과 졸업
2017년 3월~현재: 단국대학교 소프트웨어 보안 석사과정
〈관심분야〉 정보보호

박 창 섭 (Chang-seop Park) 종신회원
1983년 2월: 연세대학교 경제학과 졸업
1987년 2월: Lehigh University 컴퓨터과학과 석사
1990년 2월: Lehigh University 컴퓨터과학과 박사
1990년 3월~현재: 단국대학교 소프트웨어학과 교수
〈관심분야〉 정보보호, 네트워크 보안, 무선인터넷 및 모바일 컴퓨팅 보안