6LowPAN 환경에서의 안전한 IEEE 802.15.4 가입 프로토콜★

안승현* · 박창섭** · 연한별***

요 약

IoT (Internet of Things) 환경에서 센서노드들과 주고받는 데이터에 대한 보안의 중요성이 높아지고 있다. IoT에 기본이 되는 IEEE 802.15.4에서는 센서노드와 PAN Coordinator 또는 센서노드와 센서노드간의 안전한 통신을 위한 키가 사전에 공유되어 있음을 가정하고 있다. 특히, 네트워크 가입 과정에서 센서노드에 대한 개별 인증이 고려되지 않는 문제점이 존재한다. 본 논문에서는 모든 디바이스에게 사전 공유된 키가 있음을 가정한 기존 연구들의 문제점을 해결한 안전한 가입 프로토콜을 제안한다.

Secure IEEE 802.15.4 Join Protocol for 6LoWPAN

Seung-Hyun Ahn* · Chang-Seop Park** · Han-Beol Yeon***

ABSTRACT

The security of the data exchanged between sensor nodes in IoT (Internet of Things) environment becomes increasing. In the conventional IEEE 802.15.4, the key for secure communication between the sensor node and the sensor node and the PAN Coordinator or the sensor node is assumed to be pre-shared in advance. Especially, there is another problem in that sensor node authentication is not considered during the association process. In this paper, we propose a security scheme that solves the problems of previously proposed protocols with the pre-shared key for all devices.

Key words : 802.15.4, Join, 6LoWPAN, IoT, Association

접수일(2015년 12월 17일), 게재확정일(2015년 12월 28일)

★ 본 연구는 2015년도 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다.(No. 20131020400850)

* 단국대학교 일반대학원 전자계산학과
** 단국대학교 소프트웨어학과(교신저자)
*** 단국대학교 일반대학원 소프트웨어보안전공

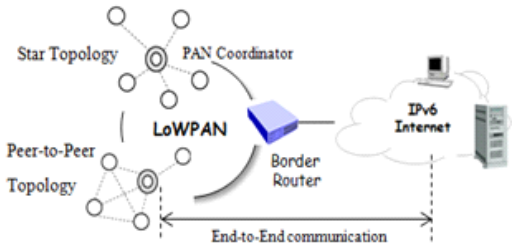
1. 서 론

무선 네트워크 기술과 센서 디바이스 기술의 발전으로 인해 각종 전자기기들과 센서들을 네트워크에 연결하는 IoT 기술과 무선 센서 네트워크에 대한 관심이 높아지고 있다. 무선 센서 네트워크는 제한된 성능의 센서노드 (Constraint sensor node)로 구성된 무선 네트워크를 뜻한다. 대표적인 무선 센서 네트워크인 LoWPAN (Low-power Wireless Personal Area Networks)의 IEEE 802.15.4 [1]에서는 암호화 및 인증을 위하여 전력소모와 계산량을 많이 요구하지 않는 사전에 공유된 대칭키를 사용한다. 새로운 센서노드가 LoWPAN에 가입 시에는 인증절차를 거쳐야 하는데, 기존 기법 [2, 3, 4, 5] 들은 사전에 공유된 그룹키를 사용하거나 마스터 키에서 도출한 그룹키를 사용하여 센서노드들이 LoWPAN에 가입하는 방식이다. 그러나 이러한 방식은 센서노드의 개별적인 식별이 불가능하며 그룹키가 노출될 경우 키의 재설정이 어려운 문제점이 있다. 본 논문에서는 이러한 문제점을 보완한 타원곡선 공개키 기반의 키 관리 프로토콜을 제안한다. LoWPAN의 핵심역할을 담당하는 PAN Coordinator에 사전 등록된 센서노드 주소를 기반으로 센서노드와 PAN Coordinator 간의 ECDH (Elliptic Curve Diffie-Hellman) 프로토콜 [6]을 통한 개별 링크키가 설정되어 센서노드의 가입이 이루어진다. 본 논문의 구성은 다음과 같다. 2장에서는 기존 6LoWPAN과 IEEE 802.15.4에서의 가입 프로토콜 및 보안 Bootstrapping 프로토콜을 소개하고 그 문제점을 논의한다. 3장에서는 기존 방식의 문제를 해결한 ECDH와 CGA (Cryptographically Generated Address) [7]를 이용한 가입 프로토콜을 제안한다. 4장에서는 기존 기법과 제안 기법을 비교분석하고 마지막으로 5장에서는 결론을 내린다.

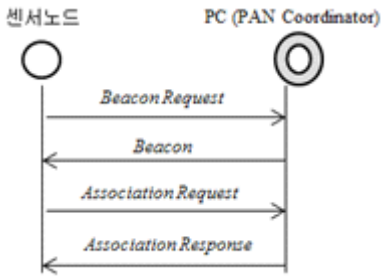
2. 관련연구

2.1 6LowPAN과 IEEE 802.15.4

6LoWPAN [8]은 IEEE 802.15.4 디바이스들로 구성된 LoWPAN에서의 IPv6 패킷 전송을 의미한다. IEEE 802.15.4 디바이스들은 주로 성능이 제한된 디바이스(constraint device)로 짧은 전송범위, 낮은 비트율, 저전력, 낮은 처리능력을 가지는 특징이 있다. 하지만, 6LoWPAN이 제공하는 Header Compression 및 Fragmentation 기능을 통해서 (그림 1)에서와 같이 LoWPAN의 센서노드와 인터넷 상의 호스트 간의 단대단(End-to-End) 통신이 가능하게 된다. IEEE 802.15.4 기반의 LoWPAN에서는 Star Topology와 Peer-to-peer Topology가 지원된다.



(그림 1) IEEE 802.15.4 기반의 6LowPAN



(그림 2) LoWPAN 가입 프로토콜

IEEE 802.15.4 디바이스의 유형으로는 센서노드 그리고 각각의 Topology 내에서 LoWPAN 내의 센서노드들의 동작을 관리하는 PAN Coordinator (PC)가 있다. Star Topology는 하나의 PC에 여러 센서노드들이 1개의 Hop으로 연결되는 구조이고, Peer-to-Peer Topology에서는 LoWPAN 내의 다수의 디바이스들이 상호 연결할 수 있는 구조로 multi-Hop 라우팅이 지원된다.

2.2 IEEE 802.15.4 가입 프로토콜

LoWPAN에 새로운 센서노드가 진입하면 (그림 2)

에서와 같이 IEEE 802.15.4의 가입 프로토콜 (Join Protocol)이 기동된다. Star Topology를 기준으로 설명하면, 새로운 센서노드는 Beacon Request 메시지를 주위에 브로드캐스트로 전송하여 PC의 Beacon 메시지를 유도한다. 이를 기반으로 센서노드와 PC 간에는 Association Request / Association Response 메시지 교환을 통해 LoWPAN 가입이 이루어지게 된다. LoWPAN 가입이 허용될 경우에는 Association Response 메시지를 통해서 16 비트의 네트워크 주소가 센서노드에게 할당된다. IEEE 802.15.4에서는 메시지의 기밀성과 무결성 보장을 위해서 한 쌍의 센서노드 또는 센서노드와 PC간에 공유되는 링크키 (Link Key)와 LoWPAN에 속한 모든 디바이스가 공유하는 그룹키 (Group Key)가 정의되지만, 이들 키에 대한 키 관리 (Key Management)의 개념은 명세하고 있지 않다. 따라서, 키 관리는 상위계층 또는 별도의 루틴을 통해서 정의되어야 한다. 또한, IEEE 802.15.4의 가입 프로토콜에서 어떻게 센서노드의 가입이 허용되는지, 즉 센서노드 인증 역시 명세 되어 있지 않다.

2.3 IEEE 802.15.4 보안 Bootstrapping 기존연구

IEEE 802.15.4에서 정의된 그룹키를 이용하여 센서노드의 LoWPAN 가입을 허용하는 2가지 유형 의 프로토콜 [2, 3, 4, 5]이 제안되었다. 첫째, 사전에 그룹키가 장착된 센서노드에게 다음과 같이 가입을 허용하게 된다 [4, 5]. 즉, *Association Request / Association Response* 메시지에 그룹키 GK가 적용되어 PC는 $MIC(GK)$를 검증함으로써 가입을 요청하는 센서노드에 대한 인증을 수행하게 된다.

$$\text{센서노드} \rightarrow PC: BeaconRequest(Fields1) \quad \text{(식 1)}$$

$$\text{센서노드} \leftarrow PC: Beacon(Fields2) \quad \text{(식 2)}$$

$$\text{센서노드} \rightarrow PC: AssociationRequest(Fields3, MIC(GK)) \quad \text{(식 3)}$$

$$\text{센서노드} \leftarrow PC: AssociationResponse(Fields4, MIC(GK)) \quad \text{(식 4)}$$

위에서 Fields1, Fields2, Fields3, Fields4는 해당 메시지에 포함되는 표준 기본필드들을 지칭하고, 그 이외의 기호는 [표 1]을 따른다. 둘째, 가입이 허용되는 PC를 포함한 모든 센서노드들에게 사전에 마스터 키 MK를 장착한다 [2, 3]. 가입을 시도하는 센서노드는 PC가 브로드캐스트하는 Beacon 메시지에 포함된 PAN-ID와 MAC64PC를 기반으로 그룹키 GK를 다음과 같이 도출하여 (식 3)과 (식 4)에서와 같이 사용한다.

$$GK = kdf(MK, PAN-ID, MAC64_{PC}) \quad \text{(식 5)}$$

<표 1> 표기법

표기법	정 의
I_j	센서노드 $j = A, B, C, ...$
GK, MK	그룹키, 마스터 키
LK_j	센서노드 I_j 와 PC 간에 설정된 링크키
$MAC64_j$	센서노드 I_j 또는 PC 의 64 비트 MAC 주소
$PAN-ID$	PC 가 구성한 LoWPAN 식별자
$kdf(.)$	Key derivation function
$H(.)$	제 2 역상 저항 해쉬함수
$MIC(K)$	이전 모든 필드에 대해 대칭키 K 를 적용하여 계산된 Message Integrity Code

[2, 3, 4, 5]에서 제안하는 기법들에서는 그룹키를 이용한 *Association Request / Association Response* 메시지에 대한 무결성을 보장함으로써, 가입을 요청하는 센서노드에 대한 그룹인증이 수행된다. 가장 치명적인 단점은 그룹키는 LoWPAN에 속해 있거나 또는 거기에 가입할 모든 센서노드들에게 이미 사전에 저장된 것이기 때문에 만약 그것이 노출될 경우에는 다수의 위조 센서노드들이 LoWPAN에 진입하여 작동되는 공격에 매우 취약하다는 단점을 가진다.

3. 제안 프로토콜

본 논문에서는 센서노드의 LoWPAN 가입에 대한 인증관련 기존 연구의 문제점을 해결하기 위해서 두 가지의 암호 Primitive인 ECDH (Elliptic Curve Diffie-Hellman)와 CGA (Cryptographically Generated A

ddress)를 사용한다. ECDH를 이용하여 PC와 센서노드 간의 공유키가 설정되면, 이를 기반으로 LoWPAN 가입에 필요한 Association을 통해 센서노드에 대한 인증을 수행한다. 하지만, ECDH의 경우 양자간에 주고 받는 DH 공개키들에 대한 인증을 위해서 DH 공개키로부터 IEEE 802.15.4 디바이스의 64비트 MAC 주소를 생성하고, 사전에 센서노드들은 PC의 MAC 주소, PC는 LoWPAN에 가입할 센서노드들의 MAC 주소를 사전에 저장해 둔다.

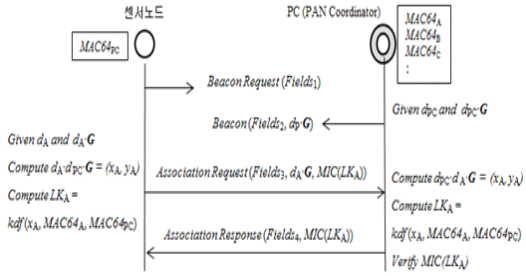
3.1 보안 Bootstrapping을 위한 초기화 작업

유한체 F_p (p는 소수) 상의 타원곡선 $E(F_p)$은 $y^2 \equiv x^3 + ax + b \pmod p$을 만족하는 Point들의 집합이다. 타원곡선 parameter는 (p, a, b, G, n)으로 정의되는데, G는 차수가 $n = |E(F_p)|$ 인 Base Point이다. 타원곡선상의 이산대수 문제는 임의의 Point $D \in E(F_p)$가 주어졌을 때, $D = d \cdot G$를 만족하는 $d \in [1, n]$를 구하는 것으로서, 송수신자 간에 공통된 키를 설정하기 위해 사용되는 ECDH (Elliptic Curve Diffie-Hellman) 프로토콜이 이 문제의 어려움에 기반을 두고 있다. 즉, 송신자와 수신자는 각각 자신의 ECDH 개인키 $d_1, d_2 \in [1, n]$를 생성하여 ECDH 공개키 $D_1 = d_1 \cdot G$, $D_2 = d_2 \cdot G$를 계산하고, 서로 ECDH 공개키를 주고받음으로써 $d_1 \cdot d_2 \cdot G = (x, y)$ 이 양자간에 공유되어 공통된 키 $x \in [0, p-1]$를 도출하게 된다. 하지만, ECDH 프로토콜만으로는 프로토콜에 참여하는 송수신자에 대한 인증은 결여되어 있기에 ECDH 공개키에 대한 인증서 발급을 통한 별도의 방식이 보완되어야 한다. 하지만, 본 논문에서는 ECDH 공개키에 일방향 해쉬함수를 적용하여 주소를 도출하는 CGA를 이용하여 인증서 사용을 대체한다.

모든 센서노드 I_j $j = A, B, C, \ldots$는 LoWPAN에 참여하기 이전에 다음과 같은 초기화 과정을 거친다. 첫째, 임의의 $d_j \in [1, n]$를 생성하여 계산된 $d_j \cdot G = D_j = (x_j, y_j)$를 기반으로 I_j의 64비트 MAC 주소 (EUI-64), $MAC64_j = H(x_j, PAN-ID)$를 도출한다. PC의 MAC 주소, $MAC64_{PC} = H(x_{PC}, PAN-ID)$, where $D_{PC} = d_{PC} \cdot G = D_{PC} = (x_{PC}, y_{PC})$ 역시 같은 방식으로 도출된다. 둘째, 각각의 센서노드 I_j에 $\{d_j, D_j, MAC64_j\}$를 구성하고 PC에는 앞으로 LoWPAN에 참여 할 센서노드들의 64비트 MAC 주소, $MAC64_j$를 미리 저장한다.

3.2 안전한 LoWPAN 가입 프로토콜

(그림 3)에서와 같이 센서노드 I_A가 *Beacon Request* 메시지를 브로드캐스트하면, PC는 자신의 ECDH 공개키 $d_{PC} \cdot G$를 탑재한 *Beacon* 메시지를 전송한다. 센서노드는 먼저 자신의 ECDH 개인키 $d_A \in [1, n]$와 PC의 ECDH 공개키를 기반으로 $d_A \cdot d_{PC} \cdot G = (x_A, y_A)$을 계산한 후에 $LK_A = kdf(x_A, MAC64_A, MAC64_{PC})$를 도출한다. 또한, 자신의 ECDH 공개키 $d_A \cdot G$를 탑재한 *Association Request* 메시지에 대한 무결성 보장을 위해 $MIC(LK_A)$를 계산하여 PC에게 전송한다. PC 역시 LK_A를 계산하여 $MIC(LK_A)$에 대한 검증이 성공하면 I_A의 LoWPAN 가입을 허용하는 *Association Response* 메시지를 보내고, I_A또한 이에 대한 무결성을 검증한다.

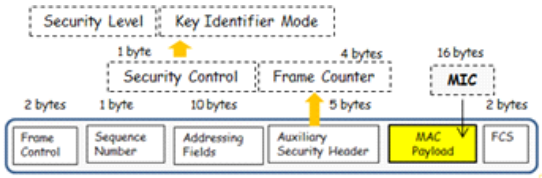


(그림 3) 제안 LoWPAN 가입 프로토콜

3.3 IEEE 802.15.4 표준 payload 수정

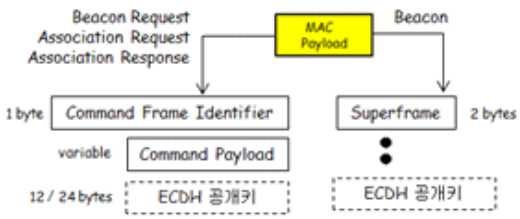
IEEE 802.15.4에서는 4가지 유형의 Frame들이 정의되는데, (그림 4)에서는 MAC Command Frame 및 Beacon Frame에 공통적으로 적용되는 구성을 보여주고 있다. *Beacon Request, Association Request / Response* 메시지 모두 MAC command Frame을 이용한다. Addressing Field에는 송수신 디바이스의 PAN-ID 및 64비트 MAC 주소가 탑재되는데, 본 논문에서와 같이 동일한 LoWPAN내의 PC와 센서노드

간의 통신에서는 송신자 또는 수신자 정보 1개만이 사용된다. 메시지에 대한 무결성이 요구될 경우에는 관련정보가 Auxiliary Security Header 부분에 명시되며, 링크키 또는 그룹키로 계산된 MIC가 MAC Payload에 첨가된다. Security Level 필드에는 메시지에 대한 기밀성 / 무결성 적용여부, Key Identifier Mode에는 링크키 및 그룹키의 접근방식에 대한 정보가 탑재된다. Frame Counter는 메시지에 대한 재생공격을 방지하기 위해 사용된다.



(그림 4) IEEE 802.15.4 Command Frame / Beacon Frame Format

(그림 5)에는 MAC Command Frame과 Beacon Frame의 MAC Payload의 세부구성을 보여주고 있다. Command Frame Identifier를 통해서 *Beacon Request, Association Request / Response* 메시지가 식별되며 Command Payload에는 해당 메시지를 구성하는 (그림 3)의 $Fields_1$, $Fields_3$,$Fields_4$들이 각각 채워지게 된다. Beacon Frame의 MAC Payload의 세부구성은 $Fields_2$에 해당하는 *Superframe*과 같은 다수의 세부 필드들로 구성된다. 본 논문에서 제안하는 ECDH 공개키는 점선으로 표시된 부분과 같이 별도로 정의된 필드에 채워진다.



(그림 5) Command Frame / Beacon Frame의 세부구성

4. 안전성 분석

ECDH와 CGA를 이용한 본 제안방식의 안전성은 타원곡선 상의 이산대수 문제의 어려움에 기반을 두고 있다. 특히, CGA를 사용하기 때문에 PC에 저장되어있는 임의의 센서노드 I_j의 MAC 주소 $MAC64_j = H(x_j, PAN-ID)$에 대한 ECDH 공개키 $d_j \cdot G = D_j = (x_j, y_j)$와 개인키 d_j 쌍을 위조할 수 없어야 한다. 즉, 공격자 Z가 선정한 개인키 d_Z 및 공개키 $d_Z \cdot G = D_Z = (x_Z, y_Z)$에 대한 MAC 주소가 $MAC64_Z = H(x_Z, PAN-ID) = MAC64_j = H(x_j, PAN-ID)$이기만 하면 MAC 주소 위조공격에 성공하게 된다. 위 공격의 성공 가능성은 MAC 주소를 도출하는 데에 사용되는 해쉬함수 $H(.)$의 출력길이와 관련이 있다. 만약 다항식 l과 보안 매개변수 n에 대해 $|H(.)| = l(n)$이면, 공격자는 공격대상의 MAC 주소를 생성할 수 있는 공개키 및 개인키를 찾기 위해서 거의 $2^{l(n)}$ 번의 계산을 수행해야 한다. 누구든지 MAC 주소를 생성할 수 있지만, PC에 사전 등록되어 있지 않다면 사용할 수 없게 된다.

Formal Proof (by Reduction)를 위해 해쉬함수를 다시 정의한다. 즉, GenH를 보안매개변수 1^n을 입력값으로 하고 키 s를 출력하는 Probabilistic Algorithm이라고 할 때, 해쉬함수는 PPT (Probabilistic Polynomial-Time) 알고리즘 $\Pi = (\mathrm{Gen_H}, \mathrm{H}^s)$으로 정의된다. 그리고 $H^s : \{0,1\}^* \rightarrow \{0,1\}^{l(n)}$는 알려진 키 s를 사용하는 해쉬함수이다. 다음 Experiment는 Π, 공격자 Z 그리고 보안매개변수 n에 대해서 정의된다.

<제 2역상 찾기 Experiment $2PR_{\Pi,Z}(n)$>

- $s \leftarrow \mathrm{Gen_H}(1^n)$.
- 공격자 Z는 (s, y)를 입력 받고, y'을 출력한다. 이때, $y, y' \in \{0,1\}^*$.
- $2PR_{\Pi,Z}(n) = 1$ if and only if $y \neq y'$ and $H^s(y) = H^s(y')$

[정의 1]

만약 모든 PPT 공격자들 Z에 대해서 $\Pr[2PR_{\Pi,Z}(n) = 1] \leq \mathrm{negl(n)}$을 만족하는 negligible function $negl(n)$이 존재한다면, 해쉬함수

$\Pi = (\mathrm{Gen}_H, H^s)$는 제2역상 저항성을 만족한다.

[정리 1]

만약, $\Pi = (\mathrm{Gen}_H, H^s)$가 제 2 역상 저항성을 만족하는 해쉬함수이면, $MAC64_j = H(x_j, PAN-ID)$는 위조공격에 대해 안전하다.

[증명]

Π'가 $MAC64_j = H(x_j, PAN-ID)$을 나타내고 W는 특정 센서노드 I_j의 MAC 주소를 위조하기 위해 Π'을 공격하는 PPT 공격자라고 하자. 이때, 다음의 Experiment를 정의한다.

MAC주소위조 Experiment $\mathrm{MACforge}_{\Pi', W}(n)$

- 공격자 W 는 $(s, x_j, PAN-ID)$를 입력받고 x_j'을 출력한다.
- $\mathrm{MACforge}_{\Pi', W}(n)$=1 if and only if $x_j \neq x_j'$ and $H^s(x_j, PAN-ID) = H^s(x_j', PAN-ID)$ 공격자 W 를 서브루틴으로 사용하여 $2PR_{\Pi,Z}(n)$ 의 Π 를 공격하는 다음의 공격자 Z 를 고려해 보자.

< 공격자 Z >

- (s, y)를 입력 받는다. $(y = x_j \| PAN-ID)$
- $q := y$
- $W(s, q)$ 실행. W는 $q' = x_j' \| PAN-ID$ 반환 $(x_j \neq x_j')$
- $y' := q'$
- Z 는 y'을 출력.

$\Pr[2PR_{\Pi,Z}(n) = 1] \geq \Pr[MACforge_{\Pi', W}(n)]$은 자명하다. 또한, $H^s(.)$가 제2역상 저항성을 만족하기 때문에 $\Pr[2PR_{\Pi,Z}(n) = 1] \leq \mathrm{negl}(n)$이 만족된다. 따라서, $\Pr[MACforge_{\Pi,W}(n)] \leq \Pr[2PR_{\Pi,Z}(n) = 1] \leq \mathrm{negl}(n)$ 이기 때문에 $MAC64_j = H(x_j, PAN-ID)$은 MAC 주소 위조공격에 안전하다.

5. 비교분석

5.1 안전성 비교분석

기존기법에서는 그룹키가 센서노드들에게 이미 사전에 저장된 것이기 때문에 만약 그것이 노출될 경우에는 다수의 위조 센서노드들이 LoWPAN에 진입하여 작동되는 공격에 매우 취약하다. 하지만, 제안방식에서는 각각의 센서노드는 PC와의 ECDH 방식을 통한 개별 링크키가 설정되고, 가입할 센서노드들의 목록이 PC에 이미 설정되어 있기 때문에 특정 센서노드의 키 정보가 노출되어도 공격은 해당 센서노드에만 국한되게 된다.

5.2 성능 비교분석

기존방식에 비해 제안방식에서는 ECDH 기반의 링크키 설정작업을 위한 추가 연산이 필요하며, ECDH 공개키 탑재를 위한 추가 필드가 요구된다. TinyOS 2.1.1.2가 탑재된 CC2420 Mote에 ECDH 코드 [8]를 올려서 ECDH를 이용한 링크키 생성에 소요되는 에너지 소모율을 계산하였다. ECDH에 사용한 F_p 상에서의 타원곡선 $y^2 = x^3 + ax + b(\mathrm{mod}\ p)$은 192비트 (24 바이트) parameter, Base Point는 compressed된 Point를 사용한다.

p = FFFFFFFF FFFFFFFF FFFFFFFF
FFFFFFFF FFFFFFFE FFFFEE37
$= 2^{192} - 2^{32} - 2^{12} - 2^8 - 2^7 - 2^6 - 2^3 - 1$

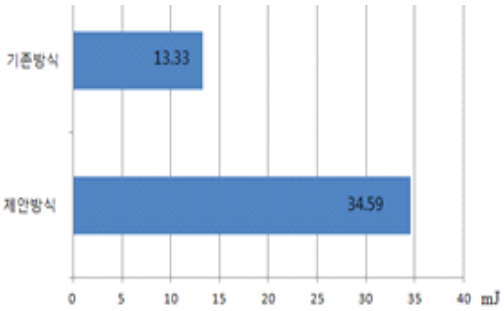
a = 00000000 00000000 00000000
00000000 00000000 00000000

b = 00000000 00000000 00000000
00000000 00000000 00000003

Base Point G = (03 DB4FF10E C057E9AE 26B07D02 80B7F434 1DA5D1B1 EAE06C7D).

링크키 계산을 위해서는 5.20 · 106 clock cycles (0.71 sec)이 소요되고, 이는 17.04 mJ에 해당된다. IEEE 802.15.4 가입 프로토콜 메시지들을 송수신하는 데에 필요한 에너지 소모율을 계산하기 위해서 디바이스들에 의해서 송수신되는 메시지 바이트 수를 고려한다. 센서 네트워크에서 1 비트를 송수신하는 데에 소요되는 에너지는 800 ~ 1,000 개의 명령어를 수행하는 데에 소요되는 에너지에 상응하기 때문에 메시지 송수신에 소요되는 에너지 소모율만을 대상으로 한다. 1 바이트의 메시지를 송수신하는 데에 소요

되는 에너지가 0.13 mJ [9]이라고 가정한다면 기존방식은 13.33 mJ, 제안방식은 17.55 mJ이 소요된다.



(그림 6) 에너지 소모율 비교

결론적으로 에너지 소모율의 경우, 사전 공유된 그룹키를 사용하는 기존방식이 본 논문의 제안방식에 비해 (그림 6)에서와 같이 약 38.8%의 효율성을 보여주고 있다. 이는 제안방식에서 링크키 계산 및 ECDH parameter 추가에 따른 전송 바이트 수의 증가로 인한 결과이다. 하지만, 제안방식의 가입 프로토콜은 LoWPAN에 최초 가입 시에 행해지는 일회성 프로토콜이기 때문에 그 실효성이 크게 떨어지지는 않는다고 판단된다.

6. 결 론

IEEE 802.15.4 LoWPAN에서 센서노드가 가입 시에는 인증절차가 수반되어야 한다. 표준 및 기존연구에서는 인증에 소요되는 키가 공유되어 있다는 가정을 하고 있다. 특히, 기존연구에서는 그룹키의 공유를 가정하고 있지만, 이에 대한 보안상의 취약함이 지적되었다. 본 논문에서는 ECDH와 CGA에 기반을 둔 안전한 가입 프로토콜을 제안하였다. 비록 추가의 연산 및 IEEE 802.15.4 표준 프레임에 추가필드로 인한 에너지 소모율이 증가되지만, 가입 프로토콜은 일회성이며 또한 양자간의 개별키인 링크키의 설정방식을 도입했다는 데에 의의가 있다.

참고문헌

[1] IEEE std. 802.15.4-2011, Part 15.4: Low-Rate WPANs, June 2011.

[2] S. Sciancalepore, S. G. Piro, E. Vogli, G. Boggia, and L. A. Grieco, “On Securing IEEE 802.15.4 Networks through a Standard Compliant Framework,” In Proc. of the 2014 Euro Med Telco Conference, pp. 1-6, Naples, Nov. 12-15, 2014.

[3] G. Piro, G. Boggia, L. A. Grieco, “A Standard Compliant Security Framework for IEEE 802.15.4 Networks,” in Proc. of the IEEE World Forum on Internet of Things, pp. 27-30, Seoul, Mar. 6-8, 2014.

[4] 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.

[5] S. Sciancalepore, A. Capossele, G. Piro, G. Boggia, G. Bianchi, “Key Management Protocol with Implicit Certificates for IoT systems,” In Proc. of the 2015 Workshop on IoT challenges in Mobile and Industrial Systems, pp. 37-42, Florence, May 18-22, 2015.

[6] Certicom Research, Standard for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography, Sep. 2000.

[7] T. Aura, “Cryptographically Generated Addresses,” IETF RFC 3972, Mar. 2005.

[8] C. Lederer, R. Mader, M. Koschuch, J. Großschadl, A. Szekely, and S. Tillich, “Energy-Efficient Implementation of ECDH Key Exchange for Wireless Sensor Networks,” in Information Security Theory and Practice – WISTP 2009, LNCS, vol. 5746. Springer Verlag, pp. 112 - 127, 2009.

[9] J. Hill, R. Szewczyk, A. Woo, S. Hollar, D. Culler, and K. Pister, “System Architecture Directions for Networked Sensors,” in Proc. of the Ninth International Conference on Architectural Support for Programming Languages and Operating Systems, vol. 35, pp. 93-104, Dec. 2000,.

[저 자 소 개]

안 승 현 (Seung-Hyun Ahn)

2013년 8월 단국대학교 컴퓨터과학과 학사
2013년 9월~ 현재 단국대학교 전자계산학과 석사 재학

email : corokuru@nate.com

박 창 섭 (Chang-Seop Park)

1983년 2월 연세대학교 경제학과 학사
1987년 2월 Lehigh University 컴퓨터과학과 석사
1990년 2월 Lehigh University 컴퓨터과학과 박사
1990년 3월~현재: 단국대학교 소프트웨어학과 교수
email : csp0@dankook.ac.kr

연 한 별(Han-Beol Yeon)

2014년 8월 단국대학교 컴퓨터과학과 학사
2015년3월~ 단국대학교 소프트웨어보안 석사 재학

email : hihihi891023@gmail.com