지그비 네트워크에서 효율적인 TCA 및 MAC 프레임 구조 설계

이협건 O, 이경화, +원광호[1], 신용태
숭실대학교
{hglee O, khlee}@cherry.ssu.ac.kr, + khwon@keti.re.kr, shin@ssu.ac.kr

An Efficient TCA and MAC Frame Structure Design in ZigBee Networks

Hyeopgeon Lee O, Kyounghwa Lee, +Kwangho Won, Yongtae Shin
Soongsil Univ.

요 약

지그비에서는 Trust Center 역할을 정의하고 이를 통한 키 분배를 통해 안전한 통신을 한다. 그러나 현재 표준에서 사용하는 TCA 는 모든 트래픽이 Trust Center 로 집중됨으로써 부하 및 지연이 발생된다. 또한 표준에서 사용하는 보안 프로토콜은 서비스의 중요도와 상관없이 암·복호화를 수행한다. 본 논문에서는 지그비 네트워크에서 효율적인 TCA 및 MAC 프레임 구조 설계하였다. 제안하는 TCA 는 Trust Center 간의 키 분배를 통해 이전의 키 정보를 재사용한다. 또한 MAC 프레임에 추후 적용 가능할 서비스들을 위해 차등적 보안 레벨을 적용하여 에너지 효율성을 높이고, 통신 지연시간을 줄였다.

1. 서 론

센서 네트워크는 유비쿼터스 환경 구현을 위한 기반 분야로서 국내외 다양한 표준기구 및 연구단체의 주도로 많은 연구개발이 진행 중이다. 그 결과 물류, 환경제어, 홈 네트워크, 교통 등 다양한 분야에서 센서 네트워크가 적용되고 있으며, 이러한 환경에서 센서를 통해 수집된 데이터들은 체계적인 분석과 서비스 간의 상호 연계를 통해 다양한 서비스 분야에 활용되고 있다[1].

지그비는 이러한 WPAN의 국제 표준인 IEEE 802.15.4를 기반으로 하는 저속 근거리 무선통신의 국제표준 스팩이다[2]. 그러나 지그비 네트워크는 멀티 홉 기반의 무선 Ad-Hoc 특성 상 보안에 취약하고 메모리나 베터리 용량 등의 제약으로 인해 일반적인 보안 기술 적용에 어려움이 따른다.

따라서 본 논문에서는 지그비 네트워크에서 효율적인 TCA 및 MAC 프레임 구조 설계를 설계하였다. 제안하는 TCA는 Trust Center 간의 키 분배를 통해 이전의 키 정보를 재사용한다. 또한 MAC 프레임에 추후 적용 가능할 서비스들을 위해 차등적 보안 레벨을 적용하여 에너지 효율성을 높이고, 통신 지연시간을 줄였다.

본 논문의 구성은 다음과 같다. 2장에서는 현재 표준에서 사용하는 TCA와 SKKE 프로토콜을 살펴본다. 3장에서는 제안하는 TCA에서 사용하는 명령·응답 메시지와 TCA 및 MAC 프레임 구조를 제시한다. 4장에서는 제안한 기법의 성능을 분석하고, 마지막 5장에서는 결론을 맺는다.

2. 관련연구

2.1 TCA(Trust Center based Authentication)

이 절에서, 우리는 현재 표준에서 사용하는 TCA 를 설명한다. Trust Center(TC)는 장치의 목록, 마스터 키, 링크키들, 네트워크 키들을 관리한다. Trust Center 는 노드 제어, 네트워크 키 갱신의 정책과 네트워크 허가를 수행한다. 또한 기존의 TCA 는 지그비의 Trust Center 의 기능을 이용한다. 초기 네트워크가 구성된 후, Joiner 인증은 같은 네트워크 안의 Trust Center 를 통하여 이루어진다. 그림 1 은 인증 기술을 보여준다.

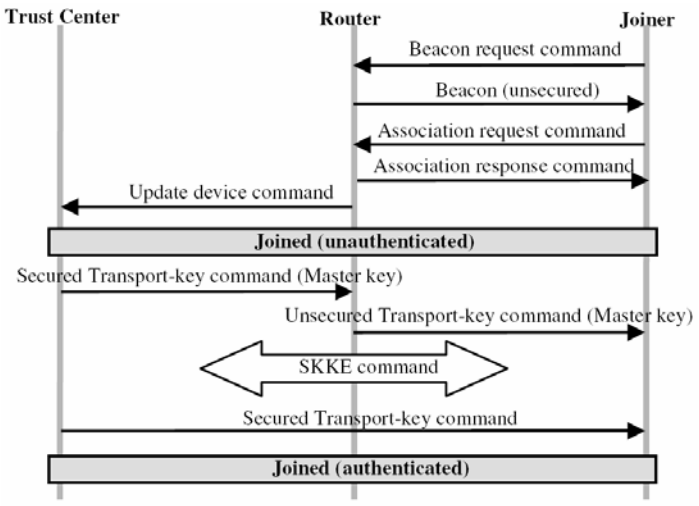

그림 1. 기본 TCA

[1] 본 연구는 지식경제부 및 정보통신연구진흥원의 IT 성장동력기술개발사업의 일환으로 수행되었습니다 [2008-S-041-01, u-City 용 센서네트워크 PHY/MAC 개발]

2.1.1 SKKE(Symmetric Key Key Establish) 프로토콜

지그비는 네트워크 키(Network Key)와 링크 키(Link Key), 그리고 마스터 키(Master Key)를 이용하여 인증 및 암호화를 수행한다. 네트워크 키는 네트워크 레벨에서의 인증 및 암호화에 사용되며, 링크 키는 장치 레벨에서의 인증 및 암호화에 사용된다. 그리고 마스터 키는 장치 간에 링크 키를 유도하기 위한 신뢰성 있는 정보로 사용된다.

생성된 키는 Trust Center 와 신규 노드간 SKKE 프로토콜을 사용해 전달된다. SKKE 는 Trust Center 와 노드가 마스터 키를 사용하여 상호 신뢰할 수 있는 비밀키(링크 키)를 유도하는 과정을 의미한다[1].

그림 2 는 신규 노드가 Trust Center 를 통해 네트워크에 조인 할 경우, 신규 노드간 인증을 위한 키 전달 과정을 나타낸다.

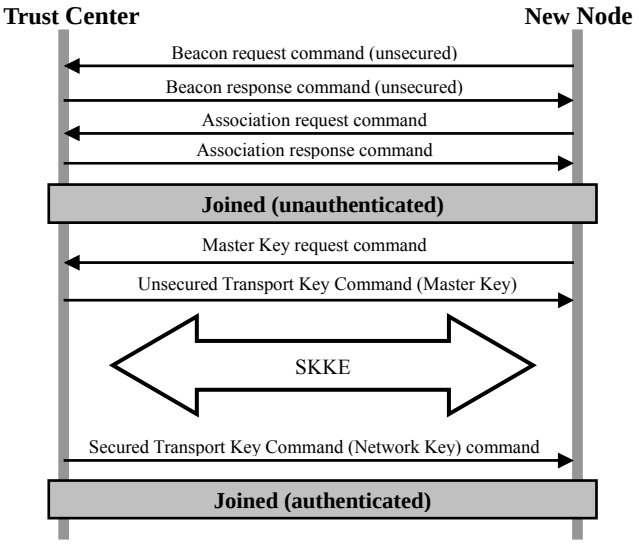

그림 2. Trust Center 와 신규 노드간 인증을 위한 키 전달 과정

신규 노드가 Trust Center 와 비컨 및 결합 명령을 주고받으며 인증 과정이 시작된다. 우선 Trust Center 는 신규 노드에게 마스터 키를 전송하고 SKKE 프로토콜 과정을 거쳐 링크 키를 생성한다.

SKKE 프로토콜 과정이 성공적으로 끝나면 Trust Center 는 신규 노드에게 네트워크 키를 전송하며 인증을 완료한다.

2.2 제어 프레임

제어 프레임[2]은 각 프레임의 맨 처음 시작 부분에 있는 2 바이트 필드로서, 무선 노드와 노드 간에 전송되는 제어 정보를 가지고 있다. 센서 노드가 네트워크로의 결합 및 인증을 끝내고, 실제 데이터 프레임의 전달을 돕는데 사용된다.

통신에 사용하는 프레임은 일반적으로 비컨(Beacon) 프레임, 데이터(Data) 프레임, 응답(Ack) 프레임, 명령(Command) 프레임으로 구분된다.

2.2.1 비컨(Beacon) 프레임

비컨 프레임은 비컨 신호의 주기적 전송을 통해 각 노드에게 무선 네트워크의 존재를 알리고, 상호 교신에 참여할 수 있게 하는 역할을 한다[2]. 그림 3 은 일반적인 비컨 프레임 구조를 나타낸다.

MHR					MSDU	MFR
Octets : 2	1	Variable			Variable	2
Frame control	Sequence number	Address info.	...	Address info.	Data payload	FCS

그림 3. 일반적인 비컨 프레임 구조

2.2.2 데이터(Data) 프레임

데이터 프레임은 망의 데이터 링크층 프로토콜에 의하여 정의되며 망 노드 간의 세션 키 상에서만 존재한다[2]. 그림 4 는 일반적인 데이터 프레임 구조를 나타낸다.

MHR					MSDU	MFR
Octets : 2	1	Variable			Variable	2
Frame control	Sequence number	Address info.	...	Address info.	Data payload	FCS

그림 4. 일반적인 데이터 프레임 구조

2.2.3 응답(Ack) 프레임

응답 프레임은 패킷이 에러 없이 수신되었다는 것을 송신자에게 확인시켜 주기 위해 제공되는 프레임이다[2]. 그림 5 는 일반적인 응답 프레임 구조를 나타낸다.

MHR		MFR
Octets : 2	1	2
Frame control	Sequence number	FCS

그림 5. 일반적인 응답 프레임 구조

2.2.4 명령(Command) 프레임

명령 프레임은 상대방 노드의 원격제어에 사용된다[2]. 그림 6 은 일반적인 명령 프레임 구조를 나타낸다.

MHR					MSDU		MFR
Octets : 2	1	Variable			1	Variable	2
Frame control	Sequence number	Address info.	...	Address info.	Command type	Command	FCS

그림 6. 일반적인 명령 프레임 구조

3. 제안하는 TCA 및 MAC 프레임

3.1 제안하는 TCA 에서 사용하는 명령 · 응답 메시지

본 논문에서 센서 노드의 키 관리 및 인증을 위해 표 1 과 같은 명령 타입(Command type)을 정의해 사용한다. 표 1 은 키 관리 및 인증을 위한 명령 타입을 나타낸다.

표 1. 키 관리 및 인증을 위한 명령 타입

CMD_SKKE_1	0x01
CMD_SKKE_2	0x02
CMD_SKKE_3	0x03
CMD_SKKE_4	0x04
CMD_REQUEST_KEY	0x05
CMD_TRANSPORT_KEY	0x06
CMD_UPDATE_DEVICE	0x07
CMD_REMOVE_DEVICE	0x08
Reserved	0x09~0xFF

명령 SKKE 프로토콜 과정에서 명령 타입 필드는 SKKE-1, SKKE-2, SKKE-3, SKKE-4 프레임 중 하나의 값을 나타내고, 그 외는 본 논문에서 사용되는 키에 대한 요청, 전송, 갱신 및 폐기를 나타낸다.

3.1.1 CMD_SKKE_#seq

모든 Key Establishment 명령 프레임은 불안전하게 보내진다. 앞으로 일반적인 APS 프레임 구조의 APS Header 부분의 임의의 필드는 설명하지 않는다. 그림 7 은 일반적인 SKKE 명령 프레임 구조를 나타낸다.

MHR		MSDU				MFR
Octets : 1	1	1	8	8	16	2
Frame control	Counter	Command identifier	Initiator Address	Responder Address	Data	MIC

그림 7. 일반적인 SKKE 명령 프레임 구조

- ***Command Identifier Field*:** APS command type (*CMD_REQUEST_KEY*, 표 1 참조)을 나타낸다.
- ***Initiator Address Field*:** 키 수립 프로토콜에 있는 Initiator로 작동하는 장치의 64비트 확장된 주소이다.
- ***Responder Address Field*:** 키 수립 프로토콜에 있는 Responder로 작동하는 장치의 64비트 확장된 주소이다.
- ***Data Field*:** Command Identifier 필드에 따라 달라진다.

3.1.2 CMD_REQUEST_KEY

키 요청을 위한 장치에 의하여 사용되는 APS 명령 프레임은 아래와 같이 정의된다. 그림 8 은 Request Key 명령 프레임 구조를 나타낸다.

MHR header		MSDU			MFR
Octets : 1	1	1	1	0/8	2
Frame control	Counter	command identifier	Key Identifier	Partner Address	MIC

그림 8. Request Key 명령 프레임 구조

- ***Command Identifier Field*:** Request Key APS command type(*CMD_REQUEST_KEY*, 표 1 참조)을 나타낸다.
- ***Key Identifier Field*:** 표 3과 같이 값이 지정된다.
- ***Partner Address Field*:** Key Type Filed의 값이 '2'(Application Key)가 되었을 때, 키를 보낸 Partner Device의 확장된 64비트 주소를 포함한다.

3.1.3 CMD_TRANSPORT_KEY

키 전송을 위한 장치에 의하여 사용되는 APS 명령 프레임은 아래와 같이 정의된다. 그림 9 는 Transport Key 명령 프레임 구조를 나타낸다.

MHR header		MFR			MFR
Octets : 1	1	1	1	Variable	2
Frame control	Counter	Command identifier	Key Identifier	Key Descriptor	MIC

그림 9. Transport Key 명령 프레임 구조

- ***Command Identifier Field*:** Transport Key APS command type(*CMD_TRANSPORT_KEY*, 표 1 참조)을 나타낸다.
- ***Key Identifier Field*:** 표 3과 같이 값이 지정된다.
- ***Key Descriptor Field*:** 적절한 인증 사용되는 인자값들과 함께 전송한 키의 실제적인 값을 갖는다.

3.1.4. CMD_ UPDATE_DEVICE

장치 갱신을 위해 사용되는 APS 명령 프레임은 아래와 같이 정의된다. 그림 10 은 Update Device 명령 프레임 구조를 나타낸다.

MHR header		MFR				MFR
Octets : 1	1	1	8	2	1	2
Frame control	Counter	command identifier	Device Address	Device Short Address	Status	MIC

그림 10. Update Device 명령 프레임 구조

- ***Command Identifier Field*:** Update-Device APS command type(*CMD_UPDATE_DEVICE*, 표 1 참조)을 나타낸다.
- ***Device Address Field*:** 상태가 갱신된 장치의 확장된 64비트 주소를 나타낸다.
- ***Device Short Address Field*:** 상태가 갱신된 장치의 16비트 주소를 나타낸다.
- ***Status Field*:** 장치의 상태 코드를 나타낸다.

3.1.5 CMD_REMOVE_DEVICE

장치의 제거를 위해 사용되는 APS 명령 프레임은 아래와 같이 정의된다. 그림 11 은 Remove Device 명령 프레임 구조를 나타낸다.

MHR header		MFR		MFR
Octets : 1	1	1	8	2
Frame control	Counter	command identifier	Child Address	MIC

그림 11. Remove-Device 명령 프레임 구조

- ***Command Identifier Field*:** Remove Key APS command type(*CMD_REMOVE_KEY*, 표 1 참조)을 나타낸다.
- ***Child Address Field*:** 네트워크로부터 제거하는 것을 요청받은 장치의 확장된 64비트 주소를 포함한다

3.2 제안하는 TCA

3.2.1 동일한 서브넷 상에서의 인증

동일한 서브넷 상에서의 인증은 신규 노드가 동일 한 서브넷에 위치하는 Trust Center 를 통해 인증을 받는 경우이다.

센서 네트워크내의 모든 센서 노드는 자신이 속한 서브넷에 존재하는 Trust Center 를 통해 자신의 정보를 등록 요청한다. 이 단계에서 사용자 정보와 장치 정보를 함께 등록한다.

그림 12 는 Trust Center 에서 이 정보를 이용하여 등록 요청한 센서 노드의 개인키를 생성하여 발급하는 세부 과정을 나타낸다.

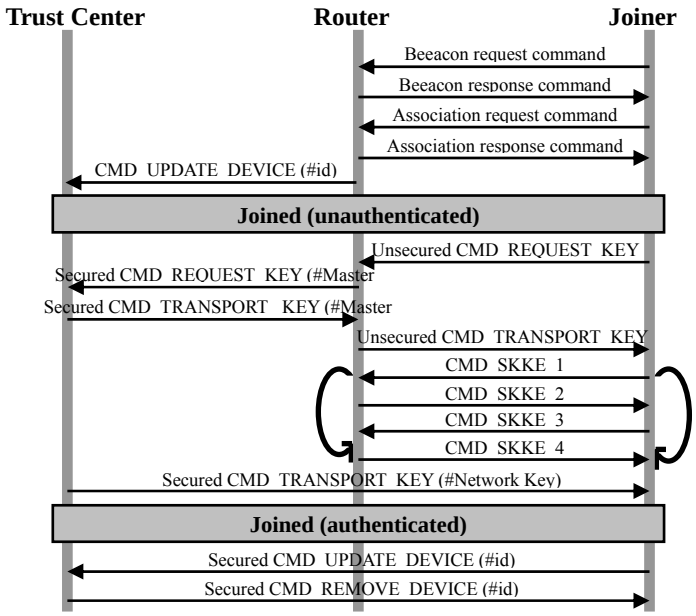

그림 12. 동일한 서브넷 상에서의 인증

· **단계 1:** Joiner가 네트워크에 조인 시 비컨 및 결합을 위한 프레임을 전송한다.

$$J \rightarrow \forall v \in MA$$

· **단계 2:** Router가 Trust Center에 Joiner 등록을 요청한다.

$$\forall v \in MA \rightarrow TC \in MA: CMD\_UPDATE\_DEVICE(J_{ID})$$

· **단계 3:** Trust Center가 Joiner에게 링크 키 생성을 위한 마스터 키를 전송한다.

$$TC \in MA \rightarrow J: CMD\_TRANSPORT\_KEY(M_{KEY})$$

· **단계 4:** Trust Center와 Joiner 간 SKKE 프로토콜을 통해 링크 키를 생성한다.

$$TC \in MA \rightarrow J: CMD\_SKKE\_\#seq$$

· **단계 5:** Trust Center가 Joiner에게 네트워크 키를 전송하고 인증을 완료한다.

$$TC \in MA \rightarrow J \in MA: CMD\_TRANSPORT\_KEY(N_{KEY})$$

3.2.2 서로 다른 서브넷 상에서의 인증

서로 다른 서브넷 상에서의 인증은 초기 인증 과정을 거친 노드(이하 이동 노드)가 다른 서브넷으로 이동하여 인증을 받는 경우이다. 서로 다른 서브넷 상에서의 인증은 서로 다른 서브넷 상으로 노드가 이동할 경우 기존의 복잡한 인증 절차 없이 Trust Center 간에 노드의 인증 정보를 주고 받음으로서 인증 절차를 간소화 시켰다. 그림 13 은 서로 다른 서브넷 상에서의 인증 과정을 나타낸다.

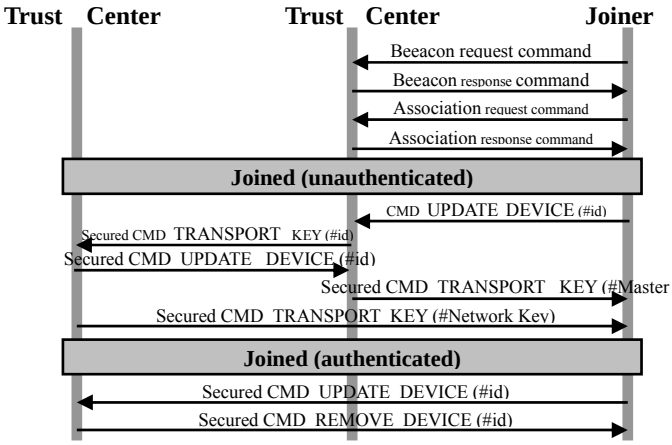

그림 13. 서로 다른 서브넷 상에서의 인증

· **단계 1:** Joiner가 다른 서브넷으로 조인 시, 비컨 및 결합을 위한 프레임을 전송한다. 그 뒤 등록을 요청한다.

$$J \rightarrow TC_B \in MA: CMD\_UPDATE\_DEVICE(J_{ID})$$

· **단계 2:** Trust Center B는 노드 인증을 위해 이전 Trust Center A로부터 노드의 초기 인증 정보를 전달받는다. 이 때 인증에 필요한 중요한 정보를 획득하게 된다.

$$TC_A \in MA \rightarrow TC_B \in MA: CMD\_UPDATE\_DEVICE(J_{ID})$$

· **단계 3:** Trust Center와 Joiner 간 SKKE 프로토콜을 통해 링크 키를 생성한다.

$$TC_B \in MA \rightarrow J: CMD\_SKKE\_\#seq$$

· **단계 4:** Trust Center가 Joiner에게 네트워크 키를 전송하고 인증을 완료한다.

$$TC_B \in MA \rightarrow J \in MA: CMD\_TRANSPORT\_KEY(N_{KEYv})$$

3.3 제안하는 TCA 를 위한 MAC 프레임 구조

그림 14 는 본 본문에서 제안하는 키 관리 및 인증을 위한 프레임 구조를 나타낸다.

제안하는 MAC 프레임은 프레임 헤더(MAC Header: MHR), 페이로드(MAC Service Data Unit: MSDU), 푯터(MAC Footer: MFR)로 구성된다.

센서 네트워크에서의 각 노드의 통신을 위한 필드는 일반적인 프레임 구조를 따르기 때문에 키 관리 및 인증을 위한 프레임 구조에 초점을 맞추어 설명한다.

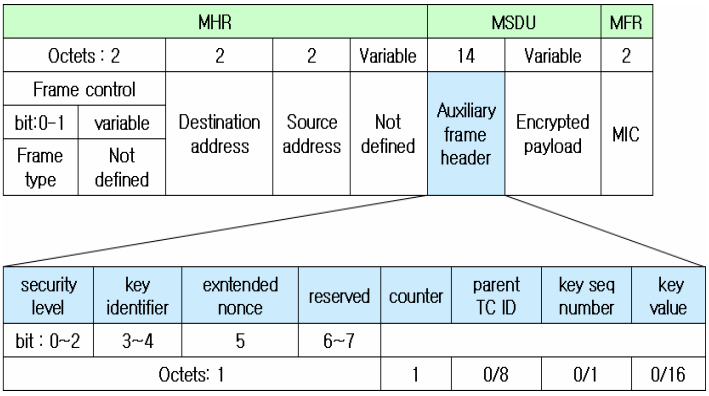

그림 14. 제안하는 MAC 프레임 구조

3.2.1 Security level

보안 레벨(Security level) 필드는 센서 노드 간의 통신에 사용되는 데이터의 보안 기능의 지원여부를 나타낸다.

표 2 는 본 논문에서 사용되는 데이터의 보안 레벨을 나타낸다.

표 2. 키 관리 및 인증을 위한 보안 레벨

None	0x00
Low	0x01
High	0x02
Reserved	0x03~0xFF

3.2.2 Key identifier

키 식별(Key identifier) 필드는 센서 노드 간의 통신에 사용되는 데이터의 암・복호화에 사용되는 키의 식별을 위해 사용된다.

표 3 은 본 논문에서 사용되는 키 구분 값을 나타낸다.

표 3. 키 관리 및 인증을 위한 Key identifier 필드 값

세션 키	0x00
마스터 키	0x01
링크 키	0x02
네트워크 키	0x03
Reserved	0x04~0xFF

3.2.3 Counter

카운터(Counter) 필드는 중복된 프레임 처리의 방지를 위해 사용되는 필드이다.

3.2.4 Parent TC ID

Parent TC ID 필드는 센서 노드 자신이 속한 서브 네트워크 영역의 Trust Center 의 고유한 식별 ID 값을 나타낸다.

3.2.5 Key seq number

Key seq number 필드는 Trust Center 에 의한 주기적인 네트워크 키 갱신에 의해 악의적인 노드로부터 전방향 보안성을 보장하기 위해 사용된다.

3.2.6 Key value

Key value 필드는 센서 노드 간의 통신에 사용되는 데이터의 암・복호화에 사용되는 128 비트 키 값을 나타낸다.

4. 성능평가

이 장에서는 제안하는 TCA 의 에너지 효율성 및 지연 시간에 대한 성능을 분석한다.

4.1 TCA 에 따른 에너지 효율성

이 절에서, 제안한 기법의 TCA에 따른 에너지 효율성을 분석한다.

표4는 TCA에 따른 에너지 효율성 분석을 위한 시스템 파라미터를 나타낸다.

표 4. 성능 분석을 위한 시스템 파라미터

통신반경, R	*10m*
Trust Center 와의 거리, d	*10m~300m*
통신 cycles 수, T	*1*
Propagation 지연 손실, k	*2*
총 패킷 길이, l	*1000 bits*
transmitter 에서의 총 에너지 소모량, δ	*30J*
전파상수(Propagation constant), μ	*2*

현재 표준의 TCA 는 키 분배를 위하여 멀티 홉(multi-hop) 통신을 한다.

통신 주기 T 동안의 멀티 홉 통신에 필요한 에너지량은 식 1 과 같다.

$$E_m = T\left((2\delta + \mu R^k)(\frac{d^2}{R^2} - 1) + (1 + \mu R^k)\right) \quad \text{식(1)}$$

제안하는 TCA 는 키 분배를 위하여 싱글 홉(single-hop) 통신을 한다. 주기 T 동안의 멀티 홉 통신에 필요한 에너지량은 식 2 와 같다.

$$E_s = T(\delta + \mu d^k) \quad \text{식(2)}$$

키 전송에 필요한 총 에너지량 δ 을 각각 20J 로 했을 경우, 기존 TCA 기법과 제안하는 TCA 기법의 총 에너지 소모량은 그림 15 와 같다.

실험 결과, 신규 노드가 Trust Center 를 통해 키를 전달받을 경우, 제안하는 방식이 기존 방식보다 키 분배를 위한 에너지 소모가 적음을 알 수 있다.

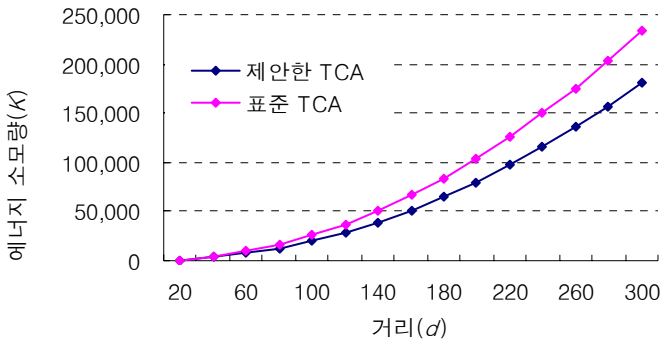

그림 15. 키 분배에 필요한 총 에너지 소모량

4.2 보안 레벨에 따른 지연 시간

이 절에서, 제안한 기법의 보안 레벨에 따른 지연시간을 분석한다.

표 5 는 보안 레벨에 따른 지연 시간 분석을 위한 시스템 파라미터를 나타낸다.

표 5. 성능 분석을 위한 시스템 파라미터

홉당 암・복호화, t_{Enc}, t_{Dec}	*449ms,456ms*
노드 수, n	*1<n*
통신 시간, t_{Trans}	*10ms*
할당 및 채널 제어 시간, Δt	*10ms*

제안한 기법의 보안 레벨에 따른 통신 지연시간은 식 3 와 같다.

$$T_{NONE} = \sum_{i=1}^{n} i \times (t_{Trans} + \Delta t) \quad (1 < n)$$

$$T_{LOW} = \sum_{i=1}^{n} i \times (t_{Transm} + \Delta t) + t_{Enc} + t_{Dec} \quad (1 < n) \qquad \text{식(3)}$$

$$T_{HIGH} = \sum_{i=1}^{n} i \times (t_{Enc} + t_{Trans} + t_{Dec} + \Delta t) \quad (1 < n)$$

제안한 보안레벨에 따른 통신 지연시간은 그림 16 과 같다.

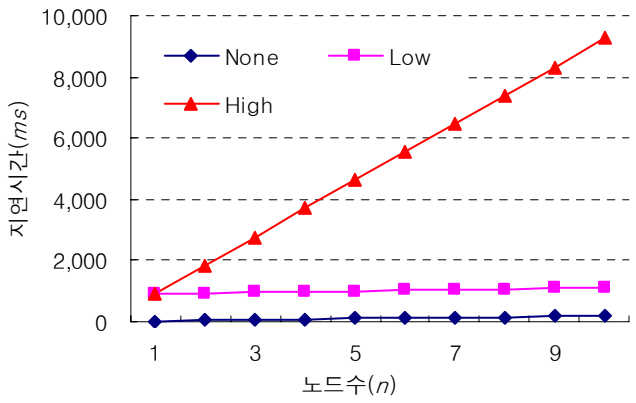

그림 16. 제안한 보안레벨에 따른 통신 지연시간

실험 결과, 통신 지연시간은 보안레벨을 낮게 설정한 경우 에는 통신 지연시간이 줄어드는 것을 알 수 있다. 추후 적용 가능할 서비스들을 위해 차등적 보안 레벨을 적용한다면 에너지 효율성 및 통신 지연을 줄일 수 있다.

5. 결론

센서 네트워크의 대표적 기술인 지그비에서는 Trust Center 역할을 정의하고 이를 통한 키 분배를 통해 안전한 통신을 한다. 그러나 현재 표준에서 사용하는 TCA 는 모든 트래픽이 Trust Center 로 집중됨으로써 부하 및 지연이 발생된다. 또한 표준에서 사용하는 보안 프로토콜은 서비스의 중요도와 상관없이 수행한다.

본 논문에서는 지그비 네트워크에서 효율적인 TCA 및 MAC 프레임 구조 설계를 설계하였다. 제안하는 TCA 는 Trust Center 간의 키 분배를 통해 이전의 키 정보를 재사용한다. 또한 MAC 프레임에 추후 적용 가능할 서비스들을 위해 차등적 보안 레벨을 적용하여 에너지 효율성을 높이고, 통신 지연시간을 줄였다.

성능 분석을 통해 제안하는 기법이 기존의 기법보다 에너지 소모 및 통신 지연시간 측면에서 효율적임을 입증하였다.

참고문헌

[1]ZigBee Alliance Document, “ZigBee Specification Pro/2007”, 2007

[2]IEEE Std 802.15.4: “Wireless Medium Access Control(MAC) and Physical Layer(PHY) Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs),” 2003

[3]S. A. Camtepe and B. Yener, “ Key Distribution Mechanisms for Wireless Sensor Networks: A Survey,” Technical Report TR-05-07 Rensselaer Polytechnic Institute, Mar. 2005.

[4]A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," ACM Wireless Networks, vol. 8, no. 5, Sept. 2002

[5] Q. Gu, and J. Drissi, Localized Broadcast Authentication in Large Sensor Networks, Int. J. of Intelligent Control and Systems, 12(4): 341- 350, 2007.