Journal of KIIT. Vol. 20, No. 1, pp. 103-111, Jan. 31, 2022. pISSN 1598-8619, eISSN 2093-7571 103
http://dx.doi.org/10.14801/jkiit.2022.20.1.103

사물인터넷을 위한 경량화된 센서 네트워크 인증 프로토콜

신 광 철*

Lightweight Sensor Network Authentication Protocol for the Internet of Things

Kwang-Cheul Shin*

요 약

사물 인터넷(IoT)에서 센싱정보는 안전하게 공유해야 하므로 물리적, 환경적인 보안측면에서 매우 중요하다. 그러나 IoT 자원은 계산능력, 전력, 메모리 등 에너지 제한으로 안전한 통신과 인증이 어렵다. 서로 다른 상호 연결된 엔티티 간의 인증 및 데이터 기밀성을 해결해야 하는 것이 사용자의 주요 관심사이다. 특히 센서 네트워크는 무선채널의 취약성과 하드웨어적 제약을 가지므로 기존의 무선통신 네트워크방식과는 다른 인증방식이 필요하다. 센서 네트워크에서 보안성이 유지되고 네트워크 성능을 갖는 저비용의 경량화 인증스킴이 요구된다. 본 논문은 스타형태의 센서 토포러지와 기지국(BS, Base Station) 간 전송데이터에 해시값 인증코드를 첨부하여 시도/응답방식으로 설계하였다. 제안은 다양한 애플리케이션에 적용 가능한 새로운 경량 인증 프로토콜로 질의코드와 응답코드의 순서쌍이 오로지 하나만 존재하는 특징을 가진 유일랜덤순차코드(URSC, :Unique Random Sequence Code)를 사용한다. 또한 엔티티의 시간(타임스탬프)을 사용하여 상호인증과 기밀성 및 무결성을 확인할 수 있는 경량화된 인증프로토콜을 제안한다.

Abstract

In the Internet of Things (IoT), sensing information must be shared secretly, so it is very important in terms of physical and environmental security. However, since IoT resources have energy limitations such as computational power, power, and memory, secure communication and authentication are difficult. Resolving authentication and data confidentiality between different connected entities is the primary focus of users. In particular, the sensor network has the weakness of the wireless channel and hardware limitations. Therefore, an authentication method different from the existing wireless communication network method is required. In a sensor network, a low-cost, lightweight authentication scheme that maintains security and has network performance is required. This paper is designed as a challenge/response method by attaching a hash value authentication code to transmission data between a star-type sensor topology and a base station (BS). The proposal of this paper is a new lightweight authentication protocol applicable to various applications, and uses the Unique Random Sequence Code (URSC), which has only one ordered pair of query code and response code. In addition, we propose a lightweight authentication protocol that can verify mutual authentication and confidentiality and integrity using the entity's time (time stamp).

Keywords
IoT, sensor node, base station, mutual authentication, session key

* 성결대학교 산업경영공학과
- ORCID: https://orcid.org/0000-0003-2375-0640

· Received: Dec. 15, 2021, Revised: Jan. 07, 2022, Accepted: Jan. 10, 2022
· Corresponding Author: Kwang-Cheul Shin
Dept. of Industrial Management Engineering, Sungkyul University, Anyang, Korea,
Tel.: +82-31-467-8916, Email: skcskc12@hanmail.net

Ⅰ. 서 론

지난 몇 년 동안 사물 인터넷(IoT)이라는 패러다임이 무선 통신 및 네트워킹 분야에서 빠르게 발전하고 있다. RFID(Radio-Frequency IDentification) 태그, 센서, 휴대폰, 웨어러블 등과 같이 이기종 개체를 상호 연결하여 공통의 목표를 달성하기 위해 상호 작용하는 개체로 에너지 및 컴퓨팅 리소스 측면에서 모두 낮은 기능을 가지므로 복잡한 보안 시스템의 구현을 지원할 수 없다[1][2]. IoT는 다양한 공격, 특히 도청의 위험이 있는 무선통신으로 주요 보안 문제는 인증 및 데이터 무결성으로 IoT 컨텍스트에서 인증은 각 개체의 진위여부를 확인할 수 있는 중요한 개념이다. 사물인터넷(IoT)은 일상생활을 크게 개선할 수많은 응용 프로그램들로 개인의료 응용 프로그램은 실제적이고 가장 효과적인 사물인터넷 중 하나로 간주된다.

개인의료 시스템은 기지국과 연결된 상황별 센서로 구성된 무선 주파수 기반 무선 네트워킹 기술이다. 일반적으로 개인 건강관리를 달성하기 위해 건강 관련 데이터의 수집은 의료시스템을 통해 환자를 지속적으로 모니터링 할 수 있으므로 응급 상황 발생 시 신속하고 효과적인 의료 개입이 가능하여 응급 상황을 예측할 수 있다[3]. 악성 노드에 의한 전송으로 건강 관련 데이터를 수정하면 잘못된 의료 처방이 발생하거나 긴급 개입이 지연될 수 있어 재앙적인 결과를 초래할 수 있다. 이러한 중요 오류나 부정한 건강관련 데이터를 방지하기 위해 다양한 애플리케이션에 맞는 경량화된 인증 프로토콜이 필요하다.

네트워크의 성능과 보안 기능을 유지하기 위해 본 논문에서는 다양한 IoT 애플리케이션 중 개인의료 지원을 위한 경량 인증 프로토콜을 제안한다. 제안 프로토콜은 유일랜덤순차코드인 URSC코드와 타임스탬프를 사용하여 암호연산이 아닌 해시연산만으로 최소의 계산량과 에너지 소비로 시도/응답 방식의 질의와 응답의 매칭을 통해서 개체간의 인증, 전송데이터의 무결성, 신선성 동시에 실현한다.

본 논문의 구성은 2장에서 IoT관련 보안의 문제와 관련 인증방법에 대해 살펴보고 3장에서 URSC 코드와 타임스탬프를 이용한 경량의 인증 프로토콜을 제안하였고 4장에서 제안 프로토콜의 안전성을 분석하며 5장에서 논문의 결론과 향후 방향을 제시한다.

Ⅱ. 관련연구

IoT는 사물(개체)과 사물간 무선 네트워크를 통하여 데이터를 수집하고 전달하며 디바이스들을 통해 네트워크로 연결하여 전송하는 기술이다. IoT는 일반적으로 지능형 의사결정에 사용되는 방대한량의 데이터를 전송하는 글로벌 네트워크이다.

그림 1과 같이 IoT 시스템구조는 여러 개의 도메인과 도메인 내에 하나의 베이스스테이션(게이트웨이)이 존재하며 인터넷을 통해 여러 개의 서버 또는 디바이스들과 연결되어 있는 형태이다[4]. IoT 인증스킴의 분류 그림 2는 IoT 구조의 계층 각각에 적용할 다양한 인증기술을 제시했다[5][6]. 해시, 대칭 또는 비대칭 암호화 알고리즘을 사용하는 인증스킴으로 지문, 망막과 같은 신체적 특성을 기반으로 하는 인증요소(Authentication factor)로 피지컬과 보행분석이나 음성인식, 개인의 행동특성을 기반으로 하는 행동으로 구분한다.

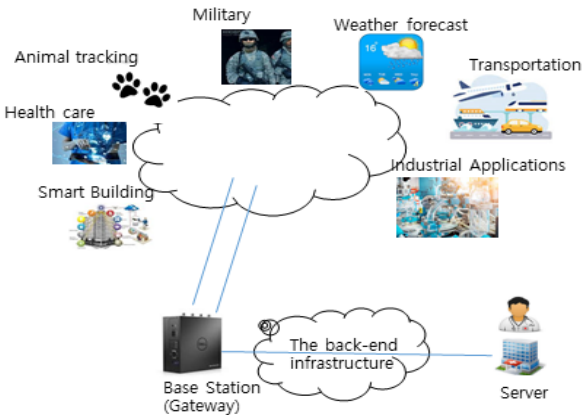

그림 1. IoT 분야
Fig. 1. IoT in various domains

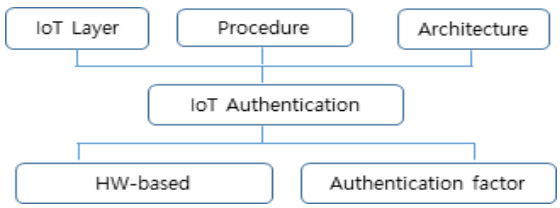

그림 2. IoT 인증 체계의 분류
Fig. 2. Taxonomy of IoT authentication schemes

절차(Procedure)는 단방향인증, 양방향인증, 중앙기관이 당사자를 두고 상호인증을 수행하며 인증구조(Architecture)는 통신 당사자 간에 직접 인증방식인 분산형과 신뢰서버를 두고 인증에 사용하는 중앙집중식이 있다. 사물인터넷 계층(IoT Layer)은 종단노드가 인지한 정보를 수집, 처리, 디지털화하는 지각계층과 인식된 데이터를 수신하고 처리하는 네트워크계층, 데이터를 수신한 후 사용자가 요청한 서비스를 제공하는 애플리케이션계층으로 구분한다.

이처럼 IoT 인증체계는 접근권한이 없는 공격자가 프로토콜의 취약점을 악용할 여러 가지 방법(스푸핑, 스니핑 등)을 찾아내지 못하도록 하는 최소한의 정의이다. IoT장치는 에너지와 처리능력, 메모리가 제한되어 몇 Kb의 RAM과 수십 Kb의 비휘발성 메모리(EEPROM)에 불과하다. 또한 IoT장치들은 관리하기 위한 일들이 많고 센서노드를 추가해야 하는 확장가능성도 고려해야하기 때문에 가볍고 정교한 인증 프로토콜을 필요로 한다.

환자의 건강상태나 환경의 모니터링과 같은 중요한 기능은 IoT 장치에서 수집된 데이터에 의존하는 영역이 많다. 이러한 데이터는 안전하고 상호인증된 방식으로 공유되어야 한다. IoT 장치는 배터리로 구동되기 때문에 처리, 메모리, 전원 가용성에 리소스가 제한되므로 센서노드와 베이스스테이션을 기본 엔티티로 하는 경량인증프로토콜이 제안되었다.

H.khemissa et al'.s 등은 건강관련 데이터수집을 보호하기 위해 센서와 기지국(BS)간의 상호인증 스킴을 제안하였다[7]. 이들은 초경량으로 Nonce와 HMAC(Keyed-Hash 메시지인증코드)을 사용하여 상호전송 메시지에 대한 무결성을 강조하였다. 임의의 난수를 사용함으로써 재생공격에 강하다고 주장하고 있으나 이전에 사용한 난수를 증명할 수 없어서 취약하다. B. R. Abdulrahman et al'.s 등은 IoT 환경에서 경량인증 및 키교환 프로토콜을 제안하였다[8]. 이들은 IoT 디바이스와 게이트웨이(베이스스테이션)가 무선채널을 통해 통신하는 IoT 환경을 위한 프로토콜로 초기에 두 개의 마스터키와 지속적으로 변경되는 세션키를 갖는 특징이 있다. 대칭키 암호화와 HMAC 기반의 키 파생기능만을 사용하여 인증과 키교환을 함으로써 기밀성 및 무결성을 강조하였으나 제한된 자원에 비해 많은 연산비용을 요구한다. 본 논문에서는 특수한 성질을 가진 유일 랜덤순차와 타임스탬프를 사용하여 그림 1의 네트워크 모델을 가정하여 설계한다.

III. 경량의 센서 네트워크 인증 프로토콜 제안

3.1 제안개요

네트워크 구조는 그림 3과 같이 상황별 센서, 베이스스테이션(기지국), 백엔드 인프라, 의료서버(또는 기관)로 구성된다. 제안된 프로토콜은 상황센서 노드에서 엔티티의 데이터를 수집하고 IoT와 서버 사이의 인터페이스기능, 착발신 신호 송출, 통화 채널 지정, 통화 채널 감시, 자기 진단기능 등을 수행하는 기지국으로 전송하는 구조이다. 센서와 기지국은 무선인터페이스를 사용하며 의료서버로 전송되는 데이터는 와이파이나 5G등의 백엔드인프라 인인터넷을 통해 전송된다.

센서노드는 에너지 자원 및 계산 등 제약을 받으나 기지국은 더 많은 기능을 갖는다. 각 센서노드는 식별자를 가지며 간단한 대칭키 암호화를 수행할 수 있는 능력이 있다. 본 논문의 제안 프로토콜은 IoT의 센서와 기지국 양 엔티티 간의 기밀성과 무결성, 신선성을 유지하면서 경량화 상호인증에 중점을 둔 프로토콜로 등록단계와 인증 및 세션키 교환단계로 구분한다.

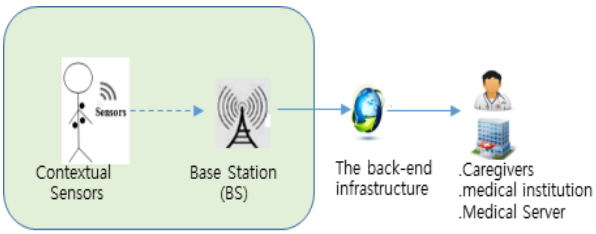

그림 3. 센서 네트워크 모델
Fig. 3. Sensor network model

3.2 등록단계

3.2.1 기지국의 URSC 코드생성과 분배

랜덤한 유일순차코드인 URSC는 순차코드의 증가패턴이 무작위로 정해지는 불규칙 특성으로 길이

가 L(본 논문에서는 센서노드 수)인 순차코드에 대해서 호핑(Hopping) 패턴을 찾는 것이다[9]. URSC의 생성알고리즘[10]을 요약하면 다음과 같다.

1단계 : 소수 p와 코드길이 L(<p)을 선택
2단계 : 거리 호핑패턴 D를 선택
$D=[d_1, d_2, d_3, ..., d_L]$
$\forall$(임의, 모든) $1 \le d_i \le q-1$ and $\sum d_i \equiv 0 (\mathrm{mod}\ q)$
3단계 : D의 모든 순열에 대해서 행렬을 만든다.
4단계 : 행렬의 모든 열과 행에서 같은 수가 반복되지 않는 코드를 순차코드 행렬로 사용한다.

표 1과 같은 URSC코드를 생성하기 위한 절차는 다음과 같다. 한 영역의 BS에 할당된 센서노드가 4라면 임의의 소수 p=7, L=4인 경우 거리호핑 패턴을 임의로 D=[4, 5, 8, 9]를 선택했을 때 위 생성 알고리즘에 적용하면 다음과 같이 되어 시퀀스오더 4개 생성된다. 알고리즘에서 반복되는 코드라는 것은 행렬 M 중에서 하나의 행이 [0 1 4 1]이라면 1이 2회 반복되므로 폐기하고 다시 생성한다.

표 1. 할당된 URSC 코드
Table 1. Distributed URSC code

Sensor node	Sequence order	Sequence code			
SN_1^0	A	0	4	2	1
SN_1^1	B	1	5	3	4
SN_1^2	C	2	6	4	5
SN_1^3	D	3	0	5	6

모든 행과 열에 같은 수가 없다면 M을 순차코드 행렬로 사용하며 기지국은 자신이 관리하는 영역의 센서노드들에게 비밀리에 순차코드생성자(시퀀스코드)와 시퀀스오더를 분배한다. 각각의 센서노드들은 순차코드 생성자를 이용하여 순차코드를 생성하고 자신의 시퀀스오더에 해당하는 순차코드(URSC)를 보관한다. 센서노드는 이웃하는 센서노드들이 어떤 시퀀스오더를 보유하고 있는지 모른다.

3.2.2 초기등록

그림 4에서 센서노드 SN_1^0는 자신의 ID(SN_1^0는)을 안전한 채널로 베이스스테이션에 전송한다. 베이스스테이션은 비밀난수 x가 포함된 마스킹(해시값)된 $MSID_1^0=h(SN_1^0 \oplus x)$을 계산하고 센서노드에 전송한다.

베이스스테이션은 바인딩 테이블에 각 센서의 식별자(ID)를 포함하여 해당 매개변수(센서ID, 해시값, 순차오더, 순차코드)들을 삽입(그림 5)한다. 베이스스테이션에 모든 센서가 등록하면 초기 등록은 종료된다. 모든 센서들은 순차코드와 마스킹된 해시값을 보유한다.

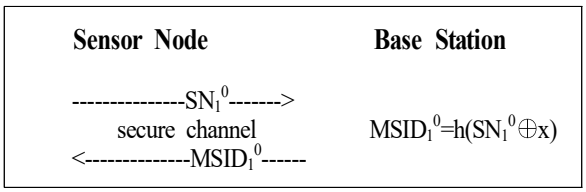

그림 4. 등록 프로세스
Fig. 4. Registration process

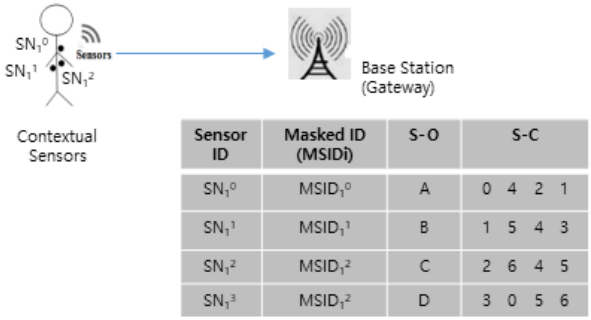

그림 5. 초기등록
Fig. 5. Initial registration

3.3 인증단계

인증단계는 센서노드와 베이스스테이션 간 상호인증을 목표로 다음과 같은 인증절차를 수행한다.

1) 베이스스테이션은 센서노드 SN_1^0에 대해 테이블에서 임의의 URSC #을 선택하여 센서노드의 식별자와 연산하여 해시값 A를 전송(Request)한다.

$$\cdot A=h(URSC\# \oplus SN_1^0) \quad (1)$$

2) 센서노드는 시퀀스오더의 시퀀스코드를 알 수 없으므로 해시값 A에 해당하는 시퀀스코드를 찾을 때까지 반복 검색한다.

$$\cdot A_{URSC\#}=\{h(URSC\# \oplus SN_1^0)\}_1^n \quad (2)$$

3) 일치하는 시퀀스코드를 찾으면 시퀀스코드와 마스킹된 ID를 사용하여 전송정보(Response) B를 계산한다.

・$B=h(URSC\#(s\text{-}c)\oplus SN_1^0)\oplus MSID_1^0$ (3)

4) 중간자공격, 재생공격에 대항하기 위해 센서노드의 시간(타임스탬프)인 Ta을 얻고 베이스스테이션에서 메시지 신선성을 확인하기 위해 C를 계산한다.

・$C=MSID_1^0\oplus Ta\oplus URSC\#(s\text{-}c)$ (4)

5) 센서노드는 B, C를 베이스스테이션으로 전송한다.

6) 센서노드의 시간 Ta를 얻기 위해 아래의 식 (5)를 계산하고 메시지가 허용한 시간(△T)에 도착(식 (6))했다면 정당한 센서노드를 인증하기 위해 식 (7)을 계산하여 B와 비교한다.

・$Ta=C\oplus h(SN_1^0\oplus x)\oplus URSC\#(s\text{-}c)$ (5)

・$T\text{-}Ta\leq\triangle T$ (6)

・$B=?h(URSC\#(s\text{-}c)\oplus SN_1^0)\oplus MSID_1^0$ (7)

7) 센서노드가 정당하면 센서노드에게 베이스스테이션에 대한 인증을 위해 이전의 시퀀스코드 다음 두 번째의 시퀀스코드(URSC#(s-c)')와 베이스스테이션의 시간(Tb)을 선택하고 D와 E를 계산하여 센서노드에게 전송한다.

・$D=h(BS_ID\oplus SN_1^0)\oplus MSID_1^0\oplus URSC\#(s\text{-}c)'$ (8)

・Time stamp Tb select (9)

・$E=h(D\parallel Ts)\oplus Tb$ (10)

8) 베이스스테이션은 식 $B=?h(URSC\#(s\text{-}c)\oplus SN_1^0)\oplus MSID_1^0$에서 센서노드를 인증하였으므로 다음과 같이 공유키인 세션키를 생성한다.

・$SK_{BS\text{-}SN}=h(D\oplus Ta\oplus Tb)$ (11)

9) 센서노드는 D와 E를 사용하여 베이스스테이션의 시간인 식 (12)를 구하고 허용된 시간에 도착(식 (13))하였다면 이전에 반복검색하여 선택한 다음의 시퀀스코드를 선택하여 베이스스테이션의 식별자 해시값 식 (14)를 구하고 아래와 같이 식 (15)를 계산하여 D와 비교한다.

・$Tb=E\oplus h(D\parallel Ts)$ (12)

・$T\text{-}Tb\leq\triangle T$ (13)

・Next URSC#(s-c)' 선택

・$h(BS_ID\oplus SN_1^0))=D\oplus MSID_1^0\oplus URSC\#(s\text{-}c)'$ (14)

・$D=?h(BS_ID\oplus SN_1^0)\oplus MSID_1^0\oplus URSC\#(s\text{-}c)'$ (15)

10) 센서노드는 식 $D=?h(BS_ID\oplus SN_1^0))\oplus MSID_1^0\oplus URSC\#(s\text{-}c)'$에서 베이스스테이션을 인증하였으므로 다음과 같이 공유키인 세션키를 생성한다.

・$SK_{SN\text{-}BS}=h(D\oplus Ta\oplus Tb)$ (16)

Ⅳ. 제안 프로토콜 분석

그동안 IoT 환경에 적용하기 위한 인증 및 키 설정 프로토콜들이 많이 제안되었다. 대부분 프로토콜들은 인증기관(CA)[11]과 같은 신뢰할 수 있는 제 3자를 두거나 공개키 암호화[12]를 많이 사용하여 IoT 장치의 리소스 제약을 고려할 때 비용이 많이 든다. MAC(Message Authentication Code)은 디지털 서명을 위한 축약메시지로 해시함수(MD5, SHA_1)를 사용하여 나온 결과 값이고 HMAC은 MAC에 암호/복호키를 사용한 값이다. 본 논문에서는 표 2와 같이 랜덤한 유일순차코드와 타임스탬프를 사용하여 암호화와 해시키를 사용하지 않는 해시기반으로 제안하여 기밀성과 무결성, 신선성을 보장하는 프로토콜이다.

표 3의 수행에서 H.khemissa et al'.s 스킴은 Nonce 값을 기반으로 MD5 또는 SHA-1과 같은 Keyed-hash 메시지 인증코드인 HMAC을 사용하였다.

표 2. 보안성비교(o: 보호, x: 비보호, △: 가능)
Table 2. Security comparison(o: protected, x: non-protected, △: available)

Attack	[7]	[8]	Proposed scheme
Mutual authentication	△	0	0
Eavesdropping attack	X	0	0
Location tracking attack	△	△	0
Reply attack	X	X	0
MITM attack	0	0	0
Data integrity	0	0	△
Scalability	0	X	0

표 3. 수행능력비교
Table 3. Performance analysis

		[7]	[8]	Proposed scheme
Sensor node	Random number generation	1	1	
	Hash	1		3
	MAC/HMAC	1	2	
	Encryption / decryption	1	4	
	F(N)	1		
Base tation / Gateway	Random number deneration	1	1	1
	Hash	1		6
	MAC/HMAC	1	2	
	Encryption / decryption	1	4	
	F(N)	1		

센서노드에 대한 위장공격과 식별자보호를 위해 ID를 마스킹하였고 데이터 무결성은 HMAC를 사용하였다. 반면 A. B. Rabiah et al'.s 등은 대칭키(AES) 암호와 HMAC 기반의 인증 및 키교환 프로토콜로 많은 연산비용을 요구한다.

4.1 안전성분석

4.1.1 상호인증

각 센서노드는 베이스스테이션의 비밀난수 x와 센서노드의 식별자가 마스킹된 값($MSID_1^0$)과 순차코드(URSC)를 보유하고 있다. 합법적인 센서노드와 베이스스테이션 만이 순차코드를 계산하여 검색할 수 있고 그 다음의 순차코드를 선택할 수 있다. 베이스스테이션은 순차코드를 확인할 수 있는 B를 수신하여 센서노드가 정확한 URSC코드를 검색하였는지를 $h(URSC\#(s\text{-}c)\oplus SN_1^0)\oplus MSID_1^0$와 비교함으로써 알 수 있고 센서노드는 다음 순차코드를 선택한 D를 수신하여 베이스스테이션이 보유한 다음번의 순차코드를 정확하게 인식하는지의 여부를 $h(BS_ID\oplus SN_1^0)\oplus MSID_1^0\oplus URSC\#(s\text{-}c)'$를 판단함으로써 베이스스테이션을 인증한다.

4.1.2 위치추적공격

센서노드와 베이스스테이션 간에 전송되는 데이터는 $B=h(URSC\#(s\text{-}c)\oplus SN_1^0)\oplus MSID_1^0$, $C=MSID_1^0\oplus Ts\oplus URSC\#(s\text{-}c)$, $D=h(BS_ID\oplus SN_1^0)\oplus MSID_1^0\oplus URSC\#(s\text{-}c)'$, $E=h(D \| Ts)\oplus Tb'$에서 보듯이 시도/응답 전송정보가 URSC코드와 타임스탬프가 각각의 세션마다 서로 다른 출력 값을 가지므로 위치추적에 안전하다.

4.1.3 도청공격

센서노드와 베이스스테이션 간에 전송데이터를 캡처(엿듣고)하여 어떤 데이터인지 알아낼 수 있느냐의 문제로 시도/응답 데이터인 B는 센서노드의 ID와 센서노드가 선택한 유일순차코드를 알아낼 수 있어야 하고 기지국의 마스킹 값인 비밀난수 x를 알아야 도청에 성공할 수 있다. 또한 C에는 센서노드의 시간인 타임스탬프가 해시되어 알아낼 방법이 없다. 응답 데이터인 D와 E도 그 다음번의 순차코드와 기지국의 타임스탬프를 알 수 없으므로 도청공격에 성공할 수 없다.

4.1.4 중간자(변조)공격

공격자는 센서노드와 베이스스테이션간의 비밀정보를 수집한 다음 합법적 센서노드로 위장하여 통신에 참여, 베이스스테이션의 인증절차를 통과하여야 하는데 4.1.3의 도청공격에서 보듯이 B, C, D, E의 기밀성으로 도청 자체가 불가하다. 양단간 기밀성이 유지되므로 중간에 메시지의 위조나 변조가 불가하며 이것은 센서노드와 기지국에서 볼 때 철저한 데이터의 무결성과 기밀성으로 확인시켜주고 있다.

4.1.5 재전송공격

재전송공격은 도청하여 수집한 전송정보를 동일하게 전송하여 제 3의 사이트로 유도하거나 취약한 비밀키 등의 정보를 알아냈을 때 정당한 사용자로 위장하거나 또는 자원을 고갈시킬 목적으로 서비스 거부공격(DoS : Denial of Service) 등을 위해 행해지는 공격이다. 일반적으로 재전송공격을 방지하기 위해 임의의 난수, 타임스탬프를 사용하며 본 논문에서는 임의 난수 대신에 URSC 순차코드와 타임스탬프(메시지의 계산가능한 유효시간부여)를 사용하여 방지하고 있다.

4.1.6 데이터 무결성

데이터의 원 정보를 유지하기 위한 무결성을 검사하는 일반적인 방법은 메시지를 요약(해시값 또는 메시지인증코드)한 축약메시지에 송신자의 개인키로 암호화(디지털 서명)하여 전송하는 방식이나 IoT의 자원제약으로 본 논문에서와 같이 해시함수만 사용하여 베이스스테인션에서는 $B=?h(URSC\#(s\text{-}c)\oplus SN_1^0)\oplus MSID_1^0$을 비교하고 센서노드에서 $D=?h(BS_ID\oplus SN_1^0)\oplus MSID_1^0\oplus URSC\#(s\text{-}c)$'를 비교하여 일치하는 값이라면 중간에 메시지가 변조되었다고 볼 수 없음을 증명한다.

4.1.7 확장성

기지국 범위에 센서노드가 추가될 경우를 고려하여 순차코드행렬 생성시 센서노드의 수를 예측하여 길이 L을 여분을 두어 생성하게 되면 새로운 센서노드가 추가될 때마다 마스킹된 값과 순차코드를 분배하면 된다.

4.1.8 신선성

신선성(Freshness)은 매 세션마다 새로운 데이터의 전송으로 중간자공격과 재생공격을 차단하는데 효과적이다. 각 시도응답에서 무작위로 선택하고 그 다음의 URSC코드를 선택함으로 동일한 URSC코드와 동일한 타임스탬프를 사용하지 않으므로 순방향 기밀성도 유지된다.

4.2 성능평가

표 4에서와 같이 제안된 인증프로토콜의 평가는 센서노드의 데이터송수신과 암호화 프리미티브 실행에 필요한 에너지를 계산 비교한다. 센서노드에는 CC2420 radio가 장착된 TelosB 센서노드 사용을 가정하여 인증에 필요한 에너지비용을 추정한다. [13]에 의하면 TelosB 센서에 대해 1바이트 데이터교환에 필요한 에너지는 송신에 5.76μJ(J:joule에너지단위), 수신에 6.48μJ, AES암호화에 42.88μJ, HMAC코드 계산에 62.15μJ가 필요하다.

표 4. 에너지비용분석
Table 4. Energy-cost analysis (pro : proposed)

	Transmission data	Received data	HMAC	AES	Total
[7]	253.44μJ	207.36μJ	124.3μJ	42.88μJ	627.98μJ
[8]	253.44μJ	285.12μJ	248.6μJ	343.04μJ	1130.2μJ
pro	230.4μJ	259.2μJ	–	–	489.6μJ

[7]의 송신메시지 크기는 마스킹된 ID 20바이트, 임의난수 8바이트, HMAC 4바이트, 프로토콜해더 12바이트로 44바이트, 수신메시지 크기는 2개의 임의난수, HMAC 4바이트, 프로토콜해더 12바이트로 32바이트이다. [8]은 송수신 메시지크기가 44바이트로 538.56μJ, HMAC 4회로 248.6μJ, AES 암호화 8회로 343.04μJ로 총비용은 1130.2μJ이다. 제안논문에서는 송수신메시지(B, C, D, E) 모두 베이스스테이션의 비밀난수 8바이트를 기준으로 Xor 연산되므로 8바이트이며 프로토콜해더 12바이트, 각각 크기는 20바이트로 송신데이터 230.4μJ, 수신데이터 259.2μJ이며 총 489.6μJ로 초 경량화된 센서 네트워크이다.

V. 결 론

무선채널을 통해 IoT 네트워크는 여러 장치들이 연결되기 때문에 엔티티 간 인증과 데이터의 기밀성, 무결성이 필수적이다. 특히 자원제약을 받는

IoT 네트워크상의 센서노드는 경량화된 상호인증이 중요하다. 본 논문은 IoT 환경에서 보안통신을 지원하는 경량인증 프로토콜을 제안하였다. 센서 네트워크의 경량화를 위해 최소한의 데이터인증에 중점을 두고 HMAC 또는 대칭키 암호화를 대신하여 URSC 코드와 타임스탬프를 사용하고 센서노드의 식별자를 마스킹하여 설계함으로써 안전성[표 2]과 최소의 메커니즘[표 2], 에너지 효율성[표 3]을 높였다. 제안된 프로토콜은 신뢰기관에 의존하지 않고 리소스가 제한된 장치들에 대해 가볍고 안전한 효율적인 상호인증을 제공한다. 이 프로토콜은 자원이 제한된 환경의 다양한 IoT 애플리케이션들이 적용하기에 적합하다. 향후 메모리 소비 및 실행 시간에 대한 보다 정확한 분석 연구를 위해 다양한 파라미터를 가지고 구현하는 것을 목표로 한다.

References

[1] S. Sicari, A. Rizzardi, L. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead", Computer Networks, Vol. 76, pp. 146-164, Jan. 2015. https://doi.org/10.1016/j.comnet.2014.11.008.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things:A survey", Computer networks, Vol. 54, No. 15, pp. 2787-2805, Oct. 2010. https://doi.org/10.1016/j.comnet.2010.05.010.

[3] M. Patel and J. Wang, "Applications, challenges, and prospective in emerging body area networking technologies", Wireless Communications, IEEE, Vol. 17, No. 1, pp. 80-88, Feb. 2010. https://doi.org/10.1109/MWC.2010.5416354.

[4] K. Priya and M. Nagendra, "A survey on secured authentication schemes over IoT devices", International Journal of Future generation Communication and Networking, Vol. 13, No. 3, pp. 3854-3862, Aug. 2020.

[5] M. El-hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Analysis of authentication techniques in Internet of Things (IoT)", In Proceedings of the 2017 1st Cyber Security in Networking Conference (CSNet), Rio de Janeiro, Brazil, pp. 18-20, Oct. 2017. https://doi.org/10.1109/CSNET.2017.8242006.

[6] M. El-hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, "Taxonomy of authentication techniques in Internet of Things (IoT)", In Proceedings of the 2017 IEEE 15th Student Conference on Research and Development (SCOReD), Putrajaya, Malaysia, pp. 67-71, Dec. 2017. https://doi.org/10.1109/SCORED.2017.8305419.

[7] H. Khemissa and D. Tandjaoui, "A Lightweight Authentication Scheme for E-Health Applications in the Context of Internet of Things", International Conference on Next Generation Mobile Applications, Services and Technologies, Cambridge, UK, pp. 90-95, Sep. 2015. https://doi.org/10.1109/NGMAST.2015.31.

[8] B. R. Abdulrahman, K. Ramakrishnan, L. Elizabeth, and K. Koushik, "A Lightweight Authentication and Key Exchange Protocol for IoT", Workshop on Decentrialized IoT Security and Standards, Catamaran Resort Hotel and Spa in San Diego, California, pp. 1-6, Feb. 2018. https://dx.doi.org/10.14722/diss.2018.23004.

[9] Kwang-cheul Shin, "A Study on the Light and Efficient Key Agreement Mutual Authentication Protocol in Wireless Sensor Environments", Journal of Korean Institute of Information Technology, Vol. 10, No. 11, pp. 49-62, 2012. https://doi.org/10.1109/ACCESS.2020.2987764.

[10] Min-Ho, Cheug-Keun Lee, Ju-Hyung Son, and Seung-Woo Seo, "Efficient security Mechanism Using lighy-weight Data origin Authentication in Sensor Networks", The Journal of Korean Institute of Communications and Information Sciences, Vol. 32, No. 7, pp. 717-723, Jul. 2007.

[11] 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. 10, No. 7, pp. 1-14, Jul. 2014. https://doi.org/10.1155/2014/357430.

[12] Y. Qiu and M. Ma, "A Mutual Authentication and Key Establishment Scheme for M2M Communication in 6LoWPAN Networks", IEEE Transactions on Industrial Informatics, Vol. 12, No. 6, pp. 2074–2085, Dec. 2016. https://doi.org/10.1109/TII.2016.2604681.

[13] G. De Meulenaer, F. Gosset, O.-X. Standaert, and O. Pereira, "On the energy cost of communication and cryptography in wireless sensor networks", in Networking and Communications, WIMOB'08. IEEE International Conference on Wireless and Mobile Computing. IEEE, Avignon, France, pp. 580–585, Oct. 2008. https://doi.org/10.1109/WiMob.2008.16.

저자소개

신 광 철 (Kwang-Cheul Shin)

1985년 2월 : 서울과학기술대학교 전자계산학과(공학사)
1990년 12월 : 국방대학원 전자계산학과(공학석사)
2003년 8월 : 성균관대학교 대학원 정보공학과(공학박사)
2004년 3월 ~ 현재 : 성결대학교 산업경영공학과 부교수
관심분야 : 정보보호, 프로젝트관리, 소프트웨어 표준화