Journal of Knowledge Information Technology and Systems

ISSN 1975-7700

http://www.kkits.or.kr

Node Mutual Authentication Based on Trust-Assessment Model in the IoT-Sensor Networks

Hong-Seop Kim*

Department of Bio-medical Information, Chungbuk Health & Science University

ABSTRACT

Interest in IoT technology is increasing these days, and core of IoT technology is sensor network technology. Although ZigBee network is widely used in IoT-sensor network, it is vulnerable to various security threats such as wiretapping of sensor information, abnormal packet flow, data forgery and denial of service attack. However, ZigBee IoT-sensor networks should operate in resource environments with limited computing capabilities. Therefore, it is imperative that IoT-sensor network security technologies be researched for lightweight design. In this paper proposed an algorithm for mutual authentication of IoT-sensor networks based on a trust assessment model that enables safe IoT-sensor network construction even with small security operations. The proposed trust-based authentication algorithm is designed with direct trust relationships between ZC-Sensor nodes belonging to the ZigBee Pico-Net and performs a trust assessment between nodes based on probability calculation and logic calculation. In addition, the proposed mutual authentication algorithm can support confidentiality, anonymity, mutual authentication and freshness in terms of security safety of the IoT-sensor network and increase the lightweight-ness of the existing authentication methods. And it will be possible to extend safety and survival period of IoT-sensor network by reducing the use of limited batteries in sensor nodes.

KEYWORDS: Internet of thing(IoT), IoT authentication, Mutual authentication, IoT sensor, ZigBee network, Sensor network, Trust model, Trust assesment, Piconet, Lightweight-ness

ARTICLE INFO: Received 22 October 2018, Revised 16 November 2018, Accepted 7 December 2018.

*Corresponding author is with the Department of Bio-Medical Information, Chungbuk Health and Science University, 10 Deokam-gil Naesu-eup, Cheongwon-ku, Cheongju, Chungbuk 28150, KOREA.

E-mail address: hskim@chsu.ac.kr

1. 서 론

사물인터넷(Internet of Things:IoT)은 유비쿼터스 센서망(Ubiquitous Sensor Network:USN)에 기반하여 RFID(Radio Frequency Identification) 등과 같은 전자태그, 스마트폰 등과 같은 스마트기기(smart device) 및 다양한 센서(sensor) 종류를 다양한 사물(things) 등에 부착하여 얻은 사물의 인식 정보를 기초로 하여 실세계 주변의 각종 환경 및 상황 정보를 인지하여 관리하기 위한 센서망(sensor network)의 응용기술이다[1]. IoT-센서망(IoT-sensor network) 기술은 비상대응체계관리, 에너지관리분야, 의료모니터링, 물류, 재고관리, 교통체계 관리, 생활환경 상태 인식 및 통제관리 등과 같은 민.관.군 다양한 분야에 응용할 수 있다[1].

IoT-센서망을 구축하기 위한 네트워크 구조로 지그비(ZigBee)가 많이 적용된다[2][3]. 지그비 IoT-센서망은 망의 구성에 있어서 자기조직적(self-organization)인 특성이 존재한다. 이 과정에서 악성 센서 노드의 접속이 가능하며 이로 인한 센서 정보의 도청, 비정상적 패킷 흐름, 데이터 위.변조 및 서비스 거부 공격 등과 같은 보안 위협에 대한 취약성이 존재한다[3][4]. 그리고 이러한 보안 취약점을 극복하기 위한 보안 대책이 많이 요구되고 있으며 관련 기술에 대한 연구 및 개발이 국내외의 관련 연구기관, 기업 및 학계를 중심으로 활발히 진행되고 있다.

지그비 IoT-센서망은 적은 배터리 용량 및 기타 정보처리 자원이 제한된 환경에서 운용되어야 하는 제약조건이 존재한다. 따라서 생존성이 높고, 안전한 지그비 IoT-센서망을 지원하기 위한 보안 기술은 적은 자원 소모 구조를 지닌 보안 구조 및 기능의 경량화 설계와 개발은 반드시 필요한 연구 방향이 된다[3][4]. 하지만 현재 지그비 IoT-센서망의 연구 개발 동향에서는 이러한 특성을 고려한 보안체계에 대한 연구 및 개발은 미흡한 실정이다.

본 논문에서는 지그비 IoT-센서망에서 자원소모가 적은 경량 보안구조를 지닌 신뢰평가를 기반으로 하는 센서 노드 상호간의 인증 기법을 제안하다. 이를 위하여, 본 논문의 제2장에서는 IoT-센서망 보안연구와 신뢰모델 연구와 관계된 기존 연구 동향 및 기존에 제안된 기법들의 평가, 제3장에서는 지그비 IoT-센서망 구성 노드 상호간의 신뢰평가를 위한 신뢰모델의 정의, 제4장에서는 제안된 신뢰평가 모델에 기반한 IoT-센서망의 피코넷(piconet) 단위의 인증기법을 기술한다. 그리고 제5장에는 제안된 신뢰평가 모델에 기반한 상호인증 알고리즘의 프로토타입 기능 구현 결과와 제안된 인증기법의 보안 안전성 등과 관련된 평가분석 결과를 기술한다.

2. 관련 기술 연구동향

2.1 IoT-센서망 보안 평가항목

IoT-센서망을 구성하는 센서 노드들의 보안 안전성을 유지하기 위해 <표 1>과 같이 비밀성(confidentiality), 상호인증(mutual authentication), 무결성(integrity), 신선성(freshness), 익명성(anonymity) 및 경량성(lightweight)이 보장되어야 한다[4-7].

표 1. IoT-센서망 보안 평가항목
Table 1. IoT-sensor Network Security Assessment Item

평가항목	평가내용
비밀성	전송 정보는 불법 도청으로 부터 안전하다.
상호인증	통신에 참여하는 개체들은 서로 상대방이 믿음의 관계임을 보장한다.
무결성	전송되는 정보는 불법적 위•변조로부터 안전함을 보장한다.
익명성	통신에 참여하는 개체 외에는 상대방의 정보를 알 수 없음을 보장한다.
신선성	한번 사용된 보안정보는 재사용되지 않고 위장공격으로 부터 안전하다.
경량성	최소 연산량 지원 등 같은 자원소비를 최소로 함을 보장한다.

2.2 IoT-센서망 보안기술 연구동향

IoT-센서망은 서론에서 기술한 바와 같은 컴퓨팅 자원이 부족한 제약 사항으로 인하여 경량화된 보안구조가 필수적이다.

대부분의 IoT-센서망 키 관리 및 보안 프로토콜 연구에는 대칭키 기반의 암호 방식을 이용하는 방법이 제안되고 있다. 그리고 IoT-센서망의 센서 인증기법에 대한 관련 주요 연구로는 SPINS(Security Protocols for Sensor Networks)[7], LEAP(Localized Encryption and Authentication Protocol)[8] 등이 존재한다.

SPINS 프로토콜은 SNEP(Secure Network Encryption Protocol)과 μTESLA(Timed Efficient Stream Loss-tolerant Authentication)로 구성된다. SNEP은 데이터의 기밀성과 노드 상호간의 데이터 인증과정 및 과거에 사용된 데이터의 재사용 공격이 불가능하게 하기 위한 키 재설정에 대한 보안 기능을 제공한다. μTESLA 프로토콜은 기존 유선망에서 사용되었던 μTESLA 프로토콜을 변형하여 센서망에 적합하게 설계된 인증 프로토콜이며 키를 알고있는 노드에 의해 해석이 가능한 대칭키 기반의 인증방식을 제공한다. μTESLA는 노드 상호간에 공유하는 비밀키의 노출을 최대한 늦추어 주는 기능을 제공하여 비 대칭키 방식을 사용하는 효과를 나타낼 수 있다. 하지만 인증 대상이 되는 노드의 수가 증가할 경우 지연시간이 길어져서 활용이 어렵고, 노드 상호간 시간 동기화가 필요한 단점을 지닌다.

LEAP는 단일 키를 사용하는 구조로는 대량 노드들로 구성된 대규모 센서망의 안전한 키 관리 구조 설계가 불가능한 문제를 해결하기 위해 제안되었다. LEAP는 4개의 암호 키와 키 설정 프로토콜로 구성되는데 암호키는 베이스스테이션(base station)과 공유하는 개인키, 망에 존재하는 모든 노드와 공유하는 방송키, 센서노드 상호간의 공유하는 Pairwise 키 및 클러스터를 구성하는 이웃 노드 상호간에 공유하는 클러스터 키로 구성된다. 이 방법은 4개의 암호키를 사용하여 개인키 유출 방지, 이웃한 센서노드의 인증 및 방송과정 중에 송수신되는 메시지의 유출 방지가 가능하며 이에 따른 IoT-센서망의 생존성을 극대화 할 수 있는 장점이 존재하지만 경량성이 떨어진다.

2.3 신뢰평가 기반 보안연구동향

신뢰평가 기반 보안 기술은 신뢰 모델에 기초하여 개체 상호간의 믿음의 관계를 설정하고 믿음의 정도에 따라 불법적 의도를 지닌 개체 및 행위를 구분하고 이를 통제하기 위해 적용이 시도되고 있는 보안 기법이다. 이러한 신뢰평가 기반 보안 기술은 주로 확률 및 논리 해석을 기반으로 하는 신뢰모델을 사용한다. 그러므로 기존 보안 기술에 비해 높은 경량성을 유지할 수 있는 장점이 존재한다.

신뢰평가 기반 보안은 전자상거래(electronic commerce), P2P(Peer to Peer) 네트워크 등의 보안 문제 해결을 위한 적용 가능성이 연구되어 왔다[9-3]. 그리고 최근에는 MANET(Mobile Ad-Hoc Network), WSN(Wireless Sensor Network) 및 IoT-센서망 분야의 안전한 통신 환경을 지원하기 위한 보안 라우팅, 인증, 역할 기반 접근통제(Role Based Access Control:RBAC) 등과 같은 보안 분야에의 적용이 시도되고 있다[9][14][15].

신뢰평가 기반 보안 연구의 핵심은 신뢰모델에 존재한다. 신뢰모델은 개체 상호간의 신뢰 관계를 설정하고 개체 사이의 신뢰의 정도를 평가할 수 있는 신뢰정보를 정의한다.

이러한 신뢰 정보를 표현하기 위해 기존 연구 결과로 제안한 신뢰모델은 뎀스터-쉐퍼

(Dempster-Shafer)의 확률 모델에 기반한 Teng의 신뢰모델[16], 퍼지논리(fuzzy logic)에 기반한 기반 Machala의 신뢰모델[17] 및 주관 논리(subject logic)를 기반으로 하는 Jøsang의 신뢰계산 모델[18]이 존재한다.

Teng의 연구에서는 현실세계의 신뢰성 평가를 위한 뎀스터-쉐퍼 이론에 기반한 신뢰값을 갖는 신뢰 행렬(trust matrix)을 사용하는 확률기반의 신뢰모델을 제안하였다[16]. 하지만 Teng의 연구는 전자상거래 환경에서 사업자, 구매자 상호간의 신뢰평가를 위해 신뢰 행렬을 구성하고 이들 신뢰 행렬의 각 요소는 뎀스터-쉐퍼 이론에 기반한 확률 계산에 의해 결정된 믿음과 불신의 값을 관리하는 측면에서 계산의 복잡성 및 기억장소 소요에 대한 문제점이 존재한다.

Manchala의 연구에서는 퍼지 논리 모델에 기반한 WTS(Weighted Trust Surface)와 FTS(Fuzzy Trust Surface)를 적용하는 신뢰 행렬을 정의하였다. 그리고 Teng의 연구에서와 같이 개체 상호간의 신뢰 거래 과정에서 신뢰도를 검증하기 위해 신뢰 행렬을 적용하는 방법을 제안하였다[17].

Jøsang의 연구에서는 현실 세계 대상들의 믿음과 불확실의 정도를 주관 논리(subject logic)로 표현하기 위해 “Opinion”을 정의하였다. 그리고 이를 기초로 확률 기반의 다양한 신뢰평가 모델을 제안하고 신뢰의 정도를 확률로 표현 가능함을 증명하였다[18][19]. Jøsang의 연구에서 제안한 신뢰 계산 모델은 Teng의 연구 및 Manchala의 연구에서 나타나는 신뢰평가를 위한 중간 노드의 도움 없이 개체 상호간의 자기 조직적 신뢰 관계 설정에 적용 가능하다. 이러한 자기 조직 특성은 지그비 IoT-센서망의 기본 동작 환경이 되며 이점은 Jøsang의 신뢰계산 모델이 지그비 IoT-센서망의 동작 특성에 잘 부합되는 신뢰모델로 평가된다.

이 같은 특성으로 Jøsang의 신뢰평가 모델은 MANET 및 USN 분야의 신뢰평가 기반 보안 기술의 신뢰모델로 주로 적용되며 주요 연구 사례로 Li의 연구, Shanker의 연구 등이 존재한다[14][20]. Li의 연구에서는 Jøsang의 연구에서 제안한 신뢰계산 모델을 MANET 라우팅에 적용하여 자기 조직적인 경량화된 안전한 경로 확보에 적용될 수 있음을 증명하였지만, 악의적 의도를 지닌 노드의 신규 참여에 대한 인증 방법이 결여되어 있다[14]. Shanker의 연구에서는 유비쿼터스 환경에서의 구성 노드 상호간 정보 관리에 Jøsang의 신뢰 계산 모델을 적용한 역할 기반 접근 제어(Role Based Access Control:RBAC) 방법을 제안하였다[20]. 그리고 앞서 살펴본 신뢰기반 보안에 적용된 신뢰모델들의 특성 비교 평가 결과는 <표 2>와 같다.

표 2. 신뢰평가 모델의 비교 (○:상,△:중,X:하)
Table 2. Comparison of trust assessment models (○:above,△:middle ,X:below)

비교모델 / 특 성		Teng 모델	Manchala 모델	Jøsang 모델
기반모델		뎀스터-쉐퍼	퍼지논리	주관논리
신뢰 관계	직접 신뢰	x	x	○
	간접 신뢰	○	○	○
자기 조직 특성		x	x	○
경량성	신뢰 정보관리	x	x	△
	계 산	x	x	x

3. 지그비 IoT-센서망을 위한 신뢰모델

본 절에서는 지그비 IoT-센서망을 위한 신뢰모델을 제안한다. 제안하는 지그비 IoT-센서망 신뢰모델은 개체 상호 간의 신뢰 관계를 표현하기 위해 동일 피코넷(pico-net)에서의 직접 신뢰모델(direct trust model)과 여러 개의 피코넷을 연동하는 간접 신뢰모델(indirect trust model)을 정의한다.

3.1 지그비 IoT-센서망의 구성모델

본 논문에서 제안하는 신뢰모델은 지그비 연합[21][22]에서 제안하는 IoT-센서망 표준 사양인 지그비 망(Zigbee Network) 모델에 적용한다. 그리고 구성형태(topology)는 <그림 1>과 같이 성형(star)구조의 피코넷 및 그물형(mesh) 구조로 구성되어 인접된 피코넷의 상호연결망인 스캐터넷(scatternet)이 혼합되어 운용되는 형태로 구성함을 가정한다.

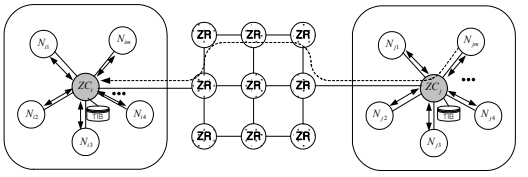


그림 1. 지그비 IoT-센서망의 구성
Figure 1. Composition of the ZigBee IoT-sensor network

<그림 1>에서 지그비 IoT-센서망은 지그비 코디네이터(ZigBee Coordinator:ZC)와 종단 센서(End Point Sensor:EPS)들로 노드들을 구성된다. 지그비 코디네이터는 단위 피코넷 구성 센서들의 관리, 주변 환경에 대한 정보, 센서들의 정보를 수집한다. 그리고 지그비 라우터(ZigBee Router:ZR)는 스캐터넷을 구성하는 노드가 되며 독립적으로 운영되는 다른 지그비 피코넷 상호간을 연동하게 된다. 종단 센서들은 자신의 감지 영역내의 환경 정보를 수집하여 코디네이터에게 전송하는 기능을 수행하며 IoT-센서(IoT sensor)의 기능을 지닌다.

지그비 IoT-센서망의 i번 지그비 피코넷은 ZC_i를 중심으로 m개의 종단 센서($\{N_{i1}, N_{i2}, N_{i3}, .., N_{im}\}$)들이 자기 조직으로 형성된 구조이며 동일 피코넷에 소속된 종단 센서들에 의해 수집된 정보는 ZC_i를 통하여 관리된다. 그리고 다른 피코넷에 소속된 종단 센서들의 수집된 정보는 지그비 라우터에 의해 중계된다. 또한 지그비 IoT-센서망은 <그림 1>과 같이 피코넷 단위내의 ZC와 EPS 사이의 점대점 통신, ZC와 같은 피코넷 상의 모든 EPS로의 방송, ZR을 경유한 피코넷 상호간 통신 방식을 지원한다.

3.2 IoT-센서망 신뢰모델

본 절에서는 <그림1>과 같이 구성된 지그비 IoT-센서망의 센서 노드 상호간의 신뢰를 표현하기 위한 신뢰모델을 제안한다. 본 논문에서 제안하는 신뢰모델은 비대칭적(asymmetric) 관계 속성을 지닌 직접 신뢰와 전이적(transitive) 관계 속성을 지닌 간접 신뢰모델로 정의한다. 직접신뢰 모델은 동일 피코넷 상의 ZC와 EPS인 센서 상호간의 신뢰를 정의한다. 그리고 간접신뢰모델은 ZR을 통한 피코넷 상호간의 연동과정을 통한 스캐터넷 구성 노드 상호간의 신뢰를 정의한다.

3.2.1 피코넷 내에서의 직접신뢰모델

직접 신뢰모델은 <그림 2>에서와 같이 1 홉(hop) 단위로 직접 인접한 노드i와 노드 j 상호간의 신뢰관계로 정의한다.

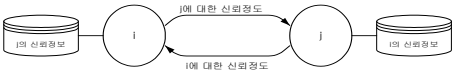


그림 2. 노드 i와 j사이의 직접신뢰
Figure 2. Direct trust relationship between node i and j

서로 인접된 노드 i와 j가 존재할 경우, 노드 i와 j의 직접 관계를 지닌 신뢰정보($\mathbb{T}_{ij}$)는 <정의 1>과 같이 정의한다.

【정의 1】 노드 i(N_i)의 노드 j(N_j)에 대한 신뢰정보($\mathbb{T}_{ij}$)는 $< E_{ij}, \xi_{E_{ij}}, I_{E_{ij}}, S_{E_{ij}|n} >$로 구성한다.
- E_{ij} : 노드 i(N_i)에서 관리하는 노드 j(N_j)이며 $E_{ij} \in \{N_1, N_2, ...N_j, ...N_m\}$이다.

- $\xi_{E_{ij}}$: 노드 i가 관리하는 노드 j의 경험정보이며 $\xi_{E_{ij}} = (f_s, f_f)$이다.
- $I_{E_{ij}}$: 노드 i에서 결정되는 노드 j에 대한 신뢰정보이다.
- $S_{E_{ij}\{c|n\}}$: 노드 i에서 관리하는 노드 j의 신뢰상태 집합이며 $S_{E_{ij}\{c|n\}} = \{Trust, Uncertainty\}$이다.

경험 정보 $\xi_{E_{ij}}$는 노드 i가 관리하는 노드 j의 경험 정보로서 노드 j의 신뢰를 결정하기 위한 기초정보로 적용하며 $\xi_{E_{ij}}$의 f_s는 개체 j가 통신 성공, 보안 인증 성공 등과 같은 신뢰성 있는 동작(event)을 수행한 빈도수이며 f_f는 개체 j가 통신 실패, 보안 인증 실패 등과 같은 불신의 동작을 수행한 빈도수로 결정한다. 그리고 경험정보 값은 식 1.과 같이 계산한다. 또한 개체 i가 갖는 경험정보의 값은 항상 양의 정수 값을 지니며 초기치는 (0,0)으로 설정한다.

$$\begin{cases} f_s = f_s + 1 \ , \text{if } event \in success \\ f_f = f_f + 1 \ , \text{if } event \in fail \end{cases} \quad (1)$$

신뢰정보 $I_{E_{ij}}$는 $\xi_{E_{ij}}$를 기초로 노드 i에서 노드 j의 믿음의 정도를 표현하기 위해 계산되는 신뢰정보이다. 이 신뢰 정보를 통하여 노드 i는 노드 j의 신뢰 상태를 결정한다. 노드들에 대한 신뢰의 정도를 표현하기 위한 $I_{E_{ij}}$는 식 2.와 같이 센서 노드 개체(E_i)에 대한 믿음(belief)의 정도를 표현하는 $Bel(E_i)$로 구성한다. 그리고 $Bel(E_i)$는 다시 식 3. 같이 개체(E_i)의 전체 경험(ξ_{E_i})중 정상적인 통신이 발생할 확률로 정의한다. $Bel(E_i)$의 계산 결과는 식 4.와 같이 0.0과 1.0 사이에 존재한다.

$$I_{E_i} = \{Bel(E_i)\} \quad (2)$$

$$P(\xi_{E_i} = f_s) = \frac{f_s}{f_s + f_f} \quad (3)$$

$$Bel(E_i) \in [0,1] \quad (4)$$

신뢰 상태($S_{E_{ij}\{c|n\}}$)는 노드 i가 관리하는 노드 j의 변화되는 신뢰상태를 정의하다. 그리고 상태 값이 "$Trust$"일 경우는 노드 j가 확실하게 믿을 수 있는 신뢰 상태임을 표현하고 "$Uncertainty$"일 경우는 노드 j의 신뢰상태가 불확실 상태에 있음을 표현한다. 여기서, $S_{E_{ij}\{c\}}$는 노드 j의 현재 신뢰상태(current)이며 $S_{E_{ij}\{n\}}$은 앞으로 새롭게 변화될 상태(new)를 나타낸다. 노드 j의 $S_{E_{ij}\{n\}}$는 $S_{E_{ij}\{c\}}$와 $I_{E_{ij}}$를 적용하여 "$\{S_{E_{ij}(c)} \times I_{E_{ij}} \rightarrow S_{E_{ij}(n)}\}$" 같이 새로운 신뢰 상태로 변화한다. 그리고 신뢰평가 대상인 센서노드의 $S_{E_i\{n\}}$의 상태는 <그림 3>과 같이 결정한다.

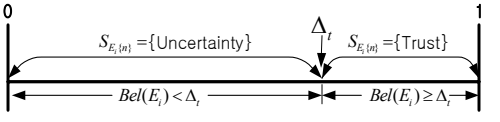


그림 3. 신뢰 상태의 결정
Figure 3. Determining the Confidence

<그림 3>에서 Δ_t는 신뢰 임계값(threshold)으로 정의한다. 그리고 신뢰 임계값은 평가 대상이 되는 임의의 개체 i의 신뢰 상태를 결정하기 위한 믿음의 정도에 대한 기준으로 활용한다. 이러한 신뢰 임계값은 신뢰 정보가 적용되는 IoT-센서망의 보안 안전도 특성에 따라 [0,1]의 범위에서 관리자(manager)의 신뢰평가 정책에 의해 결정한다.

3.2.2 캐스터넷에서의 간접신뢰모델

간접신뢰모델은 전이적 속성을 지니며 <그림 4>와 같이 2홉 이상 떨어진 특정 노드에 대한 신뢰 관계를 믿을만한 중간 노드의 신뢰 권고를 받아 설정하는 관계이다. 그리고 간접신뢰모델은 여러 인접된 노드의 다중 홉(multi-hop)의 연결을 통하여 중간 노드의 신뢰평가 대상 대상노드의 신뢰정보를 평가하기 위한 신뢰조합(trust combination) 과 특정 노드의 대상정보가 인접된 여러 노드의 신뢰 정보가 서로 상이할 경우 이를 평가하기 위한 신뢰합의(trust consensus) 모델로 정의한다.

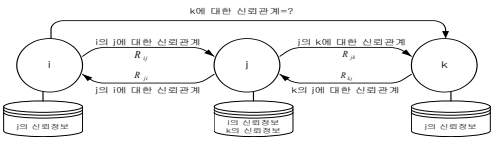


그림 4. 노드 i와 k의 간접신뢰 관계
Figure 4. Indirect trust relationship between node i and j

<그림 4>에서 노드 i와 j는 직접 신뢰 관계(R_{ij})를 유지하고 노드 j는 노드 k와 직접 신뢰 관계(R_{jk})를 유지하고 있다. 그리고 노드 i와 k는 직접 연결되는 채널이 존재하지 않을 경우 노드 i가 새로운 노드 k와의 신뢰 관계를 설정하기 위하여 노드 k와 직접 신뢰 관계를 설정하고 있는 노드 j의 신뢰 권고를 통하여 노드 i가 노드 k에 대한 신뢰를 평가한다.

신뢰조합에 의한 신뢰평가 연산은 간접 신뢰 관계를 지닌 노드 i와 k사이의 중간 노드 j의 신뢰 정보를 고려한 노드 i에서의 노드 k에 대한 신뢰는 식 5. 같이 노드 i와 j 및 노드 j와 k 상호간의 현재 신뢰 상태에 대한 논리곱(AND) 연산으로 결정한다.

$$S_{E_{ijk}\{n\}} = ((S_{E_{ij}\{c\}} \wedge S_{E_{jk}\{c\}}) \wedge (S_{E_{ji}\{c\}} \wedge S_{E_{kj}\{c\}})) \quad (5)$$

여기서, <그림 5>와 같이 다중 홉(multi-hop)상의 간접 신뢰 상태의 조합은 식 6. 같이 정의한다.

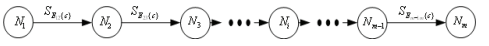


그림 5. 다중 홉 상의 간접 신뢰
Figure 5. Indirect trust for multi-hop

$$S_{E_{i..m}\{n\}} = (\bigwedge_{i=1}^{m-1}((S_{E_{i\,i+1}\{c\}}) \wedge (\bigwedge_{i=m-1}^{1} S_{E_{i+1\,i}\{c\}}))) \quad (6)$$

신뢰합의에 의한 신뢰평가 연산은 <그림 6> 같이 노드 i와 노드 k에 대한 식 5.와 식 6.을 기초로 하는 간접신뢰 상태를 인접한 여러 이웃 노드 $N = \{N_1, N_2, ..., N_m\}$들이 서로 다르게 권고하는 경우가 발생하는 경우에 인접된 여러 노드의 신뢰 정보를 종합하여 합의된 신뢰 정보를 결정한다.

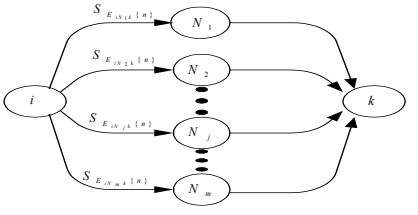


그림 6. 다수 노드들의 신뢰합의
Figure 6. trust consensus for multi-nodes

신뢰합의 연산은 확률에 기반하여 식 7., 식 8., 식 9., 식 10. 같이 정의한다.

여기서, Θ는 식 5.과 식 6.을 적용하여 2홉 또는 다중 홉 상의 간접 뢰 관계를 통하여 결정된 신뢰 상태($S_{i\,Nj\{n\}}$)에서 신뢰($Trust$)를 판정한 빈도수(f_t) 및 불확실($Uncertainty$)을 판정한 빈도수(f_u)로 식 7.과 같이 정의하며 Θ의 값은 식 8. 같이 결정한다.

$$\Theta = (f_t, f_u) \tag{7}$$

$$\begin{cases} f_t = f_t + 1, if\ S_{iNjk\{n\}} = \{Trust\} \\ f_u = f_u + 1, if\ S_{iNjk\{n\}} = \{Uncertainty\} \end{cases} \tag{8}$$

$$P(\Theta = f_t) = \frac{f_t}{f_t + f_u} \tag{9}$$

$$P(\Theta = f_t) \in [0, 1] \tag{10}$$

이때, 다수 노드에서 권고하는 신뢰 상태에 대한 합의된 신뢰 정도는 다수의 노드에서 권고한 신뢰 상태 전체수에서 신뢰($Trust$) 상태를 권고한 빈도수(f_t)에 대한 확률로 식 9. 같이 정의한다. 그리고 계산된 값의 범위는 식 10. 같이 0.0에서 1.0 사이에 존재한다.

식 8.를 적용하여 결정되는 합의된 노드 k에 대한 노드 i의 신뢰 상태는 식 11. 같이 신뢰 임계값(Δ_t)을 적용하여 다수 노드에서 권고된 신뢰 권고의 정도($P(\Theta = f_t)$)가 Δ_t보다 크거나 같으면 합의된 새로운 신뢰 상태는 $\{Trust\}$로 결정하며 기타 조건에서는 불확실 상태 $\{Uncertainty\}$로 결정한다.

$$S_{\overline{iNjk\{n\}}} = \begin{cases} Trust & , if\ P(\Theta = f_t) \geq \Delta_t \\ Uncertainty & , Otherwise \end{cases} \tag{11}$$

3.2.3 신뢰정보베이스

노드 ID (E_i)	경험 정보(ξ_{E_i})		신뢰정보 (I_{E_i})	신뢰 상태 ($S_{E_i\{c\}}$)	제한 시간
	f_s	f_f			
N_1			$\{Bel(E_1)\}$		
....	....	....	.....	....	.....
N_j			$\{Bel(E_j)\}$		
...	...	...	...	....	.....
N_m			$\{Bel(E_m)\}$		

그림 7. TIB 구조
Figure 7. TIB Structure

지그비 IoT-센서망을 구성하는 ZC 및 센서들은 인접한 이웃 노드들($\{N_1, N_2, ..., N_j, .., N_m\}$)의 신뢰평가를 위한 <정의 1>의 신뢰 정보를 관리하기 위한 신뢰정보베이스(Trust Information Base:TIB)의 구조는 <그림 7> 같다. <그림 7>의 TIB의 구성요소는 <정의 1>의 신뢰정보와 같으며 제한 시간(expire time)은 인접된 노드의 신뢰 정보가 TIB에 기록되어 일정 시간이 지난 후 인접 노드의 존재 유무를 확인하여 관련된 신뢰 정보를 재구성하기 위해 사용된다.

3.3 제안 신뢰 모델의 지그비 IoT-센서망 적용

제안한 신뢰 모델은 <그림 1> 같이 구성된 지그비 IoT-센서망 환경에서 노드들의 신뢰평가를 위해 적용한다. <그림 1>에서 직접 신뢰 관계는 $ZC_i : N_{i4}$, $ZC_j : N_{j2}$ 등과 같이 같은 피코넷에 소속된 노드 상호간의 신뢰평가를 위해 적용한다. 그리고 간접 신뢰 관계는 $ZC_i : N_{j3}$, $ZC_j : N_{i2}$ 등과 같이 ZR로 연동되어 있는 스캐터넷에서 서로 다른 피코넷의 노드 상호간의 신뢰평가를 위해 적용한다.

여기서, 적용되는 직접 신뢰 및 간접 신뢰평가 방식의 선택은 노드들의 라우팅 과정에서 전송되는 라우팅 패킷(routing packet)에 존재하는 홉(hop) 수를 활용하여 <알고리즘 1>과 같이 결정한다.

알고리즘 1. 홉 수를 사용한 신뢰평가
Algorithm 1. Trust Assessment Using Hop-Count

```
Procedure Trust_Relation(HOP_COUNT) {
    /* HOP_COUNT : 도착지에서의 홉 수*/
    Select case (HOP_COUNT)
                    case =1 : {
                            직접신뢰평가;
                        }
                    case >1 : {
                            간접신뢰평가;
                        }
    End Select
}
```

홉 수는 라우팅(routing) 과정중 경유하는 노드의

수를 알기 위해 적용된다. <그림 8> 같이 출발 노드(source node)에서 패킷에 수록되는 초기 홉 수는 0으로 결정한다. 그리고 중간 노드를 경유할 때마다 1씩 증가한다. 그러므로 목적지 노드(destination node)에 도착한 후의 패킷에 수록된 최종 홉 수를 통하여 총 경유한 노드의 수를 알 수 있다[23]. 이점을 활용하면 ZC에 수신된 홉 수가 1이면 같은 피코넷에 소속된 노드가 보낸 패킷이고 홉 수가 1보다 크면 다른 피코넷에 소속된 노드가 보낸 패킷임을 판단할 수 있다.

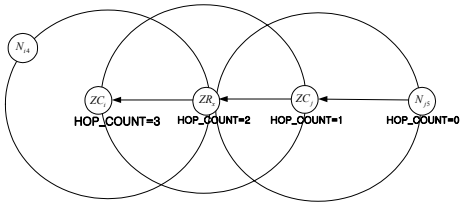


그림 8. 홉 수를 사용한 신뢰 관계 선택
Figure 8. Select a Trust Relationship Using Hop Number

이에 대하여 <알고리즘 1>에서 HOP_COUNT는 출발 노드에서 전송된 패킷이 목적지 노드(destination node)에 도착한 후의 최종 홉 수이다. 이러한 HOP_COUNT를 비교하여 HOP_COUNT가 1이면 대상 노드는 같은 전송 범위 내에 있는 노드로 판정하여 신뢰평가 방법으로 직접 신뢰평가를 선택한다. 그리고 HOP_COUNT가 1보다 크면 대상 노드가 전송 범위 밖의 노드로 판정하여 신뢰평가 방법으로 간접 신뢰평가를 선택한다.

4. 신뢰기반 상호인증

본 논문에서 제안하는 신뢰모델에 기반한 상호인증 기법은 <그림 1>과 같이 구성된 지그비 IoT-센서망의 피코넷 j에서 ZC_j-센서노드 상호간의 직접 신뢰모델을 인증 과정에 적용하며 신뢰기반 상호인증의 동작 구조는 <그림 9>와 같다. 그리고 제안하는 신뢰기반 상호인증 과정은 크게 신규 센서 노드 접속 초기화 단계와 초기화 과정이 끝난 센서 노드들의 데이터 송신 단계로 구분하여 동작 흐름을 설계하였다. 그리고 지그비 IoT-센서망을 구성하는 노드들은 불필요한 전력소모를 줄이기 위해 특별한 동작이 없을 경우 수면(Sleep) 상태를 유지함을 가정한다.

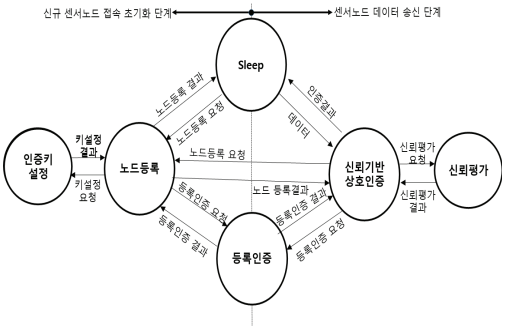


그림 9. 신뢰평가 기반 상호인증 구조
Figure 9. Trusted Mutual Authentication Architecture

4.1 접속초기화 단계의 동작

접속 초기화 단계는 신규 센서 노드가 네트워크에 접속되거나 데이터를 송신한 센서 노드가 ZC의 TIB에 존재하지 않을 경우 센서 노드의 안전한 접속을 처리하는 과정이다. 이 과정은 <그림 9> 같이 수면(Sleep)단계, 노드등록(Node registration) 단계, 인증키 설정(key setup), 등록인증(registry authentication) 과정으로 구분하여 동작한다.

4.1.1 등록인증 프로토콜

센서 노드와 ZC 상호간의 등록인증은 <그림 9>에서 ZC와 센서 상호간에 마스터키(master key)를

사용한 안전한 인증키 설정(key setup) 과정과 설정된 인증키를 기반으로 접속되는 센서 노드의 안전성을 검증하기 위한 등록인증 과정으로 구분한다. 그리고 등록인증 과정에 적용되는 기호는 <표 3>과 같다.

표 3. 인증기호
Table 3. Authentication Symbols

기호	의 미
ID_{n_i}	i번 센서 노드(N_i)의 ID
ID_z	ZC의 ID
R_{N_i}	센서 노드의 랜덤수(nonce)
R_{ZC_j}	ZC의 랜덤수(nonce)
MK_{ij}	그룹 j의 ZC-센서노드 i사이의 안전하게 설정된 대칭키 기반 마스터키
KA_{ij}	마스터 키에 의해 생성되는 ZC와 센서 노드 상호간의 인증키
$H(x)$	키 생성을 위한 단 방향 해시 함수
$\{m\}$	메세지 단위
$E_{MK_{ij}}(x)$	마스터 키를 사용하여 x를 암호화 한다.
$D_{MK_{ij}}(x)$	마스터 키를 사용하여 암호화된 x를 복호화 한다.
$m_1 \| m_2$	2개의 메세지 m_1, m_2를 결합한다.

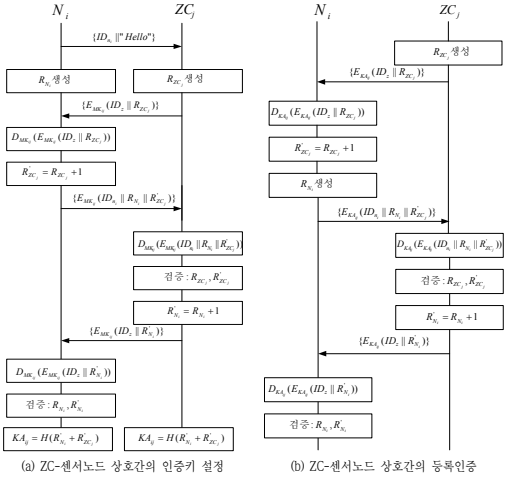


그림 10. ZC-센서노드 상호간의 등록인증
Figure 10. Registration Authentication of ZC-Sensor nodes

ZC-센서노드 상호간의 마스터 키는 불법적인 키 유출을 방지하기 위해 직접 인증에 적용하지 않고 ZC-센서 노드 상호간의 신규 인증키(KA_{ij})를 생성하여 인증에 적용한다. 그리고 ZC와 센서 노드 상호간의 안전한 키 설정 과정은 <그림 10-(a)>와 같다. 그리고 <그림 10-(a)>의 인증키 설정 과정을 통하여 ZC와 센서 노드 상호간에 안전하게 인증키(KA_{ij})를 생성한 후 ZC-센서 노드 상호 등록인증을 위해 안전하게 보관한다.

ZC-센서노드 상호 등록인증은 인증키 설정과정을 수행한 후 ZC-센서노드 상호간에 안전하게 설정된 인증키를 기반으로 <그림 10-(b)>와 같이 수행한다.

4.1.2 노드등록 알고리즘

알고리즘 2. 신뢰기반 노드 등록 알고리즘
Algorithm 2. Trust-based Node Registration Algorithm

Procedure Registration(M_i) {
/* M_i:N_i의 등록 요청 메세지($M_i = \{ID_i \| "Hello"\}$) */
Key_Setup ; /* 키설정 */
$\xi_{ZC,N_i}(0,0)$; /* 경험 정보 초기화:$f_s = 0, f_f = 0$ */
Select case (등록인증)
case Accept : {
Accept N_i; /* N_i의 센서망 등록요구 허락 */
$f_s = f_s + 1$;
$Bel(E_{ZC,N_i}) = \frac{f_s}{f_s + f_f}$; /* 신뢰정보 재계산 */
}
case Reject : {
Reject N_i; /* N_i의 센서망 등록요구 거부 */
$Bel(E_{ZC,N_i}) = 0$;
}
End Select /* 등록인증 */
if $Bel(E_{ZC,N_i}) \geq \Delta_t$ then /* 신뢰 상태 평가 */
$S_{E_{ZC,N_i}\{n\}} = \{Trust\}$
else
$S_{E_{ZC,N_i}\{n\}} = \{Uncertainty\}$;
End if
/*TIB갱신,$\xi_{ZC,N_i} = (f_s, f_f)$ */
Update_TIB($ID_i, \xi_{ZC,N_i}, Bel(E_{ZC,N_i}), S_{E_{ZC,N_i}\{n\}}$);
} /* End of Registration */

노드 등록은 신규 센서가 네트워크에 접속될 때 안전한 센서 노드만이 센서 네트워크에 접속되게 하여 IoT-센서망의 안전성을 높이며 센서 노드에 대한 신뢰 정보 초기화 과정을 수행하며 이를 위한 제안되는 노드등록은 <알고리즘 2>와 같이 동작한다.

4.2 데이터 송신 단계의 동작

알고리즘 3. 신뢰기반 상호인증 알고리즘
Algorithm 3. Trust-based Mutual Authentication Algorithm

```
Procedure Mutual_Authentication(M_i) {
  /* M_i :N_i의 수신 메세지(M_i = {ID_i||Data}) */
TIB_Retrive(ID_i) ; /* TIB의 신뢰 정보 검색 */
if ID_i ∉ TIB then Registration(M_i) ;
 Select case (S_{E_ZC,N_i{C}})
      case Trust: {
        if 위험경고수신 then
              Reject M_i;
              Bel(E_ZC,N_i) = 0;
         else
              Accept M_i;
              f_s = f_s + 1;
         Bel(E_ZC,N_i) = f_s / (f_s + f_f);/* 신뢰 정보재계산 */
         End if
        }
     case Uncertainty : {
       if Bel(E_ZC,N_i) = 0 then Reject M_i
        else
         Select case (등록인증)
              case Accept : {
                 Accept M_i ; /* M_i의 수신 허용*/
                 f_s = f_s + 1;
              }
              case Reject : {
                 Reject M_i ; /* M_i의 수신 거부*/
                 f_f = f_f + 1 ;
              }
         End select /* 등록인증 */
         Bel(E_ZC,N_i) = f_s / (f_s + f_f); /* 신뢰정보 재계산 */
    End if
                }
End Select  /* 신뢰 상태 검증 */

  if Bel(E_ZC,N_i) ≧ Δ_t then      /* 신뢰 상태 결정 */
          S_{E_ZC,N{n}} = {Trust}
     else
          S_{E_ZC,N_i{n}} = {Uncertainty};
  End if
/*TIB갱신,ξ_ZC,N_i = (f_s, f_f) */
  Update_TIB(ID_i, ξ_ZC,N_i, Bel(E_ZC,N_i), S_{E_ZC,N_i{n}});
} /* End of Mutual_Authentication */
```

데이터 송신 단계는 안전하게 등록된 센서 노드가 수집한 데이터를 ZC에게 송신할 경우 신뢰기반 인증을 수행하는 과정이다. 이 과정은 <그림 9> 같이 수면 상태에서 센서 노드가 송신한 데이터를 수신한 ZC는 데이터를 전송한 센서가 안전한 노드인가를 확인하기 위해 상호인증을 수행한다.

상호인증 수행 상태에서는 데이터를 송신한 센서 노드의 믿음의 정도를 알기 위해 제안한 신뢰모델에 기반한 신뢰평가를 수행하여 믿음의 정도가 신뢰 가능한 수준이라고 평가되면 대칭 키 기반의 등록인증을 수행하지 않고 센서 노드의 데이터 수신을 허락(accept)한다. 하지만 신뢰평가 결과 센서 노드의 믿음의 정도가 신뢰가 불확실한 정도라면 등록인증을 수행한 후 센서 노드의 데이터 수신 가능 여부를 결정하며 본 논문에서 제안하는 신뢰기반 상호인증은 <알고리즘 3>과 같이 동작한다.

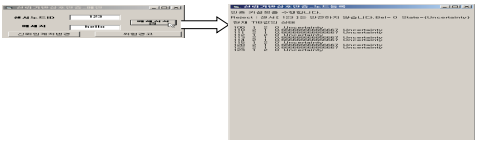
5. 구현 및 평가

본 장에서는 앞서 기술한 피코넷 단위의 지그비 IoT-센서망에서의 신뢰모델을 적용한 <알고리즘 2>와 <알고리즘 3>의 상호인증 알고리즘의 구현 및 평가 결과를 기술한다.

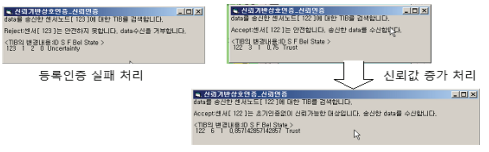
5.1 알고리즘 구현

제안된 알고리즘의 구현을 위하여 <그림 11>과 같이 Visual Studio를 사용하여 모듈 단위로 구현하여 시험분석에 적용하였다.

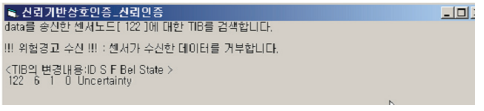
(a) 센서 휴면(sleep) 상태표현, 신뢰임계값 설정, 위험경고 설정



(b) 노드 등록 및 TIB 설정 상태



(c) 신뢰기반 상호인증 결과처리



(d) 위험 경고가 발생된 센서노드의 인증처리

그림 11. 신뢰기반 상호인증 알고리즘 구현
Figure 11. Implementing Trust-based Mutual Authentication Algorithm

5.2 평가

본 논문에서 제안한 신뢰기반 상호인증 모델은 신규노드 등록 절차의 등록인증을 통해 사전에 안전한 센서 노드들만 센서 네트워크 접속을 허가한다. 그리고 등록과정의 등록인증 과정을 통해 구성된 안전한 IoT-센서망에서 구성 노드 상호간의 신뢰 정보를 평가하여 인증을 수행한다.

그리고 이 절에서는 본 논문에서 안전한 지그비 IoT-센서망을 위해 제안한 신뢰기반 상호인증 알고리즘의 보안안전성 및 신뢰모델에 기초한 상호인증 기법의 경량성에 대한 평가 분석한 결과를 기술한다.

5.2.1 보안 안정성 평가

본 논문에서 적용한 등록과정의 등록인증에서는 대칭키 기반 인증을 수행한다. 이는 ZC-센서노드 상호간에 안전하게 분배된 인증키를 보유한 센서 노드만이 센서 네트워크의 접속이 가능하므로 노드 등록 단계에서의 안전성을 높일 수 있다. 그리고 제안한 등록인증 방식은 인증 메세지의 생성을 단순한 랜덤수 생성만을 적용하기 때문에 계산량을 줄일 수 있다. 그리고 적용된 등록인증에 대한 보안 안전성은 <표 1>에서 기술한 비밀성, 익명성, 상호인증, 신선성 측면에서의 안전성을 지원하고 있지만 무결성은 지원하지 않는다.

제안된 등록인증 알고리즘은 비밀성 확보를 위해 ZC-센서노드 인증을 위해 R_{N_i}와 R_{ZC_j}를 전송할 때 안전하게 분배된 인증키(KA_{ij})로 암호화($\{E_{KA_{ij}}(ID_{n_i}||R_{N_i}||R_{ZC_j})\}$)하여 전송한다. 이는 ZC-센서노드 인증 과정에서 인증 메세지의 비밀 보장이 가능하고 악성 노드의 도청 공격으로부터 안전성을 확보한다. 익명성 확보를 위하여 통신에 참여하는 ZC와 센서 노드 상호간에 노드 식별자(ID_{n_i}, ID_z)를 인증키로 암호화하여 전송한다. 이는 노드 식별자 유출로 인한 위장 공격으로부터 안전함을 나타낸다. 또한 등록인증 단계에서 센서 노드(N_i)와 j번째 그룹의 ZC 상호간에 안전하게 설정된 인증키(KA_{ij})를 보유한 대상만이 R_{N_i}와 R_{ZC_j}의 복호화가 가능하기 때문에 상호인증성을 지원한다. 등록인증 및 키 설정 과정에 사용되는 랜덤수 R_{N_i}과 R_{ZC_j}는 인증이 수행될 때마다 무작위로 새로운 값이 생성되기 때문에 재사용이 불가능함에 따라 신선성 지원이 가능하다. 그리고 센서 노드의 초기 등록과정에서 <표 4>과 같이 보안 안정성을 지원할 수 있다.

표 4. 제안된 신뢰 기반 인증모델의 보안 안전성 평가
Table 4. Security Safety Assessment of Proposed Trust-based Authentication Models

지원단계 / 안전성 지원	노드등록 단계		신뢰기반 상호인증
	인증키 설정	등록 인증	
비밀성	○	○	○
익명성	○	○	○
상호인증	○	○	○
무결성	X	X	X
신선성	○	○	○

5.2.2 신뢰기반 인증과정 평가

신뢰기반 상호인증 절차는 <그림 8>에서와 같이 등록인증 과정과 신뢰평가를 통한 인증과정으로 구분된다.

신뢰기반 상호인증 과정은 센서 노드의 등록 완료 후 일정 횟수 정도는 신뢰 임계값의 크기에 따라 등록과정의 등록인증을 통과한 센서노드 임에도 불구하고 등록인증 과정을 재 수행해야 한다. 하지만 통신에 참여하는 센서 노드의 신뢰 정보는 통신 횟수의 증가에 따른 등록인증의 성공 횟수가 많아질수록 믿음의 정도는 증가한다. 그리고 믿음의 정도가 정해진 신뢰 임계값 이상이면 신뢰 가능한 노드로 평가하게 된다. 신뢰 가능한 노드로 평가된 센서 노드는 이후의 통신 과정에서는 등록인증을 수행하지 않고도 신뢰평가만으로 ZC와의 안전한 통신이 가능하며 관련된 보안 동작 계산량 및 수행 절차 감소와 이에 따른 경량화가 가능하다. 이를 증명하기 위해 제안된 <알고리즘2>와 <알고리즘 3>을 <그림 10>과 같이 구현하여 <표 5>의 실험조건을 설정하여 신뢰기반 상호인증을 수행하는 과정에서 등록인증의 수행 빈도수와 신뢰평가 인증의 수행 빈도수를 측정한 결과는 <그림 12>와 같다.

표 5. 실험조건
Table 5. Experimental Conditions

(1) 총 100회의 통신을 수행한다.
(2) 신뢰 임계값은 각각 1.0, 0.9, 0.8, 0.7, 0.5로 서로 다르게 적용하고 신뢰임계값(Δ_t) 별로 인증 방법의 수행 빈도수를 측정한다.
(3) 통신에 참여하는 센서 노드는 정상적인 인증키를 소유한 안전한 노드이다

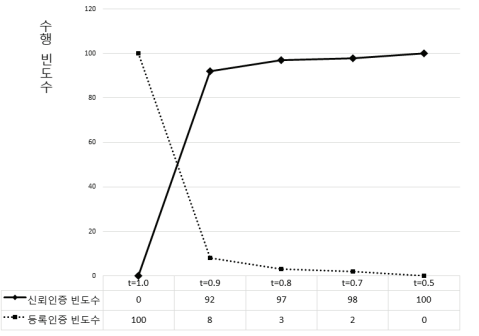


그림 12. 신뢰 임계값(Δ_t) 변화에 따른 인증방식의 적용 빈도수의 변화
Figure 12. The Frequency of Application of Autentication Methods According to Changes in Trust Thresholds

<그림 12>의 결과에 대한 특징을 분석하여 보면 첫째. 안전한 센서 노드인 경우 등록인증만을 적용하여 인증을 할 경우 안전한 노드임에도 불구하고 매 통신 세션마다 등록인증 과정이 요구된다. 하지만 제안한 상호인증 모델은 센서 노드의 활동 초기에 일정한 횟수 이하의 등록인증을 수행하지만 통신 횟수가 증가하고 인증 성공 횟수 증가에 대한 신뢰평가 정보를 기초로 안전한 것으로 평가된 센서 노드들에 대해서는 등록인증 없는 신뢰평가만으로 안전한 노드를 구분할 수 있다.

둘째. 신뢰 임계값이 작아질수록 등록인증의 수행보다는 연산량이 상대적으로 적은 신뢰평가를 통한 인증의 수행 빈도수가 높아진다. 반면에 신뢰 임계값이 커질수록 등록인증의 수행 빈도수가 증

가된다. 이점은 신뢰 임계값의 크기에 따라 센서망에서 인증 과정의 강도 및 이에 따른 인증 과정의 경량성 조절이 가변적으로 가능한 특성이 제안한 신뢰기반 상호인증 모델에 존재하는 것을 알 수 있다.

따라서 신뢰성이 보장된 안전한 센서 노드의 경우 제안한 신뢰기반 인증모델에서 신뢰평가 정보만을 갖고 인증을 수행할 경우, 대칭키 기반의 인증 방식보다 인증 과정의 각 센서 노드와 ZC의 계산량 및 동작 절차가 감소하게 될 것이고 이에 따른 ZC-센서노드 상호간의 보안인증 절차를 경량화 할 수 있을 것으로 판단된다.

6. 결 론

본 논문에서는 지그비 IoT-센서망을 위한 신뢰평가 모델과 제안된 신뢰평가 모델에 기반한 상호인증 알고리즘을 제안하였다.

제안된 신뢰모델은 지그비 IoT-센서망을 구성하는 ZC와 센서 노드 상호간의 믿음의 관계 설정을 통한 안전한 IoT-센서망 구성에 적용이 가능하다. 또한 안전한 IoT-센서망 구축을 위한 보안키 관리, 역할 접근 제어(RBAC) 등과 같은 다양한 신뢰 기반 경량 보안 기술 그리고 IoT 센서망을 구성하는 노드들에 대한 능동적 장애 관리 분야 등에 응용이 가능할 것으로 판단한다.

제안된 신뢰평가 기반 상호인증 알고리즘은 안전한 지그비 IoT-센서망을 구성하기 위해 초기 등록인증 과정을 통한 보안 신뢰성을 확보한 센서 노드들에 대해서는 연산량이 많고 절차가 복잡한 보안키 기반 등록인증을 매번 적용하지 않고서도 ZC-센서 노드 상호간의 믿음의 정도를 계산한다. 그리고 이에 따른 보안 신뢰상태를 평가하여 상호인증을 수행하기 때문에 보안 인증과정상의 연산량 및 인증 절차 감소 측면의 경량성이 존재한다. 또한 신뢰평가를 사용한 상호인증과정에서 신뢰 임계값을 관리자가 보안 안전의 중요도에 따라 가변적으로 조절하여 IoT-센서망의 인증수준 조절이 가능하고 이에 따른 경량성 및 보안 안전수준 조절이 가변적으로 가능하다. 이점은 신뢰성 높은 센서 노드들에 대해서는 보안 연산절차를 최소로 수행하여 배터리 소모를 줄이면서 지그비 IoT-센서망의 안전성을 보장할 수 있으며 이에 따른 지그비 IoT-센서망의 생존 기간 연장이 가능한 것으로 판단한다.

본 논문의 결과를 기반으로 향후 첫째, 센서 노드 위장을 통한 신뢰정보 조작 방지에 대한 방안, 둘째, 대규모 지그비 IoT-센서망에서 여러 지그비 IoT-센서망 그룹 상호간의 신뢰평가 모델에 기반한 스캐터넷 에서의 간접신뢰 방식을 이용한 계층적 인증방식, 셋째, 신뢰평가 모델에 기반한 안전한 대칭키 분배 및 관리 기술 등에 대한 추가 연구를 수행 할 계획이다.

References

[1] S-G. Hong, H. Lee, J-C. Choi, M-N. Bae, and K-B. Lee, *Internet of things software platforms technology trends*, Electronics and Telecommniucations Trends. Vol. 30, No. 5. pp. 49-58, 2015.

[2] J. Ko, S-G. Hong, B-B. Lee, and N-S, Kim, *Trends of converging smart devices with IoT technology*, Electronics and Telecommniucations Trends. Vol. 28, No. 4. pp. 79-85, 2013.

[3] H. Karl, and A. Willig, *Protocols and architectures for wireless sensor networks*, WILEY, pp.281-283, 2005.

[4] B-H. Kim, J-M. Lim, and C-S. Park, *Analysis of ZigBee security mechanism*, Journal of Security Engineering, Vol. 9, No. 5, pp. 417-480, 2012.

[5] H. Chan, A. Perrig, and D. Sung, *Random key predistribution schemes for sensor networks*, In Proceedings of the IEEE Security and Privacy, 2003 Symposium, pp. 197-213, 2003.

[6] L. Bussard and Y. Roudier, *Authentication in Ubiquitous Computing*, In Proceedings of the Workshop on Security in Ubiquitous Computing UBICOMP 2002, 2002.

[7] A. Perrig, R. Szewczyk. V. Wen, D. Cullar, and J-D. Tygar, *SPINS:Security protocols for sensor networks*, Wireless Networks Journal(WINET), Vol. 8, No. 5, pp. 521-534, 2002.

[8] S. Zhu, S. Setia, and S. Jajodia. *LEAP:Efficent security mechanisms for large-scale distributed sensor networks,* The 10th ACM Conference on Computer and Communications Security (CCS '03) Washington D.C., pp. 62-72, Oct. 2003.

[9] H. Yang, X. Meng, and S. Lu, *Self-organized network layer security in mobile ad hoc networks*, In Proceedings of ACM Workshop on Wireless Security (WiSe'02), Atlanta, USA, pp. 11-20, Sep. 2002.

[10] T. Beth, M. Borcherding, and B. Klein, *Valuation of trust in open networks*, in Proceedings of the European Symposium on Research in Computer Security. Brighton, UK: Springer-Verlag, pp. 3-18, 1994.

[11] R. Yahalom, B. Klein, and T. Beth, T*rust relationships in secure systems a distributed authentication perspective*, in Proceedings of IEEE Computer Society Symposium on Research in Security and Privacy (RSP '93), pp. 150-164, 1993.

[12] A. Abdul-Rahman, and S. Halles, *A distributed trust model*, in Proceedings of New Security Paradigms Workshop '97, pp. 48-60. 1997.

[13] L. Xiong, and L. Liu, *A reputation-based trust model for peer-to-peer e-commerce communities,* In Proceedings of the 4th ACM conference on Electronic Commerce, pp. 228-229, 2003.

[14] X. Li, M-R. Lyu, and L. Liu, *A trust model based routing protocol for secure Ad-Hoc networks*, IEEE Aerospace Conference, pp. 6-13. Mar. 2004.

[15] L. Echenauer, and V-D. Gligor, *A key-management scheme for distributed sensor networks,* In Proceedings of the 9th computer communication security, pp. 41-47, 2002.

[16] Y. Teng, V. V. Phoha, and B. Choi, *Design of trust metrics based on dempster-shafer theory,*http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.21.8090&rep=rep1&type=pdf, Jan. 2001.

[17] D-W. Manchala and Trust metrics, *model and protocol for electronic commerce transactions,* In Proceedings of The 18th International Conference on Distributed Computing Systems, pp. 312-321, May 1998.

[18] A. Jøsang*, A logic for uncertain probabilities,* International Journal of Uncertainty, Fuzzyness and Knowledge-Based Systems, Vol. 9, pp. 279-311, 2001.

[19] *A.* Jøsang*, A metric for trusted systems,* In Proceedings of the 15th IFIP/SEC International Information Security Conference, IFIP, 1998.

[20] B. Shand, N. Dimmock, and J. Bacon, *Trust*

for ubiquitous, transparent collaboration, In Proceedings 1st IEEE Annual Conference on Pervasive Computing and Communication, Mar. 2003.

[21] S. Saleem, S. Ullah, and K-S. Kwak, *A study of IEEE 802.15.4 security framework for wireless body area networks,* Sensors 2011-Volume 11", Issue 2, Jan. 2011.

[22] ZigBee Alliance, *ZigBee specification- r17,* part 1.1.4, http://www.zigbee.org/, Jan. 2008.

[23] H. Karl, and A. Willig, *Protocols and architectures for wireless sensor networks,* WILEY, pp.281-283, 2005.

IoT-센서망에서 신뢰평가 모델 기반 노드 상호인증

김홍섭

충북보건과학대학교 바이오의료정보과 부교수

요 약

최근 사물인터넷(IoT) 기술에 대한 관심이 증가되고 있으며 IoT 기술의 핵심은 센서망 기술이다. IoT-센서망은 지그비 망구조가 많이 활용되고 있지만 지그비 IoT-센서망은 특성상 센서 정보의 도청, 비정상적인 패킷의 흐름, 데이터 위•변조 및 서비스 거부 공격 등과 같은 다양한 보안 위협에 취약점이 존재한다. 하지만 지그비 IoT-센서망은 컴퓨팅 능력이 제한된 자원 환경에서 운용되어야 한다. 따라서 IoT-센서망보안 기술은 경량화 설계에 대한 연구가 반드시 필요하다. 본 논문에서는 적은 보안 연산으로도 안전한 IoT-센서망 구축이 가능한 신뢰평가 모델 기반 IoT-센서망 상호인증 알고리즘을 제안하였다. 제안된 신뢰평가에 의한 인증 알고리즘은 지그비 피코넷에 소속된 ZC-센서 노드 상호간의 직접신뢰 관계를 적용하여 설계되었으며 확률 계산 및 논리 연산 중심으로 노드들의 신뢰평가를 하여 IoT-센서망의 ZC-센서 노드 상호간의 인증을 수행한다. 또한 본 논문에서 제안된 상호인증 알고리즘은 IoT-센서망의 보안안전성 측면에서 비밀성, 익명성, 상호인증, 신선성을 지원 가능하고 신뢰평가모델을 적용함에 따라서 기존 인증 방식보다 경량성을 높일 수 있다. 그리고 센서 노드들의 제한된 배터리 소모를 줄여 IoT-센서망의 안전성 및 생존 기간 연장이 가능할 것이다.

Hong-Seop Kim received the bachelor's degree in the Department of Computer Science and Statistics from the Chungbuk University in 1990. He received the M.S. degree and the Ph.D. degree in the Department of Computer Science from Chungbuk University in 1992 and 2007, respectively. He has been a professor in the Department of Biomedical Information at Chungbuk Health and Science University since 1994. His current research interests include information protection, network security, IoT-service & security, Bio-ICT converged security, bio-informatics, etc. He is a regular member of the KKITS.

E-mail address: hskim@chsu.ac.kr