Journal of Digital Convergence
Vol. 18. No. 10, pp. 233-238, 2020

ISSN 2713-6434 / eISSN 2713-6442
https://doi.org/10.14400/JDC.2020.18.10.233

클라우드 환경에서 IoT 정보 오류를 고려한 지형 정보 기반의 키 관리 기법

정윤수[1], 최정희[2*]
[1]목원대학교 정보통신융합공학부 교수, [2]목원대학교 스톡스대학 SW교양학부 교수

A Key Management Technique Based on Topographic Information Considering IoT Information Errors in Cloud Environment

Yoon-Su Jeong[1], Jeong-hee Choi[2*]
[1]Professor, Dept. of Information Communication & Engineeringe, Mokwon University,
[2]Professor, Division of Software Liberal Arts, Stokes College, Mokwon University

요 약 클라우드 환경에서는 센서 및 웨어러블 장치를 이용한 IoT 기기가 다양한 환경에서 응용되고 있으며 그에 따른 IoT 기기에서 생성되는 정보를 정확하게 판별하는 기술들이 활발하게 연구되고 있다. 그러나, 전력 및 보안과 같은 IoT 환경의 제약사항으로 인하여 IoT 장치에서 발생하는 정보가 매우 취약하기 때문에 금전 피해 및 인명 피해가 증가하고 있다. 본 논문에서는 IoT 정보를 정확하게 수집・분석하기 위해서 IoT 정보 오류를 고려한 지형 정보 기반의 키 관리 기법을 제안한다. 제안 기법은 IoT 장치를 클라우드 환경에서 임의로 배치할 경우 IoT 장치의 연결성을 확보하기 위해서 IoT 배치 오류를 허용하는 동시에 지형 정보를 n개의 그룹으로 그룹핑 하도록 한다. 특히, 각 그룹핑 된 지형 정보에는 전체 키 풀에서 랜덤하게 선택된 임의의 키를 할당한 후 IoT 정보에 포함된 지형 정보의 키와 확률적으로 높은 키 값을 IoT 장치의 연결성으로 확보할 수 있도록 한다. 특히, 제안 기법은 확률적 딥러닝을 이용하여 IoT 지형 정보의 키를 시드로 추출하기 때문에 IoT 장치에 대한 정보 오류를 낮출수 있다.

주제어 : 클라우드, 사물인터넷, 지형 정보, 키 관리, 딥러닝, 확률 기반, 클러스터링

Abstract In the cloud environment, IoT devices using sensors and wearable devices are being applied in various environments, and technologies that accurately determine the information generated by IoT devices are being actively studied. However, due to limitations in the IoT environment such as power and security, information generated by IoT devices is very weak, so financial damage and human casualties are increasing. To accurately collect and analyze IoT information, this paper proposes a topographic information-based key management technique that considers IoT information errors. The proposed technique allows IoT layout errors and groups topographic information into groups of dogs in order to secure connectivity of IoT devices in the event of arbitrary deployment of IoT devices in the cloud environment. In particular, each grouped terrain information is assigned random selected keys from the entire key pool, and the key of the terrain information contained in the IoT information and the probability-high key values are secured with the connectivity of the IoT device. In particular, the proposed technique can reduce information errors about IoT devices because the key of IoT terrain information is extracted by seed using probabilistic deep learning.

Key Words : Cloud, Internet of Things, terrain information, key management, deep learning, probability-based, clustering

*Corresponding Author : Jeong-hee Choi(jhchoi@mokwon.ac.kr)
Received August 13, 2020 Revised September 2, 2020
Accepted October 20, 2020 Published October 28, 2020

1. 서론

클라우드 환경은 스마트 기기 및 웨어러브 시장의 성장으로 인하여 IoT 분야는 다양한 환경에서 그 수요가 증가하고 있다[1]. 클라우드 환경은 IoT 기술을 이용하여 애드혹, 멀티홉, 메시 네트워크를 구성하고 서로 상호작용하여 다양한 응용에서 활용 가능하다[2,3]. 그 이유는 데이터를 수집·분석하는 IoT 장치가 고정되었지만, 최근에는 이동성이 가능한 IoT 장치를 이용하기 때문이다[4,5].

IoT 장치와 관련된 보안 기술에는 대칭키 기반 키 관리 기술(결정적 방식과 확률적 방식 등)이 많이 사용된다[6-9]. 그러나, IoT 장치가 배치되는 지형 정보에 따라 사용방법 및 효율성이 달라질 수 있다. 지형이 단순하고 IoT 장치 수가 적을 경우에는 결정적 방식이 효율적이지만 지형이 복잡하고 IoT장치 수가 많을 경우 사용되는 키가 많아질 경우에는 확률적 방식을 많이 사용하게 된다.

클라우드 환경에서는 IoT 정보를 효율적으로 처리하는 방법들이 다양하게 제시되고 있다[4-6]. 특히, 클라우드 IoT는 기업의 요구사항에 의해서 탄생된 서비스로써 기존 서비스보다 저렴한 비용과 IoT 기기의 편리한 관리성을 통해 데이터를 수집 및 분석할 수 있다. 클라우드 환경에서 IoT 장치의 배터가 모두 소모되었든지 인터넷 연결이 좋지않았을 때 문제가 발생하지 않도록 하는 것이 가장 큰 특징 중에 하나이다. 이 특징은 보통 IoT 디바이스 새도라는 의미로도 사용된다. 그러나, 기존 방법들은 IoT 장치를 지형 정보에 고려하지 않고 클라우드로 전송되는 정보 수에 대한 오류를 고려하지 않고 있다. IoT 배치 오류가 발생하거나 IoT 통신이 커버되지 않는 지역에서는 IoT의 정확한 위치를 예측하는 것이 어렵고 네트워크의 키 연결성에 큰 영향을 미치게 되므로 IoT 배치 오류를 고려한 키 관리 기술이 필요하다.

본 논문에서는 클라우드 환경에서 IoT 정치를 이용하여 서버와 IoT 장치 간 정보 송·수신을 효율적으로 처리하기 위해서 IoT 정보 오류를 고려한 지형 정보 기반의 키 관리 기법을 제안한다. 제안 기법은 클라우드 환경에 임의로 배치된 IoT 장치의 확률 연결성을 확보하기 위해서 IoT 배치 오류를 허용하는 동시에 지형 정보를 n개의 그룹으로 그룹핑 하도록 한다. 제안 기법은 그룹핑 된 각 지형 정보는 전체 키 풀에서 랜덤하게 선택된 임의의 키를 할당한 후 IoT 정보에 포함된 지형 정보의 키와 확률적으로 높은 키 값을 IoT 장치의 연결성으로 확보한다. 특히, 제안 기법은 IoT 지형 정보의 키를 시드로 추출하기 때문에 IoT 장치에 대한 정보 오류를 낮출수 있다.

이 논문의 구성은 다음과 같다. 2장에서는 지형정보 관련 기 관리 기법에 대해서 알아본다. 3장에서는 IoT 정보 오류를 고려한 지형 정보 기반의 키 관리 기법을 제안하고, 4장에서는 지형 정보 기반의 키 관리 기법들을 제안 기법과 비교 평가하고, 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

IoT 관련 키 관리 기법은 크게 결정적(deterministic) 방식, 확률적(probabilistic or non-deterministic) 방식, 위치 기반(location based) 방식으로 나뉘어 사용된다[6, 7,13]. 결정적 방식은 배치 전 적재된 단일 초기 키(initial key)와 배치 후 IoT 장치와 주고받는 정보를 이용하여 IoT 장치 간 키 쌍(pairwise-key)를 계산하여 주변 IoT 장치와 키를 나누어 사용한다[8]. 그러나, 결정적 방식은 단일 초기 키가 공격자에게 노출될 경우 전체 네트워크의 안전성이 보장받지 못하는 단점이 있다[9].

확률기반 키 관리 방식은 매우 큰 키풀에서 랜덤하게 키들을 선택하여 IoT 가 배치되기 전에 키 링의 형태로 IoT장치에 적재된다. 확률기반 키 관리 방식은 네트워크에 배치 후 주변 IoT들과 키 링의 공유키를 찾아내기 때문에 주변의 IoT와 키를 나눠가질 확률이 존재한다[10,11]. 그러나, 확률기반 키 관리 방식은 정확하게 키를 공유한 IoT 장치 그룹을 선택하는 것이 어려워 키 연결성이 낮고 네트워크 크기가 고정되어 있다[11, 12].

위치 기반 방식은 IoT 장치에 정확하면서도 컴팩트한 키 링을 사전 적재함으로써 IoT 장치 배치 후 공유키와 경로 키 설정 관련 프로토콜을 간단하게 설정할 수 있다. 그러나, 위치 기반 방식은 경량·저전력 키 관리 기술 이외에는 부적합한 단점이 있다. 또한, 배치 오류가 증가하거나 통신 오류가 발생한다면 IoT 네트워크의 커버리지와 연결성을 높이기 위한 추가 연구가 필요하다[13-15].

3. IoT 정보 오류를 고려한 지형 정보 기반의 키 관리 기법

이 절에서는 클라우드 환경에서 IoT 정보가 수집된 정보를 효율적으로 분석 처리하기 위해서 Fig. 1과 같이 지형 정보를 이용한 키 관리 기법을 제안한다.

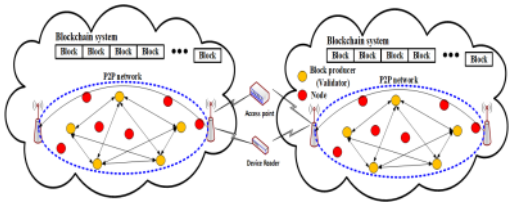

Fig. 1. Proposed Model

3.1 시스템 구성

제안 기법은 클라우드 환경에서 IoT의 지형 정보를 이용하여 키 관리를 효율적으로 하기 위해서 시스템 모델은 IoT 장치, 서버, 키 생성 센터 등 3가지로 구성된다. 제안 기법의 시스템 모델은 내·외부의 제 3자와 통신할 때 발생할 수 있는 채널 공격에 대한 보안상 안전이 보장되어야 한다고 가정한다.

· IoT 장치

IoT 장치는 서버에 등록된 장치로써 수집 정보를 보내는 역할을 담당한다. IoT 장치는 인터넷 통신 채널을 통해서 서버에 접속한 후 서버에 등록된 위치 정보와 비교 후 일치 유·무를 확인한다.

· 서버

서버는 IoT 장치 정보를 모두 저장하고 있으며 IoT 장치에서 수집되는 정보를 모두 저장하고 있다. 서버는 클라우드 환경에서 수집된 IoT 정보 오류를 체크하여 사용자 요구가 있을 경우, 요구사항에 따라 IoT 정보를 제공한다.

· 키 생성 센터

키 생성 센터는 IoT 장치의 지형 정보를 기반으로 키를 생성하고 관리하는 역할을 담당한다. 키 생성 센터는 IoT 지형 정보를 $n-bit$ 블록 형태 구분 후 IoT 장치 간 연계 정보 θ와 함께 대칭 암호 알고리즘에 적용하여 IoT 장치 간 여계 키를 생성한다.

3.2 지형 정보를 이용한 IoT 위치 측정

제안 기법에서는 Thomas 알고리즘의 다변 측량법을 Fig. 2와 같이 이용하여 지형 정보측정을 위한 공간 내에서 발생할 수 있는 거리의 최소값과 최대값을 설명함으로써 정확도를 보정하는 동시에 오차를 보정할 수 있다.

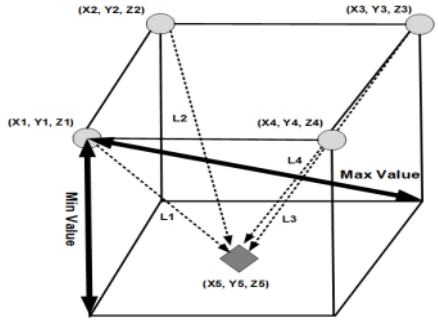

Fig. 2. Terrain Information Location Information Measurements

제안 기법에서는 클라우드 환경에 위치한 IoT 정보의 오류를 최소화하면서 지형 정보 기반의 키 관리를 효율적으로 유지하기 위해서 식 (1)을 이용하여 IoT 장치의 위치를 계산한다.

$$\begin{aligned} L_1^2 &= (X5-X1)^2+(Y5-Y1)^2+(Z5-Z1)^2 \\ L_2^2 &= (X5-X2)^2+(Y5-Y2)^2+(Z5-Z2)^2 \\ L_3^2 &= (X5-X3)^2+(Y5-Y3)^2+(Z5-Z3)^2 \\ L_4^2 &= (X5-X4)^2+(Y5-Y4)^2+(Z5-Z4)^2 \end{aligned} \quad (1)$$

Fig. 1처럼 클라우드 환경에 배치된 IoT 장치는 식 (1)의 위치 정보를 이용하여 서로 완전 쌍키(FP: full pairwise key)를 설정하며 인접한 IoT 장치와는 사전 정의한 확률과 임의로 선정한 IoT 장치의 통신 범위를 바탕으로 랜덤 쌍키(FPrandom pairwise key)를 설정한다. 이 같이 설정하는 이유는 IoT 장치에 대한 배치 오류에 대한 저항성이 뛰어나며 높은 키 연결성을 확보할 수 있기 때문이다.

3.3 IoT 위치 정보 검증

제안 기법에서는 클라우드 환경에 배치된 IoT 장치의 지형 정보 $TI(x)$는 식 (2)처럼 N-1차 다항식을 사용하여 IoT 장치의 지형 정보를 샘플링하여 분산되도록 함으로써 IoT 장치의 위치정보의 무결성을 검증할 수 있다.

$$TI(x) = \begin{cases} a_1+a_2x^1+\cdots+a_nx^{n-1} \mod s & ,\text{if } a,n>1 \\ 1 & ,otherwise \end{cases} \quad (2)$$

여기서, n은 IoT 장치의 장치 수를 의미하고, a는 IoT 장치의 지형 정보의 크기를 의미한다.

IoT 지형 정보에 위장될 기존 IoT 지형 정보 p와 IoT 장치의 지형 정보의 크기 a를 식 (3)처럼 생성한다.

$$a_n = p \mod s \tag{3}$$

IoT 지형 정보는 분산 암호화된 지형 정보를 참조하여 각 지형 정보의 차이를 식 (3)처럼 계산한 후 식별하게 된다.

$$a_n^{'} = a_n - p_n \tag{4}$$

IoT 지형 정보는 $\sum_{i=1}^{n} a_n$은 기존 IoT 지형 정보 p에 대해서 식별된 은닉 정보 $a_1 + a_2 + \cdots + a_n$을 중첩함으로써 IoT 지형 정보를 무손실로 복원할 수 있다.

3.4 IoT 장치 키 생성 및 검증

제안 기법에서 사용되는 IoT 지형 정보의 무결성을 검증하기 위해서 공개키와 개인키를 사용된다. 개인키는 임의의 랜덤수 x_1^0과 x_1^1을 사용하여 생성되면 공개키는 개인키(x_1^0과 x_1^1)에 따라 각각 대응된 공개키 PK_i^{θ}를 생성한다. 공개키 PK_i^{θ}에 사용된 i는 공개키의 수를 의미하고, θ는 개인키가 x_1^0와 x_1^1 일 때 각각 0과 1로 매칭된다.

IoT 정보 오류를 고려한 지형 정보 기반의 키를 IoT 장치가 서버로부터 위임받기 위해서는 서버가 서명 권한이나 유효기간과 관련된 정보를 식 (5)처럼 생성하여 식 (6)과 같은 서명을 생성하여 보내야 한다.

$$Generate \quad gi_i \quad (i \in Z^*) \tag{5}$$

$$Sig = (-1)^{x_i^0} \cdot e^{x_i^1} \cdot H(gi_i) \mod s \tag{6}$$

IoT 장치는 서버에게 서명, 개인키 및 공개키를 공개키로 암호화하여 식 (7)처럼 전달한다.

$$Transfer \ E_{PK_i^{\theta}}(Sig, \ x_1^0, \ x_1^1, \ gi_i) \tag{7}$$

서버는 IoT 지형 정보는 $\sum_{i=1}^{n} a_n$에 대한 은닉 정보 $a_1 + a_2 + \cdots + a_n$를 생성하여 IoT 장치의 지형 정보 p와 일치하지 않는다면 IoT 장치에게 IoT 지형 정보를 재요청한다.

4. 성능 평가

제안 기법은 위치 기반의 기존 기법과 키 연결성, 저장 효율성, 통신 효율성 등으로 평가하였다. 키 연결성은 기존 기법(FP, RP, FRP 등)에 비해 평균 13.2% 향상되었고, 저장 효율성은 평균 28.2% 향상된 결과를 얻었다. 마지막으로 통신 효율성은 지형 정보를 이용한 제안 기법이 평균 8.2% 향상되었다.

4.1 실험환경

실험 평가를 위해서 IoT 지형 정보 분석과 그에 따른 시뮬레이션을 NS-3를 이용하였으며 〈Table 1〉과 같은 기본 파라미터를 설정하였다. IoT 장치가 실제 지형 정보에 가깝게 처리하도록 Blender 2.8의 직관적인 UI와 높은 자유도를 사용하였다. 또한, IoT의 지형 정보에 대한 좌표는 Unity를 활용하여 획득하였다.

Table 1. Simulation parameter

Parameter	Value
Number of server	1
Number of IoT	100
Number of relay nodes	12
Link capacity	1Gbps
Link round trip delay	20ms
Internet Timeout Timer	250ms
Number of Subnet	s={2, 4, 6, 8, 10, 12}
Number of IoT Information	d = {1, 5, 10, 25}
Buffer	50 packet
Traffic	5 pkts/s

4.2 키 연결성

Table 2는 클라우드에 배치된 IoT 장치를 그리드 분할 수에 따라 키 연결성을 나타내고 있다. Table 2에서 제안 기법은 IoT 장치의 정보 오류를 최소화하기 위해서 IoT 장치간 확률 값을 연계하도록 하였다. 성능평가 결과, IoT 장치를 서로 연계하여 그리드를 분할 수를 증가

할수록 키 연결성은 평균 13.2% 낮아지는 결과를 얻었다. 이 같은 결과는 IoT 장치간 정보 오류를 최소화하도록 IoT장치간 연계 확률값을 유지하였기 때문에 나타난 결과이다.

Table 2. key connection comparison

Grid Split Count	Key connection (%)			
	FP	RP	FRP	Proporse scheme
2×2	91.357	93.528	95.745	97.531
4×4	83.746	85.671	87.928	91.258
6×6	71.355	75.973	79.693	84.326
8×8	60.934	64.689	72.546	77.698
10×10	52.547	56.672	60.361	69.247
12×12	43.651	49.165	53.248	61.214

FP : Full pairwise key, RP : Random Pairwise
FRP : Full and Random Pairwise

4.3 저장 효율성

Table 3는 클라우드 환경에서 IoT 정보 오류를 고려한 지형 정보기반의 키 정보 저장에 대한 효율성을 평가하였다. Table 3처럼 IoT 정보 오류를 최소화하기 위해서 IoT 장치가 확률 연계 값을 서버가 처리하기 때문에 기존 모델보다 저장 효율성이 평균 28.2% 높았다. 이 같은 결과는 제안 기법이 IoT 지형 정보를 $n-bit$ 블록 형태 구분 후 IoT 장치간 연계 정보 θ와 함께 대칭 암호 알고리즘에 적용하여 IoT 장치 간 여계 키를 생성하였기 때문이다.

Table 3. Storage efficiency comparison

Grid Split Count	storage efficiency (Bytes)			
	FP	RP	FRP	Proporse scheme
2×2	486.3	524.9	567.3	589.3
4×4	422.1	458.9	504.9	524.7
6×6	353.8	407.4	436.7	473.5
8×8	287.5	321.5	364.7	401.6
10×10	211.3	277.3	304.8	364.3
12×12	169.8	216.7	268.9	321.4

FP : Full pairwise key, RP : Random Pairwise
FRP : Full and Random Pairwise

4.4 통신 효율성

Fig. 5은 IoT 장치에서 수집한 IoT 정보들의 오류를 고려한 통신 효율성을 나타내고 있다. 제안 기법은 IoT 장치에 정보를 추출할 때 개인키와 공개키를 사용하여 IoT 지형 정보의 무결성을 검증하게 된다.

Table 4. communication efficiency

Grid Split Count	Communication efficiency (%)			
	FP	RP	FRP	Proporse scheme
2×2	77.8	80.3	82.4	86.7
4×4	71.2	75.3	78.6	83.2
6×6	64.3	69.2	73.3	81.4
8×8	58.6	62.1	69.7	78.3
10×10	52.3	56.7	66.6	74.8
12×12	48.6	52.4	63.1	72.1

FP : Full pairwise key, RP : Random Pairwise
FRP : Full and Random Pairwise

Table 4의 실험결과처럼, 제안 기법은 IoT 정보 오류를 고려하여 지형 정보의 확률 연계를 적용하였기 때문에 기존 모델보다 통신 효율성이 평균 8.2% 높게 나타났다. 이 같은 결과는 IoT 정보 오류를 고려한 지형 정보 기반의 키를 IoT장치가 서버로부터 위임받도록 서명 권한이나 유효기간과 관련된 정보를 이용하여 서명을 생성하였기 때문에 나타난 결과이다.

5. 결과

최근 클라우드 환경에서 사용되는 스마트 기기 및 웨어러브 장치들에 대한 수요가 다양한 분야에서 증가하고 있다. 클라우드 환경에서는 IoT 기술을 이용한 정보 보호를 위한 다양한 기술들이 개발되고 있다. 그러나, IoT가 배치된 지형 정보를 이용한 기술들은 여전히 연구가 필요한 상황이다. 본 논문에서는 IoT 정보를 정확하게 수집・분석하기 위해서 IoT 정보 오류를 고려한 지형 정보 기반의 키 관리 기법을 제안하였다. 제안 기법은 IoT 장치를 클라우드 환경에서 임의로 배치할 경우 IoT 장치의 연결성을 확보하기 위해서 IoT 배치 오류를 허용하는 동시에 지형 정보를 n개의 그룹으로 그룹핑하였다. 특히, 각 그룹핑 된 지형 정보에는 전체 키 풀에서 랜덤하게 선택된 임의의 키를 할당한 후 IoT 정보에 포함된 지형 정보의 키와 확률적으로 높은 키 값을 IoT 장치의 연결성으로 확보할 수 있도록 하였다. 성능평가 결과, IoT 장치를 서로 연계하여 그리드를 분할 수를 증가할수록 키 연결성은 평균 13.2% 낮아지는 결과를 얻었다. IoT 정보 오류를 최소화하기 위해서 IoT 장치가 확률 연계 값을 서버가 처리하는 저장 효율성은 평균 28.2% 높았

다. 또한, IoT 정보 오류를 고려하여 지형 정보의 확률 연계를 적용한 제안 기법은 기존 모델보다 통신 효율성이 평균 8.2% 높게 나타났다. 향후 연구에서는 본 연구의 결과를 기반으로 지리 정보를 이용한 IoT 활용 분야에 적용할 계획이다.

REFERENCES

[1] L. Cheng, S. Kotoulas, T. E. Ward & G. Theodoropoulos. (2017). Improving the robustness and performance of parallel joins over distributed systems, *Journal of Parallel and Distributed Computing, 109,* 310-323.

[2] M. Zaharia, M. Chowdhury, M. J. Franklin, S. Shenker & I. Stoica. (2010). Spark: cluster computing with working sets, P*roceedings of the 2nd USENIX conference on Hot topics in cloud computing(HotCloud'10),* 10-10.

[3] W. R. Heinzelman, A. Chandrakasan & H. Balakrishnan. (2000). Energyefficient communication protocol for wireless microsensor networks, *Proceedings of the 33rd annual Hawaii international conference on System sciences, IEEE,* 10.

[4] G. Chen, C. Li, M. Ye & J. Wu. (2009). An unequal cluster-based routing protocol in wireless sensor networks, *Wireless Networks, 15(2),* 193-207.

[5] H. Mao, M. Alizadeh, I. Menache & S. Kandula. (2016). Resource management with deep reinforcement learning, *Proceedings of the 15th ACM Workshop on Hot Topics in Networks. ACM,* 50-56.

[6] C. Y. Chen & H. C. Chao. (2014). A survey of key distribution in wireless sensor networks, *Security and Communication Networks, 7,* 2495-2508.

[7] M. A. Simplício Jr., P. S.L.M. Barreto., C. B. Margi, & T. C.M.B. Carvalho (2010). A survey on key management mechanisms for distributed wireless Sensor networks, *Computer Networks, 54,* 2591-2612.

[8] S. Zhu, S. Setia & S. Jajodia. (2003). LEAP: efficient security mechanisms for large-scale distributed sensor networks, *In Proc. of ACM CCS.*

[9] B. Cao, J. Zhao, Z. Lv, X. Liu, X. Kang & S. Yang. (2018). Deployment optimization for 3D industrial wireless sensor networks based on particle swarm optimizers with distributed parallelism, *Journal of Network and Computer Applications, 103,* 225-238,

[10] H. Chan, A. Perrig & D. Song. (2003). Random key predistribution schemes for sensor networks, *In Proc. of IEEE S&P.*

[11] L. Eschenauer & V. Gligor. (2002). A key-management scheme for distributed sensor networks, *In Proc. of ACM CCS.*

[12] T. Kwon, J. Lee & J. Song. (2009). Location-based pairwise key predistribution for wireless sensor networks, *IEEE Trans. on Wireless Communications, 8(11).*

[13] M. Farsi, M. A. Elhosseini, M. Badawy, H. A. Ali & H. Z. Eldin. (2019). Deployment techniques in wireless sensor networks, coverage and connectivity: a survey, *IEEE Access, 7.*

[14] J. W. Choi, J. H. Bang, L. H. Kim, M. R. Ahn and T. Y. Kwon, "Location-Based Key Management Strong Against Insider Threats in Wireless Sensor Networks," IEEE Systems Journal, Vol. 11, Issue 2, 2017

[15] C. G. Ma, G. Geng, H. Q. Wang and G. Yang. (2009). Location-Aware and Secret Share Based Dynamic Key Management Scheme for Wireless Sensor Networks, Proceedings of the 2009 International Conference on Networks Security, *Wireless Communications and Trusted Computing, 1.*

정 윤 수(Yoon-Su Jeong) [정회원]

· 2000년 2월 : 충북대학교 전자계산학과 이학석사
· 2008년 2월 : 충북대학교 전자계산학과 이학박사
· 2009년 8월 ~ 2012년 2월 : 한남대학교 산업기술연구소 전임연구원
· 2012년 3월 ~ 현재 : 목원대학교 정보통신융합공학부 조교수
· 관심분야 : 유무선통신 보안, 정보보호, 센서 네트워크, IoT, 이동통신, 암호이론,
· E-Mail : bukmunro@mokwon.ac.kr

최 정 희(Jeong-hee Choi) [정회원]

· 1999년 2월 : 서원대학교 상업교육학과 졸업
· 2002년 8월 : 충북대학교 컴퓨터과학과 졸업 이학석사
· 2019년 2월 : 충북대학교 컴퓨터과학과 졸업 공학박사
· 2020년 3월 ~ 현재 : 목원대학교 스톡스 대학 SW교양학부 교수
· 관심분야 : 정보보호, 인증, 클라우드
· E-Mail : jhchoi@mokwon.ac.kr