Journal of KIIT. Vol. 18, No. 9, pp. 75-88, Sep. 30, 2020, pISSN 1598-8619, eISSN 2093-7571
http://dx.doi.org/10.14801/jkiit.2020.18.9.75

가중치 기반의 더미 난독화 방식을 이용한 위치정보 프라이버시 보호기법 연구

이동혁*, 박남제**

A Study on the Privacy Protection Method of Location Information using Weight-based Dummy Obfuscation Method

Donghyeok Lee*, Namje Park**

2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2019S1A5C2A04083374).

요 약

최근 위치기반서비스(LBS)의 사용이 증가되면서 위치정보에 대한 프라이버시 보호 문제가 중요한 이슈로 부상하고 있다. 위치정보의 수집은 객체의 프라이버시 문제와 직결될 수 있으며, LBS 서버에서 사용자의 위치정보에 대한 분석을 수행함으로써 다양한 개인정보를 추측할 수 있다. 특히, LBS 서버는 비즈니스상의 목적으로 개인정보를 제3자에게 공개할 수 있다는 위험성이 존재한다. 기존 위치정보보호를 위한 난독화, 더미방식 등 다양한 기법이 제안된 바 있다. 그러나 기존 방법은 데이터 분석에 취약하며 정밀도가 낮다는 단점이 있다. 본 논문에서는 더미 난독화 기반의 위치정보보호 기법을 제안하였다. 제안한 방법은 위치정보를 노출하지 않는 더미 영역을 생성하여 기존 난독화 방식에 비해 안전성을 가진다. 또한, 가중치를 고려하여 위치영역을 설정하고 민감도에 따라 정보공개 수준을 다르게 하여 사용자의 선호도를 고려한 프라이버시 보호가 가능하다.

Abstract

Recently, as the use of location-based services has increased, the issue of privacy protection for location information has emerged as an important issue. However, the collection of location information is directly related to the privacy problem of the object. Therefore, in this paper, a method for protecting location information based on dummy obfuscation was proposed. The proposed method has the advantage that it has safety compared to the existing obfuscation method by creating a dummy area that does not expose location information. In addition, since the location area is set in consideration of the weight, it is possible to protect the privacy according to the user's preference by varying the level of information disclosure according to the sensitivity.

Keywords

dummy data, obfuscation, LBS security, location privacy, privacy protection

* 제주대학교 과학기술사회연구센터, 사이버보안인재교육원 학술연구교수
- ORCID: https://orcid.org/0000-0001-7516-469X
** 제주대학교 초등컴퓨터교육전공, 대학원 융합정보보안학과 교수(교신저자)
- ORCID https://orcid.org/0000-0003-4434-8933

· Received: Jun. 18, 2020, Revised: Aug. 21, 2020, Accepted: Aug. 24, 2020
· Corresponding Author: Namje Park
Dept. of Computer Education, Teachers College, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Tel.: +82-64-754-4914, Email: namjepark@jejunu.ac.kr

Ⅰ. 서 론

최근 무선 네트워크 기술과 스마트폰 사용의 일상화에 따라 위치기반서비스(LBS, Location Based Service)가 매우 일상적으로 사용되고 있다. LBS 환경에서는 사용자가 유용하게 활용할 수 있는 다양한 서비스를 제공할 수 있다. LBS는 모바일 환경에서 강점을 가지는 주요한 서비스 중 하나이며, 5G 환경이 도래함에 따라 LBS는 향후에도 지속적으로 확대될 것으로 보인다.

그러나 LBS 서비스가 편리함과 편의성을 가져다주는 만큼, 민감한 데이터 노출 문제가 많은 사람들의 큰 우려를 낳고 있다. 사용자의 위치정보는 서로 다른 위치서비스 제공업체 간에 공유되므로 신뢰할 수 없는 제 3자가 해당 위치정보를 마케팅 등 허가받지 않은 목적이나 부적절한 방법으로 취득할 가능성도 존재한다. 만약 최근 사용자의 위치 추적정보를 분석한다면, 사용자의 집 주소, 직장, 건강 상태 등에 대한 분석이 가능할 수 있어 사용자의 위치정보 제공 시 반드시 보안을 고려하여야 한다. 이러한 문제를 해결하기 위하여 기존에 난독화, 더미 데이터, 암호화 방식과 같은 다양한 기법이 연구되었다. 그러나 기 제안된 방식은 데이터 분석에 취약하다는 단점이 있다. 예를 들어, 위치정보에 대한 난독화를 수행한다고 하더라도 일정 범위 이내의 장소에 한정될 수 밖에 없으며, 더미 데이터 방식을 적용한다면 SNS를 통하여 단 한번의 위치정보만 공개되더라도 데이터 경로 추적이 용이하게 된다. 위치정보의 원활한 제공과 프라이버시 보호는 동시에 달성하기 쉽지 않은 부분이 있으며, 지금까지의 연구로서는 LBS 시스템의 가용성과 프라이버시 보호 문제를 완전히 해결할 수 없어 이에 대한 지속적인 연구가 필요한 상황이다. 따라서 본 논문에서는 안전한 위치정보 제공을 위한 가중치를 갖는 더미 난독화 방식을 제안하였다. 제안한 방식은 위치정보를 노출하지 않는 더미 영역을 생성하여 기존의 방식에 비해 안전성을 갖는다.

Ⅱ. 관련 연구

2.1 위치정보와 프라이버시

2.1.1 위치정보 및 LBS

위치정보는 유무선 통신망 등 다양한 방식으로 수집될 수 있으며, 위치정보는 개인정보의 하위개념으로 볼 수 있다. LBS는 위치정보를 이용하거나 활용하여 제공되는 서비스를 의미한다[1]. 위치기반서비스를 위한 시스템 구성요소는 일반적으로 그림 1과 같다.

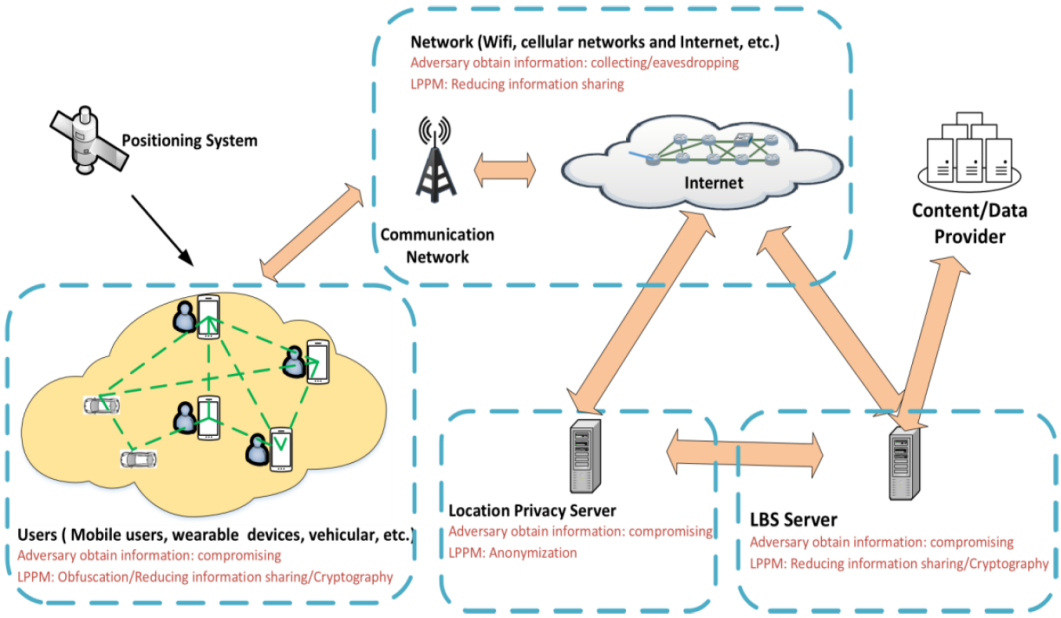


그림 1. 위치기반서비스 시스템 모델
Fig. 1. Location-based service system model

- 포지셔닝 시스템 : GPS 위성은 가장 널리 사용되는 포지셔닝 시스템이다. 그 외에 셀룰러, WiFi 등을 이용할 수도 있다.
- 사용자 : 일반적으로 대부분의 LBS 시스템은 모바일 환경에서 사용되는 경우가 많다. 그 이외에도 차량, 웨어러블 장치 등에서 사용될 수 있다.
- 네트워크 : 통신 네트워크, 무선 로컬 네트워크 및 셀룰러 네트워크 등 다양한 방식으로 데이터 전송이 가능하며 인터넷을 통해 전송된다.
- LBS 서버 : LBS 서버는 위치정보를 획득/처리하는 서버이다. 실시간 LBS 서비스를 위해 객체의 위치 추적이 필요하여 대용량의 DB가 필요하다.
- 위치정보보호서버 : 위치정보보호서버는 개인정보보호 알고리즘을 통하여 위치정보를 보호한다.

2.1.2 위치정보 프라이버시

위치정보를 활용한 LBS 시스템은 서비스를 제공하기 위한 다양한 위치정보 수집이 필요하기 때문에 개인 위치정보 노출의 위험성이 매우 크다. 위치정보 프라이버시는 정상적인 상황에서 객체의 위치가 체계적이고 안전하게 관리되며, 제3자 등에 의해 향후 다른 목적으로 사용되지 않을 것을 보장하는 것이다. 위치정보 프라이버시는 반드시 지켜져야 하나, 실질적으로 휴대폰, RFID, 카메라 등과 같은 장치에서 사용자가 인지하지 않는 상황에서 위치정보가 수집될 수 있다. 또한, 딥러닝을 통한 얼굴 인식 등을 통하여 사용자의 위치정보 노출이 가능하다.

위치정보를 제공할 경우 다음과 같은 사항이 필수적으로 고려될 필요가 있다. 먼저, 정보의 공개 방법을 고려하여야 한다. 여기에는 위치정보 자체가 얼마나 공개되는지, 예를 들어 허가된 사람에게만 공개할지, 혹은 전체 사용자에게 공개할지에 대한 여부가 고려되어야 하며, 해당 위치정보가 암호화 및 난독화된 상태로 저장되는지, 정보가 제3자에게 제공되어 다른 목적으로 사용될수 있는지에 대한 여부를 고려하여야 한다. 그리고 어떤 종류의 정보가 공개되는지 여부에 대한 고려가 필요하다. 특히, 특정 시간, 신원정보와 연결되는 위치정보를 공개할 것인지, 혹은 위치 자체만 공개할 것인지에 대한 여부, 그리고 공개되는 위치정보가 정밀도가 높은 데이터인지 혹은 보안을 위해 어느정도 가공된 정보인지에 대한 고려가 필요하다. 공개되는 위치정보의 정확도가 높을수록 프라이버시 침해 위협은 높아질 것이며, 여기에 신원 정보와 시간정보 등을 매핑하여 제공한다면 위치 데이터를 통한 다양한 분석이 가능하여 개인정보 노출의 위험성이 더욱 더 커지게 될 것이다.

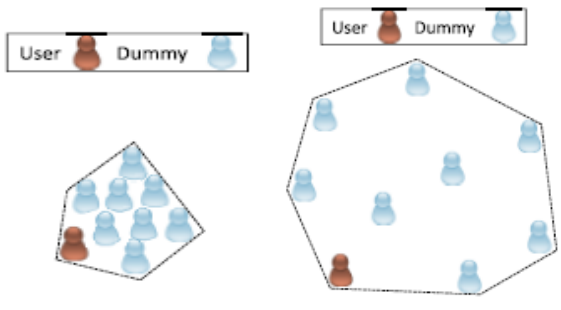
2.2 기존의 위치정보보호기법(LPPM) 연구

현재 개인정보 유출을 방지하기 위해 암호화, 난독화, 더미 데이터 생성 등 다양한 방식의 연구가 수행된 바 있다. 본 절에서는 이러한 기존의 LPPM의 연구에 대해 살펴본다.

2.2.1 더미 데이터 생성 기술

더미 데이터는 위치정보를 보호하는데 사용되는 효과적인 방법 중 하나이다. 더미기반의 위치정보보호 방식은 실제 위치정보 이외의 더미 위치정보를 생성하는 방법이며, 실제 위치정보 및 더미 위치정보의 모든 위치는 LBS 서버에 제공된다[2]. 이 경우, LBS 서버는 사용자의 위치를 실제로 구별할 수 없게 되어 개인정보를 보호할 수 있다[3][4].

그림 2는 더미 데이터의 생성을 나타낸다. (a)의 경우 더미 데이터가 군집 형태를 이루고 있어 보다 낮은 익명성을 제공하며, (b)의 경우는 보다 높은 익명성이 제공된다. 즉, 익명성 수준을 낮게 할수록 실제 위치정보가 더 많이 노출된다[5]-[8].



(a) (b)

그림 2. 더미 데이터의 익명성 영역[9]
Fig. 2. Anonymous area of dummy data

그러나 더미 데이터 방식은 빈도 분석에 취약할 수 있다. 예를 들어 사용자가 자신의 집에서 주기적으로 요청을 수행할 경우, 사용자의 집 주변에 더 많은 더미 데이터가 발생하게 되며, 데이터 분석을 통하여 사용자의 실제 위치는 더미 데이터가 빈번하게 발생하는 지역에 있다는 것을 추정할 수 있다. 따라서 기존의 더미 기반 기법은 사용자의 위치정보를 완전하게 보호하는데 한계점이 있다[10][11].

2.2.2 암호화 기반 기술

암호화 기반 기술은 암호화를 사용하여 위치정보를 보호하는 방식이다. 이러한 방법은 현재 사용자의 위치를 노출하지 않고 LBS 서버에 저장할 수 있다는 장점이 있다. 그러나, 암호화된 데이터로 저장하는 방식은 질의 과정에서 복호화가 필요하므로 효율성 측면에서 저하를 가져올 수 있다[12]-[14]. 지금까지의 암호화 기반 기술은 주로 데이터에 대한 보안 질의에 대한 연구가 진행되어 왔으나, 암호화된 데이터는 통계적 질의가 어렵게 되므로 근본적으로 위치정보 처리에 한계점을 가지고 있다.

2.2.3 위치 난독화 기술

위치 난독화 기술은 위치정보의 정밀도를 의도적으로 줄이는 방법을 통하여 위치정보를 보호하는 방식이다. 즉, 사용자의 위치정보는 정확한 위치 좌표 대신 특정 영역 자체를 전송하게 되어 실제 위치정보가 아닌 범위 정보를 갖는 데이터가 전달되어 처리된다[15]-[20]. 또한 위치값에 대한 좌표변환을 통하여 위치데이터를 변화시키는 방법이 연구된 바 있다 그림 3은 Andreas 등이 제안한 좌표변환을 나타낸다[21].

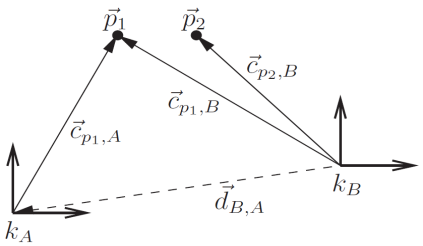


그림 3. Andreas의 난독화 기법
Fig. 3. Anonymous area of dummy data

좌표변환은 한 좌표계에 있는 좌표를 다른 좌표계에 있는 좌표로 변환하는 것을 의미한다. $C_{p1,A}$는 좌표계 k_A에서 점 p_1의 좌표를 나타내고 $C_{p2,B}$는 좌표계 k_B에서 점 p_2의 좌표를 나타낸다. 이와 같이 좌표변환을 이용해 p_1과 p_2 사이의 거리를 알아낼 수 없도록 하여 위치추적이 어렵도록 한다.

2.2.4 기존 기술의 한계점 분석

위치정보를 안전하게 제공하기 위한 기존 연구에 대해 2장에서 살펴보았다. 실질적으로 위치정보보호에 대한 효율성 및 정확성 모두를 완전히 만족시키는 것은 대단히 어렵다고 볼 수 있다[22]-[26].

더미 데이터 방식은 위치정보가 노출됨에 따라, 특정한 시점의 위치만 노출되더라도 위치추적 분석이 용이해질 수 있다는 문제가 있다. 그림 4에서는 더미 데이터 방식에서의 특정 두 시점을 나타낸다.

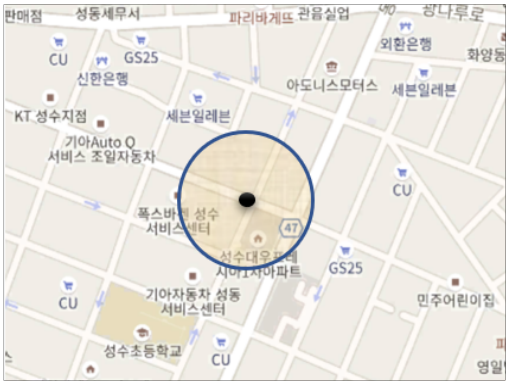
만약 악의를 가진 공격자가 두 시점을 모두 획득할 경우, 실질적으로 인접한 더미 영역을 통하여 각 더미의 연관관계를 생성할 수 있다.

그림 4. 더미 데이터의 위치 이동
Fig. 4. Change the location of dummy data

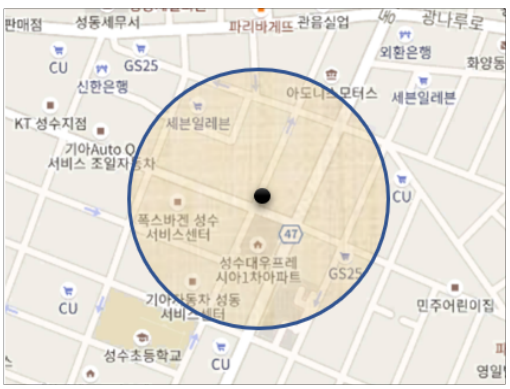
이 경우, 단 한번의 위치정보만 노출되어도 해당 위치정보의 추적을 통해 다른 더미와 위치추적 정보를 분석할 수 있다. 최근 SNS를 통해 특정 시점에 대한 위치정보가 노출되는 경우가 많으며 용이하게 정보 수집이 가능하다. 공격자가 이러한 위치정보를 파악하게 된다면 역분석에 더욱 취약하다고 볼 수 있다[27][28].

위치 난독화 기술은 프라이버시 보호성을 높일수록 실제 위치의 정보와 많은 차이가 나게 되어 원활한 서비스 제공에 지장을 받을 수 있다. 그리고 원활한 정보 제공을 위해 난독화 수준을 낮추게 된다면 반대로 프라이버시 노출 확률이 더 커지게 될 것이다[29].

그림 5는 위치 난독화 기술을 나타낸다. 여기에서 (a)의 경우는 난독화 수준을 낮춘 경우를 나타내며, (b)의 경우는 난독화 수준을 높인 경우를 나타낸다. 만약 난독화 수준을 높인다면 원본 위치추정의 난이성으로 원활한 LBS 서비스 제공이 어려울 수 있다는 한계점이 존재한다.



(a)



(b)

그림 5. 위치정보의 난독화
Fig. 5. Obfuscation of location information

반면, 원활한 서비스 제공을 위해 (a)와 같이 난독화 수준을 낮춘다면 사용자가 일정 범위 이내에 있다는 유추가 가능하게 되어 실질적으로 프라이버시 보호 효과를 크게 얻을 수 없다. 그리고 난독화 기술을 적용한다 하더라도 다른 시점의 난독화된 위치를 모두 수집할 경우 사용자의 위치 경로가 노출될 가능성이 있다[30]-[38].

그림 6은 난독화된 데이터의 특정 세 시점을 획득한 결과를 나타낸다. 비록 위치정보 데이터의 난독화가 수행되었으나, 큰 궤적은 분석을 통해 알 수 있으며, 사용자의 라이프 특성 등을 인지하고 있는 공격자라면 대략적인 사용자의 이동현황, 어디를 방문했는지에 대한 유추가 가능하게 되어 역분석의 위험이 있다[39]-[41].

그림 6. 난독화된 데이터의 위치 이동
Fig. 6. Movement of obfuscated location data

III. 새로운 위치정보보호 기법 제안

본 장에서는 위치정보의 안전한 제공을 위한 고려사항을 살펴보고, 더미 난독화 기반의 안전한 위치정보 처리기법을 제안한다.

3.1 위치정보의 안전한 제공을 위한 고려사항

안전한 LBS 서비스 제공을 위해 위치정보 자체의 특성을 고려할 필요가 있다. 위치정보서비스의 제공을 위해 다음과 같은 고려사항이 필요하다.

3.1.1 대규모 데이터 취급

위치정보시스템의 저장 및 처리를 위해서는 대용량의 위치정보를 취급해야 한다. 특히, 위치추적 서

비스 등의 제공을 위해서는 특정 한 시점의 위치정보 뿐만 아니라 실시간의 정보를 수집하여야 하므로 매일 엄청난 양의 위치정보 데이터가 생성된다.

3.1.2 위치정보 간의 연관성

특정 위치정보는 경우에 따라 높은 연관성을 가지는 경우가 많다. 예를 들어, 신원 A의 사용자와 B의 사용자가 사회적으로 높은 연관성을 가질 경우 위치정보 또한 이러한 높은 연관관계를 맺을 확률이 크다. LBS 서버에 악의를 가진 자가 접근을 하여 특정 위치정보에 대한 연관성을 분석한다면 의도치 않게 많은 정보가 노출될 수 있다.

3.1.3 장소에 따른 민감도 차이

위치정보의 민감도 수준은 장소에 따라 다를 수 있다. 예를 들어, 특정 개인이 극장을 가는 등의 일상적인 행적에 대한 일시적인 위치 자체는 크게 중요하지 않을 수도 있으나, 집 또는 직장에 대한 위치정보는 매우 높은 중요성을 가진 정보로 생각될 수 있어 장소에 따른 민감도가 고려되어야 한다.

3.2 제안 방식 개요

3.2.1 위치정보의 표현방법

LBS의 위치정보는 특정 좌표 뿐만 아니라 다른 데이터의 연결이 필요하다. 특히, 사용자의 신원, 위치, 시간이라는 세가지 정보가 포함되어야 한다. 그림 7은 위치정보의 세가지 속성을 나타내고 있다.

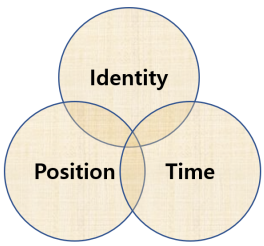


그림 7. 위치정보의 세가지 속성
Fig. 7. Properties of location information

- Identity(신원) : 사용자의 이름, 이메일 주소 또는 다른 사람과 구별될 수 있는 어떤 식별자가 될 수 있다. LBS 시스템에서는 경우에 따라 일관된 사용자 신원을 사용할 수도 있고, 일관되지 않은 신원정보를 사용할 수도 있다. 예를 들어, '친구 찾기'와 같은 기능을 사용하는 경우 일관된 신원정보가 필요하며, 지도 어플리케이션을 통하여 익명으로 근처 맛집을 찾는 경우는 별도의 일관된 신원 정보는 필요하지 않다.
- Position(공간) : 공간 정보는 위치를 연결하는 기본 수단이다. 위치는 좌표 집합으로 표현되거나 상점 이름과 같이 위치를 설명하는 정보로 표현할 수 있다. 위치정보는 절대적인 위치정보 또는 상대적인 위치정보로 표현할 수 있다. 절대적인 위치정보는 GPS 좌표와 같은 직접적인 절대좌표로 표현할 수 있으며, 상대적인 위치정보는 물리적 근접성에 기반하여 표현될 수 있다. 예를 들어 정확한 위치로 표현하는 대신 반경 몇킬로 이내의 정보를 제공할 경우에 사용될 수 있다.
- Time(시간) : LBS 시스템은 위치정보 이외에도 타임스탬프 등으로 시간정보를 위치와 연결하는 경우가 많다. 예를 들어 실시간 위치 추적 정보와 같은 서비스 제공에는 시간 정보가 필수적으로 요구된다. 이러한 경우 난독화 등으로 반경이 넓게 위치정보를 임의로 조절한다면 원활한 위치추적이 어렵게 될 수 있다.

3.2.2 더미 난독화 방식

본 논문에서 제안하는 더미 난독화 방식을 설명하면 다음과 같다. 더미 난독화 방식은 기존의 난독화 방식과 더미 데이터 방식을 보완할 수 있는 새로운 방식으로, 가중치를 기반으로 더미를 난독화하여 각각 다른 크기의 영역으로 처리하는 기법이다.

더미 난독화 방식은 그림 8에 나타나 있다. (a)는 일반적인 더미 데이터 방식을 의미하며, (b)는 본 논문에서 제안하는 더미 난독화 방식을 나타낸다.

더미 난독화 방식은 다음과 같은 특성을 갖는다.

- 난독화된 더미 : 더미 데이터는 정확한 값을 갖지 않으며, 난독화된 상태로 제공된다. 기존의 더미 방식에서는 원본데이터에 한하여 정확한 값을 가지고 있으나 제안하는 방식은 원본 데이터도 난독화처리를 수행하여 영역 정보 형태로 제공한다.

(a) (b)

그림 8. 더미 난독화 방식
Fig. 8. Dummy obfuscation method

- 가중치의 반영: 각 더미의 난독화는 일률적으로 처리되는 것이 아니라, 각 위치에 따른 가중치를 부여하여 서로 다른 난독화 수준을 갖게 한다.

3.3 세부사항

본 절에서는 더미 난독화 방식의 세부 내용을 설명한다.

3.3.1 표기법

본 논문에서 제안한 방식을 설명하기 위해 필요한 약어는 표 1에 나타나 있다.

표 1. 약어
Table 1. Notation

Abbreviation	Description
ID_D	Dummy ID
PK	Pre-shared key
TS	Timestamp
D_CNT	Dummy generation value
$HMAC(\cdot)_K$	Result of HMAC with key K

3.3.2 더미 개수 및 더미 아이디 결정

특정 단일 데이터만 저장할 경우 개인 위치정보의 식별 가능성이 있으므로, 데이터 저장 시에 일정 수준 이상의 더미를 생성한다. 여기에서, 먼저 더미의 개수를 결정할 필요가 있으며, 더미의 개수는 관리자에 의해 적정한 수치로 조절될 수 있다. 그리고 주요하게 고려할 사항은 더미의 개수가 증가할수록 안전성은 높아진다고 볼 수 있으나, 더미 개수에 비례하여 대용량 데이터가 축적됨에 따라 효율성이 저하될 수 있다. 따라서 가용성을 해치지 않은 선에서 더미 데이터의 적절한 수치 조절이 필요하다. 본 논문에서는 설명을 위해 위치정보 입력 시 원본 데이터와 4개의 더미 데이터를 가진 총 5개의 데이터를 입력하는 것으로 한다.

우선, 더미 아이디인 ID_D는 다음과 같은 식으로 생성할 수 있다.

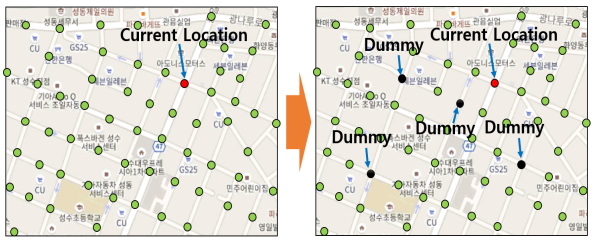
$$ID_D = HMAC(TS \| D\_CNT)_{PK} \quad (1)$$

이렇게 생성하는 경우, D_CNT 값을 활용하여 더미 데이터인지 실제 값인지에 대한 여부를 판단할 수 있다. 즉, D_CNT 값이 최초값의 특정 배수에 해당할 경우 실제 위치라는 의미이고, 그렇지 않을 경우 더미 데이터로 판단할 수 있다. 따라서, ID_D값을 통해 더미 데이터의 필터링이 가능하다. 여기에서, PK를 알고 있는 경우에만 ID_D로부터 의미있는 값을 도출할 수 있으며, 그렇지 않을 경우는 단순 HMAC의 결과값이므로 해당 ID_D 값으로부터 의미있는 결과를 도출해 낼 수 없다.

3.3.3 더미 위치의 결정을 위한 고려사항

그림 9는 더미 위치의 결정 과정을 나타낸다. 우선, (a)와 같이 특정 간격으로 더미 후보지가 사전에 선정되어 있으며, (b)에서는 사용자의 현재 위치와 현재 위치를 중심으로 선정된 더미 데이터를 나

타낸다. 더미 후보지의 선정을 위해 사용자의 방문 빈도 등 다양한 고려사항이 필요하다. 여기서는 더미 위치의 결정을 위한 고려사항을 살펴본다.



(a) (b)

그림 9. 더미 위치 선정
Fig. 9. Selection of dummy position

(1) 방문 이력에 따른 고려

만약 더미의 위치가 사용자가 위치할 수 없는 특정한 지역에 존재하는 경우, 분석을 통하여 해당 사용자의 실제 위치가 아님을 유추할 수 있으므로 해당 더미 데이터 자체는 보안상 의미가 사라질 수 있기 때문이다. 즉, 더미 후보지는 도로망 내에 위치하거나, 최소의 방문회수 이력이 있는 장소를 중심으로 선정하는 것이 바람직하다.

(2) 더미 후보지 속성에 따른 고려

더미 후보 데이터는 크게 다음과 같은 4가지의 속성으로 구분할 수 있다.

① A1 : 다른 사용자의 방문이 많으며, 현재 사용자의 방문 또한 잦은 장소 (예:도서관)
② A2 : 다른 사용자의 방문은 많으나, 현재 사용자의 방문은 드문 장소 (예:화장품가게)
③ A3 : 다른 사용자의 방문이 없으나, 현재 사용자의 방문은 뚜렷하게 많은 장소 (예:집)
④ A4 : 다른 사용자의 방문 및 현재 사용자의 방문 모두 거의 없는 장소 (예:쓰레기매립장)

만약 전체 데이터에 대한 분석을 수행 가능한 공격자가 있다면 이와 같은 특성을 구분하여 더미 데이터가 실제로 사용자의 위치일 가능성에 대해 추정할 수 있다. 만약, 위에서 언급된 A4 지역에 해당하는 장소에 더미 데이터가 지정된 경우, 분석을 수행하는 공격자는 해당 위치정보가 더미 데이터일 확률이 높을 것이라고 가정할 수 있을 것이다. 한편, 사용자의 라이프스타일이나 선호도를 어느 정도로 분석하여 인지할 수 있는 공격자의 경우 A3의 경우에도 마찬가지로 사용자가 있을 확률이 낮을 것이라고 판단이 가능하다. 따라서, 더미 위치 선정 시 더미 후보지를 A1 및 A2에 해당하는 후보지를 우선적으로 선정하는 것이 바람직하다.

(3) 인접도에 대한 고려

공격자는 사용자가 더미 데이터를 포함한 전체 반경 이내에 사용자가 존재함을 확신할 수 있다. 특히 더미 데이터가 현재 위치와 인접할 경우, 공격자에 의한 사용자의 위치정보 추정이 더욱 용이해진다. 따라서 차후 분석을 어렵게 하기 위해서는 더미 데이터 전체적으로 충분한 거리를 두어 인접하지 않도록 선정하는 것이 역분석 방지에 효과적이다.

(4) 시간에 대한 고려

더미 데이터 구성 시 반드시 시간적인 부분을 고려하여야 한다. 예를 들어 새벽시간에 레스토랑에 위치하는 경우, 해당 데이터는 더미 데이터일 것이라고 예상하고 필터링이 가능하다. 또한, 사용자의 라이프 패턴과 전혀 다른 시간대에 위치할 경우에도 마찬가지로 더미 데이터라고 추정할 수 있다. 따라서 시간 정보는 더미후보지를 결정하는데 주요하게 고려해야 하는 요소로서 사용자의 라이프 패턴 및 해당 위치의 영업 여부를 고려하여 더미 위치를 결정하여야 한다. 그림 10에 나타난 것과 같이 더미 위치 선정을 위해 방문이력, 속성, 인접도, 시간의 네가지 요소를 사전에 고려할 필요가 있다.

그림 10. 더미 위치 선정 시 고려사항
Fig. 10. Considerations for selecting a dummy location

3.3.4 가중치의 결정

난독화의 수준을 조절함을 통해 분석을 어렵게 하기 위해 가중치의 결정이 필요하다. 여기에서는 장소를 기반으로 각 더미의 위치에 따른 가중치를 선정한다. 가중치를 결정할 때 주요하게 고려해야

할 사항으로 사용자의 민감도와 사용자 방문 빈도가 있다. 먼저, 가중치를 결정할때 사용자가 해당 방문지에 대하여 얼마나 민감하게 느끼는지 여부를 가장 우선적으로 생각하여야 한다. 서비스 제공자의 관점에서 정보 노출의 중요성을 낮게 생각하는 위치라고 할지라도, 사용자 입장에서는 민감하게 받아들일 수 있다. 따라서 이러한 민감도는 사용자 입장에서 설정되어야 하므로 서비스 제공자 차원에서 일괄적으로 설정하는 것이 아니라, 사용자가 직접 설정할 수 있도록 할 필요가 있다.

또한, 사용자 방문 빈도도 중요한 요소로 고려되어야 한다. 여기서 사용자 방문 빈도란 전체 인구 측면에서의 방문 빈도가 아닌, 사용자 개인이 방문한 빈도를 의미한다. 더미 데이터 가운데 사용자 방문 빈도가 높은 지역일수록 실제 사용자 위치가 맞을 확률이 더 클 수 있다. 따라서, 사용자 방문 빈도가 높다면 해당 영역에 대해 난독화 수준을 높일 필요가 있다. 가중치는 이러한 사용자의 민감도와 사용자 방문 빈도 두가지 요소를 반영하며, 가중치는 아래와 같은 식으로 계산할 수 있다.

$$weight = sensitivity \times frequency \quad (2)$$

표 2는 가중치를 결정한 예를 나타낸다. 여기에서 가중치가 사용자가 사전에 설정한 민감도와 방문 빈도에 따라 결정된 것을 나타내고 있다. 사용자는 각 위치별로 사전에 민감도를 설정하며, 본 예에서는 사용자가 집, 직장, 도서관, 영화관, 식당을 각각 5,4,2,1,3의 민감도로 설정한 경우를 나타낸다.

표 2. 가중치의 결정
Table 2. Decision of weight

Location	Sensitivity	Frequency	Weight
Home	5	35	175
Workplace	4	30	120
Library	2	20	40
Theater	1	5	5
Restaurant	3	10	30

표 3은 민감도 수준 정책을 나타낸다. 여기에서 민감도가 5인 경우는 매우 민감한 지역임을 나타내며, 4인 경우는 사용자가 일정 수준의 민감도를 느낄 수 있는 지역이다. 3인 경우는 낮은 수준의 정보 노출이 발생할 수 있으며, 2의 경우는 일반적으로 사람들이 많이 방문하는 것으로, 정보 노출의 위험성이 많지 않은 곳을 의미한다. 1의 경우는 사용자가 정보 공개에 개의치 않는 안전한 지역으로 설정된다.

여기에서, 민감도 수준은 사용자가 직접 설정하는 영역이다. 민감도 수준은 서비스 제공자 차원에서 일괄적으로 처리되어서는 안되며, 개별 사용자에 따라 장소의 민감도가 다르게 설정되어야 한다. 동일한 장소라고 할지라도 각각의 사용자가 느끼는 민감도는 다를 수 있으며, 사용자의 상황에 따라 공개 노출을 꺼리는 지역이 있을 수 있기 때문이다. 따라서 서비스 제공자는 표 3의 민감도 수준 정책에 따라 사용자가 직접 민감도를 조절할 수 있는 방안(웹페이지, 모바일 등)을 마련하여야 한다.

표 3. 민감도 수준
Table 3. Sensitivity level

Sensitivity	Description
5	Very sensitive place
4	A rather sensitive place
3	Slight privacy exposure
2	A place many people visit
1	No risk of information disclosure

3.3.5 가중치를 적용한 더미 생성

더미 데이터에 대한 가중치를 결정한 이후에는 최종적으로 가중치를 적용한 더미영역을 생성할 수 있다. 그림 11은 최종 생성된 더미 영역을 나타낸다. 여기에는 각 더미의 영역 정보만 나타나 있으며 정확한 값은 나타나 있지 않다. 즉, 실제 위치 혹은 생성한 더미 위치는 해당 영역 내에 존재하고 있으며, 정확하게 어디에 있는지는 알 수 없다.

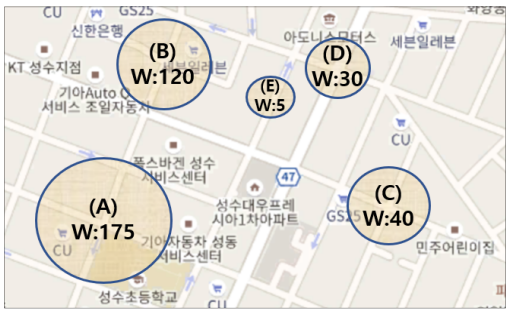


그림 11. 최종 생성된 더미 영역
Fig. 11. Finally generated dummy area

또한, 위치의 민감도, 방문빈도를 통한 가중치 결정에 따라 각각의 영역의 크기는 달라지며, 프라이버시 노출 위험이 높을수록 영역의 크기가 커지게 되므로 정보 노출의 위험이 적어지며, 공개되어도 안전한 장소라면 보다 세밀한 영역이 설정되어 정보 공개율을 높이는 방식으로 프라이버시를 보호할 수 있다.

표 2에서 나타난 예시에 대응하여, 그림 11에서는 A:Home, B:Workplace, C:Library, D:Theater, E:Restaurant를 각각 나타낸다. 각각의 더미후보지 가중치에 따라, A는 175, B는 120, C는 40, D는 30, E는 5로 각각 설정되었다. 이 가중치는 난독화 범위를 나타내는 원의 반지름에 비례하며, 가중치가 클수록 난독화 범주가 넓어지게 되므로 더욱 원본에 대한 추정이 어렵게 된다.

여기에서, 가중치의 증가에 따라 난독화 범위가 넓어지더라도 실제 저장되는 값은 범위 내의 특정한 좌표이며, 범위 정보 자체를 저장하지는 않는다. 만약 범위 정보를 저장하게 될 경우 넓은 범위를 가진 더미일수록 민감한 지역에 속할 수 있다는 역분석을 수행할 수 있다. 따라서 더미를 범위데이터 자체로 취급하여 데이터베이스상에 저장하는 것은 바람직하지 않다. 즉, 범위 내의 특정 좌표를 랜덤하게 특정하여 해당 특정 좌표만 저장해야 하며, 이러한 경우 공격자는 범위 정보를 확인할 수 없다.

Ⅵ. 제안기법 분석결과

4.1 난독화 방식

난독화 방식은 특정 범주 영역을 제공한다. 이러한 경우, 적어도 특정 범주 내에 실제 위치가 존재한다는 부분은 확신할 수 있다. 그러나 제안한 방식은 난독화 방식에 비해 다수의 영역 정보를 제공하여 실제 사용자가 위치한 영역이 어디인지를 분석을 통해서는 구체적으로 확신할 수 없다. 그러나 제안한 방식은 실제 위치에 대한 정밀도를 난독화 방식에 비하여 더 높게 설정할 수 있다.

제안한 방식은 더미 데이터를 기반으로 다수의 영역을 동시에 제공함으로써 기본적으로 난독화 방식에 비해 역분석이 어렵다. 보다 높은 정밀도를 제공할 수 있음에 따라 효율성 측면에서도 제안한 방식이 더욱 높다고 할 수 있으며, 더미 아이디인 ID_D의 D_CNT와 PK값을 이용하여 데이터가 더미인지 아니면 실제 데이터인지 PK를 사전에 알고 있는 사람은 판단이 가능하다. 즉, 인가된 자는 더미 데이터의 필터링이 가능하여 원본 데이터를 보다 구체적으로 식별할 수 있다.

그림 12는 기존 난독화 방식과 제안 방식을 비교하고 있다. 제안 방식은 가중치가 반영되며 민감도가 높은 위치에 대해서는 사용자가 직접 난독화 레벨을 조절할 수 있어 기존의 방식보다 능동적인 위치정보보호가 가능하다.

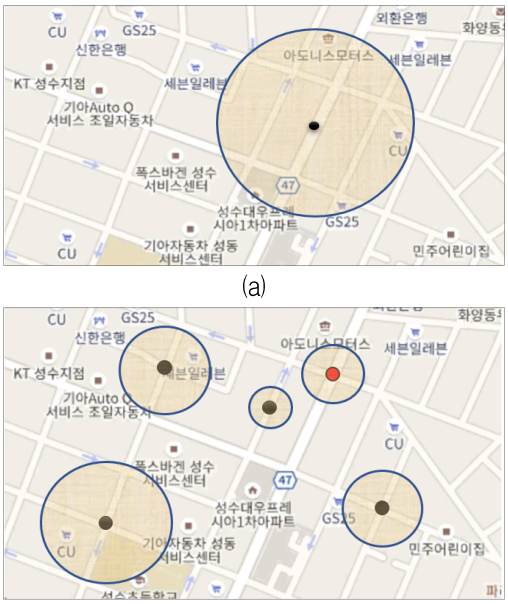


그림 12. 기존 난독화 방식과 제안 방식 비교
Fig. 12. Obfuscation and the proposed method

4.2 더미 기반 방식

더미 기반 방식은 최소한 하나의 데이터는 원본에 대한 정확한 위치를 나타낸다. 이러한 특징에 따라 더미 데이터에서의 정확한 위치에 대한 파악이 한번이라도 일어나게 되면 다음 저장된 위치에서 가장 가까운 위치를 찾아낼 수 있어 위치추적 분석도 용이하게 된다. 최근에는 페이스북과 같은 SNS 등에서 특정 시간과 사용자의 위치를 노출하게 되는 경우가 많다. 이러한 경우, 더미 기반 방식으로 데이터를 저장할 경우, 실제 위치에 대한 역분석이 가능하다.

제안한 방식은 원본 그대로를 나타내지 않고 난독화된 범위 영역을 나타낸다. 따라서 특정 시점의 데이터를 인지한다 하더라도 위치 추적이 기존의 더미 방식에 비해 어렵게 되어 더욱 안전하다.

4.3 암호화 기반 방식

기존의 암호화 기반 방식은 위치데이터를 암호화하여 저장하는 방식으로써 효율성 측면에서 문제점이 존재한다. 즉, LBS 서버상에서 영역질의 같은 다양한 질의가 어려우며, 만약 전체 데이터를 가져와서 복호화를 수행한다면 복원 과정에서 데이터 전체에 대한 복호화를 수행해야 하므로 오버헤드가 존재하여 효율성 측면에서 큰 문제가 발생한다. 제안한 방식은 위치정보의 범위적 영역을 가지고 있어 특정 영역 내에 존재하는 위치에 대한 질의가 가능하다. 또한 더미 아이디 기반으로 필터링이 가능하여 더미 데이터 가운데 실제 위치를 구별할 수 있어 암호화 기반 방식에 비해 보다 효과적으로 사용될 수 있다는 장점이 있다.

4.4 기존기법과 제안기법 비교분석

기존의 난독화 방식은 정밀도가 낮다는 한계가 있다. 특히, 난독화 수준을 높이려면 치명적으로 정밀도가 낮아질 수 밖에 없으며, 반대로 정밀도를 높이기 위해서는 난독화 수준을 낮추어야 한다. 이러한 점은 원활한 서비스 제공에 한계점이 될 수 있다. 더미 방식의 경우는 높은 정밀도를 제공할 수 있으나, SNS 등 다양한 경로에서 단 1회의 정보 노출만으로 위치추적정보 분석이 가능해질 수 있다는 단점이 있다.

암호화 방식의 경우, 보안성 측면에서는 안전하나, 서비스 제공을 위한 가용성이 크게 저하될 수 있어 효율적으로 위치정보 서비스를 제공할 수 없다. 제안한 방식은 난독화 방식과 더미 방식의 장점을 모두 가진 가중치 기반의 더미 난독화 방식을 제공하며 사용자가 설정한 민감도에 따라 정보 공개율을 조절할 수 있으며, 이에 따른 가중치가 적용되어 안전하게 위치정보를 보호할 수 있다. 표 4는 기존방식과 제안한 방식을 비교하고 있다.

표 4. 기존 방식과의 비교
Table 4. Comparison with the existing method

Method	Inference attack	Precision	Efficiency	Weight
Obfuscation	△	×	△	×
Dummy	△	○	○	×
Encryption	○	○	×	×
Our Method	○	△	○	○

V. 결 론

LBS 환경은 많은 편의성을 제공해주지만 그에 따른 프라이버시 노출에 대한 위험성을 동시에 가지고 있다. 위치 프라이버시는 개인의 단순 정보 노출 뿐 아니라 물리적 안전의 문제와도 직결될 수 있으므로 매우 중요하게 인식할 필요가 있다.

그러나 난독화, 더미, 암호화 등과 같은 기존의 위치정보보호 기법은 정확성, 효율성 등에 한계점이 존재하였으며, 사용자의 개인 민감 정도를 반영할 수 없다는 단점 또한 존재하였다. 따라서 본 논문에서 더미 난독화 기반의 안전한 위치정보 보호 기법을 제안하였다.

제안한 방법은 기존의 난독화 방식과 더미 데이터 방식에 비해 실제 위치정보에 대한 분석을 어렵게 하므로 보다 높은 안전성을 가지고 있으며, 또한, 더미 아이디를 기반으로 더미 데이터에 대한 필터링이 가능하며 실제 위치에 대한 범위 정보가 제공됨으로써 질의 측면에서 암호화 기반 방식에 비해 효율성을 가진다. 아울러 사용자의 개인 민감정보를 정책적으로 반영할 수 있다는 장점이 있으며, 민감정보와 사용자의 방문빈도를 통한 가중치가 반영되어 기존에 연구되었던 방식에 비해 보다 능동적인 위치 프라이버시 보호가 가능하다.

최근 코로나19가 확산되고, 확진자의 위치정보가 공개되면서 많은 이들이 위치정보 노출에 대한 경각심을 갖고 있다. 위치정보는 매우 안전하게 취급되어야 할 정보이며, 코로나19 사태가 진행되면서 대중에게 더욱 많은 중요성이 인식되고 있어 앞으로 더욱 많은 연구가 진행되어야 할 것으로 보인다.

향후 더미 데이터의 최적 개수 선정에 대한 연구를 진행할 예정이다.

References

[1] B. Liu, W. Zhou, T. Zhu, L. Gao, and Y. Xiang, "Location privacy and its applications: A systematic study", IEEE Access, Vol. 6, pp. 17606-17624, Apr. 2018.

[2] J. Liu, X. Jiang, S. Zhang, H. Wang, and W. Dou, "FADBM: Frequency-Aware Dummy-Based Method in Long-Term Location Privacy Protection", 2019 IEEE 25th International Conference on Parallel and Distributed Systems (ICPADS), IEEE, Tianjin, China, pp. 384-391, Dec. 2019.

[3] Namje Park, Byung-Gyu Kim, and Jinsu Kim, "A Mechanism of Masking Identification Information regarding Moving Objects Recorded on Visual Surveillance Systems by Differentially Implementing Access Permission", Electronics, Vol. 8, No. 7, 735, pp. 1-17, Jun. 2019.

[4] Y. B. Zhang, Q. Y. Zhang, Z. Y. Li, Y. Yan, and M. Y. Zhang, "A k-anonymous location privacy protection method of dummy based on geographical semantics", International Journal of Network Security, Vol. 21, No. 6, pp. 937-946, Nov. 2019.

[5] Namje Park, Hongxin Hu, and Qun Jin, "Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT)", Journal of Distributed Sensor Networks, Vol. 12, No. 1, Article ID 2965438, 3 pages, Jan. 2016.

[6] H. Liu, X. Li, H. Li, J. Ma, and X. Ma, "Spatiotemporal correlation-aware dummy-based privacy protection scheme for location-based services", IEEE INFOCOM 2017-IEEE Conference on Computer Communications, IEEE, Atlanta, USA, pp. 1-9, May 2017.

[7] Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, and Howon Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", Conferences of Asia-Pacific Web Conference, Harbin, China, 741-748, Jan. 2006.

[8] Zheng, Yanliu, Juan Luo, and Tao Zhong. "Service recommendation middleware based on location privacy protection in VANET", IEEE Access, Vol. 8, pp. 12768-12783, Jan. 2020.

[9] S. Hayashida, D. Amagata, T. Hara, and X. Xie, "Dummy generation based on user-movement estimation for location privacy protection", IEEE Access, Vol. 6, pp. 22958-22969, Apr. 2018.

[10] Namje Park and Namhi Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle", Sensors, Vol. 16, No. 1, pp. 1-16, Dec. 2015.

[11] Z. Wu, R. Wang, Q. Li, X. Lian, G. Xu, E. Chen, and X. Liu, "A Location Privacy-Preserving System Based on Query Range Cover-Up or Location-Based Services", IEEE Transactions on Vehicular Technology, Vol. 69, No. 5, pp. 5244-5254, May 2020.

[12] Donghyeok Lee and Namje Park, "Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance", The Journal of Supercomputing, Vol. 73, No. 3, pp. 1103-1118, Mar. 2017.

[13] J. Liu, Z. Xu, X. Xu, and Z. Zou, "Research on User Privacy Protection Algorithm in Location Service", 2020 12th International Conference on Measuring Technology and Mechatronics Automation (ICMTMA), IEEE, Phuket, Thailand, pp. 953-956, Feb. 2020.

[14] Jinsu Kim, Namje Park, Geonwoo Kim, and Seunghun Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia", Electronics, Vol. 8, No. 4, Apr. 2019, https://doi.org/10.3390/electronics8040412.

[15] N. Wang, J. Fu, J. Li, and B. K. Bhargava, "Source-location privacy protection based on anonymity cloud in wireless sensor networks", IEEE Transactions on Information Forensics and Security, Vol. 15, pp. 100-114, May 2019.

[16] Donghyeok Lee, Namje Park, Geonwoo Kim, and Seunghun Jin, "De-identification of metering data

for smart grid personal security in intelligent CCTV-based P2P cloud computing environment", Peer to Peer Networking and Applications, Vol. 11, No. 6, pp. 1299-1308, Nov. 2018.

[17] L. Kuang, Y. Wang, X. Zheng, L. Huang, and Y. Sheng, "Using location semantics to realize personalized road network location privacy protection", EURASIP Journal on Wireless Communications and Networking, Article No. 1, Jan. 2020.

[18] Namje Park and Hyochan Bang, "Mobile middleware platform for secure vessel traffic system in IoT service environment", Security and Communication Networks, Vol. 9, No. 6, pp. 500-512, Apr. 2016.

[19] Guk-Han Jo and Young Joon Song, "State Analysis and Location Tracking Technology through EEG and Position Data Analysis", Journal of JAITC, Vol. 8, No. 2, pp. 27-39, Dec. 2018.

[20] Donghyeok Lee and Namje Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree", Multimedia Tools and Applications, pp. 1-18, Mar. 2020.

[21] Gutscher, Andreas, "Coordinate transformation-a solution for the privacy problem of location based services?", Proceedings 20th IEEE International Parallel & Distributed Processing Symposium, IEEE, Rhodes Island, Greece, 7 pages, Apr. 2006.

[22] Jinu Choi, Sukhoon Lee, and Dongwon Jeong. "Development of Lifelog Collection Interface and Visualization System for User Location Information Analysis", Journal of KIIT, Vol. 17, No. 7, pp. 1-11, Jul. 2019.

[23] N. Park and D. Lee, "Electronic identity information hiding methods using a secret sharing scheme in multimedia-centric internet of things environment", Personal and Ubiquitous Computing, Vol. 22, No. 1, pp. 3-10, Feb. 2018.

[24] Hyesun Jang, Jaehyun Choi, Yangwon Lim, Hankyu Lim, and Daejea Cho, "A Study on the LBS-Based Path Deviation Detection", Journal of KIIT, Vol. 11, No. 3, pp. 183-189, Mar. 2013.

[25] Jinsu Kim and Namje Park, "Lightweight knowledge-based authentication model for intelligent closed circuit television in mobile personal computing", Personal and Ubiquitous Computing, pp. 1-9, Aug. 2019.

[26] Donghyeok Lee and Namje Park, "A Study on Metering Data De-identification Method for Smart Grid Privacy Protection", Journal of KIISC, Vol. 26, No. 6, pp. 1593-1603, Dec. 2016.

[27] Jinsu Kim and Namje Park, "A Face Image Virtualization Mechanism for Privacy Intrusion Prevention in Healthcare Video Surveillance Systems", Symmetry, Vol. 12, No. 6, pp. 891, Jun. 2020.

[28] Namje Park and Marie Kim, "Implementation of load management application system using smart grid privacy policy in energy management service environment", Cluster Computing, Vol. 17, No. 3, pp. 653-664, Sep. 2014.

[29] Jinsu Kim, Jaeyoung Cho, and Namje Park, "Block Chain Based CCTV Image Forgery · Modulation Verification Mechanism", Journal of KIIT, Vol. 17, No. 8, pp. 107-114. Aug. 2019.

[30] Donghyeok Lee and Namje Park, "CCTV Video Privacy Protection Scheme Based on Edge Blockchain", Journal of KIIT, Vol. 17, No. 10, pp. 101-113. Oct. 2019.

[31] Prince Waqas Khan, Yung-Cheol Byun, Sang-Joon Lee, and Namje Park, "Machine Learning Based Hybrid System for Imputation and Efficient Energy Demand Forecasting", Energies, Vol. 13, No. 11, 2681, 23 pages, May 2020.

[32] Jinsu Kim and Namje Park, "Development of a board game-based gamification learning model for training on the principles of artificial intelligence learning in elementary courses", Journal of The Korean Association of Information

Education, Vol. 23, No. 3, pp. 229-235, Jun. 2019.
[33] Prince Waqas Khan, Yung-Cheol Byun, and Namje Park, "A Data Verification System for CCTV Surveillance Cameras Using Blockchain Technology in Smart Cities", Electronics, Vol. 9, No. 3, pp. 484. Mar. 2020.
[34] Jinsu Kim and Namje Park, "Role Based Access Control based File Access Control Mechanism with Smart Contract", Journal of KIIT, Vol. 17, No. 9, pp. 113-121. Sep. 2019.
[35] Mijin Kim, Jongho Moon, Dongho Won, and Namje Park, "Revisit of Password-Authenticated Key Exchange Protocol for Healthcare Support Wireless Communication", Electronics, Vol. 9, No. 5, pp. 733, Apr. 2020.
[36] Jinsu Kim and Namje Park, "Dynamic/Static Object Segmentation and Visual Encryption Mechanism for Storage Space Management of Image Information", Journal of KMS, Vol. 22, No. 10, pp. 1199-1207, Oct. 2019.
[37] Prince Waqas Khan, Yung-Cheol Byun, and Namje Park, "IoT-Blockchain Enabled Optimized Provenance System for Food Industry 4.0 Using Advanced Deep Learning", Sensors, Vol. 20, No. 10, pp. 2990, May 2020.
[38] Donghyeok Lee and Namje Park, "A Study on COP-Transformation Based Metadata Security Scheme for Privacy Protection in Intelligent Video Surveillance", Journal of KIISC, Vol. 28, No. 2, pp. 417-428, Apr. 2018.
[39] Namje Park, Younghoon Sung, Youngsik Jeong, Soo-Bum Shin, and Chul Kim, "The Analysis of the Appropriateness of Information Education Curriculum Standard Model for Elementary School in Korea", International Conference on Computer and Information Science, Springer, pp. 1-15, Jun. 2018.
[40] Jinsu Kim and Namje Park, "BlockChain Technology Core Principle Education of Elementary School Student Using Gamification", Journal of The Korean Association of Information Education, Vol. 23, No. 2, pp. 141-148, Apr. 2019.
[41] Donghyeok Lee and Namje Park, "Technology and Policy Post-Security Management Framework for IoT Electrical Safety Management", The Transactions of The Korean Institute of Electrical Engineers, Vol. 66, No. 12, pp. 1879-1888, Dec. 2017.

저자소개

이 동 혁 (Donghyeok Lee)

2007년 2월 : 동국대학교 전자상거래기술전공 공학석사
2018년 2월 : 제주대학교 컴퓨터교육학과 공학박사
2007년 6월 ~ 2008년 5월 : 한국전자통신연구원 정보보호연구단 연구원
2008년 11월 ~ 2015년 6월 : KT 플랫폼개발단 과장
2018년 3월 ~ 현재 : 제주대학교 과학기술사회연구센터 학술연구교수
관심분야 : 블록체인, 클라우드, 지능형 영상감시 시스템, 5G보안, 데이터 비식별화, 컴퓨터교육 등

박 남 제 (Namje Park)

2008년 2월 : 성균관대학교 컴퓨터공학과 박사
2003년 4월 ~ 2008년 12월 : 한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월 ~ 2009년 12월 : 미국 UCLA대학교 공과대학 Post-Doc, WINMEC 연구센터 Staff Researcher
2010년 1월 ~ 2010년 8월 : 미국 아리조나 주립대학교 컴퓨터공학과 연구원
2010년 9월 ~ 현재 : 제주대학교 초등컴퓨터교육전공, 일반대학원 융합정보보안학과 교수
2011년 9월 ~ 현재 : 교육부 창의교육거점센터장, 과학기술사회(STS)연구센터 부센터장, 정보영재 주임교수, 사이버보안인재교육원장
관심분야 : 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등