Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.30, NO.4, Aug. 2020 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2020.30.4.679

5G 기반 고정밀 측위 빅데이터 활용을 위한 위치정보 프라이버시 보호 기법 제안*

이 동 혁,[1†] 박 남 제[2‡]
[1]제주대학교 과학기술사회연구센터(학술교수), [2]제주대학교 융합정보보안학과(교수)

A Proposal of Privacy Protection Method for Location Information to Utilize 5G-Based High-Precision Positioning Big Data*

Donghyeok Lee,[1†] Namje Park[2‡]
[1]Science Tech. Soc. Research Center, Jeju National University(Research Professor)
[2]Dept. Conv. Info. Secu., Graduate School, Jeju National University(Professor)

요 약

향후 5G 기술은 4차산업시대를 견인하는 핵심 인프라가 될 것이며, 지능화된 초융합 서비스를 위해서는 위치정보 등 다양한 개인정보의 수집이 필요할 것이다. 특히, 자율주행차 등 높은 품질의 서비스 제공을 위해서는 고정밀 측위 데이터가 요구된다. 만약 특정 고정밀 위치정보가 악의를 가진 자에 의해 노출될 경우, 심각한 프라이버시 위험이 발생할 수 있다. 그러나 기존의 암호화, 더미 위치생성, 난독화 등의 위치정보보호 기법은 빅데이터 수집을 위한 정확성 유지 및 통계처리 등에서 한계점이 있다. 따라서 본 논문에서는 위치정보를 노출시키지 않은 상태에서 통계질의 및 데이터 분석이 가능한 새로운 기법을 제안하였다. 제안한 방식은 랜덤 영역 버킷화와 다항식 기반의 변환처리를 통하여 원본을 재식별할 수 없도록 한다. 또한, 원본 데이터의 품질을 훼손하지 않으므로 고정밀 측위 빅데이터의 활용성을 극대화할 수 있다는 장점이 있다.

ABSTRACT

In the future, 5G technology will become the core infrastructure driving the 4th industrial era. For intelligent super-convergence service, it will be necessary to collect various personal information such as location data. If a person's high-precision location information is exposed by a malicious person, it can be a serious privacy risk. In the past, various approaches have been researched through encryption and obfuscation to protect location information privacy. In this paper, we proposed a new technique that enables statistical query and data analysis without exposing location information. The proposed method does not allow the original to be re-identified through polynomial-based transform processing. In addition, since the quality of the original data is not compromised, the usability of positioning big data can be maximized.

Keywords: Location Information, Location Privacy, Privacy Protection, High-Precision, Big Data

Received(04. 14. 2020), Modified(06. 11. 2020), Accepted(06. 30. 2020)

* 이 논문 또는 저서는 2019년 대한민국 교육부와 한국연구재단의 지원을 받아 수행된 연구임 (NRF-2019S1A5C2A04083374).

† 주저자, bonfard@jejunu.ac.kr
‡ 교신저자, namjepark@jejunu.ac.kr(Corresponding author)

I. 서 론

최근 5G 시대가 도래하면서 초연결, 초지능 및 초융합 시대가 도래하고 있다. 이는 5G 환경의 주요 키워드로써, 5G 기술의 등장은 단순히 쾌적한 통신 환경을 제공하는데 그치지 않고 향후 4차산업혁명 시대를 견인하는 핵심 인프라로 작용하게 될 것이다. 특히, 초융합 환경을 통하여 지능형 추천서비스, 헬스케어 서비스, 스마트 홈에서의 다양한 최적화 기능 등 기존에는 상상하지 못했던 고품질의 서비스를 제공받을 수 있을 것이다. 또한 초저지연 및 초고속의 장점을 활용하여 고해상도의 CCTV 모니터링이 가능하며, 고정밀화된 위치수집 기반의 지능화된 치안 서비스 및 선제적인 예방조치 등이 가능할 것이다.

이러한 5G 서비스를 적용하기 위해서는 프라이버시 보호에 대한 대책이 반드시 필요하다. 5G 환경의 특성상 고정밀 데이터에 대한 수집이 발생할 것이며, 이는 보다 정보 주체에 대한 역분석을 용이하게 하며, 개인의 신원이나 행동양식 등을 용이하게 추론할 수 있게 한다. 만약 가명화된 상태라 하더라도 개인정보의 역추적이 용이해질 수 있다는 것을 인지할 필요가 있다. 프라이버시에 대한 안전한 대책 없이 개인정보를 수집하게 된다면, 특정 시스템이나 서비스에 대한 위해 뿐만 아니라 고정밀 위치정보 노출 및 분석과 추정을 통하여 물리적 영역에서의 안전에도 침해를 받을 수 있는 등 사회적으로 매우 심각한 문제가 될 수 있다. 따라서 5G 환경을 위한 선제적인 개인정보보호 조치가 필수적으로 요구되는 상황이다.

그러나, 개인정보에 대한 프라이버시 보호조치를 과도하게 수행할 경우, 빅데이터 수집과 활용성 측면에서 제한을 받을 수 있다. 예를 들어 개인정보보호를 위하여 정밀도가 다소 낮은 데이터로 가공하여 저장한다면 서비스 측면에서는 낮은 품질을 기대할 수 밖에 없다. 고품질의 서비스가 요구되는 5G 환경에서는 이러한 상충관계를 극복할 수 있는 새로운 개인정보보호 방식이 필수적으로 고려되어야 한다[1].

따라서 본 논문에서는 5G 기반에서의 측위 빅데이터 활용을 위한 새로운 위치정보 프라이버시 보호 기법을 제안한다. 제안한 방식은 랜덤 영역 버킷화와 다항식 기반의 변환 처리를 통하여 사용자의 위치정보를 재식별할 수 없는 다른 값으로 변환하여 원본 위치정보를 분석할 수 없게 한다. 또한, 분포 추정 등 데이터 분석을 통하여 정보 주체의 신원이나 행동양식을 추정할 수 없게 한다. 그리고 필요한 경우 키를 가지고 있는 정당한 접근자에 의해 원본 데이터로 복원이 가능하며, 변환된 상태에서도 그대로 통계 질의가 가능하다. 특히, 변환 과정에서 원본 데이터의 정밀도를 훼손하지 않으므로 고정밀 측위 빅데이터의 활용성을 극대화할 수 있어, 활용성과 프라이버시 보호의 상충관계를 해결할 수 있다는 장점이 있다.

II. 관련 연구

2.1 5G와 위치정보 프라이버시

2.1.1 5G 환경과 위치정보

5G 환경에서는 초고속 인프라를 바탕으로 기존에 경험하지 못한 다양한 서비스의 제공이 가능하다. 특히, 오차범위가 매우 낮은 고정밀 GPS(Global Positioning System) 측위 데이터는 고품질 서비스를 제공하는 지능형 융합기술에 필수적으로 요구되는 정보이다. 예를 들어, 자율주행차가 안정적으로 주행하는데 있어 오차범위가 최소화된 고정밀 측위 데이터가 필수적으로 요구될 것이며, 이러한 고품질 측위 데이터를 바탕으로 자율주행 차량은 보다 안정적인 시내 주행이 가능하다. 또한 고정밀 차량 위치 빅데이터의 분석을 통하여 교통정보의 정밀하고 신속한 판단이 가능하여 예측이 쉽지않은 교통 환경에서의 선제적인 대응이 가능하다. 이러한 고품질의 서비스를 제공받기 위해서는 위치정보의 정확도 여부, 즉 데이터 품질이 매우 중요하다. 이러한 양질의 위치정보 빅데이터의 활용은 5G 환경에서의 원활한 서비스 제공에 필수적인 요소가 될 것이다.

2.1.2 위치정보 프라이버시 보호의 필요성

우리가 사용하는 위치기반서비스는 이미 일상에 존재하는 다양한 위치데이터를 수집하고 있다. 이러한 위치수집 정보는 개인의 생활양식과 행동패턴을 파악하는데 매우 유용하게 활용되고 있다. 특히, 최근 코로나 사태에 따른 확진자 동선 추적에 위치정보가 매우 효과적으로 활용되고 있으며, 실시간으로 동선이 공개됨에 따라 위험 지역의 회피가 가능하다.

그러나 위치정보의 수집은 프라이버시 문제와 직결되며, 개인의 누적 이동정보를 지속적으로 수집하게 된다면 단지 개인의 프라이버시 노출 문제 뿐만 아니라, 물리적인 안전에 대한 위해로까지 확대될 수

있음을 고려하여야 한다. 만약 개인위치추적정보가 누출된다면 생명 및 신체에 대한 침해 가능성, 침해의 즉시성, 장래위험의 유발가능성이 있으며, 이러한 부분은 다른 개인정보에 비해 현저하게 심각한 결과로 이어질 수 있다는 점에 항시 주목하여야 한다[2]. 특히, 5G 초융합 환경에서는 이러한 문제를 더욱 가중시킬 수 있어 각별히 안전하게 보호하여야 한다.

2.1.3 위치정보 비식별화 조치의 한계점

데이터 3법 개정에 따라, 개인정보처리자는 적절한 요건을 갖춘 경우 수집한 개인정보를 정보 주체의 동의 없이 추가로 활용할 수 있다. 즉, 가명화 등 적절한 비식별화 조치를 통한다면 개인정보를 활용할 수 있게 되었다. 일반적으로 널리 알려진 비식별화 방법론은 가명처리, 총계 처리, 데이터 삭제, 데이터 범주화, 데이터 마스킹과 같은 방법이 있다.

그러나 이러한 비식별화 방법은 근본적으로 한계점을 가지고 있다. 예를 들어, 프라이버시 보호를 위해 데이터의 정밀도를 낮춰 원본 데이터를 변경하는 방법을 선택한다면 원본 데이터의 품질을 그대로 보장하지 못하며, 특히 고정밀 측위 빅데이터의 경우 범주화 등의 가공을 통하여 원본 데이터가 훼손된다면 데이터 품질 저하로 이어지므로 정밀한 서비스를 제공하는데 문제가 될 수 있다. 이러한 경우, 데이터 자체의 품질은 훼손하지 않은 상태에서 정보 주체의 신원을 은닉하는 가명화 기법을 적용하는 경우를 생각해 볼 수 있다. 그러나 이러한 경우, 데이터의 역분석을 통한 신원정보 추론을 용이하게 한다. 특히, 고정밀 위치정보의 경우에는 신원정보 추론이 더욱 용이하다. 예를들어 새벽 시간에 특정 개인의 위치정보가 반복적으로 위치한 곳은 자택일 확률이 높으며, 활동 경로 추적을 통해 집, 직장 등의 정보를 파악한다면 해당 정보 주체를 용이하게 파악하게 될 수 있다. 따라서 기존의 비식별화 방식으로는 위치정보를 완벽하게 보호하는데는 한계가 있으며, 만약 개인정보에 대한 보호조치를 극단적으로 수행하려면 그만큼 정보 품질이 낮아질 수 있어 빅데이터 활용 측면에서의 활용성이 크게 낮아지게 된다. 이렇게 개인정보보호와 데이터의 품질은 상충관계를 가지고 있다. 이러한 문제는 고품질 5G 서비스를 위한 선결 과제이며, 선제적으로 조치하여 문제점을 방지할 필요가 있다.

2.2 기존의 위치정보보호 분석

2.2.1 암호화 기반 기술

암호화 기반의 위치정보 기법은 암호화 기술을 이용하여 위치정보를 보호하는 방식이다. Mascetti et al.은 서비스 제공업체를 신뢰하지 않는 경우 대칭키 암호화를 기반으로 LBS(Location Based Service) 서버에 현재 사용자의 위치를 나타내지 않으면서 사용자에게 전달할 수 있는 방법을 제안하였다[3]. 그러나, 이러한 접근 방법은 근본적으로 서버상에 통계적인 질의가 불가능하다는 한계점을 가지고 있다. 한편, Chen 등은 서로 다른 데이터 공급자가 서로 다른 키를 사용하여 데이터를 암호화하는 방식을 통하여 LBS 서버가 질의데이터에 대한 내용을 추론하는 것을 방지할 수 있는 보안 질의 프로토콜을 제안하였다[4]. 그러나 이러한 방식은 주로 보안 질의 자체의 안전성에 초점을 두고 있으며 LBS 서버 자체를 비신뢰영역으로 두고 있어 서버상에서 데이터 분석 및 통계처리를 진행할 수 없다는 단점이 있다.

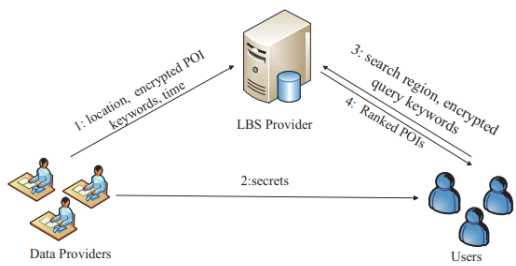

Fig. 1. Chen's Query Security Method

2.2.2 더미 위치정보 생성 기술

위치정보의 정밀도를 감소시키기 위한 방법으로, 더미 위치정보 생성 기법이 있다. 이는 위치정보의 정확성은 일정부분 보장하는 대신 다른 더미 위치정보를 추가하는 방식이다. H.Kido 등은 여러개의 더미 위치를 실제 위치와 함께 LBS 서버에 전송하여 사용자의 실제 위치를 비식별화 할 수 있는 방안을 제안하였다. 이러한 경우 더미 위치정보는 사용자의 모바일 장치에서 무작위로 결정되어지므로 특정한 신뢰된 서버가 필요하지 않다는 장점이 있다[5]. 또한, Tun-Hao You et al. 는 무작위 또는 회전 패턴을 통하여 사용자의 더미 궤적을 생성하는 기법을 제

안하였으며[6], P.R.Lei 등은 회전 방식을 이용하여 거리 편차를 만족하는 사용자 궤도를 회전시켜 더미와 사용자의 궤도를 식별할 수 없는 방식을 제안하였다[7]. 그리고 Hyo Jin 등은 공격자가 사용자에 대한 라이프 스타일 등의 사전 정보를 안다고 가정할 경우 데이터 분석시에 보안이 취약할 것을 고려하여 더미 데이터 위치 선정 시 사용자가 주로 머무르는 특정 장소를 고려하였다. 즉, 더미 데이터 선정 시 사용자가 자주 머무르는 특정 위치에 가중치를 제공하는 방법으로 접근하여 더미 데이터의 비중을 조절함으로써 분석을 어렵게 하는 방식으로 접근하였다[8]. 또한, Chen 등은 실제 환경의 물리적 제약을 고려한 더미를 생성하는 기법을 제안하였다. 이 방법은 의미론적인 다양성과 위치에 대한 물리적 분산을 모두 고려하는 방식으로 접근한 바 있다[9].

한편, Takahiro Hara 등은 모바일 기기에서 LBS 서비스를 사용할 때의 위치 프라이버시를 보호하기 위하여 LBS 서버가 사용자를 더미 위치정보와 식별이 어렵게 하는 방식을 제안하였다. 이는 더미 위치정보의 움직임을 보다 자연스럽게 시뮬레이션 하는 방법을 통한 사용자의 위치추적 방지 기법을 제안하였다. 이 방법은 확률을 이용하여 더미의 위치를 정함으로써 사용자와 식별이 어렵게 한다[10].

그러나 이러한 난독화 기술은 실제 빅데이터 분석에 있어 의미없는 가상의 데이터가 포함된다는 단점이 있다. 이러한 경우 서비스 품질에 결정적인 영향을 미칠 수 있다. 예를 들어 특정 위치에 대한 인구분포 등을 파악할 때 정확한 결과를 얻을 수 없게 되며, 별도의 필터링 대책이 요구되므로 빅데이터 분석 및 활용성 측면에서 문제가 된다.

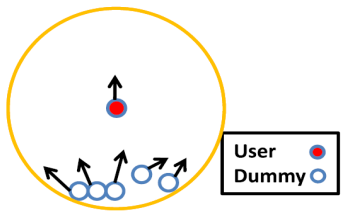

Fig. 2. Hara's Anonymization Method

2.2.3 위치 난독화 기술

위치 난독화 기술은 사용자로부터 LBS 및 클라이언트로 전송된 위치정보의 정밀도를 줄임으로써 프라이버시를 보호한다. Ardagna 등은 정확한 위치 대신 원형 영역을 LBS 서버에 전송하는 방식을 제안하였다[11,12]. 한편, Gutscher는 좌표 변환에 기반한 접근법을 제안하였으며, 여기에서 모바일 장치는 LBS 서버로 보낼 경우 이동이나 회전 등 간단한 기하학적 연산을 수행하는 방법을 고안하였다[13,14,15]. 그리고 Xiao 등은 위치 데이터의 시간적 상관관계를 차지하는 위치정보 프라이버시를 유지하기 위한 프레임워크를 제안하였다[16]. 해당 연구에서는 위치정보 서비스 제공시에 사용자 위치의 시간적 상관관계의 분석을 통하여 사용자의 위치에 대한 역추정이 가능함을 지적하고 사용자의 위치 분석을 어렵게 하기 위하여 차분 프라이버시를 기반으로 해결방안을 제시하였다. 또한 Soma 등은 질의시에 검색 공간을 타원형 영역으로 세분화하는 기하학적인 특성을 활용하는 방식으로 접근하였다[17,18,19,20,21]. 이 방법은 위치기반 서비스 제공업체에 사용자의 거짓 위치 또는 은폐된 위치를 전송하여 데이터를 보호하는 기법을 제안하여 사용자의 실제 위치를 공개하지 않는다.

그러나 이러한 위치 난독화 기술은 원본의 정확한 정보를 가지고 있지 않다는 치명적인 단점이 있다. 이러한 경우, 고정밀을 요구하는 서비스에는 부적절하다고 볼 수 있으며, 서비스 품질을 위해서는 만약 위치정보가 난독화 되었더라도 필요시 원본으로 복원할 수 있는 별도의 메커니즘이 필요하다[22,23,24,25].

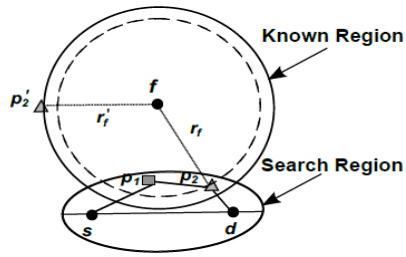

Fig. 3. Soma's Location Security Method

III. 제안 방식

본 장에서는 위치정보보호를 위한 새로운 기법을 제안한다. 이를 위해 우선적으로 5G 기반에서의 위치정보보호 모델 및 우선적으로 고려되어야 할 사항을 언급하고, 이후 세부 절차를 설명하고자 한다.

3.1 제안 방식 개요

3.1.1 5G 기반 위치정보보호 모델

그림 4는 제안 방식의 개요를 나타낸다. 사용자 측에서는 GPS 신호를 위성으로부터 수신하고, 스마트폰, 자율주행차 등에서 수신된 위치정보를 LBS 서버로 전송한다. LBS 서버는 수신된 위치정보를 평문으로 저장하지 않고, 본 장에서 설명하는 랜덤 영역 버킷화 및 변환 방식을 적용하여 저장한다. 또한, LBS 서버에는 어떠한 신원 정보도 저장하지 않는다. LBS 서버는 기본적으로 신뢰영역에 속하나, 만약 악의적인 공격자에 의해 데이터가 노출되더라도 해당 서버에 저장된 정보로부터는 의미있는 정보를 수집할 수 없으며, 정당한 키를 알지 못하는 경우에는 LBS 서버의 유지보수 담당자 등 내부자에 의해서도 위치정보 분석을 통하여 개인정보를 파악할 수 없다[26,27,28,29]. 한편, 서비스 제공자인 SP(Service Provider)는 LBS 서버로부터 위치정보를 수신받아 사용자에게 적절한 위치정보 서비스를 제공할 수 있다.

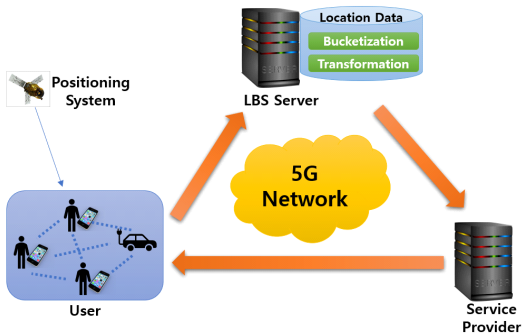

Fig. 4. Overview of Proposed Scheme

3.1.2 고정밀 위치정보보호를 위한 고려사항

고품질의 위치정보 서비스 제공을 위해서는 고정밀화된 위치정보가 필요하다[30,31]. 이러한 서비스 제공을 위해서 정보의 활용성과 개인정보보호 달성이라는 두가지 측면을 모두 만족해야 한다[32,33]. 여기서는 고정밀 위치정보의 프라이버시를 위한 고려사항을 살펴본다.

① 정보손실의 최소화 : 고품질의 원활한 5G 기반 위치정보 서비스를 위해서는 고정밀 데이터가 요구된다. 이는 프라이버시 보호 조치를 수행하더라도 원본 데이터의 훼손이 없어야 한다는 의미이며, 만약 정보 손실이 발생한다면 데이터의 품질 저하로 인하여 높은 수준의 서비스를 제공할 수 없다. 보안을 위한 목적이더라도 원본 데이터가 훼손되어서는 안되며, 정당한 키를 소지한 접근자에 의해서는 원본 데이터로 복원이 가능해야 한다.

② 프라이버시 보호 : LBS 서버에는 어떠한 개인정보를 확인하거나 추정할 수 있는 신원정보가 저장되어서는 안된다. 특히, 여러 정보를 조합하더라도 신원정보를 알아낼 수 없어야 하며, 개인정보를 침해할 수 있는 모든 정보는 프라이버시 보호를 위해 일방향 해쉬 또는 비식별화를 통하여 저장되어야 한다.

③ 분석 및 추론 공격 방지 : 비식별화된 데이터로부터 분석 및 추론을 통하여 원본을 복원할 수 없어야 한다. 예를 들어, 분포 확인을 통하여 원본 데이터의 신원을 역추적하거나 행동반경을 포착하는 등 추가적인 정보를 습득하기가 매우 어려워야 한다.

④ 질의 용이성 및 보안성 확보 : 위치정보를 질의할 경우 의미있는 결과를 가져올 수 있어야 한다. 특히, 데이터 분석을 위한 통계적 질의가 가능해야 하며, 이 과정에서 질의문과 질의 결과가 노출되더라도 평문이 추정되지 않아야 한다. 특히, 질의문 분석을 통해 정보 주체의 신원을 파악할 수 없어야 한다.

3.2 세부 절차

3.2.1 약어

본 장의 설명에 사용된 약어는 Table 1.과 같다.

Table 1. Notation

Abbreviation	Content
BID	Random Domain Bucket ID
pk	Pre-shared Secret Key
sk	Session Key
Q_n	Starting Point for n-th Bucket
sts	Scaled Timestamp
$b(m,n)$	m,nth Random Area Bucket
$E(\cdot)_K$	Result of Encryption with key K
$H(\cdot)$	Result of Hash
$PRNG(\cdot)_K$	Pseudorandom Number Generation
$HMAC(\cdot)_K$	Result of HMAC with key K

3.2.2 알고리즘 설계

(1) 데이터 처리 흐름

제안 방식에서는 먼저 전체 지리적 영역을 분할하여 랜덤한 사이즈를 갖는 랜덤 영역 버킷화를 수행하고, 랜덤 영역내의 거리값에 대하여 다항식 기반의 변환과정을 수행한다. 데이터베이스에는 이러한 랜덤 영역에 대응하는 랜덤 버킷 아이디와 x,y축의 변환된 거리값을 저장하게 된다. 제안 방식은 이 과정에서 원본정보를 저장하지 않는 것이 특징이며, 변환된 값만으로는 원본 데이터를 추정할 수 없게 한다. 한편, 사전 공유된 pk를 알고 있는 접근자는 원본값에 대한 복원이 가능하며, pk를 알지 못하는 경우는 서버 관리를 담당하는 내부자라 하더라도 원본 데이터를 복원할 수 없다. SP와 LBS 서버간의 질의 과정에서는 평문 정보를 노출하지 않으며, 악의를 가진 공격자가 질의 요청과 결과를 모두 수집한다고 하더라도 원본 정보를 확인하거나 추정할 수 없게 한다.

그림 5는 위치데이터의 처리 흐름을 나타내며, 전체 동작 절차는 다음과 같다.

① 클라이언트는 안전한 채널 또는 암호화를 통하여 GPS 위치정보를 LBS 서버에 전송한다.
② LBS 서버는 랜덤영역 버킷화를 수행하고, 현재 GPS값에 대한 버킷의 위치를 결정한다.
③ LBS 서버는 세부 위치정보인 R값을 안전하게 보호하기 위하여 변환 절차를 수행한다.
④ LBS 서버는 최종 변환된 결과값을 저장한다.
⑤ 서비스 제공자는 위치기반 서비스 제공을 위하여 LBS 서버에 위치정보 질의를 수행한다.
⑥ LBS 서버는 결과 데이터를 응답한다.
⑦ 서비스 제공자는 위치기반서비스를 제공한다.

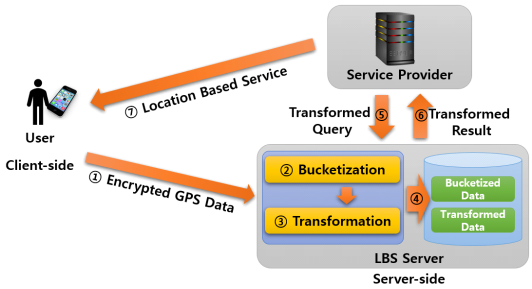

Fig. 5. Data Processing Flow

(2) 랜덤 영역 버킷화

랜덤 영역 버킷화 단계에서는 지리적 영역을 랜덤 사이즈를 가진 특정한 버킷으로 구분한다.

가로 x, 세로 y 값을 갖는 특정 좌표 위치값이 있을 때, 해당 위치값은 특정 랜덤 영역 버킷에 속하게 된다. 랜덤영역 버킷은 $b(m,n)$와 같은 형식으로 표현할 수 있으며, 그림 4에서는 특정 좌표가 속한 랜덤영역의 버킷 위치를 나타낸다. 아래 그림에서는 가로 x, 세로 y값을 갖는 좌표는 버킷 b(4,2)에 위치하고 있음을 알 수 있다. 그리고 R_x, R_y값은 해당 위치값이 속한 버킷 b(4,2) 내에서의 내부 x, y위치값을 의미한다. 또한, x축 상의 버킷은 n값을 나타내며, y축 상의 버킷은 m값을 나타낸다. 다시말해, n은 x축상의 n번째 버킷이라는 의미이며, m은 y축상의 m번째 버킷이라는 의미를 가진다. 즉, 버킷이 증가함에 따라, m,n값도 증가하게 된다.

아래 그림 6은 좌표상의 랜덤 영역 버킷을 나타내며, 특정 객체가 b(4,2), b(4,3), b(3,3)의 영역을 각각 순서대로 이동해 왔음을 알 수 있다.

랜덤 버킷을 생성하는 방법은 다음과 같다. 각각의 버킷 사이즈는 랜덤하게 정해지며, 각 버킷마다 랜덤한 사이즈를 가지게 된다. 이러한 특성은 특정 버킷의 분포를 알아내는 것만으로 해당 버킷이 어느 영역에 위치해 있는지 파악이 어렵게 한다. 랜덤 버킷은 아래의 식을 통하여 구할 수 있다. 여기에서, 의사난수의 SEED 역할을 하는 sk 및 사전 공유된 값인 pk를 알지 못하면 이 값을 계산할 수 없으며, 랜덤 버킷을 구할 수 없게 된다.

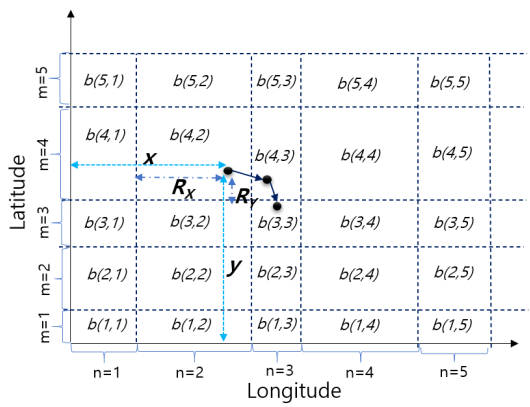

Fig. 6. Random Bucketization

$$Q_n^{sk} = \sum_{i=1}^{n} PRNG(n+pk)_{sk}$$

특정 버킷의 위치는 위의 식에 따라 결정되며, 특정 n번째 버킷의 시작값은 Q_{n-1}^{sk}이며, 종료값은 Q_n^{sk}이 된다. 이러한 식으로 모든 버킷의 시작값과 종료값을 구할 수 있으며, 아래 그림 7은 해당 식에 따른 랜덤 버킷이 구분된 결과를 나타낸다. 모든 버킷의 사이즈는 의사난수의 특성에 따라 랜덤하게 결정되며, pk를 사전에 알지 못하는 인가되지 않은 접근자는 랜덤 버킷을 생성할 수 없다는 특징이 있다.

앞서 식에서 sk는 세션 키로써, 특정한 시간대에서만 사용되는 키이다. 세션 키는 특정한 시간을 공유하는 위치값에 대해서는 동일한 값을 가진다. 그러나, 서로 다른 시간값을 가지는 경우, 세션 키는 달리 발생한다는 특징이 있다. 이러한 특성에 따라, 동일한 위치라 할지라도 시간값이 다르면 서로 다른 결과값을 가지게 된다. 다시 말해, 시간값이 상이할 경우, sk를 기반으로 연산되는 랜덤 영역 버킷의 사이즈가 달라지며, 달리 표현해 서로 다른 시간이라면 동일한 지점에 위치해 있더라도 서로 다른 버킷상에 위치하게 된다. 세션 키 sk는 계량화된 타임스탬프 값인 sts를 기반으로 아래와 같이 계산할 수 있다.

$$sk = H(sts \| pk)$$

sts는 계량화된 시간값을 의미한다. 일반적으로 타임스탬프에서는 초, 밀리초 단위까지 포함될 수 있으나, 이러한 경우 pk를 알고 있더라도 향후 동일한 타임스탬프 값을 사전에 알지 못하면 sk를 생성하기 어려우므로 계량화된 타임스탬프 값이 필요하다. 다시 말해, 계량화된 시간값은 특정 범주 내 시간 간격 내에서는 동일한 sts 값을 출력하는 것을 의미한다. sts의 생성을 위한 시간 간격은 정책에 따라 10초, 1분 또는 10분 등의 간격을 통해 생성될 수 있다.

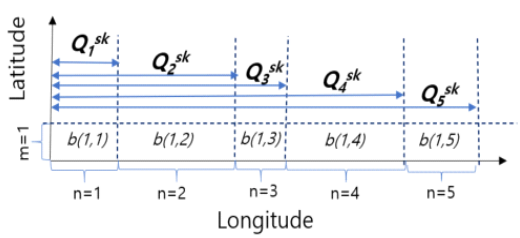

Fig. 7. Determination of Random Bucket

해당 특정 시간대에 속한 위치정보는 각각 동일한 세션 키인 sk값을 가지는 특성이 있다. 따라서, 동일한 시간대에 속하는 데이터는 모두 동일한 버킷 사이즈를 가지며, 이러한 데이터에 대해서는 통계질의나 데이터 분석이 가능하다. 만약 시간대가 상이하여 세션 키가 서로 다른 경우는 버킷 사이즈가 전혀 달라지게 되므로 서로 다른 시간의 데이터는 서로 연관성을 띠지 않는다. 이러한 경우, 각 위치데이터는 상이한 기준을 가지므로 통계질의, 데이터 분석을 어렵게 한다. 특히, 개인의 위치추적 정보는 시간에 따라 서로 다른 버킷 사이즈를 갖게 되므로 세션 키를 구성할 수 없는 정당하지 않은 자에 의하여 위치추적정보가 재구성되기는 매우 어렵다.

그림 8은 시간의 흐름에 따른 버킷의 변화를 나타낸다. 여기에서 임의의 경도값 a가 있다고 하고, ㄴ $sts_1 \sim sts_5$와 같이 다섯 개의 특정 시간값이 있다고 가정할 경우, 아래의 그림과 같이 해당 경도값이 속하는 버킷 값은 시간의 흐름에 따라 변화하게 된다. 아래 그림에서 특정 경도값 a가 속한 버킷은 $sts_1 \sim sts_5$ 시점별로 각각 b(1,4), b(1,3), b(1,5), b(1,2), b(1,4)와 같이 변하며, 위치가 동일하더라도 시간에 따라 상이한 버킷 값을 가진다.

모든 버킷은 버킷 ID를 가지며, $b(m,n)$에 대한 버킷 ID는 sk를 키로 한 HMAC 연산을 기반으로 구한다. 버킷 ID는 버킷의 구분을 위해 필요하며, 만약 BID 값이 동일한 경우, 동일한 버킷상에 위치해 있다고 가정할 수 있다. 모든 버킷은 단일한 ID를 가지며, 버킷 ID는 아래의 식으로 구할 수 있다.

$$BID = HMAC(H(m) \| H(n)))_{sk}$$

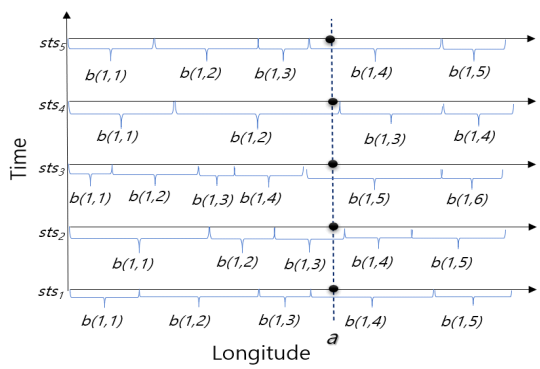

Fig. 8. Bucket Changes Over Time

(3) 다항식 기반의 R값 변환

R값은 x축 R_x, y축 R_y값을 가진 버킷 내에 속한 상대적인 좌표이다. 즉, 특정 위치가 속한 버킷 내부에서의 x축, y축 시작점으로부터의 거리를 의미하며 버킷은 위치정보의 대략적인 값을 나타낼 수 있고 R값을 통해 해당 버킷 내에서의 세밀한 위치를 나타낼 수 있다. 여기에서 R 값이 노출될 경우, 데이터 분석을 통한 위치정보 역추정이 가능하여 구체적인 개인정보 노출이 발생할 수 있다. 따라서 이 단계에서는 다항식을 기반으로 R값을 변환한 $f(R)$값을 생성한다. R값의 변환을 위해 임의의 값 $R_1 < R_2$인 모든 R_1및 R_2에 대하여 $f(R_1) < f(R_2)$ 가 항상 성립하는 단조증가 함수를 이용한다. 여기에서 단조증가함수를 사용하는 이유는 변환된 상태에서의 원활한 통계질의 처리를 위해서이다. 단조증가함수를 적용하면 원본과 변환값의 정렬 순서가 변함이 없다는 특징이 있다. 이러한 특징에 따라, 함수를 적용한 결과값에 SQL질의 등 통계처리가 그대로 적용 가능하다는 장점이 있다. 따라서 R값의 변환을 위해, 아래와 같이 단조증가 함수를 구성한다. 다음의 식을 통하여 변환된 $f(R)$값을 구할 수 있다.

$$f(R) = Q_n^{sk}(R)^2 + Q_{n-1}^{sk} + Q_{n+1}^{pk}$$

위의 다항식을 적용하여 R값을 변환할 수 있다. 만약 pk값을 사전에 알지 못한다면, pk를 인자로 하는 sk값 또한 구성할 수 없으며, 이러한 경우 다항식의 역함수를 구성할 수 없게 되므로 해당 단조증가 함수로 변환된 R값을 원본으로 되돌릴 수 없다. 즉, sk와 pk 값을 반드시 사전에 알고 있어야 원본 데이터를 확인할 수 있다. 여기에서, $f(R) = y$에서 해당 변환값의 원본 데이터 R을 구할 수 있는 역함수 $f^{-1}(y)$은 다음과 같다.

$$f^{-1}(y) = \sqrt{\frac{y - Q_{n-1}^{sk} - Q_{n+1}^{pk}}{Q_n^{sk}}}$$

이 과정에서 세션 키인 sk및 사전 공유된 pk를 알고 있는 정당하고 인가된 자만 원본을 복원할 수 있으며, 해당 값을 알지 못하는 인가되지 않은 사용자는 원본 데이터를 복원할 수 없다.

(4) 데이터의 저장

최종적으로 데이터의 변환을 완료한 후, 데이터베이스에 저장 시 다음과 같은 값을 저장한다.

① BID : 버킷의 ID를 나타내며, 특정 버킷의 위치인 m과 n값에 대한 HMAC의 출력값이다. 만약 평문에서 동일한 위치 좌표이더라도 시간의 변화가 발생하면 버킷 위치 또한 변화하게 되므로 BID의 값도 변경된다.

② $f(R_X)$, $f(R_Y)$: R_X, R_Y를 각각 다항식을 통해 변환한 값으로, 변환된 값만 저장하며 원본인 R_X, R_Y는 어느 곳에도 저장하지 않는다.

③ $HMAC(ID)_{sk}$: 개인 신원정보에 대하여 sk를 키로 한 HMAC 결과를 보관하며, 원본 개인신원정보 자체는 보관하지 않는다.

④ H(sk) : 세션키의 해시값을 보관한다. 세션키는 시간정보를 바탕으로 생성되므로, pk를 사전에 알고 있는 인가자는 시간정보와 pk값을 바탕으로 sk 및 H(sk)를 생성할 수 있다.

이러한 정보를 바탕으로 인가된 접근자에 한하여 위치정보 데이터에 대한 범위검색 등이 가능하다. 만약, 사전 공유된 pk를 알지 못하는 경우에는 세션키인 sk를 연산할 수 없으므로 정상적으로 질의문을 구성할 수 없으며 데이터에서 유의미한 결과를 추출할 수 없다. 데이터베이스에 저장된 데이터만으로는 개인신원정보나 시간정보는 해쉬값만 저장하고 있으며 위치정보는 변환된 값만 저장하고 있기 때문이다.

(5) 데이터에 대한 질의

pk를 사전에 알고 있는 정당한 사용자는 데이터베이스의 값에 대해 통계분석 등을 위해 범위 조건을 지정한 SQL 질의가 가능하다. 특정시각에서 위도 lat_a~lat_b, 경도 lon_a~lon_b 사이에 속한 위치정보를 검색한다고 가정하면, 절차는 다음과 같다.

먼저, 특정시각의 계량화된 타임스탬프인 sts값을 생성하고 pk를 통해 sk 값을 생성한다. 해당 sk 값과 pk를 알고 있으므로, 해당 시점에서의 랜덤 버킷 또한 생성할 수 있으며, lat_a, lat_b, lon_a, lon_b가 속한 버킷 아이디 및 R값을 구할 수 있다.

이후 각각의 버킷 아이디인 BID 값을 추출하고, R_x, R_y값을 이용해 다음과 같은 범위검색 질의를 생성할 수 있다. 질의문에서는 평문이 포함되지 않으므

select [field] from table
where bucket_id = [BID]
and lat_r >= $f(R_{lat\_a})$
and lat_r <= $f(R_{lat\_b})$
and lon_r >= $f(R_{lon\_a})$
and lon_r <= $f(R_{lon\_b})$
and hashed_sk = $H(sk)$

Fig. 9. Query of Transformed Data

로 질의문상 어떠한 비밀 정보도 노출되지 않는다.

IV. 분 석

4.1 안전성 분석

4.1.1 외부 노출에 따른 추론 공격

위치정보는 그 자체만으로 많은 추론을 가능하게 한다. 특히, 특정 시간에 어디 위치하고 있는지를 파악하는 것만으로 해당 객체의 신원이나 직업 등을 용이하게 추정할 수 있다. 따라서 위치정보 자체가 노출이 되더라도 분석 및 추론 공격에 의해 해당 객체의 정보가 노출이 되지 않아야 한다. 제안한 방식은 사전 공유된 pk 및 세션 키인 sk를 알지 못하면 위치정보를 복원할 수 없다. 특히, 제안한 방식에서는 시간정보를 데이터 어디에도 저장하지 않는다는 특징이 있다. 시간정보는 해쉬된 값으로만 저장하며, 해쉬함수의 일방향성이라는 특징에 따라 원본 시간정보를 복원할 수 없다. 이러한 점은 공간과 시간정보를 결합하여 추론하는 것을 불가능하게 하므로 위치정보 데이터가 모두 노출된 경우를 가정한 경우에도 위치정보 주체의 신원정보를 파악할 수 없다. 또한, 제안한 방식은 위치정보 평문에 대한 어떤 정보도 저장하지 않으며, 버킷값과 변환된 R값으로 구분하여 저장한다. 또한 R값은 버킷 내의 상대적인 위치값으로 그 자체로 절대값인 위치정보를 표현하고 있지 않다. 따라서 R값에 대한 노출이 발생한다 하더라도 어느 GPS 좌표인지 알 수 없다. 만약, R값을 통해 특정 버킷 내부에서의 동선 파악 분석을 시도하는 경우, 제안한 방식은 시간의 흐름에 따라 버킷 자체가 변화하므로 시간대별로 R값의 연결성이 사라지게 된다. 또한, 데이터베이스에는 R값에 대한 변환된 값을 저장하므로 동선 분석이 매우 어렵다는 특징이 있다.

4.1.2 내부자에 의한 공격

위치정보 서비스 제공 과정에서 LBS 시스템 관리자 등 내부자가 존재하며, 해당 내부자가 데이터에 접근하는 경우를 가정해 볼 수 있다. 만약 유지보수 관리자 등 내부자에 의하여 데이터가 노출된 경우를 가정하더라도, 해당 정보 열람의 인가를 받은 경우에만 pk를 기반으로 sk 값을 구성할 수 있다. 제안한 방식에서는 기본적으로 위치정보가 비식별화되어 있으며, 평문 위치정보는 어디에도 저장하고 있지 않으므로 내부자라 하더라도 비밀키인 pk를 알지 못하면 원본 정보를 복원할 수 없다. 또한, 시간정보가 해쉬처리되어 있어 원본 시간정보를 복원할 수 없음에 따라 전체 데이터로부터 유의미한 시공간 정보를 파악할 수 없으므로 정보주체의 신원 추정을 할 수 없다.

4.1.3 질의 분석 공격

제안한 방식에서는 데이터베이스에 평문 위치정보를 저장하지 않으며, 질의 과정이나 질의 결과에서 평문에 대한 정보를 포함하지 않는다. 따라서 위치데이터에 대한 질의를 수행할 경우, 질의문과 결과 모두를 수집하더라도 평문의 데이터를 노출하지 않는다. 특히, 시간정보가 해쉬처리되어 있으므로 변환된 위치정보와 시간정보를 결합하여 유의미한 정보를 조합할 수 없다. 앞서 3.2.2.의 (5)에 나타난 것과 같이, 질의문과 그 결과를 수집하더라도 어떤 유의미한 분석 결과를 얻을 수 없어 질의 보안성을 가진다.

4.1.4 분포 분석에 따른 추정 공격

위치데이터의 분포를 추정하여 특정 객체의 신원 파악을 시도할 수 있다. 예컨대, 특정 위치에서 얼마나 머물고 있는지 혹은 특정 시간대에 어디에 있는지를 바탕으로 객체의 신원이나 행동양식을 파악할 수 있으며, 데이터 분포 추정을 통해 이러한 분석을 행할 수 있다. 그러나 제안한 방식에서의 랜덤 버킷과 변환값은 동일한 위치이더라도 서로 다른 값을 가진다. 이러한 점은 특정 객체의 위치추적을 까다롭게 하며, 특히 시간 정보는 연속적인 값이 아닌 해쉬값으로만 존재함으로써 위치정보를 시간 순서대로 나열할 수 없다. 매 시간에 따라 발생하는 위치값은 모두 상이하게 나타나며, 이러한 특성은 분포 분석에 따른 신원 및 행동양식에 대한 추정을 매우 어렵게 한다.

4.2 효율성 분석

4.2.1 질의 효율성 측면

제안한 방식은 변환한 값 상태 그대로 통계적 질의가 가능하다. 특히, 범위검색 기반의 질의문 구성이 가능하여 평문 데이터와 유사한 수준으로 데이터 질의 처리가 가능하며, 통계적 질의 또한 가능하다. 또한, 이러한 질의는 pk와 sk를 알고 있는 경우에만 구성이 가능하다. 만약 이러한 비밀 정보를 알지 못한다면 질의문을 구성할 수 없다. 데이터베이스에는 암호화된 값 또는 해시값, 변환된 값만 존재하며, 평문 상태로 저장되어지지 않기 때문이며, 질의문 구성 시 이러한 암호화, 해시, 변환된 값을 구성할 수 없다면 데이터베이스에 의미있는 질의를 할 수 없다.

4.2.2 데이터 정확성 측면

기존의 비식별화 방식인 더미 위치정보 생성, 난독화 기술은 원본 데이터를 훼손시킨다. 특히, 더미 위치정보 생성 기법은 특정 범위 내의 위치정보 개수 집계시 정확한 값을 알 수 없으며, 난독화 기법은 원본 값 자체를 변화시키거나 정확하지 않은 일정 범주 내의 위치정보를 제공함으로써 데이터의 정확성을 보장할 수 없다. 이러한 점은 고정밀 위치정보 제공 시 걸림돌이 될 수 있다. 제안한 방식은 랜덤영역 버킷화 및 단조증가함수를 활용하여 위치정보에 대하여 오차를 최소화한 의미있는 질의가 가능하며, 이러한 질의 결과는 pk를 알고 있는 정당한 사용자에 의해 필요시 평문으로 복원이 가능하다.

4.2.3 기존 방식과의 비교

2장에서 언급한 것과 같이 기존의 위치정보보호기법은 크게 암호화 방식, 더미 데이터 추가, 난독화 방식 등으로 구분할 수 있다. 아래 표 2에는 기존의 암호화 기반 접근 방식, 더미 데이터 추가, 난독화 기법과 제안 기법에 대한 비교 결과가 나타나 있다.

암호화 방식은 데이터의 정확성, 추론공격, 질의 분석공격을 방지할 수 있으나 범위검색이 불가능하여 통계적 질의가 어려우므로 실제 서비스 적용에는 적합하지 않은 측면이 있다. 한편, 더미 데이터와 난독화 기법은 범위검색을 일부 지원 가능하나 정확한 데이터를 얻기가 힘들다는 단점이 있다. 또한, 데이터

Table 2. Comparison with Existing Methods

Query Type	Encryption-based [3][4]	Dummy Data [8][9][10]	Obfuscation [13][14][15]	Our Scheme
Range Query	×	△	△	○
Accuracy	○	△	△	○
Inference Protection	○	○	○	○
Query Analysis Protection	△	×	△	△

분석공격에 대한 장점이 있으나, 질의문 분석 공격은 암호화 기법에 비해 안전성을 완전하게 보장할 수 없다. 제안한 기법은 범위검색을 지원하며, 데이터의 정확성을 훼손하지 않으므로 질의시 의미있는 결과를 리턴한다. 특히, pk를 사전에 알지 못하는 접근자에 의해서는 원본데이터 확인이 불가능하며, 시간이 변함에 따라 버킷과 R값이 지속적으로 변화하므로 데이터 분석 및 추론공격으로부터 안전함을 보인다.

4.3 실험 결과

본 절에서는 제안 방식에 대한 실험 결과를 살펴본다. 실험 결과는 그림 10과 같으며, 여기서는 위치추적 데이터에 대하여 R값에 대한 변환 결과를 측정하였다. 실험 결과 분석을 용이하게 하기 위하여 y축을 중심으로 한 R_y축 값을 기준으로 실험하였다.

또한 x축은 계량화된 시간정보를 나타내며, 편의상 sts값이 증가하는 시점의 시퀀스 번호로 표기하였다. 또한, y축에서는 R_y값의 변화를 나타내었다.

Original 그래프는 평문 R_y값을 나타낸다. 그리고 R-Transformation 그래프는 R_y값이 본 논문에서 제안한 방식으로 변환된 $f(R_y)$값을 나타낸다.

Original 그래프는 객체의 y축 움직임을 나타낸다. 객체의 위치정보가 변경되거나, 혹은 정지해 있음과 상관없이 시간의 흐름에 따라 R_y값의 변환값인 $f(R_y)$값은 실시간으로 변화됨을 알 수 있다. 이러한 특성에 따라, 변환된 R_y데이터와 원본 위치데이터와의 유사성은 현저히 떨어짐을 알 수 있으며, 악의를 가진 공격자가 데이터베이스에 저장하고 있는 R-Transformation 정보를 수집하더라도 해당 변환된 정보를 통해서는 원본 위치 데이터에 대한 추적이 매우 어렵다는 것을 알 수 있다. 실제로 데이터베이스에 저장되는 값은 변환된 $f(R)$값이며, 원본R값에 대한 정보는 어느 곳에도 저장되지 않는다.

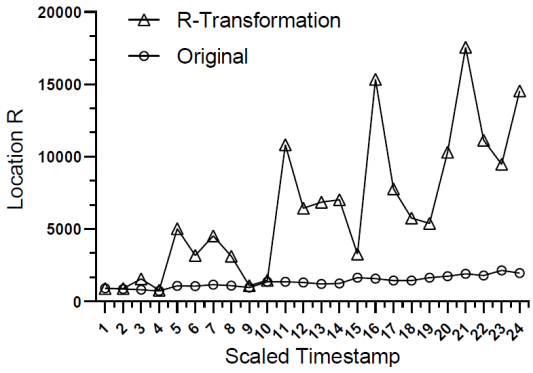

Fig. 10. Experimental Results

V. 결 론

최근 코로나 사태로 인하여 위치정보 수집과 프라이버시 보호에 대한 관심이 점차 높아지는 추세이다. 그러나 5G 환경에서는 고정밀 측위 데이터 수집과 빅데이터로의 활용이 필요하며, 프라이버시 보호와 빅데이터의 활용이라는 상충되는 속성에 대한 선제적인 해결이 필요한 상황이다. 따라서 본 논문에서는 빅데이터의 활용성을 유지하면서 위치정보의 안전한 보호가 가능한 새로운 기법을 제안하였다. 제안한 기법은 랜덤 영역 버킷화 및 다항식 기반의 변환 처리를 기반으로 평문 위치정보를 전혀 다른 값으로 변환하여 저장할 수 있다. 또한, 이러한 변환되어 저장된 위치정보에 통계질의 수행이 가능하며, 원본의 품질 자체를 훼손하지 않으므로 빅데이터 활용에도 유용하게 사용될 수 있다. 특히, 제안한 기법은 기존의 암호화 기법, 더미 데이터 추가 기법, 난독화 기법에 비해 범위검색, 정확도에서 효율적임을 보였고, 추정공격, 질의문 분석 공격에도 안전함을 보였다.

4차산업혁명의 주요 인프라인 5G 환경에서의 위치정보 프라이버시를 유지하기 위한 안전한 보안기술은 앞으로 주요한 연구분야로 자리잡을 것이며, 향후 이에 대한 선제적인 보안 대책을 연구할 예정이다.

References

[1] Liu, Bo, et al., "Location privacy and its applications: A systematic study", IEEE Access, vol.6, pp.17606-17624. Apr. 2018.

[2] Woo, Dae Sik, "A Study on a Rational Improvement Plan of Location Information Act for Securing Safety of the People", The Journal of Police Science, 18(2), pp.71-95, Jun. 2018.

[3] Mascetti, Sergio, et al. "Privacy in geo-social networks: proximity notification with untrusted service providers and curious buddies", The VLDB Journal, vol.20, no.4, pp.541-566, Aug. 2011.

[4] Chen, Pei, et al., "Preserving location and content privacy for secure ranked queries in location based services", 2016 IEEE Trustcom/BigDataSE/ISPA., pp.892-899, Aug. 2016

[5] Kido, Hidetoshi, Yutaka Yanagisawa, and Tetsuji Satoh., "An anonymous communication technique using dummies for location-based services", ICPS'05. Proceedings., pp.88-97, Jul. 2005.

[6] You, Tun-Hao, Wen-Chih Peng, and Wang-Chien Lee., "Protecting moving trajectories with dummies", 2007 International Conference on Mobile Data Management, IEEE, pp. 278-282., May. 2007.

[7] Lei, Po-Ruey, et al., "Dummy-based schemes for protecting movement trajectories", Journal of Information Science and Engineering, vol.28, no.2, pp.335-350, Mar. 2012.

[8] Do, Hyo Jin, et al., "Another dummy generation technique in location-based services", 2016 International Conference on Big Data and Smart Computing (BigComp). IEEE, pp. 532-538, Jan. 2016.

[9] Chen, Shu, and Hong Shen., "Semantic-aware dummy selection for location privacy preservation", 2016 IEEE Trustcom/BigDataSE/ISPA. IEEE, pp. 752-759, Aug. 2016.

[10] Hara, Takahiro, et al., "Dummy-based user location anonymization under re-

al-world constraints", IEEE Access, vol.4, pp.673-687, Feb. 2016.
[11] Ardagna, Claudio A., et al., "An obfuscation-based approach for protecting location privacy", IEEE Transactions on Dependable and Secure Computing, vol.8, no.1, pp.13-27, Jun. 2009.
[12] Ardagna, Claudio Agostino, et al., "Location privacy protection through obfuscation-based techniques", IFIP Annual Conference on Data and Applications Security and Privacy, Springer, Berlin, Heidelberg, pp.47-60, Jul. 2007.
[13] Gutscher, Andreas., "Coordinate transformation -a solution for the privacy problem of location based services?", Proceedings 20th IEEE International Parallel & Distributed Processing Symposium, IEEE, pp.7-13, Apr. 2006.
[14] Donghyeok Lee, Namje Park, "A Study on Metering Data De-identification Method for Smart Grid Privacy Protection", Journal of the Korea Institute of Information Security & Cryptology, 26(6), pp.1593-1603, Dec. 2016.
[15] Namje Park, "Implementation of terminal middleware platform for mobile RFID computing", International Journal of Ad Hoc and Ubiquitous Computing, vol.8, no.4, pp.205-219, Jan. 2011.
[16] Xiao, Yonghui, and Li Xiong., "Protecting locations with differential privacy under temporal correlations", Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security, pp.1298-1309, Oct. 2015.
[17] Jinsu Kim, 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. doi:10.3390/sym12060891.
[18] 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, Jan. 2017.
[19] Namje Park and Namhi Kang, "Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle", Journal of Sensors (Basel), vol.16, no.1, pp.1-16, Dec. 2015.
[20] Jinsu Kim, 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. https://doi.org/10.1007/s00779-019-01299-w.
[21] Soma, Subarna Chowdhury, et al., "Trip planning queries with location privacy in spatial databases", World Wide Web, vol.20, no.2, pp.205-236, Mar. 2017.
[22] Namje Park, Byung-Gyu Kim, 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, pp.735, Jun. 2019.
[23] Donghyeok Lee, Namje Park, Geonwoo Kim, Seunghun Jin, "De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment", Journal of Peer-to-Peer Networking and Applications, Vol.11, No.6, pp.1299-1308, Nov. 2018.
[24] Seoyeon Yoon, "Traffic data use and location information protection", Planning and Policy, 405, pp.12-17, Jul. 2015.
[25] Namje Park, 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.
[26] Jinsu Kim, Namje Park, Geonwoo Kim, Seunghun Jin, "CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia", Electronics, vol.8, no.4, pp.412, Apr. 2019.
[27] Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, and Howon Kim, "WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment", LNCS, Advanced Web and Network Technologies and Applications, vol.3842, pp. 741-48, Jan. 2006.
[28] Chen, Pei, et al., "Preserving location and content privacy for secure ranked queries in location based services", 2016 IEEE Trustcom/BigDataSE/ISPA., IEEE, Aug. 2016.
[29] Namje Park, Donghyeok Lee, "Electronic identity information hiding methods using a secret sharing scheme in multi-media-centric internet of things environment", Personal and Ubiquitous Computing, vol. 22, no.1, pp.3-10, Feb. 2018.
[30] Jongcheol Shin, "Direction of Privacy Policy to Revitalize the Data Industry", Planning and Policy, 451, pp.5-12, May. 2019.
[31] Namje Park, Hongxin Hu, Qun Jin, "Security and Privacy Mechanisms for Sensor Middleware and Application in Internet of Things (IoT)", International Journal of Distributed Sensor Networks, vol.2016, Jan. 2016.
[32] Donghyeok Lee, Namje Park, "Blockchain based privacy preserving multimedia intelligent video surveillance using secure Merkle tree", Multimedia Tools and Applications, pp.1-18, Mar. 2020, https://doi.org/10.1007/s11042-020-08776-y.
[33] Namje Park, Hyo Chan 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.

〈저자소개〉

이 동 혁 (Donghyeok Lee) 정회원
2007년 2월:동국대학교 전자상거래기술전공 공학석사
2018년 2월:제주대학교 컴퓨터교육전공 공학박사
2007년 6월~2008년 5월:한국전자통신연구원 정보보호연구단 연구원
2008년 11월~2015년 6월:KT 플랫폼개발단 과장
2018년 3월~현재:제주대학교 과학기술사회연구센터 학술연구교수
〈관심분야〉 DB 보안, 클라우드 보안, IoT 보안, 블록체인, 데이터 비식별화 등

박 남 제 (Namje Park) 종신회원
2008년 2월:성균관대학교 컴퓨터공학과 박사
2003년 4월~2008년 12월:한국전자통신연구원 정보보호연구단 선임연구원
2009년 1월~2009년 12월:미국 UCLA대학교 공과대학 Post-Doc.
2010년 1월~2010년 8월:미국 아리조나(ASU) 주립대학교 컴퓨터공학과 연구원
2010년 9월~현재:제주대학교 초등컴퓨터교육전공, 대학원 융합정보보안학과 교수
제주대학교 창의교육거점부센터장, 과학기술사회연구부센터장, 사이버보안인재교육원장
〈관심분야〉 융합기술보안, 컴퓨터교육, 스마트그리드, IoT, 해사클라우드 등