Journal of Convergence for Information Technology
Vol. 9. No. 7, pp. 1-7, 2019
e-ISSN 2586-4440
DOI : https://doi.org/10.22156/CS4SMB.2019.9.7.001

5G의 이질적인 환경에서 사용자 프라이버시를 효율적으로 보호하기 위한 다중 그룹 정보 관리 기법

김겸순[1], 연용호[2], 정윤수[3*]
[1]충북대학교 수학과 강사, [2]목원대학교 교양교육원 조교수, [3]목원대학교 정보통신융합공학부 조교수

Multi-group Information Management Techniques to efficiently Protect User Privacy in Heterogeneous Environments of 5G

Kyoum-Sun Kim[1], Yong-Ho Yon[2], Yoon-Su Jeong[3*]
[1]Lecturer, Department of Mathematics, Chungbuk National University
[2]Assistant Professor, College of Liberal Education, Mokwon University
[3]Assistant Professor, Division of Information and Communication Convergence Engineering, Mokwon University

요 약 최근 차세대 무선통신인 5G가 일상 생활에서 실용화되면서 다양한 분야에서 많은 변화가 이루어지고 있다. 그러나, 5G의 향상된 속도와 지연 시간이 개선되었지만 여전히 사용자 보안에 대한 개선이 요구되어 지고 있다. 본 논문에서는 5G의 이질적인 환경에서 사용자의 프라이버시 정보를 효율적으로 보호하기 위한 다중 그룹의 정보 관리 기법을 제안한다. 제안 기법은 서로 다른 이기종의 장치에서 생성되는 사용자의 프라이버시 정보를 서로 다른 그룹에서 연계 처리할 수 있도록 연계 정보를 클러스터링하여 분산 관리할 수 있도록 하는 것이 목적이다. 제안 기법은 주기적으로 사용자의 프라이버시 정보를 동기화하여 사용자별 프라이버시 정보를 가상의 공간에서 독립적으로 처리한다.

주제어 : 5G, 프라이버시, 다중 연계, 정보 처리, 개인 정보 수집

Abstract With the recent commercialization of the next generation of wireless 5G in everyday life, many changes have been made to organizations, industries and businesses of various sizes in various fields. However, although the improved speed and latency of 5G has improved, improvements in encryption, authentication and privacy are still required. In this paper, multiple groups of information management techniques are proposed to efficiently protect users' privacy in the heterogeneous environment of 5G. The proposed technique aims to allow distributed management of users' privacy links by clouding the privacy information generated by different heterogeneous devices to efficiently interface with different groups. Suggestion techniques process user-specific privacy information independently in a virtual space so that users can periodically synchronize their privacy information.

Key Words : 5G, Privacy, Multiple links, Information processing, Personal information collection

*Corresponding Author : Yoon-Su Jeong(bukmunro@mokwon.ac.kr)
Received May 14, 2019
Revised June 19, 2019
Accepted July 20, 2019
Published July 28, 2019

1. 서론

5G는 기존 무선 통신 기술에 비해 속도와 관련된 성능이 압도적으로 높은 것이 특징이다 [1]. 그러나, 5G 환경에 적합한 보안 기능이 뒷받침되지 않는다면 사용자의 중요 정보가 노출될 뿐만 아니라 도·감청 및 DDoS 공격 가능성이 매우 높다 [2]. 특히, 5G는 기존 세대의 보안 문제 이외에 추가적으로 발생할 수 있는 보안 문제점들이 존재한다.

5G 환경을 위한 보안 연구는 ITU, NGMN, ETSI, 3GPP, 5G-PPP 등의 표준화 연구를 중심으로 활발하게 이루어지고 있다. Z. Yan et al.은 5G 환경을 구성하고 있는 중간 장치들의 프라이버시 정책 관리 소홀로 발생할 수 있는 보안 문제점들을 정의하고 있다[3]. L. T. Sorensen et al.은 이기종 장치간에 서로 사용자의 프라이버시를 공유했을 경우 기존에 존재하던 보안 문제 이외에 추가적인 보안 문제가 발생할 수 있다[4]. F. Kemmer et al.은 사용자 데이터가 서로 다른 클라우드 환경에 저장되었을 경우 서로 다른 레벨에 따라 데이터가 관리되어야 하는 구조를 제안하였다 [5]. 5G 환경은 서로 다른 장비들이 다양한 환경에서 사용자의 편의를 극대화하기 때문에 그에 따른 다양한 보안 정책이나 사용자 프라이버시 보호에 대한 기술이 필요하다.

본 논문에서는 5G의 이질적인 환경에서 사용자의 프라이버시를 효율적으로 보호하기 위한 다중 그룹의 정보 관리 기법을 제안한다. 제안 기법은 서로 다른 이기종의 장치에서 생성되는 사용자의 프라이버시 정보를 서로 다른 그룹에서 연계 처리할 수 있도록 연계 정보를 클러스터링하여 분산 관리할 수 있도록 하는 것이 목적이다. 제안 기법은 주기적으로 사용자의 프라이버시 정보를 동기화하도록 사용자별 프라이버시 정보를 가상의 공간에서 독립적으로 처리한다. 특히, 제안 기법은 확률기반의 블록 체인으로 사용자의 프라이버시 정보를 익명으로 생성되도록 계층적 구조의 다단계 접근을 통한 사용자의 프라이버시에 대한 접근성을 향상시켰다.

제안 기법은 5G의 이질적인 환경에서 사용자 프라이버시를 효율적으로 보호하기 위해서 다음과 같은 3가지 목적을 가진다.

첫째, 제안 기법은 5G의 이질적인 환경에서 사용자의 정보를 익명으로 손쉽게 접근하기 위해서 가상 환경에서 계층적 구조의 다단계 접근 방법을 사용한다.

둘째, 사용자의 프라이버시 정보를 서로 다른 크기의 코드로 분할하여 PCF(Policy Control Function)에 따라 AMF(Mobility management. Function)의 이동성 관리와 관련된 정책을 동적으로 제공한다.

셋째, 제안 기법에서 처리되는 사용자의 프라이버시 정보는 일정한 규칙에 따라 순서를 교체 분산 배치하도록 하여 사용자의 접근 용이성을 향상시킨다.

이 논문의 구성은 다음과 같다. 2장에서는 5G 보안 표준 및 기존 관련 연구에 대해서 알아본다. 3장에서는 사용자 프라이버시를 보호하기 위한 다중 그룹 정보 관리 기법을 제안하고, 4장에서는 제안 기법을 평가하고 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

2.1 5G 표준화 연구

5G 보안 관련 표준화는 ITU, NGMN, ETSI, 3GPP, 5G-PPP 등에서 추진하고 있다[6]. ITU는 특정 워킹 그룹 없이 8개 영역(데이터 보안, 통합 플랫폼, 가상화 통신망 보안, 서비스 접근, 데이터 무결성, IoT 보안, 내용 보호, 이용자 인증 등)의 5G 보안에 대해서 다루고 있다[7,8]. NGMN은 보안, 프라이버시, 식별자 등 5G의 Trust 요소에 대해서 활동하고 있다. ETSI(European Telecommunications Standards Institute)는 NFV(Network Function Virtualization)의 상호작용을 통한 4가지 Trust 형식(No delegation, Direct delegation, Collaboration trust, Transitive trust)을 정의하고 있다. 3GPP는 5G 시스템에 대한 보안 구조 및 절차를 재정의한 후 5G 인증 및 키 동의를 체결하였다. 5G-PPP는 5G 보안과 관련하여 8가지 분야(5G 보안 요구사항 및 위협, 5G 보안 구조, 5G에 대한 접근 제어, 5G 내의 프라이버시, 5G 내의 Trust 모델, 보안 모니터링 및 관리, Slicing/Virtualization 및 강력한 분리, 보안 표준화 추진 등)를 연구 진행하고 있다[9].

2.2 HetNet

HetNet(Heterogeneous Network)은 다수의 독립된 단말들이 기지국을 통해 서로 다른 용량의 신호들을 전송하는 네트워크를 의미한다[10]. HetNet는 기존 LET의 MIMO 방식과 비교하여 용량 증대 및 간섭 개선 효과에 대한 장점이 있다. HetNet을 사용하는 5 세대 이동통신망은 4세대 이동통신망보다 수 GHz 대역에서 수십 GHz 대역의 주파수를 사용하지만 셀 반경이 4세대 이동통신보다 짧아 기지국의 신호 처리량이 증가하는 단점을 가지고 있다. 5세대 이동통신은 HetNet 환경에서 다수의 스몰셀간의 간섭을 최소화하

려고 많은 기술들이 검토되고 있다. HetNet은 스몰셀 간 실시간으로 통계 제공이 가능하도록 설계되어 네트워크 품질 향상 및 운용 비용이 절감된다.

2.3 기존연구

5G 환경은 기존 구축된 인프라와 사회에서 요구하는 보안 위협에 대한 안전성을 더욱 요구하고 있다. Table 1은 5G 환경에서 가장 많이 발생할 수 있는 보안 위협을 분류하여 SDN, 가상화, 클라우드, 프라이버시 측면에서 기존 보안 기술들이 지원가능 유·무를 나타내고 있다. 기존 보안 기술들은 보안 위협으로부터 완벽하게 지원할 수 없는 제약적인 사항들이 존재하기 때문에 5G 환경에서 발생할 수 있는 추가적인 보안 기술들이 필요하다.

Z. Yan et al.은 5G 환경을 구성하고 있는 중간 장치들의 프라이버시 정책 관리 소홀로 발생할 수 있는 보안 문제점들을 정의하고 있다 [3]. L. T. Sorensen et al.은 이기종 장치간 서로 사용자와 데이터의 프라이버시를 공유했을 경우 기존에 존재하던 보안 문제 이외에 추가적인 보안 문제를 언급하고 있다 [4]. F. Kemmer et al.은 사용자 데이터가 서로 다른 클라우드 환경에 저장되었을 경우 서로 다른 레벨에 따라 데이터가 관리되어야 하는 구조를 제안하였다[5].

Table 1. Security Challenges in 5G Technologies

Security Threat	Software Defined Networking	Virtualization	Cloud	Privacy
Dos/DDos	√	√		
Configuration verification	√			
Access controal	√	√	√	
traffic isolation		√		
identity security				√
location security				√
integrity verification			√	
service access control			√	

3. 이질적인 환경에 따른 사용자의 프라이버시 다중 연계 처리 기법

3.1 개요

최근 5G 기술이 일반 대중들에게 서비스되면서 5G 환경에서 발생할 수 있는 보안 기술들에 대해 많은 관심을 가지고 있다. 특히, 휴대폰이 대중화되면서 사용자의 프라이버시 노출과 관련된 보안 요구사항이 증가하고 있다. 이 절에서는 5G의 이질적인 환경에서 사용자의 프라이버시 정보를 연계하기 위한 관리 기법을 제안한다. 제안 기법은 휴대폰과 같은 서로 다른 지역에서 동작되는 이기종 장치 내 사용자의 프라이버시 정보를 그룹 연계하여 처리할 수 있도록 연계 정보를 분산 클러스터링 한다.

제안 기법은 Fig. 1처럼 서로 다른 이질적인 환경에서 동작되는 이기종의 장치에서 발생되는 사용자의 프라이버시 정보를 서로 분산 연계 처리할 수 있도록 함으로써 서비스의 안전성을 향상시킬 수 있다. 특히, 제안 기법은 서로 다른 장소에서 사용자의 프라이버시 정보를 손쉽게 접근 제어하기 위해서 사용자의 위치정보와 상태 정보를 이진 값으로 구성하여 계층적으로 관리한다. 제안 기법은 이 같은 과정을 통해 주기적으로 사용자의 프라이버시를 동기화시킬 수 있을 뿐만 아니라 사용자별 프라이버시 정보를 가상의 공간에서 독립적으로 처리할 수 있다.

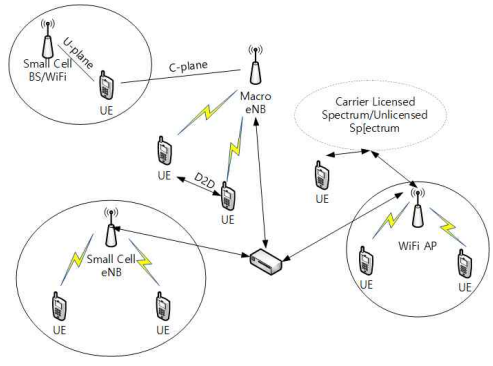

Fig. 1. Heterogeneous Networks

제안 기법은 5G의 이질적인 환경에서 사용자 프라이버시를 효율적으로 보호하기 위해서 가상 환경을 계층적 구조의 다단계 접근 구조를 구성하고 사용자 위치 정보에 따른 코드

부여를 통해 이동성 관리와 관련된 정책을 동적으로 제공하여 사용자의 프라이버시 정보를 일정 규정에 따라 순서를 교체 분산 배치하도록 한다.

3.2 계층별 사용자 프라이버시의 분할 가변 정보 연계

이 절에서는 사용자의 프라이버시 정보를 사용자 위치 정보와 함께 가변으로 분할한 후 분할 된 정보를 다중 해쉬체인으로 연계함으로써 사용자의 프라이버시에 대한 접근제어의 효율성을 향상시키도록 한다. 사용자의 프라이버시 정보를 분할하는 방법은 사용자가 소속된 그룹 관리자와 사용자의 프라이버시를 처리하는 지역 관리자로 구분한 후 지역 관리자에서 생성한 임의의 난수를 이용하여 그룹 관리자에 저장되어 있는 사용자 프라이버시 정보를 비교분석한다.

제안 기법은 그룹 관리자와 지역 관리자 사이에 서로 동의된 공유키 K_{SH}를 이용하여 식 (1)의 정보를 지역 영역에 위치한 사용자에게 전달한다. 식 (2)는 그룹 관리자에게 등록한 공유키 K_{SH}와 랜덤수(N_U, N_{CS})를 사용하여 인증 유·무를 그룹 관리자에게 승인받는다.

$$E_{PK_{CS}}(N_U),\ MAC_{K_{SH}}(N_U,\ Cert) \quad (1)$$

$$E_{PK_{CA}}(N_U,\ N_{CS}),\ h(MAC_{K_{US}}(N_U,\ N_{CS},\ ASI),\ Cert) \quad (2)$$

여기서, 난수 N_U와 인증서 $Cert$는 사용자가 사전에 등록한 정보이며, 난수 N_{CS}는 지역 관리자가 생성한 난수를 의미한다. PK_{CS}는 지역 관리자의 공개키를 의미하고, PK_{CA}는 그룹 관리자의 공개키를 의미한다.

인증이 승인되면 사용자의 프라이버시 정보의 연계 정도(DC)를 식 (3)처럼 생성한다. 생성된 연계 정도는 사용자의 프라이버시 정보의 정확도에 영향을 받는다.

$$DC = \frac{P(IV)}{P(IV)P(C)} \quad (3)$$

여기서 IV는 사용자 프라이버시 정보의 중요도를 의미하고, C는 사용자 프라이버시 사용 횟수를 의미한다.

3.3. 사용자 프라이버시 연계 처리

이 절에서는 특정 지역에서 사용되는 사용자의 프라이버시 정보에 대한 사용 현황을 연계 정보에 적용하여 특정 레벨에서 사용자의 프라이버시를 처리할 수 있도록 쌍대비교 행렬에 적용한다. 쌍대비교 행렬에 적용된 사용자의 프라이버시 정보는 다중 해쉬 함수에 적용하여 가변 정보로 처리한다. 사용자 프라이버시 연계 처리는 다음과 같이 4단계로 구성한다.

• Step 1: 특정 지역에 소속된 사용자는 프라이버시 정보와 위치 정보를 식 (4)처럼 쌍으로 묶어 프라이버시 정보에 대한 상관관계를 행렬로 분석한다.

$$PrivacyInfo_i = \begin{pmatrix} (0,0) & \cdots & (Privacy_{1k}, Location_{1k}) \\ \vdots & \ddots & \vdots \\ (Privacy_{k1}, Location_{k1}) & \cdots & (0,0) \end{pmatrix} \quad (4)$$

여기서, k는 사용자 프라이버시 사용 횟수를 의미한다. ($Privacy_{xy}$, $Location_{xy}$) 쌍 정보는 사용자 프라이버시와 위치 정보 간의 상관관계를 의미한다.

• Step 2: 특정 지역에 위치한 사용자는 자신의 프라이버시 정보가 지역에서 사용될 수 있도록 식 (5)의 과정을 통해 추출한다.

$$a_{nk} = a_{(n-1)(k-1)} + a_{(n-1)k} \ (\ n,\ k\ \rangle\ 1) \quad (5)$$

여기서, $a_i(1 \le i < q)$는 지역 관리자가 임의의 솟수 $q(q \ge n+1)$를 생성한 후 Z_q에서 임의로 선택한 사용자 프라이버시 정보를 의미한다. k는 a_i를 이용하여 변환된 이진수를 의미한다.

지역관리자는 식 (5)처럼 생성된 임의의 다항식의 성질을 이용하여 사용자의 프라이버시 정보 $a_{nk} = \binom{n-1}{k-1}$를 추출한다.

• Step 3: 제안 기법은 사용자의 프라이버시 정보 a_{nk}를 관계 성분으로 평가하여 사용자의 프라이버시 정보를 계층

적으로 나타낸다.

• Step 4: 제안 기법은 H_U: {0,1} → Z_N처럼 사용자의 프라이버시 정보를 표현한 후 계층적으로 다중 연계를 수행할 수 있도록 H_U: {0,1}* × Z_N → Z_p처럼 처리한다.

4. 평가

본 절에서는 5G의 이질적인 환경에서 사용자의 다중 연계 처리에 대한 평가를 수행하기 위해서 [11-15]의 연구를 바탕으로 보안 평가와 성능평가를 수행하였다.

4.1. 보안평가

4.1.1 구성 요소간 상호 인증

제안 기법은 임의로 생성한 개인키(p, q)와 공개키(N=pq, e)를 사용하여 구성 요소간 상호 인증을 보장한다. 인증된 사용자만이 5G의 이질적인 환경에서 사용자의 프라이버시를 다중 연계할 수 있다. 합법적인 사용자만이 사전에 등록한 비밀키 K_{US}와 랜덤수(N_U, N_{CS})를 가지고 있기 때문에 그룹 관리자의 인증 유·무를 승인받을 수 있다.

4.1.2 보안 키 설립

제안 기법은 그룹 관리자와 지역 관리자 사이에 서로 동의된 공유키 K_{SH}를 이용하여 사전에 등록한 사용자의 비밀키 K_{US}와 랜덤수(N_U, N_{CS})를 이용하기 때문에 사용자의 프라이버시는 그룹 관리자와 지역 관리자로부터 독립적이다. 따라서 제안 기법의 보안 키는 어떤 공격자도 키잉 자료를 공개하거나 가로채거나 세션 키를 얻는 것은 불가능하다.

4.1.3 Withstanding 프로토콜 공격

제안 기법은 그룹 관리자와 지역 관리자 사이에 서로 동의된 공유키 K_{SH}를 이용하여 지역 영역에 위치한 사용자에게만 전달하기 때문에 인증이 승인되면 사용자의 프라이버시 정보의 연계 정도는 사용자의 프라이버시 정보의 정확도에 영향을 받아 Withstanding 프로토콜 공격에 안전하다.

4.1.3 사용자 익명성과 비연결성

제안 기법은 지역 관리자와 그룹 관리자의 공개키를 이용하여 난수 N_U와 인증서 $Cert$를 암호화하여 사용자의 프라이버시 정보를 안전하게 전달할 수 있어 사용자의 익명성을 보장한다. 또한, 제안 기법은 사용자의 프라이버시 정보 a_{nk}를 관계 성분으로 평가하여 사용자의 프라이버시 정보를 계층적으로 나타낸 후 H_U: {0,1}* × Z_N → Z_p처럼 처리하기 때문에 그룹 관리자, 지역 관리자 그리고 사용자 간이 서로 비연결성으로 유지할 수 있다.

4.1.4 추적성

제안 기법은 제3자가 악의적으로 사용자의 프라이버시를 임의로 사용하는 것을 막기 위해서 특정 지역에서 사용되는 사용자의 프라이버시 정보에 대한 사용 현황을 연계 정보에 적용하여 특정 레벨에서 사용자의 프라이버시를 처리할 수 있도록 쌍대비교 행렬에 적용하여 추적성을 보장한다.

4.2. 성능평가

제안 기법의 성능 평가를 위해 시뮬레이션에 사용되는 파라미터 설정은 5세대 이동통신에서 지원하는 이기종 장치의 HetNet의 설정 정보를 참조하여 Table 2와 같이 설정하였다.

Table 2. Simulation Parameters for Performance Evaluation

Parameter	Setting
IoT	ARM11
Inter-site distance	300m~500m
Bandwidth	10MHz
Carrier frequency	2GHz
Path loass	38+30log10(R)
UE power class	23 dBm (200mW)
Max Pico TX/RX power	24dBm
Pico BS noise	6 dB
Min separation UE to BS	2 m,
Max output power	20 dBm

제안 기법은 이기종 장치들이 포함된 네트워크 공간 크기를 300m~500m 로 설정하고, 대역폭은 10MHz로 설정하였다. 주파스 대역은 2GHz 에서 38+30log10(R)의 경로 손실율을 설정하였다. 이기종 장치의 송·수신 전력량은 24dBm로 설정하고, 베이스스테이션의 노이즈는 6dBm으로 설정한다.

4.2.1 처리시간

Fig. 2는 HetNet 환경에서 이기종 장치간 사용자의 프라이버시를 다중 연계 처리할 경우 이기종 장치 수에 따른 서

버의 처리시간을 비교한 결과이다. 실험 결과처럼, 제안 기법은 사용자의 프라이버시 정보를 사용자 위치 정보와 함께 가변으로 분할하여 다중 해쉬체인으로 연계함으로써 처리 시간이 17.3% 향상된 결과를 얻었다. 이 같은 결과는 제안 기법에서 사용자의 프라이버시 정보를 소속된 그룹 관리자와 지역 관리자로 구분하여 임의의 난수를 통해 사용자 프라이버시 정보를 비교분석하였기 때문이다.

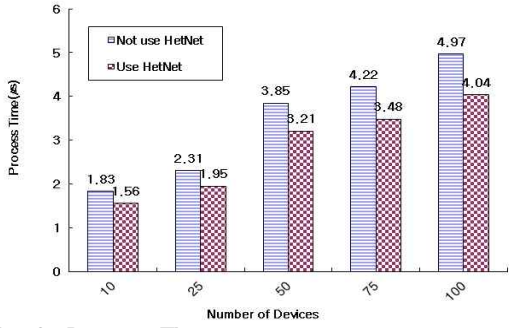

Fig. 2. Process Time

4.2.2 효율성

Fig. 3은 HetNet 환경에서 이기종 장치에 사용되는 사용자의 프라이버시 정보의 연계 처리 과정에서 발생할 수 있는 서버의 효율성을 평가한 결과이다. 실험 결과, 제안 기법은 HetNet 환경의 특정 그룹에서 사용자의 프라이버시를 연계하기 위해서 쌍대비교 행렬에 사용자의 프라이버시 정보를 이진 값으로 적용하여 해쉬 함수에 적용했을 경우 서버의 효율성이 평균 15.9% 향상된 결과를 얻었다. 이 같은 결과는 제안 기법이 특정 지역에 소속된 사용자의 프라이버시 정보와 위치 정보를 쌍으로 묶어 상관관계로 나타낸 후 행렬로 분석하였기 때문에 나타난 결과이다.

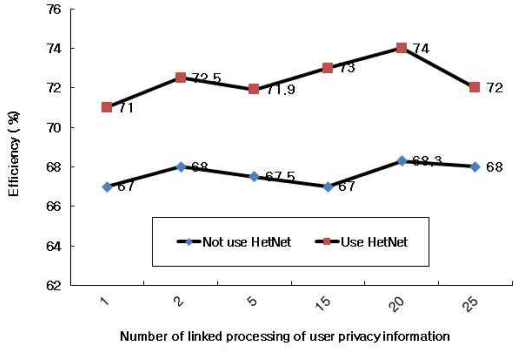

Fig. 3. Efficiency of Server

4.2.3 패킷 손실율

Fig. 4는 HetNet 환경을 구성하는 이기종 장치들이 사용자의 프라이버시 정보를 연계 처리하였을 때 발생하는 패킷의 손실율을 평가한 결과이다. 실험 결과처럼 제안 기법은 이기종 장치들이 구성되는 HetNet의 그룹 크기에 따라 사용자의 프라이버시 정보를 관계 성분으로 평가하여 사용자의 프라이버시 정보를 계층적으로 나타냈을 경우 패킷의 손실율은 평균 23.3% 낮게 나타났다. 이 같은 결과는 서버에서 주기적으로 사용자의 프라이버시를 동기화시킬 수 있을 뿐만 아니라 사용자별 프라이버시 정보를 가상의 공간에서 독립적으로 처리하기 때문에 나타난 결과이다.

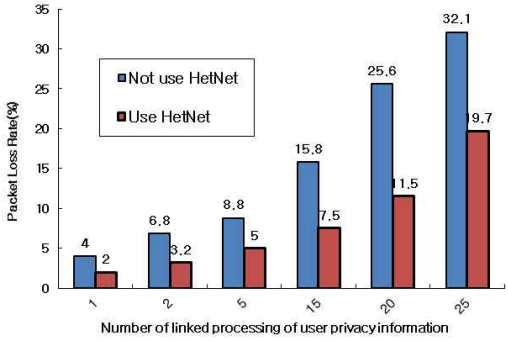

Fig. 4. Packet Loss Rate

5. 결론

최근 5G 서비스가 일반 사용자에게 제공되면서 새로운 서비스에 대한 기대감이 증가하고 있다. 그러나, 5G 서비스에 적합한 보안 기능이 완벽하게 제공되지 못하는 상황에서 사용자의 중요 정보는 제3자에게 악의적으로 갈취당할 수 있다. 본 논문에서는 5G의 이질적인 환경에서 사용자의 프라이버시를 효율적으로 보호하기 위한 다중 그룹의 정보 관리 기법을 제안하였다. 제안 기법은 서로 다른 이기종의 장치에서 생성되는 사용자의 프라이버시 정보를 서로 다른 그룹에서 연계 처리할 수 있도록 하였다. 제안 기법은 주기적으로 사용자의 프라이버시 정보를 동기화하여 사용자별 프라이버시 정보를 가상의 공간에서 독립적으로 처리할 수 있도록 계층적 구조의 다단계 접근을 수행한다. 향후 연구에서는 본 연구의 결과를 기반으로 5G 환경에서 운영되는 사용자 프라이버시 정책을 연구할 계획이다.

REFERENCES

[1] M. Agiwal, A. Roy & N. Saxena. (2016). Next Generation 5G Wireless Networks: A Comprehensive Survey. *IEEE Communications Surveys Tutorials, 18(3),* 1617-1655.

[2] N. Alliance. (2015). NGMN 5G white paper. *Next Generation Mobile Networks, White paper*.

[3] Z. Yan, P. Zhang & A. V. Vasilakos. (2016). A security and trust framework for virtualized networks and software-defined networking. *Security and Communication Networks, 9(16),* 3059-3069.

[4] L. T. Sorensen, S. Khajuria & K. E. Skouby. (2015). *2015 IEEE 81st Vehicular Technology Conference(VTC Spring),* 1-4.

[5] F. Kemmer, C. Reich, M. Knahl & N. Clarke. (2016). Software defined privacy. *2016 IEEE International conference on Cloud Engineering Workshop(IC2EW),* 25-29.

[6] D. J. Kim, Y. J. Jung & H. Y. Lee. (2018). Trends and Prospects for 5G Standardization. *2018,* TTA Special Report, 1-8. http://www.tta.or.kr/data/reportDown.jsp?news_num=5347

[7] X. Cui, P. Zhu, X. Yang, K. Li & C. Ji. (2014). Optimized big data K-means clustering using MapReduce. *Journal of Supercomputing, 70(3),* 1249-1259.

[8] B. Bahmani, B. Moseley, A. Vattani, R. Kumar & S. Vassivitskii. (2012). Scalable k-means++. *Proceedings of the VLDB Endowment, 5(7),* 622-633.

[9] Y. H. Kim, K S. Shim, M. S. Kim & J. S. Lee. (2014). DBCURE-MR: an efficient density-based clustering algorithm for large data using MapReduce. *Journal of Information Systems*, 42, 15-35.

[10] X. Cui, J. S. Charles & T. Potok. (2013). GPU enhanced parallel computing for large scale data clustering. *Journal of Future Generation Computer Systems, 29(7),* 1736-1741.

[11] J. Cao, M. Ma, Y. Fu, H. Li & Y. Zhang. (2019). CPPHA: Capability-based Privacy-Protection Handover Authentication Mechanism for SDN-based 5G HetNets. *IEEE Transactions on Dependable and Secure Computing*, 1-1.

[12] Y. Deng, L. Wang, K. K. Wong, A. Nallanathan, M. Elkashlan & S. Lambotharan. (2015). Safeguarding massive MIMO aided hetnets using physical layer security. *Proceedings of the 2015 International Conference on Wireless Communications & Signal Processing*(pp. 1-5).

[13] X. Duan & X. Wang. (2016). Fast authentication in 5G HetNet through SDN enabled weighted secure-context-information transfer. *Proceedings of the 2016 IEEE International Conference on Communications (ICC)* (pp. 1-6).

[14] T. Ma, F. Hu & M. Ma. (2017). Fast and efficient physical layer authentication for 5G HetNet handover. *Proceedings of the 2017 27th International Telecommunication Networks and Applications Conference (ITNAC)*(pp. 1-3).

[15] S. Sheikhzadeh. M. R. Javan & N. Mokari. (2017). Radio resource allocation for physical-layer security in OFDMA based HetNets with unknown mode of adversary. *Proceedings of the 2017 Iran Workshop on Communication and Information Theory (IWCIT)*(pp. 1-6).

김 겸 순(Kyoum-Sun Kim) [정회원]

· 1996년 2월 : 충북대학교 수학과 학사
· 2012년 2월 : 충북대학교 수학과 석사
· 2017년 2월 : 충북대학교 수학과 이학박사
· 2017년 3월 ~ 현재 : 충북대학교 시간강사
· 2018년 9월 ~ 현재 : 건국대학교 시간강사
· 관심분야 : 영상복원, 수치해석, 격자론
· E-mail : giunsun@naver.com

연 용 호(Yong-Ho Yon) [정회원]

· 1988년 2월 : 충북대학교 수학과 학사
· 1990년 2월 : 충북대학교 수학과 석사
· 1997년 8월 : 충북대학교 수학과 박사
· 2011년 3월 ~ 현재 : 목원대학교 교양교육원 조교수
· 관심분야 : 격자론, 수리논리, 함의대수
· E-mail : yhyon@mokwon.ac.kr

정 윤 수(Yoon-Su Jeong) [종신회원]

· 1998년 2월 : 청주대학교 전자계산학과 학사
· 2000년 2월 : 충북대학교 전자계산학과 석사
· 2008년 2월 : 충북대학교 전자계산학과 박사
· 2012년 3월 ~ 현재 : 목원대학교 정보통신공학과 조교수
· 관심분야 : 유·무선 통신 보안, 정보보호, 바이오인포매틱, 헬스케어, 빅데이터, 클라우드 컴퓨팅
· E-mail : bukmunro@mokwon.ac.kr