COVID-19 확산 방지를 위한 저전력 블루투스 기반 프라이버시 보호 접촉 추적 기술 동향 조사

김택윤, 김효원, 도상현, 김선우
한양대학교 전자컴퓨터통신공학과

{kty0264, khw870511, dduggy7, remero}@hanyang.ac.kr

A Survey of BLE based Privacy-Preserving Contact Tracing Technology for Combating COVID-19

Taekyoon Kim, Hyowon Kim, Sanghyun Doh and Sunwoo Kim
Department of Electronics and Computer Engineering, Hanyang Univ.

요 약

COVID-19, 일명 신종 코로나 바이러스 감염증 사태를 해결하기 위한 방안으로 스마트폰 앱을 이용한 접촉 추적 기술들이 제시되었다. 저전력 블루투스를 통해 인접한 단말을 식별할 수 있고, 수신신호세기 측정이 가능하다. 따라서, 근접도 산출이 가능하지만, 블루투스 단말의 기술적 문제, 접촉 추적에서 발생하는 보안 문제로 인해 한계점 또한 존재한다. 본 논문에서는 접촉 추적에서 발생하는 프라이버시 침해 문제 해결 방안으로 저전력 블루투스 기반 보호 접촉 추적 기술 동향에 대해 조사하였다.

Ⅰ. 서 론

한국은 이번 COVID-19 사태에서 훌륭한 방역 체계를 완성하여 수많은 외신의 찬사를 받았으나 공공의 이익을 위해 개인의 프라이버시를 침해하고 있다는 비판 또한 받고 있다. 감염자 동선 추적에서 개인 프라이버시 침해는 불가피하고 이에 대처하기 위해 올해 세계 각국에서 COVID-19접촉 추적과 관련해 프라이버시 보호 기술들이 개발 및 제안되었다[1]. 본 논문에서는 이러한 프라이버시 보호 접촉 추적 기술 중 스마트폰의 BLE(Bluetooth low energy) 기반 기술에 대해 조사하고, 현재까지 개발된 대표적인 프로토콜과 해당 기술의 한계점을 알아본다.

Ⅱ. 본 론

A. 기술 개요

스마트폰에 포함된 센서를 이용하는 경우 GPS와 블루투스를 사용할 수 있다. BLE는 주변에 있는 다른 단말들을 식별할 수 있고, BLE 인터페이스에서 제공하는 수신신호세기(RSSI) 측정으로 근접도(proximity) 산출이 가능하기 때문에 인구가 밀집해 있고 빌딩이 많은 도심지역에선 GPS 위치정보를 이용한 시스템보다 더 좋은 성능을 기대할 수 있다.

BLE 동작 단말은 서로 연결되기 이전 advertising과 scanning이라는 두가지 동작을 수행한다. Advertising은 broadcasting이라고도 불리는데, 할당된 advertising 물리 채널로 패킷을 보내는 동작을 말한다. Scanning은 advertising하는 단말과 연결할 의도를 갖지 않은 채 advertising 채널로부터 패킷을 받는 동작을 말한다. 근접 단말 인식, 접촉 판별 동작은 advertising 패킷을 통해 이루어지는데, 스마트폰 블루투스 비콘(beacon)은 보안을 위해 본인의 MAC 주소를 사용하지 않는다. 그 대신 일정 시간마다 변하는 random MAC 주소를 이용하므로 MAC 주소 외에 다른 단말을 식별할 방법이 필요하다. 그림 1은 후술할 애플과 구글이 제안하는 분산형 접촉 추적 시스템의 동작 구조이다.

먼저 A와 B가 접촉하면 앱을 설치한 스마트폰들이 임의로 생성된 ID를 포함한 블루투스 비콘을 교환한다.

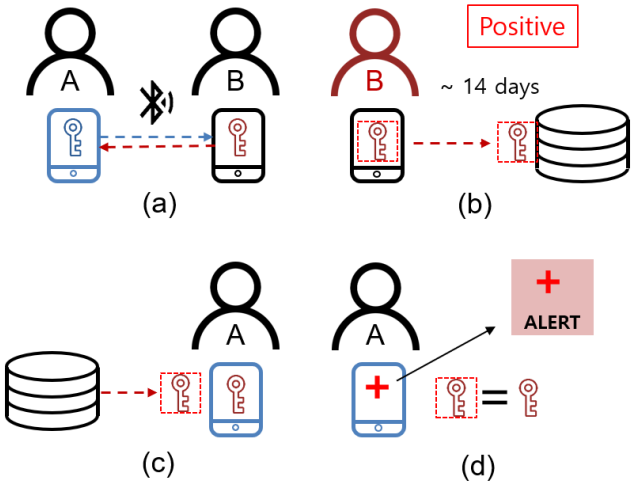

그림 1. Decentralized 접촉 추적 알림

두 기기가 근접한 상태로 일정 시간(약 15분)이 지나면 서로의 ID를 DB에 기록한다. DB에는 상대의 ID와 함께 본인이 교환에 사용한 ID도 포함된다. 후일 B가 확진 판정을 받으면 지난 14일간 B 본인이 생성한 ID를 모두 서버에 업로드 한다. A는 주기적으로 서버로부터 확진자의 ID를 다운로드하여 접촉한 기록과 일치하는 항목이 있을 경우 앱을 통해 알람을 보낸다.

서버에 데이터를 업로드 및 다운로드할 때, 어떤 데이터를 처리하는지에 따라 중앙집중형(centralized), 분산형(decentralized) 시스템으로 분류한다. 중앙집중형 시스템은 모든 기록을 서버로 업로드 한다. 보건당국에서 서버에 접근해 기록을 확인하고 접촉한 사람들에게 알람을 보낸다. 반면 분산형 시스템은 서버로 확진 환자 개인 기록만 업로드하고 앱을 설치한 다른 단말에서 이 기록을 다운로드해 접촉 여부를 판별하는 방식이다. 중앙집중형 시스템에 비해 프라이버시 보호에 이점을 갖지만 개인 단말로 연산 부하를 옮기는 형태이다. 어떤 시스템이 더 좋은 선택인지는 알 수 없으나 세계적으로, 특히 유럽에선 분산형 시스템을 더 선호하는 추세다[1].

그림 2. BlueTrace TempID 암호화 구조

B. 접촉 추적 프로토콜

코로나 바이러스 사태 이래로 수많은 접촉 추적 프로토콜들이 제시되었지만 본 논문에서는 대표적인 사례로 싱가포르의 BlueTrace, 유럽의 DP-3T, 애플과 구글의 ENF를 조사하였다.

BlueTrace: BlueTrace는 싱가포르 정부에 의해 처음 개발된 프로토콜로 세계 최초 민간에 공식적으로 도입된 싱가포르의 중앙집중형 접촉 추적 앱 TraceTogether에 사용되었다. 앱 사용자가 최초로 단말을 시스템에 등록할 때, 백-엔드(back-end)에서 개인 연락처에 기반한 고유 UserID 를 생성한다. 통신 시 UserID 와 여러 정보들을 함께 암호화한 TempID , RSSI와 추가 식별정보가 담긴 패킷을 교환한다. 그림 2는 패킷에 포함된 TempID 의 암호화 구조다. UserID, 현재 사용중인 TempID 의 생성, 만료시간, 무결성 확인을 위한 암호화 파라미터가 담겨 있다. 상호 교환된 정보들은 모두 단말의 데이터베이스에 저장되고 서버로 업로드 된다. 확진자 발생시 싱가포르 보건당국에서 기록을 확인, 개인에게 알람을 보낸다.

DP-3T: Decentralized Privacy-Preserving Proximity Tracing(DP-3T)는 유럽 다수 국가가 참여한 국제 컨소시엄 Pan-European Privacy-Preserving Proximity Tracing(PEPP-PT) 산하 프로젝트로서 PEPP-PT가 유럽 표준화 중앙집중형 시스템을 목표로 하는 반면 DP-3T는 분산형 시스템을 고려한다. DP-3T 프로토콜도 단말 구별을 위해 고유한 임시(Ephemeral) ID, EphID를 생성한다. 그림 3은 EphID 를 생성하는 방식을 그린 것이다. EphID는 일 단위로 바뀌는 비밀 키 시드(seed) SK_t 를 통해 생성되고, SK_t 는 전날의 비밀 키 시드 SK_{t-1}과 해시함수를 사용해 만든다. 단말은 SK_t를 이용해 하루동안 사용할 EphID 를 생성하고 이를 주기적으로 변경한다. 확진 환자 발생 시, 기기에서 확진자의 동의를 구한 후 최초 감염 추정일 i와 감염 추정일의 비밀 키 시드 SK_i 를 서버에 업로드한다. 앱이 설치된 다른 단말들은 이 기록을 다운로드해 자동적으로 감염된 날짜 이후에 확진자가 생성했던 EphID 를 계산하고 일치하는 기록이 있는지 판별한다.

ENF: 애플과 구글에서도 이와 같은 프라이버시 보호 접촉 추적 기술 개발에 협업을 시작했다(Apple-Google Exposure Notification, AGEN). ENF는 이 프로젝트의 프레임워크(framework)를 말한다. 앞선 설명처럼 ENF도 사용자 식별을 위해 주기적으로 변경되는 임시 ID로 통신하는데, DP-3T의 영향을 크게 받았기 때문에 개괄적인 작동 방식은 DP-3T와 동일하다. ENF와 기존 기술들의 가장 큰 차이점은 프로젝트 최종 단계에서 앱 설치 없이 Android와 iOS의 OS레벨에서 실행할 수 있게 개발된다는 점이다. 기존의 앱들은 백그라운드에서 실행될 경우 현저한 성능 저하가 일어나거나, Android 단말에서 보낸 패킷을 iOS 단말에선 읽을 수 없는 등 몇 가지 한계점이 있었다. 그러나 OS 제조업체인 애플과 구글에서 직접 이러한 문제를 해결하고 있다. 현재는 API 개발 중이며 다음으론 API를 이용한 개발 툴을 출시해 정부가 공식적으로 코로나 바이러스 접촉 추적 앱을 만드는 것을 목표로 하고 있다.

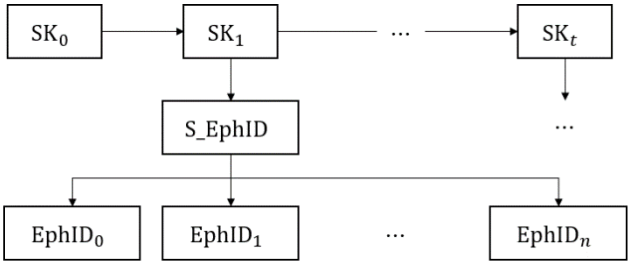

그림 3. DP-3T EphID 생성 방식

Ⅲ. 한계점 및 결론

최근 무선 이어폰과 같은 블루투스 단말이 대중적으로 보급됨에 따라 다른 블루투스 단말과 페어링(pairing) 되어 있는 등, 앱 동작 이외의 블루투스 기능으로 인해 예상되는 성능 저하는 매우 치명적이다. 또한 단말은 일정한 세기로 송신하지만 그 통계량이 바뀔 수 있다[4]. 잘못된 근접도 산출은 접촉 여부 판별에 영향을 줄 수 있다. 이런 문제들에 대한 해결책으로 BLE와 함께 GPS위치 정보 같은 문맥상 정보(context information)를 보조적으로 이용해 접촉을 판별하는 알고리즘도 제시되고 있지만 프라이버시 보호 측면에서 도입에 방해가 될 것이다. 패킷 구조가 정해져 있고 열린 공간으로 전송하는 시스템은 보안 문제가 발생하고, 패킷 스니핑(sniffing)을 이용한 중간자 공격(man-in-the-middle attack)은 시스템을 마비시킬 수 있다.

BLE 기반 접촉 추적 방식은 실현 가능성 있는 기술이 분명하지만 블루투스 기술 자체의 한계점, 사용자 동의에 의한 앱 기반 실행이라는 한계점으로 인해 현재의 접촉 추적기술을 완벽히 대체하는 해법이 될 수 없다. 또한 RSSI 측정에 기반해 접촉 여부를 판별하기 때문에 출퇴근 시간의 지하철과 같은 대규모 밀집 상황과 그렇지 않은 상황의 접촉 검출 임계 값이 유동적으로 바뀌어야 하는 등 아직 시나리오 설정도 개선의 여지가 많이 남아있다.

ACKNOWLEDGMENT

본 연구는 2020년 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터(No.2017-0-00316, 차세대 공공안전통신 원천기술 연구), 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터 육성 지원사업(IITP-2020-2017-0-01637)의 연구결과로 수행되었음.

참 고 문 헌

[1] J. Li, *et al.*, "COVID-19 Contact-tracing Apps: A Survey on the Global Deployment and Challenges." *arXiv preprint arXiv:2005.03599.* 2020.

[2] Apple and Google. Exposure Notification Bluetooth Specification v1.2, 2020. Accessed: Jul. 12, 2020 [Online]. Available: https://www.apple.com/covid19/contacttracing/

[3] C. Troncoso, *et al.*, "Decentralized privacy-preserving proximity tracing." *arXiv preprint arXiv:2005.12273.* 2020.

[4] J. Bay, *et al.*, "BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders." GovTech Singapore, Tech. Rep. 2020.