Technical Disclosure Commons

Defensive Publications Series

June 2020

Identifying Epidemic Candidates Using Mobile Devices

N/A

Follow this and additional works at: https://www.tdcommons.org/dpubs_series

Recommended Citation
N/A, "Identifying Epidemic Candidates Using Mobile Devices", Technical Disclosure Commons, (June 29, 2020)
https://www.tdcommons.org/dpubs_series/3389

This work is licensed under a Creative Commons Attribution 4.0 License.
This Article is brought to you for free and open access by Technical Disclosure Commons. It has been accepted for inclusion in Defensive Publications Series by an authorized administrator of Technical Disclosure Commons.

Identifying Epidemic Candidates Using Mobile Devices

Abstract:

This publication describes systems and techniques for identifying epidemic candidates utilizing mobile device location information. Through the use of beacons and cryptographic data, the privacy and location of a user of the mobile device are protected. The mobile device generates a beacon that includes cryptographic data, broadcasts the beacon via wireless communication from the mobile device, monitors for beacons communicated wirelessly, receives beacons from other mobile devices, stores beacons from other mobile devices for a configurable time period, communicates with a server to receive a beacon broadcast, calculates an identification using a timestamp included in the beacon broadcast, compares the calculated identification to received identifications in the beacon broadcast to determine a match that indicates exposure, and displays an alert to a user of the mobile device. A machine-learned (ML) model, on the device or at a server, can receive data associated with an exposure and analyze it. The ML model can use algorithms to make a recommendation, for example: recommend a candidate for testing.

Keywords:

Epidemic, coronavirus, COVID-19, incubation, direct exposure, indirect exposure, contact tracing, disease-risk information, near-field communication, long-range communications, proximity, carrier, candidate, hash value, non-reversible hash value, nonce, timestamp, cryptographic security, privacy, beacon, machine-learned model, ML model

Background:

In disease epidemics, for example, the current novel coronavirus (COVID-19), the objective is to be able to identify epidemic candidates (*e.g.*, individuals at risk for carrying the virus) as soon as possible to reduce disease spread. COVID-19 has an incubation period during which a carrier of the virus is asymptomatic; however, the carrier may still be spreading the disease to others. The virus is mainly spread through close contact and respiratory droplets produced when people cough and/or sneeze. The disease can persist on surfaces for significant periods of time. Once symptoms emerge for the carrier, it can be difficult to use contact tracing to identify candidates that the carrier was in proximity with (*i.e.*, direct exposure) as well as candidates that were in a shared space (*i.e.*, indirect exposure). This results in candidates only knowing about their infection with the disease after the incubation period for the disease. It would be beneficial to detect and notify candidates at risk for carrying the virus as early as possible before they have a chance to transfer it to others.

Mobile devices are ubiquitous, and many users have their mobile devices with them throughout the day to enable real-time communication and application use. A location of a mobile device gives a fairly accurate location of the user of that device. Mobile devices are able to communicate wirelessly directly with each other (*i.e.*, peer-to-peer networks) and/or with a local network. As a result, the location of a mobile device in relation to other mobile devices can give information about the proximity of the respective users of the mobile devices. It would be valuable to provide notifications to the user of the mobile device that they may have been in proximity of a disease carrier and unknowingly exposed.

However, a carrier of the disease and/or an epidemic candidate at risk for carrying the disease may be reluctant to share location and proximity information of their respective mobile

device due to privacy concerns. For example, carriers of the disease would not want candidates to know who the source of the disease transfer was. Additionally, it is important that confirmation of a positive test of a carrier is authentic so that candidates are not falsely alarmed.

Therefore, it is desirable to identify at-risk candidates for a disease using mobile device communication technologies without violating the privacy, medical status, and location history of a user of the mobile device.

Description:

This publication describes systems and techniques to utilize communications protocols on mobile devices to identify and notify direct and indirect epidemic candidates that were exposed to a carrier of a transmissible disease.

Throughout this disclosure, examples are described where a mobile device (or applications thereon) may analyze information (*e.g.*, location information, nearby networks, proximity data with other devices) associated with a user. Further to the descriptions above, a user may be provided with controls allowing the user to make an election as to both if and when systems, applications, and/or features described herein may enable the collection of user information (*e.g.*, proximity data), and if the user is sent content and/or communications from a server. For example, the user may need to download an application that performs proximity communications and sign up with a service using an identification in order to opt-in to the service. The mobile device can be configured only to use the user information after the mobile device receives explicit permission from the user of the mobile device to use the data. For example, in situations where an application analyzes proximity data to provide disease-risk information, individual users may be provided with an opportunity to provide input to control whether an application can access and make use of the

data. Further, individual users may have constant control over what applications can and/or cannot do with the information. In addition, information collected may be pre-treated in one or more ways before it is transferred, stored, or otherwise used, so that personally identifiable information is removed. For example, a user's identity may be transformed (*e.g.*, using a non-reversible hash value) so that no personally identifiable information can be determined for the user. The mobile device would not store any information persistently that would reveal location history (*e.g.*, Global Positioning System (GPS coordinates) because the system relies on exchanges of communications, it would not enable any entity (e.g., a user who was the disease carrier, a health institution) to be aware of the location history of the user or those who were in the vicinity of the user, and it would not enable a candidate to identify a source of disease transfer. Information that is cryptographically stored can be discarded after a time period. Thus, the user may have control over whether the information is collected about the user and the user's device, and how such information, if collected, may be used by the mobile device, an application, and/or a remote computing system.

A mobile device that can collect, process, and communicate proximity data can be a smartphone, tablet, smartglasses, and/or a smartwatch or any other devices with capabilities to detect and measure various forms of input data and communicate wirelessly. The mobile device can include one or more transceivers for transmitting and receiving data over a wireless network, a processor, a display, and computer-readable media (CRM). The mobile device can communicate with various wireless communication protocols including GPS, a wireless local area network (WLAN), for example, those based on the IEEE 802.11 standard (*e.g.*, WiFi, WiGig), and peer-to-peer communication (*e.g.*, Bluetooth, Bluetooth Low Energy (BLE), Ultra-Wideband (UWB)).

The CRM includes a proximity application and a machine-learned model. The proximity application represents functionality that generates a beacon that includes cryptographic data,

broadcasts the beacon via wireless communication from the mobile device, monitors for beacons, receives beacons from other entities, stores beacons from other entities for a configurable time period, communicates with a server to receive a beacon broadcast, calculates an identification using a timestamp included in the beacon broadcast, compares the calculated identification to received identifications in the beacon broadcast to determine a match that indicates potential exposure, and displays an alert to a user of the mobile device. Additionally, the proximity application may perform post-processing on beacon data to provide other data, as described below. The machine-learned (ML) model receives the data and analyzes it. The ML model can use algorithms to make a recommendation (*e.g.*, recommend a candidate for testing). The proximity application and/or machine-learned model can be provided to a mobile device via an application that uses existing application programming interfaces on the mobile device or can be part of the operating system of the mobile device. Alternatively, the proximity application and ML model can operate on a server that receives a summary of exposure information from the mobile device.

The process for identifying epidemic candidates using mobile devices requires multiple communication protocols and security measures to maintain user privacy. Figure 1 illustrates a secure process for alerting a user that they may have been in proximity to a disease carrier.

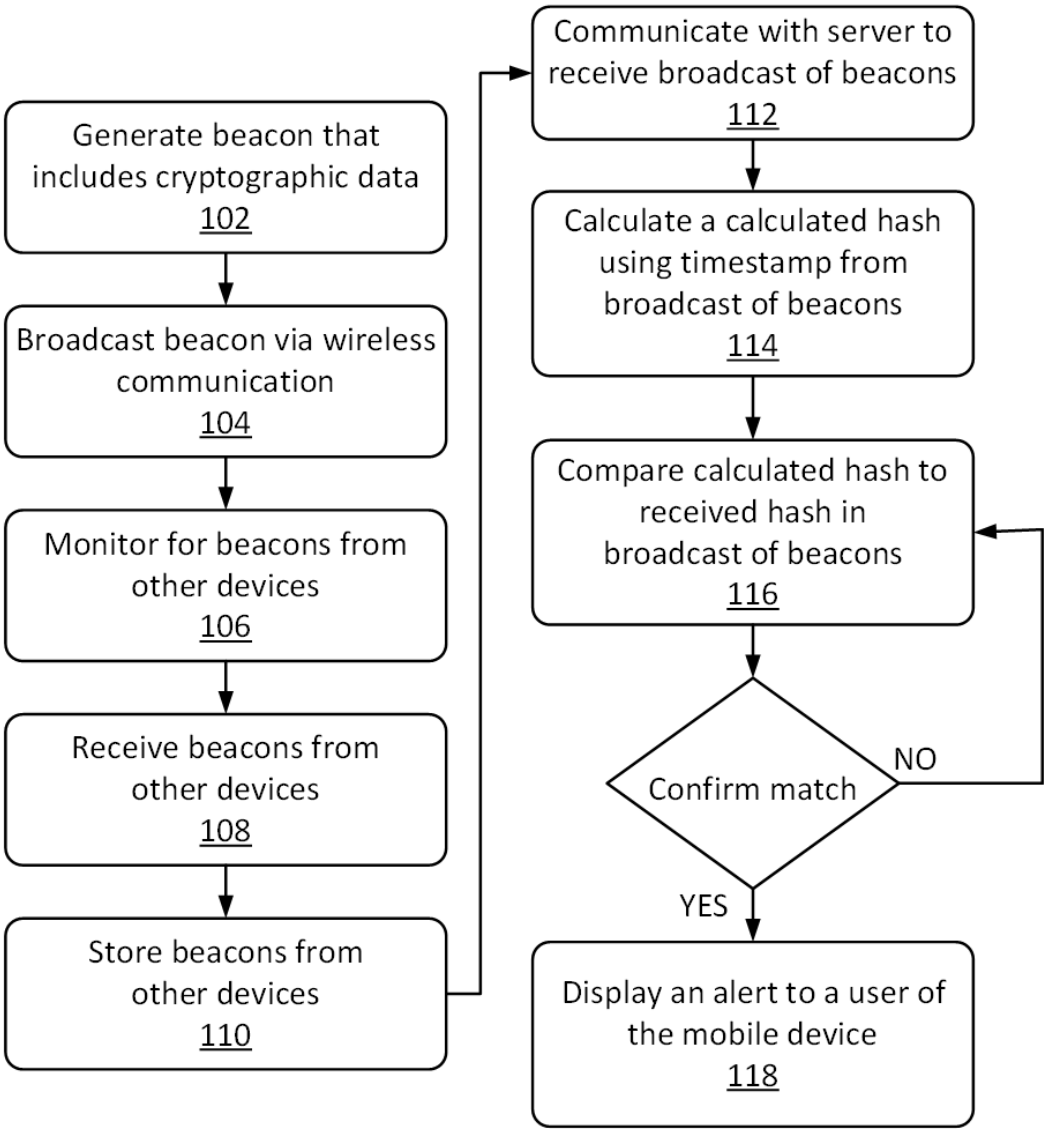

Figure 1

In a first operation at 102, a mobile device generates a beacon that includes non-reversible cryptographic security, for example, a hash value, for transmission. The hash value is generated using a timestamp of transmission based on a clock of the mobile device, and optionally, a nonce value that is generated and stored by the mobile device. At 104, the non-reversible hash value and the timestamp are included in a beacon that is broadcast from the mobile device using near-field peer-to-peer technology (*e.g.*, Bluetooth, BLE, UWB). This technology would have an expected range of a few feet to transmit the beacon to another device. The transmission distance can be

configurable and can use distance measurements (for example, Received Signal Strength Indication (RSSI)). Additionally or alternatively, the beacon can be transmitted via long-range communications (*e.g.*, WLAN) with a means to calculate the distance between the transmitting and receiving devices (*e.g.*, WiFi Round-Trip Time (RTT) technology, RSSI, etc.). The near-field and long-range communications may be used together to provide a better user experience. For example, to save power, the mobile device may use BLE and then trigger the WLAN radio to perform WiFi RTT to estimate distance. The WLAN radio may only be on when triggered to save battery life on the mobile device. To further save power, a user may be able to switch features off, or switching off features may be automated. For example, detection of the mobile device arriving or leaving a home network for a user may switch features off and on, respectively.

At 106, the mobile device monitors for beacons from other devices. The mobile device may use a configurable time period (*e.g.*, every 30 seconds) to discover beacons. At 108, the mobile device receives beacons from other devices. The devices may be mobile devices associated with users to detect direct exposure, or the devices may be associated with a location ("location devices") to detect indirect exposure. For example, location devices installed in a public place (*e.g.*, grocery store) could broadcast beacons that would be received by anyone in that broadcast area. The location devices may function as a virtual person for the duration between the exposure and the sanitizing of the location and/or the viability of the disease on surfaces. The location devices provide information about indirect exposure to the disease by a candidate who, for example, likely touched shared surfaces in a time period after a disease carrier was present at the location.

At 110, the mobile device stores beacons received from other devices for a configurable time period. The time period may be locally configured or broadcasted by a service. The period

should be close to the expected incubation period of the disease, and stored beacons significantly older than this period can be discarded to save processing and storage. The mobile device may not store every beacon it receives. For example, if the mobile device receives eight beacons consecutively from another device, it may only store the first and last beacon to save processing and storage. In another embodiment, the mobile device continuously uploads the beacons it receives to a database on a server to save storage on the mobile device. If the user of the mobile device tests positive for a disease, the beacon storage of the user device on the server can be authorized for beacon broadcast. However, as described below, calculations to confirm exposure are still done by individual mobile devices to protect users' privacy.

At 112, the mobile device communicates with a server to receive a broadcast of beacons that were stored on a device of a user who is confirmed as a disease carrier (hereinafter "carrier device"). It is important that the system is trustworthy, and it is recommended that only authorized entities (*e.g.*, health care professions) can mark "test positive" on any account to confirm a carrier. As discussed earlier, the user may need to sign up with a service using an identification (*e.g.*, an email) in order to opt-in to the service and to receive a broadcast of carrier device beacons. The broadcast of carrier device beacons from the server may be done periodically (*e.g.*, every few hours). The received of carrier device beacons includes hash values that were stored by the carrier device, each hash value ("received hash") with a corresponding timestamp. Additionally, or alternatively, the mobile device can periodically query a database on a server to retrieve carrier device beacons. The mobile device is able to use the upload date of confirmed disease carriers to avoid checking the same record in the database multiple times.

At 114, the mobile device calculates an identification ("calculated hash") using a first timestamp received from the server, the unique identification associated with the mobile device,

and the nonce value stored by the mobile device. The unique identification associated with the mobile device and nonce value will match the values used in operation 102 to generate a beacon. At 116, the mobile device compares the calculated hash to the received hash. If the calculated hash does not match the received hash, the mobile device can repeat operation 114 for the next received hash and corresponding timestamp. If the calculated hash matches the received hash, then the user's mobile device was the one that broadcast a beacon to the carrier device. Accordingly, this mobile device was in proximity, either directly or indirectly, with the carrier device. At 118, the mobile device displays an alert to the user of the mobile device.

The alert may include information associated with post-processing of the beacon data by the proximity application. Post-processing the beacon data can provide information, for example the count of consecutive beacons with hash matches to indicate a period of exposure, the number of bursts of beacons with hash matches that are time separated to indicate the frequency of exposure, timestamps to identify the stage of the disease of the carrier when exposed to the candidate, and distance between the carrier device and the mobile device. This information can be provided to an ML model to produce a risk assessment. The ML model can perform a risk assessment that can be used to prioritize candidates and display an alert, which may include a recommendation for a next action. Figure 2 illustrates an example of inputs to the ML model used to prioritize risk candidates.

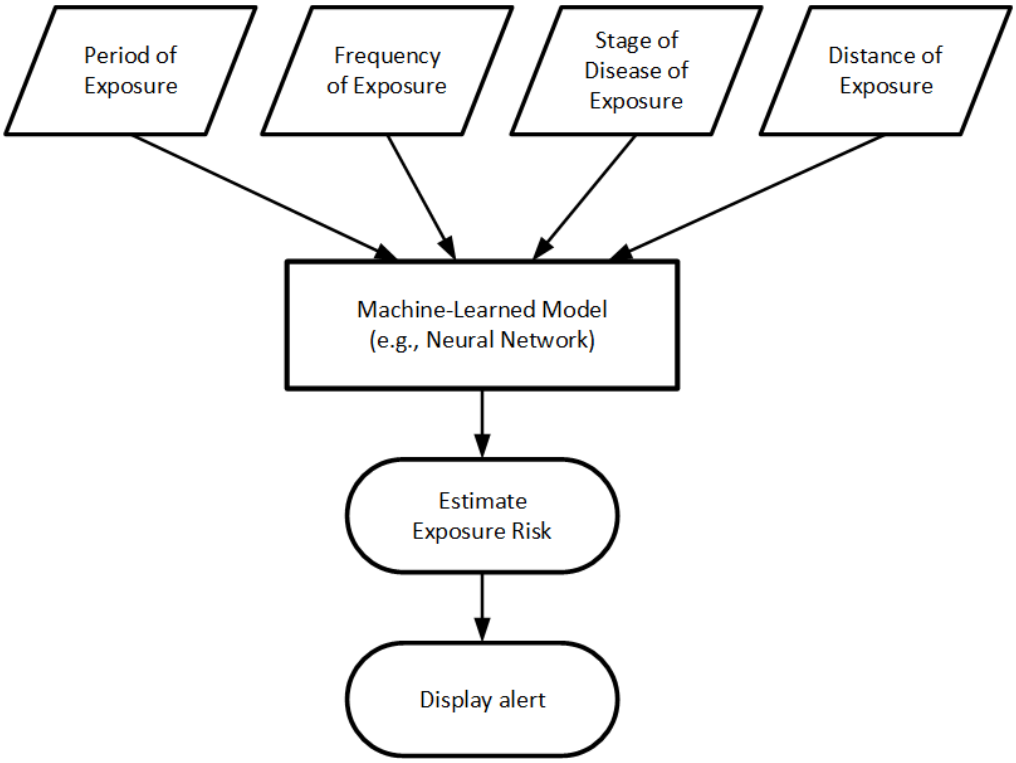

Figure 2

The techniques described allow candidates to be informed of exposure to a disease before they exhibit symptoms while protecting their privacy, medical status, and location history. Candidates can seek medical attention prior to developing symptoms and modify their routines to reduce the risk of infecting others.

References:

[1] Patent Publication: US 20100238023 A1. Method and Apparatus to Utilize Location-Related Data. Priority Date: March 15, 2006.

[2] Patent Publication: US 20140165158 A1. System and Method for Enterprise Security Through P2P Connection. Priority Date: December 6, 2012.

[3] Patent Publication: US 20060036619 A1. Method for accessing and analyzing medically related information from multiple sources collected into one or more databases for deriving illness

probability and/or for generating alerts for the detection of emergency events relating to disease management including HIV and SARS, and for syndromic surveillance of infectious disease and for predicting risk of adverse events to one or more drugs. Priority Date: August 9, 2004.

[4] Goyal, Shikha. "How to Use Aarogya Setu App, a Coronavirus Tracking App?" Jagran Josh, April 14, 2020. https://www.jagranjosh.com/general-knowledge/how-to-use-aarogya-setu-app-a-coronavirus-tracking-app-1585898723-1.

[5] Heaven, Will Douglas. "A New App Would Say If You've Crossed Paths with Someone Who Is Infected." *MIT Technology Review*, March 17, 2020. https://www.technologyreview.com/2020/03/17/905257/coronavirus-infection-tests-app-pandemic-location-privacy/.

[6] Sainz, Fred. "Apple and Google Partner on COVID-19 Contact Tracing Technology," April 10, 2020. https://www.apple.com/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/.