USC Viterbi
School of Engineering
Center for Cyber-Physical Systems and the Internet of Things

ANRG

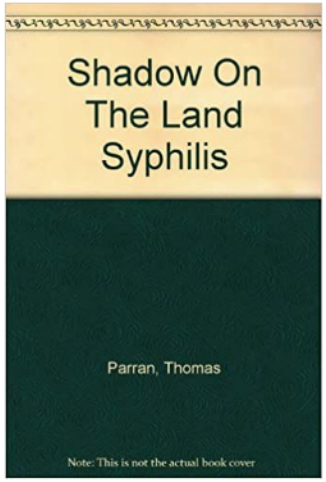
Privacy-Sensitive Mobile-based Contact Tracing for COVID-19

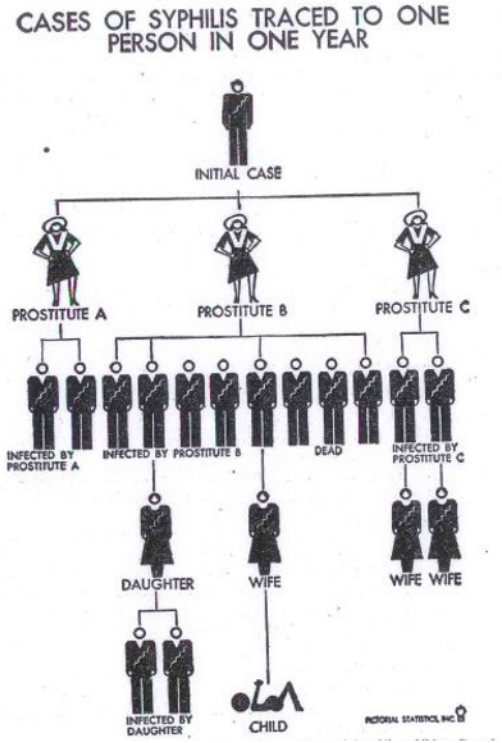
Bhaskar Krishnamachari
Department of Electrical and Computer Engineering

April 24, 2020

History of Contact Tracing

Credited to Dr. Thomas Parran Jr., Surgeon General of the United States (1936-1948)





USC mobile contact tracing study from 2008-2009

Findings from an Empirical Study of Fine-grained Human Social Contacts

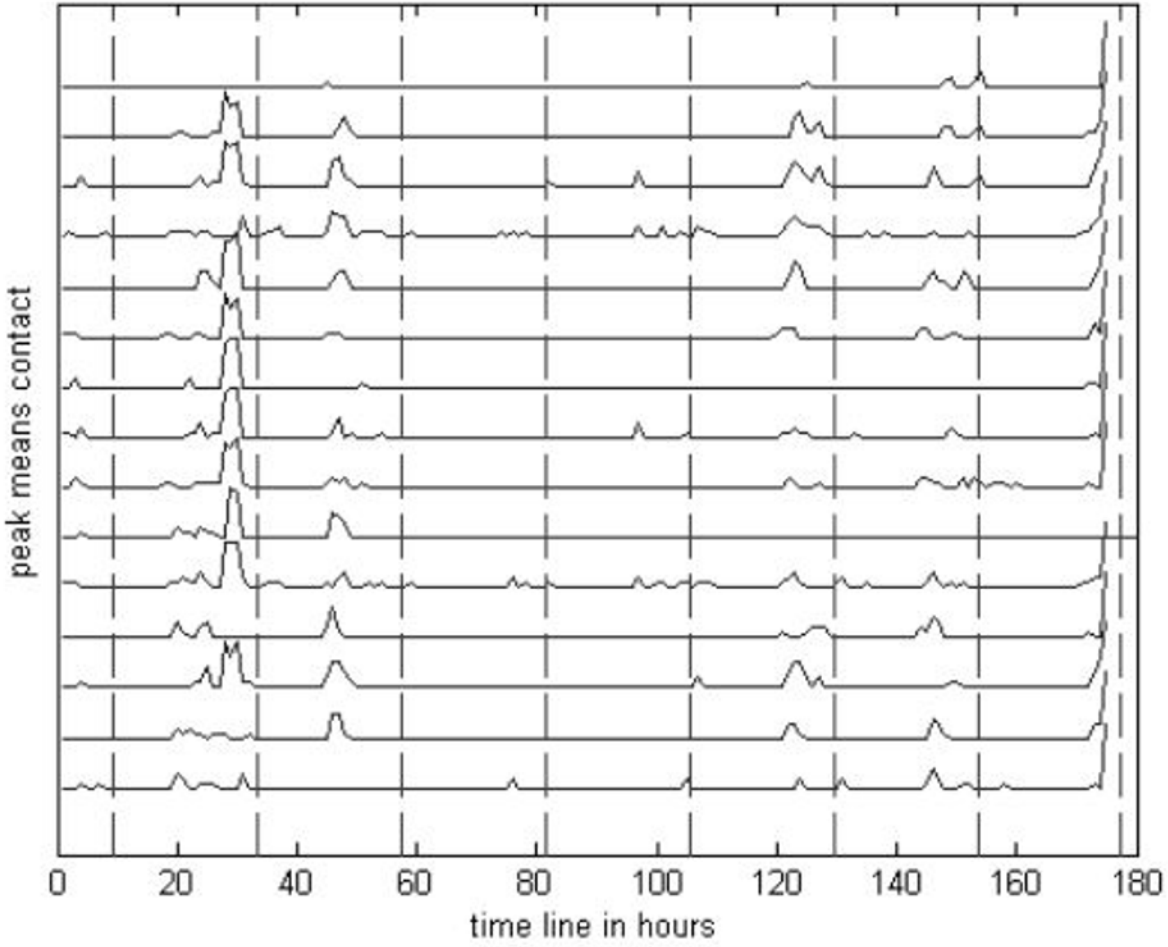
Yi Wang
Viterbi School of Engineering
University of Southern California
Los Angeles, CA 90089, USA

Bhaskar Krishnamachari
Viterbi School of Engineering
University of Southern California
Los Angeles, CA 90089, USA

Thomas W. Valente
Department of Preventive Medicine
University of Southern California
Los Angeles, CA 90089, USA

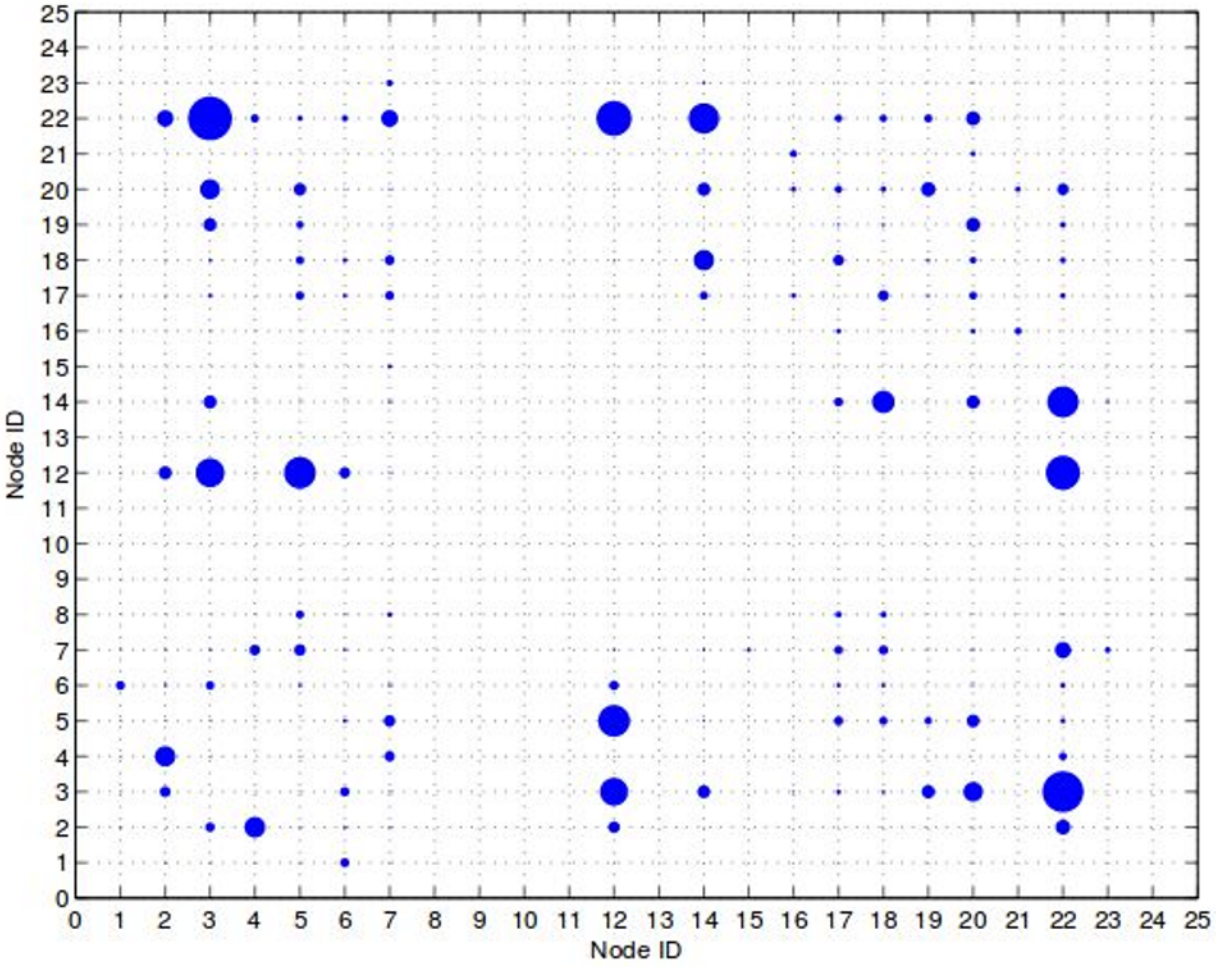
***Abstract*—An interaction based human contact study experiment has been conducted on 25 undergraduate students at USC, each carrying a wireless device (Tmote) for a week duration. Each mote transmits contact packets every 0.1 second to advertise its presence and a node receiving the packets will record the contact information. Data is processed off-line and a contact graph has been generated based on the strength of pairwise contact in order to visualize the grouping effect. All groups are identified and it has been found out that although most groups have small sizes and infrequent meetings, there exist large groups that have encountered several times in one week duration.**

Yi Wang, Bhaskar Krishnamachari and Thomas Valente, "Findings from an Empirical Study of Fine-grained Human Social Contacts", *The Sixth International Conference on* Wireless On-demand Network Systems and Services, February 2009.



Contact “Heart-beats”

For each student, showing how many other students were they in contact with through the course of the week



Contact Matrix

Frequency of pairwise encounters

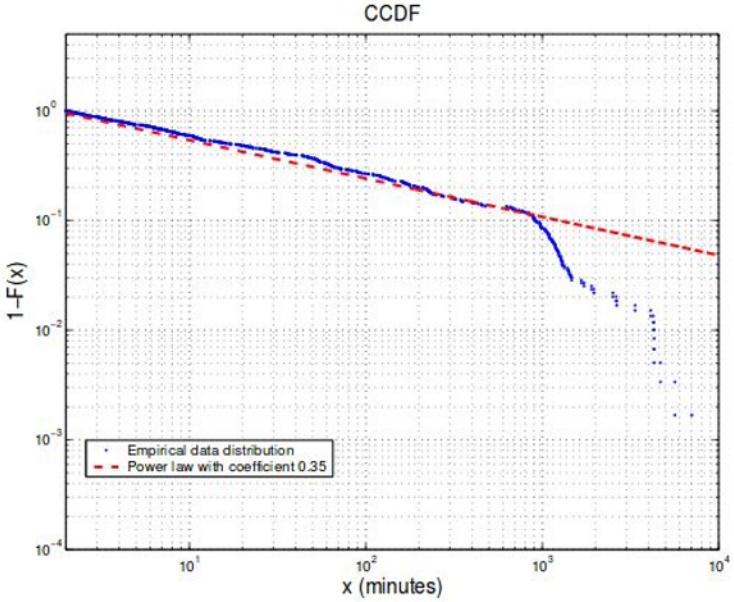


Fig. 7. Inter-contact time distribution (log scale).

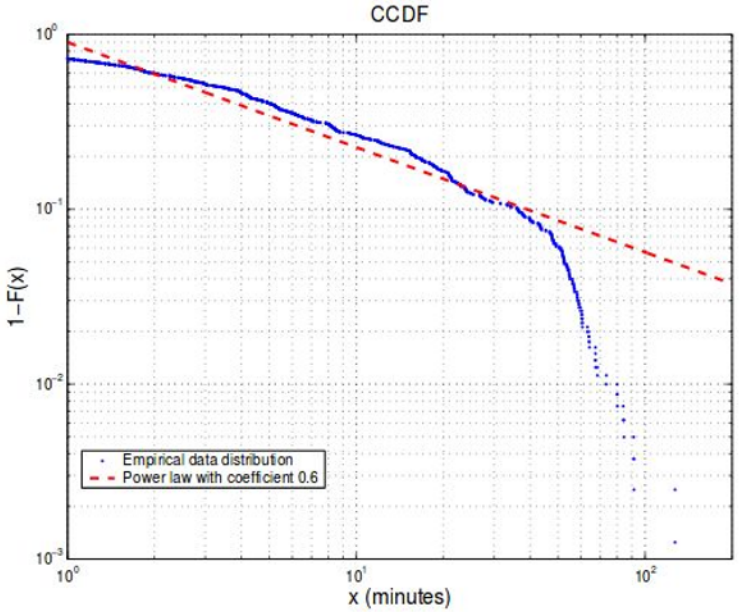
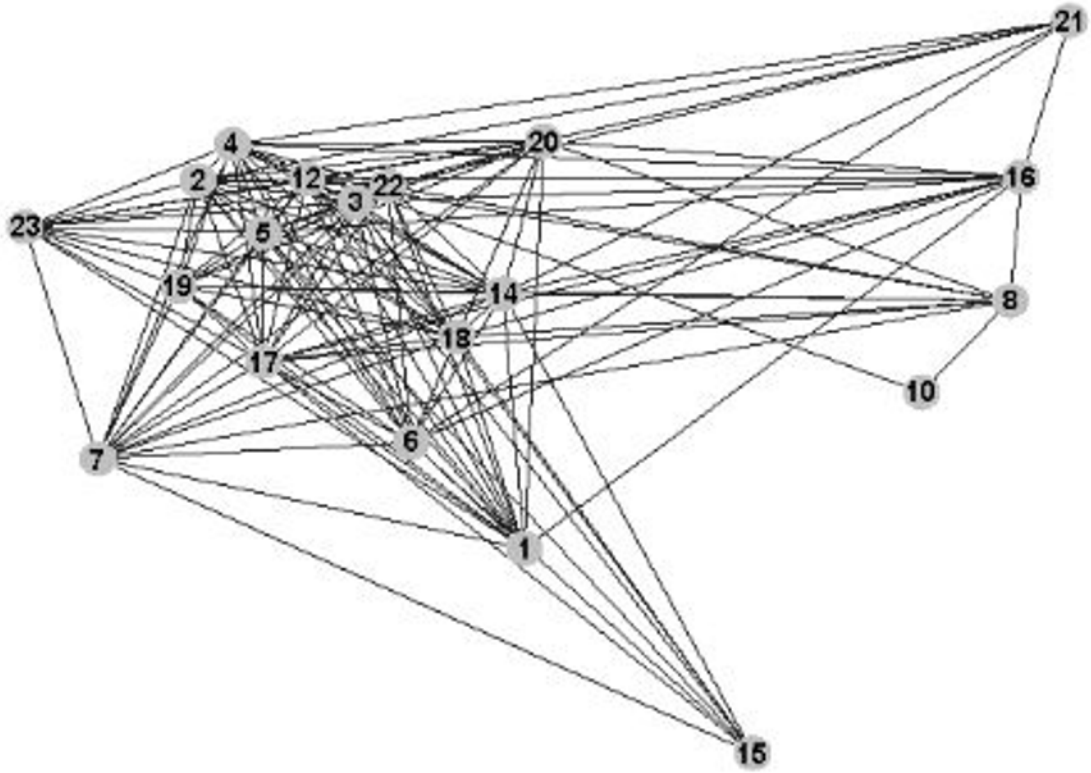


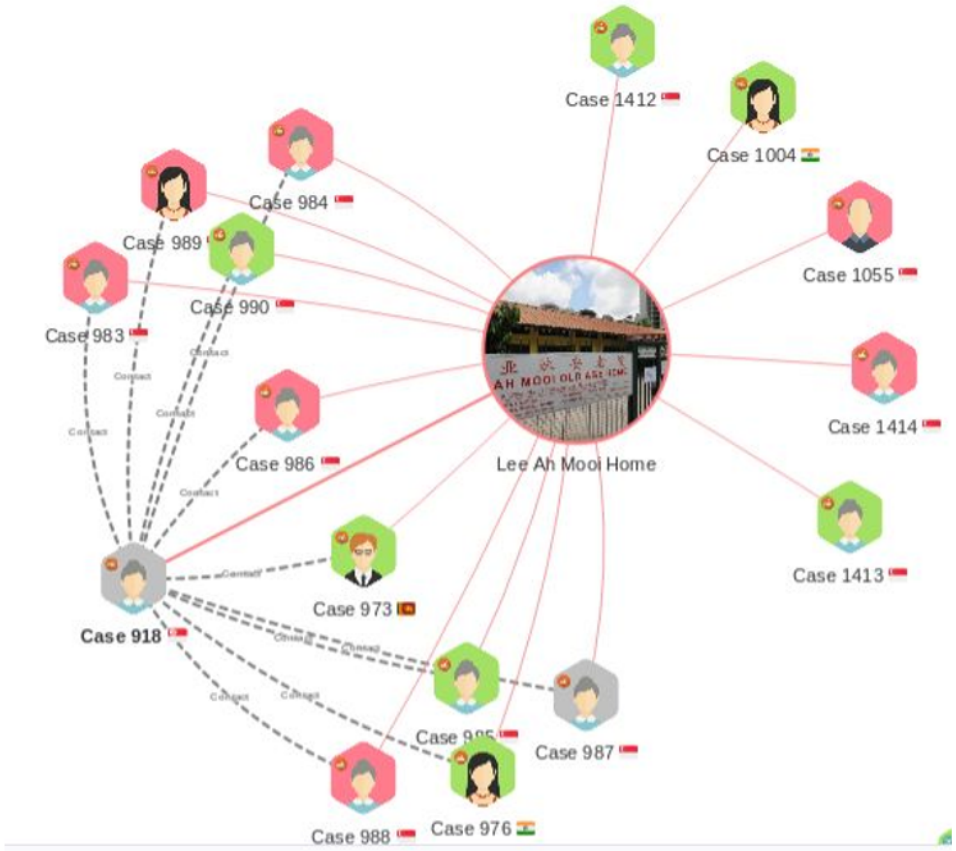
Fig. 8. Pairwise contact time distribution (log scale).

Contact Time and Inter-Contact Distributions



Contact Graph Embedding in Two Dimensions

Contact Tracing for COVID19



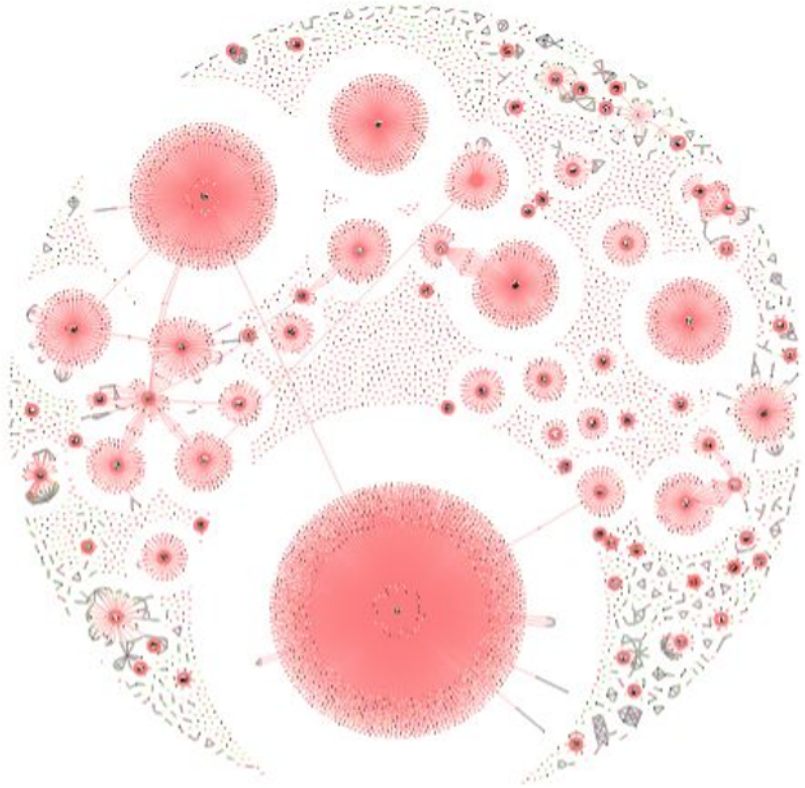
Case 918

Hospital: NCID

She was admitted on 31 March, and was confirmed to have COVID-19 infection on the same day. She passed away at 1:55am on the morning of April 3.

https://co.vid19.sg/singapore/cases

Contact Tracing for COVID19



https://co.vid19.sg/singapore/cases

Digital Contact Tracing for COVID19

How a mobile app helped China to contain the spread of covid-19?

2 min read . Updated: 01 Apr 2020, 10:56 PM IST

Srishti Choudhary

- An Oxford University study recommends countries to explore digital contact-tracing to speed up their preventive actions

75 million people have already downloaded Arogya Setu app

DISPATCH

SEOUL'S RADICAL EXPERIMENT IN DIGITAL CONTACT TRACING

In South Korea, the government is disseminating detailed tracking data on people with COVID-19.

Iran's coronavirus 'diagnosis' app looks more like a surveillance tool

Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends

Experts: Contact tracing in COVID-19 fight raises privacy concerns

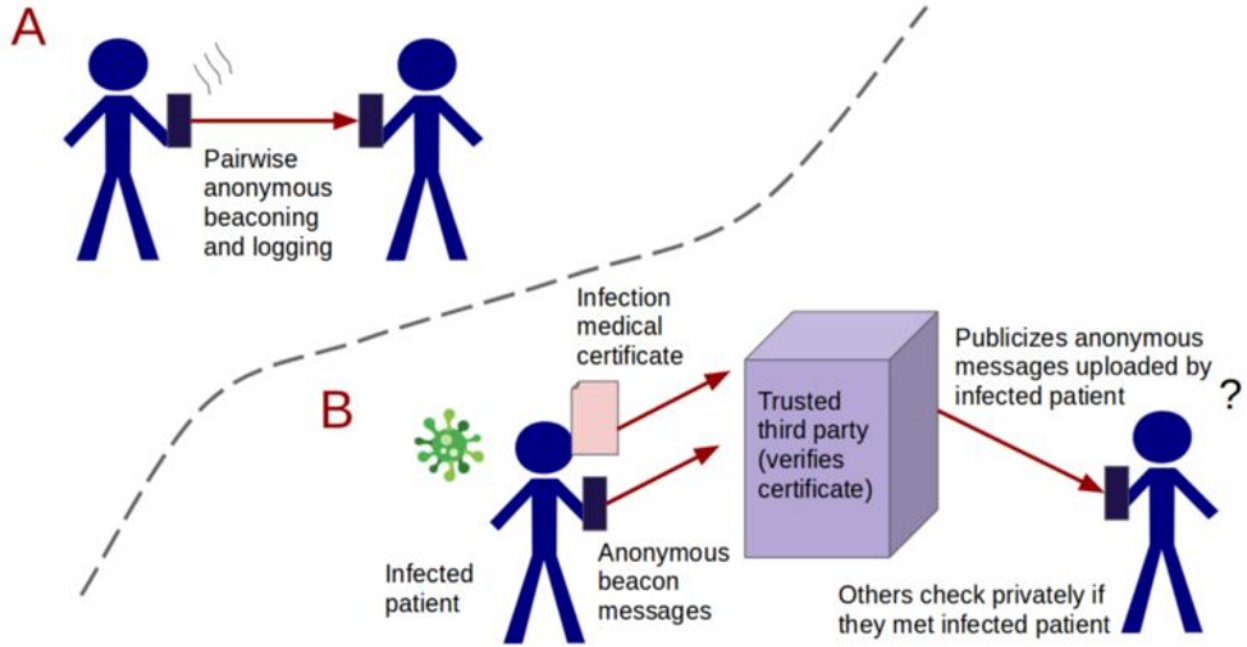
Coronavirus and privacy: The real issue with health surveillance

Bhaskar Krishnamachari
Mar 4 · 4 min read

Mobile app protocols for privacy-sensitive epidemic contact tracing

As the news about the novel Coronavirus (nCov-19 / SARS-CoV-2) grows, I have been pondering some way to use technology to enable contact tracing to help people determine quickly if they may be at higher risk. I believe it is particularly important to develop approaches that are privacy-sensitive and based on an opt-in approach. Here are two protocols I came up with, which could be potentially implemented as a mobile app. I would love to hear if

Privacy-Sensitive Contact Tracing via Mobile App



For more details see https://link.medium.com/oNay6EVI84

Arvin Hekmati, Gowri Ramachandran, and Bhaskar Krishnamachari. “CONTAIN: Privacy-oriented Contact Tracing Protocols for Epidemics“, https://arxiv.org/abs/2004.05251

Protocol 1: Encrypted Beacons

1. Each user periodically beacons, using Bluetooth, a message consisting of a unique name/ID, a time-stamp, and a random number (salt) that changes over time that is encrypted using a symmetric key. Users do not share this key with others.

2. Others that hear the encrypted message beacon log it locally.

3. Either periodically or in a batch, on an opt-in basis, each user can upload all the encrypted beacon messages they have heard to a common server.

4. If a user i becomes infected, they inform the server (with evidence that they are infected such as a medical report or “infection certificate”), which then proceeds to make all the messages uploaded by this user publicly available (still encrypted).

5. Each other user j can privately check these now publicly available encrypted messages (this could be automated) to see if they can decrypt any of them.

Protocol 2: Random Beacons

1. Each user beacons a sufficiently large (to minimize the chance of collisions with beacons generated by other users) random number and logs this random number locally.
2. Others that hear the beacon log this number locally.
3. Either periodically or in a batch, on an opt-in basis, each user can upload all the random beacon messages they have transmitted to a common server.
4. If a user i becomes infected, they inform the server (with evidence that they are infected, such as a medical report / “infection certificate”), which then proceeds to make all the random numbers uploaded by this user publicly available.
5. Other users periodically check the server and see if any of the numbers they have logged locally match those that were revealed by an infected user; if so they should proceed to get tested.

COMPANY ANNOUNCEMENTS

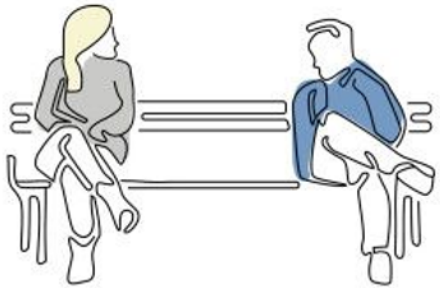
Apple and Google partner on COVID-19 contact tracing technology

Published Apr 10, 2020

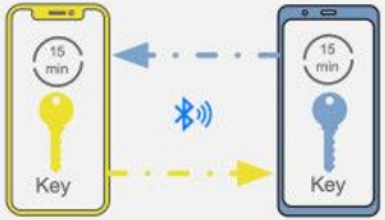
Across the world, governments and health authorities are working together to find solutions to the COVID-19 pandemic, to protect people and get society back up and running. Software developers are contributing by crafting technical tools to help combat the virus and save lives. In this spirit of collaboration, Google and Apple are announcing a joint effort to enable the use of Bluetooth technology to help governments and health agencies reduce the spread of the virus, with user privacy and security central to the design.

https://www.blog.google/inside-google/company-announcements/apple-and-google-partner-covid-19-contact-tracing-technology/

Alice and Bob meet each other for the first time and have a 10-minute conversation.



Their phones exchange anonymous identifier beacons (which change frequently).

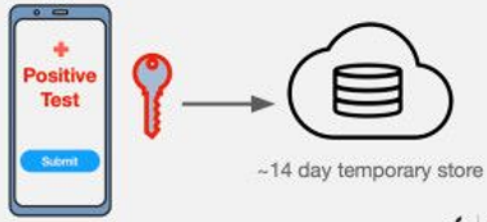


A few days later...

Bob is positively diagnosed for COVID-19 and enters the test result in an app from a public health authority.

With Bob's consent, his phone uploads the last 14 days of keys for his broadcast beacons to the cloud.

Apps can only get more information via user consent



Google

Related efforts on privacy-sensitive mobile contact tracing

- MIT Media Lab: https://www.media.mit.edu/projects/safepaths/overview/
- U. Washington: https://covidsafe.cs.washington.edu/
- EPFL: https://github.com/DP-3T/
- The Alan Turing Institute: https://arxiv.org/pdf/2004.04059.pdf
- CMU: https://www.novid.org/
- Covid Community Alert, https://coronavirus-outbreak-control.github.io/web/
- Coalition Network (nodle.io), https://www.coalitionnetwork.org/

See the annotated list of more than 50 Contact tracing app efforts from around the world maintained by USC undergrad Nina Tanaka at https://docs.google.com/document/d/1bgsNjPcvoz8fpOutEYiqCJpu2PWYHnGqPI3pcK9mUio/

Safeguards

https://www.eff.org/deeplinks/2020/04/challenge-proximity-apps-covid-19-contact-tracing

The Challenge of Proximity Apps For COVID-19 Contact Tracing

BY ANDREW CROCKER, KURT OPSAHL, AND BENNETT CYPHERS | APRIL 10, 2020

- Surveillance and Privacy Concerns
- Consent
- Minimization
- Security
- Transparency (open-source)
- Bias
- Expiration