Social distance safeguard

Purpose

- Identify and trace close contacts of positive Coronavirus cases with the purpose of slowing down spread of infection without the need to refuge to a state-based surveillance system that relies on location tracking and cameras and violates data protection regulations.
- Maintain the culture of social distancing during the Coronavirus pandemic.

Problem Statement

Current coronavirus crisis is expected to go on for a long time, it's very important that people stay conscious about social distance to prevent more infections and slow down the spread of the virus [1]. Beside Media campaigns, continuously alarming individuals to adhere to social distancing rules can play a key rule to keep the situation from deteriorating.

The definition of personal distance brings also the question of the meaning of close contact, this is particularly important in the context of backtracking individuals who potentially were infected by each case gets confirmed. Identifying those contacts quickly and applying quarantine measures enables us to stop the chain reaction and slow the spread of the virus.

A quick and effective backtracking system is especially important in:

- Slowing spread in places at earlier stages of the outbreak.
- Protecting vital sectors that have to stay running during lockdown
- preventing 2nd outbreak as the lockdown measures are gradually decreased.

Background

In response of the Novel COVID-19 virus flash widespread, WHO protective measures to public advised "Maintain at least **1 meter (3 feet)** distance between yourself and anyone who is coughing or sneezing." [2] , while CDC guidelines announced in March 22nd defines social distancing as "remaining out of congregate settings, avoiding mass gatherings, and maintaining distance **(approximately 6 feet or 2 meters)** from others when possible."[3]

Within the wide public response to the new measures on social media, this photo of a Italian man wearing a big ring in the market trying to keep people out of his personal space in such an eccentric way, **expresses the need for a tool to encourage social distancing** and to keep everyone self-conscious about crossing it in public spaces.

Another challenge is, to stop the virus' spread, health officials need to find and isolate the contacts of infected people quickly to prevent further infection.

an Oxford team designed a mathematical simulation of how "instantaneous digital contact tracing" would influence the spread of the virus. To stop the epidemic, health officials must reduce the virus' reproductive number—the average number of people each infected person transmits the virus to—to less than one. When the team modeled a scenario in which contacts were notified the instant a person tested positive, it was possible to push the reproductive rate of the virus below that threshold.[4]

Since backtracking can involve collecting personal data, Governments have been trying to balance between utilizing technology to effectively slow down the virus spread and protecting the privacy of its citizens.

This was tackled differently worldwide, China has reportedly relied on mass surveillance of phones to classify individuals by their health status and restrict their movements. [5] Other countries such as South Korea started effectively [6] using a combination of location data, video camera footage and credit card information, to track COVID-19 in their countries. With others recently catching up. [7]

But privacy experts raised concerns about how governments were using the data, how it was being stored and the potential for authorities to maintain heightened levels of surveillance, even after the coronavirus pandemic is over.

For countries with more stricter data protection laws such as the UK and Germany, this appears to be long struggle.[8][9]

As acceptance level for tracking grows higher, the need emerges for an alternative, namely a **less invasive and non-centralized monitoring system**.One idea this document is trying to implement is to **mimic virus spread** to collect information and send them **only whenever necessary and as much as necessary.**

Assumptions

- A solution that protects privacy and helps for effective tracking of Coronavirus spread can be a product of several solutions, while a peer-to-peer solution can provide granular data but in a very controlled scope, a centralized solution can receive aggregated data from telecom operators and help map the spread or detect trends of where and when people are congregating and risk spreading infection, a third solution can solely aim to monitor quarantined individuals.

- For both aforementioned use cases, a highly adoption rate by users is essential for any solution to succeed. "*It would be much more efficient to stop the spread of the coronavirus if everyone had the same app,*" quoting Sune Lehmann Jørgensen, a professor at the Technical University of Denmark who is advising danish government on how best to track the coronavirus.[10]

- Closed systems such as companies, factories and governmental offices can get an instant value of solution due to:
    - Guarantee of high adoption rate, almost every employee in the facility will use the tool as a part of facility regulation keeping the facility safe.
    - Known system boundaries introduce a better opportunity to improve the accuracy of the implemented solution.

Proposed Solution

The initial inspiration was to build some sort of virtual ring (inspired by the physical ring in the above-mentioned picture) that monitors a practical yet safe personal space of individuals without requiring any additional gear so that the solution is economical and quickly adoptable by the public.

Such a ring / tool will have two functions:

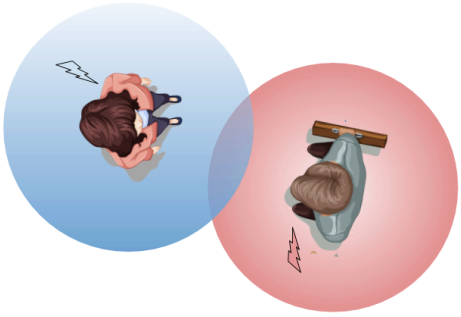
1. Similar to parking sensors in cars, the tool will notify two (or more) individuals when they enter each other's personal space. Typically a socially-awkward act done by one side or enforced by a third party (e.g. police). Warning both sides and keeping them self-aware can help maintain the new social norm.

2. record an exhaustive list of individuals who came in close contact with the owner as well as location and period of contact. In case the user is tested positive all individuals in such list will be automatically backtraced to their contact method (e.g. phone number) and notified instantly to start a self-isolation procedure, the list will also be broadcasted to infection control authorities which in turn can take necessary actions.
   UPDATE: Tracetogether and Private Kit tackle this part.

A smartphone app will monitor personal distance (1~1.5m diameter circle) using a proximity technology that is:

- widely adopted
- suitable for target range

If interference occurs, the App will record the contact and notify both users to keep their personal distance.



In addition to smartphones' high popularity and vast capabilities, proximity has always been a problem smartphone manufacturers tried to tackle, using several technologies to wirelessly assess distance of device from other devices/physical objects for different ranges that have different use cases.

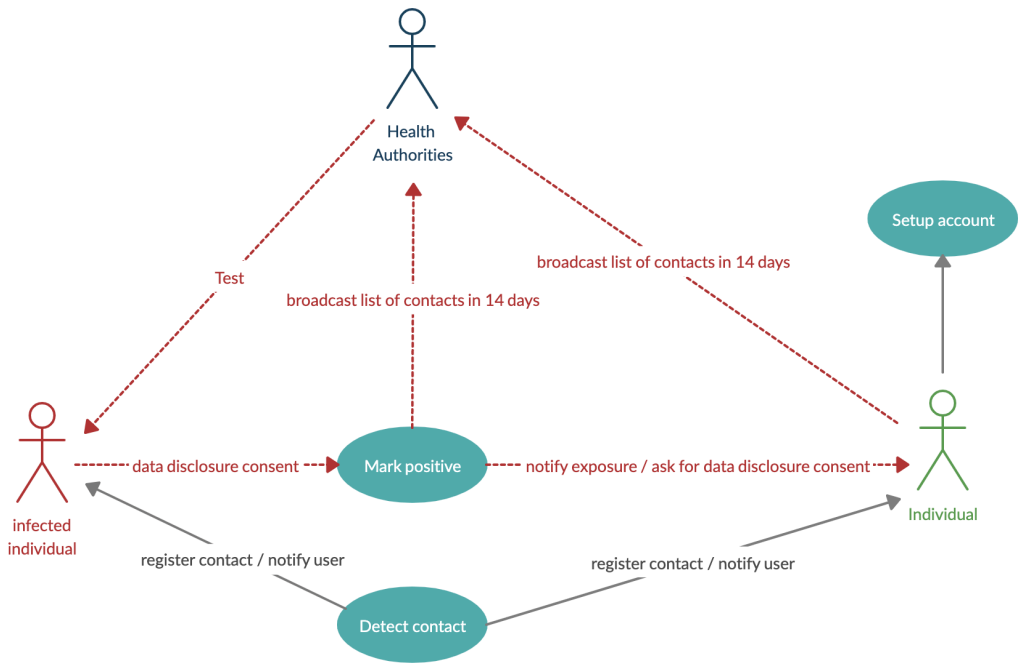
In comparison to location tracking systems, such peer-to-peer solution relies on proximity is thought to be able to:

- deliver nearly similar results without need to acquire / persist critical personal information of users, namely location information and thus, guarantee the privacy of users.
- scale up quickly with any number of users without the need of underlying expensive infrastructure.
- Avoid limitations of geographical tracking systems such as inaccurate indoors location tracking.

Requirements

- A single node is able to transmit and receive signals simultaneously.
- ±0.5m acceptable error making near range detection happen in 0.5~1.5 meters.
- Only contacts for more than 5 seconds are counted in.
- The signal produced by each node should not represent personal identity.

User Journeys



The below steps elaborates the interaction between individuals and health authorities:

1. Individuals will begin their journey by setting up an account, this will include device calibration and setting up contact methods and will obtain a certain encrypted unique Id that identifies a certain model of smartphone.

2. When two individuals approach each other at certain distance (assumably 1~1.5m) for certain period (assumably 5 seconds) a contact will be detected, as a call back both their phones will vibrate to notify them on contact and the Ids of each of them will be registered locally in other's application contact log.

3. When an individual is tested positive, they will mark themselves on the application signing a data disclosure consent and this will export the 14 days contact log to the account server which in turn will trigger a series of actions:
    a. Broadcast the contacts of the infected individual to the healthcare authorities along with any information about the contact point **the user chooses to disclose** such as location and period of contact or notes by the user.
    b. Notify individuals in list by tracing back Ids to contact method that they have been in contact with an infected person and:
        i. Giving them instructions on how to proceed / self isolate.
        ii. Requesting their consent on data disclosure policy for their last 14 days contacts.
        iii. Send the disclosed data to health authorities as consents are made.

Technical solution

For reference range of 1~2m the available technologies to measure proximity includes:

- Beacon technology based on low energy bluetooth BLE and implemented in iBeacon Eddystone standards by apple and google respectively, Altbeacon is also an open and interoperable specification.
- RFID (radio-frequency identification) which automatically identifies and tracks tags attached to objects. when triggered by an electromagnetic interrogation pulse from a nearby RFID reader device, the tag transmits digital data back.

A third proximity technology is NFC was excluded from this scope due to its extremely short range (within 10cm).

RFID usage also seems to be far-fetched. Even though passive tags are extremely cheap and available, for required range smartphone antennas cannot send interrogation radio waves and would require a reader hardware which makes this solution impractical for this use case.[11]

Beacon technology

- Beacon technology has been around since 2013 with not many advances but it has become widely supported by most smartphone devices, The most basic use of it is to determine how far a mobile device is from a beacon.[12]

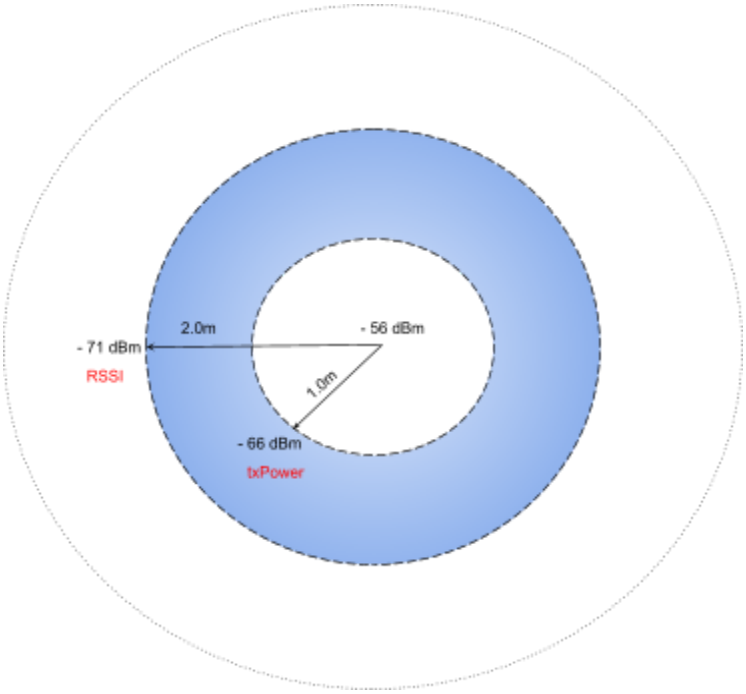
- Thousands of mobile apps depend on this technology — mainly for advertising, with dozens of libraries and APIs existing to utilize it.[13]

A brief description on how this technology works goes as follows:[1]

Each smartphone will both transmit (acting as a **beacon**) and receive packets from other nearby phones (acting as a **receiver**).

A beacon transmission packet will include a transmitter power field (txPower) that indicates how strong the signal should be at a known distance (e.g. 1 meter).

A smartphone will be first calibrated to send *txPower* by measuring the signal level at 1m (known as Received Signal Strength Indicator or *RSSI*) and then configure the beacon to transmit this value (in this example -66 dBm).



Each time a beacon advertisement packet is received, the bluetooth chipset in receivers will provide a measurement of the beacon's signal level as *RSSI*. Because every single beacon transmission also includes the calibration value *txPower*, it is possible to

[1] This is an oversimplified description of the solution. Calibration, noise filtering, calculations for different beacon models and techniques to improve accuracy is outside the scope of this document. More on that can be found in this blogpost.

compare the actual signal level with the expected signal level at 1m and then estimate the distance. In the figure, the beacon transmitted packet was received with a signal level of -71 dBm and the transmitter power calibration value sent inside the transmission was -65 dBm. Because -71 dBm represents a weaker signal level than -65 dBm this means the beacon is more than 1m.
A formula is used to calculate a distance estimate, calculations are implemented by libraries and vary based on beacon smartphone antenna, the calculation returns 2m in the above example.

Data processing

Making data submissions voluntary and anonymizing data are good options to maintain civil rights. It's a clean way of legally doing it.
Two great examples that implement privacy by design using contact tracing and provide a clear data policy are:

1. MIT's Private Kit released in 19/03/2020
2. Singapore government's TraceTogether released in 20/03/2020.

Risks

- Beacon technology advertised accuracy as "within centimeters" is questionable due to high variance in reading due to several factors[14] (e.g. RF interference, indoor/outdoor environmental factors, and obstacles) although some vendors proved it's possible to improve accuracy to acceptable limits.[15]
- Signal strength readings vary significantly over different Beacon vendors.[14]
- Nodes that are not running the app will not be detected by others, in case of poor adoption rate the solution will not be very effective

References

1. Why outbreaks like coronavirus spread exponentially, and how to “flatten the curve”
2. WHO Coronavirus disease (COVID-19) advice for the public
3. Interim US Guidance for Risk Assessment and Public Health Management of Persons with Potential Coronavirus Disease 2019 (COVID-19) Exposures: Geographic Risk and Contacts of Laboratory-confirmed Cases | CDC
4. covid-19_instant_tracing/Manuscript - Modelling instantaneous digital contact tracing.pdf at master · BDI-pathogens/covid-19_instant_tracing
5. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags
6. http://theconversation.com/coronavirus-south-koreas-success-in-controlling-disease-is-due-to-its-acceptance-of-surveillance-134068
7. Coronavirus Spy Apps: Israel Joins Iran And China Tracking Citizens' Smartphones To Fight COVID-19
8. Privacy activists fear the UK might spy on its own citizens to tackle COVID-19
9. Coronavirus: Jeder zweite Deutsche für Handy-Ortung
10. In fight against coronavirus, governments embrace surveillance
11. What Type of Smartphone Could Read RFID Tags? — Ask The Experts Forum
12. How beacons work in practice
13. rabschi/awesome-beacon: A curated list of awesome Bluetooth beacon software and tools.
14. A Measurement Study of BLE iBeacon and Geometric Adjustment Scheme for Indoor Location-Based Mobile Applications
15. How accurate are Estimote iBeacons?