DCD

Decentralized **C**omputation of **D**ensity

By **Amey Desai, Project CoCo**

Infection spreads through two main media : Direct **human-human transmission** and transmission through **contaminated surfaces/substances** (formite). Direct human transmission can be tricky to detect if there are **asymptomatic carriers**. DCD intends to detect these sources and aid in containment of infection at scale.

In a pandemic situation, the general strategy is to reduce the speed of spread or 'flatten the curve'. This approach reduces fatalities until a solution is found for the infection. To reduce the speed of spread, the simplest approach is to reduce the number of people that can possibly be exposed to infection. This is the basis of 'social distancing'. Even with social distancing, transmission from contaminated surfaces can still occur.

DCD (acronym) uses GPS data to spot crowded areas where exponential transmission may occur, locate contaminated surfaces and spot sources of spread that haven't been detected using traditional methods. DCD is a privacy-first initiative. All location data is securely stored only on the phone. No data ever leaves the phone. All communication to and from the server takes place using the **Tor protocol**.

A contaminated surface that transmits disease will be the point of intersection of any users it affects. By looking at common clusters, we can identify such locations. Similarly, the presence of asymptomatic carriers in a particular area can also be determined by DCD

Protocol

DCD divides the map into a grid with unit 10x10m. This is the limit of accuracy for mobile phone GPS systems.

Client Side (User's phone)

The mobile phone compares its location to the grid. For every grid unit it crosses into, it sets a stopwatch. If it remains in the grid for more than 300s, it

notes the grid and sends the grid's central coordinates to the server. Given that typical walking speeds are in the range of 1.5-3km/hr (0.42-0.83m/s), crossing a 10m path would generally take 12-25 s. We use the threshold of 180s to detect significant 'contact' with an area. 'Contact' refers to extended presence in an area, indicative of an increased probability of contact with other people/surfaces in the area.

Packets are routed through Tor, so the sender remains anonymous.

General location trails are stored securely on the phone. These are necessary for self-report triggered flagging. In addition, locations of visited clusters for the day will also be stored on the phone.

Server Side

The server maintains a list of grid coordinates and a counter for each coordinate. Given the high number of such grids due to the resolution(10^5/sq.km), only those points that are reported are stored. Data received in the preceding 2 hours is used for analysis, and total data from the past 48 hours is stored on the server.

When a packet is received the grid point counter is incremented by 1.

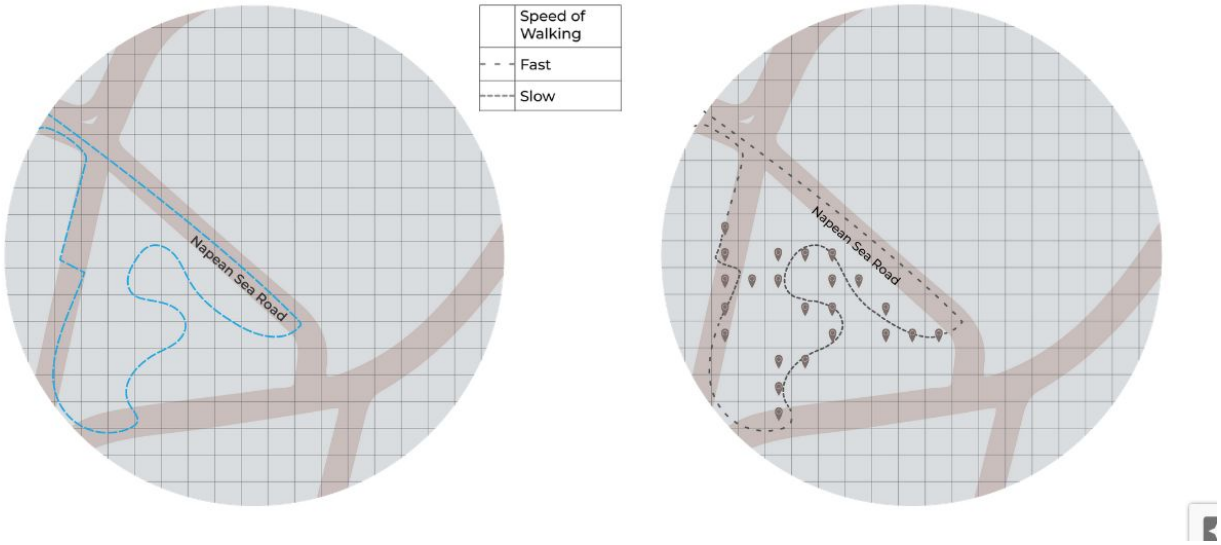
Map Visualization

Client Side

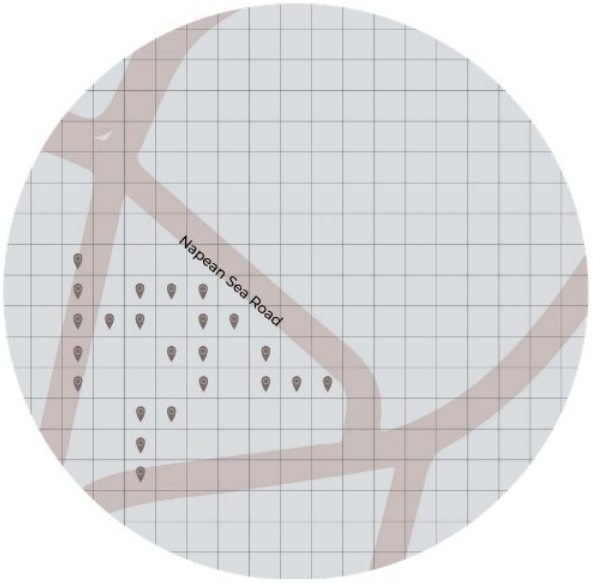
The mobile phone downloads the local density map from the server at regular intervals. Downloads are routed through Tor. Based on local cluster information, services like route optimization, travel recommendations, etc can function.

Server Side

A map will be rendered on the server, graphically representing density. A grid will only display when it's counter exceeds a threshold value of 20. The color of the grid will be used to represent relative density. Given social distancing norms, each person needs to maintain a distance of at least 1 m from others, thus occupying 3.14 sq.m on the ground. Thus about 31 people can safely occupy a 100 sq.m grid.



A B



C

Figure 1 Part A shows an example user trail. Part B shows reported locations. Grid cells where the user spends more than 3 minutes are reported. Only the reported locations are visible to the server, not the entire trail as shown in Part C.

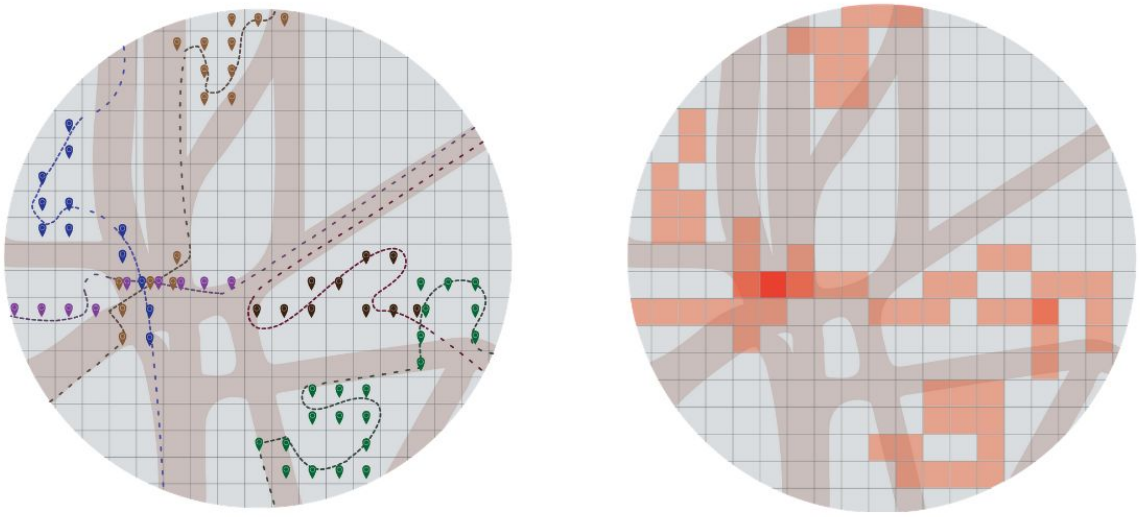


Figure 2 Identification of crowded locations. Only the flagged cells are visible to the server, which maps the crowd density in each cell which has more than the threshold for number of people.

Flagging hotspots upon self-reporting

When a user reports themself as positive, their visited clusters for the past week will be uploaded to the server. These will be flagged and notified to users according to the design policy

Preserving privacy when the number of users is low

Initially, a lower number of users can enable linkage attacks. To prevent this, a grid point on the map is only rendered when the number of users crosses a threshold

Flowing traffic

There may be scenarios where a moving crowd may be in present yet not register since individuals are moving faster than the threshold time. To overcome this potential blindspot, we liaise with bluetooth. We check the number of phones in the immediate vicinity (1 m). If the number exceeds a threshold, we check for time spent in the grid for a reduced threshold(1 minute as opposed to 3).