A CONTACT-TRACING MOBILE PHONE APP FOR SARS-COV-2 ERADICATION THAT MAINTAINS USER PRIVACY AND DATA PROTECTION **** DRAFT VERSION ****

Daniel Tang
Leeds Institute for Data Analytics*
University of Leeds
Leeds, UK
D.Tang@leeds.ac.uk

April 5, 2020

ABSTRACT

As of 2^{nd} April a large proportion of the global population are living under social distancing measures in order to control the spread of COVID-19. If these measures are successful, in a few months the prevalence in many countries will again be low. At that stage, contact tracing is likely to be an important part of the response in order to prevent a resurgence of the disease but simulations show(Tang, 2020) that manual contact tracing will be too slow and inaccurate to be effective. Here we describe the design of a mobile phone app that is capable of automatically tracing close contacts of users without compromising privacy.

***K*eywords** COVID-19, SARS-CoV-2

1 Introduction

Simulations show(Tang, 2020) that traditional methods of contact tracing will not be fast or accurate enough for successful containment of SARS-CoV-2 due to its high $R0$, high proportion of asymptomatic carriers and significant pre-symptomatic transmission. The only chance of containing the virus is by using technology to implement extremely fast and accurate tracing. Efforts in China have demonstrated that this can be achieved, but implementation in western countries is more challenging because user privacy and data protection must be preserved.

2 Design of a mobile phone app

We propose the use of a mobile phone app which turns on the phone's Bluetooth connection. A randomly chosen 8-character string is assigned to be the name of the connection[2]. If another phone with the app installed comes within 2 meters for one minute, then each phone will locally store the random Bluetooth name of the other's along with it's own Bluetooth name. The Bluetooth name of each device will change every two minutes to a new, randomly chosen string.

As a person travels through the community, the app will collect the Bluetooth names of all encounters, along with its own randomly chosen names during those contacts. Because these are randomly generated they can't be used to identify anyone or track their movements. Names of encounters over 3 weeks old are deleted.

For the UK, if 63 million users create a name every 2 minutes for 3 weeks, then there would be 9.5×10^{11} active names. There are 2^{64} possible 8 byte names so the probability that a randomly created name will clash with an existing one is approximately 5×10^{-8}. This is acceptably small.

If a person tests positive, all the exchanged Bluetooth names of contacts stored on that person's phone are made public on the Internet. Since these are just random strings, no sensitive information is disclosed. Every few hours, all apps will check the published numbers against their own locally stored record of Bluetooth names they have used. If there is a match of 8 or more numbers, the user can be notified that they are at risk and should self-isolate and be tested.

*This project has received funding from the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No. 757455)

[2]If it is possible to spoof the bluetooth MAC address then this should be done too to further protect privacy

In this way, all close contacts of a newly confirmed case (as long as they are using the app) can immediately be informed that they are at risk. The only limitation being the uptake of the app and the compliance of the user with advice to self isolate. A recent survey(Abeler, 2020) shows that public support for an app is high in the UK and that around 74% of respondents would probably or definitely install a contact-tracing app.

3 Measuring distance

When a new Blootooth device is detected, the received signal strength (RSSI) is used as a first approximation of the physical distance. If possible, apps should fix the tx-power of the bluetooth antenna to a standard value. If the received signal strength goes above a threshold an optional alarm is sounded[3]. The device whose name string has the lowest binary value sounds the alarm first. The alarm serves to alert the user that another person is near, but also serves to calibrate the Bluetooth signal strength/distance relationship for the current pair of devices in the current surroundings. Encoded within the alarm sound is the Bluetooth device name of the sender and that of the potential close contact (encoding could be done, for example, by using frequency shift keying and an error correcting code such as Reed Solomon). The close-by device listens for this alarm and has exactly one second to decode and process it. Once the alarm is recognised and the recipient name is matched, exactly one second after the receipt of the beginning of the alarm, a response alarm is sent back to the original sender. The original sender can now approximate the distance between devices by measuring the time from sending the original alarm and receiving the response, subtracting 1 second, multiplying this by the speed of sound in air and dividing by 2. Exactly one second later the original device sounds a second alarm in order to allow the other device to also calculate distance. If at any point the communication fails either of the devices can initiate a repeat alarm after waiting for an exponential backoff time.

Speed of sound in air is approximately 340 ms^{-1}, so in 1 microsecond sound would travel around 0.34mm. The timing of the alarms can be made accurate to a few tens of microseconds without any particular difficulty so the accuracy of this technique is adequate for the current purposes.

Once the actual distance is found, it can be used to calibrate the RSSI to distance model. It has been shown(Zhou & Pollard, 2006) that, for positive values of RSSI, distance can be approximated as

$$d = A10^{-\frac{R}{20}}$$

where d is the distance, R is the RSSI signal strength and A is the unknown we need to calibrate.

If calibration is not possible by this method, due to background noise or muffled/muted phone then calibration falls back to a standard value based on the make and model of the users phone. A community-generated database of these standard values for all phones could be made available online.

4 Aggregate contact monitoring through opt-in data gathering

If, as seems likely, the contact tracing is going on within a context of other social distancing measures, people could opt to allow the app to submit the number of close contacts they have each day along with (again optionally) information about the respondant. This would allow governments to closely monitor the effectiveness of different policy measures in reducing the aggregate daily number of contacts, and allow them to respond to local outbreaks effectively while minimising disruption to peoples lives.

5 Optional scientific research

The app could also be used to perform scientific research. The spread of a "virtual disease" could be studied by reserving one of the bits in the Bluetooth name and using it to denote infected or not infected with the virtual disease. It could then be observed how the virtual virus spreads between members of a set of volunteers.

6 Gamification

In order to encourage people to use the service and to encourage social distancing in public places, perhaps the app could be gamified. Perhaps there could be an in-app pet that the user must look after, and for every real-world close contact, there's a chance that the in-app pet gets infected. The longer the user manages to keep the pet healthy, the more points awarded and the faster the pet will grow from a baby into a healthy adult.

References

Abeler, J. e. (2020). Support for app-based contact tracing of covid-19. Retrieved from "https://osf.io/huqtr/"

[3]The following requires access to the devices microphone so the user can optionally deny this access

Tang, D. (2020). Contact-tracing strategies for sars-cov-2 eradication. Retrieved from "https://osf.io/p67v9/"
Zhou, S., & Pollard, J. K. (2006). Position measurement using bluetooth. *IEEE Transactions on Consumer Electronics*, *52*(2), 555–558.