DECENTRALISED, PRIVACY-PRESERVING INFERENCE FOR MOBILE PHONE CONTACT TRACING OF SARS-COV-2

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

April 30, 2020

ABSTRACT

With the announcement of Apple and Google's partnership to introduce a contact-tracing functionality to iOS and Android, it seems increasingly likely that contact tracing via a smart-phone will form an important part of the effort to manage the COVID-19 pandemic and prevent resurgences of the disease after the initial outbreak.

When deciding whether a person should be isolated, tested or released, information about test results and symptoms of that person's contacts can help inform the decision. However, the privacy preserving nature of the Apple/Google contact tracing algorithm means that centralised curation of these decisions is not possible. Here we present a decentralised algorithm that estimates the posterior probability of viral transmission events and evaluates a user's risk rating while preserving user privacy. The algorithm is a message passing algorithm, so each smart-phone can be used to execute a small part of the algorithm without releasing any sensitive information. In this way, the network of all participating smart-phones forms a distributed computation device that performs Bayesian inference and informs each user when they should start/end isolation or be tested.

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

1 Description of the problem

Suppose we have a society where mobile-phone contact tracing is in operation. When enabled phones come close they exchange proximity IDs (PIDs) which are numbers derived from a daily exposure key. The phones keep a log of the PIDs along with the time of the contact and the daily exposure keys. If anyone tests positive for SARS-CoV-2, a subset of their daily exposure keys are published on a public server. Each day, everyone's phone checks for newly published exposure keys and must assess their risk of exposure and decide whether to raise an alarm telling the user to self-isolate and arrange a test.

The problem we consider here is how to calculate whether to raise an alarm/perform a test while maintaining a users privacy about the nature of their close contacts.

2 Expressing the joint probability over transmission events

If two people, A and B, are in close contact and broadcast PIDs a and b respectively, then there is a chance $P(\tau_{a\to b})$ that A will transmit the virus to B and a chance $P(\tau_{b\to a})$ that B will transmit the virus to A. Our aim is to calculate the marginal posterior probabilities of these events, given all the tests/observations that have been done on all people to date. When we talk about transmission, we mean the movement of vital viral material from one person to another such that if the other person was susceptible, they would become infected. Transmission to an already infected person is still a transmission event, but has no effect.

*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)

So, at a time t, each smart-phone, i, has a log of close-contacts $C_i(t) = \langle c_{i1}...c_{im}\rangle$, where each $c_{ij} = \langle t_{ij}, a_{ij}, b_{ij}\rangle$, t_{ij} is the time of the contact, a_{ij} is the PID that user i broadcast at time t_{ij} and b_{ij} is the PID broadcast by the other participant.

The binary random variables $\tau_{a_{ij}\to b_{ij}}$ take values either 1 or 0. A value of 1 denotes the event that a transmission occurred from the user who broadcast a_{ij} (i.e. user i) to the user who broadcast PID b_{ij}. A value of 0 denotes the event that no they had a close contact but no transmission occurred in that direction.

When a contact first occurs, the user has no information about the other participant so the probability of transmission from others is set to a prior probability. Up-to-date regional prior probabilities can be downloaded from publicly available servers and the phone can estimate its current region from the name/ID of the most recently connected cell tower (this information will always stay local on the phone).

2.1 Conditional probability of transmission

If person A has a close contact at time t, what is the probability that they will transmit the virus to the other participant given that their log of close contacts from the start of the log at $t = 0$ up to time t is $C(t) = \langle t_1, a_1, b_1\rangle$ ... $\langle t_n, a_n, b_n\rangle$?

Define the *first-exposure time* to be the earliest time that A was exposed to the virus and let $\epsilon(t)$ be the event that the first exposure is at time t. We assume that there is a constant rate, ρ, of exposure from the environment (e.g. from surfaces or close contacts that were missed for any reason). Given this, then the probability density of first exposure since the start of the log is

$$P\left(\epsilon(t)|C(t)\right) = \left(\rho + \sum_{i=1}^{n} \delta(t-t_i)\tau_{a_i\to b_i}\prod_{j<i}(1-\tau_{a_j\to b_j})\right)e^{-\rho t}$$

Define the *disease onset time* to be the earliest time that an infected person has a non-zero probability of transmitting the disease and let $\delta(t)$ be the event that disease onset occurs at time t. If we assume that there was no infection at the start of the contact log then

$$P(\delta(t)|C(t)) = \int_0^t P(\delta(t)|\epsilon(t_\epsilon))P(\epsilon(t_\epsilon)|C(t))dt_\epsilon$$

where $P(\delta(t)|\epsilon(t_\epsilon))$ represents the incubation time of the disease and is taken to be a Weibull distribution $P_w(t-t_\epsilon)$.

Given the disease onset time, the infectiousness of a person at time t is a measure of the probability of transmission in a close contact. Let $\iota(t) = p_\tau$ be the event that a person is in the state of viral shedding etc. such that they have the probability p_τ of transmitting the virus should they have a close contact at time t.

$$P(\iota(t) = p_\tau|C(t)) = \int_0^t \delta(\iota(t|\delta(t_\delta)) - p_\tau)P(\delta(t_\delta)|C(t))dt_\delta$$

where $\iota(t|\delta(t_\delta))$ represents the clinical course of the disease and is taken to be a Beta distribution $P_\beta(t-t_\delta)$

Given a person's infectiousness, we assume that a close contact is a Bernoulli draw, based on that person's infectiousness.

$$P(\tau(t)|\iota(t)) = B(\tau(t), \iota(t))$$

Suppose we have a number of tests $\xi_1...\xi_n$ that give us information about whether a person is infected with SARS-CoV-2. The characteristics of the n^{th} test are defined by it's specificity, $P(\xi_n^-|\bar{i})$, which gives the probability that a person will test negative on test n given that they are not infected, and it's sensitivity $P(\xi_n^+(t)|\delta(t_\delta))$ which gives the probability that a person tests positive on test n at time t given that they had disease onset at time t_δ.

Tests may take the form of clinical tests (e.g. PCR tests, antigen tests or antibody tests) but may also be simple observations of the presence or absence of symptoms (e.g. fever, persistent-cough or loss of taste).

The conditional probability of a positive test result is given by

$$P(\xi_n^+(t)|C(t)) = \int_0^t P(\xi_n^+(t)|\delta(t_\delta))P(\delta(t_\delta)|C(t))dt_\delta + \left(1 - \int_0^t P(\delta(t_\delta)|C(t))dt_\delta\right)(1 - P(\xi_n^-|\bar{i}))$$

2.2 The joint probabilities

The above conditional probabilities for each individual can be put together to create the joint probability over all people.

The probability that a contact with a person at time t ends in a transmission event from that person depends only on the transmission events to that person before t, so we can imagine building up the joint from conditionals starting with the earliest contact and moving one at a time to the latest. If we let $\mathcal{C}$ be the set of all transmission events for all people, it can be seen that the joint probability is given by

$$P(\mathcal{C}) = \prod_{\tau_{a\to b}(t)\in\mathcal{C}} P\left(\tau_{a\to b}(t)|\left\{\tau_{b'\to a}(t') : \tau_{b'\to a}(t') \in \mathcal{C} \wedge t' < t\right\}\right)$$

If the i^{th} user has contacts C_i and we group the terms by onward transmission from each user, we get

$$P(C_1...C_N) = \prod_i \prod_{\langle t,a,b\rangle \in C_i} P\left(\tau_{a\to b}(t) | \left\{\tau_{b'\to a}(t') : \tau_{b'\to a}(t') \in C_i \wedge t' < t\right\}\right)$$

If we note that the probability of a positive/negative test result also depends only on the contacts prior to the test then we can also add test results to the joint. If T_i is the set of tests taken by user i, the joint becomes

$$P(C_1...C_N, T_1...T_N) = \prod_i \prod_{\langle t,a,b\rangle \in C_i} P\left(\tau_{a\to b}(t) | \mathcal{L}(C_i, a, t)\right) \prod_{\xi_n(t)\in T_i} P(\xi_n(t) | \mathcal{L}(C_i, a, t)) \tag{1}$$

where we use the shorthand

$$\mathcal{L}(C, a, t) = \left\{\tau_{b'\to a}(t') : \tau_{b'\to a}(t') \in C \wedge t' < t\right\}$$

This joint can be expanded to include each user's infectiousness at the time of each contact. For ease of notation, we imagine the infectiousness to be included in the Tuple of each contact so $\langle t, a, b, \iota\rangle \in C_i$ is a contact at time t where the broadcaster of PID a had infectiousness ι. So, the joint now looks like this

$$P(C_1...C_N, T_1...T_N) = \prod_i \prod_{\langle t,a,b,\iota\rangle \in C_i} B(\tau_{a\to b}(t)|\iota) P\left(\iota | \mathcal{L}(C_i, a, t)\right) \prod_{\xi_n(t)\in T_i} P(\xi_n(t) | \mathcal{L}(C_i, a, t)) \tag{2}$$

3 Calculating posterior marginal probabilities of transmission events

We can now calculate the posterior marginal probabilities of all transmission events, given all the test results. We do this by embedding the joint in a cluster graph and performing belief propagation. We start with N clusters, one for each user, where the i^{th} cluster is given by

$$\Phi_i(C_i, T_i) = \prod_{\langle t,a,b,\iota\rangle \in C_i} P\left(\iota | \mathcal{L}(C_i, a, t)\right) \prod_{\xi_n(t)\in T_i} P(\xi_n(t) | \mathcal{L}(C_i, a, t)) \tag{3}$$

We separate out the Bernoulli terms into their own clusters

$$\Phi_{Bi}(\langle t, a, b, \iota\rangle) = B(\tau_{a\to b}(t)|\iota) \tag{4}$$

in this way, we end up with a Bethe cluster graph which has very good properties for performing belief propagation, so we would expect belief propagation to perform well on this graph both in term of the accuracy of the results and the number of messages passed.

Given the cluster graph, belief propagation calculates the marginal probability of each cluster. The marginals can be conditioned on the results of all tests by simply setting the values of each test when calculating the messages to pass.

3.1 Passing of messages

We now describe how belief propagation can be achieved on the network of mobile phones, without the need to expose any sensitive information.

Suppose that the i^{th} phone is responsible for clusters $\Phi_i(C_i, T_i)$ and the associated onward transmission Bernoulli clusters $\Phi_{Bi}(c)$ for all $c \in C_i$. There are two types of message that need to be sent from phone i: "forward" messages from the phone's Bernoulli clusters to the Φ clusters of other phones, and "backward" messages from the phone's $\Phi_i(C_i, T_i)$ cluster to the Bernoulli clusters on other phones.

Messages are sent whenever the information contained within them exceeds a threshold value. Information is transferred between phones by sending a data payload when a daily exposure key is published. The payload is received by any mobile with a PID in its log that can be derived from the exposure key.

However, a daily exposure key will match all contacts in a given day, but in order to implement belief propagation we need to send different messages to different contacts on the same day. So how do we deliver messages to a specific contact?

For forward messages we publish the phone's current belief in the posterior marginal infectiousness distribution for the day of the exposure key (under the approximation that the infectiousness of the person was constant over that period). From this single distribution all contacts can calculate their own forward messages.

To see this, suppose the posterior infectiousness distribution is given by $\Phi_i(\iota)$, this is known to phone i. Consider now one of the same phone's Bernoulli clusters for this day. If there have been no backward messages, the forward message from the Bernoulli cluster to the other phone's Φ cluster will be equal to

$$\int B(\tau_{a\to b}(t)|\iota)\Phi_i(\iota)d\iota = \int \iota\Phi(\iota)d\iota$$

If on the other hand a backwards message, δ', has been sent into the Bernoulli cluster, we need to remove the effect of this backward message before calculating the forward message. The backward message to the Bernoulli cluster would create an onward backward message from the Bernoulli cluster to $\Phi_i(\iota)$ of

$$\delta'\iota + (1-\delta')(1-\iota) = (1-\delta') + (2\delta'-1)\iota$$

So, the posterior belief about ι becomes

$$\Phi_i(\iota) = ((1-\delta') + (2\delta'-1)\iota)\Phi'_i(\iota)$$

where $\Phi'_i(\iota)$ is the belief with the backward message removed. So, the correct forward message from the Bernoulli cluster is

$$\delta_f = \int i\Phi'_i(\iota)d\iota = \int \frac{\Phi_i(\iota)}{(1-\delta') + (2\delta'-1)\iota}d\iota \tag{5}$$

but since the receiving phone knows the value of δ' (i.e. the backward message it sent) it can reconstruct the correct forward message from the Bernoulli cluster given only $\Phi_i(\iota)$.

So, if phone i publishes a parameterised version of $\Phi_i(\iota)$ along with a daily exposure key, all contacts for that day can derive their individual forward messages. We suggest publishing $\Phi_i(\iota)$ in terms of its first n moments. By taking the Taylor expansion of equation 5 about $\delta' = 0.5$, the forward message can be expressed as a series in the moments of $\Phi_i(\iota)$.

There is a similar problem with backward messages if we wish to publish them with the user's daily exposure key; different backward messages would need to be sent to contacts that happened on the same day.

However, suppose we add another cluster between the incoming transmission edges and the $\Phi_i(C_i, T_i)$ cluster. The new cluster aggregates all incoming transmission edges for one day into a single effective transmission using a logical OR operation, so that the effective transmission is true if any of the transmissions for that day are true. The $\Phi_i(C_i, T_i)$ cluster now sends a single message to the OR cluster, δ_Φ, which is its posterior likelihood function of the aggregated transition for the day, divided by any messages sent from the OR cluster. Suppose also that the OR cluster is connected to Bernoulli clusters $1..n$ on other phones, and that we've received forward messages $\delta_1...\delta_m$ from these clusters. The OR cluster needs to send the following backward message to Bernoulli cluster j

$$\begin{aligned}
\delta'_j &= \left\langle \delta_\phi\,,\ (1-\delta_\phi)\prod_{i\neq j}(1-\delta_i) + \delta_\phi(1-\prod_{i\neq j}(1-\delta_i)) \right\rangle \\
&= \left\langle \delta_\phi\,,\ (1-2\delta_\phi)\prod_{i\neq j}(1-\delta_i) + \delta_\phi \right\rangle \\
&= \left\langle \delta_\phi\,,\ \frac{1-2\delta_\phi}{1-\delta_j}\prod_{i}(1-\delta_i) + \delta_\phi \right\rangle
\end{aligned}$$

where we send two values since the likelihood function does not sum to 1.

So, instead of sending separate backward messages to each Bernoulli cluster, we publish δ_ϕ and $\prod_i(1-\delta_i)$ along with the daily exposure key. Then, since each phone already knows it's own δ_j (i.e. the forward message it passed for that contact) they can each calculate their own backward message from the published values. In this way we only need to make a single publication to send backward messages to all contacts on that day.

4 Quantifying the cost of outcomes

We measure cost in days of life lost. If a person dies of COVID-19, the cost of that death is the expected number of extra days of life that person would have had, had they not contracted the disease.

From this, we can calculate the cost of someone becoming infected when $R < 1$. In this case, a single infection will result in an average of $-\frac{1}{\ln(R)}$ total infections. If P_d is the case fatality ratio, then we would expect $-\frac{P_d}{\ln(R)}$ deaths and an average of

$$C_{id} = -\frac{P_d L}{\ln(R)}$$

days of life lost, where L is the average number of days lost when someone dies of COVID-19, considering age distribution and life expectancy.

There is also a cost, χ, associated with a person being hospitalised for a day (this covers the personal, inter-personal and financial costs). If $\bar{h}$ is the average number of days of hospitalisation per infection then we have a total expected cost of a single infection

$$C_i = -\frac{P_d L + \chi\bar{h}}{\ln(R)}$$

Let the cost of a person having to self-isolate be C_s and let C_T be the cost of taking the necessary tests if a person is alerted. These are subjective values which must measure the social, personal and economic costs.

So, if a person is alerted, we immediately incur the costs of the tests C_T. If the tests are negative, we assume no further action is taken. If positive, we incur the cost of isolation of the person, C_s but we gain the cost of the expected number of people the isolated person will not now infect, $\bar{\rho}C_i$. $\bar{\rho}$ can be calculated from the user's posterior infectiousness and their rate of close contacts. The positive result will also update the user's belief about transmission events. Any contacts with transmission event probabilities above a threshold, p_t will also be alerted. Since we know nothing about other contacts beyond the probability of transmission during contact, we calculate the cost of alerting them as an average expected cost given the time between the potential transmission event and the time of the alert, and the direction of the transmission $C_a(\Delta t, d)$. These values can be pre-calculated using Monte-Carlo simulation.

So, the total cost of alerting someone is

$$C_a = C_T + P(\xi_n^+(t)|C(t)) \left(C_s - \bar{\rho}C_i + \sum_{\{\langle t_c,a,b\rangle \in C(t):\tau_{a\to b} > p_t\}} C_a(t-t_c,\rightarrow) + \sum_{\{\langle t_c,a,b\rangle \in C(t):\tau_{b\to a} > p_t\}} C_a(t-t_c,\leftarrow) \right)$$

If this value is negative, then we should alert the user.

5 Further work

The belief in disease onset time can also be used to schedule tests so as to trade off the varying sensitivity of the test at different stages of the disease against the need to isolate the person, and the potential delay in isolating contacts.

The cost analysis can also be extended to the whole contact-tracing system in order to optimise the value of the thresholds to minimise expected cost. This can also be extended to release strategies and re-testing strategies.

At present, for simplicity, the analysis does not account for any difference in infectiousness of asymptomatic carriers compared to symptomatics. This can easily be added without significant change to the algorithm.

It may be worthwhile getting exact costs from contacts rather from pre-computed average values. However, this may have a large impact on the amount of information that needs to be passed, and will put requirements on the frequency that published information will need to be checked.