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

May 4, 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 when a user should be notified, tested or released from isolation 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 their own 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 notify the user to self-isolate and arrange to be tested. If a user is isolated, a decision must also be made when to end the isolation.

The problem we consider here is how to calculate whether and when to notify the user, perform tests and release from isolation, while maintaining the privacy of a user's close contacts.

The decision ought to be influenced by the test results of a user's close contacts (and even contacts of contacts), since these affect the probability that the user has been exposed and the probability that the user has exposed a close contact. In order to perform the necessary inference while maintaining the privacy of a user's close contacts, careful consideration needs to be paid to the way information flows around the system.

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 first aim is to calculate the marginal posterior probabilities of these events, given all the tests/observations that have been done on all people to

*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)

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.

The binary random variables $\tau_{a\to b}$ take values either 1 or 0. A value of 1 denotes the event that a transmission occurred from A to B. A value of 0 denotes the event that A and B had a close contact but no transmission occurred from A to B.

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

Given that a 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 $C(t) = \langle t_1, a_1, b_1\rangle \ldots \langle t_n, a_n, b_n\rangle$?

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 continuous risk of exposure from the environment (e.g. from surfaces or close contacts that were missed for any reason) at a rate ρ. ρ can be calculated from the local prevalence of the disease, the uptake of the app and the rate of contacts of the user. Given this, the probability density of first exposure since the start of the log is

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

where δ is the Dirac delta function.

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 $\omega(t)$ 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

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

where $P(\omega(t)|\epsilon(t_\epsilon))$ 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.

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

where $\iota(t|\omega(t_\omega),\alpha)$ represents the clinical course of the disease and α is a binary random variable indicating whether the person is an asymptomatic carrier (in which case, their infectiousness curve may be different from symptomatics). We take infectiousness to be a Beta distribution $P_\beta(t-t_\omega)$, and multiply by a constant ι_α for asymptomatics.

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 $\xi_1 \ldots \xi_n$ 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 $P(\xi_n^+(t)|\omega(t_\omega),\alpha)$ which gives the probability that a person tests positive on test n at time t given that they had disease onset at time t_ω and whether they are asymptomatic carriers.

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

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

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 is involved in transmission events C_i, and $\mathcal{C} = \cup_{i=1}^{N} C_i$, then we can group the terms by onward transmission from each user, giving

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

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

$$P(C_1..C_N, T_1..T_N, \alpha_1..\alpha_N) = \prod_i \prod_{\langle t,a,b\rangle\in C_i} P\left(\tau_{a\to b}(t)|\mathcal{L}(C_i,a,t),\alpha_i\right) \prod_{\xi_n(t)\in T_i} P(\xi_n(t)|\mathcal{L}(C_i,a,t),\alpha_i) \quad (1)$$

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

$$P(C_1..C_N, T_1..T_N, \alpha_1..\alpha_N) = \prod_i \prod_{\langle t,a,b,\iota\rangle\in C_i} B(\tau_{a\to b}(t)|\iota) P\left(\iota|\mathcal{L}(C_i,a,t),\alpha_i\right) \prod_{\xi_n(t)\in T_i} P(\xi_n(t)|\mathcal{L}(C_i,a,t),\alpha_i) \quad (2)$$

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

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

We separate out the Bernoulli terms into their own clusters

$$\left\{\Phi_B(\tau_{a\to b}(t),\iota) = B(\tau_{a\to b}(t)|\iota) : \langle t,a,b,\iota\rangle \in C_i\right\} \quad (4)$$

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 terms 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 $\Phi_i(C_i,T_i,\alpha_i)$ and the associated onward transmission Bernoulli clusters $\Phi_B(\tau_{a\to b}(t),\iota)$ for all $\langle t,a,b,\iota\rangle \in C_i$. 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_j clusters of other phones, and "backward" messages from the phone's Φ_i cluster to the Bernoulli clusters on other phones. We use the notation δ for forward messages and δ' for backward messages

In order to reduce the total number of messages sent, messages are only sent if the information contained within them exceeds a threshold value. Since all edges that span phones represent binary variables, the information content of a message (once normalised) is just

$$I(\delta) = 1 + \delta\log_2(\delta) + (1-\delta)\log_2(1-\delta)$$

Information is transferred between phones by publishing a data payload along with a daily exposure key on a public server. The payload and exposure key is periodically downloaded by all mobiles, if any mobile has a PID in its log that can be derived from the exposure key then the payload is deemed delivered to that phone.

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 somehow we need to deliver different messages to all contacts on a given day by publishing a single data payload. We want to do this in an efficient way that protects information about the contacts.

For forward messages we do this by publishing 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. In practice, we can take the infectiousness at the mean of the contact times for that day). From this single distribution all contacts can calculate their own forward messages.

To see this, suppose the posterior infectiousness distribution for the day in question 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 Φ_B, and suppose this is connected to cluster Φ_j on the other participant's phone. If there have been no backward messages from Φ_j to Φ_B, the forward message from Φ_B to Φ_j will be equal to

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

If on the other hand Φ_B has received a backwards message, δ', from Φ_j, we need to remove the effect of this backward message before calculating the forward message. The backward message to Φ_B would in turn create another backward message from Φ_B to $\Phi_i(\iota)$ with value

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

So, the posterior belief about ι must be

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

where $\Phi'_i(\iota)$ is the belief with the backward message removed and α is a normalising constant. So, the correct forward message from Φ_B to Φ_j must be

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

where

$$\alpha = \int \frac{\Phi_i(\iota)}{(1-\delta') + (2\delta'-1)\iota}d\iota \tag{6}$$

but since the receiving phone, j, 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 equations 5 and 6 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 for all contacts in a day $\langle t_1, a_1, b_1, \iota_1\rangle ... \langle t_n, a_n, b_n, \iota_n\rangle$, we imagine an additional cluster that sits between the the Bernoulli clusters on the contacts' phones, $\Phi_B(\tau_{b_1\to a_1}(t), \_)...\Phi_B(\tau_{b_n\to a_n}(t), \_)$, and the local Φ_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 Φ_i cluster now sends a single message to the OR cluster, δ_Φ, which is its posterior likelihood function of the aggregated transmission for the day, divided by any messages sent from the OR cluster. Since we're not interested in normalisation constants we'll assume that δ_Φ is normalised and so can be sent as a single number. Suppose also that that we've received forward messages $\delta_1...\delta_m$ from the remote Bernoulli clusters. The OR cluster needs to send the following backward message to Bernoulli cluster j

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

where we've normalised the backward message for convenience even though it's a likelihood.

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 Deciding when to self-isolate, test and release

Now we have a way of estimating posterior marginal probabilities, we can use these to make decisions. We adopt a decision theoretic approach by calculating the expected cost of each option and taking the one that has the lowest cost. 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 for a day be c_s and let c_{Tn} be the cost of taking the n^{th} test. These are subjective values which must weigh up the social, personal and economic costs.

If we assume decisions are made on a daily basis then on each day we need to decide whether to self-isolate for that day and whether to take test $n \in 1...N$. Clearly, any tests with immediate results should be taken before the decision whether to self isolate for that day so the decision which tests to take should be made first. Given any test results, a person should self isolate on that day if

$$c_s < \bar{\iota}(t)\rho_c c_i$$

where ρ_c is the user's average daily rate of close contacts and $\bar{\iota}(t)$ is the user's expected infectiousness on that day, given all the evidence to date.

If we decide to test, there is a fixed immediate cost of taking a test, c_{Tn}, but in return we gain information about the disease onset distribution. We can put a value on that information by calculating the difference in expected cost with and without that information. If having the information reduces our expected cost by more than the cost of obtaining the information then, on average, it is worth paying the price of the test for the information. So, the expected cost at time t is

$$\bar{c}(t) = \min(\bar{c_0}(t), c_{Tn} + P(\xi_n^+(t)|C(t))\bar{c}(\xi_n^+(t)) + P(\xi_n^-(t)|C(t))\bar{c}(\xi_n^-(t)))$$

where $\bar{c}(\xi_n^+(t))$ and $\bar{c}(\xi_n^-(t))$ is the expected cost given a positive/negative test result and $\bar{c}_0(t)$ is the expected cost of not testing.

$$\bar{c}_0(t) = (c_s - \bar{\iota}(t)\rho_c c_i)H(\bar{\iota}(t)\rho_c c_i - c_s) + \bar{c}(t+1)$$

where $H(.)$ is the Heaviside step function.

$$\bar{c}(\xi_n^-(t)) = (c_s - \bar{\iota}(t|\xi_n^-)\rho_c c_i)H(\bar{\iota}(t|\xi_n^-)\rho_c c_i - c_s) + \bar{c}(t+1)$$

If we assume that information that raises the probability of a transmission event above some threshold, p_t will trigger isolation and contact tracing of a close contact, then the expected cost of getting a positive test is

$$\bar{c}(\xi_n^+(t)) = (c_s - \bar{\iota}(t|\xi_n^+)\rho_c c_i)H(\bar{\iota}(t|\xi_n^+)\rho_c c_i - c_s) + \sum_A c_a^{\rightarrow}(t-t_c) + \sum_B c_a^{\leftarrow}(t-t_c) + \bar{c}(t+1)$$

where

$$A = \left\{\langle t_c, a, b\rangle \in C(t) : P(\tau_{a\to b}|\xi_n^+) > p_t \wedge P(\tau_{a\to b}) \leq p_t\right\}$$
$$B = \left\{\langle t_c, a, b\rangle \in C(t) : P(\tau_{b\to a}|\xi_n^+) > p_t \wedge P(\tau_{b\to a}) \leq p_t\right\}$$

$\bar{c}_a^{\leftarrow}(\Delta t)$ is the expected cost saving of isolating and contact tracing an infector at a time Δt after the contact and $\bar{c}_a^{\rightarrow}(\Delta t)$ is the expected cost saving of isolating and contact tracing an infectee at a time Δt after the contact. These expected values can be pre-calculated using Monte-Carlo simulation.

Notice that calculation of $\bar{c}(t)$ requires calculation of $\bar{c}(t+1)$ so we have a recursion.

To make the recursion tractable, we make a few assumptions. First, since the logging of symptoms can be done with very little cost, we assume that symptoms should be logged every day unconditionally (in practice, this will consist of the logging of the onset of any relevant symptoms, with the assumption of no symptoms otherwise). Secondly, we assume that we take at most one clinical test a day, and that the appropriate clinical test (i.e. PCR, antigen or antibody) can be decided by clinical considerations based on our belief about onset time and whether there have been previous positive tests (i.e. whether we are trying to show that a person has been infected or is safe to release).

With these assumptions, we can easily calculate the recursion 7 days into the future without putting a significant computational load the phone. Since on each day either no test is performed, or a test is performed and returns positive, or a test is performed and returns negative, there are three scenarios to evaluate each day and $3^7 = 2187$ scenarios in total. Beyond the 7 day horizon, we assume that if isolated the user will remain isolated until no danger is posed or if not isolated, the user poses no further danger. Since we don't know what the result of symptom tests will be, we take a Monte-Carlo sample of symptom onset times (say 100 samples) and run each scenario with each sample, giving a total of just over $200,000$ scenarios to run. This is not a large computational load, but can be reduced further by pruning highly unlikely scenarios (such as getting two consecutive negative tests at the peak of viral shedding after positive confirmation) and unreasonable testing schedules (e.g. performing a test around symptom onset if a positive test has already been obtained).

5 Further work

Distributed calibration of the parameters of the disease dynamics could be done by allowing phones to anonymously post the rate of change of probability of their test results with each parameter. This data can be posted to a central server which could aggregate the information from many phones and publish updated parameters for phones to periodically download.

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.

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.