COVI White Paper

arXiv:2005.08502v1 [cs.CR] 18 May 2020

Motivation

- Manual contact tracing of people infected with Covid-19 is limited
- Privacy-protecting decentralized systems can offer same benefit without concentrating data
- Machine learning can incorporating many clues
  - Including medical conditions, self-reported symptoms, and numerous encounters with people at different risk levels, etc.
- Machine learning can help build up useful model

Goal

- Reduce the number of infections by following targeted recommendations based on infection risk.
- Extract crucial information to guide data-driven approach to public health policy.
- Employ a privacy-protecting decentralized approach to digital contact tracing to enhance public trust in such applications.

Overview of COVI

- Aim: reduce the spread
- Strategy: inform individuals of their infection risk

- COVI leverages probabilistic risk levels to assign Covid-19 infection risk levels to app users.
  - Likeliness of being infected, when the infection may have occurred, and the expected contagiousness on different days after infection
- When COVI computes a high risk for an individual, it will guide towards local public health services for testing followed by manual contact tracing, with consent.

App overview

- Recommendations
  - Helps users make real-time decisions daily about their activities based on their personal level of risk (out-of-app actions)
- “Action cards”
  - Prompts users to input additional/updated information to further tailor their risk profile (in-app actions)
- Survey and data visualization
  - Allow users to express what is important to them and see how the crisis is unfolding
- “Share”

Use of machine learning

- Risk predictor
  - The probability that a person has been infected
  - How contagious that person was in the recent past and today
- Epidemiological simulator
  - Fit an model which can captures the events flow
  - Movement of people, encounters between people, medical events and behaviors

Existing approach

- Manual
  - The MIT PrivateKit SafePaths/SafePlaces approach and the Singapore's TraceTogether app
  - Involves a significant amount of human work, but also enables careful professional judgment of the severity of contact
- Fully automatic
  - Requiring much less work on the part of the public health authorities
  - May be more vulnerable to malicious parties, because there is no built-in safeguard of human judgment.

- COVI: fall much closer to the fully automatic, while retaining contact with authorities by providing high-risk/infected users with recommendations

Consent

- GPS-based geolocation history (blurred positions are kept)
- Random contact IDs generated by the application
- The user’s current risk levels

- Information above will be protected before it leaves the user’s device

Consent

- Age (user-reported)
- Sex (user-reported)
- Health conditions (user-reported)
- Active symptoms (user-reported)
- Ongoing relevant behavior (user-reported)
- Coarse geographical location (measured by GPS)
- Movement statistics (measured by GPS)
- Analytics information (use of application features that does not reveal any sensitive information about the user)

Consent

- The user may revoke their consent at any time, upon which their data will be deleted from the server.
- If they do not revoke consent, their data will still be automatically expired after a period of at most 90 days.

Dramatis Personae

Alice, a user of the app
She encounters Bob on day *d*

Eve, a passive eavesdropper
Tries to obtain information by overhearing communication, but doesn't do anything active.

Bob, carry covid-19
He encounters Alice on day *d*.
Later, he wants to privately communicate that change to Alice.

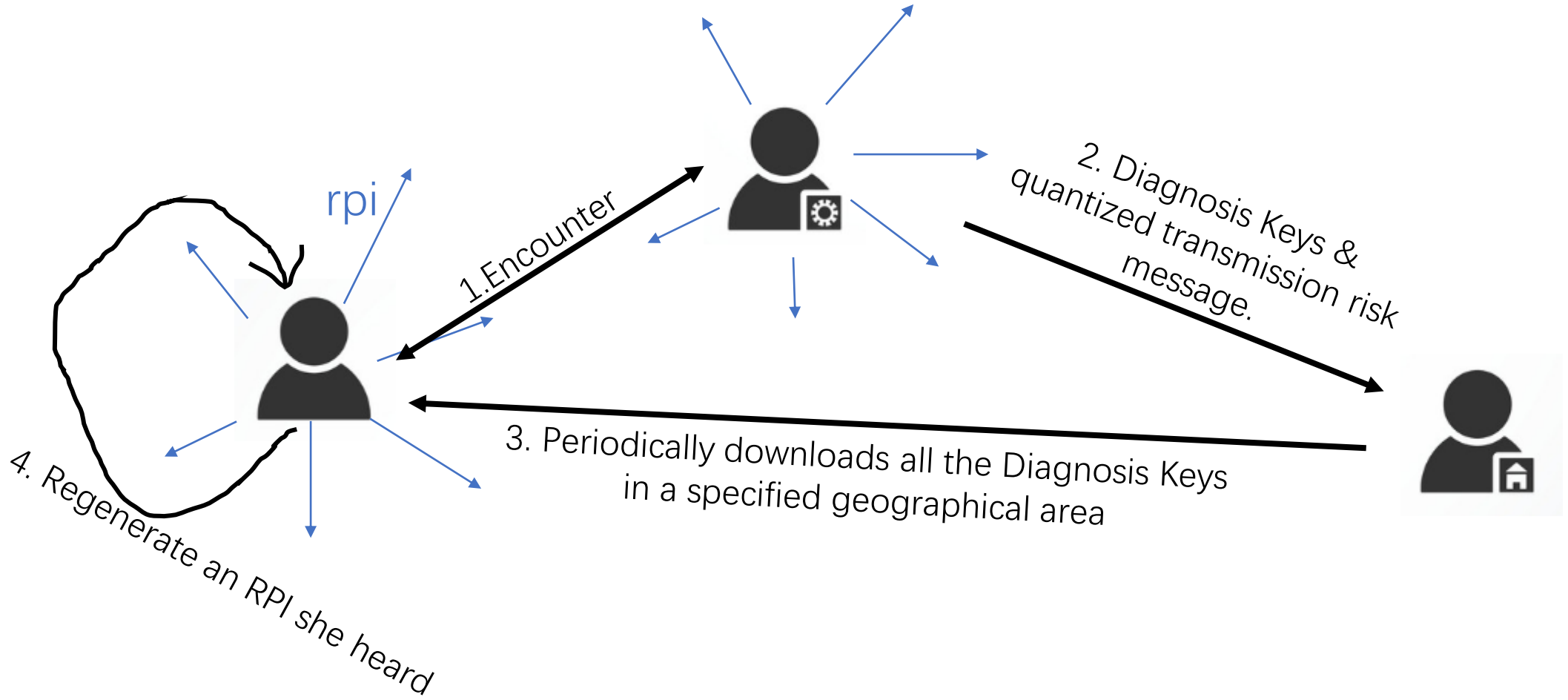
Mallory, an actively malicious actor
Tries to break the system, and will try to send false information to the servers and other parties.

Grace, the government (or other central authority)
She runs the central mailbox server containing all the reports.

Private risk messages protocol choices

- Google-Apple Exposure Notification (GAEN) Framework
  - Alice and Bob's phones are constantly broadcasting Rolling Proximity Identifiers (RPIs) via Bluetooth.
  - When Alice encounters Bob, the Alice s phone stores the RPI she hears from Bob.
  - Bob publishes Diagnosis Keys to Grace, along with an attached quantized transmission risk message.
  - Alice periodically downloads all the Diagnosis Keys in a specified geographical area from Grace.
  - Then locally regenerates the RPIs; whenever she regenerates an RPI she heard, she knows that the message is meant for her, informing her that she was exposed to Bob.

Scenario


rpi
1.Encounter
2. Diagnosis Keys &
quantized transmission risk
message.
3. Periodically downloads all the Diagnosis Keys
in a specified geographical area
4. Regenerate an RPI she heard

Private risk messages protocol choices

- TCN Coalition protocol
  - Temporary Contact Numbers
  - If the phones' owners have been in proximity with each other, they will share TCNs (roughly equivalent to GAEN's RPIs) with each other over Bluetooth
  - Alice has four of Bob's TCNs, and each time quantum is 5 minutes, then they have spent approximately 20 minutes within the distance boundary established by the protocol.
  - Phones can publish a 'report' to a central server, associating a set of TCN with a risk level payload (using the TCN report *memo* field).

Disadvantage

- Need to download all of the reports/Diagnosis Keys in a large geographical area for Alice

NHS Bluetooth + mix-nets

- When Alice and Bob are in close proximity, use Diffie-Hellman secret sharing over Bluetooth to generate two shared secret contact tokens
- A contact token can derive a ‘mailbox address’ and encryption key using a one-way hash function.
- Bob posts his risk status to Grace, he sends encrypted risk messages to the correct address

NHS Bluetooth + mix-nets

- Mix-net design
  - Establish 1, 2, ⋯, N mixing sever with public key p1, ⋯, pN, and Grace only control the last mixing server N.
  - For each message (*x, m*), Bob sends $p_1(p_2(\dots p_{N-1}(p_N((x,m)))\dots))$ to the first mix server.
  - The first mix server removes the first level of encryption, and waits until it has received encrypted reports from multiple 'Bobs', groups and shuffles them.
  - Then the first mix server forwards them as a batch to the second mix server.
  - The final mix server (controlled by Grace) is left with a series messages of the form (*x, m*), which have been decoupled from Bob.
  - Alice can then directly check all messages to an address *x* while Grace can not obviously linked to Bob.

NHS Bluetooth + mix-nets

- What if mixing server is malicious and discard Bob's message?

- Send the message through servers to ourselves and check if they are discarded.
- Involve an independent third party to verify.

Unsolved problems

- Leakage of medical data, namely the diagnosis status of a user.
- Leakage of the movement patterns of users

Model

- Update the following abstract variables each day according to this order

$$P(\text{mobility}(t)|\text{awareness}(t-1),\ \text{public health policy})$$
$$P(\text{contacts}(t)|\text{mobility}(t), \text{messages}(t-1))$$
$$P(\text{infection}(t)|\text{contacts}(t),\ \text{static})$$
$$P(\text{medical observations}(t)|\text{infection}(t))$$
$$P(\text{risk levels}(t)|\text{phone data}(t))$$
$$P(\text{messages}(t)|\text{risk levels}(t))$$
$$P(\text{awareness}(t)|\text{risk levels}(t))$$

Model

- X (Phone data): can be observed on individual phones (like the occurrence of contacts, the reported symptoms, or the test results)
- Z: cannot be directly observed, called the latent variables (like the actual viral load, contagiousness or infection status of a person)
- Risk predictor Q and the epidemiological simulator P
- The simulator P is actually a generative model $P(X, Z)$
- The risk predictor Q is actually an estimator of the conditional probability $Q(Z|X)$ and in general it should be viewed as an approximation of $P(Z|X)$.

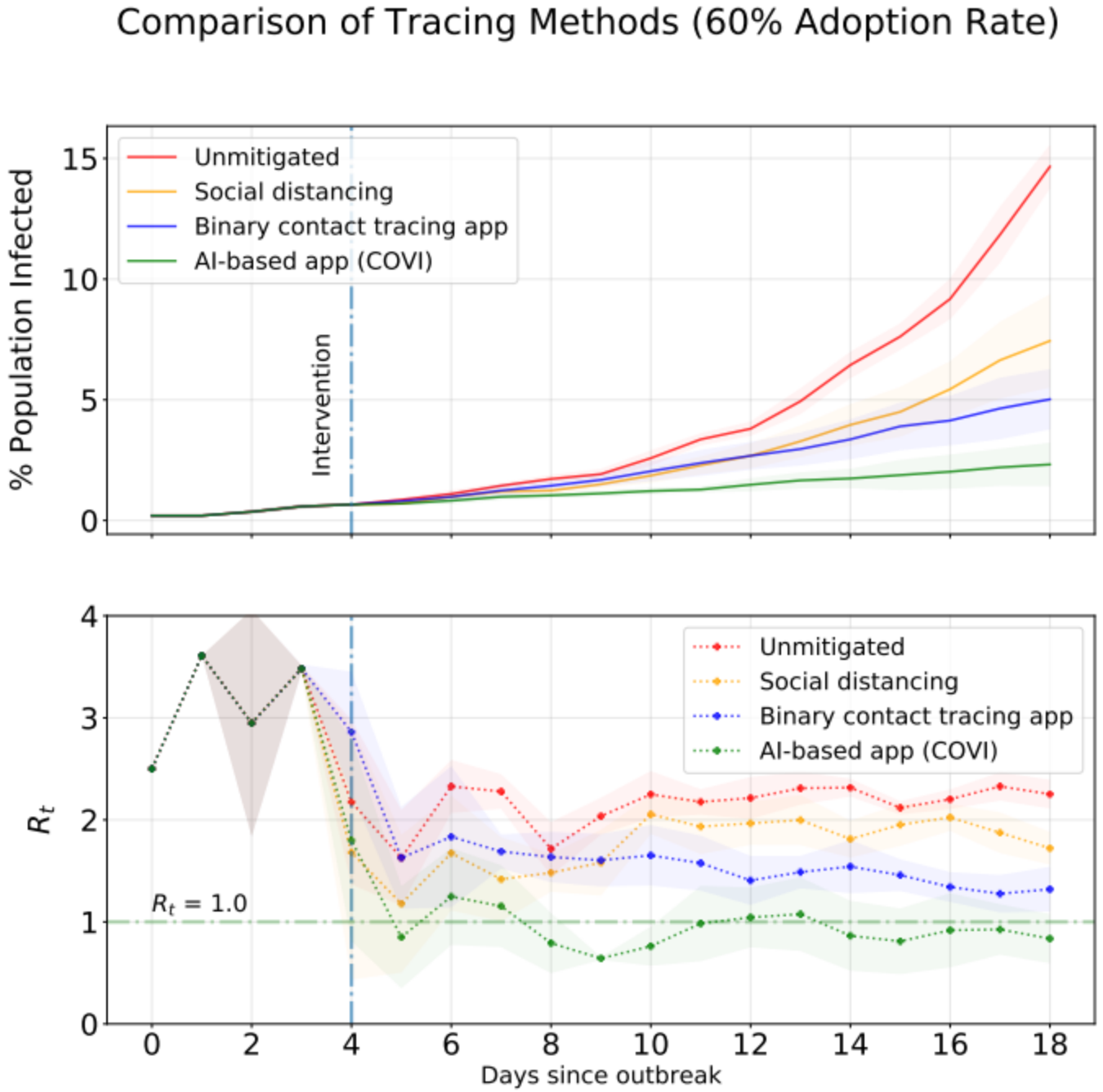
Model

- “As a first step in building a predictor, we have in fact constructed an epidemiological simulator P based on medical and mobility statistics, and generated a large set of trajectories (e.g. 30 days over a population of 30,000 people in a town), thus leading to many $(X, \vec{Z})$ pairs. ”

Simulation

- Day 4 is when the different mobility policies are put in place

- Estimated reproduction number (Rt) as simulation progresses



Thanks

Kaiyue Zhang 2020.07.03