



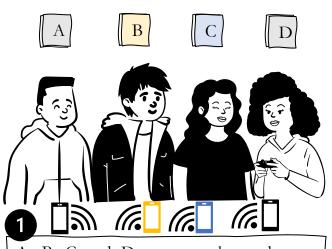
DP-ACT:
Decentralized PrivacyPreserving *Asymmetric*Digital Contact Tracing

Azra Abtahi, Mathias Payer, Amir Aminifar



Introduction

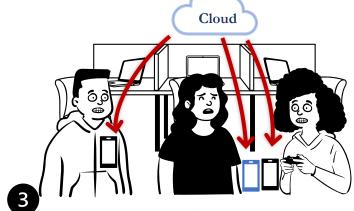
- Digital contact tracing identifies high-risk contacts during pandemics.
- State-of-the-Art Protocol: Decenteralized Privacy-Preserving Proximity Tracing (DP-3T)



A, B, C and D are coworkers who are using a COVID contact tracing app based on the DP-3T protocol.

Cloud

B is diagnosed with COVID-19. He reveals his pseudorandom IDs; he sends them to the cloud.



All the users download the revealed high-risk list from the cloud. A, C and D have the revealed pseudo-random IDs in their contact list; they receive high-risk contact alarms.

Broadcasts Ephemeral Pseudo-Random IDs

Record

- Ephemeral Pseudo-Random IDs
- Time
- Exposure Measurement

Upload $(i,seed_i) \cong$ Ephemeral Pseudo-Random IDs

Motivation: Limited Adoption of Digital Contact Tracing

During the COVID-19 pandemic adoption of digital contract tracing was limited due to privacy concerns.

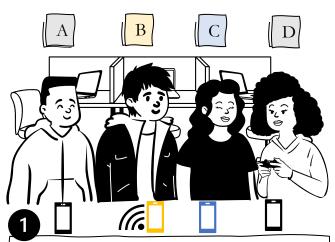


A, B, C and D are coworkers who are using a COVID contact tracing app based on the DP-3T protocol and only B is broadcasting BLE beacons.

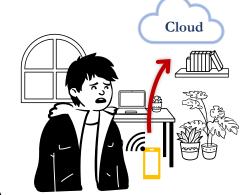
Our research question: Can the participation of users who never actively broadcast BLE beacons but passively listen to BLE beacons improve the precision of contact tracing?

Extension: Active/Passive DP-3T (A/P DP-3T)

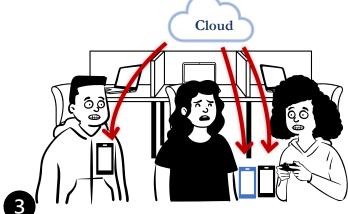
- Active Users: Broadcast BLE beacons, simultaneously record broadcasted IDs from others.
- Passive Users: Only record broadcasted IDs from other devices.



A, B, C and D are coworkers who are using a COVID contact tracing app based on the A/P DP-3T protocol and only B is broadcasting BLE beacons.



B is diagnosed with COVID-19. He reveals his pseudorandom IDs; he sends them to the cloud.

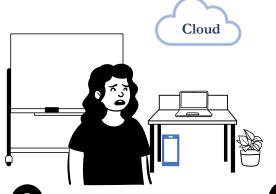


All the users download the revealed high-risk list from the cloud. A, C and D have the revealed pseudo-random IDs in their contact list; they receive high-risk contact alarms.

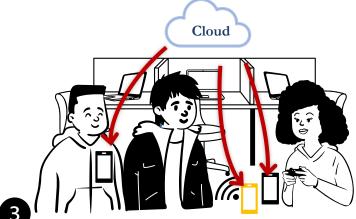
Limitations of A/P DP-3T: Passive Users Do Not *Notify*



A, B, C and D are coworkers who are using a COVID contact tracing app based on the A/P DP-3T protocol and only B is broadcasting BLE beacons.



C is diagnosed with COVID-19. She was not broadcasting BLE beacons; hence, she does not send any pseudo-random IDs to the cloud.



All the users download the revealed high-risk list from the cloud. A, B and D do not have the revealed pseudo-random IDs in their contact list; thus, they think that they have not had any high-risk contacts.

Decentralized Privacy-Preserving Asymmetric Contact Tracing (DP-ACT)



A, B, C and D are coworkers who are using a COVID-19 contact tracing app based on the DP-ACT protocol and only B is broadcasting BLE beacons.

same place & time → same recorded IDs

Key idea: passive users with overlapping recorded IDs indicate physical proximity.

> All the users download the revealed high-risk list from the cloud. A and D see that they have the revealed pseudo-random IDs in their contact list.

Cloud



C is diagnosed with COVID-19. As she was not broadcasting BLE beacons, she reveals the list of high-risk contact IDs on her app that are B's pseudorandom IDs; She sends it to the cloud and mentions that the IDs are revealed by a passive user.



All the users download the revealed high-risk list from the cloud. B sees his pseudo-random IDs there; hence, he finds out that he had a high-risk contact.

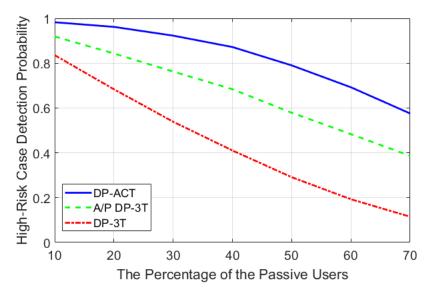
is sufficient to have at least one active participant in each contact group in order to be able to detect all highrisk contacts.



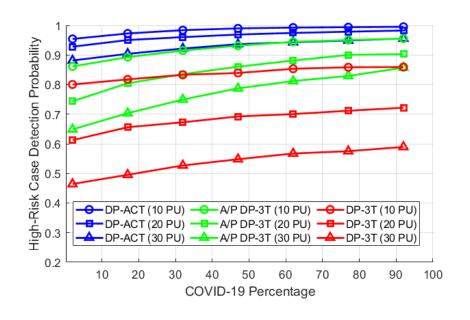
Thus, they find out that they had high-risk contacts.

Evaluation: Face-to-Face Dataset [1]

Dataset contains face-to-face interactions of individuals measured over 12 days in an office building.



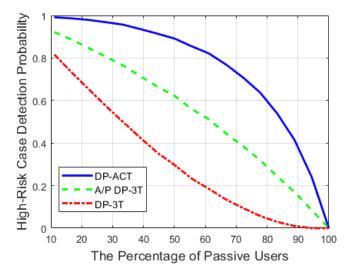
30% of users are diagnosed with COVID-19 and willing to notify others.

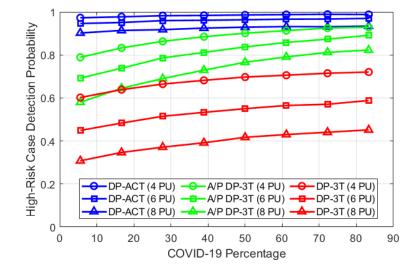


[1] Mathieu Génois and Alain Barrat. 2018. Can co-location be used as a proxy for face-to-face contacts? EPJ Data Science 7, 1 (2018).

Evaluation: Real BLE dataset [2]

- Real-world BLE datasets collected considering five different scenarios: dining together, riding a train together, working in an open-space setting, waiting in line at the supermarket, and mingling in a club/bar.
- 20 users participated in these data collections.





5 users are diagnosed with COVID-19.

[2] Mathias Payer and Daniele Antonioli. 2020. BLE measurements for GAEN/DP-3T contact tracing. https://github.com/DP-3T/bt-measurements/tree/ba9f73962b35260e12e2c0a8a37af5c6195d22a8.

Conclusion: DP-ACT Significantly Improves the Precision of **Digital Contact Tracing**

Allowing conservative user who do not want to broadcast BLE beacons to participate in the Digital Automatic Contact Tracing can significantly improve high-risk contact identification.



A, B, C and D are coworkers who are using a COVID-19 contact tracing app based on the DP-ACT protocol and only B is broadcasting BLE beacons.



C is diagnosed with COVID-19. As she was not broadcasting BLE beacons, she reveals the list of high-risk contact IDs on her app that are B's pseudo-random IDs: She sends it to the cloud and mentions that the IDs are revealed by a passive user.



All the users download the revealed high-risk list from the cloud. B sees his pseudo-random IDs there; hence, he finds out that he had a high-risk contact.



All the users download the revealed high-risk list from the cloud. A and D see that they have the revealed pseudo-random IDs in their contact list.





Paper: https://petsymposium.org /popets/2024/popets-2024-0019.pdf



Code: https://github.com/AzraSA /DP-ACT/tree/main



