DP-ACT: Decentralized Privacy-Preserving Asymmetric Digital Contact Tracing

Abtahi Fahliani, Azra; Payer, Mathias; Aminifar, Amir

Published in:
The 24th Privacy Enhancing Technologies Symposium (PETS)

2023

Document Version:
Peer reviewed version (aka post-print)

DP-ACT: Decentralized Privacy-Preserving Asymmetric Digital Contact Tracing

Azra Abtahi
Department of Electrical and Information Technology, Lund University, Sweden
azra.abtahi_fahliani@eit.lth.se

Mathias Payer
School of Computer and Communication Sciences, EPFL, Switzerland
mathias.payer@nebelwelt.net

Amir Aminifar
Department of Electrical and Information Technology, Lund University, Sweden
amir.aminifar@eit.lth.se

ABSTRACT

Digital contact tracing substantially improves the identification of high-risk contacts during pandemics. Despite several attempts to encourage people to use digital contact-tracing applications by developing and rolling out decentralized privacy-preserving protocols (broadcasting pseudo-random IDs over Bluetooth Low Energy—BLE), the adoption of digital contact tracing mobile applications has been limited, with privacy being one of the main concerns.

In this paper, we propose a decentralized privacy-preserving contact tracing protocol, called DP-ACT, with both active and passive participants. Active participants broadcast BLE beacons with pseudo-random IDs, while passive participants model conservative users who do not broadcast BLE beacons but still listen to the broadcasted BLE beacons. We analyze the proposed protocol and discuss a set of interesting properties. The proposed protocol is evaluated using both a face-to-face individual interaction dataset and five real-world BLE datasets. Our simulation results demonstrate that the proposed DP-ACT protocol outperforms the state-of-the-art protocols in the presence of passive users.

KEYWORDS

Proximity Tracing, Digital Contact Tracing, COVID-19, Internet of Things (IoT), Privacy, Decentralized, Bluetooth Low Energy (BLE), Mobile Apps, DP-3T, PEPP-PT.

1 INTRODUCTION

Contact tracing is the process of establishing who has been in contact with an infected person during the time they were infectious with the intent of warning and quarantining potentially infected people, limiting the spread of the contagion. Manual contact tracing is too slow and too labor intensive for fast-spreading highly-contagious contagions like COVID-19 [13], essentially lagging behind the spread of the disease. Digital proximity tracing speeds up contact tracing to save lives [7, 13]. This type of contact tracing relies on digital devices to keep track of contacts, often determining the proximity of subjects and the duration of contacts. Digital contact tracing attracted a lot of attention during the outbreak of COVID-19; however, it has existed as a concept before that [3, 4, 8, 12].

Proceedings on Privacy Enhancing Technologies YYYY(X), 1–13

https://doi.org/XXXXXXX.XXXXXXX

Smartphones are now in everyone's pocket. During the outbreak of COVID-19, mobile applications were the first choice to implement COVID-19 digital contact tracing. For proximity tracing in public places, several COVID-19 contact-tracing applications established manual "check-in" systems, where users scan QR-codes when entering a public place [6]. This proximity tracing scheme requires each user to manually scan a QR-code, which is error-prone and unsuitable for dynamic and large-scale environments. On the other hand, automated digital contact-tracing applications have been proposed to use Global Positioning System (GPS) and Bluetooth Low Energy (BLE) for automatic proximity tracing. However, GPS only works efficiently outdoors, where the risk of infection is lower. Therefore, for large-scale indoor environments, most protocols resort to broadcasting BLE beacons for digital contact tracing.

COVID-19 contact-tracing applications can use centralized or decentralized protocols to calculate potential exposure. In centralized protocols, the central health authority processes the contact history for all users and warns exposed users. In decentralized protocols, each user calculates their exposure locally and central authorities, by design, have no access to contact data. Hence, decentralized protocols are privacy-preserving. The first generations of COVID-19 contact-tracing applications were launched in Asia [5, 6, 11, 21, 25, 30]. However, most of the COVID-19contact-tracing applications launched in Asia rely on centralized protocols. In contrast, most of the launched COVID-19contact-tracing applications in Europe and the USA use decentralized protocols to preserve the privacy [1, 6, 21, 25, 32].

Decentralized Privacy-Preserving Proximity Tracing (DP-3T) is the state-of-the-art protocol for COVID-19 contact tracing [31, 32]. In this decentralized protocol, each user broadcasts pseudo-random IDs through BLE beacons. Despite several excellent initiatives to develop privacy-preserving contact tracing protocols and applications, their adoption by the public has been to a large extent limited. Privacy concerns are among the most important issues that limit the wide adoption of digital contact tracing mobile applications [2, 9, 10, 16–20, 26, 28, 29]. Indeed, from a technical point of view, there are certain privacy risks associated with broadcasting BLE beacons. In particular, recent studies [15, 33] highlight that the unique physical-layer imperfections and variations in the hardware design of BLE chipsets can be exploited by adversaries to uniquely identify *transmitting* mobile devices, even in the context of COVID-19 contact-tracing applications and despite pseudo-random IDs [15]. The main open research question, then, is *whether the participation of the users who do not broadcast BLE beacons, but still listen to BLE*

beacons and upload contacts upon infection, can improve the precision of digital contact tracing *compared to when these users do not participate.* We argue that this is indeed the case.

In this paper, we propose a decentralized protocol to accommodate the participation of conservative/passive users for precise digital contact tracing. In our proposed protocol, we consider both active and passive participants. Active participants broadcast BLE beacons with pseudo-random IDs, while passive participants model conservative users who do not broadcast BLE beacons but still listen for broadcasted BLE beacons. Hence, passive participants learn about their potential exposure and can take proper action. On the other hand, once infected, passive participants may release their list of high-risk contacts based on the pseudo-random IDs they have received. This allows active participants to exercise home quarantine if their pseudo-random IDs are released by the passive participants. As a result, the proposed protocol enables high-precision digital contact tracing, by enabling and leveraging the participation of conservative/passive users. We refer to our protocol as Decentralized Privacy-Preserving Asymmetric Digital Contact Tracing (DP-ACT). We discuss the properties of our proposed protocol, among which, we demonstrate that it is sufficient to have only one active participant in each contact group (i.e., groups of participants among whom every two participants are in close proximity for a considerable duration) to identify all high-risk contact groups (i.e., a contact group with at least one infected participant). Moreover, we briefly discuss the privacy/security of the proposed protocol raised by infected passive users uploading their recorded high-risk IDs. The main contributions of this paper are summarized below:

- We propose a decentralized privacy-preserving protocol, called DP-ACT, for COVID-19 digital contact tracing to enable and leverage the participation of conservative/passive users for high-precision digital contact tracing. This is the first time, to the best of our knowledge, that we consider a setting with both active and passive participants in the context of COVID-19 digital contact tracing.
- We formally analyze the proposed protocol and prove a set of formal guarantees. In particular, we show that using our DP-ACT protocol, it is sufficient to have at least one active participant in each contact group in order to be able to detect all high-risk contact groups.
- We evaluate the proposed protocol using the InVS15 dataset that contains the face-to-face interactions of individuals in an office building in France in 2015 [14]. The InVS15 dataset has a sufficiently long duration of face-to-face interactions to analyze how COVID-19 spreads in such large-scale dynamic environments and to demonstrate the effectiveness of our proposed DP-ACT protocol in comparison with the state-of-the-art protocols.
- Finally, we also consider five real-world BLE datasets collected considering five different scenarios: dining together at the table, riding a train together, working together in an open-space setting, waiting in line at the supermarket, and mingling in a club/bar [27, 32]. Our simulation results based on these five datasets show that the proposed protocol outperforms the state-of-the-art in the presence of conservative/passive users/participants.

This paper is organized as follows. In Section 2, first, we discuss the state-of-the-art protocol (i.e., DP-3T protocol) in the presence of conservative users and propose an extension of the DP-3T contact tracing protocol (i.e., Active/Passive DP-3T protocol or A/P DP-3T) allowing the conservative users not to advertise BLE beacons. Next, we discuss the shortcomings of the Active/Passive DP-3T protocol and propose a new privacy-preserving protocol to address these shortcomings (i.e., DP-ACT). In Section 3.1, we theoretically analyze the DP-ACT protocol and prove a set of interesting formal guarantees for the proposed protocol. In Section 4, we evaluate the proposed protocol against the state-of-the-art protocols based on simulation. Finally, Section 5 serves as the conclusion.

2 ASYMMETRIC PRIVACY-PRESERVING DIGITAL CONTACT TRACING

DP-3T is a popular open protocol developed for COVID-19 contact tracing. The aim of this protocol is to identify and warn high-risk contacts of users diagnosed with COVID-19, without revealing the users' identities and the place of the contacts. Hence, this decentralized protocol broadcasts ephemeral pseudo-random IDs through BLE.

In COVID-19 contact-tracing applications that are using DP-3T, a user's digital device continually broadcasts ephemeral pseudo-random IDs and simultaneously records the pseudo-random IDs received from other users' devices that are in close proximity. Then, when a user is diagnosed with COVID-19, this user can reveal the pseudo-random IDs that were previously broadcasted from their device during the contagious time by uploading them to a central server (cloud).[1]

All users' applications download the pseudo-random IDs from the cloud periodically/sporadically. Then, they check their contact ID lists and if they have the same IDs in their list, they use their recorded proximity information to calculate the duration of the contact and even the proximity of the users during the contacts to find the high-risk contacts. High-risk contact is defined as close proximity contact with an infected user for a sufficient duration, yielding a high risk of being infected. For the identification of high-risk contacts, an exposure score, which is a function of the proximity and the duration of the contact, is calculated and compared with a determined threshold. A user with a high-risk contact, called a high-risk user, receives an alarm from the application to stay in quarantine and get tested for the viral infection.

Despite several attempts to encourage the public to use the COVID-19 contact-tracing applications by increasing privacy (i.e., by using decentralized systems, BLE, and pseudo-random IDs), the adoption of digital contact tracing mobile applications has been limited and one of the most important issues that limit this adaption is

[1] In DP-3T [32], the authors proposed three different designs based on the ephemeral pseudo-random ID generation: low-cost decentralized proximity tracing, unlinkable decentralized proximity tracing, and hybrid decentralized proximity tracing. In all these designs, the ephemeral pseudo-random IDs are functions of random "Seed"s generated by the devices in each epoch. In practice, in all these designs, the infected users upload a set of epoch numbers and seeds, $(i, seed_i)$, for all relevant epochs, instead of uploading all IDs broadcasted from their device to the cloud during the time that the infected user could be contagious. Here, for the sake of simplicity of the presentation, we assume uploading the IDs to the cloud is equivalent to uploading a set of epoch numbers and seeds, i.e., $(i, seed_i)$. In practice, however, a set of epoch numbers and seeds, i.e., $(i, seed_i)$, are uploaded to the cloud, to reduce the communication overheads.

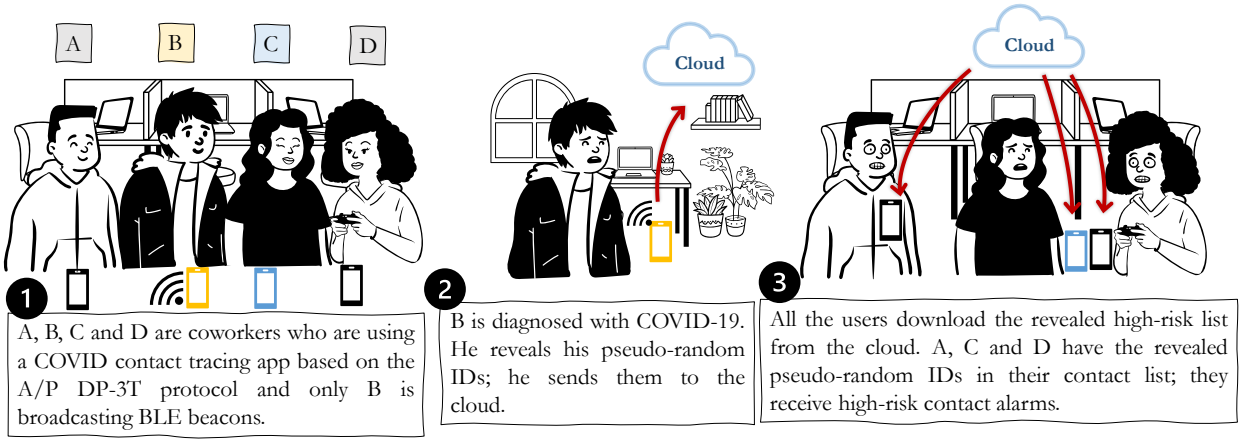


Figure 1: First example for the A/P DP-3T protocol.

privacy concerns. As discussed earlier, it has been shown that there are certain privacy risks associated with broadcasting BLE beacons [15, 33]. Now, the main open research question is whether the participation of the users who do not broadcast BLE beacons, but still listen to BLE beacons and upload contacts upon infection, can improve the precision of digital contact tracing compared to when these users do not participate. We believe that this is indeed the case. The DP-3T protocol, however, does not consider/allow passive participants. Hence, the information that could have been provided with the participation of the passive people is not exploited in the DP-3T protocol.

2.1 Active/Passive DP-3T Protocol (A/P DP-3T)

To address the limitation of DP-3T towards passive users, we discuss an initial extended version of the DP-3T protocol, where conservative users can participate in the protocol as passive participants, without broadcasting BLE beacons, alongside the active participants who broadcast BLE beacons. The remaining protocol follows the DP-3T protocol. We refer to this protocol as Active/Passive DP-3T (A/P DP-3T) because it allows passive users to participate in the digital contact tracing process. These passive participants receive the broadcasted pseudo-random IDs and download and check the revealed IDs.

Let us discuss our A/P DP-3T protocol using two examples. Fig. 1 shows a situation where an active participant is infected. Among the four coworkers A, B, C and D, only B broadcasts BLE beacons. The others have chosen not to broadcast BLE beacons. Let us assume that B receives his COVID-19 test result and is diagnosed with COVID-19. According to the DP-3T protocol, he reveals his pseudo-random IDs to the cloud. As the DP-3T protocol does not handle passive users, A, C and D are not informed about their exposure if the contact-tracing application is based on the DP-3T protocol. In contrast, considering the A/P DP-3T protocol, all users download the revealed pseudo-random IDs, and the COVID-19 contact-tracing applications on their smartphones cross-check them against their contact lists to see if they have been in close proximity contact with the infected users. The smartphones of A, C and D find the revealed IDs in their contact lists. They calculate the duration of the corresponding contacts, the proximity of the users during the contacts and finally, an exposure score. They learn that they have had high-risk contacts and A, C and D receive high-risk contact alarms.

Fig. 2 shows another example for the case where the infected user is passive and does not broadcast BLE beacons. Similar to Fig. 1, there are 4 coworkers, named A, B, C and D, who have installed a COVID-19 contact-tracing application based on the A/P DP-3T protocol. Again, only B broadcasts BLE beacons and the others have chosen not to broadcast BLE beacons. Here, we assume that C is diagnosed with COVID-19. C is not broadcasting any IDs; hence, she does not send any IDs to the cloud. Then, all users download the revealed IDs from the cloud. As A, B and D do not find the revealed IDs in their contact lists, they think that they have not had any high-risk contacts.

In summary, the first example demonstrates that the A/P DP-3T protocol addresses one of the limitations of the DP-3T protocol by simply allowing passive users to check for their own exposure. The second example, on the other hand, shows that both DP-3T and A/P DP-3T fail to detect the high-risk contacts when a passive user is diagnosed with COVID-19. Hence, there is a need for a protocol that enables and leverages the participation of passive users for precise digital contact tracing.

2.2 DP-ACT Protocol

We now discuss our proposed DP-ACT protocol to enable the participation of the conservative users as passive participants, who do not broadcast BLE beacons, alongside the active participants, who broadcast BLE beacons.

For the sake of clarity, let us define new terminologies for the IDs broadcasted by the users, IDs received by the users, and IDs downloaded from the central server/cloud, in the following.

Definition 1. *We distinguish among three types of IDs as follows:*

- *B-ID: the pseudo-random IDs broadcasted by each user.*
- *R-ID: the pseudo-random IDs received by each user.*
- *C-ID: the IDs downloaded from the cloud.*

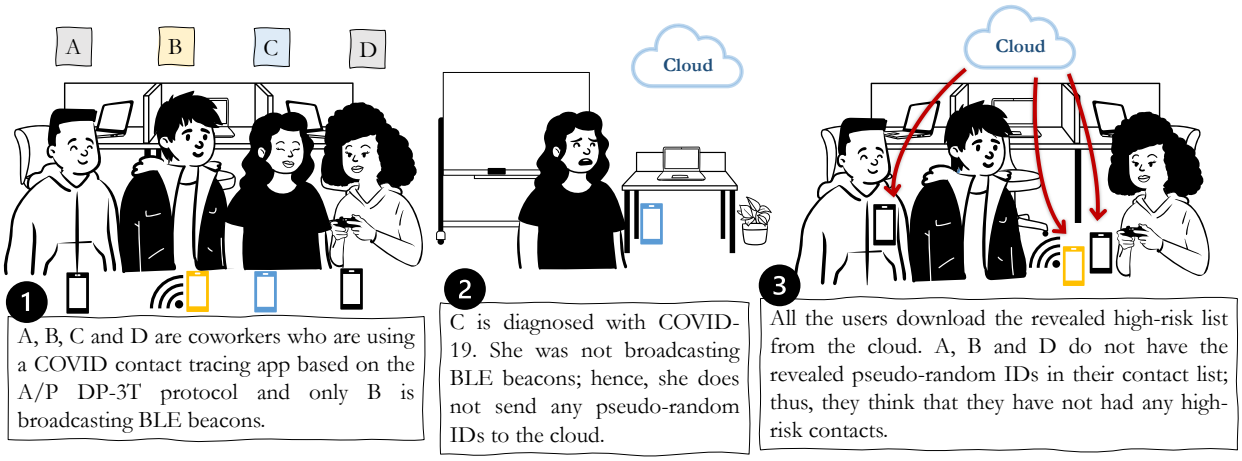


Figure 2: Second example for the A/P DP-3T protocol.

We explain the DP-ACT protocol in three parts: "Normal Operation", "Once a User is Diagnosed with COVID-19", and "Identification of the High-Risk Contacts".

2.2.1 Normal Operation:

- Active Users: In normal operation, the active users continuously broadcast BLE beacons with ephemeral pseudo-random IDs (B-IDs) and receive the broadcasted BLE beacons by the other users. They record the time of receiving the BLE beacons, the received pseudo-random R-IDs, and the Received Signal Strengths (RSS). Hence, an active user has two local pseudo-random ID lists in their application: the first one is the list of ephemeral pseudo-random IDs (B-IDs) broadcasted by this user's smartphone (their own pseudo-random ID list) and the second one is the list of the recorded pseudo-random IDs (R-IDs) broadcasted by other users (the contact ID list).
- Passive Users: In normal operation, passive users choose to not broadcast BLE beacons and only receive broadcasted BLE beacons from active users (i.e., R-IDs). Similar to active users, passive users record the time of receiving the BLE beacons, the received pseudo-random IDs (R-IDs), and the corresponding RSSs. Thus, a passive user has only one local pseudo-random ID list in their application: the list of the recorded pseudo-random IDs (R-IDs) broadcasted by other users (the contact ID list).

2.2.2 Once a User is Diagnosed with COVID-19:

- Active Users: When an active user is diagnosed with COVID-19, this user can reveal the pseudo-random IDs (B-IDs) that were previously broadcasted from their device by uploading them to the cloud. [2]
- Passive Users: When a passive user is diagnosed with COVID-19, they instead reveal the list of high-risk contact IDs (high-risk R-IDs) on their COVID-19 contact-tracing application and their corresponding contact time and the durations of the contacts (if the period of producing pseudo-random IDs by devices is short enough we do not need to send the time information). As they do not broadcast BLE beacons, they cannot release their own pseudo-random ID list. This user can send the high-risk contact IDs (high-risk R-IDs) to the cloud and indicates that the IDs are revealed by a passive user, i.e., the IDs belong to active users who had high-risk contacts with the passive infected user. In other words, there are two kinds of IDs revealed to the central server: IDs revealed by active users (B-IDs) and IDs revealed by passive users (high-risk R-IDs); hence, the types of IDs in the revealed lists should be indicated.

2.2.3 Identification of the High-Risk Contacts:

- Active Users: For the high-risk contact checking, the applications on the active users' smartphones download the revealed ID list from the cloud (C-IDs) at regular intervals and cross-check the IDs revealed by active users among C-IDs against their contact ID list (R-IDs). If they find the revealed C-IDs by active users in their contact ID list, they calculate the exposure score for the corresponding contact and compare it to a threshold. If the exposure score surpasses the threshold, the contact is high-risk, and an alarm notifies the user. Furthermore, the application on an active user's smartphone checks its own pseudo-random ID (B-IDs) list against the ID list downloaded from the cloud (C-IDs). If it finds any of their broadcasted IDs (B-IDs) on the list downloaded from the cloud (i.e., C-IDs that were originally revealed by the passive users), it discovers that the active user has been in a high-risk contact with a passive infected user and notifies this active user.

[2] For DP-ACT, just like DP-3T, we can consider different designs based on the ephemeral pseudo-random ID generation, and the infected active users can upload a set of epoch numbers and seeds, $(i, seed_i)$, for all relevant epochs instead of uploading all IDs broadcasted from their device to the cloud during the time that the infected user could be contagious. Again, for the sake of simplicity of the presentation, we assume uploading the IDs to the cloud is equivalent to uploading a set of epoch numbers and seeds, i.e., $(i, seed_i)$, without loss of generality. In practice, however, a set of epoch numbers and seeds, i.e., $(i, seed_i)$, will be uploaded to the cloud, to reduce the communication overheads.

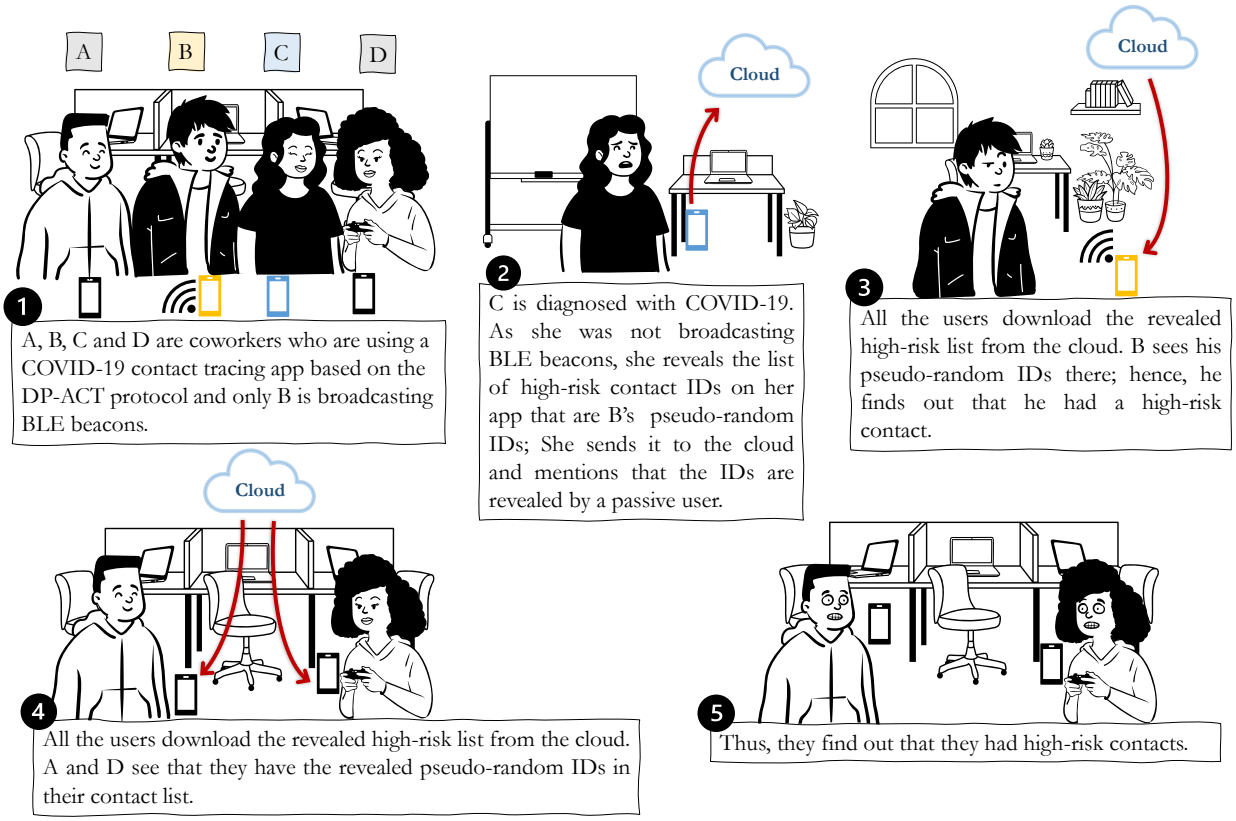


Figure 3: An example for the proposed DP-ACTprotocol.

- Passive Users: For high-risk contact checking, a passive user's smartphone downloads the revealed ID list from the cloud (C-IDs) at regular intervals. For IDs revealed by passive infected users, it also downloads their corresponding contact time. It cross-checks all IDs against the IDs on their contact list (R-IDs); if there is any intersection, it calculates the exposure score for the intersection. If the exposure score surpasses a specified threshold, the contact is high-risk, and an alarm notifies the passive user. For cross-checking of the C-IDs revealed by passive users, only passive users who had one of these C-IDs in their contact list *during the corresponding revealed contact time* receive the high-risk alarm.

Now, what happens if the participants in our second example in Fig. 2 use an application with the proposed DP-ACT protocol? Fig. 3 illustrates the proposed DP-ACT protocol in such a setting. We recall that, in this example, there are 4 coworkers, A, B, C and D, using a COVID-19 contact-tracing application with the DP-ACT protocol. Only B is an active participant and broadcasts BLE beacons; the others are passive participants and have chosen not to broadcast BLE beacons. Then, C receives her COVID-19 test result, and she is diagnosed with COVID-19. When C is diagnosed with COVID-19, as she was not broadcasting BLE beacons, she reveals the list of high-risk contact IDs on her COVID-19 contact-tracing application, which is B's pseudo-random IDs; she uploads this list to the cloud and indicates that the IDs are revealed by a passive user. All the users' applications download the revealed high-risk list from the cloud. B's application finds his pseudo-random IDs in the revealed ID list; hence, he receives a high-risk contact alarm. The applications on A and D smartphones also find the revealed pseudo-random IDs in their contact lists and notify them with high-risk contact alarms. Therefore, DP-ACT allows precision contract tracing in the presence of passive users.

3 DISCUSSION AND ANALYSIS

3.1 Performance Analysis

In this section, we analyze the proposed DP-ACT protocol and discuss its properties. Let us first define three important terminologies we frequently use in this section, i.e., "PHR Contact", "Contact Group" and "High-Risk Group", in the following.

Definition 2. *A "Potential High-Risk Contact" or "PHR Contact" is a close proximity contact with sufficient duration for each of the involved people to be infected by the other one.*

Definition 3. *A "Contact Group" is a group of participants among whom every two participants are in close proximity and have PHR contacts with each other.*

Definition 4. *A "High-Risk Group" is a contact group that has at least one infected participant.*

We shall now discuss the arrangement of active and passive participants in a contact group and the relation to the precision of the proposed DP-ACT protocol.

Theorem 3.1. *Assuming COVID-19 contact tracing based on the DP-ACT protocol, it is sufficient to have one active user in each contact group in order not to miss any high-risk contact group.*[3]

Proof. Let us consider that there are k users in a contact group who are using a COVID-19 contact-tracing application based on the DP-ACT protocol. Among these users, $k-1$ users are passive and have chosen not to broadcast any BLE beacons, and only one user is active. If the active user is diagnosed with COVID-19, they reveal their own pseudo-random IDs according to the DP-ACT protocol, and as all the passive users have the active user's pseudo-random IDs in their contact lists, after downloading the revealed high-risk pseudo-random IDs, they find them in their contacts lists and find out that they have had high-risk contacts. Thus, all the users in the group who had high-risk contact with the infected user receive high-risk alarms.

Now, let's see what happens if a passive user is diagnosed with COVID-19. This case is similar to the example explained in Fig. 3. As the infected passive user was not broadcasting BLE beacons, they reveal the list of high-risk contact IDs on her COVID-19 contact-tracing application, which is the active user's pseudo-random IDs; the infected user sends it to the cloud and indicates that the IDs are revealed by a passive user. All the users' applications download the revealed high-risk list from the cloud. The active user's application finds the active user's pseudo-random IDs in the revealed ID list; hence, the user receives a high-risk contact alarm. The applications on the other passive users' smartphones also find the revealed pseudo-random IDs in their contact lists and receive high-risk contact alarms. Therefore, all the users (in the contact group) who have been in high-risk contact receive a high-risk contact alarm. □

Theorem 3.2. *Assuming P% of participants to be passive (equivalent to probability p) at any specific time t, then p^k is the probability of a high-risk group with size k to remain undetected at time t.*

Proof. According to Theorem 3.1, the only case for a high-risk group to remain undetected is that we do not have any active participants in the contact group; in other words, all participants in the contact group are passive. If we assume that the probability of being a passive participant is p; then, the probability of having k passive participant in a contact group with k participants is p^k. □

Now, let us discuss the ability of the proposed protocol to detect high-risk users by proposing Theorem 3.3 and Theorem 3.4. As mentioned before, a high-risk user is defined as a user who has a high-risk contact with an infected one while before this high-risk contact, the high-risk user was an uninfected user.

Theorem 3.3. *Assuming Q out of N users are active users (equivalent to probability $q = 1-p$) with an average degree of d (i.e., the average number of a user's PHR contacts) at any specific time t, the average number of passive users who do not have PHR contact to any active users and may remain undetected using the DP-ACT protocol is:*

$$N \cdot (1-q) \cdot (1 - \frac{d}{N-1})^{N \cdot q},$$

which is strictly decreasing with respect to both q and d.[4]

Proof. According to the assumptions, we have $s(0) = N - N \cdot q$ passive users; thus, if an active user has contact with another user, with the probability of $\frac{s(0)}{N-1}$ this user is a passive user. Hence, this active user, on average, has PHR contact with $d \cdot \frac{s(0)}{N-1}$ passive users. As a result, the average number of the remaining passive users who do not have PHR contact with this active user is: $s(1) = s(0) - d \cdot \frac{s(0)}{N-1} = s(0) \cdot (1 - \frac{d}{N-1})$. The next active user will have PHR contact, on average, with $d \cdot \frac{s(1)}{N-1}$ *new* passive users. Therefore, the average number of the remaining passive users who do not have PHR contact with these two active users is: $s(1) = s(1) - d \cdot \frac{s(1)}{N-1} = s(1) \cdot (1 - \frac{d}{N-1})$.

Now, let us define $s(i)$ as the average remaining number of passive users who do not have PHR contact with any of i active users, considering only i active users. With every active user i, the average remaining number of passive users who do not have PHR contact with any of the earlier active users, i.e., $s(i-1)$, will be reduced by $d \cdot \frac{s(i-1)}{N-1}$. Hence, this can be formulated as a dynamical system as follows:

$$s(0) = N - N \cdot q = N \cdot (1-q),$$
$$s(i) = s(i-1) - d \cdot \frac{s(i-1)}{N-1} = s(i-1) \cdot (1 - \frac{d}{N-1}).$$

Considering Q as the number of active users, the solution to the above dynamical system may be written as follows,

$$s(Q) = s(0) \cdot (1 - \frac{d}{N-1})^{Q},$$

where $s(0) = N \cdot (1-q)$ and $Q = N \cdot q$. Therefore, the average number of passive users who do not have PHR contact with any active users and may remain undetected is given by:

$$N \cdot (1-q) \cdot (1 - \frac{d}{N-1})^{N \cdot q}.$$

Note that, these remaining passive users do not have PHR contact with any active users; hence, if they have a high-risk contact, it will not be detected by the proposed DP-ACT protocol.

□

Theorem 3.4. *Assuming Q users of N total users are active users (equivalent to probability $q = 1-p$) and the average user's degree is d at any specific time t, then the average number of high-risk users that remain undetected (i.e., do not receive the high-risk alarm) by the DP-ACT protocol for the COVID-19 percentage of C (equivalent to COVID-19 probability $c = C/100$) is:*

$$N \cdot (1-q) \cdot (1 - \frac{d}{N-1})^{N \cdot q} \cdot (1-c) \cdot (1 - \prod_{l=1}^{d} \frac{N - c \cdot N - l}{N - l}).$$

[3] The assumption related to "contact group" is only made to develop the theoretical basis behind the DP-ACT protocol. In reality, however, DP-ACT is not limited by any such assumptions, as demonstrated in the evaluation section, since we do not make any assumptions in relation to the contact group size in the datasets used in the simulations.

[4] This is valid under the assumption that the contacts and interaction patterns/graphs among the users are at random, but assuming an average degree d for the active users.

Proof. According to Theorem 3.3, when there are Q active users with the average degree of d at any specific time t, the average number of passive users who do not have PHR contact with any active users is:

$$H = N \cdot (1-q) \cdot (1 - \frac{d}{N-1})^{N \cdot q}.$$

If one uninfected user among these passive users has high-risk contact with at least one infected passive user, this high-risk contact will remain undetected as these passive users do not have PHR contact with any active users. Hence, we should find the average number of these passive users who have not been in high-risk contact with any infected users. If one uninfected user among these passive users has contact with another user, with the probability of $\frac{N-c\cdot N-1}{N-1}$ this user is an uninfected one. Thus, for a user, the probability of being an uninfected one while having d PHR contacts with uninfected users is $(\prod_{l=1}^{d} \frac{N-c\cdot N-l}{N-l}) \cdot \frac{N-c\cdot N}{N}$. Hence, the average number of uninfected passive users having PHR contacts only with uninfected passive users and not any active users is $H \cdot (\prod_{l=1}^{d} \frac{N-c\cdot N-l}{N-l}) \cdot \frac{N-c\cdot N}{N}$.

Hence, the average number of high-risk users who do not receive the high-risk alarm, H_{missed}, is:

$$\begin{aligned} H_{missed} &= H \cdot \frac{N-c\cdot N}{N} - H \cdot (\prod_{l=1}^{d} \frac{N-c\cdot N-l}{N-l}) \cdot \frac{N-c\cdot N}{N} \\ &= H \cdot \frac{N-c\cdot N}{N} \cdot (1 - \prod_{l=1}^{d} \frac{N-c\cdot N-l}{N-l}) \\ &= N \cdot (1-q) \cdot (1 - \frac{d}{N-1})^{N\cdot q} \cdot (1-c) \cdot (1 - \prod_{l=1}^{d} \frac{N-c\cdot N-l}{N-l}). \end{aligned}$$

□

Assuming a population size of $N = 100$, $C = 20\%$ and a conservative value of $d = 2$, for $q = 0.3$ and $q = 0.7$, the average numbers of the undetected high-risk users, under the proposed DP-ACT protocol, are approximated to be 11 and 2, respectively.

3.2 Privacy and Security Analysis

In this section, we briefly discuss potential privacy and security risks in DP-ACT. In our DP-ACT protocol, we mitigate the risk of device identification based on broadcasted BLE beacons for passive users by allowing them not to broadcast BLE beacons.

Passive users, if not infected, remain entirely "hidden" and retain ultimate privacy (ignoring electromagnetic side channels), similar to those who do not participate in digital contact tracing. For perspective, only 0.02% of the Singapore population were diagnosed with COVID-19 from January 23 to April 3, 2020 [23], which means that in similar situations, approximately 99.98% of passive users remain private and at most 0.02% would reveal their high-risk contact IDs. At the same time, infected passive users (i.e., up to estimated 0.02%) would reveal exclusively IDs corresponding to the high-risk contacts, which is approximated to be less than eight high-risk contacts during 71 days for each user [23]. Revealing these high-risk contacts may, however, leak information about high-risk active users and may expose them to correlation attacks, impacting their privacy. Similar information leakage may be envisioned in the case of the DP-3T protocol if the adversaries (active users or those who do not participate in contact tracing) collect and share the IDs broadcasted by other active users.

The risk of device identification based on the broadcasted BLE beacons remains, however, valid for active users in the proposed DP-ACT protocol. In the DP-3T protocol, this risk is valid for all users. On the other hand, actively broadcasting pseudo-random IDs allows a more accurate high-risk contact identification for the active user. As a result, active users opt for a *more accurate high-risk contact detection*, accepting these privacy concerns. Hence, there is an inherent trade-off between privacy and utility.

While our key focus was on utility, there are also security risks associated with DP-ACT, e.g., passive users who actively tamper with the protocol by uploading the IDs broadcasted by other active users. Similar security risks can also be discussed in the context of the DP-3T protocol, e.g., users who tamper with the protocol by uploading their own IDs to the cloud. Another security risk is flooding and replay attacks to trigger alerts. One strategy for both protocols is to require both active and passive users to upload verification confirming their diagnosis when they test positive before uploading their own or other users' IDs. We refer to the DP-3T risk analysis[5] for further discussion of potential attacks.

4 EVALUATION

In this section, we evaluate the proposed DP-ACT protocol using a face-to-face individual interaction dataset and five real-world BLE datasets in Subsection 4.1 and Subsection 4.2, respectively. All codes are available online.[6]

4.1 Face-to-Face Individual Interaction Dataset

For the evaluation of the proposed protocol, first, we consider the InVS15 dataset [14]. InVS15 contains the face-to-face interactions of individuals measured during 12 days in an office building in France in 2015. We assume that all participants use COVID-19 contact tracing mobile applications. COVID-19 has a serial interval, i.e., the time from illness onset in a primary case (infector) to illness onset in a secondary case (infected) [24], with a median of 4 days. We have considered that all users who had high-risk contact with infected users will be infected and can transfer the virus to other people after 4 days from the high-risk contacts. For simplicity, we have also assumed that none of these newly infected users can be detected without receiving the high-risk alarms due to the lack of symptoms. We consider several scenarios with different percentages ($c\%$) of initial infected users, and the objective is to find all users who had high-risk contacts with them and previous high-risk users after 4 days. We update the set of infected users who likely transfer the virus to other users (after 4 days from having a high-risk contact) day by day. For the InVS15 dataset, we define a high-risk contact as a face-to-face contact that is longer than or equal to 5 minutes.

In our simulations, we consider 1,000 runs with random COVID-19 infected users and random indexes for passive users. The *high-risk case detection probability* is defined as the ratio of the detected high-risk cases to the total number of the high-risk cases, averaged

[5] DP-3T github.
[6] DP-ACT github.

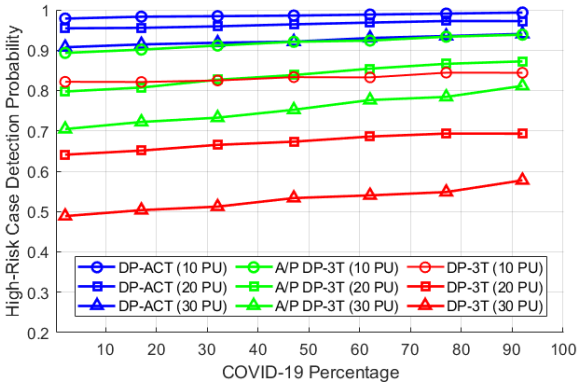


Figure 4: High-risk case detection probability versus COVID-19 percentage for the percentage of the passive users equal to 10%, 20%, and 30% when we have only considered the first 4 days of the data collection.

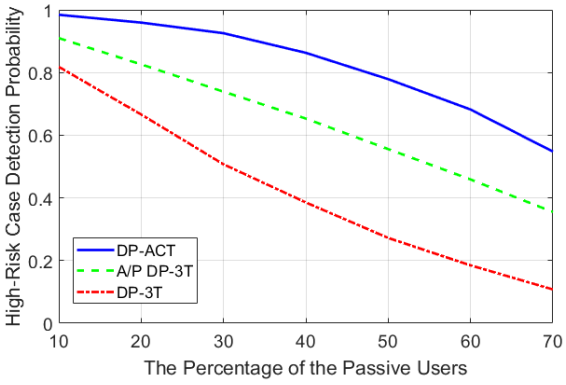


Figure 5: High-risk case detection probability versus the percentage of passive users when COVID-19 percentage is 30% and for the first 4 days of the data collection.

over these 1,000 runs. A high-risk case is a person who has a high-risk contact with an infected person (the revealed ones or the ones who are infected by revealed ones and can transfer the virus to others after 4 days). The *COVID-19 percentage* is also defined as the number of revealed COVID-19 infected users to the total number of users. As discussed before, we assume that the passive users do not install the application based on the DP-3T protocol.

Let us start by considering only the first 4 days of the data. In Fig. 4, we show the high-risk case detection probability versus COVID-19 percentage for the percentages of the passive users (PU) of 10%, 20%, and 30%, when we only consider the first 4 days of the data. We observe that using our proposed DP-ACT protocol, only less than 10% of the high-risk cases are not detected when the percentage of the passive users is less or equal to 30% and COVID-19 percentage is larger than 2%. On the other hand, considering the DP-3T and A/P DP-3T protocols, for the passive user percentage of 30%, more than 42% and 18% of the high-risk cases are not detected.

Let us define *False Alarm Probability* as the number of users who did not have a high-risk contact but received the high-risk alarm over the number of the users. According to the simulation results, the average false alarm rate for Fig. 4 (for 10% PU, 20% PU, and 30% PU when COVID-19 percentage lies between 2% to 100%) in the worst case is less than 0.022.

Fig. 5 shows the high-risk case detection probability versus the percentage of passive users for the first 4 days of the data, when 30% of the users are diagnosed with COVID-19. Here, again we observe that our proposed DP-ACT protocol outperforms the DP-3T and A/P DP-3T protocols. If we consider the proposed DP-ACT protocol, the high-risk case detection probability is greater than or equal to 0.8 when the percentage of active users exceeds 53%, while for the DP-3T and A/P DP-3T protocols, we need at least 88% and 77% active users, respectively, to achieve the detection probability of 0.8.

Now, we consider the entire 12 days in the dataset, and not only the first 4 days. Therefore, the error propagation due to not detecting the high-risk contacts in the first 4 days is also considered in the results. The high-risk case detection probability versus COVID-19 percentage for the percentages of the passive users equal to 10%, 20%, and 30% is presented in Fig. 6. The proposed protocol improves the high-risk case detection probability of the COVID-19 contact-tracing application significantly, e.g., the high-risk case detection probability of the DP-ACT protocol is 0.41 and 0.19 higher than the ones of DP-3T and A/P DP-3T, respectively, when 10% of the users are diagnosed with COVID-19 and 30% of users are passive. As it can be observed in Fig. 6, the gap between the DP-ACT protocol and both DP-3T and A/P DP-3T generally increases with the number of passive users.

Fig. 7 shows the high-risk case detection probability versus the percentage of passive users for the entire dataset, assuming 30% of the users are diagnosed with COVID-19. The high-risk user detection probability is 0.7 when the percentage of passive users is 59% if we use the proposed DP-ACT protocol, while for the DP-3T and A/P DP-3T protocols, the detection probability equals to 0.49 and 0.2, respectively, for the same percentage of passive.

Next, we estimate the transfer costs and storage requirements of the proposed DP-ACT protocol and compare it against the state-of-the-art DP-3T protocol. We define *Average Transfer Cost* as the sum of the average number of bytes sent to the cloud by a device and the average number of bytes downloaded from the cloud by a device. We also define *Average Storage* for a user as the sum of the average number of bytes downloaded from the cloud by a device, the average number of bytes for recording the own device pseudo-random IDs, and the average number of bytes for recording the IDs of other devices, time of the receiving the beacons, and the RSS values. Let us consider the low-cost design for ephemeral pseudo-random IDs just like Troncoso et al. [32], which means every day, a new random seed is generated by each device. We also consider that every 30 minutes, each device produces a new pseudo-random ID. For BLE beacon broadcasting, we consider that every 5 minutes, 8 beacons with time distances of 250 ms are sent by an active user device [27]. Note that in the A/P DP-3T protocol, the passive users do not send their pseudo-random IDs to the cloud as these IDs are neither broadcast nor recorded on other users' devices. We assume

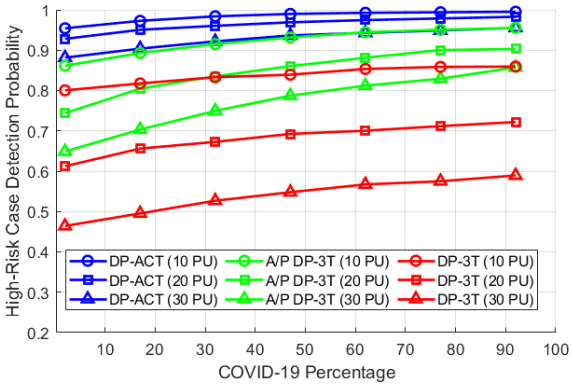


Figure 6: High-risk case detection probability versus COVID-19 percentage when 10%, 20%, and 30% of the users do not broadcast BLE beacons and the entire InVS15 dataset is used for evaluation.

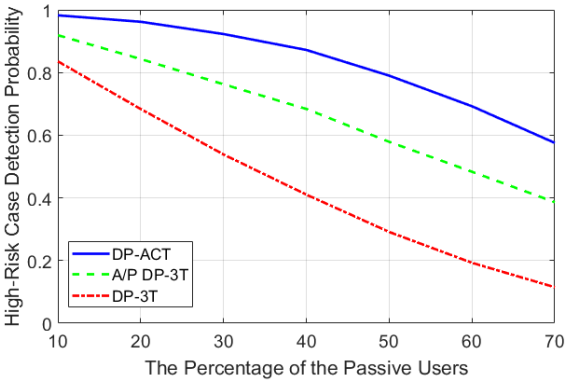


Figure 7: High-risk case detection probability versus the percentage of passive users for the entire InVS15 dataset when COVID-19 percentage is 30%.

that for each ID, 16 bytes are allocated. Each seed is 32 bytes. The storage needs for recording the contact time and an RSS value are also considered as 20 bits and 1 byte, respectively. In our DP-ACT protocol, we need one extra bit for each ID as we should determine the type of the ID (IDs may be revealed by active users or by passive users).

Table 1 presents the average transfer cost and average storage need for a device while the entire InVS15 dataset is used, assuming 20% passive users and the percentage of COVID-19 diagnosed cases of 5%. As shown in Table 1, the DP-3T protocol consumes the least average storage because in the case of using this protocol, 20% of people do not install the application and hence, do not consume any storage and transfer cost. In summary, our proposed DP-ACT protocol for 20% passive users and the COVID-19 percentage of 5% has around 3.3 times transfer cost and less than 1.3 times storage need compared to the state-of-the-art DP-3T protocol.

While we have investigated the efficiency of DP-ACT in the context of small population sizes using real datasets, the relevance of this protocol in large-scale needs further investigation. However, no such large datasets exist. To gain insight, we can consider the information provided by Ng et al. [23], who observed that, from Jan 23 to April 3, 2020, 7,770 close/high-risk contacts (1,863 household contacts, 2319 work contacts, and 3,588 social contacts) linked to 1,114 PCR-confirmed index cases were identified in Singapore. Note that the transfer cost of the DP-ACT protocol depends on the number of high-risk contacts, which is less than 8 per person during the 71 days of data collection, not the contact number. Hence, considering the aforementioned assumptions and the population of 5.686 million people in Singapore in 2020, the average transfer cost for the DP-ACT protocol is approximately 33.7 Kbytes when the percentage of passive users is 20%, while it approximately equals 23.5 Kbytes and 29.5 Kbytes for DP-3T and A/P DP-3T, respectively. The contact number determines the order of average storage needs, as the daily contact number is usually significantly larger than the number of daily high-risk contacts for a user. Hence, storage needs are within the same order of magnitude for the three protocols.

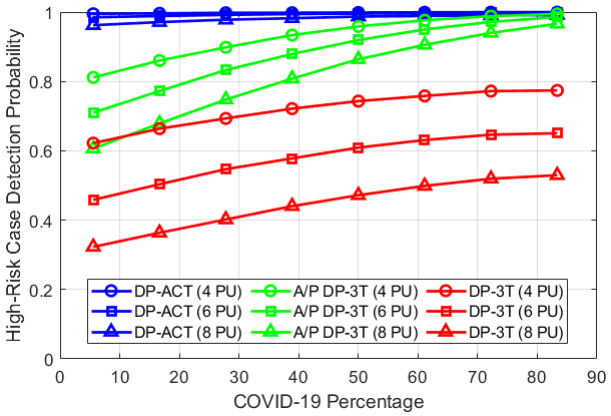
Table 1: Average transfer cost and average storage (in bytes) for a user when 20% of cases are passive users and 5% diagnosed with COVID-19.

	DP-3T	A/P DP-3T	DP-ACT
Average Transfer Cost	363	455	1191
Average Storage	381 K	479 K	480 K

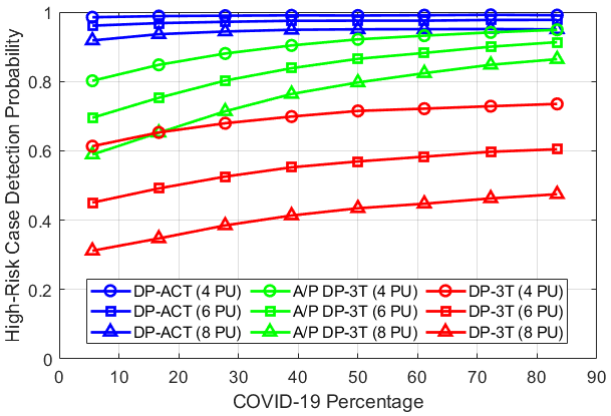
4.2 Real-World BLE Datasets

In this section, we consider real-world BLE datasets collected considering five different scenarios: dining together at the table, "scenario01-lunch"; riding a train together, "scenario02-train"; working together in an open-space setting, "scenario03-work"; waiting in line at the supermarket, "scenario04-queue", and mingling in a club/bar, "scenario05 -party" [27, 32]. These datasets were collected in laboratory conditions, and 20 users participated in these data collections (the information regarding 2 participants is missed and the datasets are collected by the other 18 users) with different smartphone models. The duration of the data collection for each of these datasets is 30 minutes. The smartphone devices exchange BLE advertisements with neighbouring devices every 2.5 - 5 minutes, and the attenuation of a beacon gives the probability of being within a certain distance from the smartphone broadcasting the beacon [27]. Here, we calculate the attenuation by function MODEL_RX_TX_COMPENSATION [27] and for simplicity, assume that both devices involved in a contact calculate the correct attenuation. Furthermore, just like the current configuration for SwissCovid [22], we define the exposure score as ES = $B_1 + \frac{B_2}{2}$, where B_1 and B_2 are the time duration of exposures for attenuation within (0,55] and (55,63], respectively. For the new simulations, we call a contact a high-risk one if ES is greater than or equal to 15 minutes and consider 10,000 runs with random COVID-19 infected users and random indexes for passive users.

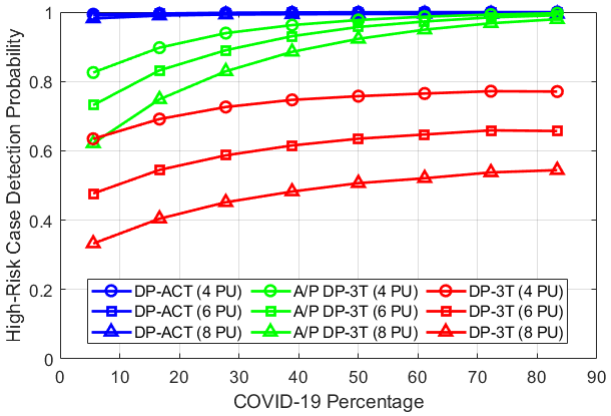
Fig. 8 presents the high-risk case detection probability versus COVID-19 percentage for 4, 6, and 8 passive users (PU), considering the real-world BLE datasets. According to this figure, when the



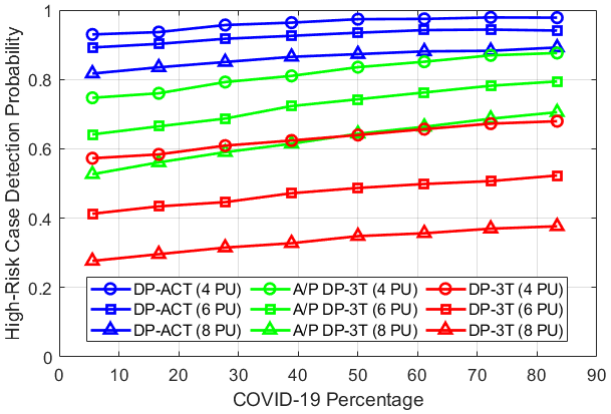
(a) Lunch Dataset.



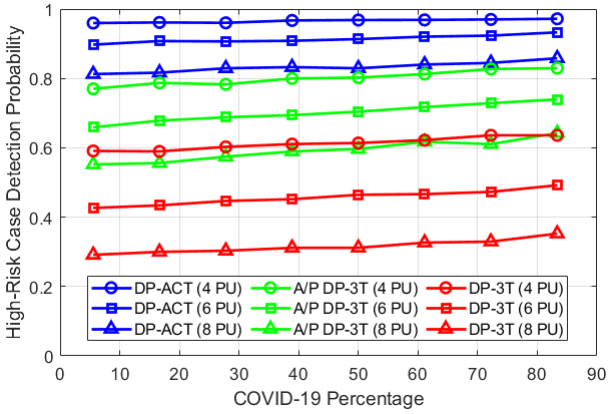
(b) Work Dataset.



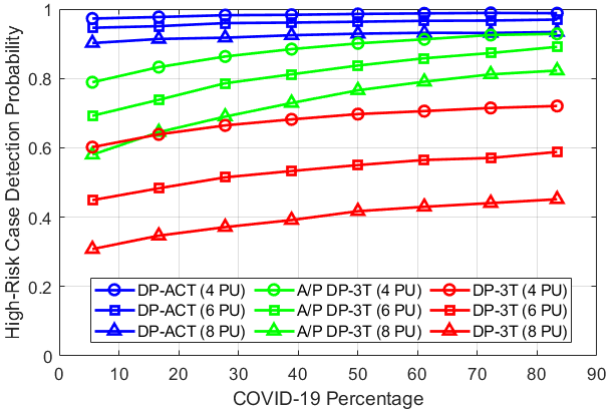
(c) Train Dataset.



(d) Queue Dataset.

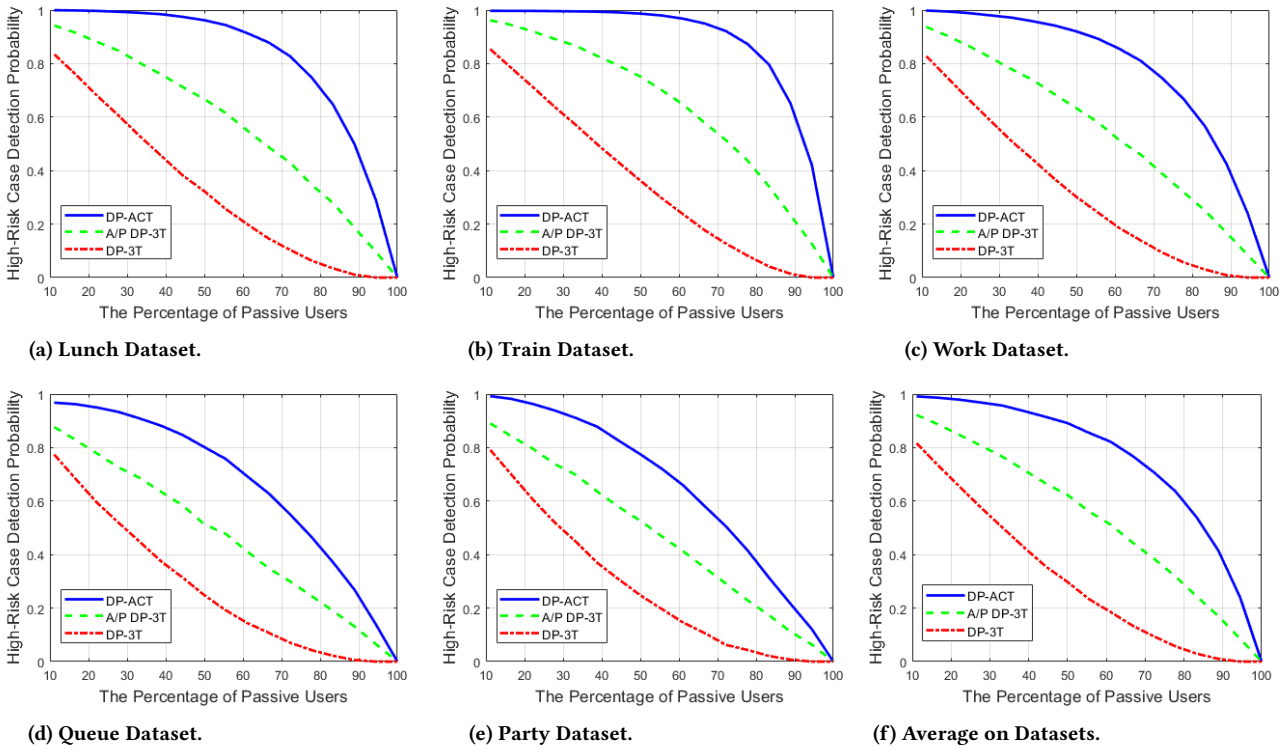


(e) Party Dataset.



(f) Average on all datasets.

Figure 8: High-risk case detection probability versus COVID-19 percentage for the number of the passive users equal to 4, 6, and 8 when real-world BLE datasets are used.



(a) Lunch Dataset. **(b) Train Dataset.** **(c) Work Dataset.**

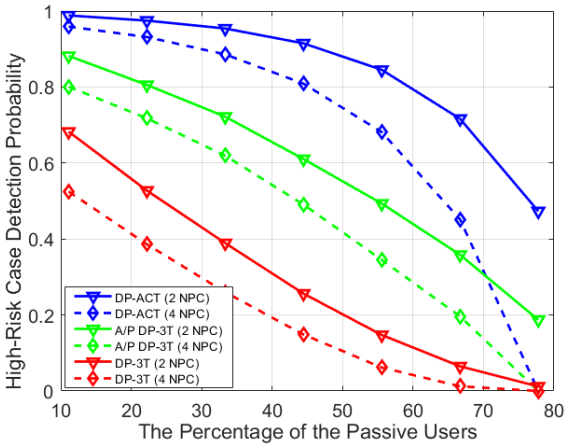
(d) Queue Dataset. **(e) Party Dataset.** **(f) Average on Datasets.**

Figure 9: High-risk case detection probability versus the percentage of passive users for real-world BLE datasets when 5 users are diagnosed with COVID-19.

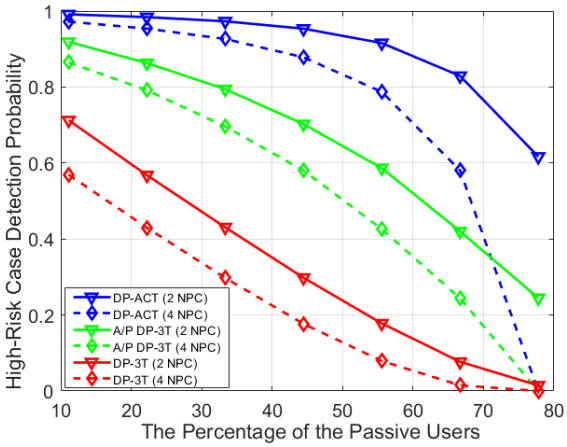
number of passive users is 8 and the COVID-19 percentage is around 5%, the proposed DP-ACT protocol outperforms the DP-3T protocol by 0.64, 0.61, 0.65, 0.54, and 0.53 in terms of the high-risk case detection probability for the lunch, work, train, queue, and party datasets, respectively, with an average of 0.6. Furthermore, when the number of passive users is 8 and the COVID-19 percentage is around 5%, the proposed DP-ACT protocol outperforms the A/P DP-3T protocol by 0.35, 0.33, 0.36, 0.29, and 0.26 in terms of the high-risk case detection probability for the lunch, work, train, queue, and party datasets, respectively, with an average of 0.31. We observe that when the proposed DP-ACT protocol is adopted, for the number of passive users less than 8 and COVID-19 percentages more than 5%, the high-risk case detection probability is higher than 0.96, 0.91, 0.98, 0.82, and 0.81 for the lunch, work, train, queue, and party datasets, respectively, with an average higher than 0.9. The average false alarm probability on all the datasets for Fig. 8 (C=4, C=6, and C=8 when COVID-19 percentage lies between 5% to 100%) in the worst case is less than 0.035.

Fig. 9 shows the high-risk case detection probability versus the percentage of passive users when five users are diagnosed with COVID-19 and real-world BLE datasets are used. According to Fig. 9, the high-risk case detection probability for the proposed protocol is higher than 0.8, when the percentages of passive users are lower than 74%, 83%, 67%, 50%, and 47% for the lunch, train, work, queue, and party datasets, respectively, with an average of 64%. On the other hand, to achieve a high-risk case detection probability higher than 0.8 for the A/P DP-3T, the percentage of passive users needs to be lower than 33%, 30%, 43%, 20%, and 22% for the lunch, work, train, queue and party datasets, respectively. Moreover, to achieve a high-risk case detection probability higher than 0.8 for DP-3T, the percentage of passive users needs to be lower than 13%, 13%, and 15% for the lunch, work, and train datasets, respectively. For the queue and party datasets, for passive user percentages of more than 11 and 5 infected users, the best high-risk case detection probability is 0.77 and 0.79, respectively (less than 0.8).

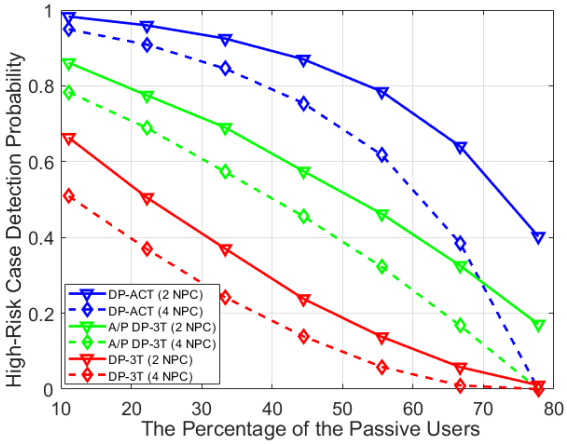
Finally, we evaluate the protocols considering a third group of people (in addition to the active and passive users), who do not install any COVID-19 contact-tracing applications. We refer to this group of people as Non-Playing Cases (NPC). Fig. 10 shows the high-risk case detection probability versus the percentage of passive users, when the real-world BLE datasets are considered. Here, we assume five users are diagnosed with COVID-19 and there are two or four non-playing cases. We observe that the performance of the protocols decreases when the number of non-playing cases increases. Furthermore, we observe that the proposed DP-ACT still significantly outperforms the state-of-the-art DP-3T protocol and the A/P DP-3T protocol, e.g., by 0.28 and 0.6, respectively, overall in terms of high-risk case detection probability, when there are 2 or 4 NPCs and the percentage of passive users is 45%.



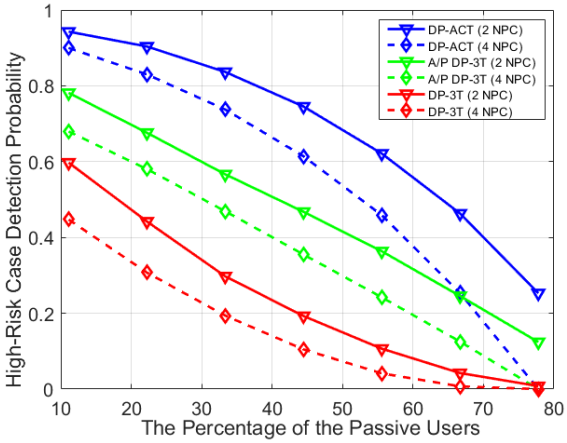
(a) Lunch Dataset.



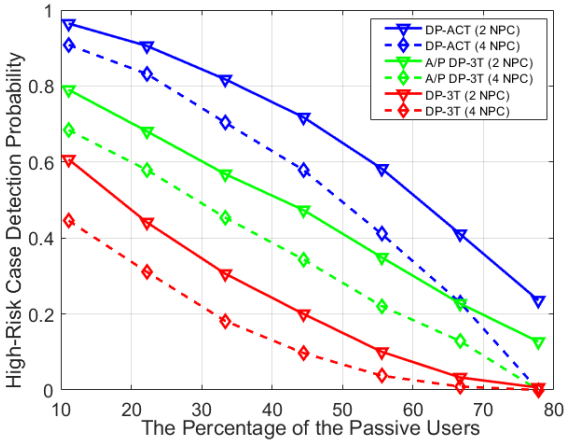
(b) Train Dataset.



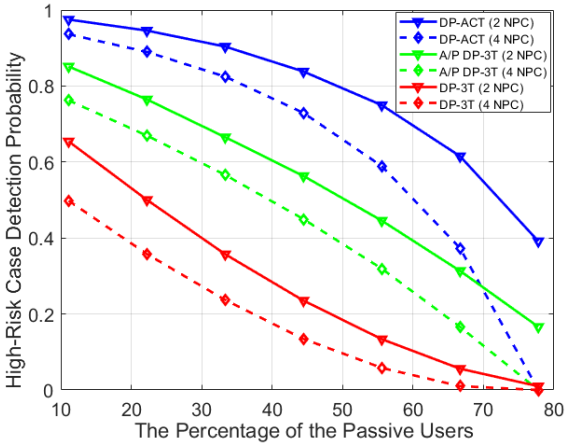
(c) Work Dataset.



(d) Queue Dataset.



(e) Party Dataset.



(f) Average on all datasets.

Figure 10: High-risk case detection probability versus the percentage of passive users for real-world BLE datasets when 5 users are diagnosed with COVID-19 and there are some non-playing cases.

5 CONCLUSIONS

In this paper, we have proposed a decentralized privacy-preserving contact tracing protocol with both active and passive participants, where passive participants model conservative users who do not broadcast BLE beacons but still listen to broadcasted BLE beacons. Our proposed DP-ACT protocol enables precision digital contact tracing, by enabling and leveraging the participation of conservative/passive users. We analyzed the proposed protocol theoretically and discussed a set of interesting properties for DP-ACT. The proposed protocol is evaluated considering both a face-to-face individual interaction dataset and five real-world BLE datasets. Our simulation results demonstrate that our DP-ACT protocol outperforms the state-of-the-art protocols in the presence of passive users.

In this work, our key focus has been on utility. In our future work, we plan to investigate more privacy/security risks associated with DP-ACT. Another promising future direction is to also consider a semi-active/semi-passive participant model where the participants opt to broadcast their pseudo-random IDs at arbitrary locations.

ACKNOWLEDGMENTS

This research has been partially supported by the Wallenberg AI, Autonomous Systems and Software Program (WASP), Swedish Research Council (VR), and Swedish Promobilia Foundation.

REFERENCES

[1] Nadeem Ahmed, Regio A Michelin, Wanli Xue, Sushmita Ruj, Robert Malaney, Salil S Kanhere, Aruna Seneviratne, Wen Hu, Helge Janicke, and Sanjay K Jha. 2020. A survey of COVID-19 contact tracing apps. *IEEE access* 8 (2020), 134577–134601.

[2] Samuel Altmann, Luke Milsom, Hannah Zillessen, Raffaele Blasone, Frederic Gerdon, Ruben Bach, Frauke Kreuter, Daniele Nosenzo, Séverine Toussaert, Johannes Abeler, et al. 2020. Acceptability of app-based contact tracing for COVID-19: Cross-country survey study. *JMIR mHealth and uHealth* 8, 8 (2020), e19857.

[3] Thamer Altuwaiyan, Mohammad Hadian, and Xiaohui Liang. 2018. EPIC: efficient privacy-preserving contact tracing for infection detection. In *2018 IEEE International Conference on Communications (ICC)*. IEEE, 1–6.

[4] Shamshul Bahri. 2007. Enhancing quality of data through automated SARS contact tracing method using RFID technology. *International journal of networking and virtual organisations* 4, 2 (2007), 145–162.

[5] Jason Bay, Joel Kek, Alvin Tan, Chai Sheng Hau, Lai Yongquan, Janice Tan, and Tang Anh Quy. 2020. BlueTrace: A privacy-preserving protocol for community-driven contact tracing across borders. *Government Technology Agency-Singapore, Tech. Rep* 18 (2020), 1.

[6] Alessandro Blasimme, Agata Ferretti, and Effy Vayena. 2021. Digital contact tracing against COVID-19 in Europe: current features and ongoing developments. *Frontiers in Digital Health* 3 (2021), 61.

[7] Isobel Braithwaite, Thomas Callender, Miriam Bullock, and Robert W Aldridge. 2020. Automated and partly automated contact tracing: a systematic review to inform the control of COVID-19. *The Lancet Digital Health* 2, 11 (2020), e607–e621.

[8] Manuel Cebrian. 2021. The past, present and future of digital contact tracing. *Nature Electronics* 4, 1 (2021), 2–4.

[9] Eugene Y. Chan and Najam U. Saqib. 2021. Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior* 119 (2021), 106718.

[10] Eugene Y Chan and Najam U Saqib. 2021. Privacy concerns can explain unwillingness to download and use contact tracing apps when COVID-19 concerns are high. *Computers in Human Behavior* 119 (2021), 106718.

[11] Hyunghoon Cho, Daphne Ippolito, and Yun William Yu. 2020. Contact tracing mobile apps for COVID-19: Privacy considerations and related trade-offs. *arXiv preprint arXiv:2003.11511* (2020).

[12] Katayoun Farrahi, Remi Emonet, and Manuel Cebrian. 2014. Epidemic contact tracing via communication traces. *PloS one* 9, 5 (2014), e95133.

[13] Luca Ferretti, Chris Wymant, Michelle Kendall, Lele Zhao, Anel Nurtay, Lucie Abeler-Dörner, Michael Parker, David Bonsall, and Christophe Fraser. 2020. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science* 368, 6491 (2020), eabb6936.

[14] 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), 1–18.

[15] Hadi Givehchian, Nishant Bhaskar, Eliana Rodriguez Herrera, Héctor Rodrigo López Soto, Christian Dameff, Dinesh Bharadia, and Aaron Schulman. 2022. Evaluating Physical-Layer BLE Location Tracking Attacks on Mobile Devices. In *2022 IEEE Symposium on Security and Privacy (SP)*. 1690–1704.

[16] Farkhondeh Hassandoust, Saeed Akhlaghpour, and Allen C Johnston. 2021. Individuals' privacy concerns and adoption of contact tracing mobile applications in a pandemic: A situational privacy calculus perspective. *Journal of the American Medical Informatics Association* 28, 3 (2021), 463–471.

[17] Yue Huang, Borke Obada-Obieh, Elissa M Redmiles, Satya Lokam, and Konstantin Beznosov. 2022. COVID-19 Information-Tracking solutions: a qualitative investigation of the factors influencing people's adoption intention. In *ACM SIGIR Conference on Human Information Interaction and Retrieval*. 12–24.

[18] Gabriel Kaptchuk, Daniel G Goldstein, Eszter Hargittai, Jake M Hofman, and Elissa M Redmiles. 2022. How good is good enough? quantifying the impact of benefits, accuracy, and privacy on willingness to adopt covid-19 decision aids. *Digital Threats: Research and Practice (DTRAP)* 3, 3 (2022), 1–18.

[19] Robert A Kleinman and Colin Merkel. 2020. Digital contact tracing for COVID-19. *Cmaj* 192, 24 (2020), E653–E656.

[20] Tianshi Li, Camille Cobb, Jackie Junrui Yang, Sagar Baviskar, Yuvraj Agarwal, Beibei Li, Lujo Bauer, and Jason I Hong. 2021. What makes people install a COVID-19 contact-tracing app? Understanding the influence of app design and individual difference on contact-tracing app adoption intention. *Pervasive and Mobile Computing* 75 (2021), 101439.

[21] Elliot Mbunge. 2020. Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls. *Diabetes & Metabolic Syndrome: Clinical Research & Reviews* 14, 6 (2020), 1631–1636.

[22] Cédric Moullet and Sebastian Matyas. 2020. SwissCovid-ExposureScore. https://github.com/admin-ch/PT-System-Documents/blob/master/SwissCovid-ExposureScore.pdf.

[23] Oon Tek Ng, Kalisvar Marimuthu, Vanessa Koh, Junxiong Pang, Kyaw Zaw Linn, Jie Sun, Liang De Wang, Wan Ni Chia, Charles Tiu, Monica Chan, et al. 2021. SARS-CoV-2 seroprevalence and transmission risk factors among high-risk close contacts: a retrospective cohort study. *The Lancet infectious diseases* 21, 3 (2021), 333–343.

[24] Hiroshi Nishiura, Natalie M Linton, and Andrei R Akhmetzhanov. 2020. Serial interval of novel coronavirus (COVID-19) infections. *International journal of infectious diseases* 93 (2020), 284–286.

[25] James O'Connell, Manzar Abbas, Sarah Beecham, Jim Buckley, Muslim Chochlov, Brian Fitzgerald, Liam Glynn, Kevin Johnson, John Laffey, Bairbre McNicholas, et al. 2021. Best practice guidance for digital contact tracing apps: a cross-disciplinary review of the literature. *JMIR mHealth and uHealth* 9, 6 (2021), e27753.

[26] Michael J Parker, Christophe Fraser, Lucie Abeler-Dörner, and David Bonsall. 2020. Ethics of instantaneous contact tracing using mobile phone apps in the control of the COVID-19 pandemic. *Journal of Medical Ethics* 46, 7 (2020), 427–431.

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

[28] Elissa M Redmiles. 2020. User concerns & tradeoffs in technology-facilitated COVID-19 response. *Digital Government: Research and Practice* 2, 1 (2020), 1–12.

[29] Lucy Simko, Ryan Calo, Franziska Roesner, and Tadayoshi Kohno. 2020. COVID-19 contact tracing and privacy: studying opinion and preferences. *arXiv preprint arXiv:2005.06056* (2020).

[30] Hallam Stevens and Monamie Bhadra Haines. 2020. Tracetogether: pandemic response, democracy, and technology. *East Asian Science, Technology and Society: An International Journal* 14, 3 (2020), 523–532.

[31] Carmela Troncoso, Dan Bogdanov, Edouard Bugnion, Sylvain Chatel, Cas Cremers, Seda Gürses, Jean-Pierre Hubaux, Dennis Jackson, James R Larus, Wouter Lueks, et al. 2022. Deploying decentralized, privacy-preserving proximity tracing. *Commun. ACM* 65, 9 (2022), 48–57.

[32] Carmela Troncoso, Mathias Payer, Jean-Pierre Hubaux, Marcel Salathé, James Larus, Edouard Bugnion, Wouter Lueks, Theresa Stadler, Apostolos Pyrgelis, Daniele Antonioli, et al. 2020. Decentralized privacy-preserving proximity tracing. *arXiv preprint arXiv:2005.12273* (2020).

[33] Chaoshun Zuo, Haohuang Wen, Zhiqiang Lin, and Yinqian Zhang. 2019. Automatic fingerprinting of vulnerable ble iot devices with static uuids from mobile apps. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. 1469–1483.