

Stop COVID ou encore ? Traçage numérique : une solution ?



La tentation masquée

AMUSEC 2021 – 9 avril

Jean-Jacques Quisquater

UCLouvain, MIT, Académie Royale de Belgique

Une stratégie démocratique de
traçage du coronavirus :
géolocalisation, backtracking,
contact tracking ... ?

Vers un déconfinement sain ?

Note liminaire

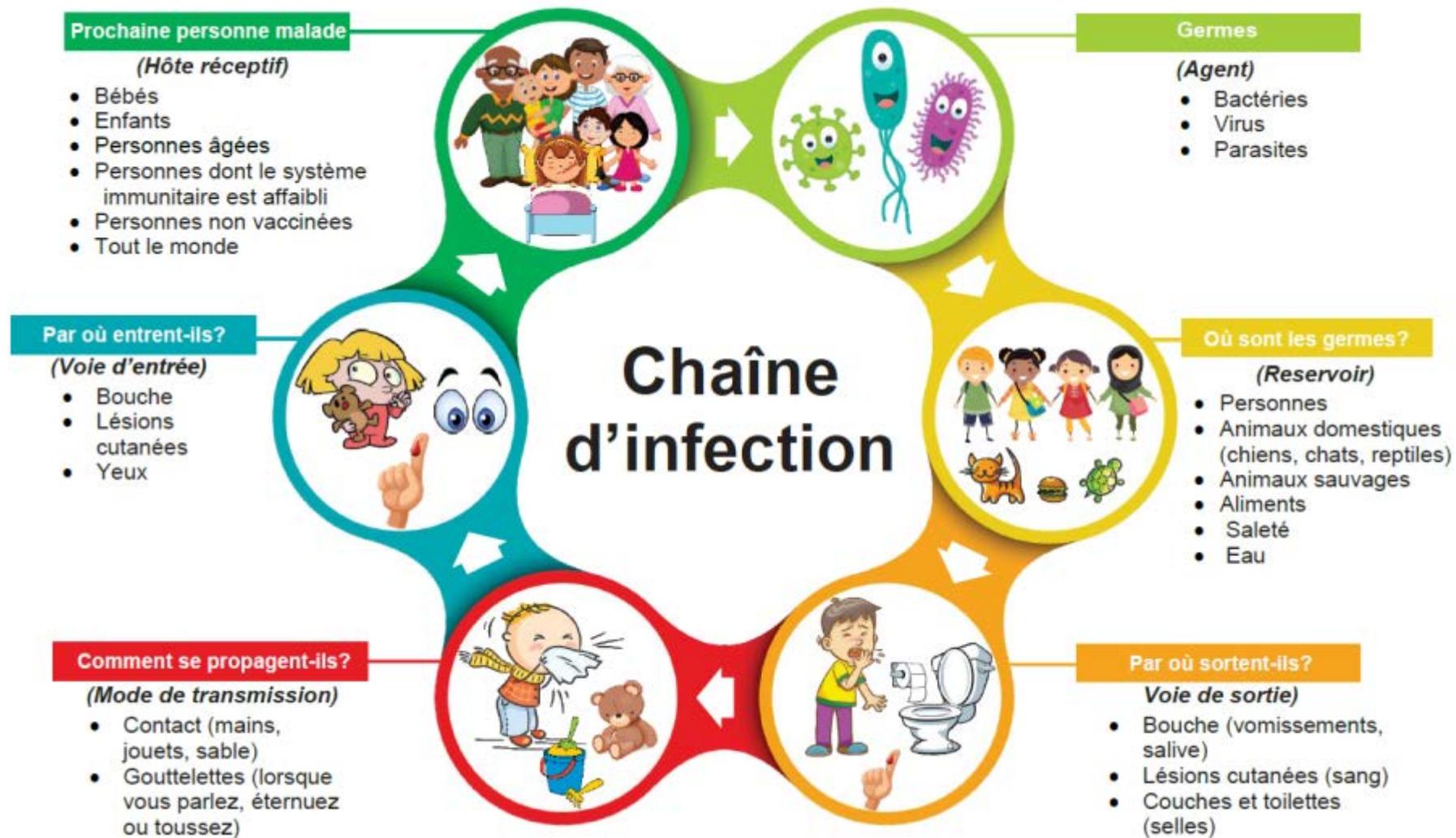
- Cette présentation se veut la plus objective possible, pas le plus complet, en n'étant pas trop technique, et ne défend en particulier aucune position. Ce qui ne veut pas dire que l'auteur n'a pas sa propre opinion. Je me suis renseigné aux meilleures sources, souvent en recoupant, et toutes les erreurs sont miennes. Merci pour vos commentaires et corrections.
- Pour des infos plus techniques, un bon point de départ est :
https://en.wikipedia.org/wiki/Digital_contact_tracing

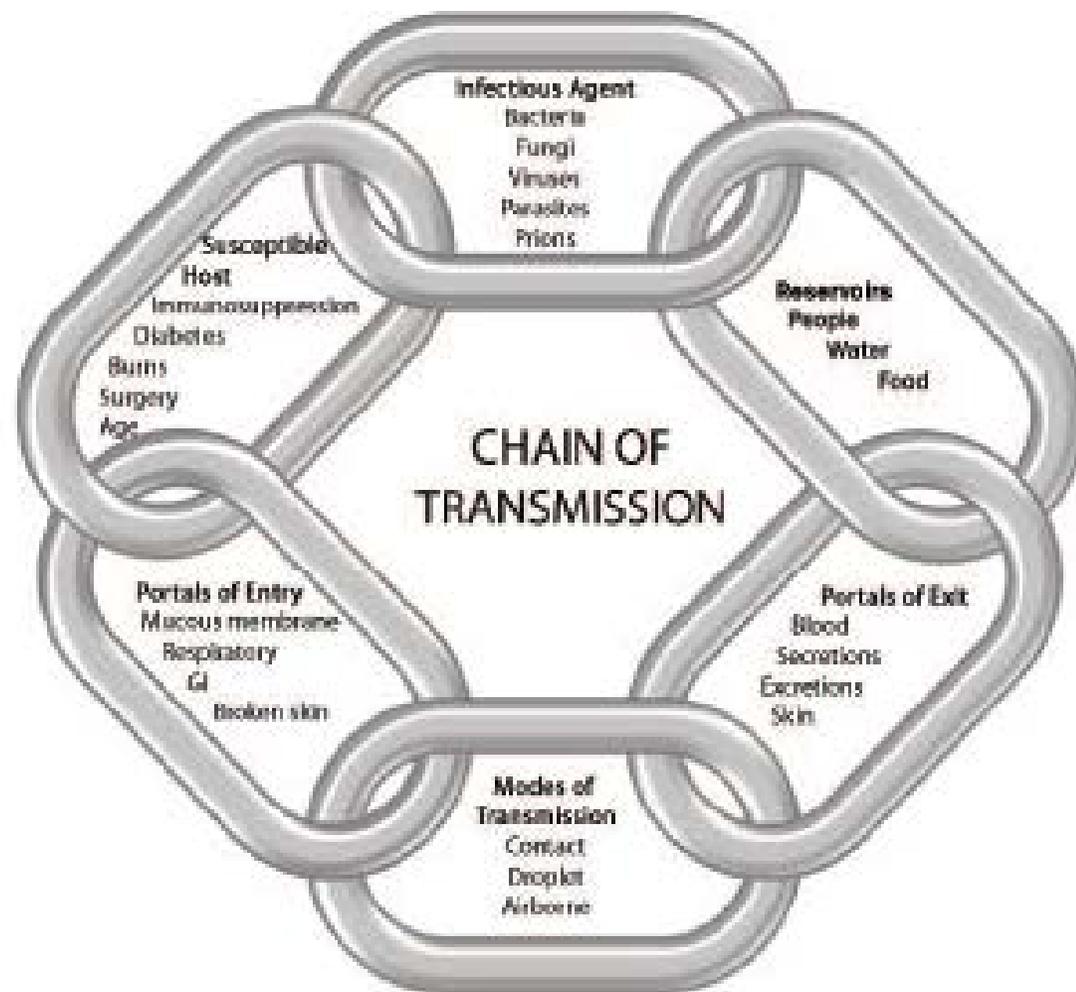
Présentation : Jean-Jacques Quisquater

- Responsable d'un groupe de travail initié par Hugues Bersini (UIB) à l'Académie Royale de Belgique, classe Technologie et Société,
- Animateur, avec d'autres, d'une liste de discussions en France sur ces apps numériques, en accompagnement de l'app française,
- Je connais à peu près tout le monde dans ce domaine et beaucoup viennent de la recherche en sécurité informatique, en cryptologie, en vue de protéger au mieux la vie privée.

En guise d'introduction

- **Juillet 1866** : dernière épidémie de choléra en Belgique, qui fera 43.000 morts sur une population de 4.800.000 habitants, soit presque un pour mille. En France, le nombre de morts est quasi le même !
- Ceci éveillera la vocation d'un médecin, Adrien Proust, venant juste de recevoir son agrégation de médecine. Il décide de consacrer sa carrière à la lutte contre les maladies contagieuses. Il promeut alors la création d'un **droit sanitaire international** et d'un **office international d'hygiène** publique, l'ancêtre de l'OMS.
- L'épidémie vaincue, il fait de la lutte contre les maladies contagieuses son combat ; une sorte de plus jamais ça ! (citation de Jean-Marc Quaranta) Il promeut l'hygiène, éviter les grands rassemblements, contrôler le commerce international, etc, pour limiter les contagions : et cela à l'échelle de leur croissance. Il n'a pas été assez écouté ni alors ni même aujourd'hui.
- Oui, c'est le père de Marcel Proust l'auteur de « A la recherche du temps perdu » ... Thème toujours d'actualité !





*On ne peut pas briser de chaînes
quand il n'y en a pas de visibles.*

Le Procès (1933) de Franz Kafka

*On ne peut pas briser de chaînes
quand il n'y en a pas de visibles.*

Le Procès (1933) de Franz Kafka

=> **Traçage**

Était-ce prévisible ? Etions-nous prêts ? Vers ... « continuous prevention, protection, and resilience. »

- Il y a eu pas mal d'avertissements de la possibilité de nouvelles pandémies,
- Des outils ? Voir H2020 PANDEM DRS-2014 (2015-2017) - PANDEmic risk and Emergency Management - Feasibility study for strengthening capacity-building for health and security protection in case of large-scale pandemics – Phase I Demo
- Peu de réactions ...,
- Nous n'étions pas prêts !

Revenons au début (mars 2020)

- En Belgique, le confinement a été annoncé le **17 mars**, idem en France,
- A Singapour, la recherche de moyens de traçage automatique a déjà commencé, et l'appli **Tracetogether** est lancée le **20 mars**,
- Il semble bien avoir un suivi en Europe puisque le 23 mars est déjà annoncé une appli en France, et la CNIL se pose déjà la question de l'utilisation de la géolocalisation le 26 mars ...,
- Le sujet est dans l'air et plusieurs projets démarrent début avril,
- EPFL : PEPP-PT (projet européen « volontaire »), centralisé et décentralisé, puis séparation vers
- DP-3T : décentralisé : la France ne suit pas,
- Open source du projet de Singapour : **9 avril**,
- Google-Apple : Exposure notification (GAEN) : annonce le **10 avril** de ce projet,

Interfederal Committee on Tracking and Tracing (depends on Inter-Ministerial Conference on Public Health)

- Technical working group on app based on DP-3T started mid May
- Another negative advice from Data Protection Authority and Council of State late May (also on app)
- 29 June Royal Decree 44 on contact tracing – to be replaced by collaboration agreement in October 2020
- New advice from DPA expected July 27

Contact tracing app

About 1 month of “political struggle”

- June 26: decision to go ahead
- July 6: call for tender sent to 20 companies
<https://www.corona-tracking.info/wp-content/uploads/2020/07/Smals-BB-001-031-2020.pdf>
- July 13: answers received
- July 21: companies selected
- Early August: public consultation

Timing: 8-9 weeks

- Development: Devside, IXOR
- Security review: NVISO



Focus sur l'application « TOUSANTICOVID »

- Application STOPCOVID encadrée par le décret n°2020-650 du 29 mai 2020 remplacée par TOUSANTICOVID.
- La minimisation de la collecte de données est assurée par le protocole ROBERT ;
- La finalité de traitement est limitée à l'alerte de personnes exposées au risque de contamination. Plus particulièrement, l'application TOUSANTICOVID n'a pas pour objet de surveiller le respect des mesures de confinement ;
- La possibilité d'introduire des faux positifs dans les notifications transmises aux personnes avait été envisagée afin de limiter les risques de réidentification. La CNIL a fortement déconseillé la mise en œuvre d'une telle mesure notamment car elle aurait poussé des personnes n'ayant pas eu de contact à risque à « se soumettre à des mesures de confinement volontaire consistant en une restriction auto-imposée de leurs libertés individuelles. »
- Au 14 janvier 2021, 12 millions de personnes ont téléchargé et activé l'application. 50 000 personnes ont été notifiées par l'application suite à une exposition. 92 000 se sont déclarés comme des cas via l'application.
- L'application envoie dorénavant une alerte aux utilisateurs ayant été en contact avec une personne ayant volontairement déclaré avoir été testée positive au coronavirus durant 5 minutes à moins d'1 mètre ou durant 15 minutes entre 1 et 2 mètres. Contre une durée de 15 minutes à moins d'un mètre auparavant.

Participants (16)

Q Trouver un participant

- É Éric Salobir
- I IKOKPATA Jean-Marie
- IP Ioannis Panoussis
- J jean-philippe.cobbaut@univ-cat...
- J jprintz

Inviter Rétablir mon son

Discussion

développement personnel, la santé m'apparaît comme un élément essentiel de ce développement. Le droit à la vie m'apparaît trop limité pour permettre de donner une base suffisante au 'droit à la santé'.

Envoyer à : Yves... (Message) Fichier

Saisir le message ici...

Introduction : contact tracing

- Il y a beaucoup de discussions en 2020 sur le traçage des contacts en vue de détecter ou d'avertir les personnes qu'elles pourraient avoir été infectées par le coronavirus. Un plan possible :
 - Définition
 - Histoire du contact tracing (tuberculose, sida, ...),
 - Vue de l'OMS : casser les chaînes, contact tracing, isolation, surveillance,
 - Théorie de la pandémie tenant compte du contact tracing et conclusions
 - Les critères à satisfaire (divers points de vue)
 - Les outils technologiques : GPS, bluetooth, smartphone, appli, ... : les limites, leur sécurité, ...
 - Quels appareils et combien de personnes en ont ?
 - Les outils cryptographiques
 - Les questions éthiques et de droit: que dit l'Europe, la CNIL, ... ?
 - Problèmes : le piratage, le détournement, utilisation commerciale et non prévue, délation, le sabotage, relais, les bugs, mises à jour, espionnage, retour à la vie démocratique,
 - Les différents projets de recherche dans le monde et leurs critiques
 - Tests des appli : correct (programme), pas de traceur caché ?
 - Les expériences et des retours :
 - Chine, Singapour, Hong-Kong, ...
 - Projets dans le monde (France, Belgique, ...)
 - Des projets commerciaux : dangers et utilités (on les donne dans des lieux avec beaucoup de public ?)
 - Une preuve de concept pédagogique
 - Revue de presse
 - Papiers scientifiques

En guise d'accroche : Singapour : première app

- Chacun dans les médias a parlé de l'approche de Singapour utilisant l'application **Trace Together**,
- Le responsable de cette application Jason Bay: c'est un bon ingénieur qui a fait ses études à Stanford : nous verrons sa page linkedin :
 - *Jason Bay is Senior Director (Government Digital Services) at the Government Technology Agency, Singapore. He is also the product lead for [TraceTogether](#), the world's first nationwide Bluetooth contact tracing system.*
- Il est aussi surprenant de trouver un blog ouvert des services du gouvernement où chacun peut s'exprimer et nous lisons donc l'avis personnel du responsable de ce projet, ...

Une première appli française : 23 mars 2020

The screenshot shows a website interface with a black top navigation bar containing a search bar, 'Connexion', 'Les Newsletters', and 'Abonnez-vous'. Below this is a secondary navigation bar with links for 'Stratégies emploi', 'Stratégies formations', 'Nos événements', 'Guides des agences', 'Compétitions & transferts', 'Data center', and 'BOUTIQUE'. The main content area features a 'MENU' and 'STRATÉGIES' header. The article title is 'CORONAPP, UNE APPLICATION GÉOLOCALISÉE POUR LUTTER CONTRE LA PROPAGATION DU COVID-19', dated 23/03/2020 by Cécilia Di Quinzio. A sub-headline reads 'Une agence web parisienne a créé en 72 heures une application géolocalisée pour lutter contre la propagation du coronavirus.' The article image shows a person wearing a face mask with the 'CoronApp' logo and the slogan 'Tous ensemble contre le virus'. At the bottom of the image are two buttons: 'je me connecte' and 'Je m'inscris'. To the right, a sidebar titled 'LES ARTICLES LES + LUS' lists five articles, and a 'DERNIERS DOSSIERS' section for 'AGENCES' features a '500' graphic.

Rechercher dans Stratégies 🔍

Connexion Les Newsletters Abonnez-vous

Stratégies emploi | Stratégies formations | Nos événements | Guides des agences | Compétitions & transferts | Data center | BOUTIQUE

MENU STRATÉGIES

Accueil > Agences > CoronApp, une application géolocalisée pour lutter contre la propagation du Covid-19

🔗 📄 ★

INNOVATION

CORONAPP, UNE APPLICATION GÉOLOCALISÉE POUR LUTTER CONTRE LA PROPAGATION DU COVID-19

23/03/2020 - par Cécilia Di Quinzio

Une agence web parisienne a créé en 72 heures une application géolocalisée pour lutter contre la propagation du coronavirus.

je me connecte Je m'inscris

LES ARTICLES LES + LUS

- 1 Jeff Bezos cède son poste de directeur général d'Amazon
- 2 Jean-Pierre Remy, serial disrupter 🗝
- 3 Publicis limite la casse en 2020
- 4 2021, annus mirabilis de la publicité raisonnable ?
- 5 Grand Prix Stratégies de l'Influence

Julien TOCHON-DANGUY
Regional Sales Manager
TIPSER

DERNIERS DOSSIERS
AGENCES

500



Jason Bay · 3rd in

Senior Director (Government Digital Services) at GovTech Singapore

Singapore · 500+ connections · Contact info

Message More...

- GovTech Singapore
Stanford University Graduate School of Business

Highlights

Reach out to Jason for...
Joining a nonprofit board, Getting coffee, Hiring.

Message Jason

About

Recovering engineer x policy geek | Builds results-oriented public sector teams | Groks digital technology | Tech for public good | We're hiring!

Jason Bay
Senior Director (Government Digital Services) at GovTech Singapore

Education

- Stanford University Graduate School of Business
MSx, Business
2018 - 2019
1-year management programme on Administrative Service Postgraduate Scholarship
Also awarded Fulbright Scholarship and designated Robert L Joss Scholar (top 10% of class)

Stanford University
Master of Science - MS, Electrical Engineering
2002 - 2005
Co-terminal graduate program concurrent with bachelor's degree

Stanford University
Bachelor of Science - BS, Electrical Engineering (Economics Minor), Distinction
2001 - 2005
Frederick Emmons Terman Engineering Scholastic Award (top 5% of engineering senior class)
Tau Beta Pi Vice-President

<https://blog.gds-gov.tech/> 18 avril 2020 le blog du [Government Digital Services, Singapore](https://www.gds.gov.sg/)

PRODUCT ENGINEERING UX AGILE CULTURE

Search Twitter Facebook Follow



Automated contact tracing is not a coronavirus panacea

Technology cannot displace human contact tracers: creator of TraceTogether.gov.sg, the world's first national Bluetooth contact tracing app

Jason Bay
Apr 10 · 4 min read



Conducting The Technical Interview

What does it take to conduct an awesome technical interview?

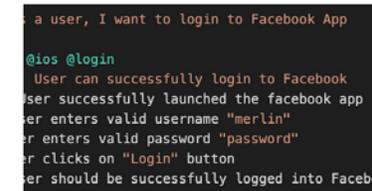
Joseph Matthias Goh
Apr 16 · 17 min read



Working From Home—The Highs and The Low

This past week, and indeed since the Ministry of Health raised our Disease Outbreak Response System Condition from Yellow to Orange, the...

Samantha Wong
Mar 15 · 5 min read ★



Mobile Test Automation—The Bigger Picture

In our previous post, we discussed what Mobile Automation Test (MAT) is. To recap, we want our MAT set-up to be:

Merlin
Apr 2 · 5 min read

To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy. 

Automated contact tracing is not a coronavirus panacea



Jason Bay [Follow](#)
Apr 11 · 4 min read



I think with all the excitement about using technology for contact tracing, as the product lead for TraceTogether, I feel compelled to call out the following section of the policy brief and white paper that we published to accompany the open-sourcing of the BlueTrace protocol and OpenTrace codebase.

If you ask me whether any Bluetooth contact tracing system deployed or under development, anywhere in the world, is ready to replace manual contact tracing, I will say without qualification that the answer is, No. Not now and, even with the benefit of AI/ML and — God forbid — blockchain  (throw whatever buzzword you want), not for the foreseeable future.



To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy. 

There are critical factors (like ventilation — see below; *update: or singing!*) that a purely automated system will not have access to. You cannot “big data” your way out of a “no data” situation. Period.

Any attempt to believe otherwise, is an exercise in hubris, and technology triumphalism. There are lives at stake. False positives and false negatives have real-life (and death) consequences. We use TraceTogether to supplement contact tracing — not replace it.

One thing that sets TraceTogether apart from most private efforts to build a Bluetooth contact tracer, is that we have been working closely with the public health authorities from day 1. Theory is theory. Application and execution is something else entirely. The team has shadowed actual real-life contact tracers in order to empathise with their challenges.

Consequently, there has never been any daylight between TraceTogether’s design, and what will best allow our epidemiologists to fight COVID-19 and protect us all.

ae
pr To make Medium work, we log user data. By using Medium, you agree to our [Privacy Policy](#), including cookie policy. ×

We look forward to working with both Apple and Google, to provide our input into the draft API specifications. We share a common objective in ensuring that the contact detection service integrates well with, and supports public health authorities around the world, to harness #techforpublicgood in our shared fight against COVID-19.

12 Apr 2020: I received feedback from the chief medical officer of a 15,000-strong organisation, pointing to the Washington choir super-spreader event, and ongoing research into how the coronavirus spreads. In this case, a contact tracing app tuned to detect 2 metre proximity would not have flagged any encounters — but a human adjusting the sensitivity thresholds of an algorithm might. Without a human-in-the-loop, matching histories across cases to contribute new knowledge to the medical community’s understanding of how the coronavirus spreads, would not be possible.

14 Apr 2020: Edits to concluding paragraph.

Human-in-the-loop vs Human-out-of-the-loop

It is possible to implement the BlueTrace protocol and have automated notification of probable close contacts of persons who have been diagnosed with COVID-19. In theory, we appreciate the privacy and scalability benefits of doing so. In practice, our ongoing conversations with public health authority officials performing epidemic surveillance and conducting contact tracing operations compel us to recommend otherwise.

An automated algorithm will necessarily generate both false negatives and false positives. A human contact tracer will similarly make mistakes. However, because a human contact tracer would seek to incorporate information beyond just physical proximity, he/she can correct for systematic biases introduced by automated notification system.

Encounters between individuals can be classified into close, casual and transient contacts for epidemiological purposes, based on proximity and duration of contact. However, these classifications depend on factors such as location/environment. For example, short-duration encounters in enclosed spaces without fresh ventilation often constitute close contact, even if encounter proximity and duration do not meet algorithmic thresholds.

Since Bluetooth-based contact tracing solutions do not, by themselves, record location/environment data, this information needs to be obtained through other means — a human-led contact tracing interview.

A human-in-the-loop system is also necessary to allow judgment to be applied, given the high likelihood of pre-symptomatic transmission of the SARS-CoV-2 virus. Since time is of the essence, contact tracers may preemptively wish to trace selected second-degree close contacts of a COVID-19 patient, in cases where there is a high likelihood of exposure and infection, even if the first-degree close contact has yet to test positive. For example, there may be epidemiological value in tracing close contacts of a close relative of an infected person.

A human-out-of-the-loop system will certainly yield better results than having no system at all, but where a competent human-in-the-loop system with sufficient capacity exists, we caution against an over-reliance on technology.

Finally, the experience of Singapore’s contact tracers suggest that contact tracing should remain a human-fronted process. Contact tracing involves an intensive sequence of difficult and anxiety-laden conversations, and it is

the role of a contact tracer to explain how a close contact might have been exposed — while respecting patient privacy — and provide assurance and guidance on next steps.

Singapore’s contact tracers are on the frontline of the fight against COVID-19; they are able to do this because they incorporate multiple sources of information, demonstrate sensitivity in their conversations with Singaporeans who have had probable exposure to SARS-CoV-2, and help to minimise unnecessary anxiety and unproductive panic. These are considerations that an automated algorithm may have difficulty explaining to worried users.

. . .

Jason Bay is Senior Director (Government Digital Services) at the Government Technology Agency, Singapore. He is also the product lead for TraceTogether, the world’s first nationwide Bluetooth contact tracing system. The views, thoughts, and opinions expressed in this article belong solely to the author, and do not necessarily reflect those of the Government Technology Agency, or any other group or individual.

~ ~ ~

Projets

- PEPP-PT : projet européen « centralisé »,
- DP-3T : projet européen « décentralisé »,
- PACT : autour du MIT
- MILA (Montreal) : histoire assez houleuse ...
- France : 2 versions, au moins: Roberr, Désiré.

Testing Apps for COVID-19 Tracing (TACT) - TEK Survey

This page displays the current counts of Temporary Exposure Keys (TEKs) that are visible on the Internet, to allow for comparisons for each day, for these regions running GAEN apps:

1. Austria
2. Belgium
3. Brazil
4. Canada
5. Switzerland
6. Czechia
7. Germany
8. Denmark
9. Ecuador
10. Estonia
11. Spain
12. Finland
13. Guam
14. Croatia
15. Hungary
16. Ireland
17. Italy
18. Latvia
19. Malta
20. Netherlands
21. Poland
22. Puerto Rico
23. Portugal
24. Slovenia
25. England and Wales
26. Gibraltar
27. Northern Ireland
28. Scotland
29. Alabama
30. Delaware
31. Nevada
32. Virginia
33. Wyoming
34. South Africa

Austria csv file				Belgium csv file				Brazil csv file				Canada csv file				Switzerland csv file				Czechia cs			
Country	Date	TEKs	Cases	Country	Date	TEKs	Cases	Country	Date	TEKs	Cases	Country	Date	TEKs	Cases	Country	Date	TEKs	Cases	Country	Date	TEKs	Cases
at	2020-06-24	29	28	be	2020-09-27	18	1827	br	2020-09-05	1	50163	ca	2020-08-07	45	354	ch	2020-06-06	10	24	cz			
at	2020-06-25	47	41	be	2020-09-28	48	1376	br	2020-09-06	4	31199	ca	2020-08-08	43	516	ch	2020-06-07	10	19	cz			
at	2020-06-26	136	28	be	2020-09-29	51	1174	br	2020-09-07	5	14521	ca	2020-08-09	46	245	ch	2020-06-08	10	9	cz			
at	2020-06-27	110	45	be	2020-09-30	80	1762	br	2020-09-08	8	10273	ca	2020-08-10	46	219	ch	2020-06-09	10	7	cz			
at	2020-06-28	226	58	be	2020-10-01	105	1337	br	2020-09-09	14	14279	ca	2020-08-11	46	686	ch	2020-06-10	10	16	cz			
at	2020-06-29	234	74	be	2020-10-02	109	2607	br	2020-09-10	18	35816	ca	2020-08-12	44	349	ch	2020-06-11	10	23	cz			
at	2020-06-30	185	69	be	2020-10-03	124	3175	br	2020-09-11	24	40557	ca	2020-08-13	42	314	ch	2020-06-12	10	33	cz			
at	2020-07-01	1408	43	be	2020-10-04	143	3389	br	2020-09-12	27	43718	ca	2020-08-14	39	477	ch	2020-06-13	10	20	cz			
at	2020-07-02	1609	107	be	2020-10-05	211	2612	br	2020-09-13	28	33523	ca	2020-08-15	42	425	ch	2020-06-14	10	31	cz			
at	2020-07-03	1582	68	be	2020-10-06	238	1968	br	2020-09-14	35	14768	ca	2020-08-16	43	220	ch	2020-06-15	10	23	cz			
at	2020-07-04	1904	109	be	2020-10-07	297	2088	br	2020-09-15	38	15155	ca	2020-08-17	42	179	ch	2020-06-16	10	14	cz			
at	2020-07-05	2272	115	be	2020-10-08	350	3577	br	2020-09-16	50	36653	ca	2020-08-18	39	214	ch	2020-06-17	10	23	cz			
at	2020-07-06	3271	115	be	2020-10-09	387	5728	br	2020-09-17	52	36820	ca	2020-08-19	40	866	ch	2020-06-18	10	33	cz			
at	2020-07-07	3643	85	be	2020-10-10	430	5385	br	2020-09-18	59	36303	ca	2020-08-20	37	324	ch	2020-06-19	10	13	cz			
at	2020-07-08	3391	56	be	2020-10-11	517	7950	br	2020-09-19	53	39797	ca	2020-08-21	39	217	ch	2020-06-20	10	35	cz			
at	2020-07-09	2425	92	be	2020-10-12	638	5327	br	2020-09-20	68	33057	ca	2020-08-22	39	694	ch	2020-06-21	10	8	cz			
at	2020-07-10	2552	102	be	2020-10-13	749	3622	br	2020-09-21	72	16389	ca	2020-08-23	41	241	ch	2020-06-22	10	49	cz			
at	2020-07-11	3432	94	be	2020-10-14	859	7360	br	2020-09-22	62	13411	ca	2020-08-24	43	257	ch	2020-06-23	10	18	cz			
at	2020-07-12	3557	74	be	2020-10-15	983	8271	br	2020-09-23	50	33324	ca	2020-08-25	44	777	ch	2020-06-24	10	22	cz			
at	2020-07-13	3247	114	be	2020-10-16	1106	10448	br	2020-09-24	49	0	ca	2020-08-26	52	309	ch	2020-06-25	17	44	cz			
at	2020-07-14	3246	51	be	2020-10-17	1322	10192	br	2020-09-25	48	66338	ca	2020-08-27	53	477	ch	2020-06-26	24	52	cz			
at	2020-07-15	4063	73	be	2020-10-18	1504	10964	br	2020-09-26	55	31911	ca	2020-08-28	55	456	ch	2020-06-27	31	58	cz			
at	2020-07-16	3108	133	be	2020-10-19	1819	9138	br	2020-09-27	61	28378	ca	2020-08-29	62	506	ch	2020-06-28	38	70	cz			
at	2020-07-17	2876	116	be	2020-10-20	1960	8227	br	2020-09-28	66	14318	ca	2020-08-30	73	297	ch	2020-06-29	48	62	cz			
at	2020-07-18	2805	169	be	2020-10-21	2012	9679	br	2020-09-29	70	13155	ca	2020-08-31	77	249	ch	2020-06-30	50	35	cz			

at	2020-11-16	490	5665	be	2021-02-19	12472	2420	br	2021-01-28	48	63520	ca	2020-12-30	2304	8189	ch	2020-10-29	6535	8620	cz	2020-10-29	6535	8620
at	2020-11-17	418	4657	be	2021-02-20	12299	3437	br	2021-01-29	47	61811	ca	2020-12-31	2339	8459	ch	2020-10-30	6410	9390	cz	2020-10-30	6410	9390
at	2020-11-18	395	5984	be	2021-02-21	11784	2640	br	2021-01-30	43	59826	ca	2021-01-01	2348	7143	ch	2020-10-31	6498	9208	cz	2020-10-31	6498	9208
at	2020-11-19	345	7091	be	2021-02-22	12323	2094	br	2021-01-31	45	58462	ca	2021-01-02	2414	991	ch	2020-11-01	6701	1	cz	2020-11-01	6701	1
at	2020-11-20	299	6995	be	2021-02-23	13006	1121	br	2021-02-01	41	27756	ca	2021-01-03	2374	4535	ch	2020-11-02	6840	1	cz	2020-11-02	6840	1
at	2020-11-21	308	6668	be	2021-02-24	13182	2102	br	2021-02-02	46	24591	ca	2021-01-04	2362	16141	ch	2020-11-03	6531	21928	cz	2020-11-03	6531	21928
at	2020-11-22	290	6611	be	2021-02-25	13218	3113	br	2021-02-03	46	54096	ca	2021-01-05	2283	10058	ch	2020-11-04	6090	6128	cz	2020-11-04	6090	6128
at	2020-11-23	268	5226	be	2021-02-26	12997	3076	br	2021-02-04	45	56002	ca	2021-01-06	2227	7250	ch	2020-11-05	5551	10075	cz	2020-11-05	5551	10075
at	2020-11-24	224	3145	be	2021-02-27	12198	2769	br	2021-02-05	49	56873	ca	2021-01-07	2195	8082	ch	2020-11-06	5108	10140	cz	2020-11-06	5108	10140
at	2020-11-25	188	4377	be	2021-02-28	11359	2760	br	2021-02-06	50	50872	ca	2021-01-08	2065	8227	ch	2020-11-07	4825	9415	cz	2020-11-07	4825	9415
at	2020-11-26	169	5802	be	2021-03-01	11550	2097	br	2021-02-07	53	0	ca	2021-01-09	1980	9237	ch	2020-11-08	4712	19	cz	2020-11-08	4712	19
at	2020-11-27	164	5526	be	2021-03-02	11671	783	br	2021-02-08	55	77475	ca	2021-01-10	1915	8393	ch	2020-11-09	4894	1	cz	2020-11-09	4894	1
at	2020-11-28	217	4954	be	2021-03-03	10297	2050	br	2021-02-09	60	0	ca	2021-01-11	1857	7283	ch	2020-11-10	4487	17311	cz	2020-11-10	4487	17311
at	2020-11-29	214	4669	be	2021-03-04	9387	3264	br	2021-02-10	61	74925	ca	2021-01-12	1808	8325	ch	2020-11-11	4226	5988	cz	2020-11-11	4226	5988
at	2020-11-30	203	4047	be	2021-03-05	8742	2643	br	2021-02-11	70	59602	ca	2021-01-13	1799	6141	ch	2020-11-12	3764	8275	cz	2020-11-12	3764	8275
at	2020-12-01	163	2748	be	2021-03-06	7767	2759	br	2021-02-12	70	54742	ca	2021-01-14	1725	7139	ch	2020-11-13	3507	6942	cz	2020-11-13	3507	6942
at	2020-12-02	157	3033	be	2021-03-07	6626	2799	br	2021-02-13	67	51546	ca	2021-01-15	1625	7447	ch	2020-11-14	3387	6740	cz	2020-11-14	3387	6740
at	2020-12-03	147	3972	be	2021-03-08	6410	2082	br	2021-02-14	71	44299	ca	2021-01-16	1587	6880	ch	2020-11-15	3243	13	cz	2020-11-15	3243	13
at	2020-12-04	130	3969	be	2021-03-09	5821	1117	br	2021-02-15	69	24759	ca	2021-01-17	1526	6359	ch	2020-11-16	3311	4	cz	2020-11-16	3311	4
at	2020-12-05	122	3815	be	2021-03-10	3962	2163	br	2021-02-16	69	32197	ca	2021-01-18	1469	6284	ch	2020-11-17	3343	12842	cz	2020-11-17	3343	12842
at	2020-12-06	105	3444	be	2021-03-11	1477	3434	br	2021-02-17	74	55271	ca	2021-01-19	1452	6420	ch	2020-11-18	3143	4569	cz	2020-11-18	3143	4569
at	2020-12-07	108	2741					br	2021-02-18	75	56766	ca	2021-01-20	1396	5028	ch	2020-11-19	2926	6122	cz	2020-11-19	2926	6122
at	2020-12-08	102	2263					br	2021-02-19	73	51879	ca	2021-01-21	1332	5701	ch	2020-11-20	2791	5013	cz	2020-11-20	2791	5013
at	2020-12-09	102	2377					br	2021-02-20	75	53582	ca	2021-01-22	1278	6111	ch	2020-11-21	2702	4952	cz	2020-11-21	2702	4952
at	2020-12-10	106	2932					br	2021-02-21	69	54940	ca	2021-01-23	1249	5827	ch	2020-11-22	2660	5	cz	2020-11-22	2660	5
at	2020-12-11	108	2686					br	2021-02-22	77	29026	ca	2021-01-24	1202	5094	ch	2020-11-23	2790	3	cz	2020-11-23	2790	3
at	2020-12-12	106	2893					br	2021-02-23	80	26986	ca	2021-01-25	1155	4679	ch	2020-11-24	2731	9753	cz	2020-11-24	2731	9753
at	2020-12-13	93	3241					br	2021-02-24	84	62715	ca	2021-01-26	1139	5617	ch	2020-11-25	2644	4249	cz	2020-11-25	2644	4249

PEPP-PT : Pan-European Privacy-Preserving Proximity Tracing

- <https://github.com/pepp-pt>

DP-3T

- Le plus utilisé,
- Projet européen indépendant,
- Décentralisé,
- Parti de EPFL,



PACT: Private Automated Contact Tracing

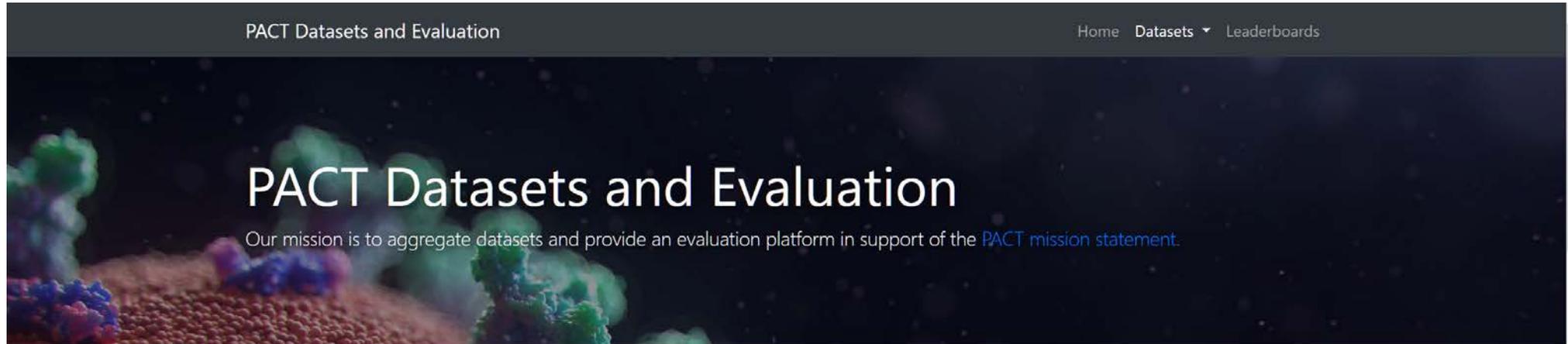


Protocol Definition Working Group

Government Partners

Data Collection Coalition

Tests et évaluations



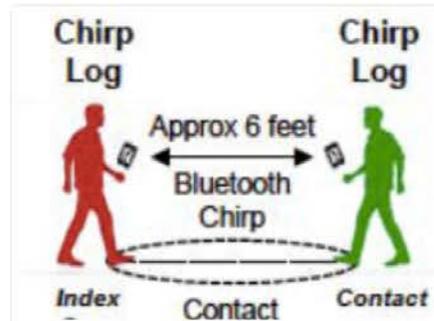
Datasets

For instructions on how to submit a dataset [click here](#).



BLE RSSI Various Static Configurations

This dataset contains ~30 second collects in various static configurations. Data was collected in various environments, with different phone carrying positions and with



H0H1

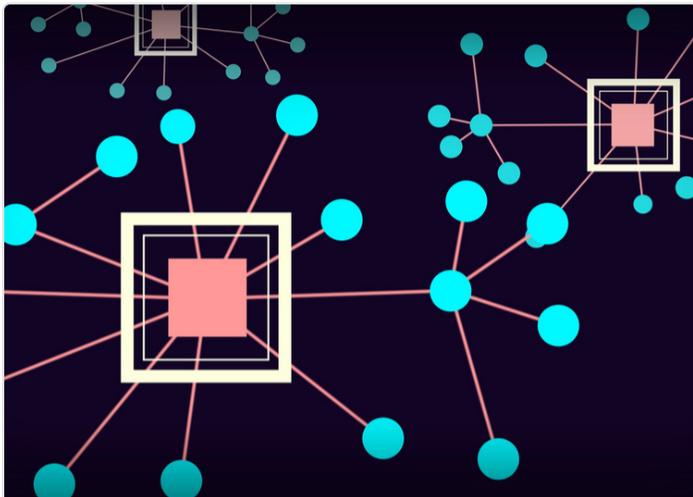
A bluetooth proximity dataset collected varying distance between participants to be far (H0, >10ft) or close (H1, <6ft).

contact tracing



KRI Anechoic Chamber Dataset

Data collected using the nRF52 BTLE Sniffer and a custom program (located at https://github.com/klimgm/btle_sniffer).

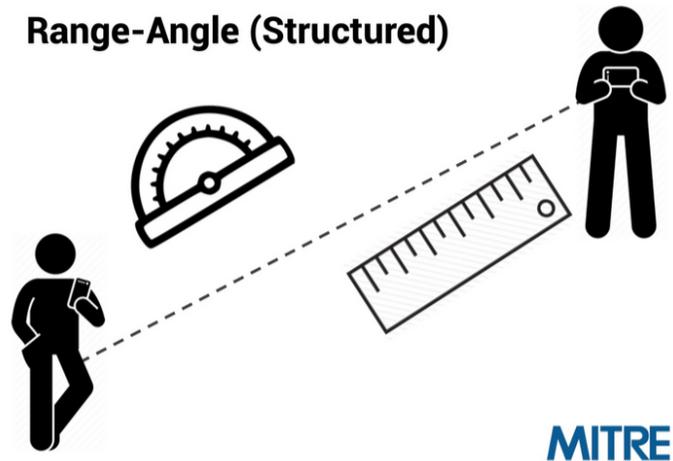


MIT Matrix Data

MIT Testing Protocol used. 10 data collections corresponding to MIT test data matrix. Each data folder contains log files for 3, 4, 5, 6, 8, 10, 12, 15 ft. The Bluetooth signal of interest is tagged with the name "BlueProxTx"

18-03-2021

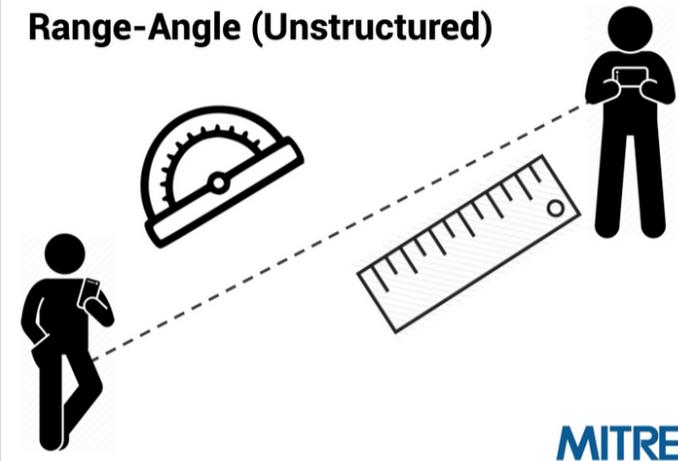
Range-Angle (Structured)



MITRE Range Angle (Structured)

This dataset contains measurements following the [Range-Angle Collection Protocol](#) collected by MITRE employees. For measurements using two iPhones, the BluetoothProximity app was used to broadcast the BLE advertisement from one device following the standard test protocol. For measurements using an iPhone and an Android device, the nRF Connect app was used on the Android device to broadcast the BLE advertisement.

Range-Angle (Unstructured)



MITRE Range Angle (Unstructured)

This dataset contains measurements similar to the the MITLL range-angle protocol, but taken in an unstructured manner. Unlike the range-angle protocol (Structured Contact Tracing Protocol, V.2.0), testers chose their own range, angle and number of tests per set. As a result the dataset does not contain complete range-angle sets, but there is more variety in environment, phone carrying position, pose, etc. The data was collected by 12 MITRE employees at their homes.



PACT Phones and Bluetooth Chipsets

This spreadsheet catalogs a wide range of commonly available phones and their Bluetooth chipsets based on openly available information as part of the PACT project. Please feel free to edit/add/enrich this data.

[Download](#)[View on Github](#)

18-03-2021



Range Angle

A bluetooth proximity dataset collected by varying range angle between participants.

[Download](#)[View on Github](#)

contact tracing



Template Dataset

A template dataset to be used for external dataset submissions.

[Download](#)[View on Github](#)

32

Coronavirus :

comment diminuer l'impact de l'infection?

Et quid pour le déconfinement ?

- Diverses techniques sont utilisées pour ralentir cette infection en vue de l'aplatissement de la courbe de son avancée en infectés parmi la population. Distance sociale, test d'infection, masques, confinement, désinfection des lieux publics, sans parler, bien sûr, des traitements médicaux des cas graves en attendant un vaccin et l'immunité collective, sont des outils importants de santé publique.
-
- Savoir aussi qui a été en contact rapproché avec qui peut être important à connaître en cas de détection d'une personne infectée. Dès cette découverte d'infection, il s'agit de retrouver les personnes rencontrées le plus vite possible pour les avertir et les confiner ou les tester. Cela se nomme (back)tracking, revenir en arrière dans l'histoire des rencontres trop proches les quinze derniers jours. Les moyens pour y arriver peuvent être purement manuels (interview basée sur la mémoire de la personne) soit automatique via une application dans un smartphone, par exemple.
- Deux niveaux :
 - Individuel:
 - Santé publique :

Modèles ...

The image shows a screenshot of the French Wikipedia page for 'Modèles compartimentaux en épidémiologie'. The page layout includes a top navigation bar with the Wikipedia logo, a search box, and user options like 'Non connecté', 'Discussion', 'Contributions', 'Créer un compte', and 'Se connecter'. A left sidebar contains various utility links such as 'Accueil', 'Portails thématiques', 'Contribuer', and 'Outils'. The main content area features a tabbed interface with 'Article' and 'Discussion' tabs, and action buttons for 'Lire', 'Modifier', 'Modifier le code', and 'Voir l'historique'. The article title is 'Modèles compartimentaux en épidémiologie'. The text begins with 'Les **modèles mathématiques de maladies infectieuses**, d'abord outils purement théoriques, ont commencé à être mis en pratique avec le problème du **SIDA** dans les années 1980.' It continues: 'Bien avant cela, depuis la pandémie de grippe espagnole, des **modèles compartimentaux** sont utilisés pour faciliter les calculs de probabilité de contagion. Ces modèles divisent la population en classes épidémiologiques.' Below the text is a 'Sommaire [masquer]' section containing a table of contents with the following items: 1 Histoire, 2 Principes fondamentaux (with sub-items 2.1 Compartiments et règles, 2.2 Représentation mathématique à l'aide d'équations différentielles, 2.3 Nombre de reproduction de base (R_0), 2.4 Limites à l'utilisation du R_0), 3 Extensions (with sub-items 3.1 Hétérogénéité des populations réelles, 3.2 Déplacements, 3.3 Prise en compte de l'âge, 3.4 Population proactive : agir face à la maladie), and 4 Annexes (with sub-items 4.1 Articles connexes, 4.2 Références, 4.3 Bibliographie, 4.4 Lectures complémentaires).

Modèles (mathématiques) de pandémie

Risques démocratiques

Risques sociaux et consensus

Risques pour la démocratie

- Traçage peut être dérouté vers le suivi des personnes,
- Et c'est ce qui s'est passé à plusieurs endroits pour diverses raisons hors pandémie (Singapour, Chine, Israël, ...),

Risques éthiques

- Par exemple, violer le secret médical,

Risques de sécurité informatique

- Piratage,
- Détournement,
- Chantage,
- ...

attaques

- Coercion et chantage :
- Rejeu :
- Relais (rejeu à distance) :
- Surveillance intérieure :
- Surveillance extérieure :
- GoPro :

Utilisation de méthodes de traçage

- Qui permette d'avertir ceux qui auraient en contact avec des personnes infectées, ceci de façon anonyme !
- Problème ancien mais dans un contexte différent (vol d'ordinateurs portables, ...),
- Distance entre personnes et durée : comment faire ?

Méthodes de géolocalisation

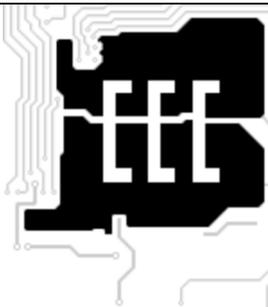
- GPS (plusieurs niveaux de précision),
- Wi-fi,
- Autres systèmes pour avions, bateaux, etc.

Avons-nous besoin de géolocalisation ?

- Non,
- Suivant le mode de propagation, nous avons besoin de la distance et de la durée,
- On pourrait utilisé des données GPS tronquées, mais ...
- Bluetooth (BLE) a été préféré : dans un premier temps, c'est le meilleur choix : mais il y a des contraintes (voir Apple et Google !)
- UWB : arrive sur les nouveaux smartphones hauts de gamme et est bien plus précis,
- Les ultra-sons ? Voir plus loin.

Les 10 critères du Chaos Club Computer

- Groupe de hackers en Allemagne bien connu qui a annoncé très vite des critères pour que cela soit respectueux de la vie privée et en toute sécurité informatique,
- L'application allemande, le modèle de la Belgique, a reçu leur approbation suivant ces critères ...



- home
- Club
- Regional CCC
- Media
- Events
- Topics
- Publications
- Contact
- Support
- Imprint
- Datenschutz

Deutsch

Calendar

10 requirements for the evaluation of "Contact Tracing" apps

2020-04-06 15:19:28, *linus*

"Corona apps" are on everyone's lips as a way to contain the SARS-CoV-2 epidemic. CCC publishes 10 requirements for their evaluation from a technical and societal perspective.

Currently, technically supported "contact tracing" is being considered as means to counteract the spread of SARS-CoV-2 in a more targeted manner. The general motivation is to allow greater freedom of movement for the broad spectrum of society by allowing quick tracing and interruption of infection chains. Contacts of infected persons should be alerted more quickly and thus be able to quarantine themselves more quickly. This, in turn, should prevent further infections. A "corona app" could therefore protect neither ourselves nor our contacts: It would be designed to break chains of infection by protecting the contacts of our contacts.

Contact Tracing as a risk technology

There are a number of suggestions for the technical implementation of this concept. These proposals range from dystopian systems of full surveillance to targeted, completely anonymous methods of alerting potentially infected persons without knowledge of the specific person.

In principle, the concept of a "Corona App" involves an enormous risk due to the contact and health data that may be collected. At the same time, there is a chance for "privacy-by-design" concepts and technologies that have been developed by the crypto and privacy community over the last decades. With the help of these technologies, it is possible to unfold the epidemiological potential of contact tracing without creating a privacy disaster. For this reason alone, all concepts that violate or even endanger privacy must be strictly rejected.

Tags

- update
- pressemittellung
- Anonymisierung

Featured



I. Societal requirements

1. Epidemiological sense & purpose

The basic prerequisite is that "contact tracing" can realistically help to significantly and demonstrably reduce the number of infections. The validation of this assessment is the responsibility of epidemiology. If it turns out that "contact tracing" via app is not useful or does not fulfil the purpose, the experiment must be terminated.

The application and any data collected must be used exclusively to combat SARS-CoV-2 infection chains. Any other use must be technically prevented as far as possible and legally prohibited.

2. Voluntariness & freedom from discrimination

For an epidemiologically significant efficacy, a "contact tracing" app requires a high degree of dissemination in society. This wide distribution must not be achieved by force, but only by implementing a trustworthy system that respects privacy. Against this background, there must be no levying of fees for use as well as no financial incentives for usage.

People who refuse to use it must not experience any negative consequences. Ensuring this is a matter for politics and legislation.

The app must regularly inform people about its operation. It must allow for simple temporary deactivation and permanent removal. Restrictive measures, e.g. an "electronic shackles" function to control contact restrictions, must not be implemented.

3. Fundamental privacy

Only with a convincing concept based on the principle of privacy can social acceptance be achieved at all.

At the same time, verifiable technical measures such as cryptography and anonymisation technologies must ensure user privacy. It is not sufficient to rely on organisational measures, "trust" and promises. Organisational or legal hurdles against data access cannot be regarded as sufficient in the current social climate of state-of-emergency thinking and possible far-reaching exceptions to constitutional rights through the Infection Protection Act.

We reject the involvement of companies developing surveillance technologies as "covid washing". As a basic principle, users should not have to 'trust' any person or institution with their data, but should enjoy documented and tested technical security.

4. Transparency and verifiability

The complete source code for the app and infrastructure must be freely available without access restrictions to allow audits by all interested parties. Reproducible build techniques must be used to ensure that users can verify that the app they download has been built from the audited source code.

II. Technical requirements

5. No central entity to trust

A completely anonymous contact tracing without omniscient central servers is technically possible. A dependence of the users' privacy on the trustworthiness and competence of the operator of central infrastructure is technically not necessary. Concepts based on this "trust" are therefore to be rejected.

In addition, promised security and trustworthiness of centralised systems - for example against the connection of IP addresses with anonymous user IDs - cannot be effectively verified by users. Systems must therefore be designed to guarantee the security and confidentiality of user data exclusively through their encryption and anonymisation concept and the verifiability of the source code.

6. Data economy

Only minimal data and metadata necessary for the application purpose may be stored. This requirement prohibits the central collection of any data that is not specific to a contact between people and its duration.

If additional data such as location information are recorded locally on the phones, users must not be forced or tempted to pass this data on to third parties or even publish it. Data that is no longer needed must be deleted. Sensitive data must also be securely encrypted locally on the phone.

For voluntary data collection for epidemiological research purposes that goes beyond the actual purpose of contact tracing, a clear, separate consent must be explicitly obtained in the app's interface and it must be possible to revoke it at any time. This consent must not be a prerequisite for use.

7. Anonymity

The data that each device collects about other devices must not be suitable for deanonymizing their users. The data that each person may pass on about themselves must not be suitable for deanonymising the person. It must therefore be possible to use the system without collecting or being able to derive personal data of any kind. This requirement prohibits unique user identifications.

IDs for "contact tracing" via wireless technology (e.g. Bluetooth or ultrasound) must not be traceable to persons and must change frequently. For this reason, it is also forbidden to connect or derive IDs with accompanying communication data such as push tokens, telephone numbers, IP addresses used, device IDs etc.

8. No creation of central movement or contact profiles

The system must be designed in such a way that movement profiles (location tracking) or contact profiles (patterns of frequent contacts traceable to specific people) can't be established intentionally or unintentionally. Methods such as central GPS/location logging or linking the data to telephone numbers, social media accounts and the like must therefore be rejected as a matter of principle.

9. Unlinkability

The design of the temporary ID generation must be such that IDs cannot be interpreted and linked without possession of a user controlled private key. They must therefore not be derived from other directly or indirectly user identifying information. Regardless of the way IDs are communicated in the event of infection, it must be ruled out that the collected "contact tracing" data can be chained over longer periods of time.

10. Unobservability of communication

Even if the transmission of a message is observed in the system (e.g. via communication metadata), it must not be possible to conclude that a person is infected himself or herself or has had contact with infected persons. This must be ensured both with regard to other users and to infrastructure and network operators or attackers who gain insight into these systems.

Role of the CCC

For well over 30 years, CCC has engaged in voluntary work at the intersection between technology and society. [Our ethical principles](#) stand for privacy, decentralization and data economy – and against any form of surveillance and coercion.

Without claiming to be exhaustive, in this article we name minimum privacy requirements that a "Corona App" must meet in order to be socially and technologically tolerable at all. CCC will under no circumstances ever provide a concrete implementation with approval, recommendation, a certificate or test seal.

It is the responsibility of the developers of contact tracing systems to prove the fulfillment of these requirements or to have them proven by independent third parties.

Comment fonctionne une appli de traçage numérique

https://www.lemonde.fr/pixels/article/2020/04/05/smartphones-applis-les-defis-du-pistage-massif-pour-lutter-contre-la-pandemie_6035608_4408996.html

The Parable of the Protocol PetitPoussetPierrePainPerrault: 7P

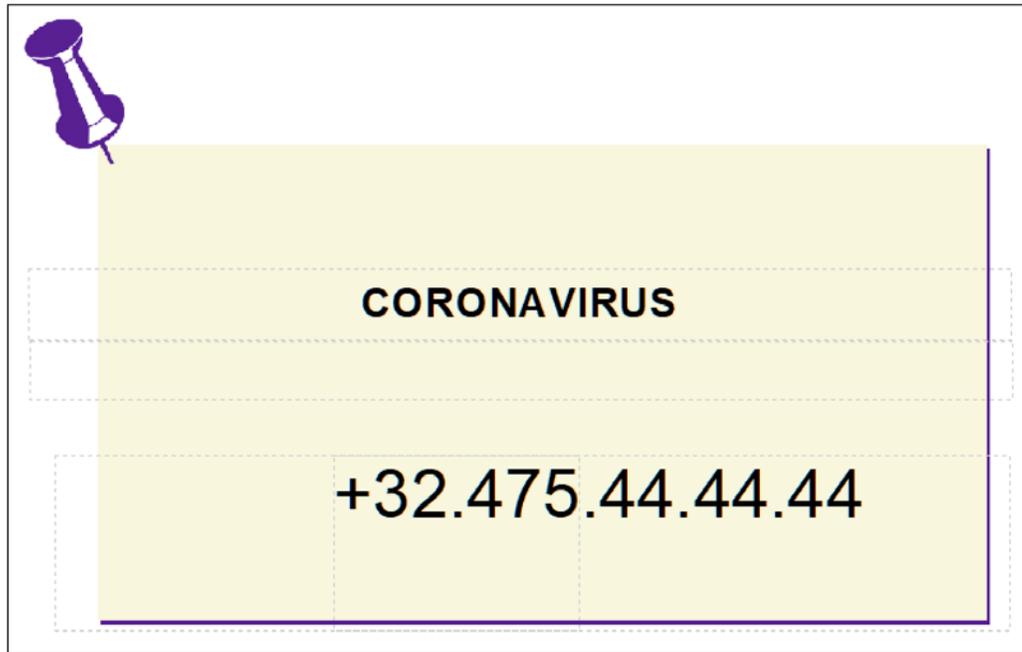
- Petit Poucet : in english, Hop-o'-My-Thumb or (Tom) Thumb
- Hansel and Gretel (brothers Grimm),
- Many versions,
- We'll use the idea of the breadcrumbs for marking some meeting of persons (not stones),

Perfect secrecy – semantic security

- Each random number we'll use is not related at all to another one giving the generation method in use (no possible CCA1 or CCA2): true random numbers are perfect but set other problems, notably optimisation or relation to a person (we avoid that),
- It means very well that **given a random number you cannot attach any person to it, neither recover a path (tracing),**
- For each random number, there are 2 instances:
 - One open always in the pocket of one person (in the so called track ref),
 - The other one magically closed, but perfectly.

The protocol 7P: Protocole Petit Poucet Pierre Pain Perrault carte de visite

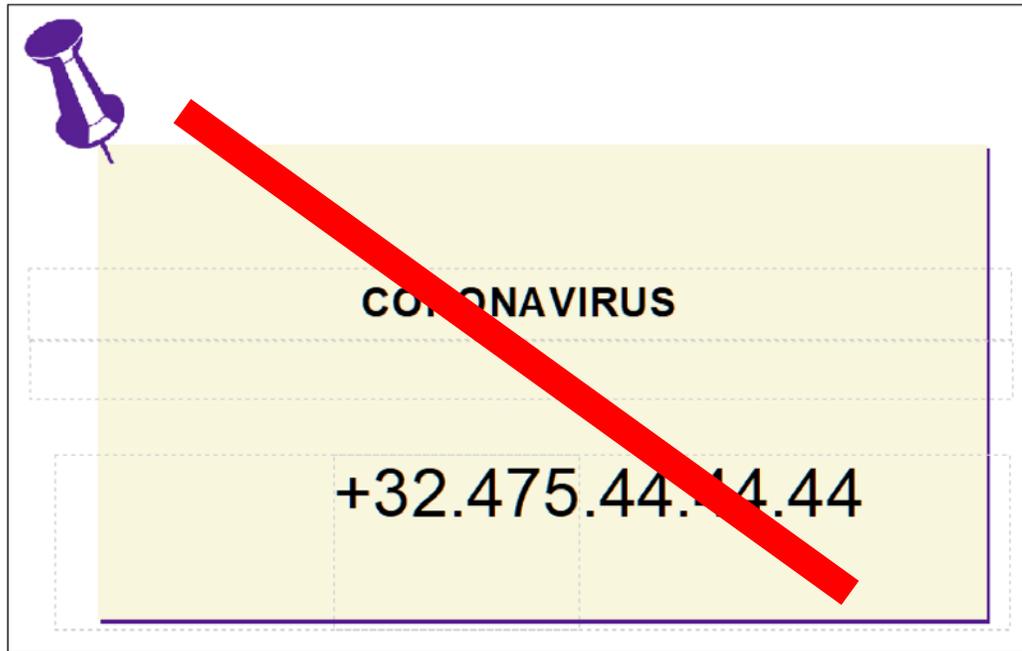
- INIT
 - Each user gets authentic business cards like this one and an authentic copy in a magic closed envelope:



The protocol 7P (NO!)

- INIT

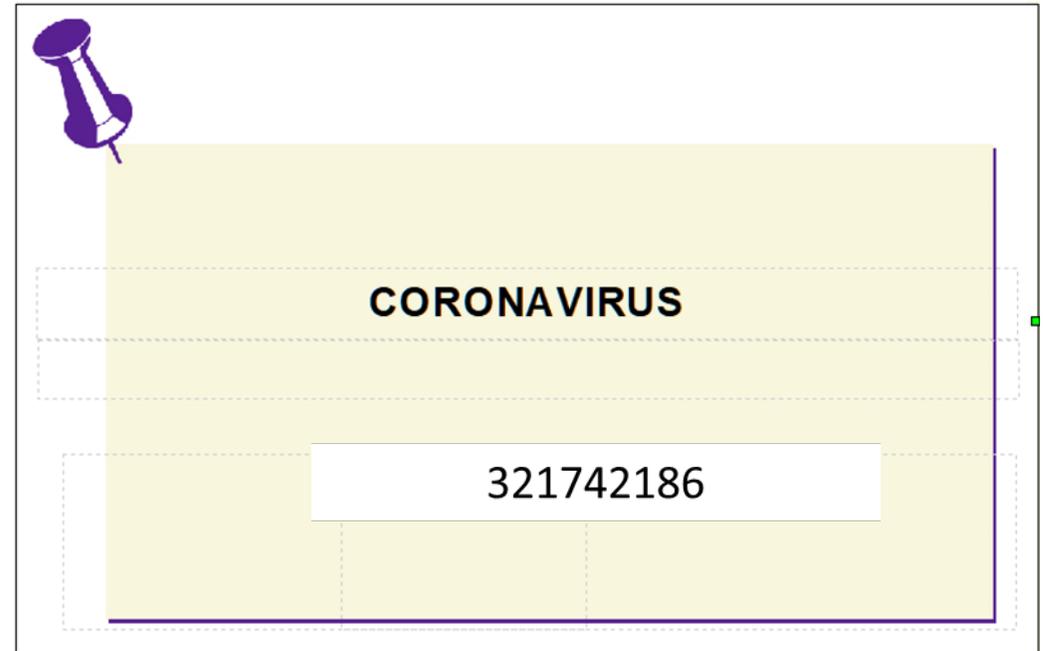
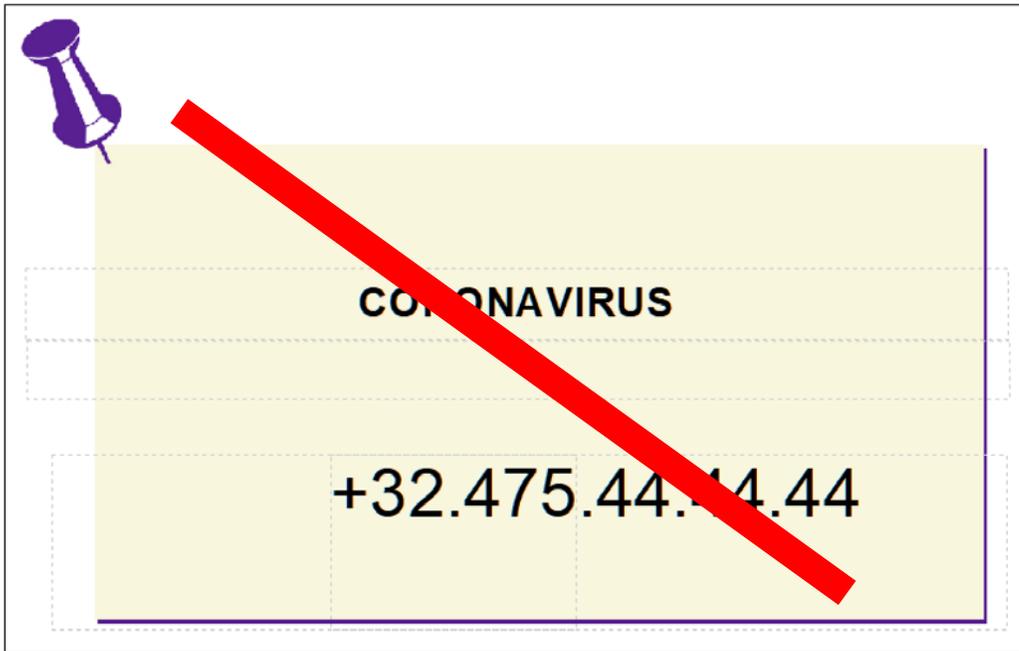
- Each user gets authentic business cards like this one and an authentic copy in a magic closed envelope:



The protocol 7P (YES!)

- INIT

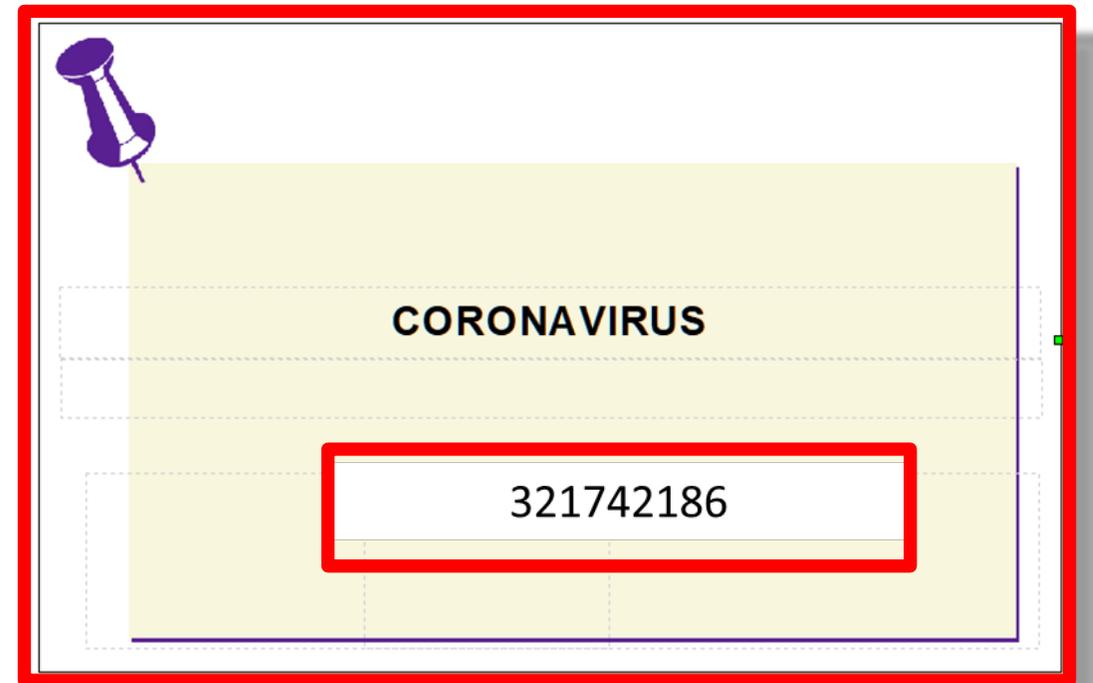
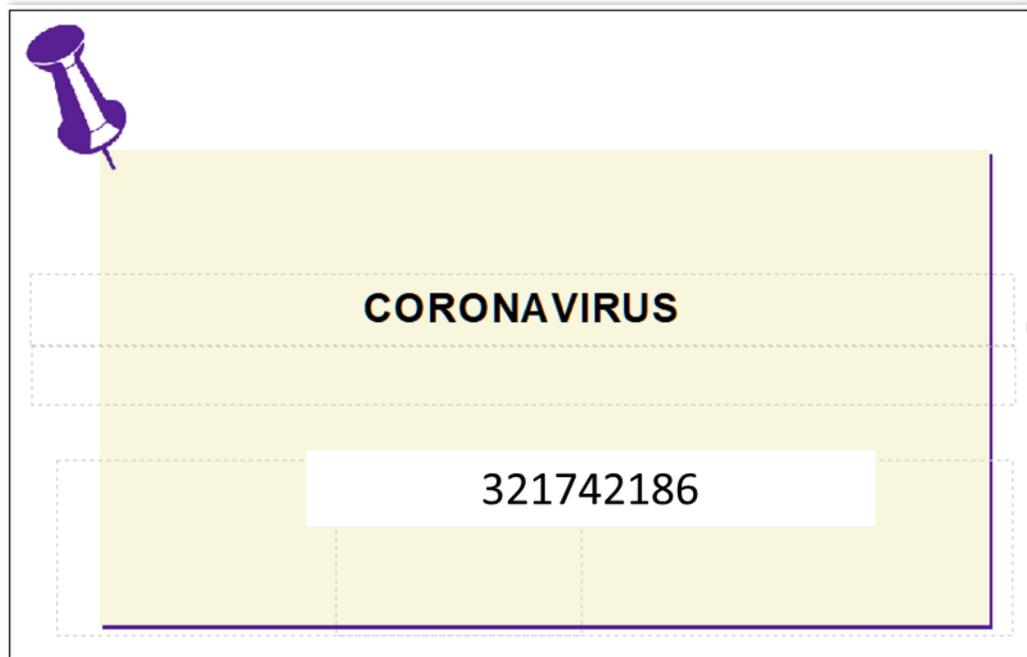
- Each user gets authentic business cards like this one and an authentic copy in a magic closed envelope:



The protocol 7P: a pair of BuCa

- INIT

- Each user gets authentic business cards like this one and an authentic copy in a magic closed envelope (true random number)



Giving your business card (in a special envelope)

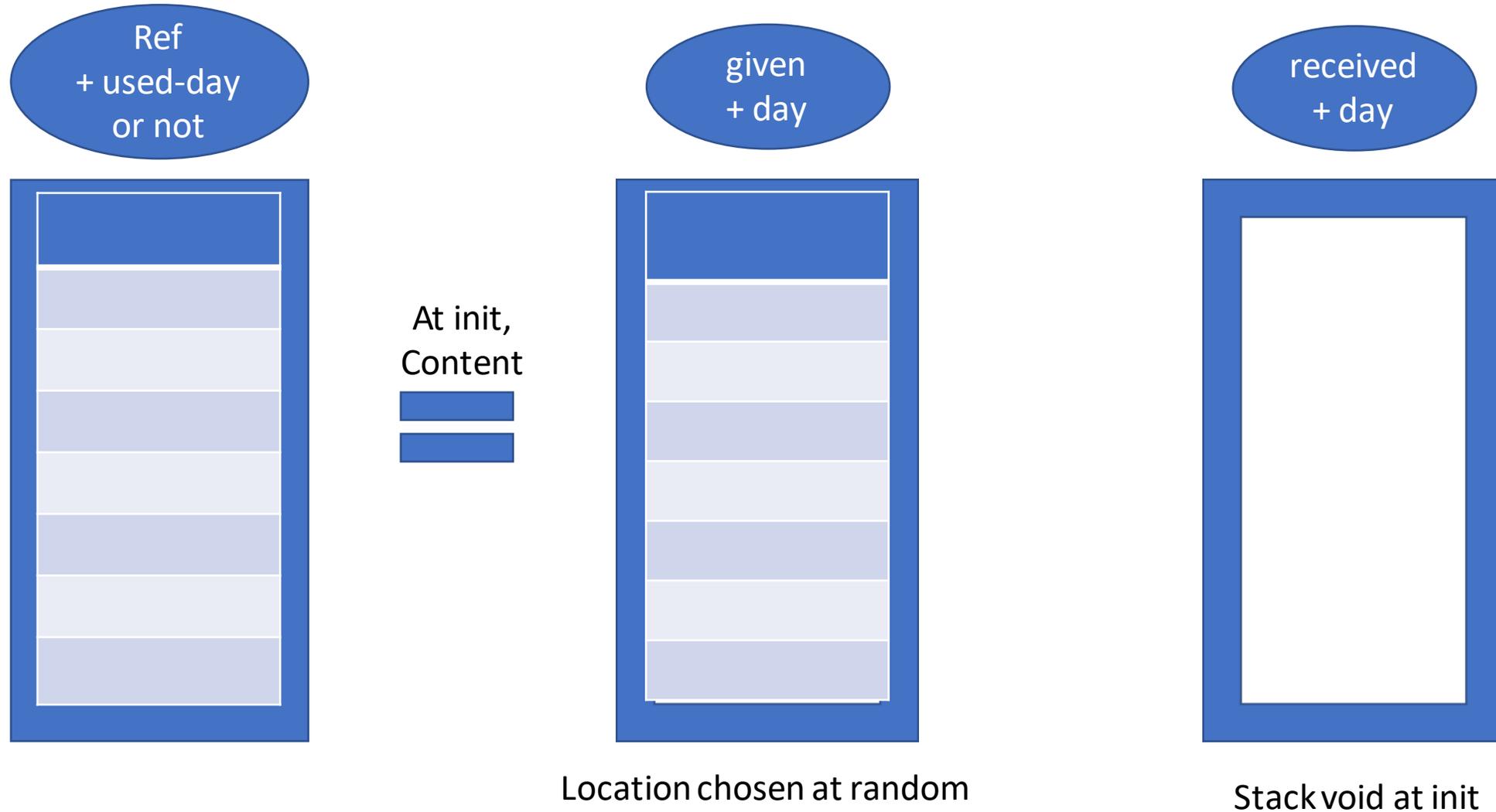
BuCa



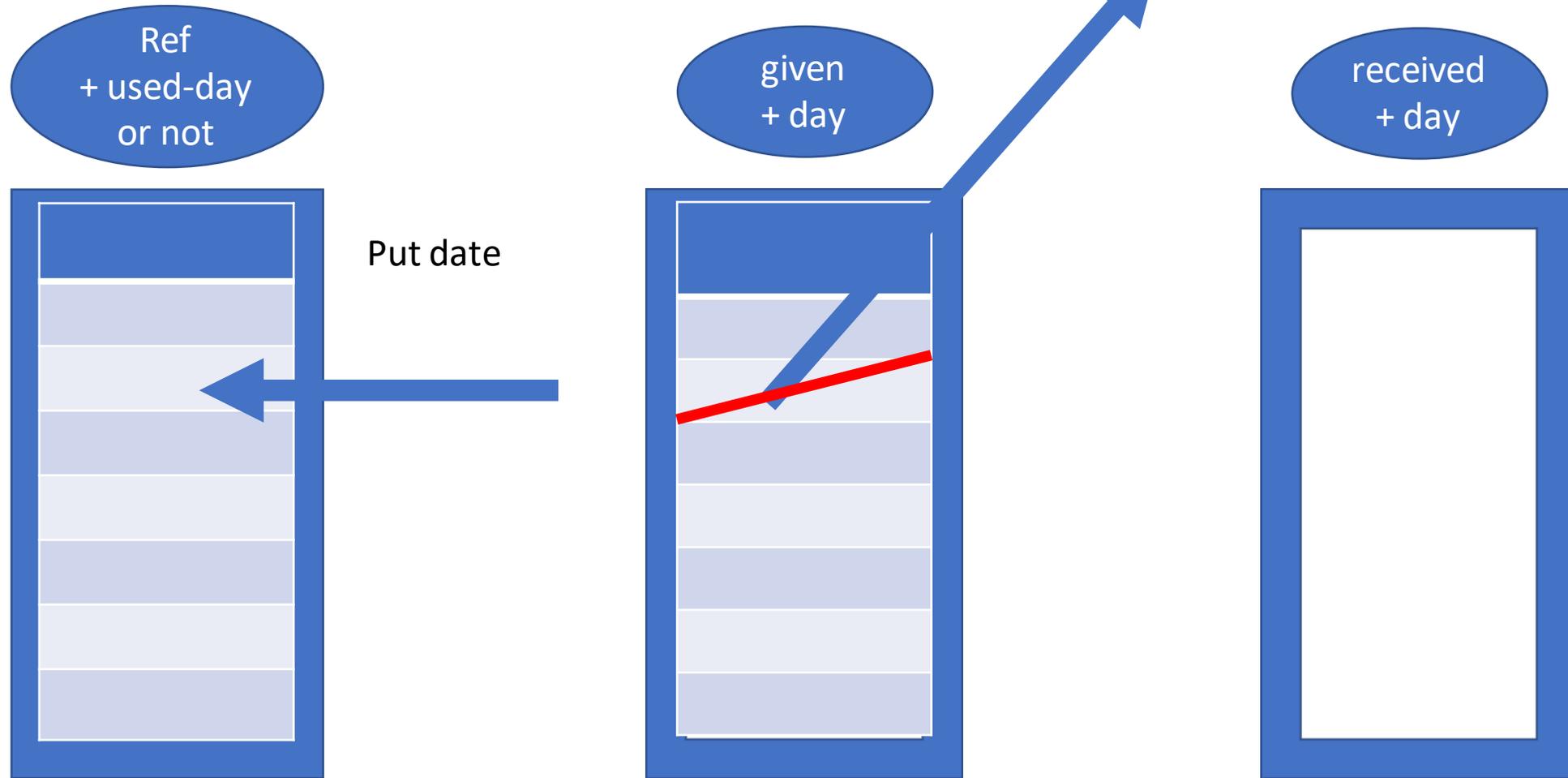
- you'll give one, only if
 - You're close (1.5m) to another person during a long time (> 15 minutes),
 - If there is no protective glass,
 - Evidently, no wall (no possibility),
 - Facultative: both have good masks, for instance,
 - Yes, there is a problem of contamination: a special box will do that.



User's init: 3 stacks of BuCa: **ref**, **given**, **received**, and later removing old cards (after 2-3 weeks)

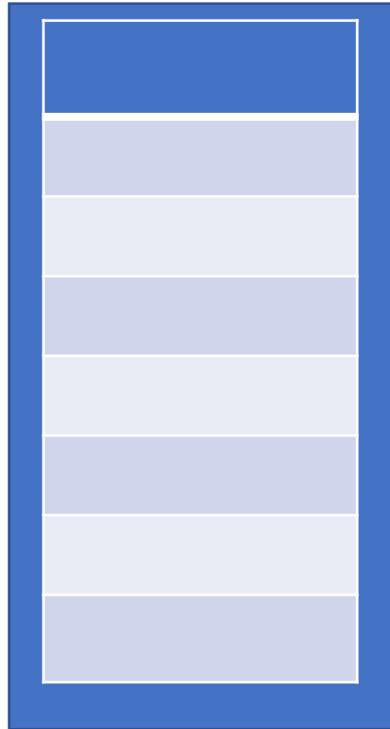


User: 3 stacks of BuCa: giving

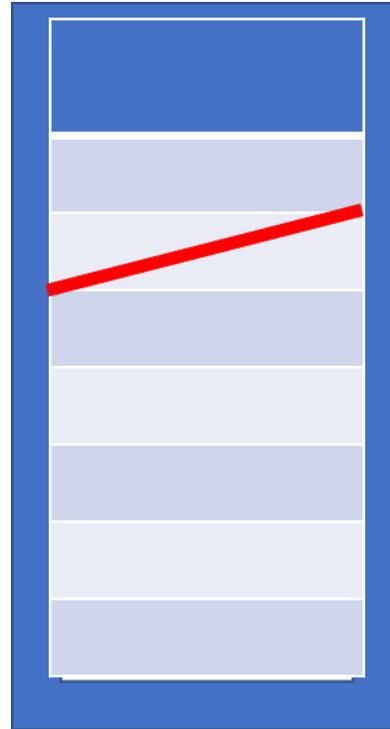


User: 3 stacks of BuCa: receiving

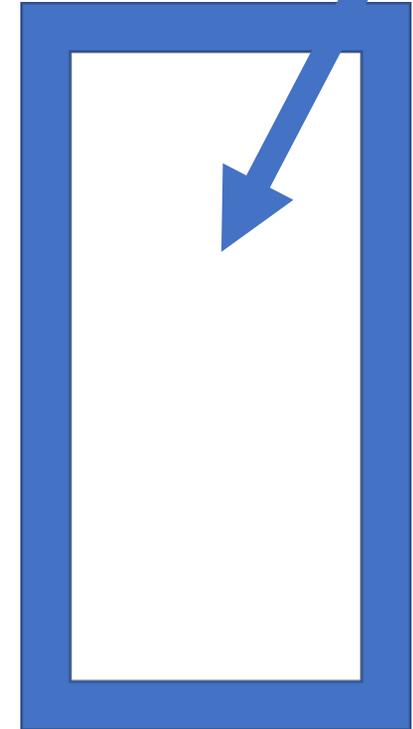
Ref
+ used-day
or not



given
+ day



received
+ day



Suppose you are detected as **infected**

- Now it is time to warn the people you meet receiving a business card,
- You've a stack of valid received cards: then it will be opened with a **magic paper cutter**: who is the owner of this one?
 - You and then you open the enveloppes,
 - Not you, then you go to a special anonymous letter box, after control, the enveloppes then are opened,
- and in each case soon the numbers are put on a public board,
- Nobody knows the relation between the public numbers with a person except the person itself (sic),
- Only other people will know they meet an infected person without any possible identification of YOU,

Secure Public Board to avoid adding dangerous noise or removing cards: the delicate part of it.



Secure Public Board to avoid adding dangerous noise or removing cards: the delicate part of it.



Il s'agit de passer du principe à une version numérique !

- Tout n'est pas si simple :
- Comment donner une carte de visite électronique de façon anonyme ?
- Comment réaliser le tableau d'affichage ?
- Et plein de problèmes imprévus,
- Et de plus, centralisation or non, totalement distribué ?
- Voyons l'application :

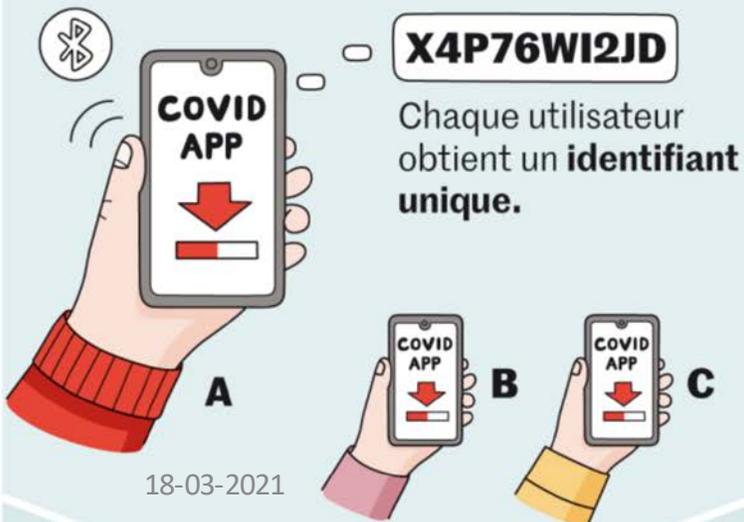
Installation de l'application

Variante :

Les utilisateurs reçoivent plusieurs identifiants numériques uniquement liés à leur personne. Cela ne change rien.

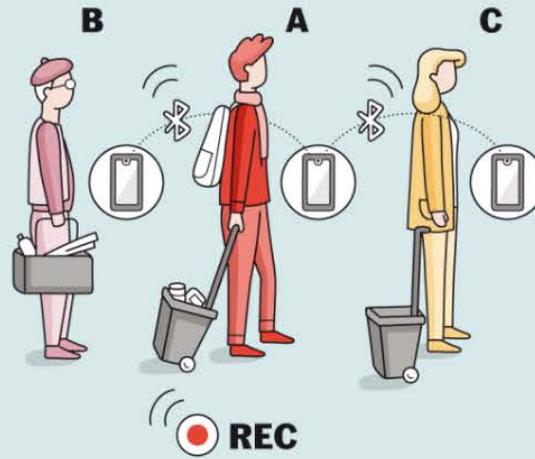
1 Installation de l'application

Les utilisateurs A, B et C installent sur leur smartphone une **application de traçage numérique**. Elle détecte par Bluetooth les autres utilisateurs de l'application à proximité.



2 Contact entre les individus

Le **sujet A**, sans le savoir, est **porteur du virus** et présente un **risque de contamination**. Il entre en contact avec d'autres sujets B et C, qui possèdent aussi l'application.



L'application **enregistre**, par Bluetooth, **qu'il a été à proximité de B et C** en stockant leur identifiant.



L'historique est **conservé sur le smartphone**, et non sur un serveur central. Selon les applications, la durée de conservation de l'historique peut varier.

Le Bluetooth porte jusqu'à plusieurs mètres selon l'environnement. En **mesurant l'intensité du signal**, cela permet de mesurer **la distance entre deux personnes**. La question du temps de « contact » doit être aussi prise en compte.

Mieux : identifiant aléatoire

Détecteur de bluetooth (danger !)

- Certains, plus ou moins bien intentionnés, voudront vérifier si nos concitoyens qui passent près d'eux utilisent l'application PetitPoucetPain,
- Le but peut être purement documentaire, statistique ou de recherche mais on peut craindre aussi une certaine stigmatisation de ceux qui n'utilisent pas l'application ou, aussi, le contraire, ceux qui l'utiliseraient et « tracerait » ainsi les autres,
- De tels détecteurs de bluetooth existent, soit comme app à charger soit comme
- On peut aussi craindre des usages commerciaux pour vous tracer dans des centres commerciaux : il est plus facile de le faire avec bluetooth qu'utiliser le signal GSM du smartphone et on peut même utiliser la localisation par triangulation avec plusieurs détecteurs coordonnés (cela peut aussi se faire à l'aide du signal wi-fi s'il est utilisé).

https://www.commentcamarche.net/download/telecharger-34088247-bluetooth-radar



Bluetooth Radar

★★★★☆ 4 votes - 4.0 / 5 | [Donnez votre avis](#)
Editeur : ShaiR | Version : 2.2 (dernière version)

[Télécharger](#)
Freeware (1,25 Mo)

Windows XP Windows Vista Windows 2000 Windows 7 - Anglais

Votre évaluation
★★★★☆

Aujourd'hui, le Bluetooth n'est plus destiné aux téléphones portables uniquement, il peut aussi fonctionner sur un ordinateur. Grâce à l'avancée de la technologie, **Bluetooth Radar** a été conçu pour permettre à votre machine de détecter les systèmes Bluetooth à proximité.

- [Principales fonctionnalités](#)
- [Plus](#)
- A lire aussi: [Detecteur bluetooth](#)



Principales fonctionnalités

On peut dire que **Bluetooth Radar** est puissant puisqu'il est capable de détecter

NEWSLETTER

Votre adresse email

TÉLÉCHARGEMENT

>> LOGICIELS À (RE)DÉCOUVRIR

-  Audio
-  fre:ac
-  Système
-  SUMo
-  Internet
-  TeamViewer
-  Internet
-  WhatsApp
-  Internet
- Messenger
- ooVoo
- Vidéo
- Molotov

https://www.yonis-shop.com/p/9718-detecteur-de-telephone-wifi-bluetooth-fm-vhf-uhf-camera-espion-micro.html

YONIS
Le meilleur du net
Shop.com

Saisissez votre recherche

Mon compte | Panier (vide)

Tablette tactile | Téléphone / Smartphone | Objets Connectés | Materiel espionnage | Jeu vidéo / Jouet | Camera sport | Idées cadeaux | Informatique | High Tech | Auto / Moto | Maison / Jardin | Sport / Santé / Beauté | Tout le stock

Materiel espionnage > Detecteur de caméra > Détecteur De Signaux Téléphone Wifi Bluetooth FM VHF UHF Caméra Espion Micro

Détecteur De Signaux Téléphone Wifi Bluetooth FM VHF UHF Caméra Espion Micro

Référence :Y-9718
État :Neuf

Cet appareil est l'idéal pour la préservation de votre vie privée. Le détecteur de fréquences vous permet de débusquer tout appareil émettant des **fréquences radio**. Cela inclut les **objectifs de caméra** et les appareils d'enregistrement d'audio. Vous pouvez désormais tenir vos réunions professionnelles en toute sûreté sans fuite d'information.

PROMO

29,49 €
64,99 € - 55%

Quantité
1 - +

Ajouter au panier

Ajouter à ma liste d'envies

Contactez nous

Notes et avis clients
Soyez le premier à évaluer ce produit

En achetant ce produit vous gagnerez **0,60 €** grâce à notre programme de fidélité. Votre panier totalisera **0,60 €** qui pourront être convertis en bon de réduction pour un prochain achat.

<https://www.the-beacons.fr/>

The Beacons - 45 rue du Sahel 75012 Paris - info@the-beacons.com

Mon Compte    

The Beacons

Boutique Production Projets Qui sommes nous FAQ 

iBeacons *Autonome* iBeacons *Outdoor* iBeacons *Longue portée*

 *Fabrication française*  *Livraison en 24H*  *Paiement sécurisé*


iBeacons *Autonome*


24h
Pile AA
Ce beacon autonome dispose d'une autonomie supérieure à un an
à partir de **15,90 € TTC**


24h
Pile bouton 1Ah
Doté d'une autonomie de 6 mois, ce beacon est idéal pour vos POC
à partir de **26,00 € TTC**

Détecter la présence de l'utilisateur grâce à un porte clé Bluetooth !

Sep 26, 2017 • Pierre-Gilles Leymarie



Salut à tous !

Savoir qui exactement est à la maison a toujours été un véritable défi dans Gladys, surtout quand il y a plusieurs personnes dans le logement.

Il n'est en effet pas possible de se baser sur des détecteurs de mouvements, car ceux-ci n'apportent pas d'informations sur l'identité de celui qui rentre dans une pièce : personne A ? personne B ? Intru ?

Pour palier à ça, beaucoup d'entre vous ont mis en place des solutions comme des badgeuses NFC dans l'entrée par exemple ou d'autres solutions basée sur du déclaratif. Mais le problème, c'est qu'en cas d'oubli lors d'un retour/départ pressé, Gladys ne sait pas si vous êtes rentré/parti, et notre domotique ne sert plus à grand chose.

Il y avait une solution alternative que j'avais proposé récemment, il s'agit du scan du réseau Wi-Fi afin de détecter votre smartphone. Cette solution fonctionnait bien, mais tout le monde ne se connecte pas forcément systématiquement au Wi-Fi et en cas de panne batterie sur le smartphone, nos scénarios domotiques tombent encore à l'eau.

Rejoignez +3 000 lecteurs !

N'hésitez pas à vous inscrire à la newsletter Gladys ! Pas de spam, juste des news que j'envoie personnellement 😊

S'INSCRIRE

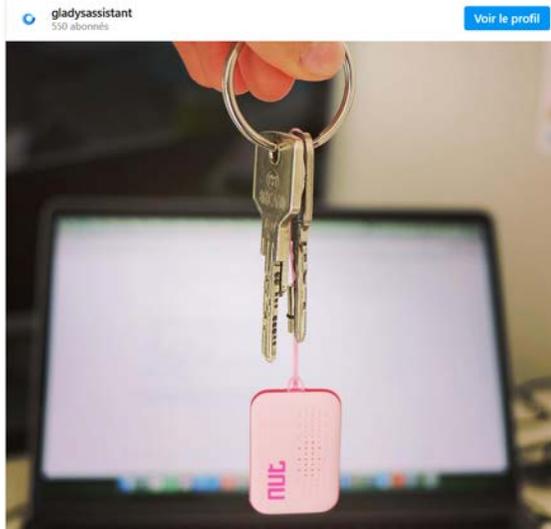
<https://gladysassistant.com/fr/article/detecter-presence-porte-cle-bluetooth> introduction (pour le soft il faut aller sur le site)

Scanner le Bluetooth avec le Raspberry Pi

Le principe est simple, nous allons utiliser un ou plusieurs Raspberry Pi afin de scanner en Bluetooth notre logement à un interval régulier. Lors du scan, le Raspberry Pi va voir les périphériques présents autour de lui : Votre bracelet connecté ? Votre porte clé Bluetooth ? Et ainsi déduire que vous êtes présent dans le logement. Car on part rarement sans ses clés de la maison, ou sans son bracelet connecté !

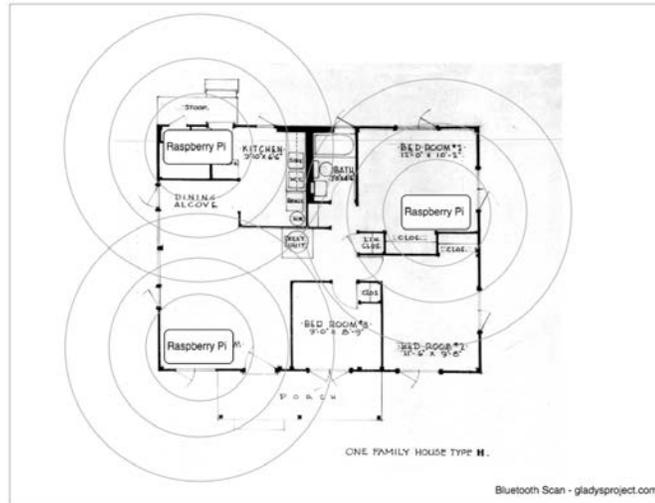
Je parle de porte clé Bluetooth, il s'agit d'un porte clé créé à la base pour éviter de perdre ses clés, qui normalement se connecte au smartphone et vous prévient quand vos clés s'éloignent.

Voilà à quoi il ressemble (on ne se moque pas du rose, au moment de ma commande c'était le moins cher - maintenant vous avez de la chance c'est le blanc le moins cher)



Avec un peu d'astuce, il est même possible de localiser l'utilisateur dans la maison en triangulant sa position si l'on a plusieurs Raspberry Pi. En effet, lorsqu'on scan le réseau Bluetooth, on reçoit des informations sur chaque device comme son RSSI (Received Signal Strength Indication) qui permet ensuite de calculer approximativement la distance entre le Raspberry Pi et le device Bluetooth. Avec plusieurs distances, on peut trianguler l'utilisateur et avoir sa position plus ou moins précise dans le logement.

Je vous ai fait un petit schéma pour que vous visualisiez mieux ce que ça va donner :



Vous remarquerez que j'ai mis ici 3 Raspberry Pi pour l'exemple, mais en pratique j'arrive largement à couvrir mon logement avec un seul Raspberry Pi 3 en le plaçant de façon central dans le salon. A voir en fonction de votre logement :)

Le matériel

En pratique, vous avez besoin de deux choses :

Le matériel

En pratique, vous avez besoin de deux choses :

- Un Raspberry Pi 3 ou un Raspberry Pi Zero
- Un porte clé Bluetooth Nut à 8€

Petit point sur le porte clé Bluetooth Nut. On me l'a conseillé à la Maker Faire Paris, et j'ai décidé de partir sur ce modèle ! Après 2 semaines d'utilisations, il est très fiable et je ne suis pas déçu de mon achat. Je n'ai pas encore de recul sur l'autonomie, mais le constructeur parle d'une autonomie d'un an. En sachant que derrière ce n'est qu'une petite pile bouton CR2016 que l'on peut racheter en lot pour vraiment pas cher (j'ai vu des lots de 5 piles à 2€ sur Amazon)

Le software

J'ai donc écrit un petit programme, dites bonjour à gladys-bluetooth, disponible sur [GitHub](#) ! Ce programme a la particularité de ne pas avoir besoin de Gladys pour tourner.

Son principe est simple, il scan le Bluetooth, et dès qu'il voit un périphérique il envoie la nouvelle à Gladys via une simple requête HTTP. On peut donc avoir de multiples instances de gladys-bluetooth sur un ensemble de Raspberry Pi Zero distribué, qui remontent l'information à un Raspberry Pi 3 central qui fait tourner Gladys.

Pré-requis

Pour utiliser Gladys bluetooth, il faut avoir Gladys en version v3.6.3 au minimum. Pensez à mettre à jour Gladys avant d'installer Gladys bluetooth !

Installation

Pour installer Gladys bluetooth, connectez-vous en ligne de commande sur votre Raspberry Pi, et exécutez les commandes suivantes :

Clonez le repository

```
git clone https://github.com/gladysassistant/gladys-bluetooth
```

Déplacez-vous dans le dossier :

```
cd gladys-bluetooth
```

Installez les dépendances grâce à yarn ou npm.

Autres possibilités:

The screenshot shows a news article on the website 'Informatique News'. The main headline is 'Des bracelets numériques anti-propagation du Covid-19'. The article is dated 'le 21-04-2020' and written by 'Marie Varandat'. The main image shows a worker in a factory wearing a digital wristband, with an orange arrow indicating a distance of '+1,5m'. The article text states: 'À l'heure où Amazon se débat devant la cour d'appel de Versailles et où de plus en plus de syndicats montent au créneau pour dénoncer les conditions de travail dans les centres logistiques, le Port d'Anvers a pris les devants en adoptant une technologie innovante de bracelets électroniques. Objectif : endiguer la propagation du Covid-19 au sein de ses équipes.' The sidebar on the left contains several other news items, including 'Ça va plutôt mal pour Magic Leap...', 'SentinelOne s'enrichit de tableaux de bord personnalisables', 'Le piratage éthique à la loupe...', 'Les équipes IT sont noyées par le nombre exponentiel d'alertes...', and 'PRTG Enterprise Monitor supervise à partir de 30 000 capteurs'.

Informatique News NEWS VIDÉOS DOSSIERS PARTNER ZONE S'inscrire

Rechercher

A LA UNE

Des bracelets numériques anti-propagation du Covid-19

le 21-04-2020
Par Marie Varandat

À l'heure où Amazon se débat devant la cour d'appel de Versailles et où de plus en plus de syndicats montent au créneau pour dénoncer les conditions de travail dans les centres logistiques, le Port d'Anvers a pris les devants en adoptant une technologie innovante de bracelets électroniques. Objectif : endiguer la propagation du Covid-19 au sein de ses équipes.

Email
Print

Ça va plutôt mal pour Magic Leap...
23 avril - 10h50

SentinelOne s'enrichit de tableaux de bord personnalisables
23 avril - 09h30

Le piratage éthique à la loupe...
David Cummins, Tenable
23 avril - 08h55

Les équipes IT sont noyées par le nombre exponentiel d'alertes provenant de leurs outils de monitoring.
Rafael Portolano, Dynatrace
23 avril - 08h45

PRTG Enterprise Monitor supervise à partir de 30 000 capteurs
22 avril - 16h00

Les entreprises des

Informatique
NEWS VIDÉOS DOSSIERS PARTNER ZONE
S'inscrire

Ça va plutôt mal pour Magic Leap...

23 avril - 10h50

SentinelOne s'enrichit de tableaux de bord personnalisables

23 avril - 09h30

Le piratage éthique à la loupe...

David Cummins, Tenable

23 avril - 08h55

Les équipes IT sont noyées par le nombre exponentiel d'alertes provenant de leurs outils de monitoring.

Rafael Portolano, Dynatrace

23 avril - 08h45

PRTG Enterprise Monitor supervise à partir de 30 000 capteurs

22 avril - 16h00

Les entreprises des

Le Port d'Anvers précise toutefois que la vie privée de ses employés reste protégée, aucune information sensible n'étant envoyée à l'employeur.

Prévus initialement pour assurer la sécurité des salariés en milieu industriel avec des objets connectés à une plateforme qui analyse en temps réel les données collectées, les bracelets Romware One de Rombit permettent d'identifier, gérer et alerter sur tout type de situation : collisions d'engin, opérations interdites sur des machines par un personnel non-qualifié, accidents de travailleurs isolés, etc.

Adoptée par le Port d'Anvers, la technologie devait à l'origine servir à mettre en évidence les situations potentiellement dangereuses sur un bateau remorqueur : homme à la mer, zones interdites à l'équipage, membre d'équipage qui tombe ou s'évanouit, etc. Face à la crise sanitaire, la société, qui emploie plus de 1600 personnes, a demandé à Rombit d'enrichir sa technologie de fonctionnalités adaptées aux impératifs de distanciation sociale.

Crédit photo: Port of Antwerp

« L'innovation et la digitalisation sont des outils précieux en temps de crise, indique Jacques Vandermeiren, PDG du Port d'Anvers. Il est essentiel que la zone portuaire continue à fonctionner et que la sécurité de nos collaborateurs soit assurée. Nous attachons donc beaucoup de crédit à ce type de solution et allons prochainement équiper nos collaborateurs sur site du bracelet Romware Covid Radius ».

0 Commentaires
InformatiqueNews.fr
🔒 Règles de confidentialité de Disqus
1 S'identifier

❤️ Recommander
🐦 Tweet
📌 Partager
Les plus récents

Un tout petit peu de cryptographie

Communications privées et courrier anonyme

- Carte postale :
- Lettre :

- Chiffrement :
- Signature :

Outils de sécurité disponibles

- Chiffrement (clé secrète, clé publique),
- Signatures numériques,
- Chiffrement probabiliste (Goldwasser-Micali), sémantiquement sûr ou mieux,
- Anonymisation,
- Differential privacy,
- Zero-knowledge proofs and protocols,
- Systèmes homomorphiques,
- Identités multiples,
- MPC : multi-party protocols,
- Blockchains,
- Mix (Chaum),

Open source !

- Système
 - Code source publié, documenté : pas possible tout-à-fait à cause de l'interface GAEN Apple-Google !
 - Audité,
 - Discuté publiquement,

Impact des erreurs de proximité

- Erreurs de localisation (étages différents, etc),
- Faux positifs,
- Faux négatifs,

- à minimiser !

définitions

- Personne infectée :
- Contact proche :
- Smartphone :
- Distance de sécurité :
- Durée de sécurité :
- Application en open source :
- Volontariat :
- Bluetooth :
- SMS : envoi de messages courts, similaires à des emails : la longueur est normalement limitée à 160 caractères normaux (l'usage de caractères spéciaux en consomme cependant beaucoup) : on peut utiliser ensemble plusieurs SMS (max. 3 ?) ou des MMS plus coûteux. L'utilisation de la cryptographie, même par courbe elliptique, peut entraîner d'assez longs messages, cependant c'est gérable.

phases principales du protocole trackov, traviata, petit poucet (caillou ou pain ?)

- Initialisation globale :
- Initialisation individuelle :
- En régime : enregistrement local et continu des contacts proches,
- Une personne est détectée médicalement comme infectée, les actions :
 - Code QR lisible seulement par les membres médicaux (pas évident, et évitons le rejeu du code QR médical !),
 - Envoi sécurisé et anonyme aux personnes rencontrées dans le passé, non traçables, surtout pour l'infecté,

Utilisation du bluetooth avec un smartphone

- Il y a deux fonctionnements possibles :
 - Soit comme une balise (beacon) : cela veut dire que le smartphone émet régulièrement un code qui, dans le cas le plus simple, est son identité (ce qui est très dangereux comme on le verra plus loin), et ce code est capté par les smartphones dans les environs. Dès qu'un smartphone est détecté par un autre, la distance entre les deux est mesurée. A la base, tout est indépendant et le smartphone ne sait pas qu'il a été détecté par un autre (ceci est théorique en fait),
 - Soit un simple signal régulier de présence d'un appareil bluetooth est envoyé (advertisement) détecté par l'autre appareil (scanning) comme ci-dessus. Puis un échange sécurisé s'établit entre les deux appareils. Chacun donne un ticket unique et originale de présence et de rencontre réciproque.

Mesure des distances par bluetooth

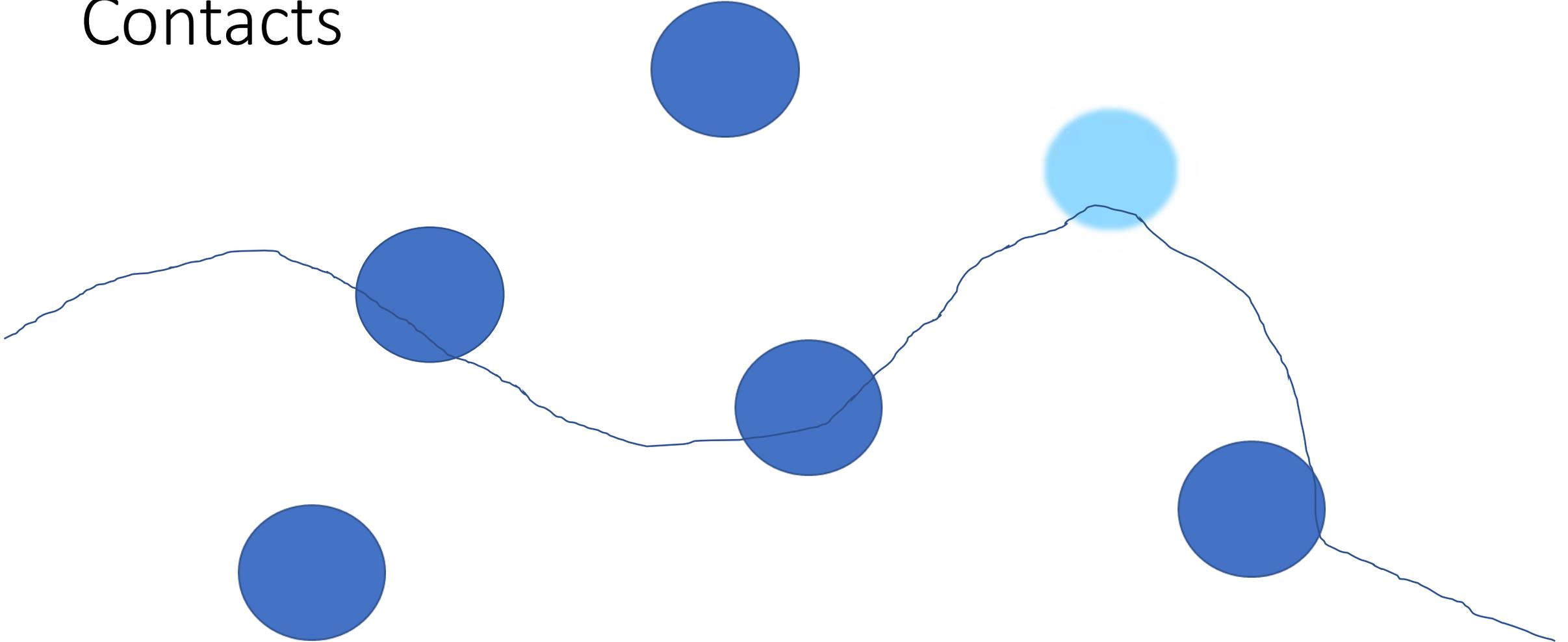
- La technologie de bluetooth n'a pas été prévue pour mesurer les distances et il y a beaucoup de variations suivant les modèles de smartphone,
- on utilise la mesure de la puissance reçue : cette dernière est fort variable mais reste constante pour un appareil donné,
- Ceci ne permet pas de détecter les obstacles, les vitres, ... !

Possibilité d'utiliser le bluetooth

- Pratiquement tous les smartphones actuellement sur le marché ont un bluetooth compatible avec cette application : il faut au moins la version 4+LE (low energy). Il faut aussi que le module radio soit de classe 1 ou 2 (la classe 3 risque d'être trop faible en puissance).
- Par classe, les GSM classiques (exemple : Nokia 105) n'ont pas le bluetooth en général. Ils ne sont pas chers.

Contacts

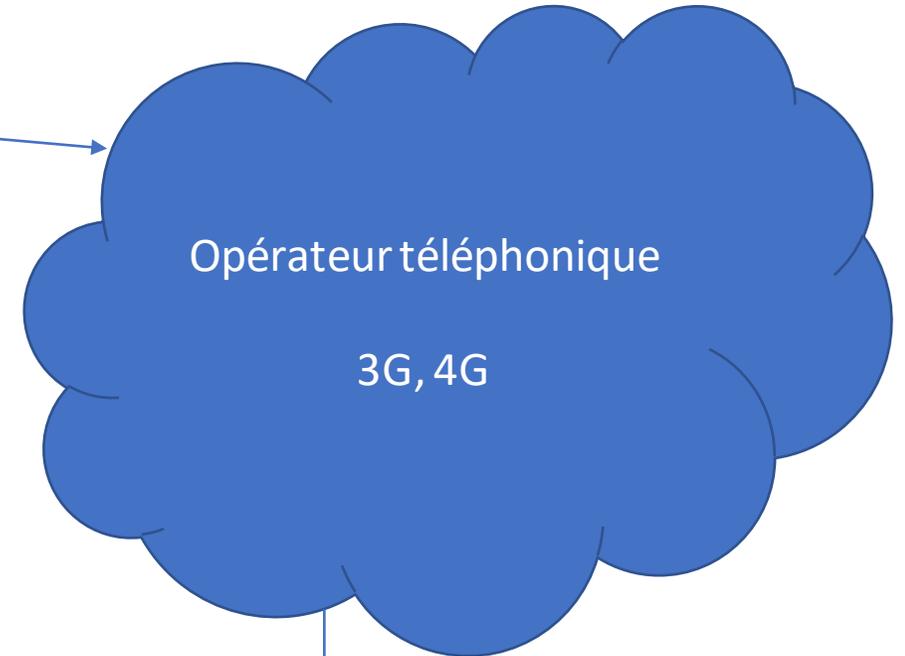
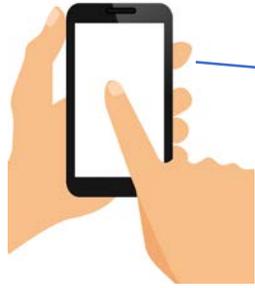
P5



Traçage des contacts (version simplifiée)

- Version totalement décentralisée,

Alice



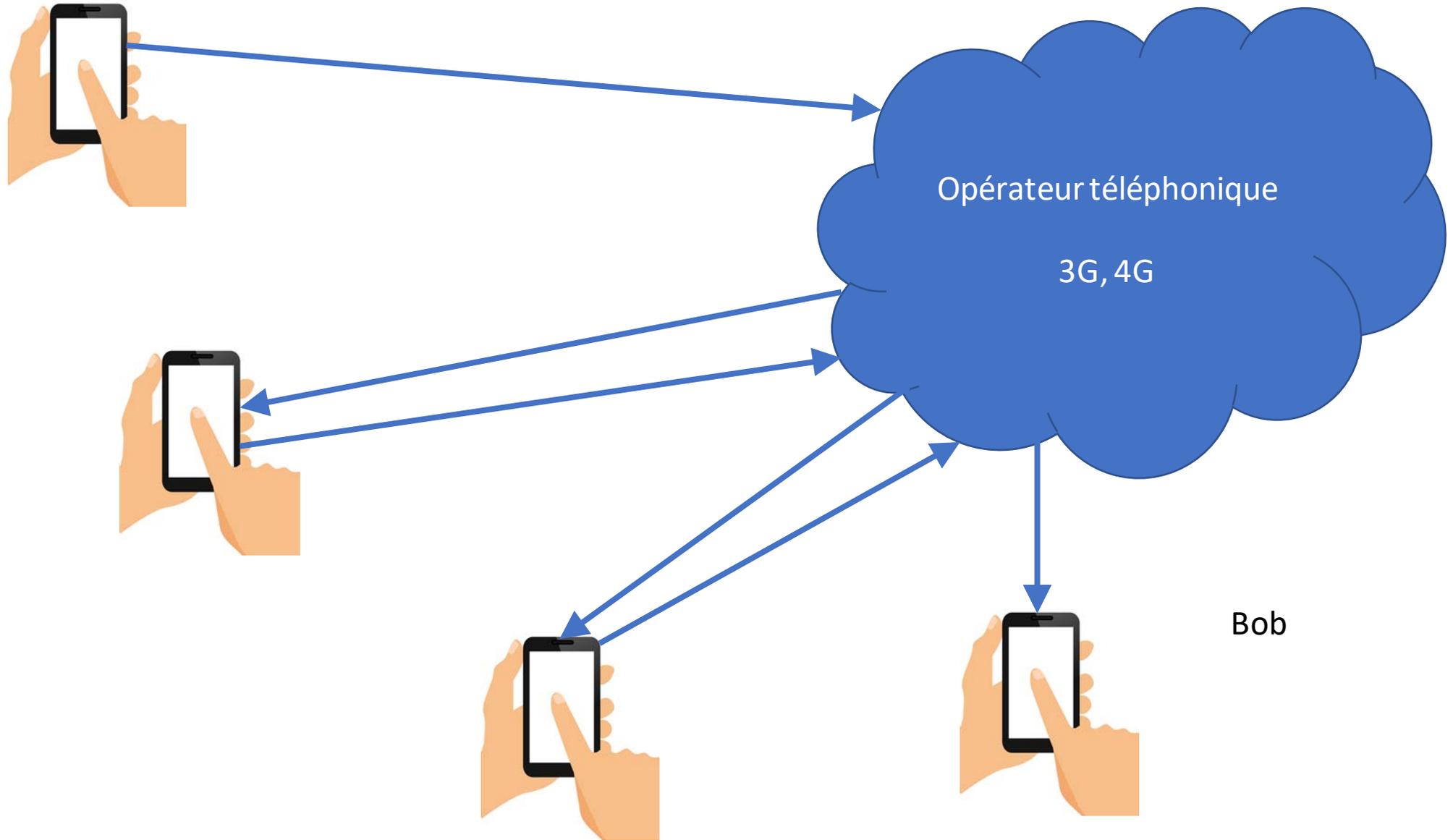
Opérateur téléphonique

3G, 4G

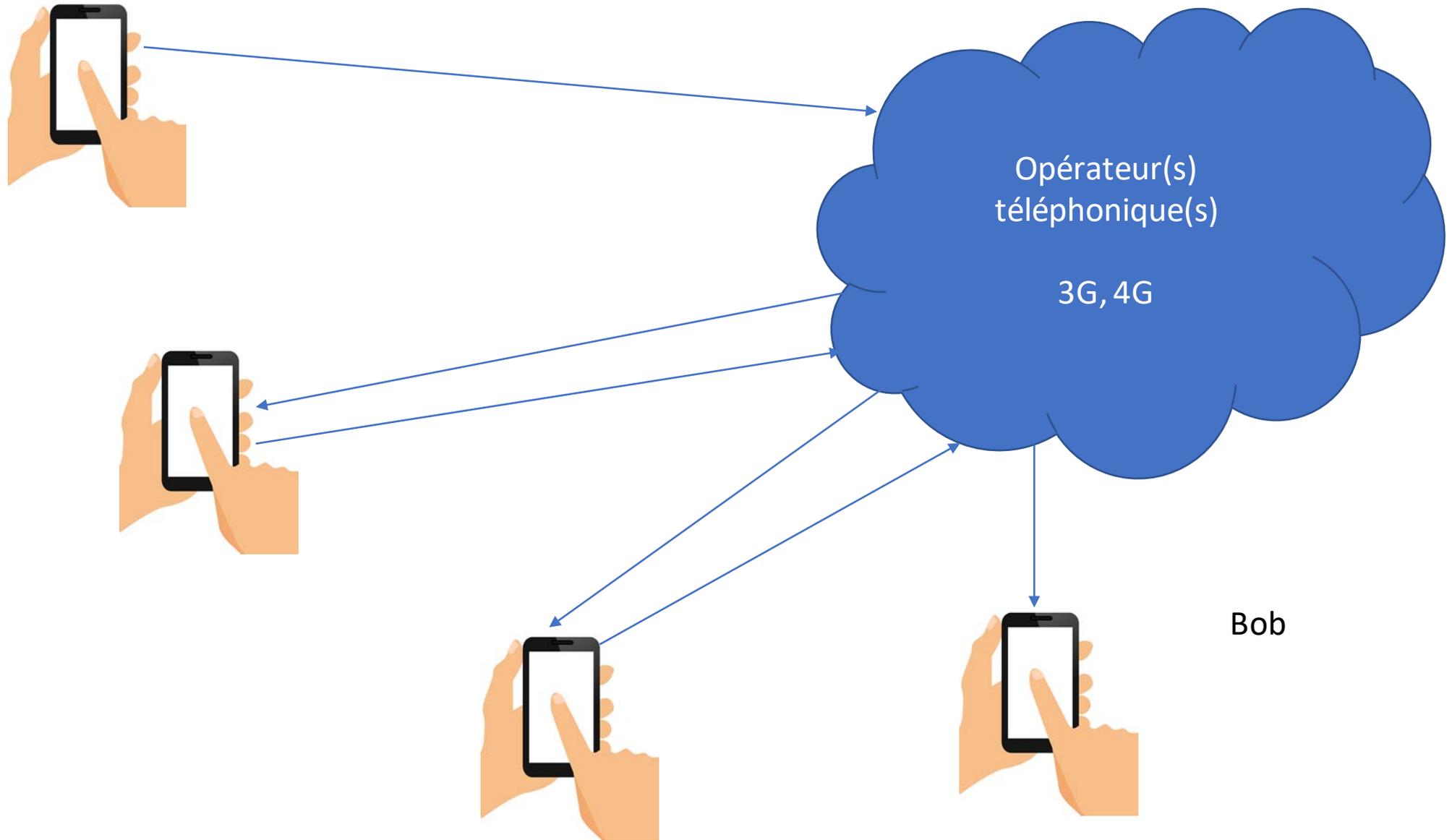
Bob



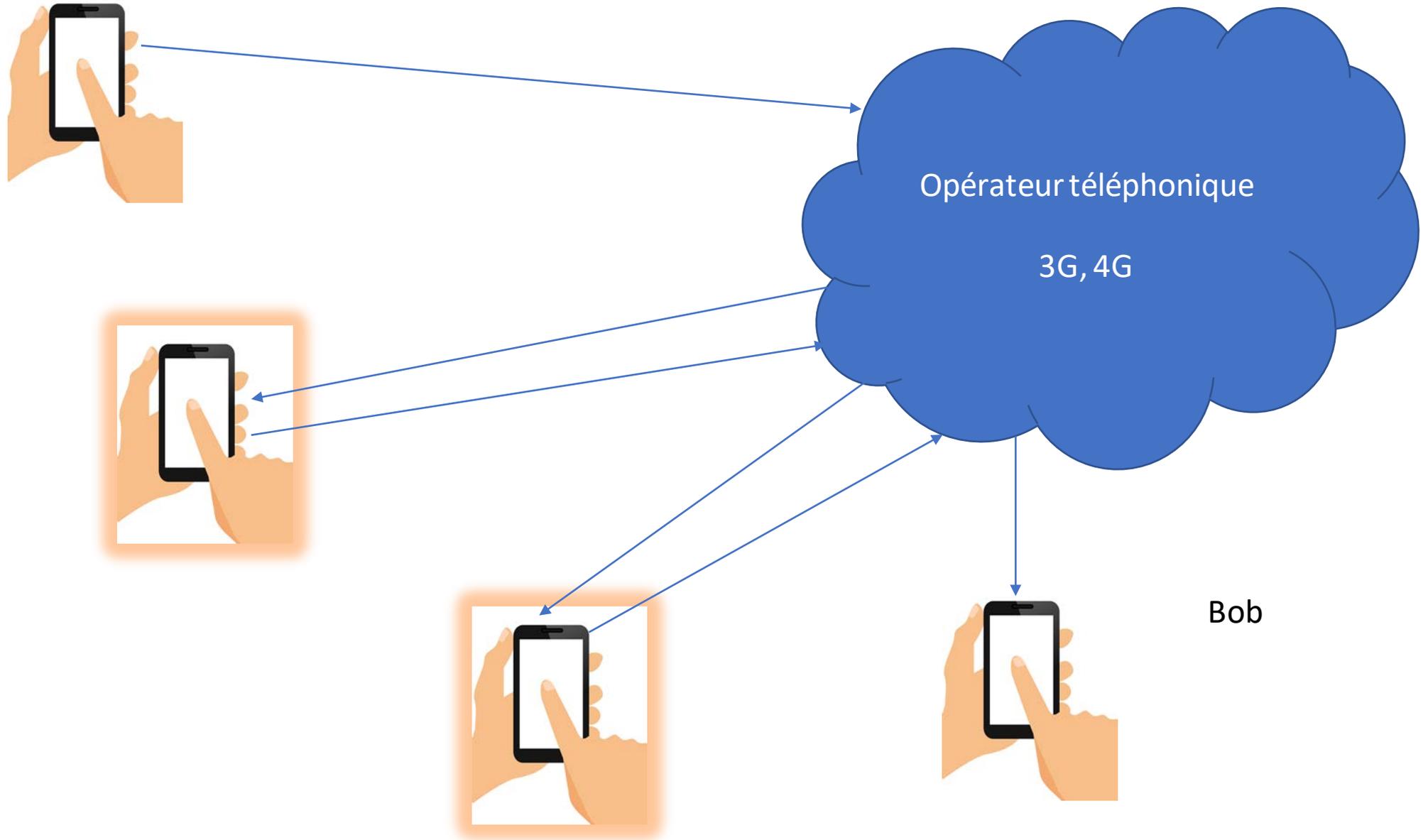
Alice



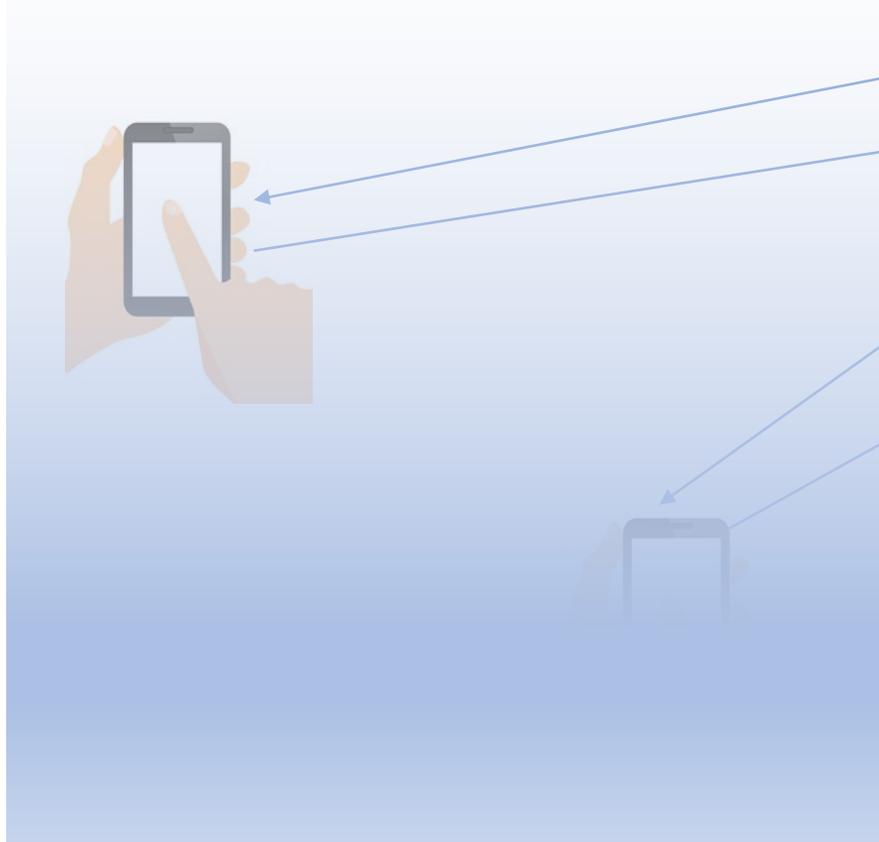
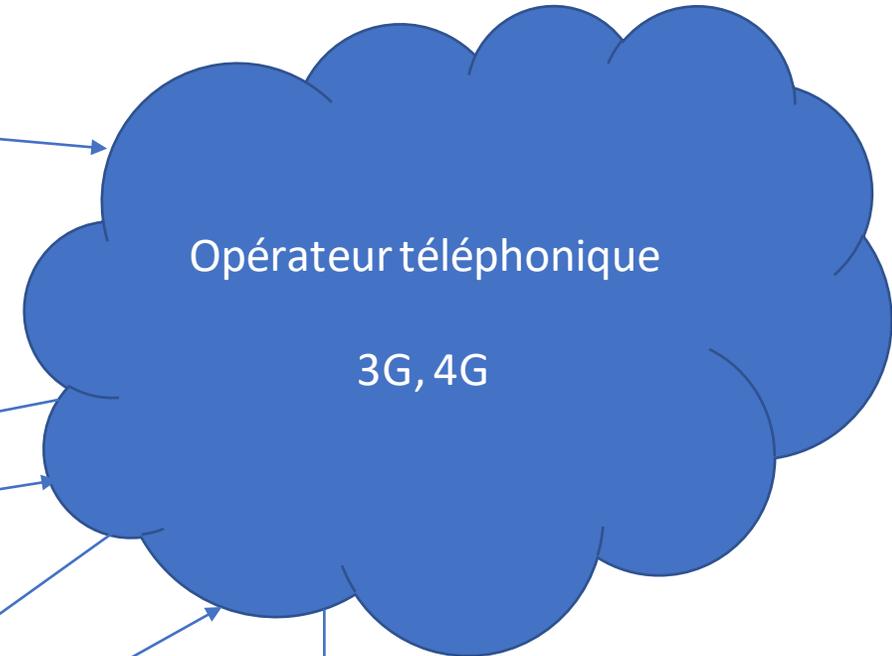
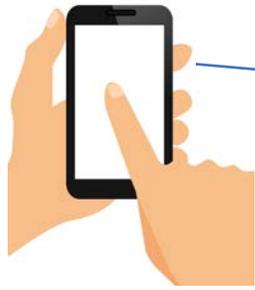
Alice



Alice



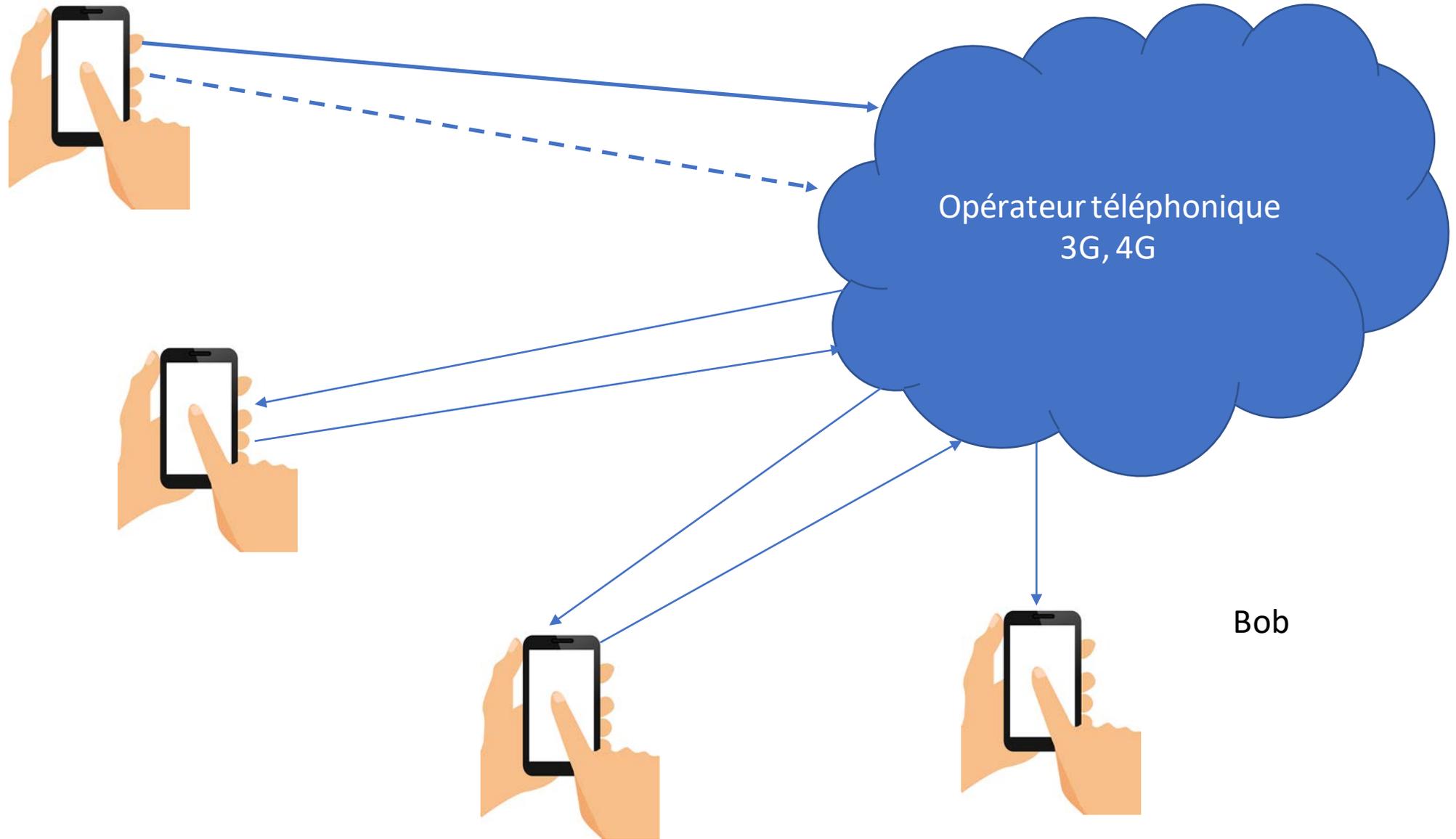
Alice



Bob



Alice



Version parano

commentaires

- Il faut que le message (1) ne soit pas visible comme un message venant d'un infecté (secret médical) : ceci se résout par un bon format et la cryptographie : le message doit être d'apparence identique aux autres : cela reste vrai pour les messages (2), (3) et (4),
- Il est possible d'avoir plus d'intermédiaires mais ce n'est pas conseillé ici,
- Le message (1) est spécial : il n'est pas précédé d'une réception,
- Le message (4) est spécial : il n'est pas suivi d'une émission,
- Les messages (1), (2), (3) et (4) sont dans cet ordre temporel,
- Pour éviter le problème du message (1) : lors de l'initialisation du processus d'alerte on envoie aussi un message formaté,
- Pour éviter le problème du message (4) : Bob envoie aussi un message (à contenu vide), au même format à un récepteur à bien choisir,
- Pour éviter les problèmes temporels, il faut ajouter des délais entre chaque émission, pas trop longs, et/ou des messages supplémentaires au même format : il n'est pas nécessaire de le faire de façon systématique,

Analyse de ce que voit l'opérateur téléphonique, un espion (stingray, IMSI-catcher, ...), etc

- Opérateur téléphonique : a une vision assez globale des communications :
 - Le message (1) sera un message d'un certain format :

Scénario de suivi des contacts proches

- Contact social : Mise en place de leur mesure de la diffusion de l'infection : être fort proche (moins qu'une certaine distance de sécurité) pour une durée (plus qu'une certaine borne),
 - Exemple : moins de 1.5 m entre 2 smartphones, pour une durée commune de 15 minutes (à préciser et discuter),
- Une application sur son smartphone personnel, chargée sur base volontaire,
 - Application totalement en open source,
- Utilisation du bluetooth du smartphone pour mesurer la distance entre deux personnes, représentées par leur smartphone, avec éventuelle prise en compte de la durée de ce contact à cette distance ou moins,
 - Le bluetooth devra donc être activé sur le smartphone personnel possible problème !),

Expert ?

The image shows a LinkedIn profile page for Christian A. Bachmann. At the top, there is a navigation bar with icons for Home, My Network, Jobs, Messaging, Notifications, and Me. A search bar is on the left. Below the navigation bar is a banner advertisement for TransparentBusiness. The profile header features a circular profile picture of a man with glasses and a blue 'Message' button and a 'More...' button. The name 'Christian A. Bachmann · 1st' is displayed, followed by his current role: 'Program Manager ULP Wireless Systems & Secure Proximity @ imec The Netherlands'. Below this, it says 'Eindhoven, North Brabant, Netherlands · 500+ connections · Contact info'. To the right of the profile information, there are logos for 'imec imec' and 'Graz University of Technology'. A 'Highlights' section shows '13 mutual connections' with a list of names including Dave Singelee, Rudy Lauwereins, and 11 others. On the right side of the page, there are two 'Promoted' posts. The first is titled 'A 10,000% ROI pre-IPO?' and the second is 'Outdated shop system?'. Below these are sections for 'People you may know' featuring profiles for Elodie Blogie, Jean-Christophe Willems, and Boubacar Maiga, each with a 'Connect' button. At the bottom right, there is a 'Messaging' chat window.

in Search

Home My Network Jobs Messaging Notifications Me

Work Try Sales Navigator for Free

A High ROI pre-IPO? - TransparentBusiness has reached \$1.6B pre-IPO Unicorn status. Apply Now Ad ...

Promoted

A 10,000% ROI pre-IPO?
TransparentBusiness has reached \$1.6B pre-IPO Unicorn status. Apply Now
[Learn more](#)

Outdated shop system?
Moving from a monolithic commerce platform to commercetools. Get your copy!
[Learn more](#)

Christian A. Bachmann · 1st
Program Manager ULP Wireless Systems & Secure Proximity @ imec The Netherlands
Eindhoven, North Brabant, Netherlands · [500+ connections](#) · [Contact info](#)

imec imec
Graz University of Technology

Highlights
13 mutual connections
You and Christian A. both know Dave Singelee, Rudy Lauwereins, and 11 others

People you may know

Elodie Blogie
Chargée de projet - recherche-action
Femmes sdf chez L'Ilot ASBL
[Connect](#)

Jean-Christophe Willems
Journaliste chez RTBF
[Connect](#)

Boubacar Maiga
NoC
Time
[Messaging](#)

Un avis d'expert :
Christian Bachmann

Détection des contacts des malades du Covid-19 : « Utiliser le Bluetooth de nos smartphones est une solution technique acceptable »

Christian Bachmann, expert de la mesure des distances par Bluetooth, juge plutôt réaliste le projet étatique de détecter avec un téléphone les rapprochements trop prolongés.

Propos recueillis par Nicolas Six · Publié aujourd'hui à 11h21, mis à jour à 11h44

 Lecture 4 min.

Le gouvernement français a annoncé, le 8 avril, la mise en chantier de « StopCovid », une application destinée aux smartphones — appareil qui équipe 77 % des Français — pour mémoriser la présence de personnes dans notre proximité immédiate, puis nous avertir si l'une d'elles contractait ensuite le Covid-19.

La France a rejoint le PEPP-PT, un groupe de laboratoires européens créé en réaction à la pandémie, qui travaille à détecter tout rapprochement prolongé dans un rayon de deux mètres autour de nous grâce aux smartphones, qui écouterait les messages radio émis par l'antenne Bluetooth des mobiles que nous croisons. En temps ordinaire, cette antenne sert surtout à transmettre de la musique vers un autoradio ou un casque sans fil.

contact tracing

Lire aussi | [Coronavirus : qu'est-ce que StopCovid, l'appli de](#)

Les plus lus

- 1 Coronavirus en direct : les Vingt-Sept s'accordent sur un plan de soutien à l'économie européenne
- 2 Coronavirus : Emmanuel Macron rencontre le Pr Raoult, Bruno Le Maire prévoit une récession à - 6 % en 2020

Prudent, le secrétaire d'Etat au numérique, Cédric O, a toutefois prévenu, dans l'entretien donné au *Monde*, que « *nous ne sommes pas certains de réussir à franchir toutes les barrières technologiques, car le Bluetooth n'a pas été prévu pour mesurer des distances entre les personnes* ». **Christian Bachmann** est responsable du programme Secure Proximity dans la société belge IMEC (Institut de microélectronique et composants), qui travaille sur cette technologie depuis plus de dix ans. Expert de la mesure des distances par Bluetooth basé aux Pays-Bas, il livre son point de vue sur sa mise en pratique dans la lutte contre la pandémie.

Plusieurs articles de recherche signalent une marge d'erreur de plusieurs mètres pour les mesures de distance par Bluetooth. Cela n'est pas un frein au développement d'une telle application ?

Ce que les scientifiques cherchent ici à faire est différent de ce qui a été fait par le passé. Le Bluetooth a surtout été utilisé pour localiser des smartphones circulant à plusieurs mètres de distance dans les surfaces commerciales. Ici, l'objectif est de détecter des smartphones à des distances beaucoup plus courtes. A mon sens, plus cette distance est courte, plus les mesures sont fiables, et plus la marge d'erreur diminue.

En outre, dans le cas présent, on peut prendre le temps de faire plusieurs mesures, et cela améliore la précision. Mais il faut bien avouer que c'est un cas d'usage assez nouveau. Notre expérience est relativement ténue en la matière. Même si quelques chercheurs

3 Coronavirus en France : « Le confinement marche » et il faudra « continuer cet effort dans le mois qui vient », selon un membre du conseil scientifique

Édition du jour

Daté du samedi 11 avril



Lire le journal numérique

En outre, dans le cas présent, on peut prendre le temps de faire plusieurs mesures, et cela améliore la précision. Mais il faut bien avouer que c'est un cas d'usage assez nouveau. Notre expérience est relativement ténue en la matière. Même si quelques chercheurs travaillent sur la mesure à très courte portée depuis des années, l'industrie ne s'y intéresse que depuis peu de temps.

Néanmoins, l'approche des chercheurs européens semble bonne. Cette solution ne sera pas efficace dans 100 % des cas, bien entendu, mais c'est la meilleure réponse pragmatique au problème posé. Il existe des techniques de localisation plus performantes, comme l'antenne radio très large bande (UWB) qui équipe l'iPhone 11, mais peu de smartphones en sont équipés.

Les mesures de distance en Bluetooth sont-elles suffisamment fiables pour un usage comme celui-ci ?

Le calcul de distance est basé sur la mesure, par le smartphone, de la puissance des ondes Bluetooth émises par l'autre appareil, qui faiblissent avec la distance. Il y a malheureusement beaucoup de perturbations qui peuvent entraîner des erreurs : le rebond des ondes Bluetooth contre le sol, les murs, le plafond, les surfaces métalliques.

ondes Bluetooth contre le sol, les murs, le plafond, les surfaces métalliques.

En outre, le signal varie si on porte le mobile à la main, en poche ou dans un sac. Certes, ces perturbations sont moins grandes à faible distance, mais la marge d'erreur demeure importante. Il y aura donc des faux positifs : la détection erronée de personnes qui sont en réalité plus loin que deux mètres, par exemple ; et il y aura aussi des faux négatifs : l'échec de détection de personnes rentrées dans ce périmètre. A mon avis, les scientifiques chercheront à contourner ce problème en réglant leur système de façon légèrement pessimiste, pour détecter trop de contacts plutôt que pas assez.

Les travaux de recherches reposent souvent sur des expériences en laboratoire qui ne rendent pas bien compte de la variété des scénarios réels. Pensez-vous qu'on peut mettre au point une solution efficace en quelques semaines ?

C'est un vrai challenge. Il existe par exemple des centaines de modèles de smartphones qui ne sont pas équipés des mêmes antennes Bluetooth, leur puissance d'émission n'est donc pas exactement la même. Pour pouvoir mesurer la distance avec précision, il faudra mesurer leurs émissions pour pouvoir les corriger.

Il faudra mener des tests dans divers environnements, avec diverses marques de smartphones, et tenter des scénarios où de nombreux mobiles sont à proximité — ce qui ne posera probablement pas de problème dans un périmètre de deux mètres, à mon avis, jusqu'à dix à vingt smartphones. Je pense que ce travail peut être mené en quelques semaines, à condition de cantonner les mesures aux modèles de smartphones les plus populaires.

Ces communications Bluetooth risquent-elles de vider la batterie des smartphones rapidement ?

Non, la technologie employée sera le Bluetooth BLE (basse énergie), dont sont équipés presque tous les smartphones en circulation. Il consomme beaucoup moins d'énergie que, par exemple, les communications avec les antennes téléphoniques des opérateurs. Je pense que l'impact sera négligeable.

Coronavirus : nos contenus sur le traçage des données

– Le dossier : [Smartphones, applis... les défis du pistage massif pour lutter contre la pandémie.](#)

– L'entretien avec Marie-Laure Denis, présidente de la Commission nationale de l'informatique et des libertés (CNIL) : « Les applications de "contact

Nos guides d'achat

avec  **wirecutter**
le meilleur de l'équipement

les meilleurs jumelles pour l'observation, la randonnée ou l'ornithologie



Le futur ?

- Meilleure décentralisation,
- Anonymat renforcé (tor ?),
- Détection en arrière,
- Détection des obstacles (utilisation des ultra-sons, ...),
- Audit : code source pas suffisant,
- Mode interactif ?
- Mise à jour sécurisée des contacts et plus fréquente,
- Meilleure internationalisation,
- Mettre mieux en relation avec les modèles d'infection (percolation, graphes, déconfinement, ...),
- Bilan (Angleterre !),
- Nouveau projet.

