Technical Perspectives of Contact-Tracing Applications on Wearables for COVID-19 Control

Viktoriia Shubina[*,†], Aleksandr Ometov[*] and Elena Simona Lohan[*]
[*]*Electrical Engineering Unit*, *Tampere University*, Tampere, Finland
[†]*Computer Science Department, University Politehnica of Bucharest*, Bucharest, Romania
Corresponding author's email: viktoriia.shubina@tuni.fi

***Abstract*—The wearables' market is rapidly evolving, with applications ranging from healthcare and activity monitoring to emerging domains such as drones and haptic helmets. Wearable-based contact tracing is gaining increased attention in the COVID-19 era for more efficient disease prevention. Therefore, it is of timely relevance to identify the leading existing wireless contact-tracing solutions and their suitability for wearables. Existing trade-offs of contact-tracing applications require a thorough analysis of technical capabilities, such as accuracy, energy consumption, availability, sources of errors when dealing with wireless channels, privacy challenges, and deterrents towards a large-scale adoption on the wearables market. Based on extensive literature research, we conclude that decentralized architectures generally offer a better place in a trade-off in terms of accuracy and user eagerness to adopt them, taking into account privacy considerations, compared to centralized approaches. Our paper provides a brief technical overview of the existing solutions deployed for contact tracing, defines main principles that affect the overall efficacy of digital contact tracing, and presents a discussion on the potential effect of wearables in tackling the spread of a highly contagious virus.**

***Index Terms*—Wearables; Contact tracing; COVID-19; Centralized/Decentralized architectures; Proximity detection; Privacy; Internet of Things; Constraints.**

I. Introduction and motivation

During an unprecedented context of the COVID-19 outbreak, consumer wearable devices, such as smart bracelets, smartwatches, or smart rings, have started to play a vital role in mitigating the spread of the contagious virus. Arguably, smartphones frequently carried on by users also may be interpreted as belonging to the category of wearables [1]. Many mobile health companies, hospital healthcare centers, and remote diagnostics startups have proved a high ability to respond promptly during a real epidemic. They have motivated the researchers worldwide to find efficient technology-based complementary solutions for disease prevention and control during the past half-year [2]–[5]. It is essential to note that none of the technological solutions are meant to replace the mitigation measures recommended by epidemiologists and exerts from the medical domain, yet technological advances can complement the existing manual ones and assist in implementing social distancing measures as described in [6].

One of the emerging and most promising technology-based solutions promising to slow down the spread of COVID-19 is the wireless and automated or semi-automated contact tracing through wireless communication technology. Generally, software-based applications with built-in sensors on mobile devices/wearables can either track and identify the user's location within hotspot areas affected by the SARS-COV-2 virus (commonly known as coronavirus) or identify the user's past and present neighboring nodes during specific time-space bounds. The main goal is to predict the probability of a user being infected with the virus, based on the past information collected from neighbors. Broadly speaking, contact tracing in the pandemic context refers to the ability of a user identification who has been exposed to the virus carried by a person tested positive for it.

A wireless contact-tracing application aims to determine the probability of being infected with COVID-19 in a fully automated or semi-automated manner and based on the wireless signals [2]. Contact tracing in the wireless world is also known as proximity tracing or user proximity detection or proximity tracking [5]. In general, contact tracing (either manual, or wireless-based, or mixed) is highly promising nowadays as it enables an increase in the application rate for preventive measures. Such as self-isolation or quarantine for infected persons and persons with a high likelihood to cross their paths with someone infected. Relevant and timely actions additionally include avoiding close contacts, wearing masks, and following proper hand hygiene for persons with a low-to-moderate likelihood to contact the disease [2], [5], [7].

Traditionally, contact tracing involves manual efforts led by governments and health service provider personnel. Nevertheless, with millions of COVID-19 positive cases worldwide, relying solely on manual contact tracing stands close to impossible. The alternative solution is to supplement the manual tracing with the use of automated or semi-automated contact-tracing procedures based on wireless devices carried on by users, such as wearable devices and smartphones [5], [7]–[9]. While there are already several contact-tracing protocols developed worldwide, as described later in Section IV, and while many wireless proximity-detection solutions based on wireless signals exist for many years, comparative surveys of existing solutions are still missing from the current literature, and the technical limitations coming from the wireless signal propagation are still insufficiently mapped out.

The fundamental objectives of this paper are to offer an explicit and compact outline of the leading wireless technology support for a contact-tracing application, the technical limitations and target technical criteria when aiming to design a contact-tracing application suitable for wearable devices, and the perspective on the open challenges of wide-scale adoption of such applications and protocols.

The rest of the paper is organized as follows. Section II provides an overview of the main concepts and principles of wireless automated contact-tracing applications.

Next, Section III elaborates on the trade-offs of developing such applications for wearables. Section IV provides an overview of existing contact-tracing applications. The last section concludes our paper and provides a brief outline of other relevant challenges on contact-tracing applications.

II. Principles of a wireless automated contact-tracing application

The key idea of a wireless contact-tracing application is illustrated in Fig. 1. Assuming that there are several mobile users in a certain geographical area, denoted starting from user A to user F, and each of them is equipped with some wearable sensors and/or mobile devices. Commonly, the users without any wireless sensors are ‘invisible’ to a basic wireless receiver – these users could not be considered in the infrastructure-based wireless contact tracing. Exceptions could be users equipped with passive tags for ambient backscatter communications or other sophisticated techniques described in [10], [11]. However, the feasibility of such approaches in the context of a contact tracing solution is yet to be investigated.

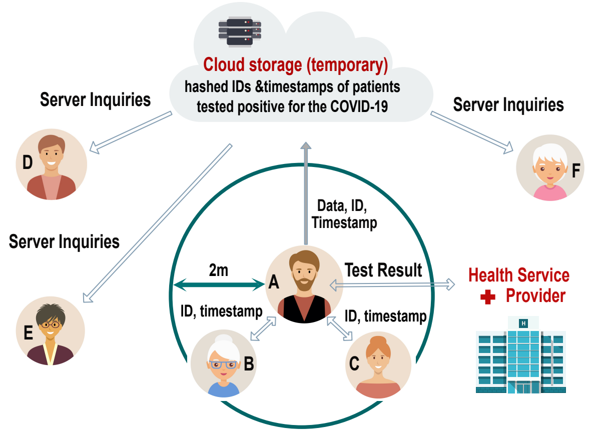


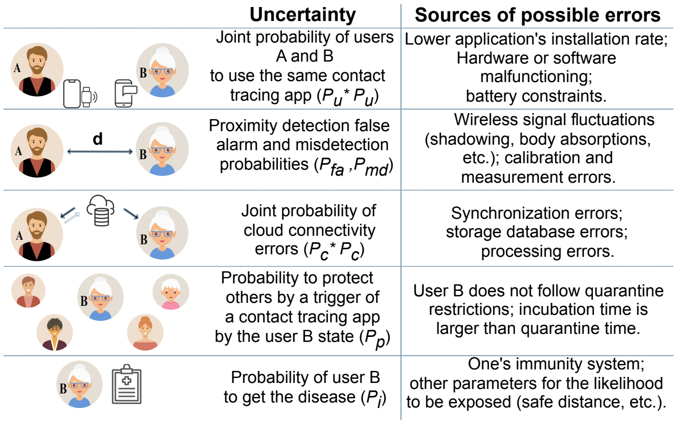
Figure 1: Illustration of the basic principles of a wireless COVID-19 contact-tracing application.

Generally, the user devices are equipped with short-range wireless communication technology, e.g., Bluetooth Low Energy (BLE) or IEEE 802.11 (a.k.a., WiFi) [12], [13]. Commonly, the user equipment transmits the beacons with timestamps along with the anonymized user IDs, thus, other users in the range of the emitter can ‘hear’ and store these anonymized IDs and timestamps of neighboring nodes on their device.

For example, when a tagged user A emits a wireless signal, the receiving users in proximity could first estimate the distance based on a number of available characteristics as presented in [14]. In case the distance is lower than a predefined threshold, e.g., the value is lower than 2 m, as the safety threshold adopted by many research papers [2], [15], [16], then the receiving user will store the anonymized ID from user tagged user and the corresponding timestamps. Therefore, a ledger of neighboring users could be created per node.

A. Technology chain and associated sources of errors in a wireless contact-tracing application

The wireless contact tracing chain and multiple sources of errors are summarized in Fig. 2. In an automated contact-tracing app, the ultimate and highly relevant parameter for the disease control is the probability of protecting P_p the other users as a product of active application use, followed by a certain action point, e.g., self-quarantine. The intuitive meaning of P_p is that P_p*100% of healthy people who might be in contact with person B, who is infectious after the contact with person A, could potentially avoid the disease due to an effective action point of person B (such as self-quarantine, wearing a mask, preserving physical distance, etc.).



	Uncertainty	Sources of possible errors
A B	Joint probability of users A and B to use the same contact tracing app (P_u* P_u)	Lower application's installation rate; Hardware or software malfunctioning; battery constraints.
A d B	Proximity detection false alarm and misdetection probabilities (P_{fa} ,P_{md})	Wireless signal fluctuations (shadowing, body absorptions, etc.); calibration and measurement errors.
A B	Joint probability of cloud connectivity errors (P_c* P_c)	Synchronization errors; storage database errors; processing errors.
B	Probability to protect others by a trigger of a contact tracing app by the user B state (P_p)	User B does not follow quarantine restrictions; incubation time is larger than quarantine time.
B	Probability of user B to get the disease (P_i)	One's immunity system; other parameters for the likelihood to be exposed (safe distance, etc.).

Figure 2: Uncertainty models and various sources of errors in the contact-tracing chain.

Undoubtedly, P_p depends on several other parameters, which are described in Fig. 2: i) the joint probability of two users found in vicinity of each other to use the same contact tracing application, e.g., with independent users and individual probability P_u per user, the joint probability becomes $P_u * P_u$, ii) the false alarm P_{fa} and misdetection P_{md} probability of estimating that two users are within infectious distance from each other, e.g., at less than 2 m for more than 15’ [2], [15], [16]), iii) the probability P_c that the connectivity to the cloud server works properly, e.g., device of user A has access to long-range wireless connectivity to the server storing information about the temporary IDs of COVID-19 positive persons during their period of being infectious, and iv) the illness probability P_i (i.e., the actual probability that user B gets the disease if (s)he was within infectious distance from a COVID-19 positive user A for a duration exceeding a threshold).

For clarity, it is essential to notice that although P_{fa} stands for a technical specification, this parameter is not mapped into the eq. (1). Due to the fact that the false alarm ratio does not affect the overall effectiveness or prevention probability of a digital contact-tracing app, as non-infectious users falsely classified as infectious users do not spread the virus. It is to be highlighted that P_{fa} levels play a significant role in the user's perceptions of the contact-tracing application's usefulness. High values of P_{fa} would mean that many non-infectious users would be recommended to self isolate without any actual need. Therefore, this scenario could affect the app installation rate (i.e., less users would be willing to install an app with a high P_{fa} estimates).

Remarkably, some non-technical effects, such as the immunity system's impact on the probability of getting the disease, are not modeled in the above model. This study is devoted to understanding the patterns and estimating the maximum prevention probability, upper-bounded through technical constraints, via:

$$P_{p,max} = P_u^2 * (1 - P_{md}) * P_c^2 * P_i, \tag{1}$$

where P_u stands for the independent users and the unique probability per user, P_{md} is the probability of misdetection, i.e., the probability to recognize a possibly infectious user as a non-infectious user, which might happen due to an incorrect distance and exposure-duration estimates by a digital contact-tracing app. P_c refers to the probability that the cloud connectivity is reliable, and P_i is the illness probability, i.e., the exact probability that user B gets infected by the disease if (s)he was at an epidemiologically unsafe distance from a COVID-19 positive user A for a period exceeding a threshold. Particular considerations will allow us to present some simplified examples based on simulated data in subsection IV-B.

Fig. 1 also shows several sources of errors that may affect the computation of each of the probabilities in the technical chain of the contact-tracing applications. The next two sub-sections provide more enhanced specifications on two significant technical constraints to be considered in the process of designing a contact-tracing application, namely, the inconstancy of the Received Signal Strength (RSS), as the primary source for the distance estimation (subsection II-B), and the timing errors (subsection II-C).

B. RSS Random Fluctuations

The wireless received signal always exhibits random fluctuations due to reflections, refractions, scattering, and diffraction on various obstacles in the signal path, e.g., furniture, cars, tree leaves, and others, body absorptions, device orientation. Moreover, particular movements in the environment, as people and cars moving around, doors opening and closing, also impact the wireless medium. Large-scale fading shadowing models typically model such random fluctuations as described in [17], [18], where random signal effects in decibels (dB) or logarithmic scales are usually characterized by a random Gaussian distribution of zero mean and certain standard deviation. Such random fluctuations are especially crucial for RSS-based distance estimates, as a user at a far distance, i.e., outside the typically 'infectious range', can be easily mistaken to be at a nearby distance, i.e., inside the typically 'infectious range' of 2m [15].

For example, assuming a free-space-loss model (FSL), a contact-tracing application based on BLE operating at 2.4 GHz carrier frequency, and a shadowing standard deviation (SD) of 5 dB. This value is a typical number according to measurements reported in [17], [18] with ignoring additional calibration and body absorptions errors. The probability of mistaking a user at 3m from the user tested positive for COVID-19 to be at only 2m is 6.2%, and the probability to mistake a user at 4m distance to be at only 2m is 3.9%. Therefore, there will be false positives and false negatives due to the random signal fluctuations of the signal used in the contact-tracing application, even in cases where the rest of the contact-tracing chain (see Fig. 1) is functioning perfectly.

C. Timing errors

While the signal fluctuation errors addressed in the subsection II-B are mostly relevant for contact-tracing solutions relying on RSS measurements, as the vast majority of current contact-tracing applications are, the timing errors are relevant to all contact-tracing wireless applications [19].

Timing errors influence both the estimation of the duration of the exposure, as well as the distance estimates between users for distances estimated from timing measurements. Clock errors between the device clocks of users A and B are certainly a part of the timing errors, especially when synchronization to the cloud server is done seldom, e.g., once a day.

Timing errors are nevertheless less influential by misdetection, e.g., not finding out that user A was at less than 2m away from user B and false alarm, e.g., mistakenly detecting that user B was at less than 2m from user A, probabilities than the random effects described in subsection II-B.

For RSS-based distance measurements, such as those based on WiFi or BLE signals, the Doppler error will have close to no impact on the distance estimates, and the 0.86s error per day will have an insignificant impact on the estimates for the duration of exposure. A centralized cloud server can efficiently deal with Doppler error compensation between two unsynchronized devices, however, such Doppler error compensation may be more challenging in decentralized approaches, detailed in the following subsection. This impact of timing errors on timing-based distance estimates makes the choice of an RSS-based distance estimation to be the preferred choice in modern contact-tracing applications.

D. Centralized versus decentralized architectures

Two main concepts have been designed in conjunction with wireless contact-tracing applications: i) a centralized (or infrastructure-based) architecture, where the main information, such as users temporary IDs and timestamps, is processed and stored on a central server (thus, the server has all the information about all devices using the app), and ii) a decentralized or federated architecture, where users keep on their device the relevant information, e.g., own temporary IDs, neighbors' temporary IDs, and timestamps, and contact the server only to report a COVID-19 infection or to download the temporary IDs of other users who reported an infection to the server.

Generally, the risk analysis, i.e., calculating the probability P_i of a user to get the disease, is calculated at the server side in centralized architectures. In contrast, P_i in a decentralized architecture is calculated on the user device. Therefore the server has access to a lower amount of user-related information, e.g., no data about the user's contacts and temporary IDs of other users who intersected the path of an infectious user need to be transmitted.

III. Trade-offs in the design of a contact-tracing application for wearables

In addition to the accuracy, a wireless contact-tracing application with a potential to be widely adopted by a free market must comply with a fair trade-off between several design constraints, namely, the following.

A. Privacy-preservation constraint

To the best of our knowledge, a privacy-preserving application is more likely to be adopted by the users. In order to preserve the users' privacy, the application must obey the data minimization principle (transfer only the minimum necessary data between the network nodes), avoid tracking of the user location at all costs, and put a reasonable time limit of the data storage window, e.g., 14 days is considered as a reasonable time limit in [7].

B. Trust constraint

The chances that the users will adopt a novel application are higher if their friends are already using it [20]. Another factor is the service provider being known and trustable along with the application not conveying large false positives or false negatives errors. Reversely, a user is more likely to remove an application that fails to provide the expected results or in cases where people from their social network are not utilizing the application.

C. Reliable range constraint

This constraint refers to two subaspects. On the one hand, only the users in close proximity, e.g., less than 2m over a certain time duration, can typically infect others. Therefore, the adopted wireless standard should provide accurate information whether the user is close to another, e.g., below 2m, and not just somewhere in the same building, e.g., within 80–100m radius, which is the typical average coverage of a BLE or WiFi-enabled indoor device. On the other hand, the available wireless connectivity should have enough coverage to connect to the nearby gateway or AP/BS and then to the cloud server, e.g., by using LTE, LoRa, Narrow-band IoT (NB-IoT), Sigfox, or Telensa [21]–[23] depending on the availability on the device. The reliable coverage constraint requires both accurate short-range and robust long-range connectivity solutions installed on the same device.

D. Low/ultra-low energy consumption constraint:

Having a long-lasting battery on the mobile device used for the contact-tracing app is of utmost importance for mass-market adoption. Therefore, the selection of the wireless technology that causes significant device battery draining is not desirable. Most wearables rely on short-range BLE for wearable-to-mobile or wearable-to-wearable connectivity. Simultaneously, most of them connect to the edge gateway or cloud servers via the high-power cellular or WiFi connectivity solutions available on their gateways, e.g., mobile phones. Standalone wearable solutions have started to use IoT long-range low-power IoT connectivity solutions such as LoRa, Sigfox, or NB-IoT [9], [22] in order to ensure long battery life. Energy harvesting solutions, i.e., gathering energy from the environment, such as motion, light, sound, and wireless interference, are also under scrutiny and might offer viable solutions for future wearables.

IV. Contact-tracing solutions of today

This section provides an overview of existing contact-tracing solutions followed by the analysis of their utility.

A. Brief survey of current contact-tracing solutions

Since the beginning of 2020, many smartphone-based and few wearable-based applications have been developed for contact tracing for COVID-19 disease control worldwide. In this paper, we observe some of the contact-tracing apps and protocols for comparison, in terms of IoT connectivity solution, type of measurement for distance estimation, i.e., proximity detection method, type of architecture, qualitative values for their accuracy, energy efficiency, and privacy levels based on works reported in various research papers, advantages, and technical challenges. The choice of the apps and protocols was based on their current popularity among users, level of interest in social media and/or in technical repositories, and the variability in the employed contact-tracing methods and underlying technologies that a broad view of possible technical solutions is provided. There are currently at least 69 governmental-approved mobile applications in at least 29 countries, as of September 2020. Most of them have proprietary features and report some limitations and the lack of user adoption rates. The vast majority of the governmental contact-tracing applications rely on BLE technology and RSS measurements, similarly with the majority of techniques discussed in this work.

The first one, the Decentralized Privacy-Preserving Proximity Tracing or DP-3T [7] is a BLE-based decentralized protocol developed for contact tracing, currently deployed on the Swiss market and under testing phase in few other EU countries such as Finland and Estonia. The DP-3T protocol also served as inspiration for the Google/Apple system, and it contends to be one of the most privacy-preserving protocols existing for contact-tracing applications today. Here, the distance estimate between two persons is based on RSS and are, therefore, susceptible to wireless signal fluctuations.

The Easy Band [16] is a wearable-based proximity-detection solution relying on BLE RSS distance measurements to detect nearby located users. The data is processed on a centralized server accessible via infrastructure connectivity for the decision-making process on people's infectiousness state around.

RSS-based solution with a centralized server storing encrypted user information and computing a score matching calculation to detect users that have possibly been infected by a close COVID-19 positive contact is EPIC ass described in [8].

The Google/Apple Exposure Notification (GAEN) system [24] also relies on BLE RSS-based distance measurements between devices and a decentralized architecture similar to DP-3T. No location information is stored about the users. The main feature of this solution is that DP-3T is a fully open-source protocol, while some parts in the Google/Apple system will remain proprietary.

The authors in [15] implemented a completely different approach by using the magnetic field intensity from magnetometers installed on smartphones instead of BLE RSS measurements. A centralized server processes the magnetometer-based metric in order to detect similar patterns of magnetic field intensities between users. Users with highly correlated patterns of this metric are assumed to be in close proximity to each other.

Nevertheless, another distinct wireless connectivity approach is offered by Tsingoal company through their LocalSense approach [25], which is time-based on UWB and Round-Trip Time (RTT) measurements. The main advantage stays in increased accuracy of the distance estimates between users, as UWB RTT measurements are known to offer 0.1m accuracy, ten times more accurate in comparison with Bluetooth solutions. The main downsides are the need for additional UWB infrastructure, as well as the privacy threats due to centralized infrastructure properties.

Mokosmart [9] is a wearable wristband developed by a Chinese company for COVID-19 contact tracing and integrating BLE and LoRa technologies in a centralized architecture.

The solution described in [26] relies on multiple sensors available on a smartphone and could offer better protection against the wireless signal variability, and transform into higher computational costs of blending heterogeneous measurements from various sensors.

The Pan-European Privacy-Preserving protocol (PEPP-PT) [27] is a centralized solution that uses the proximity tracing concept between phones of the app users by measuring BLE radio signals to assist in the restraining of contagious viruses' expanse. The researchers state that the software starts to log the encrypted proximity history only when two devices are situated in epidemiologically sufficient proximity for a reasonable time. In this scenario, the devices store only each other's anonymous identifiers. Thus, no geographic location or any additional personal information is collected. Moreover, the older events are deleted after some period of time.

Arguing that there is no fully decentralized architecture available today, the researchers in [28] proposed a ROBust and privacy-presERving proximity Tracing (ROBERT) protocol, which is built on federated server infrastructure. After the first step, where a contact-tracing app is installed, the server assigns a permanent ID to each user, and the central server possesses records of corresponding temporary IDs, which change every 15 min. The developers of the ROBERT protocol claim that no malicious entity could use the information to identify users. Privacy is preserved by encryption, and the users need to obtain trust in the server, storing the information.

TraceTogether [29] is another example of a contact-tracing application that relies on BLE signals. As a possible limitation, this application should always be running on the mobile phone background, which might cause the battery drain of the device. Anonymous identifiers are generated by encrypting the user ID with a private key and are known exclusively by the Ministry of Health.

Those mentioned above, existing COVID-19 contact-tracing mobile applications, solutions, and protocols, can be characterized via diverse metrics, such as levels of proximity detection accuracy, energy efficiency, and privacy. As a matter of fact, there is a trade-off where a high accuracy level (in relation to position estimates) that associates with privacy deficiency and vice versa. Clearly, a pattern can be seen that decentralized solutions fare better than centralized solutions in terms of privacy. Therefore, such decentralized applications as DP-3T and Google/ Apple protocol provide privacy-by-design, which makes them more robust to malicious entities in the chain of contact tracing.

Accuracy via RSS-based methods is still to be improved, however, attention must be paid to the energy consumption on the device side, as more accurate contract-tracing/proximity detection solutions in existence also have lower energy efficiency.

Additionally, we conclude that a combination of short-range and large-range ultra-low-power technologies must be deployed to overcome the technical challenges related to wireless connectivity and energy consumption on wearables more efficiently.

In the following sections, we introduce our analysis and the findings on the parameters' effect and the extent to which they affect the utility of the contact-tracing applications.

B. Illustrative example of the contact-tracing app utility

Fig. 3 illustrates an example of fundamental challenges in a multi-dimensional plane between the various sources of uncertainty in using an automated wireless contact-tracing application through a wearable device.

A target maximum prevention probability $P_{p,max} = 0.5$ is taken as reference in Fig. 3 (for clarity purpose, curves with $P_{p,max} > 0.5$ are not shown, as for such values there are no parameters fulfilling the target constraints at $P_i = 0.6$), and the isosurface 3D plots are employed to show the dependence on three technical parameters, P_u, P_c, and P_{md} described in subsection II-A. In addition, four-level of infection rate probabilities are illustrated via different colors in each curve. An

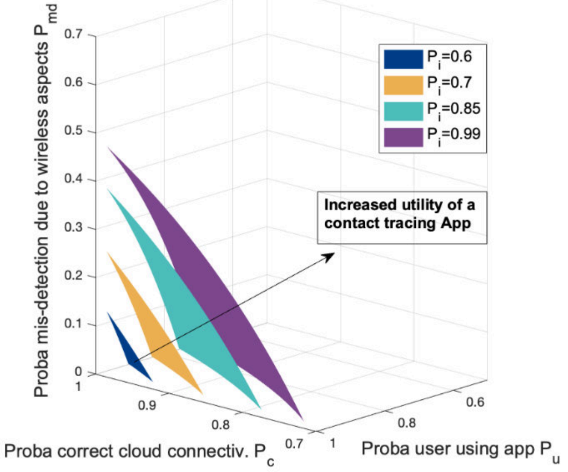


Figure 3: A simplified example of the utility of a contact-tracing application based via isosurfaces at a target prevention probability $P_{p,max}$ of 50%.

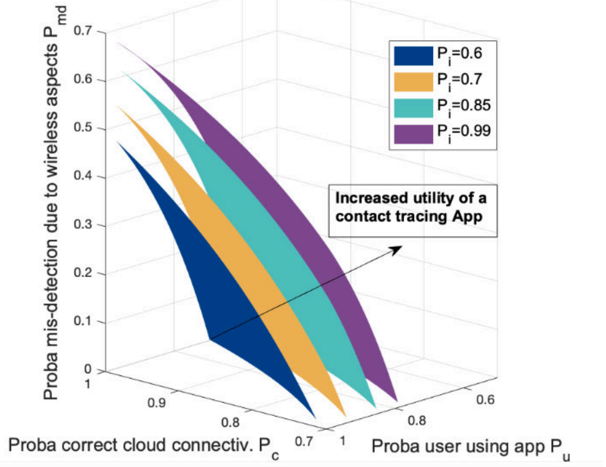


Figure 4: A simplified example of the utility of a contact-tracing application based via isosurfaces at $P_{p,max}$ of 30%.

isosurface is a surface showing all combinations (P_u, P_c, and P_{md}) providing the target constant value $P_{p,max}$. A smaller surface illustrates the fact that the target prevention probability can be achieved with stricter conditions on the (P_u, P_c, and P_{md}) probabilities, while a larger surface shows a better prevention probability for a wider combination of probabilities of connectivity errors, user adoptions, and misdetections due to the wireless signal variability.

As seen in Fig. 3, a target prevention probability of 50% better than in the absence of a mobile contact-tracing app can be achieved if at least 71% of users adopt the application and if the connectivity to the cloud is robust in at least 70% of the cases. If the target prevention probability decreases to only 30% (see Fig. 4), this can also be achieved with a 50% user adoption rate and 70% correct cloud connectivity, and up to 45% misdetection probabilities are also satisfactory.

It should be noticed that these numbers are just examples of the multi-dimensional problem an expert has to solve when designing an efficient contact-tracing application. The statistics point out the fact that it is not enough to have more than 90% user adoption of a contact-tracing application in order to achieve high efficiency in digital contact tracing, yet all multi-dimensional aspects of the problem should be considered. By comparing the curves, one gets useful insights about parameters, e.g., allowing one to fine-tune the trade-offs between the parameters in multi-dimensional space, the absolute values are to be taken with a grain of salt, as no medical or epidemiological insights have been used in the current assumptions. The simplified model illustrated in Fig. 3 serves as a basis for understanding the technical constraints on wireless signals that are used for contact-tracing applications.

V. Discussion and Conclusions

A comparison of standalone and non-standalone solutions on wearables and the main challenges of contact-tracing approaches on the wearable market is presented in Table I. A fully standalone solution has the advantage of better portability, easier use, and, very often, longer battery life than non-standalone solutions. Thus, in our view, standalone solutions could be more suitable for a wide adoption within a large and diverse population than a non-standalone solution. While the main technological limitations in non-standalone approaches are also similar to standalone ones, wearable-based standalone solutions introduce additional challenges dictated by the low power consumption and low size constraints.

Table I: Challenges and potential solutions on wearable-based contact tracing.

Type	Challenge	Solutions to be investigated
Standalone solutions	Long-range low-power connectivity to the cloud servers	LoRa and NB-IoT are among the most energy efficient long-range solutions; Ambient backscattering device-to-infrastructure communications and other energy harvesting solutions.
	Optimal tradeoff between a small-size device and a high computational power	Compressive sensing; approximate computing.
Standalone & non-standalone	Short-range low-power connectivity	BLE is nowadays the top choice for low-power short-to-medium range connectivity due to its widespread use on wearables.
		Ultra-low-power short-range solutions need also to be investigated further as well as ambient backscattering device-to-device communications and other energy harvesting solutions.
	Increased accuracy of the distance estimates for proximity detection	High-sensitivity approaches through better path loss models, better calibration, adaptive filtering, e.g., taking user speeds into account and environmental sensing, e.g., simultaneous mapping and distance estimation.
	User privacy	Blockchain and decentralized/federated architectures; Open-source code.

As an outcome, we conclude that most advanced digital contact-tracing applications can be effective in disease prevention when suitably used with other prevention methods, as a part of a systematic approach that corresponds to the implementation of other precautions. The multi-dimensional problem could be solved with scientists' efforts to identify and adopt a combination of the most robust solutions and, therefore, to achieve better results in accurately tracing the contacts, implementing prevention measures, and stabilize the pandemic situation worldwide.

In this paper, we have provided several technical perspectives on digital contact-tracing applications via mobile devices and wearables for effective COVID-19 control. We have derived an upper-bound on the effectiveness of a digital contact-tracing app (called here maximum prevention probability), which carries the message of how much a digital contact-tracing app could help versus the situation when no digital contact-tracing app is used. We have seen that several technical parameters can influence such an app's effectiveness, and these technical parameters are determined by the wireless technologies used in estimating the distances between users, their connectivity to the cloud, and their exposure duration. In addition to the technical considerations, many ethical and privacy-related aspects must be taken into account during a wide-scale adoption of digital contact-tracing apps, and these remain a topic of future investigations. For instance, there are ethical challenges in centralized systems, where a lot of user-related information is stored in centralized cloud servers. In addition, the effectiveness of a digital contact-tracing app also depends on the infection risk of each person, which is an epidemiological factor that requires further research outside the technical domain.

A potential further research direction can be found in advancing technical specifications of digital contact-tracing applications, e.g., the needed minimum periodicity of broadcast signals used for localization and its relationship with the user movement speed and device energy consumption. To improve wireless mobile communications' signal strength, one could consider focusing on wearable antennas' directivity, precisely due to their limited size constraints.

Acknowledgments

The authors gratefully acknowledge funding from European Union's Horizon 2020 Research and Innovation programme under the Marie Skłodowska Curie grant agreement No. 813278 (A-WEAR: A network for dynamic wearable applications with privacy constraints, http://www.a-wear.eu/).

References

[1] S. Bansal and D. Kumar, "IoT Ecosystem: A Survey on Devices, Gateways, Operating Systems, Middleware and Communication," *International Journal of Wireless Information Networks*, pp. 1–25, 2020.

[2] E. Hernández-Orallo and et al., "Evaluating How Smartphone Contact Tracing Technology Can Reduce the Spread of Infectious Diseases: The Case of COVID-19," *IEEE Access*, 2020.

[3] L. Reichert, S. Brack, and B. Scheuermann, "A survey of automatic contact tracing approaches," *Cryptol. ePrint Arch., IACR, Bellevue, WA, USA, Tech. Rep*, vol. 672, p. 2020, 2020.

[4] M. Scudellari, "COVID-19 Digital Contact Tracing: Apple and Google Work Together as MIT Tests Validity," *IEEE Spectrum*, vol. 13, 2020.

[5] J. Li and X. Guo, "COVID-19 Contact-tracing Apps: A Survey on the Global Deployment and Challenges," *Preprint arXiv:2005.03599*, 2020.

[6] C. T. Nguyen and et al., "A comprehensive survey of enabling and emerging technologies for social distancing—Part II: Emerging technologies and open issues," *IEEE Access*, vol. 8, pp. 154 209–154 236, 2020.

[7] C. Troncoso and et al., "Decentralized Privacy-Preserving Proximity Tracing," *Preprint arXiv:2005.12273*, 2020.

[8] T. Altuwaiyan, M. Hadian, and X. Liang, "EPIC: Efficient Privacy-Preserving Contact Tracing for Infection Detection," in *Proc. of IEEE International Conference on Communications (ICC)*. IEEE, 2018, pp. 1–6.

[9] MokoSmart, "Moko Smart LoraWan-based Wearable for Contact Tracing," https://www.mokosmart.com/lorawan-ble-wearable-wristband-beacon-covid-19-contact-tracing-solution/ [Accessed September 21, 2020].

[10] R. Biswas, J. Säe, and J. Lempiäinen, "Power Budget for Wide Area Ambient Backscattering Communications," in *Proc. of IEEE Vehicular Networking Conference (VNC)*. IEEE, 2018, pp. 1–6.

[11] M. A. M. Marinho and et al., "Spherical Wave Array Based Positioning for Vehicular Scenarios," *IEEE Access*, vol. 8, pp. 110 073–110 081, 2020.

[12] A. Ometov and et al., "Facilitating the Delegation of Use for Private Devices in the Era of the Internet of Wearable Things," *IEEE Internet of Things Journal*, vol. 4, no. 4, pp. 843–854, 2016.

[13] A. Ometov and et al., "Reliability-centric Analysis of Offloaded Computation in Cooperative Wearable Applications," *Wireless Communications and Mobile Computing*, vol. 2017, 2017.

[14] A. Basiri and et al., "Indoor Location Based Services Challenges, Requirements and Usability of Current Solutions," *Computer Science Review*, vol. 24, pp. 1–12, 2017.

[15] S. Jeong, S. Kuk, and H. Kim, "A Smartphone Magnetometer-based Diagnostic Test for Automatic Contact Tracing in Infectious Disease Epidemics," *IEEE Access*, vol. 7, pp. 20 734–20 747, 2019.

[16] A. K. Tripathy and et al., "EasyBand: A Wearable for Safety-Aware Mobility during Pandemic Outbreak," *IEEE Consumer Electronics Magazine*, 2020.

[17] Y. Wang and et al., "Characterization of the Indoor Multiantenna Body-to-Body Radio Channel," *IEEE Transactions on Antennas and Propagation*, vol. 57, no. 4, pp. 972–979, 2009.

[18] E. S. Lohan and et al., "Received Signal Strength Models for WLAN and BLE-based Indoor Positioning in Multi-Floor Buildings," in *Proc. of International Conference on Localization and GNSS (ICL-GNSS)*. IEEE, 2015, pp. 1–6.

[19] N. Ahmed and et al., "A Survey of COVID-19 Contact Tracing Apps," *IEEE Access*, 2020.

[20] M. Bailey and et al., "Peer Effects in Product Adoption," National Bureau of Economic Research, Tech. Rep., 2019.

[21] P. Figueiredo e Silva, V. Kaseva, and E. S. Lohan, "Wireless Positioning in IoT: A Look at Current and Future Trends," *Sensors*, vol. 18, no. 8, p. 2470, 2018.

[22] F. Wu, J.-M. Redouté, and M. R. Yuce, "We-Safe: A Self-Powered Wearable IoT Sensor Network for Safety Applications Based on LoRa," *IEEE Access*, vol. 6, pp. 40 846–40 853, 2018.

[23] D. Kozyrev and et al., "Mobility-centric Analysis of Communication Offloading for Heterogeneous Internet of Things Devices," *Wireless Communications and Mobile Computing*, 2018.

[24] K. Michael and R. Abbas, "Getting Behind COVID-19 Contact Trace Apps: The Google-Apple Partnership," *IEEE Consumer Electronics Magazine*, 2020.

[25] Tsingoal, "UWB Social Distancing," https://www.social-distancing-contact-tracing.com [Accessed September 21, 2020].

[26] K. A. Nguyen, Z. Luo, and C. Watkins, "Epidemic Contact Tracing with Smartphone Sensors," *Preprint arXiv:2006.00046*, 2020.

[27] PEPP-PT, "Pan-European Privacy-Preserving Proximity Tracing," https://www.pepp-pt.org [Accessed September 21, 2020].

[28] M. Cunche and et al., "On Using Bluetooth-Low-Energy for Contact Tracing," Ph.D. dissertation, Inria Grenoble Rhône-Alpes; INSA de Lyon, 2020.

[29] R. Abbas and K. Michael, "COVID-19 Contact Trace App Deployments: Learnings from Australia and Singapore," *IEEE Consumer Electronics Magazine*, 2020.