5G and Beyond for Contact Tracing

Domenico Giustiniano, Giuseppe Bianchi, Andrea Conti, Stefania Bartoletti, and Nicola Blefari Melazzi

***Abstract*—The COVID-19 pandemic has suddenly raised the need for technological solutions capable to trace contacts of people and provide location-based analytics. Several countries have adopted proximity-based (short-range) technologies, such as Bluetooth, which however appear hindered by deployment issues, security leakages, lack of reliability, and data governance concerns. This paper posits that 5G and beyond can play a primary role in contact tracing and group movement monitoring. Contact tracing based on 5G location-based analytics benefits from the pervasive deployment of cellular networks, the several years of effort to design cellular standards for localization and analytics, and the best practices of cellular operators to handle location data.**

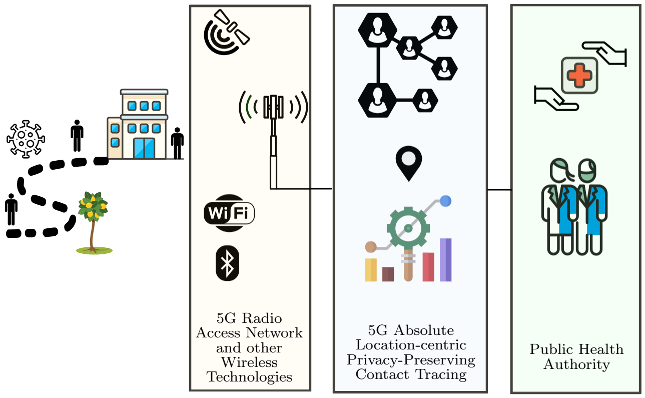
WiFi
5G Radio Access Network and other Wireless Technologies
5G Absolute Location-centric Privacy-Preserving Contact Tracing
Public Health Authority

Fig. 1: Vision of 5G system and beyond for contact tracing.

I. Introduction

The COVID-19 pandemic has pushed academia and industry to seek for technological solutions for tracing contact events of people and support the healthcare system. The traditional method to trace chains of infection consists of interviewing any infected person to trace back any contacts in the previous days. Such process has several shortcomings: it is very time consuming, requires ad-hoc personnel, incurs in delays in the process of identifying contacts, relies only on known contacts, it is performed in highly-emotional moments for the person tested positive for the virus, and it does not result in sufficient reliability and precision. To overcome these issues, the objective of research centers and industries is to provide a dependable, accurate, widely used, secure and privacy-preserving system for contact tracing.

As soon as the COVID-19 emergency started, several countries have launched a call for contact-tracing solutions. Most European countries have chosen mobile apps which perform proximity measurements via Bluetooth Low Energy (BLE). However, as we will discuss in details later in the paper, such approaches appear hindered by a number of concerns, including:

- limited deployment – any technology requires a sufficiently high number of users;
- security and privacy concerns – many weaknesses and privacy leakages are documented;
- lack of reliability – BLE-based apps are prone to errors due to the usage of signal-strength measurements to infer contacts; and
- data governance – there exists a double standard in governing users' location data, with fine-grained tracking of device location available only to private companies such as Google or Apple.

This paper proposes the concept of cellular network-assisted contact tracing, focusing on the key technological enablers and privacy aspects. Figure 1 illustrates at high level that 5G networks and beyond can provide a unique opportunity, in addition to communication, also for providing location awareness, thereby fulfilling the requirements set forth by a reliable and trustworthy digital contact tracing system.

We posit in this work that the densification of cellular networks, together with emerging technologies such as massive multiple-input–multiple-output (MIMO) and millimeter wave (mmWave), as well as new techniques to estimate the surrounding environment and people behaviour, can be a strong asset for contact tracing, and can be leveraged to increase its accuracy and reliability. We will also discuss the fusion of cellular data with other technologies for contact tracing, as well as the open challenges to access these measurements. Our approach is driven by the work conducted in 3GPP (3rd Generation Partnership Project) to extend the cellular network with localization and analytical functionalities, and provide greater flexibility and reconfigurability with respect to

This research is supported in part by the European Union's Horizon 2020 research and innovation programme under Grant 871249 and in part by Ministerio de Ciencia, Innovación y Universidades Grant RTI2018-094313-B-I00. The authors would like to thank all the LOCUS project's partners (https://www.locus-project.eu) and Ignacio Berberana for insightful discussions.

past cellular technologies. Our approach is also driven by the proposal of 3GPP to integrate all localization technologies (such as global navigation satellite system (GNSS), WiFi, and Bluetooth) with the cellular one, to further increase the localization performance.

Our paper starts from the latest developments of 3GPP, including the ongoing effort on beyond 5G. Although no work has been conducted in 3GPP for contact tracing yet, we will show that the architectural work in 3GPP for positioning, analytics and service-based deployments lays the foundation to develop reliable and contact tracing solutions. Notwithstanding all the advantages that localization, tracing, and monitoring solutions can provide, great care must be devoted to preserve the privacy of users. The increasing sensibility of citizens to privacy issues calls for system that fully protect user data and transparently show how they do so. To mitigate privacy issues, contact tracing solutions can be designed with the aim of decoupling the knowledge of absolute position from that of user identity in the process of inferring contacts.

II. Limitations of app-based solutions

This section discusses the limitations of app-based solutions.

Limited deployment. All approaches require the installation of an app, but struggle to reach a sufficient number of users for a meaningful exploitation of the technology. Fig. 2 shows the rate of downloads over the population size for the official apps of four different countries from October 2020 to March 2021 (SwissCovid in Switzerland, Immuni in Italy, TousAntiCovid in France, and COCOA in Japan). Such deployment rate is compared to the rate of positive cases registered in the app out of the total number of the detected cases in the country within the same month. Despite the number of downloads is slightly increasing over time, a large part of users is inactive, and the system is aware of a very small percentage of the detected positive cases in the country. Reasons for this outcome include ineffective communication and limited awareness, lack of trust by end users in the app's implementors and/or deployers, and market fragmentation.

Security and privacy concerns. Since these contact tracing apps were developed and deployed in a very short time, they could not be properly scrutinized in terms of security — a process which normally takes years and multiple rounds of assessment. As a result, many security weaknesses (e.g., quite straightforward replay attacks) as well as privacy leakages are documented [1].

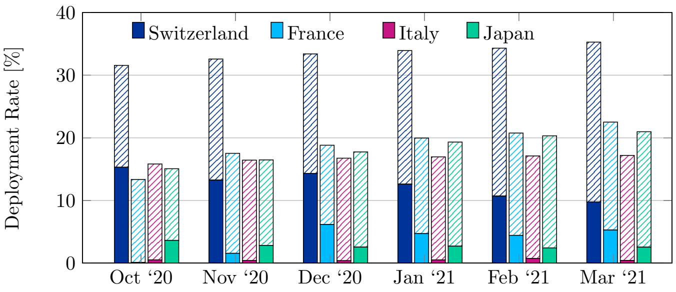

Fig. 2: Deployment rate of official BLE-based apps. Dashed bars represent the rate of app downloads in the population. Full bars refer to the rate of reported positive cases among the detected positive cases in the country.

Lack of reliability. BLE-based apps are prone to errors as they use signal-strength measurements to infer contacts. Current detection rules fail significantly, ranging from no exposure notifications with Swiss and German detection rules to a true positive and negative rate of 50% with the Italian detection rule [2]. False negatives might allow the virus to spread further without being controlled, whereas false positive might have severe emotional impacts on the victims and might create unnecessary load on the healthcare system.

Data governance. The handling of data in the various contact tracing apps is not uniform across countries, despite the reliance on the same BLE-based Google/Apple Exposure Notification service. For example, each country has adopted different rules for the registration of the positive cases (e.g., on a voluntary basis) and this affects the number of positive cases that are effectively registered in the app (see Fig. 2). Moreover, a sort of contradiction emerges from the analysis carried out in [3]. On one side, health authority client apps do not access any absolute location information. Their careful data protection is traded off with a performance toll: the availability of (selected) raw BLE measurements and GNSS data would in fact significantly improve the contact tracing effectiveness. On the other side, fine-grained tracking of device location over time appears to be performed by private companies such as Google or Apple. It is true that a tech-savvy user may eventually disable Google's tracking, but we find such double standard in governing users' location data quite striking.

III. 5G localization and contact tracing

This section covers the following aspects:

- the design of absolute location-centric (ALC) tracing that exploits both spatial and temporal dimensions based on soft decision;
- a discussion on contact tracing accuracy expected with 5G New Radio (5G NR) compared to absolute positioning via device-to-device communication;
- the exploration of how to leverage 5G system for

determining contextual data and to take advantage of other common technologies in mobile devices for contact tracing;

- the challenges to leverage measurements from other technologies that are present in mobile devices (e.g., WiFi) for 5G positioning and contact tracing.

A. Contact tracing in cellular networks

Positioning in 3GPP has received attention since one decade ago with Release 9. Until Release 15, the main focus has been on location services for emergency services and lawful intercept. More recently, Release 16 and 17 include solutions to fulfill the positioning requirements of new location-based services in sectors such as industry, eHealth, and intelligent transportation systems.

Cellular networks perform estimates of the absolute location $\hat{\mathbf{p}}$ of the mobile client. Considering two mobiles, contact tracing through cellular networks requires the estimation of the Euclidean distance between pairwise positions. Because diseases like COVID-19 rely on droplets, the air can remain contaminated for a few minutes and objects for much longer. Therefore, a reliable contact tracing technique must consider both spatial and temporal dimensions.

More formally, let us consider a cellular provider collecting position traces $\hat{\mathbf{p}}_1(t)$ and $\hat{\mathbf{p}}_2(t)$ for two mobile devices. Differently from current BLE-based apps approaches, we advocate for soft decisions instead of hard decisions in the derivation of contact tracing. In fact, tracing contacts is *not* a simple binary decision between being or not in contact, and should rather be handled as a soft decision. The localization function responsible for deriving contact traces should determine a probability function that increases monotonically as the spatio-temporal distance $\|\hat{\mathbf{p}}_1(t)-\hat{\mathbf{p}}_2(t+\tau)\|$ between two users decreases. This function could leverage contextual information to strengthen the output function, a factor that is ignored by current app-based systems.

B. Accuracy with 5G NR

For estimating contact events, ALC tracing needs very accurate absolute position estimates. State-of-the art 3GPP positioning is achieved using observed time difference of arrival (OTDOA). With this method, the mobile device measures the received signal time difference using positioning and/or cell-specific reference signals sent from multiple base stations, called eNodeB (eNB) in LTE and gNodeB (gNB) in 5G NR.

We provide a high-level summary of the expected accuracy with time-based localization in Table I, based on frequency bands, maximum sub-carrier spacing, and FFT size of each technology. LTE is subjected to a ranging error of about 9.8 m. However, impairments such as multipath limit the practical positioning accuracy to about 20 m accuracy for 80% of the indoor mobile users [4]. Solutions based on 5G NR provide higher localization accuracy than LTE, resulting in ranging error of 2.44 m at frequencies below 6 GHz, and 0.61 m at mmWave frequencies. A characterization of the impact that multipath and propagation blockage have on localization, especially at higher frequencies (mmWave), is still an ongoing process for some scenarios.

TABLE I: Time-based localization accuracy in cellular network (technology, frequency, accuracy, sub-carrier spacing).

Tech.	Fr. [GHz]	Acc. [m]	Sub-car. [kHz]	FFT size [bins]
4G LTE	≤ 6	9.8	15	2048
5G NR	≤ 6	2.44	60	2048
5G NR	> 6	0.61	120	4096

Together with time-based measurements, the advent of massive MIMO and beamforming capabilities in 5G enables angle-based localization. Indeed, a work item in Release 17 is currently specifying the localization methods based on uplink angle-of-arrival and downlink angle-of-departure. In this context, a soft-decision framework, e.g., based on soft information-based localization algorithms, could enable the efficient data fusion of different types of measurements (e.g., timing, angles) and context information [5] for high-accuracy location awareness.

C. Absolute location versus device-to-device

5G localization leverages cellular communication, which has to go through the full path of the network, instead of performing direct measurements between devices. The latter concept, called device-to-device (D2D) communication, has not taken off in 5G NR for several reasons, including business models, security and privacy. The only exception is the introduction of 5G NR sidelink transmissions in Release 16 for vehicle-to-everything (V2X) services. Additional work on 5G NR sidelink is expected in Release 17 for public safety applications (e.g., disaster relief), where emergency workers can benefit from D2D communications.

D2D measurements could be affected by distance manipulation attacks, as with any other technology (like BLE) relying on proximity measurements. Instead, ALC contact tracing is more robust against attacks to security that could amplify or reduce the estimated distance between mobiles. These attacks have the objective of increasing or decreasing the transmitted signal power and delaying or anticipating the response affecting the round-trip-time (RTT) measurements [6]. Furthermore, direct proximity measurements between mobile devices, as those performed by 5G NR sidelink and BLE, can only measure spatial distance, but have no knowledge that another user was in the area a few minutes before.

D. Map inference and Vital signals

We propose to use soft decisions instead of hard decision in the derivation of contact tracing. This probability can benefit from using:

- environment knowledge, such as being outdoor or indoor, environment size, detection of barriers (such as walls) between the two users;
- vital and contextual signals of each user such as running, coughing, breathing rate and so on.

Contextual data, such as a digital map, can allow the 3GPP location elements to estimate the presence of obstacles such as walls and objects between two mobile devices, and thus provide a more reliable estimate of contact events. Through a pervasive deployment, 5G has the opportunity to create unprecedented insights into building structure, and in particular on the presence of walls and objects between humans, starting from the body of work in the field [7], [8], [9].

Another important aspect for tracing contacts and disease spreading is the estimation of vital signals, such as how deeply humans breath. Prior work has shown that breathing and heart rates can be estimated through reflection from human body using WiFi channel state information (CSI) [10]. Vital sign monitoring can be applied to the contact tracing problem: it has been shown that deeper breathing can be associated with higher probabilities to spread infections such as COVID-19. So far, there has been little research on monitoring vital signal based on 5G waveforms. However, there is a huge potential, thanks to the large bandwidth, large number of antennas and pervasive deployment offered by 5G.

E. 5G RAT-independent positioning

For positioning, 3GPP standards leverage not only the cellular radio interface but also any other technologies available in the mobile device, called Radio Access Technology (RAT) independent infrastructure. In particular, 3GPP already supports RAT-independent measurements with WiFi (signal strength, AP identifiers, and RTT measurements), GNSS (position fix), and inertial sensors.

Integration in smartphones. The operative system (OS) in the mobile devices (e.g. from Apple and Google) may put interfaces such as Wi-Fi and Bluetooth in low consumption mode to save power. This can be detrimental for positioning, as the cellular modem interrogating the Wi-Fi/Bluetooth modules in the smartphone may receive positioning measurements with unacceptable latency, which would degrade the fusion process with RAT-independent measurements. Furthermore, Apple and Google have the monopoly on positioning and, as already stressed, have their own solutions for contact tracing. Therefore, they do not seem to have incentives to give access to such measurements for positioning.

Nevertheless, integration in the same processor is occurring at fast pace. Processors such as the new Snapdragon models from Qualcomm with 5G modem have already technologies such as GNSS and WiFi integrated. This could allow 5G to request access to RAT-independent data without involving the mobile OS. Yet, this is not the general trend, and there are different options for different manufacturers, such as external modules with GNSS-related commands, which are tunnelled via dedicated interfaces and modules that provide hybrid positioning technologies combining cellular and GNSS positioning methods. Furthermore, inertial sensors, although considered in 3GPP studies, are not integrated with the cellular modem yet.

IV. 5G AND BEYOND ARCHITECTURE AND CONTACT TRACING

This section describes a high-level architecture for contact tracing; in particular:

- it presents the 3GPP functions that can be utilized for deriving contact tracing;
- it identifies which functions, among the existing ones, could be extended to fully unleash the potential of 3GPP architecture for contact tracing.

For the study, we refer to the architecture shown in Fig. 3, which summarizes the key functional elements of 3GPP-based architecture that can be leveraged for contact tracing.

A. 3GPP functions for contact tracing

The aim of this section is to show that past and current efforts in 3GPP standards set the ground for implementing contact tracing through the cellular network. In particular, 3GPP has defined:

- the enhanced LoCation Service (eLCS) architecture to support location services;
- the Network Data Analytics Function (NWDAF) to extract analytics.

eLCS architecture and contact tracing. There are two key elements in the eLCS architecture that can be leveraged for contact tracing, the Location Management Function (LMF) and the LCS client. The LMF interacts with the Access and Mobility Management Function (AMF), entry point in the control plane for gNBs, and responsible for handling connection and managing mobility. The LMF initiates the process of localizing the mobile. Positioning in the LMF exploits the densification of cellular networks, together with emerging technologies such as massive MIMO and mmWave for

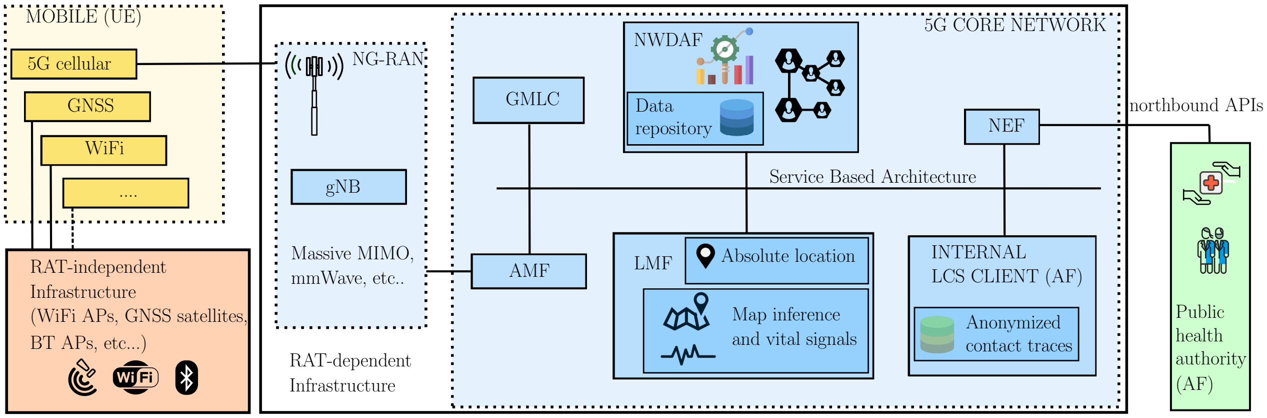
MOBILE (UE)
5G cellular
GNSS
WiFi
....
RAT-independent Infrastructure (WiFi APs, GNSS satellites, BT APs, etc...)
NG-RAN
gNB
Massive MIMO, mmWave, etc..
RAT-dependent Infrastructure
5G CORE NETWORK
GMLC
AMF
NWDAF
Data repository
NEF
northbound APIs
Service Based Architecture
LMF
Absolute location
Map inference and vital signals
INTERNAL LCS CLIENT (AF)
Anonymized contact traces
Public health authority (AF)

Fig. 3: 3GPP-based architecture can be leveraged for 5G and beyond contact tracing.

5G RAT-dependent positioning. Furthermore, measurements received by RAT-independent infrastructures such as WiFi, GNSS and inertial sensors can be accessed by the LMF for increased accuracy, latency, integrity, etc. All measurements are requested by the LMF using the 5G NR positioning protocol messages. The LMF then fuses all inputs and determines the location estimate for the target mobile using the selected technologies.

The LCS client is instead the entity that sends a request to the LCS server, called gateway mobile location center (GMLC) in the 3GPP architecture, in order to access location data of the mobile. The LCS client can be external to the 3GPP architecture or internal. The LCS client inside the network provider may have an internal anonymization layer applied to the location data before being shared outwards with any other client/service, and thus of interest for contact tracing. 5G has continued to extend the location functionalities. In 5G, location information can be also accessed by an internal or external Application Function (AF) (which provides application services to the subscriber), or to a Control Function (CF) internal to the network. These functions can be seen as LCS clients as well.

NWDAF and contact tracing. For the extraction of contact tracing analytics, statistical information related to past events and predictive information, we can rely on the NWDAF, a type of Network Function that can collect several types of data sets in a centralized manner. NWDAF can use the Unified Data Repository to store standardized 3GPP location information of the mobile devices, and the Unstructured Data Storage Function to support storage and retrieval of unstructured data, e.g., extracted contact tracing and group movements analytics (currently not defined by 3GPP). Location data analytics extracted by NWDAF can be provided to other Network Functions within the 5G Core, and the AF is an example of service consumer.

In order to better decouple location data from analytics, the best practices in cellular network providers for handling location data can be applied. In particular, the function responsible for requesting contact traces in the 5G Core may operate as internal LCS client or internal AF, and may perform an anonymization process before sharing contact tracing data with the authorized entities. The public health authority accessing anonymized contract traces data could instead operate as external AF using the CAPIF APIs. This interface includes common aspects applicable to any northbound APIs, to access data in a controlled and secure way through the Network Exposure Function (NEF), also masking sensitive network and user information.

B. *Specific extensions for contact tracing*

We envision that the dense deployment of gNodeBs can be also exploited to infer the knowledge of buildings structure and human behaviour through 5G waveforms. The exploitation of contextual information for contact tracing would require specific and punctual extensions to the 3GPP architecture.

First, the LMF could be enhanced to provide not only absolute location data but also map data and vital signals as inferred with 5G waveforms. As the role of LMF will become more complex, this function may be also be decoupled into two separate functions: the first one responsible for requesting location measurements and computing the mobile location, and the second one for inferring map data and vital signals. Second, the NWDAF could store not only location data, but also maps and vital signals in a data repository and can use this data set to perform contact tracing analytics.

V. PRIVACY IN CELLULAR NETWORK-ASSISTED CONTACT TRACING

This section discusses the key hurdles that a cellular-based contact tracing method must solve to become viable. We then propose potential solutions to each problem by leveraging the current 3GPP architecture, the best practices of network providers and ongoing research in the scientific community. Privacy concerns, and the relevant risks of transforming a contact tracing system into a global surveillance system, are often brought about as a main argument by detractors of cellular-based tracking systems. Privacy is a key requirement of any contact tracing system, and therefore must be handled with great care. Transmission of user data is not per se a privacy leakage. What is more important is that anonymous analytics running in the 5G network must guarantee that the identity of the user cannot be learned from the processed data.

Viability of privacy preserving technologies. Location privacy is definitely not a newly emerging issue in contact tracing. Approaches devised to enhance privacy in location services have been designed since the early stages of mobile networking and computing research [11]. The privacy community has contributed with diverse solutions, from very basic forms of pseudonymization, to more advanced technologies including cryptographic techniques, e.g. multiparty computation or homomorphic encryption techniques, location generalization/obfuscation, and differential privacy [12]. While early works, especially in the cryptographic community, could be considered unpractical, in the last decade a careful attention has been paid to the practicality and viability of the proposed solutions, with multiparty computation techniques scaling to millions of users [13] and used in the real world [14]. In terms of algorithmic solutions, federated learning approaches could be applied to improve data privacy, data security and data access rights, using not only the NWDAF in the Core Network but also the RAN Intelligent Controller defined by the Open RAN Alliance for performing embedded AI/ML intelligence in the RAN.

Organizational measures and GDPR. We argue that privacy enhancement technologies, albeit highly advisable, might not be strictly necessary, in front of the recent push of operators to enforce privacy via organizational measures. In particular, in Europe, since the introduction of the General Data Protection Regulation in May 2018 (GDPR), operators have taken significant measures to implement and apply data protection to any information concerning an identified or identifiable natural person. Even if GDPR, mainly for pragmatism and cost reasons, does not yet impose strict mandatory rules concerning pseudonymization but only aims at incentivize its application, operators already extensively employ separation of duties and strict access control means in their organization.

As an example of how operators might organize themselves for handling contact data, we can look at the best practice of network operators in 4G networks. Several operators already today are making use of location information for commercial purposes mainly in the transportation area, but have carefully organized the handling of location data and the delivery of such value added services via subsidiary units or even separated companies, thus enforcing a compelling separation of duties. Indeed, while the subsidiary companies are in charge of extracting and handling location information from the anonymized operator logs, the deanonymization information is kept by the operator, therefore yielding a final situation in which the operator knows the users identities but only the coarse location (cell identifier), while the opposite holds for the subsidiary company commercializing (aggregate, and further K-anonymized data with features that are in common to many users) [15]) user mobility patterns.

Leveraging 3GPP provisions on location data handling. In 4G networks, location data is not handled by the network provider apart from cell registration signalling information performed in the Mobility Management Entity in 4G (called AMF in 5G). 5G deployments are going to significantly change the landscape, as network providers will have access to accurate position data. However, there is reason to believe that the principles behind the consolidated successful business model of 4G applied to coarse location data of users could be implemented in the more compelling case of 5G localization. For instance, the subsidiary unit mentioned above could be in charge of handling the anonymized traces in order to detect contact events.

New means to guarantee privacy will be incorporated as well. From Release 16, 3GPP requires that the user can choose and change her location privacy settings for commercial use cases. Contact tracing is not a commercial use case, but it still requires to share data with more (authorized) entities than what was necessary until Release 15 with emergency services. In particular, it must be made available to public health authority, via a simple and secure interface, in order to trace back the contacts of the person tested positive. In this regard, negative examples are not due to implementation of 3GPP privacy provisions but to how contact tracing data is handled and managed (as data directly accessed by the national security agency[1]). For the process occurring after a person has been detected positive, 3GPP can leverage the standardized procedures for location services to address the target mobile using a pseudonym of the identifier through encryption.

[1] https://techcrunch.com/2020/03/18/israel-passes-emergency-law-to-use-mobile-data-for-covid-19-contact-tracing/

End users perception. Users are often willing to install apps that require access to personal data, but privacy leakage caused on purpose (through explicit request) or not (IP address, implementation bugs, etc.) is a critical problem. Privacy in cellular networks requires that the perception of privacy threat of users is correctly addressed by communication campaigns.

VI. Conclusions

Tracing people contacts and obtaining location-based analytics while preserving privacy is an important tool to control pandemics. Several countries adopted solutions based on short-range technologies and dedicated proximity-based apps. However, after several months of real world testing, the effectiveness of such approaches appears questionable, with emerging concerns in terms of deployment, security, reliability, and data governance.

This paper has presented how cellular networks can be exploited for contact tracing, especially considering that 5G and beyond promise to support accurate location awareness. Albeit still necessarily qualitative (experimentation could be performed in partnership with different stakeholders including Telecom providers), our analysis has highlighted the winning assets of cellular networks: massive deployment, largely scrutinized security, years of experience by operators in governing sensible users' data, and the ever increasing support for efficient localization facilities which are characterizing the evolution of the 3GPP standards — with localization services becoming a first class citizen in the incoming 5G releases. Starting from experiments based on the current network, we foresee that contact tracing can be a significant use case for future releases in the 3GPP standarization process.

References

[1] D. J. Leith and S. Farrell, "Coronavirus contact tracing: Evaluating the potential of using bluetooth received signal strength for proximity detection," *SIGCOMM Comput. Commun. Rev.*, vol. 50, no. 4, p. 66–74, Oct. 2020.

[2] ——, "Measurement-based evaluation of google/apple exposure notification api for proximity detection in a light-rail tram," *PLOS ONE*, vol. 15, no. 9, pp. 1–16, 09 2020.

[3] ——, "Contact tracing app privacy: What data is shared by europe's GAEN contact tracing apps," in *IEEE Conference on Computer Communications, INFOCOM 2021*. IEEE, 2021.

[4] H. Ryden, S. M. Razavi, F. Gunnarsson, and I. Olofsson, "Cellular network positioning performance improvements by richer device reporting," in *2018 IEEE 87th Vehicular Technology Conference (VTC Spring)*, 2018, pp. 1–5.

[5] A. Conti, S. Mazuelas, S. Bartoletti, W. C. Lindsey, and M. Z. Win, "Soft information for localization-of-things," *Proc. IEEE*, vol. 107, no. 11, pp. 2240–2264, Nov. 2019.

[6] A. Ranganathan and S. Capkun, "Are we really close? Verifying proximity in wireless systems," *IEEE Security Privacy*, vol. 15, no. 3, pp. 52–58, 2017.

[7] J. G. P. Rodrigues and A. Aguiar, "Extracting 3D maps from crowdsourced GNSS skyview data," in *The 25th Annual International Conference on Mobile Computing and Networking*, ser. ACM MobiCom '19, New York, NY, USA, 2019.

[8] S. Bartoletti, A. Conti, and M. Z. Win, "Device-free counting via wideband signals," *IEEE J. Sel. Areas Commun.*, vol. 35, no. 5, pp. 1163–1174, May 2017.

[9] Y. Xie, J. Xiong, M. Li, and K. Jamieson, "MD-track: Leveraging multi-dimensionality for passive indoor Wi-Fi tracking," in *The 25th Annual International Conference on Mobile Computing and Networking*, ser. ACM MobiCom '19, 2019.

[10] F. Adib, H. Mao, Z. Kabelac, D. Katabi, and R. C. Miller, "Smart homes that monitor breathing and heart rate," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, ser. ACM CHI '15, New York, NY, USA, 2015, p. 837–846.

[11] M. J. Beller, L. . Chang, and Y. Yacobi, "Privacy and authentication on a portable communications system," in *IEEE Global Telecommunications Conference GLOBECOM '91*, 1991, pp. 1922–1927 vol.3.

[12] A. Gkoulalas-Divanis and C. Bettini, Eds., *Handbook of Mobile Data Privacy*. Springer, 2018.

[13] M. Burkhart, M. Strasser, D. Many, and X. Dimitropoulos, "SEPIA: Privacy-preserving aggregation of multi-domain network events and statistics," *Proceedings of USENIX Security Symposium*, vol. 1, 10 2010.

[14] D. Archer, D. Bogdanov, Y. Lindell, L. Kamm, K. Nielsen, J. Pagter, N. Smart, and R. Wright, "From keys to databases—real-world applications of secure multi-party computation," *Computer Journal*, vol. 61, pp. 1749–1771, 12 2018.

[15] A. Machanavajjhala, D. Kifer, J. Gehrke, and M. Venkitasubramaniam, "L-diversity: Privacy beyond k-anonymity," *ACM Trans. Knowl. Discov. Data*, vol. 1, no. 1, p. 3–es, Mar. 2007.

Domenico Giustiniano is Research Associate Professor at IMDEA Networks Institute, Madrid, Spain. His research interests are in wireless systems, including LiFi, spectrum sensing and 5G localization. e-mail: domenico.giustiniano@imdea.org.

Giuseppe Bianchi is Professor at the University of Roma Tor Vergata, Italy, and CNIT affiliate. His research activity includes wireless networks, programmable network systems, privacy and security, traffic modelling and control. e-mail: giuseppe.bianchi@uniroma2.it.

Andrea Conti is a Professor at the University of Ferrara, Italy, and a CNIT affiliate. His research interests include localization and tracking, wireless communications, and quantum information science. e-mail: a.conti@ieee.org.

Stefania Bartoletti is Researcher at the National Research Council of Italy (IEIIT-CNR) and CNIT, working on location-aware wireless networks. e-mail: stefania.bartoletti@cnr.it.

Nicola Blefari Melazzi is Professor of telecommunications with the University of Roma Tor Vergata and is currently the Director of CNIT, a non-profit Consortium among 38 Italian Universities. e-mail: blefari@uniroma2.it.