On One D2D Usage Model for 5G Networks

Dmitry Namiot
Lomonosov Moscow State University
Moscow, Russia
dnamiot@gmail.com

Manfred Sneps-Sneppe
Ventspils University of Applied Sciences
Ventspils, Latvia
manfreds.sneps@gmail.com

Abstract—**This article discusses a new model for using D2D interaction and proximity services (ProSe). This model allows telecommunications operators to offer their customers a micro-positioning system that will allow users (customers) of the service to offer information services (information services) to mobile subscribers who find themselves in a certain specified area. Applications of this kind of services include retail, office centers, campuses, and transport infrastructure systems. These sorts of systems will allow telecommunications operators to compete in providing these sorts of solutions with systems using wireless network approaches in the unlicensed spectrum. This work examines the software component of such a service. The proposed approach focuses on security.**

I. INTRODUCTION

The practical implementation of 5G networks has already begun. And at the same time, discussions about what can be the main application (killer application) for 5G networks have not gone anywhere [1], [2]. Obviously, most of the work on 5G networks focuses on the radio component of these networks. There are really few works devoted to the applied aspects of creating services. At the same time, it is obvious that an increase in the data transfer rate in itself is not some kind of explanatory characteristic.

It turns out that there are not so many examples of the real use of the benefits of 5G today. For example, the so-called tactile Internet can be attributed to one of them. The Tactile Internet was defined by the International Telecommunication Union (ITU) in August 2014. ITU described it as an Internet network with low latency and extremely short transit times. Its deployment should provide high availability and reliability, as well as support high-security standards. This technology is based on the use of a distributed cloud computing system, where cloud environments are close to the place of their use (Mobile Edge-Cloud), as well as virtual or augmented reality for touch and tactile control [3]. It is expected (confirmed in experiments) that this adds a new dimension to the human-machine interaction - Fig. 1.

At the same time, the low latency will be sufficient to create interactive systems operating in real time. In general, the direction of augmented reality looks to benefit from 5G due to the need to transfer large amounts of video data with low latency [4].

It should be noted that the 5G ideology itself does not imply any software frameworks (software models) specific to this technology. Accordingly, the use of 5G in services should exploit some of the capabilities of this network, which is important for this particular service. In this example with augmented reality, the main point is low latency, which allows simulating tactile sensations (with a small delay, transmit a signal to a sensor (actuator), which simulates tactile sensations on the receiving side).

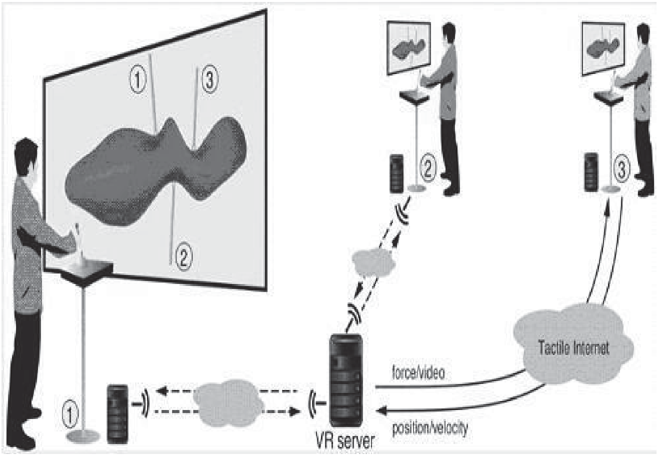

Fig. 1. Tactile Internet - version of ITU [5]

In this article, we consider one of the new additions (innovations, specific features) of the 5G model - a system of direct interaction between devices (D2D – device to device). As it will be shown below, the main function - communication between devices is not used for security reasons. But on the other hand, an integral part of this functionality is used - the definition of closely located mobile devices.

We can note several works that consider D2D from the point of view of communications in terms of M2M interaction. In particular, the paper [18] discusses the interaction of robotic devices. But this is a typical example of a closed system. We, first of all, focus on public services. And in them, direct interaction with another device will always be problematic from a security point of view. And D2L doesn't add anything new here. Direct communication with an unknown device is always a security issue.

The remainder of the article is structured as follows. Section II deals with the D2D model itself and its capabilities. Section III discusses the limitations of D2D. Section IV describes the proposed model for D2D deployment. And section V provides the conclusion.

II. ON THE D2D MODEL

The D2D model itself from a network point of view is described in sufficient detail, including in the works of the authors [6]. The story began when the 3GPP working group released in 2015 a specification (specifically version 12), among other functions of which the connection of an LTE device with another device (device to device or D2D) was added [7]. This specification introduced the term Proximity Service (ProSe). According to this specification, proximity services (telecoms often use the term services here) allow devices in close proximity to discover each other. Once discovered, these devices can communicate directly with each other. The goals for these direct communications are to reduce network load (so-called offloading), increased bandwidth. Also, direct communications can provide connectivity in areas without the network coverage. In other words, the main purpose of proximity services in the 3GPP specification was defined as the search (definition) of devices for direct interaction or use directly by the telecommunications provider to delegate (perform) its functions (so-called offloading, mobile data offloading [8]). This is illustrated in Fig. 2, which depicts the interaction model.

This figure shows the main parts of ProSe services and the interfaces between them. The components include two mobile devices (UEs) and applications on them (Prose App), PC1, PC2, PC3, PC4, PC5 are various radio-interfaces, the ProseApp is an application server. Also, this figure shows the radio access network (Evolved Universal Terrestrial Radio Access Network or E-UTRAN) and the Evolved Packet Core (EPC).

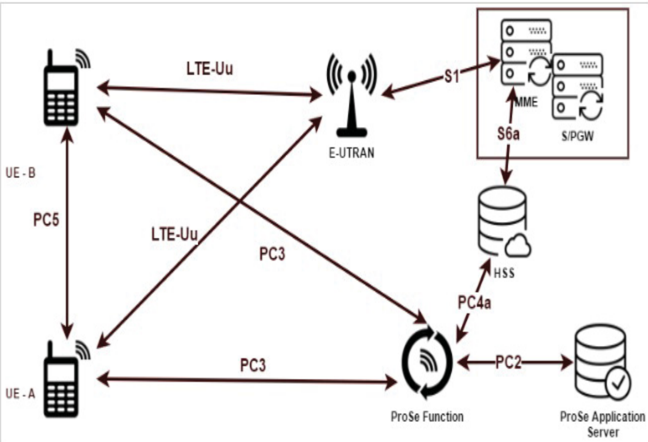

Fig. 2. ProSe functional [9,10].

The specification (in its various implementations) introduces the following concepts.

ProSe Application ID: ProSe application ID used to open proximity services (ProSe), identify information for ProSe enabled applications

ProSe Application Code: this temporary disposable code associated with the ProSe Application ID and used in the ProSe discovery process (search for services)

ProSe Restricted Code: it is similar to the above-mentioned code but makes information about a service (data) available only to a limited group of users. The feature supports the search for services nearby with the imposed restrictions, when only a certain selected group of mobile devices (users) should have access to data.

Discovery Filter: it is a combination of ProSe *Application Code* or *ProSe Restricted Code* and some search mask (pattern) to track the receipt of data on a given condition. The mask here is some analogue of a Regular Expression.

ProSe Function: this element is responsible for providing devices (UE) with access to ProSe services, as well as supporting work with *ProSe Application ID* and *ProSe Application Code*. The specification describes this as a logical function. Technically, this is some web server because ProSe function handles incoming HTTP requests from its users.

ProSe Application Server stores all the information about metadata: functions, users, etc.

ProSe combines the following processes:

- ProSe Direct Discovery. This process defines how a device (UE in Fig.2) discovers and identifies other (s) nearby devices
- ProSe Direct Communication. This process uses LTE resources from the cellular network for messaging.

ProSe Discovery could be performed at the network level (EPC level ProSe Discovery) and at the wireless network level (WLAN).

As part of Direct Discovery, the device sends out ProSe Application Code, received from the network. Other devices in the vicinity can receive this code and the fact of receiving such identification information is a confirmation that the sender and the recipient are in the proximity.

The specification defines two possible modes for ProSe Direct Discovery to operate. The mode determines who can detect the proximity of a particular device. The mode is determined for the device sending *ProSe Application Code*. In the case of an open mode, broadcasted *ProSe Application Code* can be received by any other device. Or, in other words, any device can determine its proximity to the sender. In the case of a limited mode, the broadcaster will limit which devices can receive its broadcast. Or, in other words, only a limited set of devices can determine proximity to the sender. It can also be noted that limited mode requires support for the PC3 interface in Fig. 2 and will not work without the network coverage.

The simplified model (algorithm) of the entire system is focused on building communication between closely spaced devices through PC5 (sidelink) (Fig. 3)

D2D is envisioned to become the backbone of many services based on “local” (at the current location) service delivery. According to this model, two mobile devices will interact directly, but under the control of the telecom operator. It should be noted that the operating model and any description of the programming interfaces are not yet available (even in subsequent specifications).

A typical telecommunications-related paper considering D2D ends up at this point. After solving the problem of efficient (primarily in terms of energy) search for closely located devices, all papers usually followed by words that now such devices can connect to each other and transmit data. Services are not specified in any way. In practice, all papers are talking almost everywhere about the high speed of data transfer between devices and, accordingly, about the organization of the connection between devices.

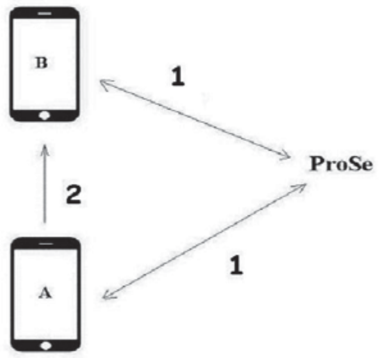

Fig. 3. D2D model.

In this model:

1 - signal channels

2 - communication channel without using base stations (sidelink).

We have two comments about this position. First, since we are writing about services (the last layers of the ISO Standard Model), this is where it starts. And here we must conclude that there are no services for D2D yet, since data transmission sounds too abstract. And the second note is that there are currently no direct connections between devices in public services for security reasons. And security concerns won't go away with increased network speeds. So, in our opinion, services (services) based on direct connections have obvious limitations. We will discuss this in Section III.

III. ON D2D LIMITATION

The description of the use of 5G D2D at the present also does not go beyond, relatively speaking, popular science frameworks. It is expected that there will be a paradigm shift from centralized connections to direct connections between users. Here is a direct quote from [11]: "with the widespread adoption of D2D interoperability, we expect user devices to become more involved in 5G service delivery and, in some cases, even take on some of the roles of the operational network infrastructure. In particular, they can help provide wireless connectivity, such as offering D2D-based data relaying, contactless gaming, content distribution, caching, and other forms of cooperative communication". This is illustrated in Fig. 4.

It should be noted that programming issues are traditionally not considered in the literature, affecting only network aspects. The higher levels of the OSI model are left without consideration. Concerning D2D, there are proposals for the implementation of web interfaces for working with PC5 (see Fig. 1) [12]. But in this case, considering service architectures, we would like to focus on the following aspect. All direct connections (for example, shown in Figure 4) assume, by definition, a connection from a user device to another device on the network. The fact that this other device is authorized (present) in the operator's network does not fundamentally change anything. There is always a connection with an unknown device and downloading content from this unknown device. And this fact is one of the biggest security concerns.

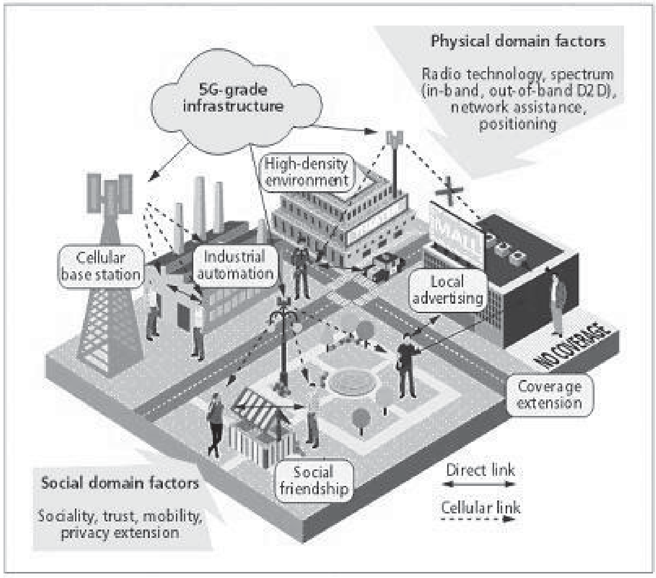

Fig. 4. Network-assisted D2D [11]

You can recall examples of using direct connections, which were abandoned (at least, mass use was stopped) precisely because of security problems. For example, downloading Flash in web pages, for Android devices, is downloading applications from arbitrary sources (by default, this is disabled in the OS). An earlier example is Bluetooth marketing, where it was suggested to download content from arbitrary advertising nodes. The encryption functions and authorization of network nodes do not fundamentally change anything - the content will be downloaded from an unknown for the downloading node, which it does not control and cannot check in any way.

In fact, to date, there is only one working example of downloading content from unknown devices - this is downloading HTML (in fact, text, which is safe) from some site (which should also be treated as an unknown device).

In our opinion, D2D will work (could be used) in some limited cases only. These include:

- Various kinds of VPN solutions. All devices will "trust" each other. The loss of data for a specific device on such a network is simply a network failure, and the corresponding services will be engaged in recovery. Private data does not exist in such a system.
- A service that "internally" uses direct data transmission. These implementation details are hidden from users of the service, it is enough that users trust the service itself. An existing example is Skype and its P2P connections. We also note that security problems in such services begin precisely from the P2P part (and the same Skype is an example of this).

- The most realistic approach is offloading. The telecommunications operator performs part of its services using D2D. The user trusts the operator, the way of providing services is hidden from the user.

Otherwise, it is difficult to imagine that in public services, users agree to download content from unknown devices. Or imagine that it will remain without consequences. An example (or anti-example) is the Bluetooth Mash specification [13]. It transfers data between network nodes without establishing a connection. The reason is exactly the same - in a mesh network, the nodes are unknown.

We propose to take only one phase from the D2D model for public services - DD (Device Discovery). Receipt of the above-mentioned *ProSe Application Code* by any of the mobile devices will mean that the recipient is nearby (according to the specification it is 90-500 m) from the sender. This may, in our opinion, serve as the basis for public services. The sending device identifies some place (geographically). Fixing proximity to this location is a process that replaces location determination for the recipient. Instead of calculating the coordinates of the receiver and determining the distance to a given location, we can directly get an estimate of that distance (close or not). Why might this be necessary? There are at least several reasons to note here:

- Calculating geo-coordinates can be difficult. For example, when working indoors
- The concept of “place” can be dynamic. “Place” can be moved. For example, it can be a car, a train car, etc.
- Privacy: in the specified model, the recipient of the *ProSe Application Code* should not share their location, as in classic geo-services. The recipient plays a passive role in this model. Accordingly, it is impossible to identify those who receive information about intimacy.

In general, proximity information should be considered part of the context. Context, in the modern interpretation, is arbitrary, in one way or another measurable characteristics that can be added to a location. These characteristics include, for example, physical information about the environment, which, usually, is presented in the form of data from various sensors (sound, vibration, etc.), social characteristics (for example, belonging to a social network) [14].

Formally, the context can be defined as a triplet

$<R, A, P>$, where R - a set of resources, A - a set of actions (shares), P - policies (restrictions)

Naturally, the context is always considered in some limited areas. Most often, this is a certain area near the point of the request (view) of the data.

The context can also include information about available wireless nodes. This was used, for example, in [14], [15]. Highlights of this approach are:

- The limited coverage area of wireless networks serves as a proximity metric. In other words, signal availability (visibility / reachability of a wireless node) automatically means being close to that node.
- Wireless networks are widely represented in technical systems (for example, Bluetooth in technical devices, Wi-Fi networks at train stations, etc.)
- Since we are not talking about organizing connections, but only about fixing the presence of a node, then such nodes can be created specifically to determine the context (fixing proximity). In particular, they can be created on the mobile devices of the participants in the process.

Actually, the use of wireless network nodes (Bluetooth Low Energy, Wi-Fi) is a similar model. For example, Bluetooth Low Energy (BLE) -based tags are an established way of determining proximity. There are several standards for using advertising mechanisms for wireless nodes in BLE - Apple iBeacon, Google EddyStone [16], etc. These tags are used, among other things, to determine proximity, without referring to geo-coordinates. The availability of the tag signal (tag identification) is the fixation of the fact of proximity. This information is available for use from mobile devices (phones) that support BLE. As shown in our works (for example, [17]) this approach can be used for any wireless networks. In all cases, the fact of determining proximity will be the receipt of some identification information from the reference node (the node, the proximity to which is determined). Such information can be an advertising package in BLE, SSID in the case of Wi-Fi, etc. ProSe Application Code, as worded like this, is just another form of identification. The difference lies in the nature of its distribution. BLE tags, for example, independently manage advertising mailings, and in the case of D2D, everything happens under the control of the operator.

As in the case of wireless nodes, the obtained identification information (ProSe Application Code) can be used as a key to retrieve data from some storage (database). Accordingly, this approach can also be presented as an analogue of a QR code, when, instead of a visual representation, there is a set of identifiers of network nodes. A big plus, of course, is the fact that scanning of such a non-visual QR code can be carried out automatically, without any requirements for performing special actions by the user (aiming the camera, etc.). The absence of requirements for “manual” user work allows, obviously, to use this approach in M2M applications. No user interface is needed here and these kinds of “codes” can be scanned automatically.

Another advantage of this approach is that the “codes” depend on the availability of wireless nodes and their identification. Both of these characteristics are dynamic. Accordingly, the presented data will also be dynamic. This is especially important for transport systems. If wireless nodes are associated with vehicles (wagons, cars, etc.), then the data associated with vehicles will “move” with them also.

IV. D2D-BASED SERVICE FOR OPERATORS

The idea of the service is that the telecommunications operator can provide the customer with the service of building a micro-positioning system. Suppose there is some retailer that provides a mobile application to its users (visitors). This is a very typical picture today. The application helps users navigate the store (mall), shows special offers, supports a loyalty program, etc.

There are several options to distinguish where the customer is located in such an application. First, it is possible to request a location using GPS and its add-ons such as AGPS. Indoors this can be very inaccurate. You can build your own positioning system using wireless networks. This is a rather expensive process, since such a system must be maintained by constantly updating the so-called radio maps. Finally, it is possible to use proximity based systems by placing Bluetooth tags. Conceptually, this is the same as RFID tags, for example, but RFID is practically not present in modern mobile phones, and the same BLE is in all modern smartphones. The application on the user's phone can determine the visible tags and, depending on this, make an assumption about the location of the visitor (hence, about special offers available in this place, etc.). The tagging system also needs maintenance, of course. The signal distribution area for tags is small, so their number is usually very large. It can take quite a lot of work to support the new system configuration (new areas).

This is where the new model appears. The telecommunications operator provides a set of *ProSe Application Code* that will be sent from mobile devices (phones or other devices with an operator's SIM card). The retailer (customer of the service), at its discretion, places devices at its locations, and its application for its own customers determines the positions of the latter according to the adopted *ProSe Application Code*. Key points to note:

- Neither the operator nor the customer of the service knows the location of the end-users
- The customer of the service can arbitrarily move the basic mobile devices. For example, they can be placed on moving objects (cars, trains, etc.), and then a significant event is, for example, a car entering a warehouse, a train arriving at a station, etc.

Such a service will allow the service's customers to create virtual geo-perimeters at their sites. Applications on mobile devices of users will be able to respond to the crossing of such virtual perimeters (the beginning and end of receiving codes from reference devices). This is illustrated in Fig. 5.

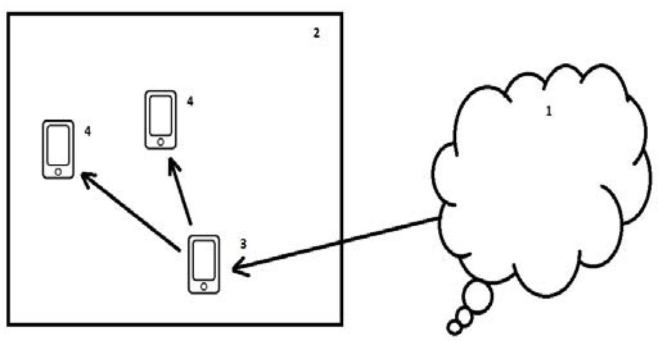

Fig. 5. Service of virtual perimeters

In this figure:

1 - telecom

2 - the site of the customer of the service

3 - supporting device

4 - mobile devices of customers. They can check the fact of being in the vicinity of the support device

This solution allows the customer (retailer, in this example) to outsource all micro-positioning work to the operator. If the receipt of a specific *ProSe Application Code* is associated with the receipt of any information, then such associations <*ProSe Application Code, associated data*> can also be stored on the operator's side. In fact, it will be some kind of database with the <*key, value*> model. The telecommunications operator will act as a provider of proximity services. For a potential customer, such a configuration will mean the ability to define micro-locations in an arbitrary room (place) without any programming. You just need to order *ProSe Application Code* (Codes) and fill in the associated data.

The operating model is depicted in Fig. 6. The code that is sent out to determine proximity (1 in Fig. 6) is, at the same time, the key in the database to retrieve the content (2 in Fig. 6). Replaceable (updatable) codes are modeled by setting the lifetime for records in the database.

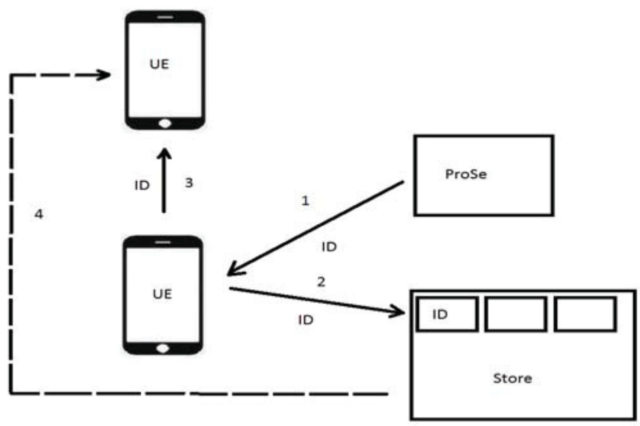

Fig 6. On the operational model

There are no connections between devices in this scheme. The device, having received a code for determining (confirming) proximity, can use this code to request content related to the fact of proximity to the sender (4 in Figure. 6). The sending device, actually, acts as a tag. And it's a movable tag that can be placed anywhere.

In the work [12], a schema (model) of content presentation for such an architecture was also proposed. It was suggested to choose Hypercat as the data presentation format. Hypercat [19] is an open source system that British Telecom is positioning as a search engine for the Internet of Things. Conceptually, it can be thought of as annotated web links. This allows arbitrary content, including datasets, to be presented for services based on spatial proximity. For example, content that describes a link to some corporate site might look like this (it is a plain JSON text):

```
{
  "item-metadata": [
   {"rel":"urn:X-tsbiot:rels:isContentType",
"val":"application/vnd.tsbiot.catalogue+json"},
  {"rel":"urn:X-tsbiot:rels:hasDescription:en",
"val":"Some corporation "},
  {"rel":"urn:X-tsbiot:rels:supportsSearch","val":"urn:X-tsbiot:search:simple"} ],
  "items": [{
     "href":"https://some-site.com /",
     "i-object-metadata": [{
     "rel":"urn:X-tsbiot:rels:phone",
"val”:”+7 495 XXX-XX-XX"},
   {"rel":"urn:X-tsbiot:rels:email",
"val":"info@some-site.com "}]
}]}
```


Note also that such a scheme allows very flexible billing solutions from the operator's side. The cost of the service can be determined by the number of allocated *ProSe Application Code*, the volume of their distribution, the time of distribution. If the operator also maintains a database for network proximity, then data on the actual use of the data is added here.

VII. Conclusion

In this paper, we have described a new D2D 5G usage model. The proposed scheme allows telecom operators to provide their users with new opportunities for creating services using location information. Within the framework of this model, customers of the service (service) get the opportunity to provide mobile subscribers with customized information tied to the elements of micro-positioning, which are provided by the telecom operator based on D2D. It can be seen that only one phase from D2D process is used in such a model - direct discovery (DD).

The proposed scheme expands network proximity models based on BLE tags or similar devices, providing centralized control of positioning elements, greater reliability, scalability, flexible system reconfiguration, as well as increased coverage. From the standpoint of the implementation of systems using positioning information, the proposed model differs in that it does not require users to share information about their own location in any form. This requirement is the main problem with data security in geo-information systems. In the proposed model, users independently determine their relative position, and in this regard, the scheme is completely safe from the point of view of working with data. In general, the proposed model expands the capabilities of context-sensitive programming for mobile applications.

Acknowledgment

We would like to thank the reviewers for the early versions of this article for criticism and comments that have contributed to the improvement of this work.

References

[1] Albreem, Mahmoud AM. "5G wireless communication systems: Vision and challenges." 2015 International Conference on Computer, Communications, and Control Technology (I4CT). IEEE, 2015.

[2] Cheng, Jiangfeng, et al. "Industrial IoT in 5G environment towards smart manufacturing." Journal of Industrial Information Integration 10 (2018): 10-19.

[3] Simsek, Meryem, et al. "5G-enabled tactile internet." IEEE Journal on Selected Areas in Communications 34.3 (2016): 460-473.

[4] Zhuang, Yufeng, et al. "Using 5G Mobile to Enable the Growing Slate of VR and AR Applications." Augmented Reality and Virtual Reality. Springer, Cham, 2020. 185-194.

[5] The Tactile Internet ITU-T Technology Watch Report https://www.itu.int/dms_pub/itu-t/opb/gen/T-GEN-TWATCH-2014-1-PDF-E.pdf Retrieved: Oct, 2020

[6] Namiot, Dmitry, and Manfred Sneps-Sneppe. "On Proximity Application Server." 2020 26th Conference of Open Innovations Association (FRUCT). IEEE, 2020.

[7] Zou, Kingsley J., et al. "Proximity discovery for device-to-device communications over a cellular network." IEEE Communications Magazine 52.6 (2014): 98-107.

[8] Rebecchi, Filippo, et al. "Data offloading techniques in cellular networks: A survey." IEEE Communications Surveys & Tutorials 17.2 (2014): 580-603.

[9] 3GPP TS 24.334 V12.1.1, December 2014; Technical Specification Group Core Network and Terminals, Proximity-services (ProSe) User Equipment (UE) to ProSe function protocols; Stage 3; Release 12.

[10] LTE Direct http://www.3glteinfo.com/lte-direct/ Retrieved: Oct, 2020

[11] Ometov, Aleksandr, et al. "Toward trusted, social-aware D2D connectivity: bridging across the technology and sociality realms." IEEE Wireless Communications 23.4 (2016): 103-111.

[12] Namiot, Dmitry. "3GPP D2D Specification and Public Services." International Journal of Open Information Technologies 8.2 (2020): 39-46.

[13] Baert, Mathias, et al. "The Bluetooth mesh standard: An overview and experimental evaluation." Sensors 18.8 (2018): 2409.

[14] Sneps-Sneppe, Manfred, and Dmitry Namiot. "On physical web models." 2016 International Siberian Conference on Control and Communications (SIBCON). IEEE, 2016.

[15] Sneps-Sneppe, Manfred, and Dmitry Namiot. "About M2M standards and their possible extensions." 2012 2nd Baltic Congress on Future Internet Communications. IEEE, 2012.

[16] Newman, Nic. "Apple iBeacon technology briefing." Journal of Direct, Data and Digital Marketing Practice 15.3 (2014): 222-225.

[17] Namiot, Dmitry, and Manfred Sneps-Sneppe. "On proximity-based information delivery." *International Conference on Distributed Computer and Communication Networks*. Springer, Cham, 2018.

[18] Alsamhi, S.H., Ma, O. & Ansari, M.S. Survey on artificial intelligence based techniques for emerging robotic communication. Telecommun Syst 72, 483–503 (2019). https://doi.org/10.1007/s11235-019-00561-z.

[19] Namiot, Dmitry, and Manfred Sneps-Sneppe. "On Search Services for Internet of Things." *International Conference on Distributed Computer and Communication Networks*. Springer, Cham, 2017.