Available online at www.ijournalse.org

**Emerging Science Journal**

(ISSN: 2610-9182)

Vol. 5, No. 3, June, 2021

# A Comparative Study of Bluetooth SPP, PAN and GOEP for Efficient Exchange of Healthcare Data

Athanasios Kiourtis [1*], Argyro Mavrogiorgou [1], Dimosthenis Kyriazis [1]

[1] *Department of Digital Systems, University of Piraeus, Piraeus, 18534, Greece*

**Abstract**

*Objectives:* Current research aims to address the challenges of exchanging healthcare information, since when this information has to be shared, this happens by specifically designed medical applications or even by the patients themselves. Among the problems that the Health Information Exchange (HIE) initiative is facing are that (i) third party health data cannot be accessed without internet, (ii) there exist crucial delays in accessing citizens' data, (iii) the direct HIE can only happen among Healthcare Institutions. *Methods:* Towards the solution of these issues, a Device-to-Device (D2D) protocol has been specified, running on top of the Bluetooth protocol for efficient data exchange. This research is focused on this D2D protocol, by comparing the different Bluetooth profiles that can be used for transmitting this data, based on specific metrics considering the probabilities of transferring erroneous data. *Findings:* An evaluation of three Bluetooth profiles takes place, concluding that two of the three profiles must be used to respect the D2D protocol nature and be fully supported by the main market vendors' operating systems. *Novelty:* Based on this evaluation, the specified D2D protocol has been built on top of state-of-the-art short-range distance communication technologies, fully supporting the healthcare ecosystem towards the HIE paradigm.

**Keywords:**

Bluetooth Protocol;
Bluetooth Profiles;
SPP; PAN; GOEP;
Health Information Exchange.

**Article History:**

| | | | |
|---|---|---|---|
| **Received:** | 19 | February | 2021 |
| **Revised:** | 05 | May | 2021 |
| **Accepted:** | 11 | May | 2021 |
| **Published:** | 01 | June | 2021 |

## 1- Introduction

Current electronic healthcare research promises to solve the challenge of maintaining and facilitating the exchange, sharing and analysis of healthcare data. It is undeniable that collecting healthcare data generated across a variety of sources encourages efficient communication between healthcare practitioners and patients, whereas it increases the overall quality of patient care providing deeper insights into specific conditions [1]. Nevertheless, when this information must be shared between the aforementioned healthcare ecosystem entities, this happens by specifically designed medical applications, protocols or even by the patients themselves, who often bring their files from appointment to appointment. Currently, the European Commission is presenting the need for a highly-secure system which can aid citizens in having access to their electronic medical and non-medical files in all European Union's (EU) Member States by 2021 [2-4]. The overall goal deals with making easier European citizens' interaction and exchange of their healthcare data in any location across the EU, to have the ability to easily exchange it, to make better the overall monitoring and facilitate emergency care. This can also be described as the main objective of the current research. Regarding the EU Member States, in France, the Shared Medical Record [5] was officially launched in November 2018, as a health record in electronic form that manages health information through storage, centralization, and security techniques including data such as pathologies, consultation reports, examination results, etc.).

* **CONTACT**: Kiourtis@unipi.gr

**DOI:** http://dx.doi.org/10.28991/esj-2021-01276

Furthermore, the northern European countries (Finland, Sweden, Denmark, and Estonia) are among the first ones in the transformation of their administrations to a digital form [5]. Through services which can be found online, or the identity card which is connected everywhere, almost all the different citizen are able to use the Internet connection for procedures including cases of administration, as well as health services. In Denmark, the Medcom [6] initiative took place in 1994 as a network for health information in a national level, including a portal connected over the Internet for managing healthcare information among healthcare practitioners and citizens. Sweden included at national level a strategy towards electronic healthcare in 2006, namely the Swedish Medical Record (NPÖ). The Swedish Medical Record [7] gives authorization access to specific healthcare personnel, and consequently it can receive connections from any existing computer system. In Spain, it has been launched the Diraya program [8] having as a goal to ensure continuous healthcare of high value through the harmonization of the ingested data for being easily accessible to every stakeholder, including both citizens and healthcare personnel. It is undeniable that a system in the EU for exchanging healthcare data would provide many benefits since it would facilitate EU citizens to easily travel among the different countries without thinking the challenges of not having along with them their personalized medical prescriptions or treatments. Furthermore, in the case that an emergency occurs abroad, the citizen's medical records would be accessed in a faster and easier way. Hence, citizens would receive faster and more efficient treatment in a more secure manner, including also appropriate and personalized care. Nevertheless, this is not only the case for the EU Member States, since the need for exchanging health information among healthcare practitioners is rapidly growing along with multiple challenges and efforts at national and worldwide level, with the overall goal to improve the quality, safety, and efficiency of health care delivery [9, 10].

Among the various implementations and initiatives towards the Health Information Exchange (HIE) paradigm, some of them can lead to a time-consuming process which can result in inaccurate information, with increased inefficiencies, leading to care of low value. Additional issues are (i) that third party health data cannot be accessed without internet connection - which cannot be always available, (ii) that there exist crucial delays in accessing current citizens' data, while (iii) a major obstacle is that direct exchange of health information can only happen among Healthcare Institutions, without the active participation or involvement of the current data owners (i.e., citizens). Moreover, there exist several smart devices' applications that are offering the ability to exchange health information between citizens and healthcare practitioners, which are however using vendor-specific and non-interoperable protocols, without respecting any common data representation or terminology structures. Finally, the usage of multiple credentials to authenticate citizens and Healthcare Institutions - even in the same countries, could be also a major barrier towards this objective. Nevertheless, most of these research projects and initiatives are using different protocols, facilitating the process of long-range and short-range distance communication towards health data exchange.

In this paper, a newly specified protocol is being taken into consideration, the Device-to-device (D2D) Protocol [9], in the form of a secure communication protocol for exchanging messages and healthcare-related data between two nearby devices, adopting short range communication technologies, and in particular Bluetooth v4.0. Shortly, the D2D protocol is being specified as an open specification protocol that can give the ability to EU citizens to exchange health information stored in their smart devices, directly with Healthcare Institutions. This health information is structured in a common format with respect to the widely adopted Health Level Seven (HL7) Fast Healthcare Interoperability Resources (FHIR) standard [12], whereas the D2D protocol can check the conformance of the exchanged information based on specifically parameterized HL7 FHIR interoperability profiles. Furthermore, the D2D protocol provides a fully encrypted communication channel with easily usable symmetric key authentication, supporting data encryption and decryption mechanisms [13], without allowing any third-party access to this communication. Hence, taking into consideration the D2D protocol and its Bluetooth-based communication, three different Bluetooth profiles will be used and compared for securely exchanging health data between a citizen and a Healthcare Practitioner, to understand the Bluetooth profiles' nature and identify their strengths and potential cases of usage. It should be mentioned that these Bluetooth profiles form the definitions of possible applications that provide the specification of the overall behaviors that Bluetooth-enabled devices use for communication with other Bluetooth devices, in a specific application area.

The rest of the document is structured as follows. Section 2 presents the related work regarding techniques, implementations, and research projects supporting data and health data exchange, concluding to the needs for using the Bluetooth protocol for the cases of HIE. In Section 3, it is presented the evaluation scenario under which the overall comparison will take place, Section 4 involves the discussion of the derived results, while Section 5 concludes with our next steps.

## 2- Related Work

### *2-1- Information Exchange Techniques*

With regards to the research conducted using a mix of distance communication protocols for exchanging data of any type (i.e., not only health data), Mochel et al (2007) [14] present a Bluetooth scatternet protocol (SNP) that gives the ability to the user to have a serial link to all the connected members in a transparent wireless Bluetooth network. The

authors show how their software layer makes several tasks simpler, such as the synchronization of central pattern generator controllers for actuators, the collection of sensory data and the construction of modular robot structures. In Qiu et al. (2020) [15], the authors propose a method for securely storing and exchanging data that consists of a specific encryption algorithm along with fragmentation and dispersion for data safety and privacy protection, even when both transmission media and keys are compromised. Furthermore, Chong et al. (2017) [16] describe a system consisting of an "image beacon" with the ability of broadcasting color images over a very long period using a set of devices with Bluetooth Low Energy (BLE) technology. To this end, Chung et al. (2015) [17] proposed an information exchange method among devices at short-range distances, through inaudible frequencies and Wi-Fi.

### *2-1-1- Long-range Distance Health Information Exchange Techniques*

Among the research projects which are using long-range distance wireless communication technologies to exchange health information, there exist several solutions. The Direct Secure Messaging [18] is a digital messaging tool which is used in healthcare for such communication and can be used with multiple interfaces such as an email client, or healthcare Information Technology (IT) portals. Carequality [19] provides a national-level framework of interoperability to facilitate information exchange among specifically designed networks. Through using cloud fax [20], documents and reports in digital format can be stored into folders and arranged in such a way, without the need of any physical paper. KONFIDO [21] is a research project with the goal to construct a way for cross-border health information exchange in the most secure manner, being built on top of existing and continuously evolving EU frameworks, (OpenNCP, epSOS, eIDAS). Another research is from Gavrilov et al. (2018) [22] where the authors propose a model for an Electronic Health Record (EHR) for Health Data Exchange based on a SaaS (Software as a service) service model developed on top of cloud computing technology. Furthermore, in Masud et al. (2018) [23] it was implemented an anonymous, query-based, on the fly secure data exchange protocol between two clouds for collaborative cloud-based healthcare environments.

### *2-1-2- Short-range Distance Health Information Exchange Techniques*

As for the research projects aiming in short-range distance communication protocols for exchanging healthcare data, in Basjaruddin et al. (2017) [24], it was developed a medical record system based on Near Field Communication (NFC). The authors developed an electronic medical record (EMR) application where it is used by healthcare practitioners and patients. The patients use the application only for reading the content while the healthcare practitioners can view and change the EMR content, even add a new patient EMR. De Almeida et al. (2020) [25] performed a research in Wi-Fi Direct in which WPA2 devices, such as smartphones, laptops etc. can establish a direct Wi-Fi connection without using a wireless access point for exchanging health data. In the same context, Fuliang et al. (2020) [26] also did a research in Wi-Fi Direct and they proposed a real-time data transmission system by using Wi-Fi Direct for the transfer of healthcare data. The results of the research showed that the healthcare data are transported with greater reliability through Wi-Fi Direct than through Wi-Fi.

### *2-2- Bluetooth Protocol*

Based on the extensive list of methodologies that are using both short-range and long-range distance communication technologies, it becomes clear that several research tasks and methodologies are offering solutions to solve the challenge of exchanging healthcare information. These methodologies do not consider however challenges such as the fact that third party health data cannot be accessed without internet connection, that there exist crucial delays in accessing current citizens' data, or that there exist several smart devices' applications which are using vendor-specific and non-interoperable protocols to exchange data. In our work in [11], the D2D protocol has been specified, serving the purposes of exchanging healthcare information, providing an open specification protocol for transferring health information that is structured in a common format with respect to the widely adopted HL7 FHIR standard, providing a fully encrypted communication channel, and being functional even in cases where internet connection is not available. Among the different protocols and research projects, in [27] we have made a thorough research with regards to which protocol is most suitable for transferring health data, according to specific data transmission and security requirements, in short-range distances. Based on this research, we have concluded that the Bluetooth protocol is the most suitable candidate for such requirements, hence in the current paper this research is being expanded on identifying the most suitable Bluetooth profile to be used for such cases. In general, Bluetooth can be best described as a packet-based short-range wireless communication technology consisting of an architecture with both masters and slaves, where the involved devices can exchange roles using their applications, upon specific agreement. Prior to explaining and analyzing the Bluetooth profiles to be compared, there should be analyzed some Bluetooth-related terminologies [28], regarding the Bluetooth controller, Bluetooth Logical Link Control and Adaptation Protocol (L2CAP) and the Bluetooth profiles, which will be thoroughly used on the overall comparison.

### *2-2-1- Bluetooth Controller*

The Bluetooth controller consists of the baseband and the radio that is responsible for the link management functionality, to store data in specific packets, to decode and encode the channel, as well as to determine the frequency of operations.

*Channels*: A channel consists of a frequency with a pseudorandom nature with the ability of hopping sequence, slot timing, and an access code. In Bluetooth Channels, specific transports take place which can be either asynchronous (ACL) or synchronous (SCO). Moreover, the Logical links which are used on top of the transports create the connection between the master and the slave.

*Packets*: A Bluetooth packet consists of three parts: an access code, a payload, and a packet header, where additionally the payload has a specific payload header and a data unit at a higher layer. This payload header has specific information regarding the link control, as well as an error check. This standard defines several packet types, while data transmission is using different packet types. All the different kinds of transports use common packets, being usually called as control packets. In that case, the POLL packet is used by the master for polling the slaves, whereas the NULL packet is used for data packets acknowledgment.

*Automatic Repeat Request* (*ARQ)*: Bluetooth uses an ARQ for the retransmission of baseband packets that includes errors. It should be taken into consideration that ARQ tries packet transmission until it either succeeds or a timeout occurs, leading to the L2CAP packet flushing.

### *2-2-2- Bluetooth L2CAP*

The L2CAP defined a data link layer with the ability to provide connection-oriented, as well as connectionless services, to protocols and applications that can be found in upper layers. In L2CAP, the flush timeout describes the time needed to transmit a packet before it is dropped by the controller. Moreover, the retransmission timeout describes the total time needed in order for the L2CAP to wait for receiving an acknowledgement for an information frame before its retransmission. The mode of the L2CAP channel specifies its configuration, and the way it must behave, consisting of the (i) Basic mode without any support of retransmissions, and as a result it has low reliability, and the (ii) Streaming mode that is only used for data with isochronous nature.

### *2-3- Bluetooth Profiles*

In the case of Bluetooth, a device should understand specific Bluetooth profiles, in the form of definitions of specific applications which have a pre-defined nature that Bluetooth devices use to communicate with each other. In these profiles it can be found the settings to change and to manage the overall communication from the start. Through using a Bluetooth profile, it saves time for transmitting the parameters anew before the bi-directional link becomes effective. As a result, for two devices to communicate to complete a specific task, both devices must use a common profile. As depicted in Figure 1, there exist several Bluetooth Profiles, according to the task that must be performed and the domain in which they should be applied. These domains are categorized into five (5) main categories, with regards to the Medical domain (i.e., Medical Group) that deals with medical devices supporting Bluetooth connection, the Serial Port Profile domain (i.e., SPP Group) that consists of devices that emulate serial cable data transfer, the Telephony domain (i.e., Telephony Group) that deals with smart Bluetooth connected devices that support mobile phones and communication devices, the Personal Access Network domain (i.e., PAN Group) consisting of devices that have the ability to create local network groups to communicate over Bluetooth, and the Audio/ Video domain (i.e., A/V Group) that supports Bluetooth devices that deal with audio and video files, which in most cases are of large data size and complexity. Some of these profiles are depicted below: Advanced Audio Distribution Profile (A2DP), Audio/Video Remote Control Profile (AVRCP), Common ISDN Access Profile (CIP), General Audio/Video Distribution Profile (GAVDP), Generic Object Exchange Profile (GOEP), Hard Copy Cable Replacement Profile (HCRP), Human Interface Device Profile (HID), Personal Area Networking Profile (PAN), Phone Book Access Profile (PBAP), Serial Port Profile (SPP), Service Discovery Profile (SDAP), SIM Access Profile (SAP, SIM), Video Distribution Profile (VDP), Wireless Application Protocol Bearer (WAPB), Basic Imaging Profile (BIP), Basic Printing Profile (BPP), Cordless Telephony Profile (CTP), Device ID Profile (DID), Dial-up Networking Profile (DUN), Fax Profile (FAX), File Transfer Profile (FTP), Generic Access Profile (GAP), Hands-Free Profile (HFP), Headset Profile (HSP), Intercom Profile (ICP), Object Push Profile (OPP), or Synchronization Profile (SYNCH). Among this extensive list of Bluetooth profiles, since the D2D protocol is being used among devices running the most commonly installed Operating Systems (OS) [29] (Android, Windows and iOS/iPadOS Operating Systems), the three best candidates are the Serial Port Profile (SPP), the Personal Area Networking Profile (PAN), and the Generic Object Exchange Profile (GOEP) which are designed to be supported by the latter vendors.

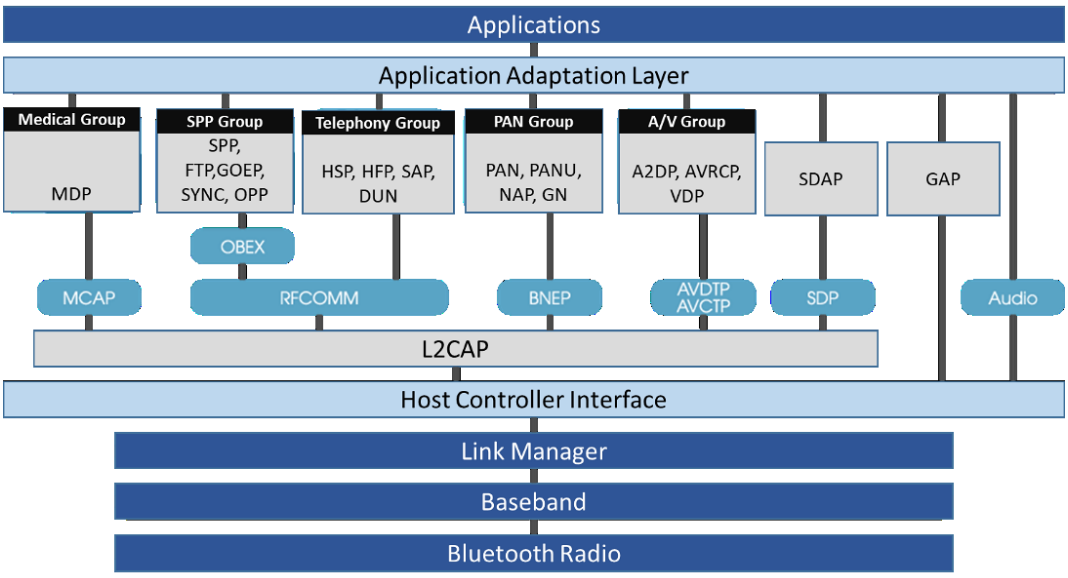


**Figure 1. Bluetooth profiles and their application domains.**

### *2-3-1- Bluetooth Serial Port Profile (SPP)*

The Bluetooth SPP profile [30] defines the requirements for Bluetooth devices that are necessary for creating emulated serial cable connections using the RFCOMM protocol between the involved devices. The requirements can be described as services which are provided to the involved applications, as well as through the definition of the features and processes that are needed for communication among the interacting devices. In the Bluetooth SPP profile, the following roles are defined:

- Initiator: it initiates a connection to another device.
- Acceptor: it waits for another device to initiate the connection.

Figure 2 shows the protocols and entities used in the Bluetooth SPP profile. Shortly, the Baseband, LMP and L2CAP are the OSI layer of the Bluetooth protocols. RFCOMM is the Bluetooth adaptation of GSM TS 07.10, providing the needed serial port emulation, while SDP is the Bluetooth Service Discovery Protocol. The required procedures that should be defined in the Bluetooth SPP profile are divided in three different steps, referring to the (i) establishment of a link and the set-up of a Virtual Serial Connection, (ii) the acceptance of the link and the establishment of a Virtual Serial Connection, and (iii) the registration of the Service Record in a local SDP database. More details regarding the usage of this Bluetooth profile can be found in Chen and Zhuang (2007) study [30].

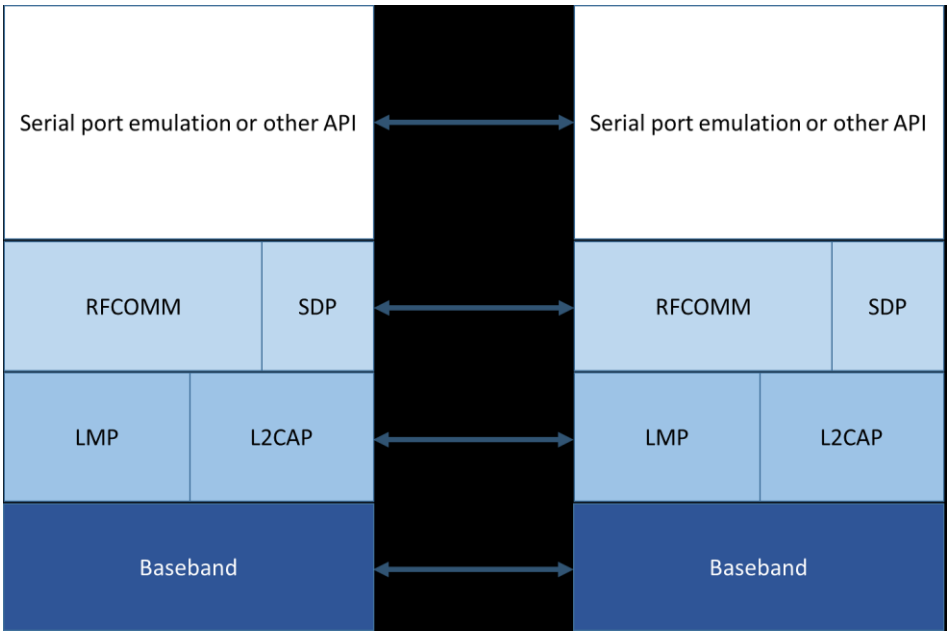


**Figure 2. Bluetooth SPP profile and the interacting protocols.**

### *2-3-2- Bluetooth Personal Area Network (PAN) Profile*

The Bluetooth PAN profile [31] describes the way that two or more Bluetooth devices can create an ad-hoc network and how it can be re-used for accessing a remote network through a network access point. For the PAN profile, two general scenarios are usually discussed: (1) the Network access points, and (2) the Group Ad-hoc Networks. Each case has unique network architecture and requirements, creating multiple combinations of a PAN profile. In the Bluetooth PAN profile, the following roles are defined:

- Group Ad-hoc Network (GN) and GN service can be considered as a Bluetooth device that supports the GN service for forwarding Ethernet packets to each of the connected Bluetooth devices, speaking about the PAN users, as needed.
- PAN User (PANU) is the Bluetooth device that can use either the NAP or the GN service. PANU supports the client role for both the NAP and GN roles.

Figure 3 shows the protocols and entities used in the Bluetooth PAN profile. The Baseband, LMP and L2CAP are the parts of the Bluetooth protocols that reside in the OSI layer. As in the previous case, SDP is the Bluetooth Service Discovery Protocol, while the Management Entity (ME) is the entity that coordinates the procedures for the initialization, parameterization, and connection management.

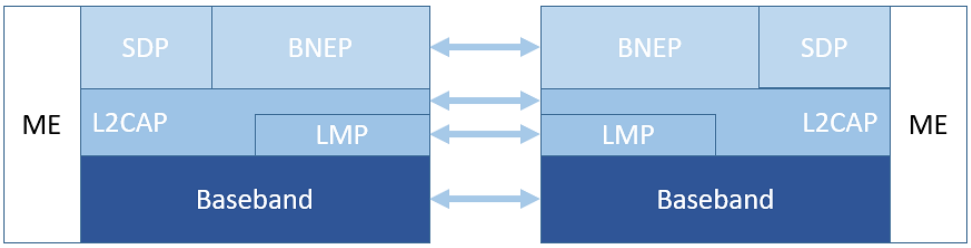


**Figure 3. Bluetooth PAN Profile and the interacting protocols.**

The required procedures that should be defined in the Bluetooth PAN profile are divided in two categories, following different steps based on whether the PANU wants to connect to a GN or the GN wants to connect to a PANU in order to finally create an ad-hoc network. More details regarding the usage of this Bluetooth profile can be found in Kuijpers et al. (2002) [31].

### *2-3-3- Generic Object Exchange Profile (GOEP)*

The Bluetooth GOEP profile [32] describes the protocols and procedures that the involved applications must use, providing the usage models for facilitating the overall object exchange capabilities. Such models can be a Synchronization, File Transfer, or Object Push model. In the Bluetooth GOEP profile, the following roles are defined:

- Server: it provides an object exchange server to and from which data objects have the ability to be pushed and pulled, respectively.
- Client: it can push or/and pull data object(s) to and from the Server.

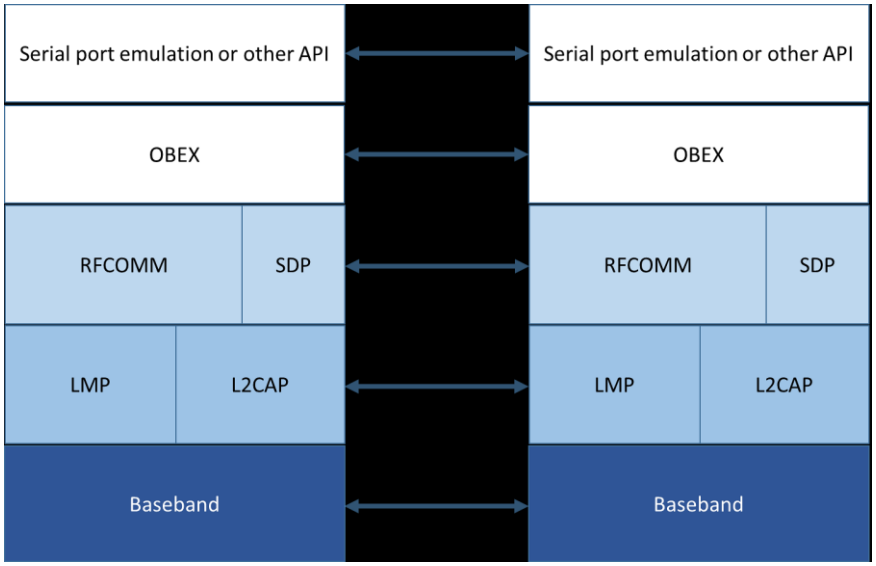


**Figure 4. Bluetooth GOEP Profile and the interacting protocols.**

Figure 4 shows the protocols and entities used in the Bluetooth GOEP profile. The Baseband, LMP and L2CAP are the OSI layer 1 and 2 Bluetooth protocols. RFCOMM is the Bluetooth adaptation of GSM TS 07.10. SDP is the Bluetooth Service Discovery Protocol, while OBEX is the Bluetooth adaptation of IrOBEX. The Application Client layer gives the ability to send and retrieve data object from the side of the Server using the OBEX operations. The application Server is offering storage capabilities for the data to and from which the data object can be sent or retrieved. More details regarding the usage of this Bluetooth Profile can be found in [32].

## 3- Materials and Methods

### *3-1- Evaluation Scenario and Working Environment*

For the purposes of the D2D protocol, six (6) different programming libraries have been designed, implementing the functionality of the protocol. In more detail, the first set of libraries implements the functionality of the D2D protocol using the Bluetooth SPP profile, the second set of libraries implements the functionality of the D2D protocol using the Bluetooth PAN profile, whereas the third set of libraries implements the functionality of the D2D protocol using the Bluetooth GOEP profile.

In all cases, apart from the programming libraries two applications were designed and implemented in order to be used for invoking the functions and operations offered by the implemented programming libraries. Having in mind that the D2D protocol aims in transferring health data over Bluetooth between a citizen and a Healthcare Practitioners (HCP), these two applications (i.e., Citizen Application, HCP Application) are serving the needs of the citizen and the HCP accordingly. These applications were designed and implemented for Android OS devices, using Android Studio [33]. The reason that it was implemented Android OS applications instead of iOS/iPadOS applications is two-fold: (i) Android offers easier usage of the Bluetooth technologies, and (ii) the reason of this paper is to compare the specification of the D2D protocol on top of different Bluetooth profiles, and not the implementation of the end-users' applications.

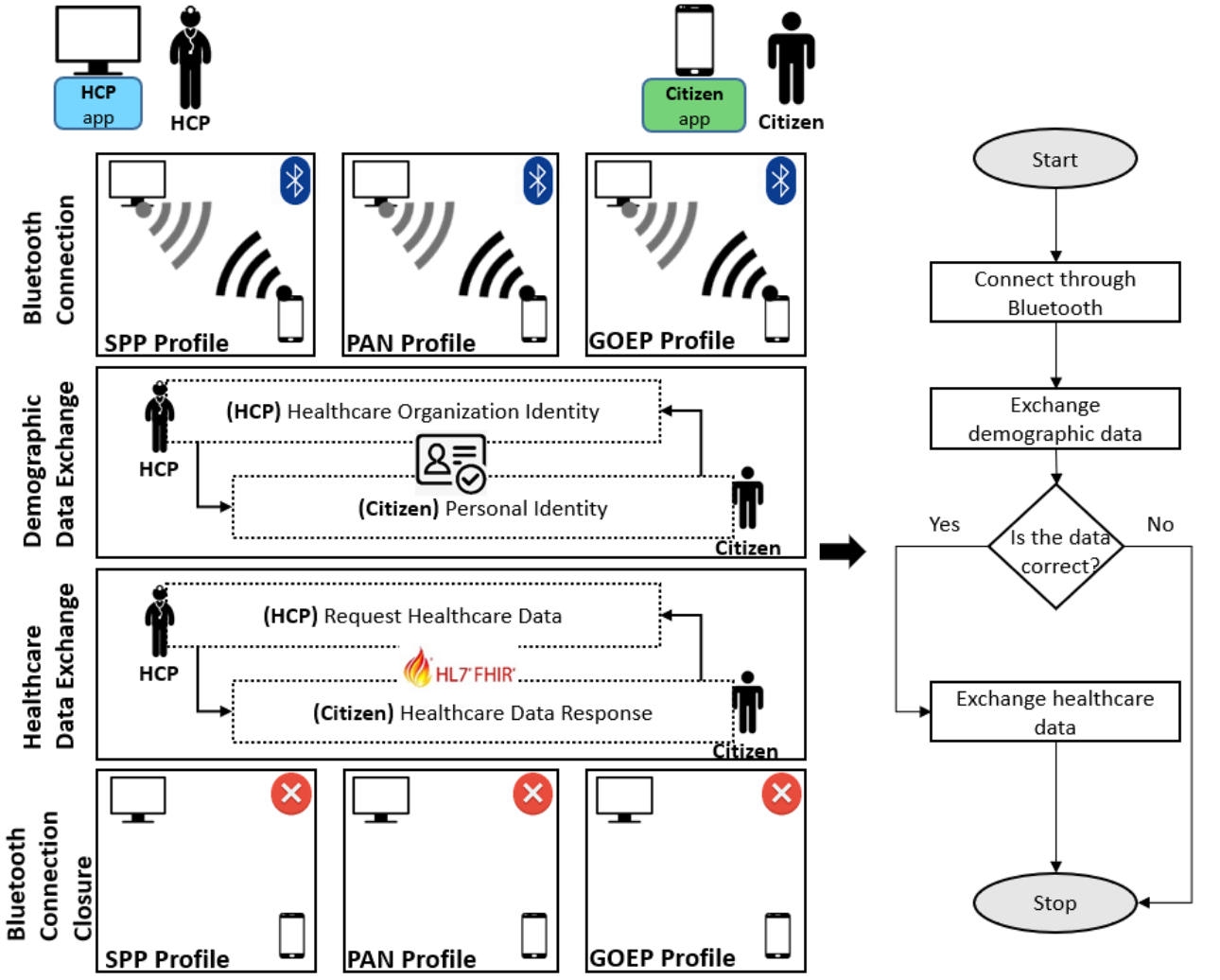


**Figure 5. Device-to-Device (D2D) Protocol process following the Bluetooth SPP, Bluetooth PAN and the Bluetooth GOEP profiles.**

Figure 5 depicts a flowchart of the scenario which was followed to compare the Bluetooth SPP, the Bluetooth PAN, and the Bluetooth GOEP profiles, using the D2D protocol paradigm, in which a citizen and an HCP are securely exchanging health data structured in HL7 FHIR format over Bluetooth, using the implemented applications. Shortly, during the Bluetooth Connection step, the two involved parties have to connect to each other over the Bluetooth Protocol, supporting one of the three different Bluetooth profiles. As soon as the HCP and the Citizen are connected, in the next step (Demographic Data Exchange) the two parties must identify each other by exchanging over Bluetooth, through the D2D protocol, identification data from the side of the supporting Healthcare Organization (for the HCP), and personal data (i.e., Personal Identity for the Citizen). The next step includes the exchange of Healthcare Data (Healthcare Data Exchange), in which the identified interacting parties are exchanging the requested data to be securely transferred through the D2D protocol and be visualized and examined from the side of the HCP. The overall process is then terminated, where in the last step (Bluetooth Connection Closure), the overall connection between the Citizen and the HCP terminates, and both parties stop the overall interaction. In Figure 6a, a medical image is depicted that was exchanged through the D2D protocol having the size of 35 Mbytes and is depicting a random hand X-ray result. What is more, in Figure 6b, an instance of the exchanged healthcare dataset that was used for evaluation is provided, including the demographic details of a random citizen structured in HL7 FHIR format (i.e., name, address, contacts, and identity number), having the size of 6 Kbytes.

```
<?xml version="1.0" encoding="UTF-8"?>

<Patient xmlns="http://hl7.org/fhir">
  <id value="example"/>
  <text>
    <status value="generated"/>
    <div xmlns="http://www.w3.org/1999/xhtml">
      <table>
        <tbody>
          <tr>
            <td> Name</td>
            <td> Peter James
              <b> Chalmers</b>  (&quot;Jim&quot;)
            </td>
          </tr>
          <tr>
            <td> Address</td>
            <td> 534 Erewhon, Pleasantville, Vic, 3999</td>
          </tr>
          <tr>
            <td> Contacts</td>
            <td> Home: unknown. Work: (03) 5555 6473</td>
          </tr>
          <tr>
            <td> Id</td>
            <td> MRN: 12345 (Acme Healthcare)</td>
          </tr>
        </tbody>
      </table>
    </div>
  </text>
</Patient>
```

**(a)** **(b)**

**Figure 6. (a) Sample of exchange image, (b) Sample of exchanged textual data.**

### *3-2- Device-to-Device Protocol over Bluetooth*

In order for the Bluetooth pairing and connection between the devices that host the Citizen app and the HCP app to be realized, a specific process between the client and the server application must be followed. In our case, both the Citizen app and the HCP app will behave as a true peer-to-peer endpoint by exposing both server and client behavior. Typically, the pairing process that is being followed is based on the Figure 7.

In general, for Bluetooth-enabled devices to exchange data, they must create a communication channel through a specific process of pairing. One of the devices has the role of the discoverable device, which is made available for receiving requests of incoming connection. The other device identifies the discoverable device through a process for service discovery. After the acceptance of the pairing request by the discoverable device, the devices bond to each other through exchanging security keys, which are cached for later use. As soon as these processes are completed, the two devices can interact and exchange data. When the overall communication is completed, the initiator device frees the communication channel that had linked it to the discoverable device. The two devices have a bonded status, in order to be easily reconnected in a future session. This process can be summarized as follows:

- Initialization: The Bluetooth enabled applications initialize the Bluetooth stack.
- Client: A client consumes the remote services. This is done by first discovering any nearby devices, and afterwards for each discovered device it searches for services of interest
- Server: A server makes all the services available to the previous clients. It registers these services in the SDDB, and it then waits for receiving connections, and accepts them, serving the clients that make them. In the case that the service is not needed anymore, the application removes it from the SDDB.

As described before, to use Bluetooth, a device must be compatible with the subset of Bluetooth profiles.

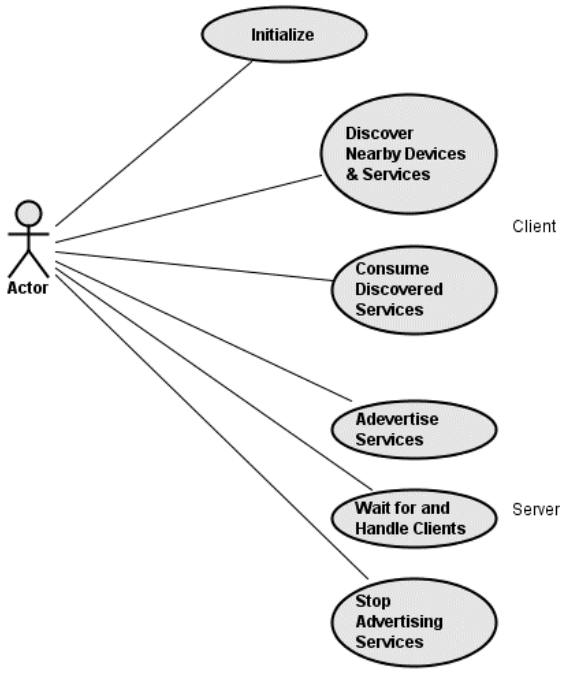


**Figure 7. Bluetooth pairing process.**

### *3-3- Evaluation Metrics*

To compare the Bluetooth SPP profile, the Bluetooth PAN profile, and the Bluetooth GOEP profile, the following evaluation metrics were considered for the three profiles, for their further comparison with regards to the purposes of the D2D protocol [34].

*Transmission time*: This metric refers to the transmission time (transfer rate), in which a data exchange process takes place with each different Bluetooth profile.

*Power Consumption*: This metric refers to the power that the devices consume when using the Bluetooth profiles.

*Probability of packet flush*: A specific flush timer is initiated when a packet enters the transmit buffer of the controller. In the case of timeout, the packet is flushed. Each data packet must have a specific number of slots in order to have a successful data exchange. Generally, the Bluetooth baseband uses an ARQ in order to send again baseband packets that contain errors. ARQ retransmissions can happen for a specific number of times, denoted by the number of transmissions $N_{Tx\_thresh}$, before a timeout occurs. The probability of packet flush is given by Equation 1:

$$N_{Tx\_thresh} = \left| \frac{\text{flush timeout}}{\text{successful packet transmission duration}} \right| \quad (1)$$

The probability of packet flush is given by Equation 2:

$$\Pr\{packet\ flush\} = \Pr\{N_{TX} > N_{TX\_thresh}\} = 1 - \sum_{n=1}^{N_{TX\_thresh}} PN_{TX}{}^{(n)} = (1-Psucc)^{N_{Tx\_thresh}} \quad (2)$$

*Probability of L2CAP retransmission*: A L2CAP retransmission happens in the case that there is a timeout in the retransmission timer. Such thing can happen if the original packet or its acknowledgment is flushed. Consequently, when both packets are transmitted without any errors, no other retransmissions take place. The probability of L2CAP retransmission is given by Equation 3:

$$P_{RTx} = \Pr\{L2CAP\ retranmission\} = 1 - \Pr\{succesful\ packet\ delivery\} * \Pr\{succesful\ ack\ delivery\} = 1 - \left[1 - \left(1 - P_{succ_{packet}}\right)^{N_{Tx_{packet}}}\right] * \left[1 - \left(1 - P_{succ_{ack}}\right)^{N_{Tx\_ack}}\right] \quad (3)$$

where $N_{Tx_{packet}}$ and $N_{Tx\_ack}$ are the threshold values for the number of retransmissions of measurement packets and acknowledgments, respectively. The probability distribution $PN_{RTX}$ of the random variable $N_{RTX}$, in accordance to the number of L2CAP retransmissions is given by Equation 4:

$$PN_{RTX}{}^{(n)} = P_{RTX}{}^{(n)}(1 - P_{RTx}) \quad (4)$$

*Probability of packet loss*: Packets which are not retransmitted by L2CAP are lost in the case of flushing. This can happen to all streaming packets and packets that use the Bluetooth SPP and Bluetooth GOEP profiles. Hence, for these profiles the loss probabilities are equal to the flushing probabilities, while for the Bluetooth PAN profile, the loss probabilities are the L2CAP retransmission failure probabilities. Hence, for SPP and GOEP packets the probability of packet loss is provided by Equation 5:

$$\Pr\{packet\ loss\} = \Pr\{packet\ flush\} \tag{5}$$

Furthermore, for PAN packets the probability of packet loss is given by Equation 6:

$$\Pr\{packet\ loss\} = 1 - \Pr\{NRTx\ \leq 2\} = 1 - \sum_{n=0}^{2} PN_{RTX}{}^{(n)} \tag{6}$$

## 4- Results and Discussion

The overall process described by the scenario was followed for the three (3) different Bluetooth profiles, while it was repeated ten (10) different times, calculating the results for the different evaluation metrics for each case. Furthermore, in order to perform the overall testing scenario, and test the overall specification of the D2D protocol, there have been developed two different applications with a basic User Interface (Citizen application and HCP application), for invoking the operations offered by the D2D protocol, and serving the needs of the citizen and the HCP. The Citizen application has been developed in Android Studio using Java for Android (Android v4.3.1), while the HCP application has been developed in NetBeans using Java (Java v8.0). For both applications, an initial dataset was loaded (structured in XML HL7 FHIR format) in order to be exchanged following the overall process defined by the D2D protocol in Section 3. Figure 8 depicts an instance of the basic user interface of these two applications, showcasing that the two applications are paired, while the interacting parties are successfully connected. For each case, the different Bluetooth profiles were used, for the same data types and sizes.

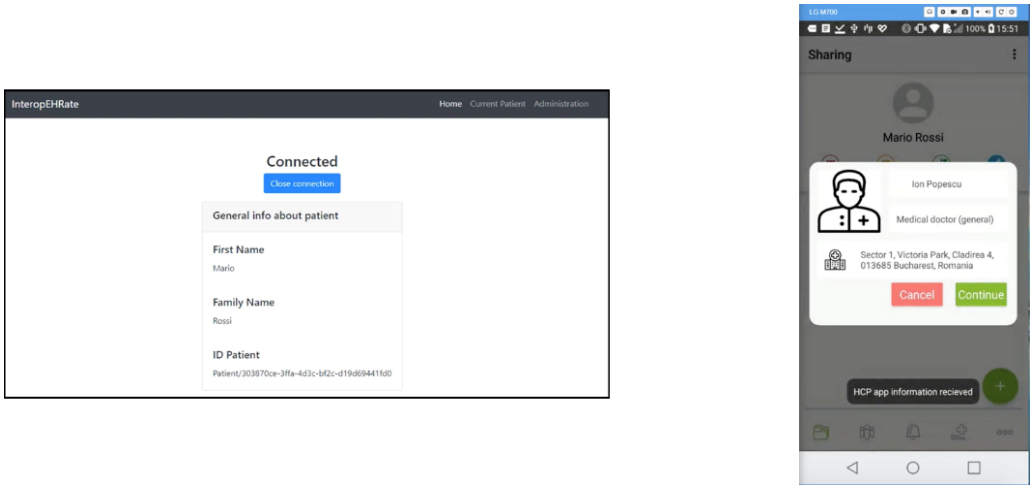


**Figure 8. Basic user interfaces of the interacting applications.**

The average mean of the results of the ten (10) iterations are depicted in Table 1, for each one of the different evaluation metrics.

**Table 1. Comparison results of the Bluetooth SPP, Bluetooth PAN and Bluetooth GOEP profiles.**

| Average mean of: | Bluetooth SPP Profile | Bluetooth PAN Profile | Bluetooth GOEP Profile |
|---|---|---|---|
| Transmission time | ~6 sec | ~7 sec | ~8 sec |
| Power Consumption | low | low | low |
| Probability of packet flush | 0,02 | 0,04 | 0,06 |
| Probability of L2CAP retransmission | 0,01 | 0,02 | 0,03 |
| Probability of packet loss | 0,01 | 0,03 | 0,03 |

Based on the results of Table 1, among the different evaluation metrics, the Bluetooth SPP profile can be considered as the best candidate for the purposes of the D2D protocol. It performs much better in the provided scenario, achieving higher transmission time with decreased probabilities of packet loss, flush and L2CAP retransmission. In more detail it

can be seen that with regards to the Transmission time, the Bluetooth SPP profile performs better since its average mean was almost 6 sec., in comparison with the Bluetooth PAN profile which was 7 sec. and the Bluetooth GOEP profile which was 8 sec. Such a difference is caused due to the fact that the Bluetooth SPP profile follows a different protocol stack than the other two, minimizing the overall obligatory pairing and data exchange interactions (Figure 9).

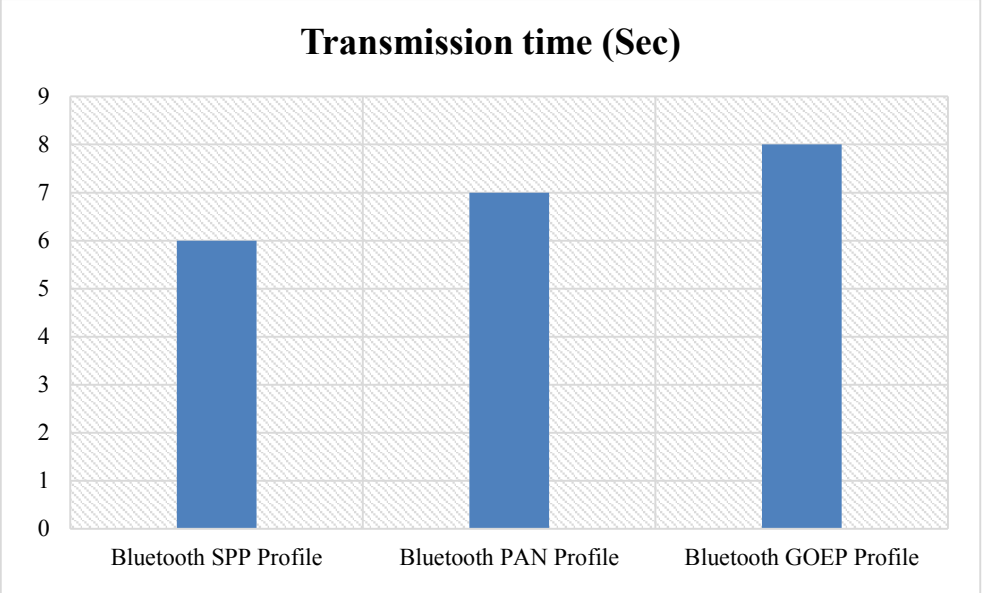


**Figure 9. Transmission Time results of the Bluetooth SPP, Bluetooth PAN and the Bluetooth GOEP profiles.**

As for the Power consumption, in all cases there was not any significant difference, since for the three Bluetooth profiles there was not calculated any major battery consumption of the interacting devices. In more detail, the BT-Power-Calc [35] was parameterized to calculate the Bluetooth power consumption. This calculator included both advertising and peripheral use cases, having also the ability to configure different use case profile parameters. The estimate of the overall power consumption was provided, depicting that in all three cases the consumption was extremely low to be considered as a metric of high impact. Consequently, this metric was considered to be out of context for the current scenario. With regards to the Probability of packet flush (Figure 10a), the Bluetooth GOEP profile dealt with most packet flushes, since it is built for exchanging binary objects having a nature similar to client-server applications, and as a result the exchanging of roles between the involved parties was leading to more packet flushes, increased L2CAP retransmission (Figure 10a) and as a result, an increased probability of packet loss (Figure 10c). On the other hand, as for the Probability of packet flush (Figure 10a) the Bluetooth SPP profile was slightly better than the Bluetooth PAN profile, since the nature of the D2D protocol is more identical to the environment created and supported by the Bluetooth SPP profile.

Consequently, by the time that the D2D protocol follows the paradigm of emulating a serial cable data transfer instead of creating a local area network, this resulted into less L2CAP retransmission and packet losses for the Bluetooth SPP profile (Figures 10b and 10c), resulting into being the most appropriate candidate for the overall D2D protocol communication. Nevertheless, it should be considered that the overall implementation was performed mainly for devices supporting Android operating systems. However, it should be also mentioned that the overall purpose of the D2D protocol is to be supported by the top market OS, including the support of the operating systems of Windows and Apple devices. Despite the fact that Windows devices do not have any specific restrictions and requirements, it has been studied that Apple generally supports a short list of Bluetooth profiles, such as the Hands-Free Profile (HFP), the Phone Book Access Profile (PBAP), or the Advanced Audio Distribution Profile (A2DP), which however cannot serve the purposes of the D2D protocol. Among the supported Bluetooth profiles, the Bluetooth PAN profile is considered as the most appropriate for the current D2D protocol specification for Apple devices, since the Bluetooth SPP profile cannot be supported by the latter due to Apple's development restrictions [36]. Consequently, the overall study results that in the case that the D2D protocol would not be considered to be vendor specific but would only be considered to be efficient and effective, then the Bluetooth SPP profile should be the only choice among the different Bluetooth profiles. However, taking into consideration the desired nature of the D2D protocol to be fully supported by the main market OS, it should be specified for also supporting the Bluetooth PAN profile for the cases of Apple devices.

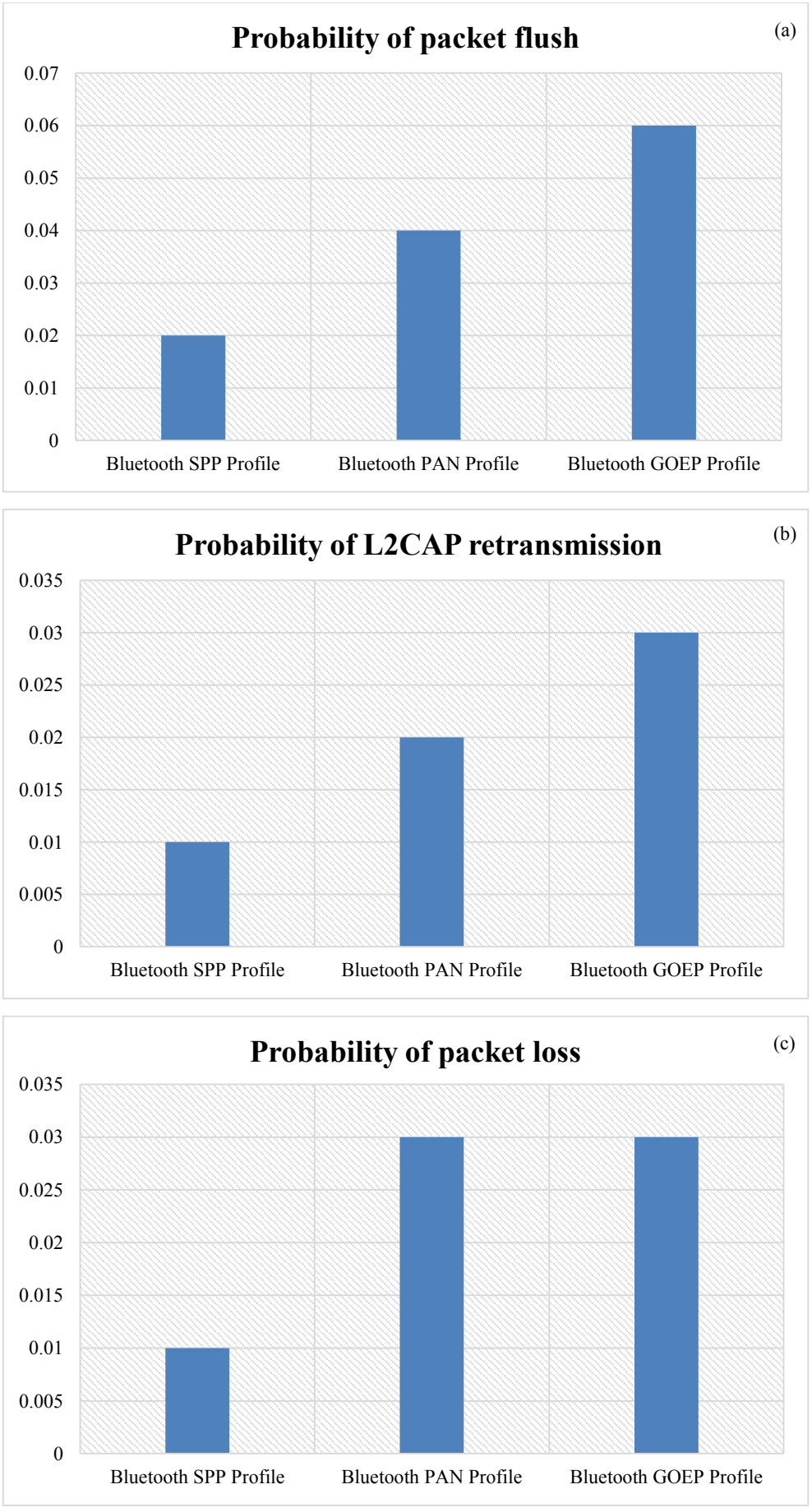


**Figure 10. (a) Probability of packet flush results, (b) Probability of L2CAP retransmission results, and (c) Probability of packet loss results of the Bluetooth SPP, Bluetooth PAN and the Bluetooth GOEP profiles.**

Nevertheless, it should be considered that the overall implementation was performed mainly for devices supporting Android operating systems. However, it should be also mentioned that the overall purpose of the D2D protocol is to be supported by the top market operating systems, including the support of the operating systems of Apple devices. To this context, it has been already defined that Apple generally supports a short list of Bluetooth profiles, such as the Hands-Free Profile (HFP), The Phone Book Access Profile (PBAP), or the Advanced Audio Distribution Profile (A2DP), which however cannot serve the purposes of the D2D protocol. Among the supported Bluetooth profiles, the Bluetooth PAN profile is considered as the most appropriate for the current D2D protocol specification for Apple devices, since the Bluetooth SPP profile cannot be supported by the latter due to Apple's development restrictions [26]. Consequently, the overall study results that in the case that the D2D protocol would not be considered to be vendor specific but would only be considered to be efficient and effective, then the Bluetooth SPP profile should be the only choice among the different Bluetooth profiles. However, taking into consideration the desired nature of the D2D protocol to be fully supported by the main market operating systems, it should be specified for also supporting the Bluetooth PAN profile for the cases of Apple devices.

## 5- Conclusion

The objective of this paper was to deliver a high-level specification of the proposed D2D protocol that is used on facilitating the exchange of healthcare data over Bluetooth, as well as a descriptive evaluation of the different Bluetooth profiles that can implement the overall D2D protocol functionality. For this evaluation, specific metrics were chosen to compare and evaluate the performance and the efficiency of each different Bluetooth profile, trying to present their nature and behavior through exchanging healthcare data between the interacting applications of the involved parties (healthcare practitioners, citizens), without the usage of internet connection. The conclusions to that study are that the D2D protocol could be specified with a more generic nature, being more efficient and effective, through prioritizing the Bluetooth profiles that could be potentially used for its purposes. Nevertheless, as it was already made clear there exist several implementations and research projects that aim towards the goal of securely exchanging health data. Most of them are using either specifically specified or designed vendor-specific protocols, whereas there exist implementations which are trying to solve the aforementioned issue, in a more generic scope. It is within our future goals to perform additional evaluation with several Bluetooth profiles, as well as different short-range distance communication protocols (e.g., Wi-Fi Direct), including additional evaluation metrics whose nature will be changing according to requirements derived from the size of the data to be transferred, the importance of the data transfer, or the circumstances under which the data transfer will take place.

## 6- Declarations

### *6-1- Author Contributions*

Conceptualization, A.K. and A.M.; methodology, A.K.; software, A.M.; validation, A.K. and A.M.; formal analysis, D.K.; investigation, A.K.; resources, A.M.; data curation, A.K.; writing—original draft preparation, A.K.; writing—review and editing, D.K.; visualization, A.M.; supervision, D.K.; project administration, D.K.; funding acquisition, D.K. All authors have read and agreed to the published version of the manuscript.

### *6-2- Data Availability Statement*

No new data were created or analyzed in this study. Data sharing is not applicable to this article.

### *6-3- Funding*

The research leading to this result has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 826106 (InteropEHRate project).

### *6-4- Conflicts of Interest*

The authors declare that there is no conflict of interests regarding the publication of this manuscript. In addition, the ethical issues, including plagiarism, informed consent, misconduct, data fabrication and/or falsification, double publication and/or submission, and redundancies have been completely observed by the authors.

## 7- References

[1] Schneble, Christophe Olivier, Bernice Simone Elger, and David Martin Shaw. "All Our Data Will Be Health Data One Day: The Need for Universal Data Protection and Comprehensive Consent (Preprint)" (November 4, 2019). doi:10.2196/preprints.16879.

[2] Nalin, Marco, Ilaria Baroni, Giuliana Faiella, Maria Romano, Flavia Matrisciano, Erol Gelenbe, David Mari Martinez, et al. "The European Cross-Border Health Data Exchange Roadmap: Case Study in the Italian Setting." Journal of Biomedical Informatics 94 (June 2019): 103183. doi:10.1016/j.jbi.2019.103183.

[3] Commission makes it easier for citizens to access health data securely across borders. Available online: https://ec.europa.eu/commission/presscorner/detail/en/IP_19_842 (accessed on February 2021).

[4] eHealth Information Exchange for Citizens. Available online: https://www.dhs.pa.gov/contact/DHS-Offices/Pages/eHealth-HIE%20for%20Citizens.aspx (accessed on February 2021).

[5] Séroussi, Brigitte, and Jacques Bouaud. "Adoption of a nationwide shared medical record in France: Lessons learnt after 5 years of deployment." In AMIA Annual Symposium Proceedings. American Medical Informatics Association (2016): 1100.

[6] Medcom. Available online: https://www.medcom.dk/medcom-in-english/about-medcom (accessed on February 2021).

[7] Swedish Medical Record. Available online: https://www.swedish.org/patient-visitor-info/medical-records (accessed on February 2021).

[8] Diraya. Available online: https://joinup.ec.europa.eu/collection/junta-de-andalucia/solution/diraya/about (accessed on March 2021).

[9] Chandrasekaran, Ranganathan, Balaji Sankaranarayanan, and John Pendergrass. "Unfulfilled Promises of Health Information Exchange: What Inhibits Ambulatory Clinics from Electronically Sharing Health Information?" International Journal of Medical Informatics 149 (May 2021): 104418. doi:10.1016/j.ijmedinf.2021.104418.

[10] Lenert, Leslie, and Brooke Yeager McSwain. "Balancing Health Privacy, Health Information Exchange, and Research in the Context of the COVID-19 Pandemic." Journal of the American Medical Informatics Association 27, no. 6 (April 26, 2020): 963–966. doi:10.1093/jamia/ocaa039.

[11] Kiourtis, Athanasios, Argyro Mavrogiorgou, Dimosthenis Kyriazis, Alessio Graziani, and Francesco Torelli. "Improving Health Information Exchange through Wireless Communication Protocols." 2020 16th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob) (50308) (October 12, 2020). doi:10.1109/wimob50308.2020.9253374.

[12] Kiourtis, Athanasios, Argyro Mavrogiorgou, and Dimosthenis Kyriazis. "A Semantic Similarity Evaluation for Healthcare Ontologies Matching to HL7 FHIR Resources." Digital Personalized Health and Medicine: Proceedings of MIE 2020 270 (2020): 13.

[13] Kiourtis, Athanasios, Argyro Mavrogiorgou, Sofia-Anna Menesidou, Panagiotis Gouvas, and Dimosthenis Kyriazis. "A Secure Protocol for Managing and Sharing Personal Healthcare Data." Integrated Citizen Centered Digital Health and Social Care (November 23, 2020). doi:10.3233/shti200701.

[14] Mockel, Rico, Alexander Sprowitz, Jerome Maye, and Auke Jan Ijspeert. "An Easy-to-Use Bluetooth Scatternet Protocol for Fast Data Exchange in Wireless Sensor Networks and Autonomous Robots." 2007 IEEE/RSJ International Conference on Intelligent Robots and Systems (October 2007). doi:10.1109/iros.2007.4399458.

[15] Qiu, Han, Meikang Qiu, Meiqin Liu, and Gerard Memmi. "Secure Health Data Sharing for Medical Cyber-Physical Systems for the Healthcare 4.0." IEEE Journal of Biomedical and Health Informatics 24, no. 9 (September 2020): 2499–2505. doi:10.1109/jbhi.2020.2973467.

[16] Shao, Chong, and Shahriar Nirjon. "ImageBeacon." Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (April 18, 2017). doi:10.1145/3054977.3054985.

[17] Chung, Myoungbeom, and Ilju Ko. "Data-Sharing Method for Multi-Smart Devices at Close Range." Mobile Information Systems 2015 (2015): 1–11. doi:10.1155/2015/931765.

[18] Direct Secure Messaging. Available online: https://directtrust.org/what-we-do/direct-secure-messaging (accessed on February 2021).

[19] Carequality. Available online: https://www.himss.org/resource-environmental-scan/carequality (accessed on February 2021).

[20] Cloud Fax. Available online: https://www.healthworkscollective.com/tag/cloud-fax-solution/ (accessed on March 2021).

[21] KONFIDO. Available online: https://konfido-project.eu/ (accessed on February 2021).

[22] Gavrilov, Goce, Boro Jakimovski, Ivan Chorbev, and Vladimir Trajkovik. "Cloud-Based Electronic Health Record for Health Data Exchange." Proceedings of the 8th International Conference on Applied Internet and Information Technologies (October 5, 2018). doi:10.20544/aiit2018.p03.

[23] Masud, Mehedi, and M. Shamim Hossain. "Secure Data-Exchange Protocol in a Cloud-Based Collaborative Health Care Environment." Multimedia Tools and Applications 77, no. 9 (October 28, 2017): 11121–11135. doi:10.1007/s11042-017-5294-5.

[24] Basjaruddin, Noor Cholis, Edi Rakhman, Kuspriyanto, and Mikhael Bagus Renardi. "Developing Electronic Medical Record Based on NFC." Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence - CSAI 2017 (2017). doi:10.1145/3168390.3168420.

[25] De Almeida, Thales Teixeira, José Geraldo Ribeiro Júnior, Miguel Elias M. Campista, and Luís Henrique M. K. Costa. "Wi-Fi Direct Performance Evaluation for V2P Communications." Journal of Sensor and Actuator Networks 9, no. 2 (June 6, 2020): 28. doi:10.3390/jsan9020028.

[26] Li, Fuliang, Xingwei Wang, Zijian Wang, Jiannong Cao, Xuefeng Liu, Yuanguo Bi, Weichao Li, and Yi Wang. "A Local Communication System Over Wi-Fi Direct: Implementation and Performance Evaluation." IEEE Internet of Things Journal 7, no. 6 (June 2020): 5140–5158. doi:10.1109/jiot.2020.2976114.

[27] Vidakis, Konstantinos, Argyro Mavrogiorgou, Athanasios Kiourtis, and Dimosthenis Kyriazis. "A Comparative Study of Short-Range Wireless Communication Technologies for Health Information Exchange." 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE) (June 2020). doi:10.1109/icecce49384.2020.9179478.

[28] Fraga-Lamas, Paula, Peio Lopez-Iturri, Mikel Celaya-Echarri, Oscar Blanco-Novoa, Leyre Azpilicueta, Jose Varela-Barbeito, Francisco Falcone, and Tiago M. Fernandez-Carames. "Design and Empirical Validation of a Bluetooth 5 Fog Computing Based Industrial CPS Architecture for Intelligent Industry 4.0 Shipyard Workshops." IEEE Access 8 (2020): 45496–45511. doi:10.1109/access.2020.2978291.

[29]Mobile Operating System Market Share Worldwide. Available online: https://gs.statcounter.com/os-market-share/mobile/worldwide (accessed on February 2021).

[30] Chen, Ya-hui, and Yi-qi Zhuang. "Research and Realization of File Transfer Based on Bluetooth's SPP Profile." Communications Technology 11 (2007).

[31] Kuijpers, G., T.T. Nielsen, and R. Prasad. "Optimizing Neighbor Discovery for Ad Hoc Networks Based on the Bluetooth PAN Profile." The 5th International Symposium on Wireless Personal Multimedia Communications (December 2002). doi:10.1109/wpmc.2002.1088161.

[32] Bluetooth Profiles. Available online: https://docs.huihoo.com/symbian/s60-5th-edition-cpp-developers-library-v2.1/GUID-35228542-8C95-4849-A73F-2B4F082F0C44/sdk/doc_source/guide/Short-Link-Services-subsystem-guide/ShortLinkServices/BluetoothProfiles/BTProfiles.html (accessed on March 2021).

[33] Android Studio. Available online: https://developer.android.com/studio (accessed on March 2021).

[34] Noueihed, Jad, Robert Diemer, Samarjit Chakraborty, and Stefanie Biala. "Comparing Bluetooth HDP and SPP for Mobile Health Devices." 2010 International Conference on Body Sensor Networks (June 2010). doi:10.1109/bsn.2010.40.

[35] Bluetooth Power Calculator. Available online: https://www.ti.com/tool/BT-POWER-CALC. (accessed on February 2021).

[36] MFi Program Enrollment. Available online: https://mfi.apple.com/en/help/login-help/MFi-Enrollment.html (accessed on February 2021).