Improving Opportunistic Networks by Leveraging Device-to-Device Communication

Radu-Corneliu Marin, Radu-Ioan Ciobanu, Ciprian Dobre

***Abstract*—Several popular low-level device-to-device techniques, such as Bluetooth and Wi-Fi Direct, are seen today as enablers for fifth generation (5G) mobile networks, as the communication infrastructure for future Internet of Things systems. However, most of these technologies do not support direct over-the-air communication between end users / devices. Opportunistic networks propose the use of delay-tolerant and wireless communication over such technologies, towards routing messages between end users. In our previous studies, we have shown how taking advantage of the existing Wi-Fi infrastructure leads to high hit rates and low latency based on the increased wireless range coupled with high bandwidth. In this paper, we extend our proposed architecture for covering infrastructure-less environments through a novel mechanism that allows connecting peers through Wi-Fi Direct in a seamless and secure fashion. Furthermore, we emulate real-life user traces to empirically prove that our solution improves hit rate with 13% without impacting battery life.**

***Index Terms*—Opportunistic networking Wi-Fi device-to-device communication.**

I. Introduction

Opportunistic networks (ONs), originally coined by Pelusi et al. [1], are generally considered as a natural evolution of Mobile Ad-hoc Networks (MANETs) comprised mostly of mobile wireless devices ranging from small wireless-capable sensors to smartphones or tablets, which aid in transmitting data horizontally by taking advantage of the already-existent interactions between devices [1], [2], [3]. They are generally seen as enablers for fifth generation (5G) networks. For this, ONs employ short-range communication protocols (e.g., IEEE 802.11, Bluetooth) in order to disseminate data and decongest existing backend protocols.

Communication in ONs is fully decentralized as the composing nodes are only aware of other nodes they are in close proximity to (based on the range of the transmission media) and have no previous knowledge of the network topology. This has multiple implications: firstly, no assumptions can be made about the existence of paths between opportunistic nodes, as the network is very dynamic and disconnections are the norm. As such, ONs employ a paradigm entitled *store-carry-and-forward* (SCF) [1] in which nodes begin by storing local data either generated locally or received from peers; usually being hand-held devices, nodes are characterized by a high-degree of mobility and move around the network while carrying the stored data until the destination of data items is encountered, case in which a routing process is started for sending the data to their rightful recipients. This leads to the second implication: encountering a data message's destination is not always the case for data forwarding; ONs are based on the altruism of nodes which help in carrying other encountered nodes' data through the networks towards reaching the desired destination in exchange for them bearing the node's messages as well. This is the actual key factor of ONs which attempts to maximize throughput while reducing latency, and which leads to our final implication: understanding human mobility is of paramount importance in designing efficient opportunistic networking protocols [4]. As opposed to Mobile Edge Computing (MEC), where mobile devices connect to a frontier cell tower and therefore can coordinate by communicating over such an infrastructure, all routes in ONs are dynamic and nodes have no predetermined method of knowing they will interact in any fashion.

The main problem in opportunistic networking is that most of the technologies that can be used do not support direct over-the-air communication between end users / devices, and this is what we aim to address with this paper. In our previous work [5], [6], we have designed and implemented a mobile application for tracking interactions between peers in wireless networks which was used in multiple such tracing experiments, and which proved that Wi-Fi is more feasible than Bluetooth as opportunistic networking support. In this article, we extend our previous work by implementing an opportunistic communication engine based on the *Interest Spaces* framework [7] and which not only can be deployed in Wi-Fi networks, but can also handle non-infrastructure networks. As such, we introduce a novel mechanism in which nodes can act altruistically by hosting Wi-Fi Direct access points (APs) which allow peers connecting to them to interact in a seamless and secure fashion. Although this mechanism is largely useful when there is a lack of any pre-existing Wi-Fi infrastructures, it can also be deployed for bridging communities connected to neighboring Wi-Fi networks. Furthermore, we use the traces we previously collected [5] to prove that it improves the performance of ONs – increasing hit rate with up to 13% and lowering latency with up to 21%, with a minimal impact on battery usage ($\approx$ 7-8%). We believe that the techology has evolved sufficiently so that opportunistic networks can start being deployed on a global scale. Wi-Fi Direct has become more and more popular (and is starting to be enabled by default in Android, for example), and 5G (which will have device-to-device support) is just around the corner.

The remainder of the article is organized as follows. Sec-

R.-C. Marin and R.-I. Ciobanu, are with University POLITEHNICA of Bucharest, Splaiul Independentei 313, 060042 Bucharest, Romania, e-mails: radu.marin@cti.pub.ro, radu.ciobanu@cs.pub.ro. C. Dobre (corresponding author) is with the National Institute for Research and Development in Informatics, 8-10 Maresal Averescu, Bucharest, Romania, e-mail: ciprian.dobre@cs.pub.ro.

TABLE I
COMPARISON OF WIRELESS AND MOBILE SUPPORT TECHNOLOGIES

Metric	Bluetooth	BLE	NFC	ZigBee	WFD	WiFi	LoRa
Infrastructure	No	No	No	No	No	Yes	Yes
Max range (m)	100	50	0.2	100	200	100	2,200
Speed (Mbps)	2.1	1	0.4	0.25	250	600	0.05
Power	1	0.05	0.05	0.33	33	33	0.05
Security	WPA2	AES	N/A	AES	WPA2	WPA2	AES

tion II presents a general overview of networking support and provides an in-depth comparison of wireless communication protocols that can be deployed in ONs. Section III presents details on both our opportunistic communication engine, as well as on the novel mechanism for extending it over Wi-Fi Direct (WFD). While Section IV provides an analysis of our experimental results, Section V concludes the paper with a summary of our observations, as well as our thoughts for future work.

II. OPPORTUNISTIC NETWORKING SUPPORT

The novelty of ONs stems from the use of any available wireless communication media for establishing connections between mobile peers and exchanging data among them [1]. However, there are currently multiple such solutions and none has been deemed the most feasible to be used in opportunistic networking; multiple criteria must be taken into consideration while choosing a media to be used in ONs: security, range, power consumption, speed and infrastructure requirements. Table I contains a comparison of the following technologies:

- *Bluetooth* is a low-power and low-cost short-range communication technology for fixed and mobile devices, invented by the Swedish company Ericsson in 1994. It uses short-wavelength UHF radio waves in the ISM band from 2.4 and 2.485 GHz, and has become ubiquitous in most mobile devices nowadays. In 2010, a new version of Bluetooth was added to the standard by the Bluetooth Special Interest Group, called Bluetooth Smart/Bluetooth Low Energy (BLE) with the purpose of providing a considerably lower power consumption, while keeping a similar communication range.
- *Near Field Communication (NFC)* is a short-range wireless connectivity technology that enables smartphones and other devices to establish radio communications with each other by bringing them in close proximity. It is mostly used for making transactions, exchanging digital content, and connecting electronic devices, being compatible with many existing contactless cards and readers.
- *ZigBee* is a specification for a suite of protocols destined for Internet of Things (IoT) devices with small, low-power digital radios, standardized in 2003 by the ZigBee Alliance. It is based on an IEEE 802.15.4 standard, and can be used to transmit data over long distances by passing them through a mesh network of intermediate devices, in an opportunistic fashion. Similarly to NFC, ZigBee is generally employed by applications with low data rates that need to have high autonomy.
- *Wi-Fi* is a networking technology that uses the 2.4 GHz UHF and 5 GHz SHF ISM radio bands for offering wireless connection between devices and access points. It follows the IEEE 802.11 standards, and is completely ubiquitous nowadays. However, for situations where two devices in close range wish to communicate but have no AP to connect to, there is also Wi-Fi Direct (WFD), which is a related technology that allows devices to communicate through the wireless interface without needing a fixed AP.
- *LoRa* is a proprietary technology for Low-Power Wide-Area Networking (LPWAN), which offers a long range protocol for public and private networks with a low power consumption. It uses the LoRaWAN protocol to perform communication between remote sensors and gateways connected to the network, and stands at the basis of the Internet of Things. Its main goal is to be used for collecting data from small sensors and devices towards static gateways that are able to process and aggregate the data.

The first row in Table I shows which of them require an infrastructure, and which do not. The ones that do not require the existence of a prior infrastructure can be used for opportunistic communication between devices in range, as an alternative to Wi-Fi, which requires an infrastructure. Even though Wi-Fi networks have become nearly ubiquitous, alternative solutions might be required when there are no infrastructure-based solutions, or when they do not function correctly.

Table I shows, in the second row, the maximum range in meters for each of the six analyzed technologies. It can easily be seen that NFC has by far the worse range, since it cannot go farther than 20 cm. This happens because communication is done through electromagnetic induction, which cannot be performed if the two communicating devices are farther away. Other than NFC and LoRa, the other technologies offer similar values, with the mention that Bluetooth Smart has a lower range than regular Bluetooth, since it was designed with power saving in mind, thus reducing the maximum range. LoRa has a very high range, but it requires an infrastructure in the shape of gateways. Thus, after analyzing the maximum range for all protocols, it is clear that NFC cannot be used properly for ONs, even in very dense scenarios, because the range is extremely small. It should also be mentioned that ZigBee can have a much higher range since it uses mesh networking to transfer data (similar to opportunistic networking), but this is beyond the scope of this paper.

The third row of Table I presents the transfer speed (in Megabits per second) of each of the analyzed protocols. Wi-Fi clearly has the highest speed, and from the no-infrastructure protocols, Wi-Fi Direct has the highest speed. Since NFC, ZigBee and LoRa were created for short communication, they have very low speeds. The speeds obtained by Bluetooth and BLE are higher by one order of magnitude. From this analysis, we can conclude that ZigBee would probably be unsuitable for an ON, since the data objects that it needs to exchange are not as small as data objects exchanged by IoT devices. Nonetheless, Bluetooth speed is acceptable in certain conditions, while Wi-Fi Direct is even more feasible.

However, power consumption should also be taken into consideration when choosing a protocol, since opportunistic

nodes are battery-powered mobile devices. Thus, we show in the fourth row of Table I the power consumed by each of the analyzed technologies. We have taken Bluetooth as a gauge, which is why its power is shown as 1. The BLE protocol consumes about 95% less power than Bluetooth, as well as NFC. ZigBee is a higher consumer than NFC, even though the transfer speed is lower, but it has the advantage of a higher communication range, as shown above. Wi-Fi and Wi-Fi Direct are the highest consumers, as Bluetooth uses less than 3 percent of the power required by Wi-Fi for the same tasks.

Finally, from a security standpoint (which, as shown in [8], is an important topic in mobile networks, offering new challenges caused by the limited battery life of devices), all protocols, except for NFC, provide more than needed protection: BLE, ZigBee and LoRa use 128-bit AES, while regular Bluetooth, Wi-Fi, and Wi-Fi Direct employ WPA2 with 256-bit AES.

Although being an infrastructure-based technology, Wi-Fi is a popular communication media in opportunistic networking as it has a sufficiently large range, one of the best throughputs and with a near-ubiquitous AP presence, it is already considered a norm in modern society. Based on analyzing real-life datasets containing device interactions collected during a 3-month long experiment, we proved that Wi-Fi is more feasible than Bluetooth as opportunistic networking support [5]; due to its increased performance, Wi-Fi manages to establish up to 3 times more opportunistic contacts, while Bluetooth tends to isolate users into micro-communities. However, only using Wi-Fi is insufficient as it is unable to cover cases in which infrastructure is non-existent.

Our solution merges infrastructure-based communication technologies (i.e., Wi-Fi) with non-infrastructure based protocols (i.e., Wi-Fi Direct) towards extending coverage of the opportunistic engine initially proposed in [6]. Based on a novel mechanism which allows nodes to altruistically become APs for peers in a seamless and secure fashion, our proposed solution can be deployed without any extraneous requirements for the network, and is able to achieve high hit rates and low message delivery latencies, without impacting the battery life of mobile devices.

III. Opportunistic Networks over Wi-Fi Direct

In our previous studies [6], we have designed and implemented a mobile application destined for collecting contextual data, namely the *HYCCUPS Tracer*; the application[1] collects the following information from mobile devices: CPU usage (load, frequency usage, etc.), battery statistics (charge, plug, temperature, etc.), memory availability, screen usage, and sensor data (accelerometer, proximity, etc.). Apart from these metrics, the application also embedded an opportunistic engine capable of tracing interactions over Bluetooth by periodically scanning for beacons from paired devices, and Wi-Fi by using the AllJoyn framework [9].

AllJoyn is an open source software framework which offers a peer-to-peer communication environment for heterogeneous distributed systems across different device classes with emphasis on mobility, security and dynamism by implementing the D-Bus protocol. It provides an abstraction layer allowing it to run on multiple operating systems with the main goal of providing a software bus that offers distributed advertising and discovery of services in a secure mobile environment. In addition, the system supplies a Java-like location-transparent RMI. The object-oriented APIs provided by AllJoyn represented the corner-stone of our implementation of the *Interest Spaces* framework [7], by providing the communication support for the *ONSIDE* [10] opportunistic dissemination algorithm.

The *HYCCUPS Tracer* application was employed in a 65-day long tracing experiment [5] carried out in March-May 2012 at the Faculty of Automatic Control and Computers, University Politehnica of Bucharest, with a total of 66 volunteers varying in terms of year and specialization. We analyzed the collected HYCCUPS traces using the MobEmu emulator [11], an opportunistic network emulator that is able to replay a mobility trace and apply a desired algorithm when two nodes meet[2]; we concluded that Wi-Fi interactions using the AllJoyn framework were far more feasible than Bluetooth contacts as we observed that the long range coupled with higher bandwidth of Wi-Fi led to a staggering $\approx$ 21,000 interactions, while Bluetooth could only sum up to 34% of that value. Furthermore, after running a community detection algorithm, we discovered that Bluetooth has a tendency of isolating peers into micro-communities with seldom inter-group message exchanges. However, as previously mentioned, infrastructure-based solutions are incomplete, as our opportunistic engine could not cover the cases where wireless APs were not present. As such, we turned our attention towards Wi-Fi Direct which, in modern mobile operating systems, enforces a requirement that the device's owner should personally accept to pair to another device, similarly to Bluetooth.

In order to overcome this unacceptable need for human intervention, we have devised the following scheme over Wi-Fi Direct:

1) Use the Wi-Fi Direct legacy support (enforced by the Wi-Fi Direct standard [12]) to enable the mobile device as a local Wi-Fi AP. The local Wi-Fi Direct module generates a random Session Set Identifier (SSID) and passphrase for it.
2) Start peer discovery
   a) When peers are discovered, start advertising a *Bonjour* service over Wi-Fi Direct with an instance name constructed as follows: `SSID:Passphrase:IP`. For security reasons the instance name is encrypted using a private symmetric key contained in the application.
   b) Start searching for other such services.
   c) If a service is discovered, decrypt its instance name, and connect to the node using the credentials from the instance name.

Given that AllJoyn is able to run over any stable network interface, it will be able to opportunistically connect to any

[1] Available at http://hyccups.hpc.pub.ro, accessed on 2017-08-24.

[2] Available at https://github.com/raduciobanu/mobemu, accessed on 2017-08-24.

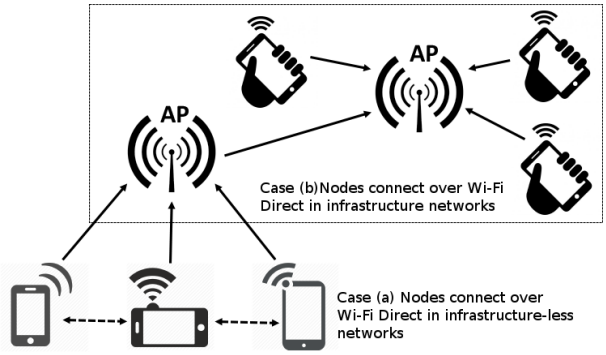

Fig. 1. Wi-Fi Direct opportunistic networking case.

other node connected to the Wi-Fi Direct AP. Unfortunately, the node that is hosting the AP is not able to connect its own network interface, therefore it will not be able to reach the nodes connecting to it. Furthermore, when a node is hosting a Wi-Fi Direct AP, it does not disconnect from its main network interface and therefore shares it with the peers that access it. This proves to be extremely useful for data offloading and leads to the following cases:

1) Three or more nodes meet: one of them is assigned as an AP and all other nodes interact amongst themselves as illustrated in Figure III, case (a). Unfortunately, two nodes in wireless range will not be able to interact one with the other over AllJoyn without infrastructure support.
2) One node connected to a Wi-Fi AP establishes itself as a Wi-Fi Direct AP: all nodes connecting to it will automatically connect to all peers from the Wi-Fi network as illustrated in Figure III, case (b).

However, the power consumption of this mechanism must be taken into account given that Wi-Fi Direct is a notable battery consumer and, as such, it cannot run continuously. Given that any decision to connect to a node is fully decentralized due to the nature of ONs, we need to synchronize the mobile devices to run the Wi-Fi Direct connecting algorithm at specific times. Based on the fact that most modern mobile OSes use Network Time Protocol (NTP) to keep the device's clock synchronized, we decided to run the algorithm 1 out of 10 minutes, every ten minutes, starting from 12 AM. This will guarantee that the connection schema will be able to find peers which are stationing nearby for at most 10 minutes. Furthermore, the algorithm contains an additional safe-guard against high power consumption, namely Step (2a) which implies that the Wi-Fi Direct AP will be created and advertised, if and only if peers are discovered at Step (1).

IV. Experimental Results

As previously mentioned, Wi-Fi Direct requires a considerable amount of energy to function, which cannot be overlooked. In order to measure the impact it has over battery life, we have designed a battery drain experiment in which the device is left idle with no human interaction in order to observe the speed with which the battery is depleted. In this sense, case (a) in Figure IV illustrates a regular power drain without using Wi-Fi Direct, while case (b) shows the impact of continuously using Wi-Fi Direct. The results are straightforward: Wi-Fi Direct drains approximately 80% from the battery life, which we consider to be unacceptable. However, in the approach proposed in the previous section, we show in case (c) that running Wi-Fi Direct for 1 minute every other 10 minutes leads to a 7% extra battery usage, which we consider to be more than acceptable. Furthermore, it proves that the Wi-Fi Direct circuitry does not suffer from the cold-start effect and its consumption is proportional to its usage, unlike GPS for instance.

Next, we studied the influence of Wi-Fi Direct over the opportunistic networking performance by emulating the tracing datasets collected in [5] and replaying them through MobEmu. In order to emulate Wi-Fi Direct interactions, we replaced the Bluetooth beacons used by the *HYCCUPS Tracer* and considered them to be contacts established using our previously proposed mechanism. The following metrics were taken into consideration:

1) Hit rate: the percentage of messages that have successfully reached their intended destinations, computed as the ratio between the number of delivered messages and the total number of generated messages.
2) Delivery cost: the ratio between the total number of messages exchanged during the course of the test and the number of generated messages.
3) Latency: the time passed between the generation of a message and its eventual delivery to the destination.
4) Hop count: the number of nodes that carried a message until it reached the destination on the shortest path.

While hit rate and latency are considered measures of network throughput, delivery cost and hop count are regarded as metrics of node and network congestion. Although the former two are consider to be of high importance, the latter two should be seriously taken into account and weighed against the former.

Furthermore, our analysis focuses on the two types of opportunistic communication:

1) Routing/forwarding: point-to-point communication between two peers; the data sent are not relevant for any of the other nodes on the path.
2) Dissemination: employs a modified form of publish/subscribe in which nodes can either act as publishers (which generate data marked with specific topics) or as subscribers (which subscribe to topics and expect to receive related data). Data dissemination in ONs is different from the classic publish/subscribe scheme due to the decentralized behavior of mobile networks.

To better understand the benefits of the proposed Wi-Fi Direct connecting mechanism, we chose to run the simulations in three cases: Wi-Fi only – ignore any Bluetooth interactions and only focus on infrastructure-based contacts, WFD1 – adding the Wi-Fi Direct mechanism on top of the Wi-Fi only case and replacing the Bluetooth contacts, and WFD2 – similar to WFD1, but choosing the nodes that become Wi-Fi Direct APs in a round-robin fashion so that such hosts also get to

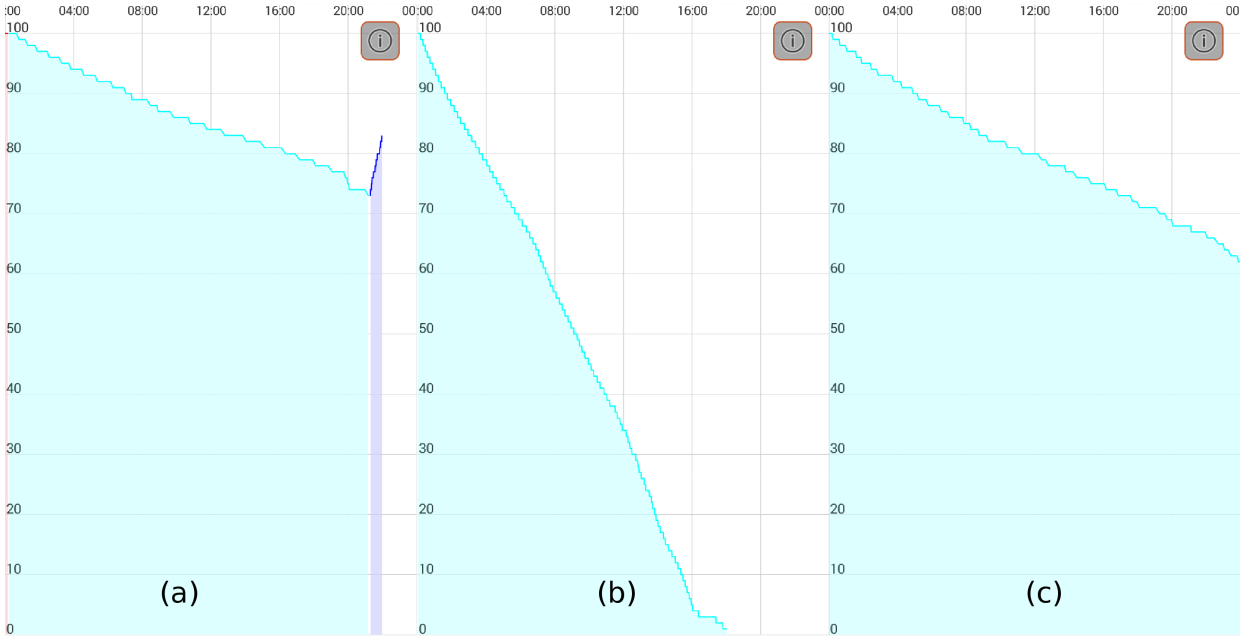

Fig. 2. Battery drain experimental results (HYCCUPS Tracer screenshots). Axis X specifies the time of day, while axis Y is the device's battery percentage. (a) regular power drain (no Wi-Fi Direct); (b) continuously use Wi-Fi Direct; (c) run Wi-Fi Direct for 1 minute every other 10 minutes.

receive the messages exchanged while they were altruistically acting as APs.

In order to analyze how the various tested algorithms behave in different conditions, we also vary a node's data memory size or the number of messages it can hold in memory. Thus, a node is able to store 500, 5000, 10,000 or an unlimited number of messages. We consider such values to map onto varied day-to-day situations and also to a diversity of mobile devices. As such, Table II shows a comparison over the three communication mechanisms when the Epidemic routing algorithm is employed. Epidemic [13] is one of the simplest forwarding strategies which simply floods the ON with all messages until the destination is reached.

As expected, the congestion of the network increased when using Wi-Fi Direct, as more paths are generated between peers. However, not only does hit rate improve with $\approx$ 5-9%, but latency is decreased with up to 30% (summing up to 4 minutes).

Table III shows a comparison over the three communication mechanisms while running the ONSIDE [10] dissemination algorithm. ONSIDE is a dissemination strategy that leverages information about a node's social connections, interests and contact history, in order to improve hit rate and delivery latency. This is done by carefully selecting the nodes that act as forwarders, instead of simply flooding every node.

Similar to routing, dissemination is also affected by congestion due to more paths being generated in the network, but it gains a significant improvement in hit rate to up to 13%, with latency decreasing with $\approx$ 25% (summing up to almost 4 minutes as well).

Interestingly enough, there is a noticeable improvement in ON performance between WFD1 and WFD2, seeing as Wi-Fi Direct altruistic nodes get a chance to receive their intended messages much faster in WFD2. Unfortunately, we have yet to find a way for balancing AP hosts in real-life as there is no centralized node that can coordinate and decide which node gets assigned as AP next. However, clock-skews in mobile devices might trigger a small degree of randomness when

TABLE II
WI-FI DIRECT INFLUENCE OVER OPPORTUNISTIC ROUTING

Wi-Fi Only	**500**	**5,000**	**10,000**	**Unlimited**
Hit rate	0.37	0.60	0.67	0.72
Delivery cost	84.14	86.80	103.07	55.92
Hop count	22.64	23.35	18.05	9.26
WFD1	**500**	**5,000**	**10,000**	**Unlimited**
Hit rate	0.45	0.62	0.67	0.73
Delivery cost	144.54	196.85	264.70	86.67
Latency (s)	917.54	766.58	750.59	760.11
Hop count	45.70	46.30	42.83	9.69
WFD2	**500**	**5,000**	**10,000**	**Unlimited**
Hit rate	0.47	0.65	0.71	0.77
Delivery cost	145.43	209.94	284.73	89.99
Latency (s)	840.69	681.36	653.99	670.00
Hop count	42.50	43.67	48.82	10.14

TABLE III
WI-FI DIRECT INFLUENCE OVER OPPORTUNISTIC DISSEMINATION

Wi-Fi Only	**500**	**5,000**	**10,000**
Hit rate	0.33	0.55	0.64
Delivery cost	5.67	7.62	6.67
Latency (s)	1,012.55	880.37	866.15
Hop count	25.97	22.43	16.36
WFD1	**500**	**5,000**	**10,000**
Hit rate	0.43	0.61	0.71
Delivery cost	10.38	16.99	19.33
Latency (s)	911.95	755.92	750.49
Hop count	45.39	44.23	38.69
WFD2	**500**	**5,000**	**10,000**
Hit rate	0.46	0.63	0.72
Delivery cost	10.42	17.57	19.02
Latency (s)	834.24	670.62	666.01
Hop count	41.69	42.40	35.73

determining which node is first chosen by the rest of its peers to act as a Wi-Fi Direct AP.

V. Conclusions

In this article, we have proposed a novel mechanism for connecting peers in opportunistic networks over Wi-Fi Direct in a secure and seamless fashion, without requiring any human intervention throughout the process of pairing. Furthermore, we have presented our opportunistic engine implementation over Wi-Fi and have shown how easily it is able to accommodate the addition of Wi-Fi Direct without impacting the battery life of mobile devices. Furthermore, we have empirically proven through emulating real-life user traces that our mechanism improves the performance of ONs by increasing hit rate with up to 13% and reducing latency with 25%, while consuming only an additional 7-8% battery life.

Since we have only tested our proposal through simulations, for future work we would like to deploy the opportunistic engine enhanced with the Wi-Fi Direct connecting mechanism into a new tracing experiment of an even greater scale, in which we can properly observe human mobility and synergic patterns in both infrastructure-based and infrastructure-less opportunistic networks.

Acknowledgement

The research presented in this paper is supported by project MobiWay, PN-II-PT-PCCA-2013-4-0321, and Traffic and Data Offloading in Mobile Networks – TTOff, H2020 as part of Measuring Mobile Broadband Networks in Europe.

References

[1] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic networking: data forwarding in disconnected mobile ad hoc networks," *IEEE Communications Magazine*, vol. 44, no. 11, pp. 134–141, Nov. 2006.

[2] J. M. Batalla, G. Mastorakis, C. X. Mavromoustakis, and J. Zurek, "On cohabitating networking technologies with common wireless access for home automation system purposes," *Wireless Communications*, vol. 23, no. 5, pp. 76–83, Oct. 2016.

[3] Y. Nikoloudakis, S. Panagiotakis, E. Markakis, E. Pallis, G. Mastorakis, C. X. Mavromoustakis, and C. Dobre, "A fog-based emergency system for smart enhanced living environments," *IEEE Cloud Computing*, vol. 3, no. 6, pp. 54–62, Nov 2016.

[4] M. Conti, S. Giordano, M. May, and A. Passarella, "From opportunistic networks to opportunistic computing," *IEEE Communications Magazine*, vol. 48, no. 9, pp. 126–139, Sep. 2010.

[5] R.-C. Marin, C. Dobre, and F. Xhafa, "Exploring predictability in mobile interaction," in *Proceedings of the 2012 Third International Conference on Emerging Intelligent Data and Web Technologies*, ser. EIDWT '12. Washington, DC, USA: IEEE Computer Society, 2012, pp. 133–139.

[6] R.-C. Marin, "Hybrid contextual cloud in ubiquitous platforms comprising of smartphones," *International Journal of Intelligent Systems Technologies and Applications*, vol. 12, no. 1, pp. 4–17, Jul. 2013.

[7] R.-I. Ciobanu, R.-C. Marin, C. Dobre, V. Cristea, C. X. Mavromoustakis, and G. Mastorakis, "Opportunistic dissemination using context-based data aggregation over Interest Spaces," in *2015 IEEE International Conference on Communications (ICC)*. IEEE, 2015, pp. 1219–1225.

[8] A. Merlo, M. Migliardi, and L. Caviglione, "A survey on energy-aware security mechanisms," *Pervasive and Mobile Computing*, vol. 24, no. C, pp. 77–90, Dec. 2015.

[9] "AllJoyn," https://allseenalliance.org/framework, accessed on: 2017-08-24.

[10] R.-I. Ciobanu, R.-C. Marin, C. Dobre, V. Cristea, and C. X. Mavromoustakis, "ONSIDE: Socially-aware and interest-based dissemination in opportunistic networks," in *2014 IEEE Network Operations and Management Symposium (NOMS)*, May 2014, pp. 1–6.

[11] R. I. Ciobanu, C. Dobre, and V. Cristea, "Social aspects to support opportunistic networks in an academic environment," in *Proceedings of the 11th International Conference on Ad-hoc, Mobile, and Wireless Networks*, ser. ADHOC-NOW'12. Berlin, Heidelberg: Springer-Verlag, 2012, pp. 69–82.

[12] "Wi-Fi Direct," https://www.wi-fi.org/discover-wi-fi/wi-fi-direct, accessed on: 2017-08-24.

[13] X. Zhang, G. Neglia, J. Kurose, and D. Towsley, "Performance modeling of epidemic routing," *IEEE Computer Networks*, vol. 51, no. 10, pp. 2867–2891, 2007.