The Open University of Israel

Department of Mathematics and Computer Science

Peer-to-Peer Communication in Wireless Networks as an Alternative to Internet Access

Final Paper submitted as partial fulfillment of the requirements
Towards an M.Sc. degree in Computer Science
The Open University of Israel
Computer Science Division

By

Gary Draishpits

Prepared under the supervision of Dr. Leonid Barenboim

November 2016

Abstract

Peer-To-Peer (P2P) networks exist for a long while now [17]. People use them on a daily basis. BitTorrent, Skype, WhatsApp, and many other popular applications, implement elements of P2P networks [11]. Nevertheless, although wireless technologies, such as Wi-Fi and 3G, exist for years, wireless P2P communications are not common [18] and a simple text message sent via WhatsApp from one student to another, who is sitting in the same classroom, will still go through the Internet using wireless LAN or a cellular network. This paper, presents the reasons for the low popularity of the wireless P2P communications among consumers, analyzes them and presents possible required improvements following which the message will go from device's A wireless transmitter to device's B wireless receiver, without visiting the Internet.

Table of Contents

1 Introduction

1.1 In scope

The purpose of the paper is to examine wireless P2P communications in the real world, specifically among private users. A world where there are many private devices that encapsulate several wireless technologies. For instance, a smartphone or a hand bracelet with cellular, Wi-Fi and Bluetooth communication ports. These devices belong to different owners, are not aware of each other, move around, and consequently, the neighbors are prone to constantly change. A straightforward example is a crowded area, such as a train station or a shopping center where a family member is trying to find another family member with the help of nearby devices.

1.2 Out of scope

The goal is to focus on practical solutions, primarily in the private sector. Theoretical subjects, such as clean environments where there are no security and privacy concerns, will be avoided as much as possible and discussed only if relevant to practical topics. WAN P2P connectivity between dedicated stations, such as building to building, is also not in scope.

2 Current state – General analysis

2.1 Wireless P2P use cases

A good practice being used to examine a technology is to see what use cases this technology brings to the user. The most popular, and we would carefully claim, basing on a search of the Android Play Store [18] and several market leading smartphones, the only ones used so far, are the following:

- The common and straightforward use case of a file transfer from one device to another device.
- Connection of a peripheral device to a computing device. The most popular is Miracast [36] – a wireless display supported by the majority of TV sets.
- Tethering is a use case where one device shares its cellular data connection with other device/s. Using Wi-Fi the sharing device acts as an access point and allows the other devices to connect to it using Wi-Fi. Bluetooth also can be used for tethering. This is achieved via Bluetooth PAN Profile.
- Gaming. A very small number of games are listed as such that offer some P2P experience via Wi-Fi or Bluetooth.

2.2 Could it be implemented earlier?

According to Wikipedia [17] Intel introduced Wi-Fi Direct, in its My WiFi technology by 2008 and Google announced Wi-Fi Direct support in Android 4.0 in October of the following year. Bluetooth, a P2P technology by nature, was invented by Ericson in 1994. It seems that, considering the rapid evolution of smartphones since the introduction of the first Apple's iPhone, and the maturity of wireless technologies, wireless P2P connectivity was not limited by the wireless standards.

2.3 Motivation

As mentioned previously, wireless standards supported P2P communication for quite a while. If so, why there are so few and limited practical implementations?

1.1.1 An alternative to P2P

In order to understand the reasons for limited usage of P2P, let us take a look at the alternative. Why should the message sent from one of the students, sitting in the classroom, go directly to the device of the second student, sitting in the same classroom? The infrastructure of wireless LAN and TCP/IP fully supports the use cases of instant messaging, file transfer and any other data transfer between two peers, using the Internet. With current Internet speeds, the message can go across the world to a server in another continent and return in just a few seconds. There is little Return of Investment (ROI) for developers to develop applications using wireless P2P when the same applications can be easily developed while relying on the Internet.

1.1.2 Cellular operators

A cellular operator is an interesting stakeholder when looking at wireless P2P connectivity. On one hand, when data is transferred using the operator's infrastructure, the operator can charge money for this transfer. That means that a cellular operator should be against wireless P2P connectivity as it causes loss of money. On the other hand, smartphones, and soon to come, wearable and Internet of Things (IOT) devices produce huge amount of data. This data means overloaded networks that require more equipment and more maintenance. Offloading the cellular data should be welcomed, and indeed there are solutions that enable this offloading [14]. The problem is that this offloading is done to wireless LAN instead of wireless P2P connection.

3 P2P Networks vs. P2P

3.1 P2P algorithms and mesh networking

P2P algorithms and mesh networks are the essence of P2P communication. They may hold the answer as to why P2P wireless communications are so rare. For instance, looking at the Structured P2P networks – Content Addressable Network, Tapestry, Chord, etc. As implied by their type, there is some structure that helps locate the data [11]. Every structure must be maintained. Same goes for unstructured P2P networks – Gnutella, BitTorrent, etc. Although called unstructured, there are still super nodes, clusters, etc. that define some level of structuring as well as join, leave and routing procedures. For Internet based P2P networks, that comprise of workstations that are connected through the Internet and their power source is not limited, these networks provide a good solution. However, when the P2P stations are mobile and connected wirelessly, meaning – limited power source (battery) and connectivity is broken every few seconds, these structuring mechanisms produce too much overhead that makes it unusable for mobile wireless P2P connectivity.

This also brings us back to use cases. Mobile wireless P2P connection is, by far, not the ultimate solution for continuous data sharing. The connection may break even before the actual data transmission starts due to the high duration of network join procedure.

3.2 A different mindset

Perhaps we should change the mindset when thinking about mobile wireless P2P connectivity and drop the "network" part. Instead of network with join and leave actions that require routing maintenance, we will think about a group of nodes that are being used for a very short period of time to accomplish a very specific task and "forget" about it once the task is over. There are no Join and Leave procedures, there is no routing. A node's role may be completed once it forwards a message to another node.

3.3 From P2P to Peer-to-Crowd (P2C)

Due to upper network layers, we tend to address wireless communication as P2P. Nevertheless, it is important to remember that wireless communication, even between two peers, is broadcast by nature. There is a collision avoidance mechanism in the Wi-Fi 802.11 standards that makes sure that while the sending peer transmits the data and the receiving side transmits the acknowledgement, the rest of the nearby stations keep quiet. The nearby stations ignore the frames that are not destined for them.

In our case, the purpose of the gossiping is delivering the data to as many peers as possible in the minimum time frame. Therefore, we will mark our frames in such a way that all the nearby stations will know not to ignore our frames, but instead, forward them to the next protocol layer.

2 The Model

Is there really a model where P2P devices can present a valuable alternative to the Internet? The keyword of this question is “valuable”, as basically the Internet is a data exchange framework. There are enough routing algorithms for P2P networks and they can definitely be used for data exchange. Nevertheless, Internet prevails. The reason for that is very straightforward – there is no need for alternative.

If so, what is the purpose of this paper?

We claim that there is indeed no need to replace the Internet, for most purposes. However, there are specific use cases where the P2P framework presents a better backbone for data exchange.

Let us examine a few examples.

2.1 Use Cases

2.1.1 Local Area Emergency Search

The Police is looking for a suspect on a train station or an airport. Time is critical and the policemen need help from the surrounding public. A policemen sends a message that is received by people around and anyone who saw the suspect can immediately call the police. An obvious remark will be – “such a message may probably cause panic…” This is indeed a problematic situation. We will address this more in the section that deals with security aspects. For now, let’s say that the message will be encrypted and only the people with Need-To-Know credentials, such as the airport security personnel will be able to decrypt it.

2.1.2 A Lost Pet

When someone is losing their pet, the first thing they would do is search around the neighborhood, perhaps ask around and hang posters asking for anyone who may have seen their animal friend, to call them.

Can the Internet help here? Unless we have enough email addresses of people that live in the neighborhood or some social network page or a website of the neighborhood where enough people from the neighborhood visit, the Internet is not much of an assistance here.

What if we could walk around the neighborhood, and "ask around" by sending P2P messages from our smartphone to the people in the neighborhood? As we walk by, our smartphone will send a message to any peer device it can find. This message will contain a brief information about the fact that we are looking for a pet and our telephone number that one can call in case they've seen it.

2.1.3 Localized Advertisement

We see several variations of this use case in many futuristic movies. A person walks into a mall and starts receiving data about the special offers from the different stores in the mall. We can solve it using the Internet by placing advertisement posters inside the mall encouraging the shoppers to download the mall's or a store's app.

There is also a second view of this use case and it is from the point view of the shopper. Shoppers may want to share their experience with other people in the mall. Perhaps to return a favor to some nice merchant, share about a good product they have found, perhaps warn other shoppers of a dishonest seller or even ask if someone knows where some product can be found within this mall.

2.1.4 Localized "Chat-Room"

Enhancing the second part of the "Localized Advertisement" presents a different use case. In this UC, people are discussing, sharing opinions and basically chatting with people who are located in the same area. For instance, a shopping mall, a sports arena during a game, traffic jam, etc.

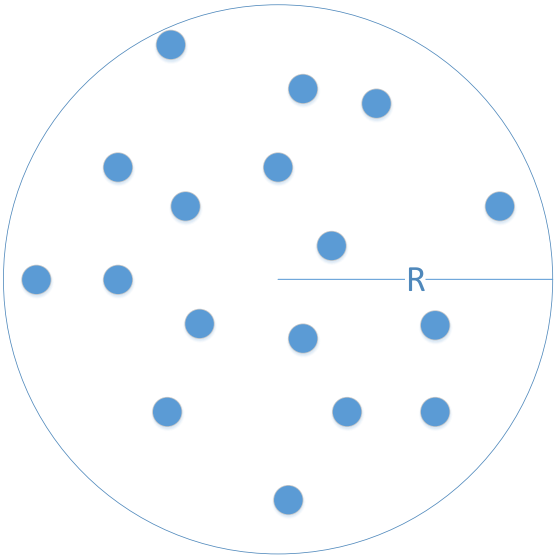
This will be similar to a WhatsApp group messaging or a forum thread, but instead of every participant registering to a centralized service, the service will be defined by geographical borders.

2.2 The Basic Model

The readers may have noticed that the use cases deal with a localized area and/or people that do not know each other.

We believe that these are the areas where wireless P2P communication can be a valuable alternative to the Internet.

Therefore, the model we propose is as follows –



- N number of nodes in a localized area covered by the R radius.
- The nodes are not familiar with each other and are not necessarily aware of each other.
- There is no centralized controlling entity.
- All nodes are independent and considered equal.
- The nodes are mobile and may move at any direction at any given time.
- A node communicates with one peer at a time.

2.3 Gossiping

The described use cases remind the most common way of human communication – gossiping. Gossiping is spreading rumors, or information in our case. The spreading of the information is unmanaged, practically uncontrollable, yet very efficient.

There is a theory that claims that one of the things that significantly contributed to the evolution of the human kind and its undeniable domination on Earth is our ability and urge to gossip.

There are Gossip protocols and algorithms that are designed particularly for the purposes of data sharing in environments that are very similar to those we discuss in this paper. Nevertheless, many of the propositions that rely on gossiping still try to maintain a structure while managing the network and the routing between the nodes.

In this paper we strive to remain as close as possible to the basics of human gossiping – spread the information without much caring who and where it reached. Having stated that, this is still about computer science and SW engineering, so we are going to be responsible and attempt to define some rules that will prevent information looping and flooding.

2.4 Limiting Data Propagation and Flooding

2.4.1 Basic Algorithm

```
- Aj: Choose a neighbor Bi.
- Aj: Send the message to Bi.
- Bi: Decide whether to –
    o Drop the message.
    o Forward the message.
```

2.4.2 Problem 1 – Choosing the next neighbor

Naturally, we won't send the same message twice to any node. There are quite a few articles [4] that discuss and propose different algorithms for choosing a neighbor.

2.4.2.1 Signal Strength

A node with a good signal strength is a good candidate as it means it is nearby and will most probably be able to receive the message in full before disappearing (we assume that nodes are in constant movement).

2.4.2.2 Battery

The next neighbor may be the one that has the largest remaining power. Power means that there is a good chance that this node will keep forwarding the message further.

2.4.2.3 Not Interested Mode

A node may be in a "Not Interested" mode that will inform the sending node that this particular node is not interested in receiving messages. This may be due to specific user configuration.

2.4.3 Problem 2 – Deciding whether to forward or drop the message

2.4.3.1 Time to Live (TTL) as Hop count

TTL or Hop counter is a very basic argument that will be configured by the original sender. Every receiver will drop the message in case the TTL reached its limit.

2.4.3.2 Timeout

Use time to decide when to stop forwarding the message. If the time when the message has started its journey plus the Timeout is greater than the current time, don't forward it anymore.

2.4.3.3 Second Delivery

Drop a message if it was already received and processed before.

2.4.3.4 Flooding

A station may decide not to forward a message in a case when it is receiving too many same messages from the surrounding peers. The "too many" number will be specific to an implementation.

2.4.3.5 Power Saving

A node may drop a message in case it has low power and cannot afford itself the processing and/or forwarding of the message.

2.4.3.6 Unreliable Sender

If there is a setting demanding sender verification and such verification cannot be performed, the message may be dropped.

2.4.3.7 User Configuration

A user is the ultimate master of the device and shall be able to configure some rules that will assist in deciding whether to forward the message or not.

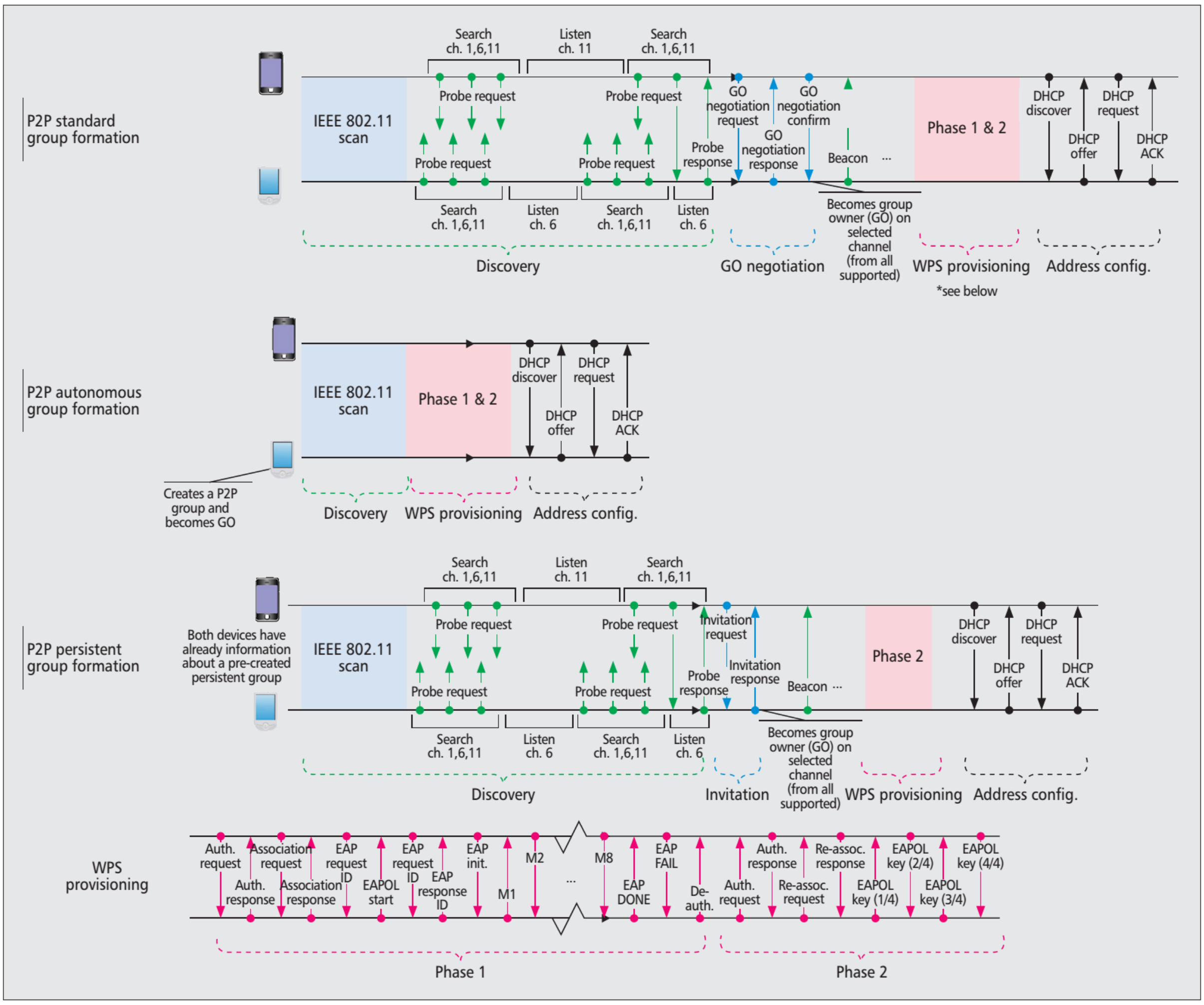
2.4.3.8 Corrupted Message

If the message is corrupted, drop it.

3 Wi-Fi Direct

3.1 Analysis

The following diagram [7] summarizes the different processes for WFD connection establishment.



If a device wants to send a message to another device via WFD, the minimal conditions that must apply are the following –

1. Both devices should be listening over the air.
2. Both devices should find each other.
3. One device should initiate the connection and the other accept it.

This simple algorithm produces a very simple yet significant problem. A device that needs to distribute a message, will not be able to do that, simply because other devices in the area are not proactively listening and thus they will never find each other. It is very possible that a device that will scan for WFD devices in a dens area, like an airport, will not find any device.

3.2 Proposed Changes

Following are several changes we propose in Wi-Fi protocols and features that will allow and/or improve to use P2P communication to spread information in a much more efficient way than it is allowed today.

Some of the proposed changes can be applied together, while for others, coexisting with other changes is more challenging.

3.2.1 Security

We discuss specific security aspects and propose solutions in the Security section. For instance, a station may consider some security measures in order to validate the identity of the sender before connecting to it.

Nevertheless, the main purpose of the data transfer is spreading the information to as many endpoints as possible. Due to that, we consider the data itself, for the majority of the cases, as not confidential and propose a few changes based on this assumption.

3.2.2 Scanning

Following the previous section we understand that in order for a device to participate in any WFD communication, it should be scanning the air. There are 2 methods of scanning – Active, when the station is actively asking who is around by sending a "Probe Request" frame; and Passive, when the station is only listening to the Beacon frames that are being sent by the Wi-Fi Access Point or a Wi-Fi Direct peer.
An active scanning method shall be applied in a station that wants to transfer data. A passive method shall be applied in a station that does not need to transfer any data, but is willing to receive any WFD messages.

3.2.3 WFD GO

It is very apparent that the station that wishes to spread the information should be the Group Owner and the receiving station should be client. That means that we shall follow the "P2P Autonomous Group formation" where the station creates a group as GO prior to connecting to another station. This will save us the phase of "GO Negotiation".

3.2.4 WFD WPS Provisioning

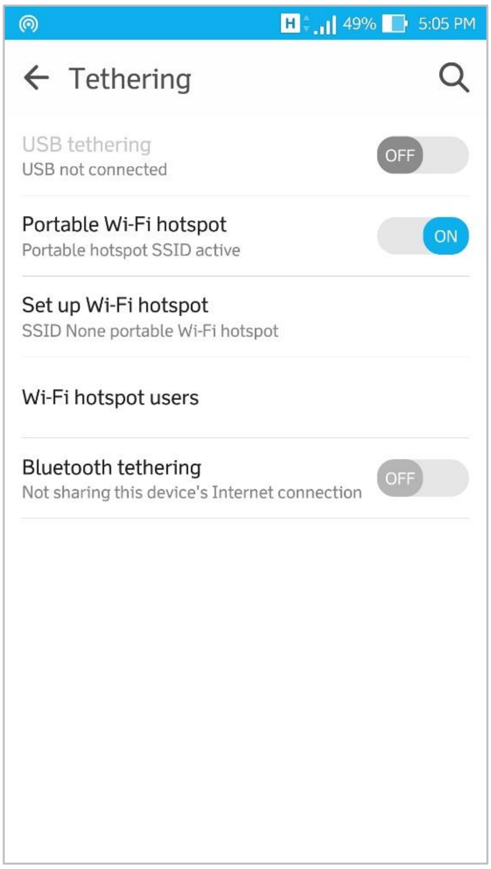
We have mentioned previously that the nature of the use cases we intend to solve is such in which we want to share the data, rather than protect it. That means that securing the connection between every two peers is not mandatory and in most cases may be dropped. Thus, the two WPS provisioning phases are not required.

3.2.5 Tethering

Tethering or Soft-AP is when a client device, such as a smartphone, acts as a Wi-Fi Access Point and allows other client devices to connect to it and use its Internet connection.

For our purposes, we introduce a special tethering mode. When a device needs to transfer data to its surroundings, it shall enable tethering and send beacon frames that contain a special additional information that will signal to other stations that there is some piece of data that we would like to share. There are several propositions for embedding new information within the beacon frame [5]. Another flag will be added to indicate whether the sending device also supports the traditional tethering for the purpose of Internet sharing.

Stations that are interested in receiving the information will connect to the Soft-AP of the sending device using standard Wi-Fi BSS connection flow and receive the data.



H 49% 5:05 PM

Tethering

USB tethering
USB not connected
OFF

Portable Wi-Fi hotspot
Portable hotspot SSID active
ON

Set up Wi-Fi hotspot
SSID None portable Wi-Fi hotspot

Wi-Fi hotspot users

Bluetooth tethering
Not sharing this device's Internet connection
OFF

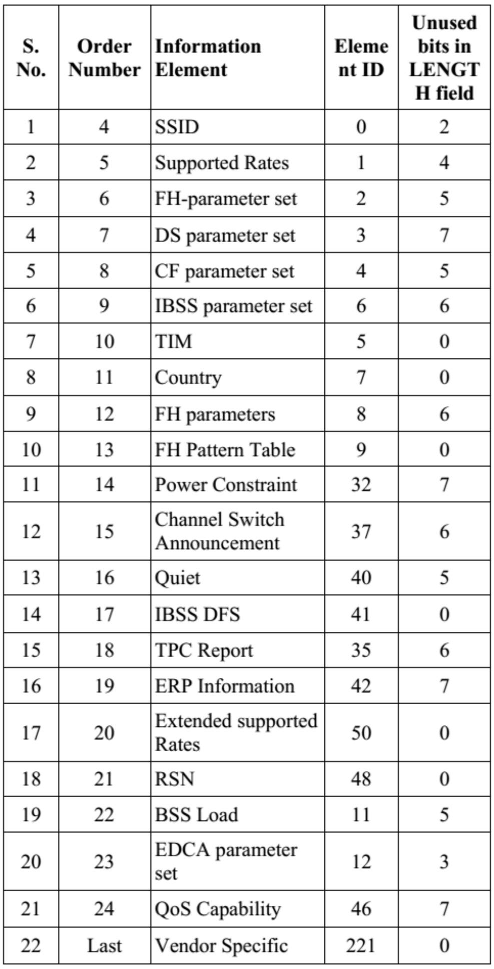
Figure 1 – Android Tethering Settings Menu

3.2.6 Broadcast

We have mentioned that the data we want to spread is not confidential. Also, wireless communication is basically a broadcast over the air. All surrounding stations hear the broadcast, check the destination and ignore the frames that are not destined to them.

Since our goal is to spread the information as much as possible, stations shall not ignore the message, as long as it doesn't contradict the conditions for dropping the message we described earlier.

Unicast frames shall be marked in some way to notify the stations that they should not ignore these messages. If the frames are sent as broadcasts the frames will need some marking as well to be identified as specific P2P frames.



S. No.	Order Number	Information Element	Eleme nt ID	Unused bits in LENGT H field
1	4	SSID	0	2
2	5	Supported Rates	1	4
3	6	FH-parameter set	2	5
4	7	DS parameter set	3	7
5	8	CF parameter set	4	5
6	9	IBSS parameter set	6	6
7	10	TIM	5	0
8	11	Country	7	0
9	12	FH parameters	8	6
10	13	FH Pattern Table	9	0
11	14	Power Constraint	32	7
12	15	Channel Switch Announcement	37	6
13	16	Quiet	40	5
14	17	IBSS DFS	41	0
15	18	TPC Report	35	6
16	19	ERP Information	42	7
17	20	Extended supported Rates	50	0
18	21	RSN	48	0
19	22	BSS Load	11	5
20	23	EDCA parameter set	12	3
21	24	QoS Capability	46	7
22	Last	Vendor Specific	221	0

Figure 2 – Compiled data of number of free bits in LENGTH field of all Information Elements [5].

3.2.7 Cancelation of Acknowledgments

There are several reasons for a station, receiving a message, to decide to ignore it and not to forward. In case it does decide to forward the message, it will start broadcasting it soon after receiving it. It is very likely that the original station will still be around to hear the broadcasts of the new station. One such broadcast will be enough to notify the originator that its message has started distribution by other peers.

4 Wi-Fi Aware

4.1 Description

Wi-Fi Aware [24], also known as Wi-Fi Neighbor Awareness Networking (NAN), is a new development of the Wi-Fi Alliance. At the time of writing these lines (August 2016), Google Scholar [27] as well as IEEE Xplore [26] list no papers related to Wi-Fi Aware technology.

In order to help understand what is Wi-Fi Aware, we quote here a few scenarios, from "Wi-Fi Aware™: Better Proximity Technology for Personalized Experiences" [25] by Wi-Fi Alliance.

Figure 3 - Wi-Fi Aware usages

> *"A user attending a concert receives alerts of friends present in the arena, and if his settings allow, alerts him to their location. He then sends a brief message to nearby friends to agree on a meeting location. This device-to-device discovery process does not require connection to a Wi-Fi hotspot. However, the user may want to go beyond the basic information exchange to share a photo of the band. In this scenario, the application is able to establish a Wi-Fi Direct or infrastructure connection and ultimately enable a "see what I saw" application."*
>
> *"A user is walking through a large farmers market with hundreds of booths, and she downloads a Wi-Fi Aware-based "Farmers Market" application and subscribes to notifications for specific products or discounts. As she walks through the market, her phone alerts her when she is near a booth with the produce that is of interest and on sale. If the farmer is running a special discount, she can immediately get more information. Other types of applications enable businesses or brands to become more engaged in the consumer experience or deepen their customer knowledge by offering services or tailoring promotions based on the customer's preferences. Then a user with a "Personal Shopper" application to which he has personalized preferences, could walk through a retail mall and as he pauses by store windows or displays, the phone automatically send alerts about discounts on preferred brands or items of interest. Venues, municipalities, and service providers will also leverage Wi-Fi Aware applications for proximity-based advertising and revenue generation services that deliver personalized information to target customers at the appropriate time and location."*

It seems that Wi-Fi Aware offers a connection that, similarly to Bluetooth Low Energy based sensors, starts with periodic beacon broadcasts that announce to nearby Wi-Fi Aware stations of some service offered by the beacon transmitter.

An interested station will subscribe to the service provider or connect using legacy Wi-Fi BSS or Wi-Fi Direct for further information (Figure 4).

According to Figure 5 it is apparent that it will also be possible to request a service and in case a service provider is around, it may offer the service to the requestor.

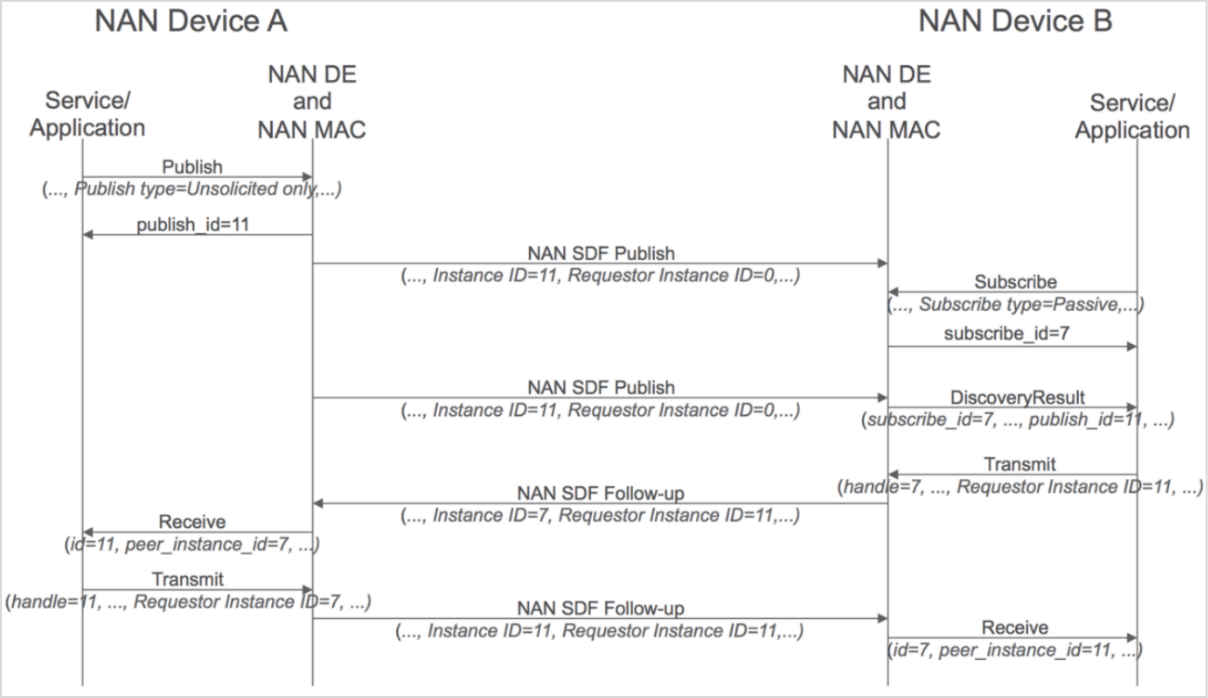

NAN Device A
NAN Device B
Service/ Application
NAN DE and NAN MAC
NAN DE and NAN MAC
Service/ Application
Publish
(..., Publish type=Unsolicited only,...)
publish_id=11
NAN SDF Publish
(..., Instance ID=11, Requestor Instance ID=0,...)
Subscribe
(..., Subscribe type=Passive,...)
subscribe_id=7
NAN SDF Publish
(..., Instance ID=11, Requestor Instance ID=0,...)
DiscoveryResult
(subscribe_id=7, ..., publish_id=11, ...)
Transmit
(handle=7, ..., Requestor Instance ID=11, ...)
NAN SDF Follow-up
(..., Instance ID=7, Requestor Instance ID=11,...)
Receive
(id=11, peer_instance_id=7, ...)
Transmit
(handle=11, ..., Requestor Instance ID=7, ...)
NAN SDF Follow-up
(..., Instance ID=11, Requestor Instance ID=11,...)
Receive
(id=7, peer_instance_id=11, ...)

Figure 4 - "[24] Figure 4-4: Unsolicited Publish Command Data Flow"

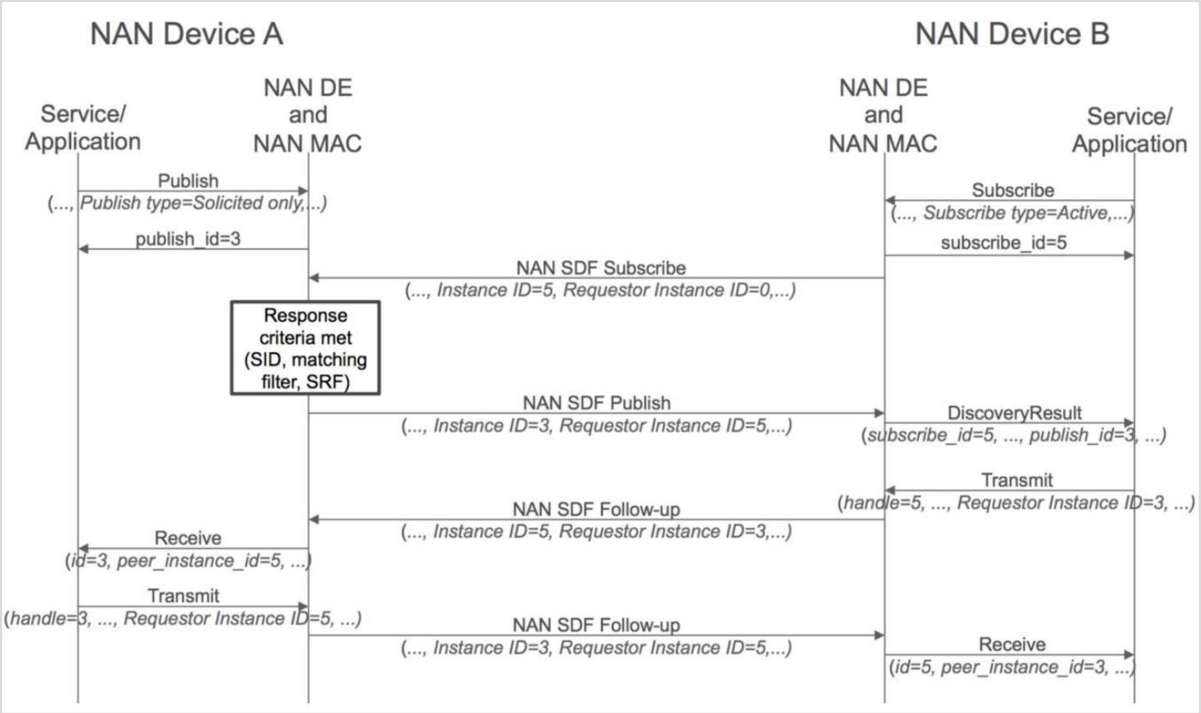

NAN Device A
NAN Device B
Service/ Application
NAN DE and NAN MAC
NAN DE and NAN MAC
Service/ Application
Publish
(..., Publish type=Solicited only,...)
publish_id=3
Subscribe
(..., Subscribe type=Active,...)
subscribe_id=5
NAN SDF Subscribe
(..., Instance ID=5, Requestor Instance ID=0,...)
Response criteria met (SID, matching filter, SRF)
NAN SDF Publish
(..., Instance ID=3, Requestor Instance ID=5,...)
DiscoveryResult
(subscribe_id=5, ..., publish_id=3, ...)
Transmit
(handle=5, ..., Requestor Instance ID=3, ...)
NAN SDF Follow-up
(..., Instance ID=5, Requestor Instance ID=3,...)
Receive
(id=3, peer_instance_id=5, ...)
Transmit
(handle=3, ..., Requestor Instance ID=5, ...)
NAN SDF Follow-up
(..., Instance ID=3, Requestor Instance ID=5,...)
Receive
(id=5, peer_instance_id=3, ...)

Figure 5 - "[24] Figure 4-5: Solicited Publish Command Data Flow"

4.2 Further Analysis

4.2.1 Possible Complexities

Going over the NAN technical specification v1.0 [24], we couldn't help but notice some structure complexity with quite a few roles and topologies –

- NAN Device
- NAN Cluster
- NAN Master
- NAN Anchor Master

As in most cases where there are structures with several roles, there are also defined procedures for role switching and transitions –

- NAN Non-Master to Master Role Transition
- NAN Non-Master Sync to Non-Master Non-Sync State Transition
- NAN Non-Master Non-Sync to Non-Master Sync State Transition
- NAN Cluster Initiation and Selection
- NAN Cluster Merging

It is not entirely clear what are the exact purposes of the additional possible complexities. Another question concerns the spread of information beyond the NAN cluster – can a station continue distributing the information once it was received from the service provider, i.e. can we continue "spreading the rumors" or is the original publisher the only one who is allowed to do so.

As Wi-Fi Aware is a new development, we will have to see what will be the adoption scale and the specific implementations.

4.2.2 Internet is still a rival

We would like to point out that in our opinion, the examples of Wi-Fi Aware usages, brought as new possibilities are somewhat misleading. We believe that there is no real benefit for developers to invest in Wi-Fi Aware in order to solve some of the described use cases as these are easily solved using the Internet.

A simple application that knows the location of the device, knows the friends of the user and fetches their location from the cloud, can easily identify that the friends of the user are nearby, alert him and direct to their exact location using the GNSS.

If there is no Internet connectivity, an application may use the existing Wi-Fi Direct to solve this problem. Why is it simple to solve using existing technologies? Because they are friends, they know each other and it is always easier in cases where users know and probably trust each other. It becomes difficult when users and/or devices that want and/or need to communicate are strangers.

4.3 Proposed Changes

After mentioning a few questions and concerns, we must admit that some of the ideas of this technology are similar to those proposed in this paper and we think that Wi-Fi Aware is definitely good and welcomed news.

Once Wi-Fi Aware will be commercial, some of the use cases that we have mentioned as those where wireless P2P has the advantage over the Internet, will be easier to solve. Following are several areas where we think Wi-Fi Aware implementations should focus on. These are in addition to the ideas that were proposed in the previous sections.

4.3.1 Spreading the Rumor

We believe that it will be beneficial to allow a station that received some piece of information from a publisher to continue spreading this information further. If a person is looking for their pet in the neighborhood, Wi-Fi Aware will definitely help that person to distribute their information to whoever they find around. If, however, the receiving stations/users will be allowed to continue spreading the information further, it will reach a much wider circle and help the original publisher to find their pet.

4.3.2 All Nodes were created as equals

Wi-Fi Aware defines several roles and methods for switching the roles between the stations. We trust the authors from Wi-Fi Alliance that these roles were created for important reasons. Nevertheless, roles and role switching mechanisms always produce additional delays. These delays have direct impact on response time.

When two people meet and exchange information, before proceeding on their routes, they don’t have any protocol that states that one should become a group owner or a master before saying whatever they want to communicate.

We believe that wireless P2P communications in a mobile environment should strive for the same communication model, one where all nodes are equal.

4.3.3 Structures

As we have stated throughout this paper, any networking structure produces a timing and maintenance overhead, delaying and reducing the real data for which the structure was initially formed.

In addition to reduction and even cancelation of specific roles within the network, any reduction of structures will speed and enlarge the amount of data exchange. Once the subscriber received data from the publisher, it is probable that the connection is no longer needed.

If there is a possibility for further data exchange, there may be a rational to continue it using the legacy connectivity methods via the Internet, instead of maintaining Wi-Fi Aware clusters.

5 Bluetooth

5.1 Analysis

In order to develop a way for utilizing Bluetooth in the aforementioned use cases, we first need to understand why there is a need for Bluetooth at all. There is Wi-Fi and LTE that support wireless P2P communication on a licensed and unlicensed bands. What is the purpose for Bluetooth?

Some of the reasons for Bluetooth existence are, as often for many technologies, historical, and therefore not interesting for this paper.

Bluetooth offers a wireless P2P communication that does not rely on the TCP/IP family of protocols. Instead, it defines a number of Personal Area Network (PAN) usages, such as file transfer, headset, peripheral device, etc. These usages defined by Bluetooth profiles [30] –

- Advanced Audio Distribution Profile (A2DP)
- Object Push Profile (OPP)
- Personal Area Networking Profile (PAN)
- Phone Book Access Profile (PBAP, PBA)
- Hands-Free Profile (HFP)
- Human Interface Device Profile (HID)
- …and many more

5.2 BLE

Bluetooth core specification version 4.0 introduced a new concept – Bluetooth Low Energy (BLE), sometimes referred to as "Bluetooth Smart".

BLE supports "Advertising", where a station broadcasts a limited amount of data, periodically. These transmissions do not require a connected peer and share the data to any station that is close enough to receive it.

The advertisement packet indicates whether the broadcaster supports connection and may be approached for a direct connection, or it may not support connections and the data broadcasted is the only data it will share.

An advertising packet may be up to 31 bytes and are being broadcasted at a fixed rate defined by the advertising interval, which ranges from 20ms to 10.24s.

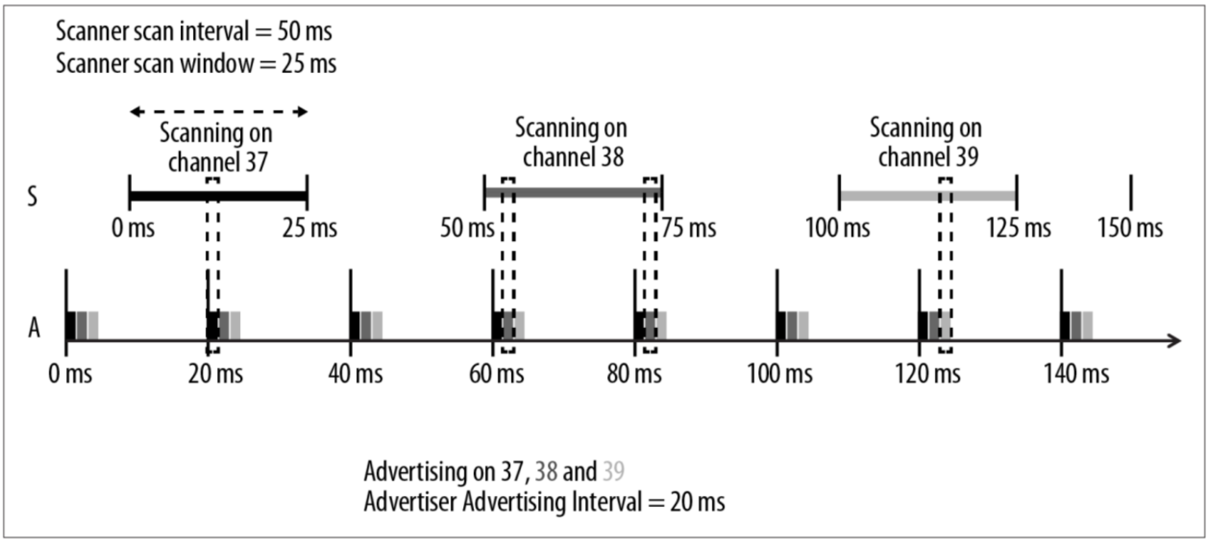


Figure 6 - [31] Advertising and Scanning

5.3 Proposed Changes

5.3.1 BLE

Since BLE supports periodic broadcasting out of the box, it is apparent that we shall rely on it for the aforementioned use cases, and not the standard Bluetooth that requires a connection establishment prior to any data exchange.

5.3.2 Advertisement payload reuse

As we have mentioned, the actual data that an advertisement packet may carry is 31 bytes which are 248 bits. 248 bit represent approximately 10^{80} different values. That’s about 10 billion values for every person on Earth.

If there is an Internet connection available at the time when a station decides to broadcast a gossip, it may generate a 248 bit string which will translate to a URL using some service that is used for this purpose.

A station that receives such advertisement will use this web service to translate the 248 bit string from the advertisement to a URL and will browse the URL for further information.

Most probably, we will have to reserve a few bits for the purpose of identifying the data – a hashed URL, an actual string message or else.

5.3.3 Advertisement payload increase

Currently the advertisement payload is limited to 31 bytes. A straightforward solution to this limitation is its cancelation. If we increase the payload, we increase the data we transmit and the advertisements will carry a full message.

5.3.4 Transmission pattern

An additional possible improvement may be that instead of increasing the length of the payload we change the pattern of the transmissions. Meaning that the advertisement will contain the following information –

- Remaining length of the payload
- A flag indicating if this is the first advertisement or a following one with the continuation of the data

This way we send one advertisement and then we send several frames with the data. Since the pattern will be repeated again and again, the scanning stations around will be able to understand when should they scan in order to catch the first packet.

6 Cellular

6.1 Analysis

6.1.1 Cellular Operator is a Business

There are very few grown up people on the planet that are not familiar with cellular phones. The number of yearly sold phones has surpassed that of the personal computers. Nevertheless, there are probably very few people on Earth, if any, that have ever used a cellular connectivity to communicate between two devices P2P, without a base station.

We believe that the main reason for that is not technological, but economical. A cellular provider is a business and its main goal is to produce profits. Customers expect the cellular coverage to be present wherever they go and will not be happy if they can't place a call or chat with their friends and family.

That means that a cellular provider cannot rely on P2P communication, which essentially relies on 3rd party HW. It makes more sense that a cellular provider will add a cellular antenna where such is required rather than developing solutions that are based on client devices for which the level of services cannot be guaranteed.

6.1.2 Legal Aspects

6.1.2.1 Users

In order for a cellular provider to use the device of user A as the data channel between users B and C, it must inform user A of this activity and possibly have a signed business agreement with A.

Same goes for users C and B. We are not legal experts, nevertheless it seems appropriate that users should be aware of the fact that their data and conversations passes not only through the cellular provider network, but also via a 3rd party devices.

6.1.2.2 Roaming

Unlike Wi-Fi and Bluetooth that operate on unlicensed bands, cellular connectivity is licensed. That means that users A, B and C may have contracts with three different operators. That, in turn, requires the operators to have a business agreement that allows this type of communication.

6.1.3 Security Aspects

The straightforward evolvement of the legal aspects that we have discussed previously are security concerns. Once a data of user B passes through a device of user A with which user B has no relationship, the data may be compromised and thus must be protected.

Throughout this paper we have mentioned that since we want to spread the information to as many peers as possible, the data itself is public. Why would we protect it in this case?

We must protect the data in this particular case as the cellular operator is a business and its services must be reliable. If a 3rd party node alters the data, users will stop using the service provided by the operator and some will probably submit a lawsuit against the provider.

6.1.4 Design Aspects

Cellular connectivity is wireless and is primarily designed to work between a client – a cellular phone and a base station.

6.1.5 LTE-D

LTE-D, which stands for LTE direct, proposes device-to-device (D2D) communication between devices using LTE. It is part of the 3GPP international standards, defined in Release 12 of 3GPP and currently known as Proximity Services or ProSe [23].

As LTE, LTE-D uses spectrum that is licensed to a network operator which can control the devices and beacons that access the spectrum. As often, control and management on a licensed spectrum simplify some aspects, such as load sharing, security and standardization. At the same time it produces some issues as well, such as network latency, legal difficulties and mandatory priory preparations that require the devices and/or users to have some kind of service agreement with the network provider.

As with Wi-Fi Aware, current papers and propositions for LTE-D discuss service based mode of operation for the technology, mainly talking about Application layer communication that utilizes LTE-D for its purposes.

6.2 Proposed Changes

Most of the different propositions that we have proposed for Wi-Fi, we can implement for LTE as well. For example, we may implement a Soft Base Station service, similarly to Wi-Fi Soft AP where devices connect to another client instead of the Base Station and receive the gossip frame.

The main question is probably – do we want to introduce changes to cellular on licensed spectrum? As already mentioned, cellular operator is a business and there are many non-technical difficulties with P2P communication over licensed channels.

We will have to wait and see how LTE-D will evolve, but currently it definitely seems like an interesting development that will open the door for P2P and P2C over the cellular.

7 Autonomous Vehicles

There are many news lately about autonomous vehicles, especially self-driving cars. These cars will have a large number of sensors in order to sense the surroundings and avoid collisions. In addition to the sensors, they will also use P2P communication for the cars to communicate with each other. Naturally, this communication will be wireless.

Why would cars want or need to communicate with each other? The reasons are basically the shortcomings of sensors. Sensors are usually limited by distance. Essentially, that means that a car may sense a vehicle that is driving next to it, but it will not sense a vehicle that is located 50 meters away behind a nearby truck.

Once every vehicle transmit their location, all vehicles will have a snapshot of the road within a defined radius. A car will know what kind of vehicles are driving nearby, how many are there, what speed every vehicle is going, are there any obstacles ahead, and so on.

IEEE 802.11p amendment to the 802.11 standard defines Vehicle to Vehicle (V2V) communication. There are two main reasons why this amendment, and V2V communication in general, are interesting to this paper –

1. V2V communication is P2P and wireless.
2. Vehicles are traveling at higher speeds than walking humans.

That means that a solution that is good enough for V2V communication, should be satisfying for P2P communication between nearby devices traveling at speeds that are lower than those of the vehicles.

A possible drawback may be that personal owned devices, such as smartphones and wearable do not support 802.11p. An answer to this problem will be that in order to enhance the usability and safety of autonomous vehicles, there is also a need for Vehicle to X communication, where X may be an infrastructure node, such as a traffic light, or a pedestrian. A smartphone of a person will be able to receive messages from nearby vehicles, for example – a speeding car with malfunctioning breaking system. In the other direction, a car will receive a notification from a pedestrian's smartphone that is crossing the street, perhaps in a location without a designated pedestrian crossing area.

8 Combination of Technologies

8.1 Introduction

This section is probably the most important section of this paper. We have listed and described several wireless technologies that, with some changes, can provide a useful backbone for P2P and D2D communication. There are also new standards (Wi-Fi Aware and LTE-D) being defined these very days that specifically address wireless P2P communication solutions for different usages and use cases.

We believe that the future of wireless P2P/D2D communication lies in the collaboration of the different technologies – Wi-Fi Direct, Wi-Fi Aware, LTE-D, Bluetooth and also the Internet.

We list here a few use cases that will emphasize the benefits of such collaboration.

8.2 Use Cases

8.2.1 A Lost Wearable Device

A wearable device is something people are wearing on their body. One good example is a smart watch, smart glasses or a jewelry bracelet. Wearable devices vary from each other with regards to the types of connectivity technologies embedded within them. Smart glasses may support a full Wi-Fi stack with the ability to connect to a Wi-Fi Access Point, a smart watch will support only Wi-Fi Direct and a smart jewelry bracelet may support only Bluetooth BLE.

What happens when the bracelet is lost? If it has GNSS and Wi-Fi or a 3G modem embedded, it may send a message to the owner's e-mail account with its location. Nevertheless, if it has only Bluetooth BLE, it will not be able to send any such message.

A possible and a useful solution is the following – once the bracelet identifies in some way that it is lost (for instance – via movement sensors plus time of day plus user configuration), it will start sending periodic beacons via BLE with request for help. A passing nearby smartphone, that encapsulates Bluetooth, Wi-Fi, LTE modem, GNSS and many more technologies, picks up the transmission and sends the owner of the bracelet a message with the exact location where it picked up the message.

The email address of the bracelet’s owner will be sent by the bracelet to the smartphone. The location will be added by the smartphone and of course the message will be sent using Wi-Fi or LTE of the smartphone.

This transmission may take place even without the knowledge of the smartphone user.

Naturally, this use case may be extended further to help locate not just a belonging but also a missing person or a pet.

8.2.2 Notification via P2P, Data on the Cloud

Throughout this paper we mention again and again the concerns of wireless P2P communications. Devices may move rapidly, a fact that may cause the connection drop before the actual data passes. One of the others major concerns is security which we devote a full section in this paper.

In order to address the mobility of the devices and the security concerns that evolve from such mobility, we may consider using P2P connection only for an introduction and for sharing the very basic information that will lead to the data, but not share the data itself through the P2P link.

For instance, a device will communicate a message describing a type of service, such as advertisements in a shopping mall, request for assistance or a general message related to the surrounding area. The data itself, however, will not be included in the message. Instead the message will include only the link to the data that users and devices may access using their Internet connection.

8.2.3 Signal Extender

This use case is already partially available using tethering. A new way of cellular and Wi-Fi collaboration may be in the following use case.

A device is having low cellular reception in some are of a structure, such as a restaurant or similar. The user will use Wi-Fi Aware to look for a nearby device that has a good LTE reception and is willing to be used as a proxy.

Once such a device is found, the first device will connect to the second via Wi-Fi Direct or Wi-Fi Aware and will use this communication channel for its LTE connection.

8.2.4 Fast Connection

Once devices establish a connection using one technology, they shall exchange details regarding the other connections. That way, when the devices are far from each other they may use LTE-D. Once they get closer they will use LTE-D to exchange the connection parameters for Wi-Fi Direct and will later switch to Wi-Fi Direct and even Bluetooth. Same goes the other way around – close devices may start communicating over Bluetooth and switch to Wi-Fi Direct and then to LTE-D once the distance increases.

8.2.5 Simultaneous Connections

In cases when a device has several connectivity technologies, it shall use as many as possible in order to transfer data to as many peers as possible at once. In this way, a device will connect to peer A using Wi-Fi Direct, to peer B using LTE-D and to peer C using Bluetooth. All connections will occur during the same time frame so the information will be spread to three peers instead of one.

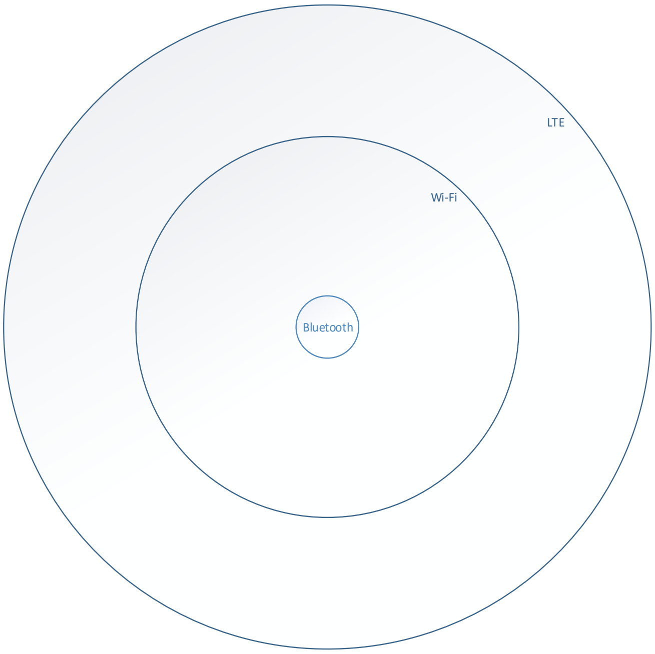


Figure 7 - Multiple Connections

In cases when the data is too large to fit into a frame of one technology, and there is no Internet connection available, the sender may use another technology to transfer the additional data. For example, it will use Wi-Fi to transfer the first half of the data and LTE for the second.

9 Security

9.1 Data Propagation Abuse

9.1.1 Brute Advertising

There are probably no people on earth who own a computing device, such as a personal computer or a smartphone, and did not receive some kind of spam message. An email message, an SMS, enormous amount of ads on every web page, so on and so force…

Every new type of communication is another channel for the advertisers to reach possible consumers. Naturally, there are two main problems to solve here. The first one, is how do we limit the amount of advertisements so it will not consume the data channel and force the user to simply stop using it? The second problem is the opposite – how do we allow users to receive relevant advertisements that will benefit them.

Every email provider offers a spam folder and some kind of AI engine to filter out spam messages. Google and Facebook keep track on users search history and display users ads based on their recent activities over the web.

So what can we do with wireless P2P channels?

One of the most efficient methods is regulation. A new message type will be standardized as an advertisement. Messages with commercial content will have to be marked as such, down to the MAC layer, so even the FW running on the wireless NIC will be able to drop such frames based on the configuration of the user. On the other hand, a user shall be able to accept advertisements when this is appropriate. For instance, when visiting an area such as a shopping mall. When a person going around a shopping mall it is very probable that this person will benefit from messages sent from the surrounding shops or by the mall's system.

We believe that, as always, the key to a Win-Win situation is transparency and balance. If users know what is going on and able to control the flow of data, everybody will benefit. If, on the contrary, users will be left in obscurity and/or will not be able to control the amount and the sources of the advertisement content, they will simply cancel this communication channel.

9.2 Peers identification

9.2.1 3rd Party Approver

As in TLS secured web traffic there is a 3rd neutral side whose role is to verify and authenticate one or both sides of a transaction.

A train station is identified as registered and validated entity, thus peers may trust it. The same way an information center announces a vocal message to the public at the train station, it may send a P2P message to their personal computing devices. Its identity is validated and identified as legitimate and may be processed without invoking the Application layer.

The simplest way to confirm an identity of the peer is using the Internet. We may be getting a message from the train station or the shopping mall via P2P, but since we also have an Internet connection, why not use it and make sure these messages are indeed from a reliable and authentic source.

A sending entity will purchase a certificate from a known CA and will sign all its messages with its private key. Any station receiving the message will be able to open the message using the entity’s public key. Of course we need to have the public key and either use an Internet for that or have all possible keys in advance.

9.2.2 Data Protection

The data we want to spread is not confidential. Due to that, we have the possibility of not securing the communication channel and speed up the pass of data. This brings a security concern – how do we ensure that a malicious node will not alter the content of the message?

9.2.3 Secure Element

Another possible way is to use a secure element, which is a hardware chip, such as a UICC, used to identify the device or the person carrying it. Every frame sent from a device will contain a token from the secure element that is not accessible by the application layer and better not from any SW layer running on the main CPU.

9.2.4 User Consent

In cases where there is no Internet, no available key storage and no secure element, there is a method that is being used by Bluetooth and Wi-Fi direct connection establishments – user consent. This method basically puts the users responsible and asks them to accept or deny the connection. Of course user consent doesn't have to be the last resort and may be used whenever appropriate.

9.3 Limiting Distribution

We focused on the fact that we want to reach as many receivers as possible. In many use cases this is very relevant. Nevertheless, what if we want to limit the distribution. Some of such limitations we have already mentioned like time and hop count (TTL and Timeout).

In this section we discuss several further possible ways to limit the distribution of the data.

9.3.1 Location

Once we initiate a spread of information, it may reach locations that are basically irrelevant and it does not benefit anyone. One such example is a lost pet for which the owner initiates a search broadcast in the neighborhood. A person driving from the neighborhood to a faraway location may reach there before the timeout or the TTL expire causing many people in the area to receive an irrelevant message.

We can limit these by restricting the distribution of the message to a geographical confinement.

9.3.2 Group of Interest

One of the use cases that we described was talking about the police searching for a suspect in a crowded area. A valid concern in such situation is that a broadcast of an alert will probably cause a panic within the crowd. To prevent this, the message shall be distributed using peers, however will be secured in such a way that only a special group of users, such as security guards of the establishment and any nearby police officers, even those on vacation, will be able to open it.

A possible way to ensure it, is priory preparation. The police will have some kind of predefined means, such as an access code, of the local security team that will allow them to encrypt the message and the security guards to decrypt it.

For a general case, any group shall be able to define an identifier that will serve to identify members of this group. Any station that does not belong to the specific group shall be able to forward the messages to other peers, but not to the upper layers of its network stack.

10 Complete Solution

10.1 Choosing the next neighbor – analysis

Before describing a complete solution we would like to take a deeper analysis of the main challenge of gossip algorithms – choosing the next peer.

There are essentially two cases – one when the nodes participate in some structure, and another case when the nodes are totally unfamiliar with each other.

In the first case, the structure that holds the nodes, may provide some information regarding the nodes and help a node choose its next peer. Nevertheless, we have already stated that structures, although very helpful for most purposes, add maintenance procedures and latency to the protocols.

The second case, when the nodes are unfamiliar and not connected to any central entity, is more interesting. We will take a closer examination of this case.

In order for a node to make a decision upon a peer, it must do two things – collect input data about its surroundings and analyze it. To collect data, a station may be passively listening for a while, or actively sending requests to and receiving responses from possible peers. There is no other way of choosing a unicast peer without the assistance of a network. It is easy to see that this process is time consuming and although this may be a matter of just a few single seconds, it may still be enough for the chosen peer to walk away before the connection is established and the data is transferred.

This is why we deviate from our initial approach of classic gossip algorithms and instead of unicast communication, prefer broadcast.

10.2 New Model

In this paper we have decided to focus on gossiping for the purpose of solving the use cases where wireless P2P can provide a better backbone than the Internet. "Gossip Algorithms" [4] is a comprehensive study and analysis of gossip algorithms and their performance. Nevertheless, there are several aspects there, that we find problematic in case we want to apply these algorithms to solve the aforementioned use cases in a real practical world –

1. They define that a node may pass information to one node only, at a time.
2. The nodes are connected in a network.
3. The studies ignore existing wireless technologies.

In this paper we introduce a different mode of information sharing, using gossip – P2C, where we rely on broadcast as the essential characteristic of wireless communication. We would like to remind our readers that wireless communication essentially comprises of broadcasts over the air, while factors like security and CSMA/CA [37] make sure that frames are treated as unicasts.

While relying on broadcast as the main mean for data transfer, we still intend to utilize unicast transfers to increase the chances and speed of information dissemination.

Last, but not least, we rely on existing, dominating wireless technologies, as it makes little sense to discuss P2P communications for existing devices while ignoring existing technologies that these devices implement.

Due to these reasons, we deviate from our basic model that was defined in section 2, where we assume that the nodes communicate to a single node at a time.

10.3 Spreading a Gossip – Broadcasting

10.3.1 GossipFrame

Gossip frames will be different according to the technology being used to send them. Nevertheless, all frames shall include the following information.

Field	Description
Sender Address	MAC Address or other unique identifier (IMEI/Phone number)
Sender Location	Geographical location of the sender
Sender Start Time	Time when gossiping started
Timeout	Time period during which forwarding the message is allowed
TTL	Hop count that limits the forwarding of the message
Location Limit	Geographical limit beyond which forwarding the message shall stop
IsDataHashed	A flag that indicates whether the data is the actual information or a hashed one that requires parsing using a dedicated service/server
IsContinuation	A flag that indicates whether the data is being sent in several messages
Data	The data hashed or not

10.3.2 Data Size

Similarly to human gossiping, we intend to spread small amounts of data. What is the appropriate limit of the data? In our opinion, the algorithm should follow the following principal –

```
If the data fits within a single frame of a technology Then
    - Send it within the frame.
If the data exceeds the size of a frame And there is an Internet connection available Then
    - Place the data on the Internet and distribute the hashed URL to access the data.
If the data exceeds the size of a frame And there is no Internet connectivity Then
- If it is the original source Then
      o Broadcast the data in several frames along with an indication that there are several frames that contain the data.
- If it is a follower (i.e. a node that is not the original sender) Then
      o It shall be the node's decision whether to send the information further or drop it.
```

10.3.3 BLE_Gossip()

```
- If Data.Length < Max_BLE_Advertisement.Length Then
      o Mark the BLE Advertisement frame as Gossip
      o Advertise the actual data periodically using BLE
- Else
      o If Internet connection is available Then
            ▪ Place the data at the cloud
            ▪ Hash the URL pointing to the data into a Max_BLE_Advertisement.Length string
            ▪ Advertise the hashed string using a marked(as Gossip) advertising packet
- Listen to any frames with the same gossip from other stations (this is the ACK)
```

10.3.4 Wi-Fi_Aware_Gossip ()

```
- If Data.Length < Max_NAN_Frame.Length Then
      o Broadcast the actual data periodically using Wi-Fi Aware
- Else
      o If Internet connection is available Then
            ▪ Place the data at the cloud
            ▪ Hash the URL pointing to the data into a Max_NAN_Frame.Length string
```

```
        ▪ Send the hashed string using a marked Wi-Fi Aware
          frame
- Listen to any frames with the same gossip from other stations (this is
  the ACK)
```

10.3.5 LTE-D_Gossip ()

```
- If Data.Length < Max_LTE-D_Frame.Length Then
    o Broadcast the actual data periodically using LTE-D
- Else
    o If Internet connection is available Then
        ▪ Place the data at the cloud
        ▪ Hash the URL pointing to the data into a Max_ LTE-
          D_Frame.Length string
        ▪ Send the hashed string using a marked LTE-D frame
- Listen to any frames with the same gossip from other stations (this is
  the ACK)
```

10.3.6 Performance Analysis

10.3.6.1 WFA, 3GPP, IEEE

For analyzing performance we need to remember that our solutions rely on existing wireless technologies, therefore the performance of our gossiping scheme will not exceed the performance of Bluetooth, Wi-Fi or LTE since these technologies rely heavily on broadcasts as part of their functionality. For instance, Wi-Fi Access Points, by default, send Beacon frames in a rate of 100ms, which translates to ten frames every second.

Stations utilize CSMA/CA to detect when the medium is available and avoid collisions. There are mechanisms that reduce transmit rate and power based on the surrounding noise.

10.3.6.2 Connectionless

Another factor that will contribute to performance is the absence of a network. We do not require the nodes to build and maintain a network. A node doesn’t care about its neighbors. It transmits the data as long as all conditions for it comply – TTL, Timeout, Geo Location, Noise Ratio.

10.3.6.3 Compared to Gossip Algorithms

When trying to compare the performances of our suggested solution versus the Gossip Algorithms proposed by the different papers, it is important to remember that, although mentioning wireless P2P, gossip algorithms that are described in many papers assume a very different environment. Therefore, making such a comparison is very difficult and even meaningless.

10.4 Spreading a Gossip – Unicast

10.4.1 Tethering_Gossip ()

```
- Configure a Wi-Fi Hotspot
- Mark the Beacon frame as Gossip
- If legacy Tethering is supported Then
    o Mark the beacon frame with legacy_tethering flag
- Send marked beacon frames periodically
- If station B requests to connect Then
    o Follow standard Wi-Fi BSS connection procedure and act as an
      Access Point
- If station B is connected Then
    o Send the Gossip to B
    o Receive an ACK from B
    o If B has a different Gossip to transfer Then
        ▪ Receive the Gossip from B
        ▪ Send ACK to B
- If legacy tethering is not required Then
    o Send a De-authentication to B and Disconnect from it
```

10.4.2 Possible Improvements

Naturally, there are usually some improvements that make the algorithm better.

- If the data is small enough to fit inside the gossip frame and there is no requirement to protect it or ensure that the identity of the sender may be verified, then there is no need to hash the data and place it on the cloud. It may be simply sent as part of the gossip frame itself.

- The gossiping methods we have described serve well the original sender. They are not good enough for the followers as there is no need to work the data itself. The original sender has done that already and it is either attached to the gossip frame or already located at the cloud.

10.5 Listening for Gossips

10.5.1 IsGossipSupported ()

```
- If Battery.Level < MinBatteryLevelForGossip Then
    o Gossip_Support = OFF
    o Return False
- Return Gossip_Support // Off or On following a separate API call
```

10.5.2 Set_Gossiping (State) API Method

```
Gossip_Support = State // possible values – OFF or On
```

10.5.3 Wi-Fi_Aware_Listen()

```
- If IsGossipSupported() AND Wi-Fi_Aware_Supported Then
    o Scan periodically for NAN frames
    o If gossip_frame_received Then
        ▪ Process_gossip_frame()
```

10.5.4 LTE-D_Listen()

```
- If IsGossipSupported() AND LTE-D_Supported Then
    o Scan periodically for LTE-D frames
    o If gossip_frame_received Then
        ▪ Process_gossip_frame()
```

10.5.5 BLE_Listen ()

```
- If IsGossipSupported() AND BLE_Supported Then
    o Scan periodically for BLE Advertisement frames
    o If gossip_frame_received Then
        ▪ Process_gossip_frame()
```

10.6 Forwarding Gossips

10.6.1 ProcessGossipFrame()

```
- If IsGossipSupported() AND GossipFrame.TTL > 0 AND
  CurrentLocation.WithinBoudariesOf(GossipFrame.Location) AND
  CurrentTime - GossipFrame.StartTime < GossipFrame.Timeout AND NOT
  IsGossipThresholdReached Then
    o UpdateTTL()
    o If BLE_Supported Then
        ▪ BLE_Gossip()
    o If Wi-Fi_Aware_Supported Then
        ▪ Wi-Fi_Aware_Gossip()
    o If LTE-D_Supported Then
        ▪ LTE-D_Gossip()
    o If Tethering_Supported Then
        ▪ Tethering_Gossip()
```

GossipFrame is the received frame.

GossipFrame.Location is the original location of the node that initiated the information dissemination.

CurrentTime is the current time at the receiver.

GossipFrame.StartTime is the original time of the initial sender.

GossipFrame.Timeout is the timeout that the initial sender configured and after which the spread of information should halt.

IsGossipThresholdReached is a threshold of the frames per second that represent the same gossip. Once a node receives a number of same gossip frames that exceeds the threshold, it shall not attempt to forward this gossip any longer.

A possible enhancement will be that if only IsGossipThresholdReached returns True, while all other indicators are normal, once

IsGossipThresholdReached is False again, a node may resume information dissemination.

We recommend to implement the **`GossipThreshold`** per technology. This way, if there is too much activity over Wi-Fi, the node will stop transmitting over Wi-Fi only, but will be able to continue distribution over Bluetooth and/or LTE if their threshold was not reached yet.

10.7 Visual Example

Let us consider the following environment. A reminder of our basic assumptions upon the characteristics of the topology –

- The nodes are not familiar with each other.
- The nodes are not engaged in any structure.
- The nodes are in constant movement.

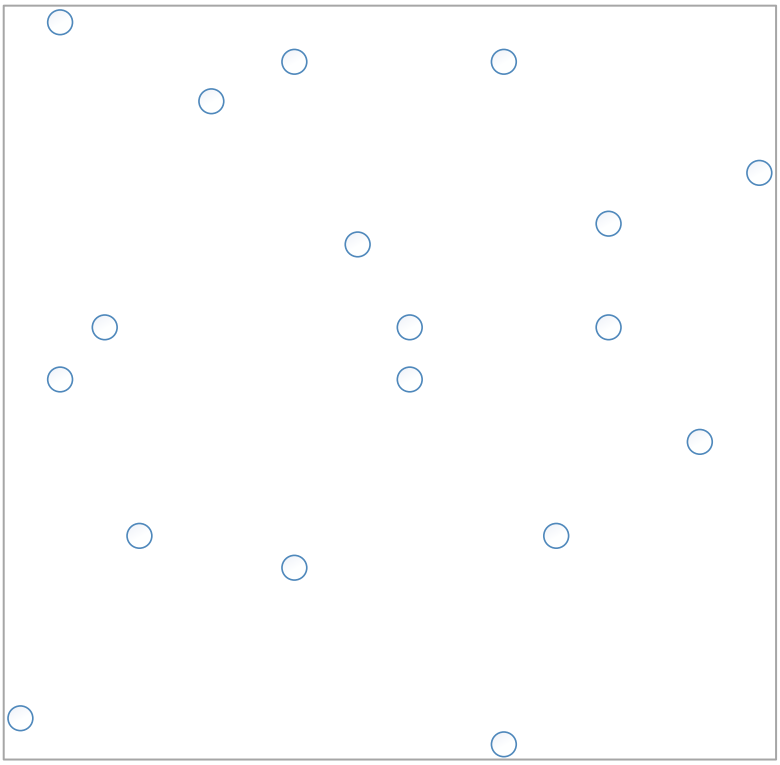


Figure 8 - Visual Example - Initial Topology

At t=0 the node **a** at the center is our original sender that has some data to spread.

It starts broadcasting over Bluetooth, Wi-Fi Aware and LTE-D.

The first ring denotes Bluetooth reachable radius, the second Wi-Fi and the third LTE.

At t=1 the nodes **b**, **c** and **e** get the gossip frame.

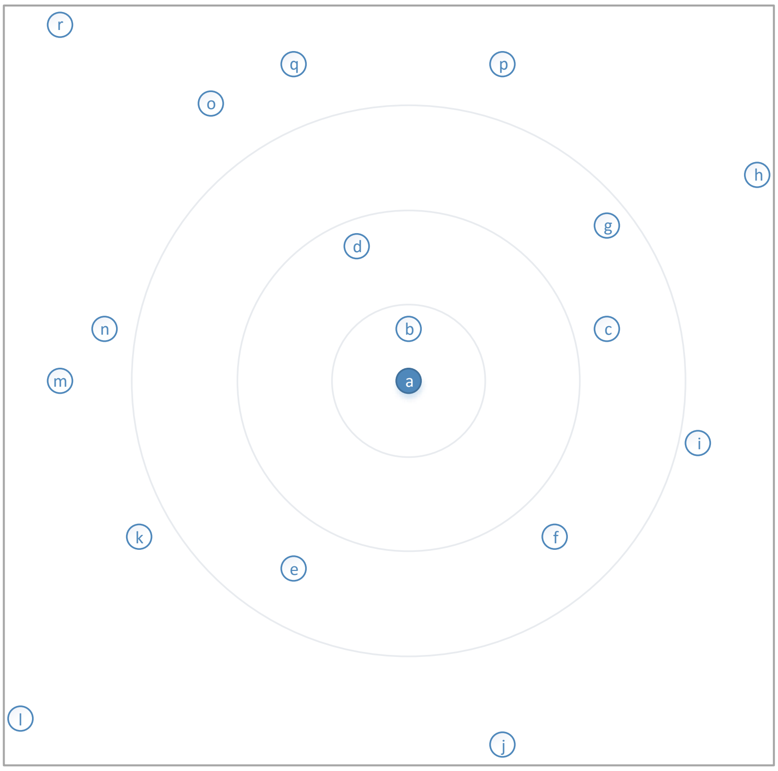


Figure 9 - Visual Example - t=0

b receives it using Bluetooth, **e** and **c** using LTE-D. For the sake of the example we show that although **d** is within the Wi-Fi radius and nodes **g** and **f** are within LTE radius, they don't receive the gossip frame because they were not listening during the specific time frame when **a** was transmitting.

At t=1 **a** as the original sender, and therefore most motivated node, continues to send the gossip over all three technologies.

e joins the spread efforts and transmits the gossip as well over Bluetooth, Wi-Fi and LTE. Since **b** received Wi-Fi transmissions of both **e** and **a**, it decides not to use Wi-Fi, but to continue gossiping using LTE only as it is configured not to gossip over Bluetooth.

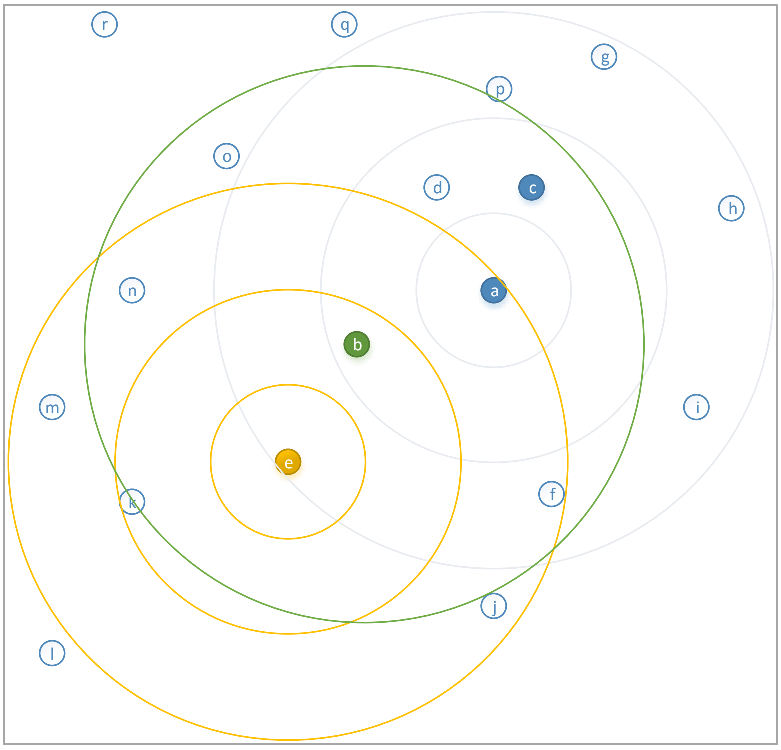


Figure 10 - Visual Example t=1

c decides not gossip at all for reasons of power save or other configuration. New nodes that receive the gossip are **o**, **d** and **n**.

This process continues until every node meets some criteria for halting the transmissions.

Few points worth mentioning –

- There may be a situation where all nodes received the gossip, yet some are still transmitting.
- A node may leave the area without receiving the gossip.
- Every node determines by itself –
  - whether it shall receive gossips
  - shall it continue spreading the received gossip
  - what technologies to use
  - when and why to stop receiving and/or transmitting

11 Future developments

In this chapter we discuss a few possible or actual future developments that will affect wireless communication in the future and P2P/P2C in particular.

11.1 Battery

At the present, power source is a significant limitation of many mobile devices.

A possible development in the future may be an invention that will allow the creation of batteries that can store much more power than those currently available. Let us consider such development – batteries that can power a high end smartphone for a week during medium to high utilization. How will it affect P2P wireless communications?

For the sake of the discussion we consider good enough computational abilities of the devices. This is true nowadays. Even medium range smartphones have sufficient performance for connected Wi-Fi, Bluetooth and LTE.

If devices don't have to take into consideration their power source, every device may become a hub and support gossiping out of the box. Users will be more willing to share the utilization of their devices once it "doesn't" consume power from their devices. Security may also be enhanced as security algorithms and technologies are always major power consumers.

11.2 Internet of Things

What will happen if, in the future, which may not be so far away, there will be many more devices that will be connected to the Internet? Will it mean that the technologies and algorithms we have described here become irrelevant?

First, let us agree that not everything will be connected to the Internet as it requires a device to support more technologies and every technology makes the device more expensive. For example, if we have smart shoes that count our steps, there is no need for them to include Wi-Fi or cellular technologies in order to report the calculation over the Internet. Instead, Bluetooth Low Energy shall be enough to share the number of steps with a smartphone.

We have mentioned before a use case where a smart bracelet that has no access to the Internet is lost. In this use case, the bracelet shall use BLE to periodically broadcast a distress call that may be picked up by a nearby device that has an Internet connectivity and will be able to inform the owner of the lost item of its whereabouts.

Based on that, we believe that IOT will not cancel the need for wireless P2P communications, but instead, will intensify its utilization.

11.3 5G

5G is an interesting development. There are no concrete specifications and standards yet, only workgroups that work on the definitions.

What it seems to be in the end though, is not just a new cellular standard. According to Wikipedia [33], The Next Generation Mobile Networks Alliance [34] defines the following requirements that a 5G standard should fulfil:

- Data rates of tens of megabits per second for tens of thousands of users
- 1 Gb per second simultaneously to many workers on the same office floor
- Several hundreds of thousands of simultaneous connections for massive wireless sensor network
- Spectral efficiency significantly enhanced compared to 4G
- Coverage improved
- Signaling efficiency enhanced
- Latency reduced significantly compared to LTE.

This is the very beginning and the Wikipedia page will probably be edited many times. Nevertheless, it is not difficult to notice and understand that these or similar requirements will not be achieved with a new cellular standard only. This should be an entire infrastructure upgrade, from the client to the cloud.

How this will affect wireless P2P?

In its essence 5G will probably still focus on connectivity from the client to the cloud and rely mainly on the Internet.

Nevertheless, we believe that the benefits that 5G may bring to wireless P2P, will be in the possible and desirable standardization of the collaboration between the different wireless technologies. As we show in this paper, such a collaboration is very appropriate and necessary for a better utilization of data exchange and reduction of latency, especially in an environment where the nodes are in constant movement.

12 Summary and Conclusions

In this paper we analyze the reasons for the very low utilization of wireless P2P technologies versus the vast dominance of the Internet. We show that Internet prevails due to the simple reason that the Internet was first and the solutions it provides are good enough. Nevertheless we claim that there are specific use cases that are difficult to solve using the Internet, while wireless P2P provides a much suitable framework.

While analyzing the use cases we conclude that gossip algorithms are appropriate for solving these. Nevertheless, we point out that there are several assumptions these algorithms make that, although very much appropriate for theoretical discussions, are problematic for practical solutions. They ignore the existence of wireless P2P technologies and dictate that a node may contact a single node at a time. We believe that for practical solutions, it is necessary to consider existing technologies, as well as attempt to harness the nature of wireless communication, which is broadcast.

One of the purposes of this paper is to provide practical analysis and solutions. Therefore, we do not ignore existing wireless technologies, Wi-Fi, Bluetooth, LTE, but analyze them and provide different suggestions that, if implemented, will allow wireless P2P communication to become a meaningful framework for different usages that are more difficult to solve using the Internet. Some of these solutions may be combined together. We also describe how to utilize wireless broadcasts and instead of P2P, focus on P2C.

In addition, we also explore the security problems that evolve in wireless P2P, and provide possible solutions.

Finally, we list a few future development that in our view will have significant impact on wireless technologies and P2P/P2C in particular.

We believe that the Internet should not be really replaced by wireless P2P communication. Instead, each should focus on the use cases that it solves best. In addition, and most importantly, we believe that all technologies should collaborate in order to solve practical problems better, faster and efficiently.

13 References

[1] Stephen Boyd, Arpita Ghosh, Salaji Prabhakar, Devavrat Shah; **"Gossip Algorithms: Design, Analysis and Applications"**; Information Systems Laboratory, Stanford University, Stanford, CA 94105-9510; IEEE 2005

[2] Ranveer Chandra, Venugopalan Ramasubramanian, Kenneth P. Birman; **"Anonymous Gossip: Improving Multicast Reliability in Mobile Ad-Hoc Networks";** Department of Computer Science, Come11 University, Ithaca, NY 14853,USA; IEEE 2001

[3] Pradeep Kyasanur, Romit Roy Choudhury, Indranil Gupta; **"Smart Gossip: An Adaptive Gossip-based Broadcasting Service for Sensor Networks";** Department of Computer Science, University of Illinois at Urbana-Champaign; IEEE 2006

[4] Devavrat Shah; **"Gossip Algorithms";** Massachusetts Institute of Technology; Foundations and Trends in Networking Vol. 3, No. 1 (2008) 1–125

[5] Vishal Gupta, Mukesh Kumar Rohil; **"Information Embedding in IEEE 802.11 Beacon Frame";** Birla Institute of Technology and Science Pilani, India; National Conference on Communication Technologies & its impact on Next Generation Computing CTNGC 2012

[6] Vishal Gupta, Mukesh Kumar Rohil; **"Bit-Stuffing in 802.11 Beacon Frame: Embedding NonStandard Custom Information";** Birla Institute of Technology and Science Pilani, India; International Journal of Computer Applications (0975 – 8887) Volume 63– No.2, February 2013

[7] Daniel Camps-mur, NEC Network Laboratories Andres Garcia-Saavedra and Pablo Serrano; **"DEVICE-TO-DEVICE COMMUNICATIONS WITH WIFI DIRECT: OVERVIEW AND EXPERIMENTATION"**; Universidad carlos iii de madrid; IEEE Wireless Communications, June 2013

[8] http://www.automotive-eetimes.com/design-center/why-80211p-beats-lte-and-5g-v2x/page/0/1

[9] Daniel Jiang, Luca Delgrossi; **"IEEE 802.11p: Towards an International Standard for Wireless Access in Vehicular Environments"**; Mercedes-Benz Research & Development North America, Inc. IEEE 2008

[10] Wi-Fi Alliance Technical Committee, P2P Task Group, **"Wifi peer-to-peer (P2P) technical specification, ver. 1.1,"** WiFi Alliance, Tech. Rep., 2010.

[11] Eng Keong Lua, Jon Crowcroft, and Marcelo Pias, University Of Cambridge, Ravi Sharma, Nanyang Technological University, Steven Lim, Microsoft Asia: **"A Survey And Comparison Of PEER-TO-PEER Overlay Network Schemes"**, IEEE Communications "Surveys", 2005.

[12] Hung-Yun Hsieh, Student Member, IEEE, and Raghupathy Sivakumar, Member, IEEE, "**On Using Peer-to-Peer Communication in Cellular Wireless Data Networks"**, IEEE Transactions on Mobile Computing, vol. 3, no. 1, January-March 2004

[13] Rossana Motta and Joseph Pasquale, "**Wireless P2P: Problem or Opportunity?"**, AP2PS 2010 : The Second International Conference on Advances in P2P Systems, 2010.

[14] Pyattaev A., **"3GPP LTE traffic offloading onto WiFi Direct"**, Wireless Communications and Networking Conference Workshops (WCNCW), 2013.

[15] Xiuqi Li andJie Wu, **"Searching Techniques in Peer -to - Peer Networks"**, Department of Computer Science and Engineering, Florida Atlantic University;

[16] Yrjö Raivio, **"Mobile Peer-to-Peer in Cellular Networks"**, Helsinki University of Technology; HUT T-110.551 Seminar on Internetworking, 2005-04-26/27

[17] https://en.wikipedia.org/wiki/Peer-to-peer

[18] https://play.google.com/store

[19] http://www.wi-fi.org/discover-wi-fi/wi-fi-direct

[20] http://www.wi-fi.org/discover-wi-fi/wi-fi-certified-miracast

[21] http://developer.android.com/guide/topics/connectivity/wifip2p.html

[22] http://developer.android.com/guide/topics/connectivity/bluetooth.html

[23] http://developer.android.com/guide/topics/connectivity/nfc/index.html

[24] http://www.wi-fi.org/discover-wi-fi/wi-fi-aware

[25] Wi-Fi Alliance; "**Wi-Fi Aware™: Better Proximity Technology for Personalized Experiences"**; July 2015

[26] http://ieeexplore.ieee.org/Xplore/home.jsp

[27] https://scholar.google.com/

[28] Signals Research Group; **"EXPANDING YOUR HORIZONS WITH LTE DIRECT, ENABLING THE NEXT GENERATION OF PROXIMAL SERVICES"**; September 2015

[29] Balaji Raghothaman, Eric Deng, Ravikumar Pragada, Gregory Sternberg, Tao Deng, Kiran Vanganuru; "**Architecture and Protocols for LTE-based Device to Device Communication"**; 2013 International Conference on Computing, Networking and Communications, Wireless Networks Symposium

[30] https://en.wikipedia.org/wiki/List_of_Bluetooth_profiles

[31] Kevin Townsend, Carles Cufi, Akiba and Robert Davidson; **"Getting started with Bluetooth Low Energy"**; O'Reily, 2014

[32] http://www.automotive-eetimes.com/design-center/why-80211p-beats-lte-and-5g-v2x

[33] https://en.wikipedia.org/wiki/5G

[34] https://en.wikipedia.org/wiki/Next_Generation_Mobile_Networks

[35] https://5g-ppp.eu/photos-from-5g-vision-press-conference/

[36] http://www.wi-fi.org/discover-wi-fi/wi-fi-certified-miracast

[37] https://en.wikipedia.org/wiki/Carrier_sense_multiple_access_with_collision_avoidance

14 תוכן עניינים

15 תקציר

רשתות Peer -to-Peer (P2P) קיימות כבר זמן רב. אנשים משתמשים בהן על בסיס יום-יומי. ביטורנט, סקייפ, WhatsApp, ויישומים פופולריים אחרים, מיישמים אלמנטים של רשתות P2P. עם זאת, למרות שטכנולוגיות אלחוטיות, כגון Wi-Fi וסלולר, קיימות מספר שנים לא קטן, תקשורת P2P אלחוטית אינה נפוצה כלל, והודעת טקסט פשוטה שנשלחה באמצעות WhatsApp מתלמיד אחד למשנהו, שיושב באותה הכיתה, עדיין תועבר דרך האינטרנט באמצעות רשת LAN אלחוטית או רשת סלולרית. עבודת גמר, אשר מפורטת במסמך זה, חוקרת את הסיבות לפופולריות הנמוכה של תקשורת P2P אלחוטית בקרב צרכנים, מנתחת אותם ומציעה שיפורים אפשריים הנדרשים כדי שנראה יישומים המתבססים על תקשורת P2P אלחוטית ואשר פותרים בעיות אמיתיות של משתמשים. בפרט, אנו עוברים על פרוטוקולים כמו Wi-Fi Direct ו-Bluetooth, אלגוריתמים ואיפיונים של רשתות P2P וסוקרים דרישות מיוחדות כמו מגבלת הספק הנובעת משימוש בסוללות. מאחר והמוקד של המחקר יהיה יישומים מעשיים, נושא ההבטחה מהווה חלק חשוב ממנו.

האוניברסיטה הפתוחה

המחלקה למתמטיקה ולמדעי המחשב

תקשורת Peer-To-Peer ברשתות אלחוטיות כאלטרנטיבה לאינטרנט

במסגרת תואר שני

מוסמך (M.Sc.) במדעי המחשב

האוניברסיטה הפתוחה

המחלקה למתמטיקה ולמדעי המחשב

מאת

גרי דרישפיץ

תחת הנחייתו של דר' לאוניד בירנבוים

נובמבר 2016