Santa Clara University

Adding Rich Tags and Security Protocols to Wi-Fi Devices For New Business Opportunities

Project for COEN331 “Wireless Mobile Network”
Summer 2013

He Shouchun

SCU ID: 00001008350

This document introduces the approaches of adding the rich static and dynamic tags to different types of Wi-Fi devices for Wi-Fi scanning. It covers the scope changes to the current 802.11 implementation, new frame and their structures, new scanning processes, new security protocols, the side effects, and how to minimize the power consumption for the added functions. Finally the paper introduces some potential business applications of the new features: Wi-Fi Direct social networking, Wi-Fi AP advertising, and Vehicle Collision-Avoidance System based on Wi-Fi and location service.

Acknowledgement

Thanks Dr. Keyvan Moataghed, the professor of my “Wireless Mobile Network” class, who gave me the introduction of 802.11 technologies in depth, and help me to choose this topic and define the scope of the new features introduced in this paper.

Thanks Dr. Ming-Hwa Wang, the professor of my “Computer Networks” and “Cloud Computing” class, who gave me introduction to the fundamental computer network and cloud computing knowledge.

Thanks Yuxia Chen (CCIE# 33685). As an expert in routing, switching, and WLAN area, she gave me lots of suggestions and advices about the feature design and implementation details, and helped me correct some misunderstanding of IEEE 802.11 technologies.

Thanks Meenakshy and Soujanya, my team mates in a project of Dr. Ming-Hwa’s class, who worked together with me on designing a Wi-Fi P2P social networking service, which leads to my conceiving of the ideas of this paper.

Table of Contents

Index of Tables

Index of Figures

Abstract

This document introduces the approaches of adding the rich static and dynamic tags to different types of Wi-Fi devices for Wi-Fi scanning. It covers the scope changes to the current 802.11 implementation, new frame and their structures, new scanning processes, new security protocols, the side effects, and how to minimize the power consumption for the added functions. Finally the paper introduces some potential business applications of the new features: Wi-Fi Direct social networking, Wi-Fi AP advertising, and Vehicle Collision-Avoidance System based on Wi-Fi and location service.

Target Audience

This paper is intended for people who are interested in the wireless mobile networking technologies with advanced knowledge of wireless standards and networking concepts. For example, professors and graduate students in computer science field, network engineers, researchers. They should have fundamental understanding in wireless networks specifically IEEE 802.11, and TCP/IP protocol stack.

The first and last chapters (introduction and business application parts) of this paper are much easier to understand than other chapters so those who have no solid network technical background, such as technical writers, business planners.

1. Introduction

Wi-Fi is widely available in homes, business offices, and entrainment environments, and is found in many types of devices, including notebook computers, gaming devices, and mobile phones, etc. The technology had been originated from 1985, and evolved from 802.11a, b, g, n, and moved toward higher speed and better usability. However, the technology is still on the way of continuous improvement.

1.1 Popularity of Wi-Fi Direct enabled mobile devices

Wi-Fi Direct, previously also called Wi-Fi P2P, is a new standard which is quite popular in these years. It enables devices (mobile phones, pads, PDAs, etc) to join in a virtual group to connect and communicate with each other via Wi-Fi without an AP. (WikiPedia) Only one device of the group needs to support Wi-Fi Direct and takes the group owner role to establish and control the connections with other Wi-Fi devices. Each Wi-Fi Direct enabled device can discover the similar devices around and send association invitation to them or accept the invitations. From end users' view the paring and communication among devices via Wi-Fi Direct is quite similar to how Blue Tooth devices works, but the connection speed among the devices is much higher and the coverage of connection is significantly far.1

It is quite easy, convenient, and secure to connect the Wi-Fi Direct devices. All Wi-Fi Direct connections are protected by WPA2 the latest Wi-Fi security technology. With Wi-Fi Direct, access point or Internet connection are no longer necessary – your personal Wi-Fi network can be setup whenever you need. (Wi-Fi Association)

Now the major smart phone operation systems, From ICS (Google) and IOS7 (Apple), Google and Apple have supported the Wi-Fi Direct features and provided the relevant API for developers to create the applications for end users in ANDROID and IOS. It can be seen that this technology will be widely used on mobile devices.

1.2 The device-to-device social networking

Social Networking is not a new concept. But from 2003 (the birth of the Facebook.com) the Internet makes social networking very hot. But in the last decade the mobile Internet was too expensive so it was not as popular and accessible as today. Even in nowadays it

[1] The Bluetooth 4.0 standard may compete with Wi-Fi Direct standard in the transfer speed and coverage. Please refer to this article:" Wi-Fi Direct vs. Bluetooth 4.0: A Battle for Supremacy", PC World. (IAN)

is not so easy to access Internet in the rural areas and most places in the developing countries.

So some people tried to create social networking functions on the mobile devices to enable those devices to make friends, chat, and send files with each other without connect to the Internet. They designed software to do device-to-device social networking based on Blue Tooth communication. (Patricia Tamarit) (Ramezani and Ameli) The idea is not so bad: Those multi-active young people (Lewis) really have the willing to make friends when they are idling in the running public vehicles or communities without Internet access. However such approaches were not quite successful due to the limitation of the Blue Tooth (10 meters distance limitation, low data transfer speed). And people could hardly match the strange Blue Tooth device name with a man or woman in the real life prevents them from taking the risks to do social networking blindly.

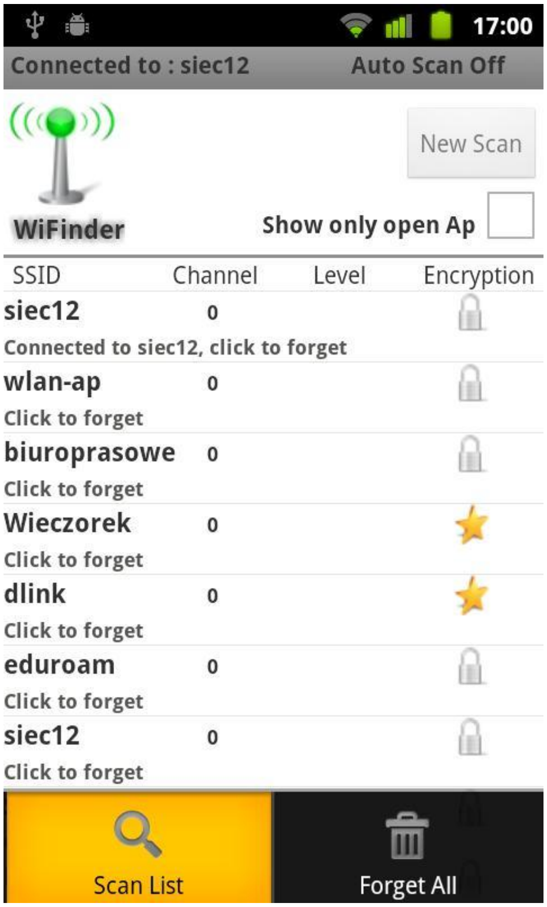
Now the Wi-Fi Direct technology has solved the most of the problems for device-to-device social networking. But the most important problem – the limited information in device identity – still be a blocker of widely use of device-to-device social networking. And if this problem can be solved, the value of Wi-Fi direct technology will be significantly increased. (He Shouchun)

1.3 Unfriendly and limited Wi-Fi device identities published before association

Currently, when users try to discover a Wi-Fi hot-spot or AP (access point), or connect another Wi-Fi device via ad-hoc or P2P (point to point), they can only see the meaning-less device names (SSID2, such as, wlan-ap, siec12, see figure 1-1 on the next page), and how the security encryption methods (such as WPA2, WEP, etc.). It may be fine to show such kind of names on an AP but not so user friendly in P2P device scanning.

[2] SSID always be understood as device names from the end users' view.

Figure 1-1 Meaningless device names shown in scanning result



Connected to : siec12 Auto Scan Off

Show only open Ap □

SSID	Channel	Level	Encryption
siec12 Connected to siec12, click to forget	0		🔒
wlan-ap Click to forget	0		🔒
biuroprasowe Click to forget	0		🔒
Wieczorek Click to forget	0		★
dlink Click to forget	0		★
eduroam Click to forget	0		🔒
siec12 Click to forget	0		🔒

1.4 Representation of mobile information

Now most of the WLAN adapters are installed on mobile devices, such as laptop, mobile phones. These adapters can work well in mobile environment; therefore they should have the capability of collecting the dynamic information around. For example, the location (either in text description, or a range, or accurate information get from GPS), temperature, etc. However the problem is that none of the existing Wi-Fi products can collect and share the environment information around with other devices. It is possible to enable the dynamic environment information publishing on Wi-Fi devices for the value-add services.

1.5 The Wi-Fi security protocols for P2P devices

Before two Wi-Fi devices associate with each other, they must have the same security protocols and use the same credentials. There are various wireless security protocols which were developed to protect home wireless networks. These wireless security protocols include WEP, WPA, and WPA2, each with their own strengths — and weaknesses. In addition to preventing uninvited guests from connecting to your wireless network, wireless security protocols encrypt the private data as it is being transmitted over the airwaves. (Wi-Fi Association)

The problem of applying current security protocols on P2P devices

However, the owners of the P2P devices may not know each other and do not know the key to access other devices. And even though they know each other, they still prefer “grant access” to other devices one by one than giving a key to all devices to lose the control of access.

Thus, the current Wi-Fi security protocols and authentication methods were designed for infrastructure BSS. They are not quite suitable for authentication of P2P social networking which is based on the IBSS structure (for ad-hoc connections) or infrastructure BSS with virtual AP (Wi-Fi direct).

Request & grant permission security model

One typical security model for the authentication between the social network entities is “Request and Permit”. The process is:

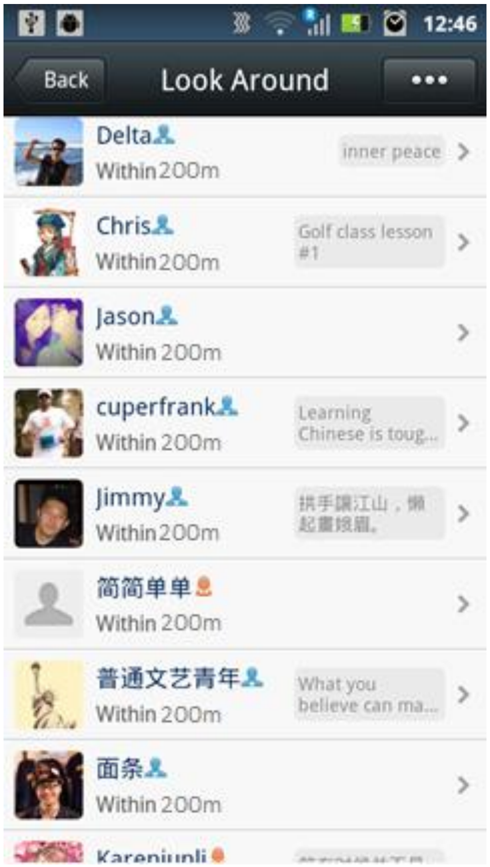
- A sends request to B for making friends (association), with something to introduce itself;
- B receives the request, check the information and A, then decide whether accept or reject the friends request, and send feedback;
- If B will accept the friend request, it also creates credentials for A to access its information.

To enable the social network on the Wi-Fi P2P devices, we need to implement a new security protocol which uses the “Request and Permit” model.

1.6 Add rich tags/identities to Wi-Fi devices

This paper brings a new idea to add rich identities and messages (in this following part of this paper they will be named as “tags”) to Wi-Fi devices. If the chipset vendors and operation system vendors follow this approach, the users can see the tags of the other Wi-Fi devices around when they are doing the scanning. These tags may include picture, owner's profile, introduction, status, website URL, etc. (See figure 1-2.)

Figure 1-2 Expected device identities shown in friends scanning



12:46

Back Look Around •••

Delta
Within200m
inner peace

Chris
Within200m
Golf class lesson #1

Jason
Within 200m

cuperfrank
Within 200m
Learning Chinese is toug...

Jimmy
Within200m
拱手讓江山，懶起畫娥眉。

简简单单
Within 200m

普通文艺青年
Within 200m
What you believe can ma...

面条
Within 200m

Karenjunli

The Wi-Fi devices can even receive messages pushed by the other devices. It should be possible for the Wi-Fi devices to push or receive those tags to or from other Wi-Fi devices before the associations have been made.

These tags not only can be used for the identity of P2P devices, but also can be used to publish the information to the device nearby (like the “cell broadcasting” or “cell entry notification” in the GSM systems). The receivers can choose to receive all the pushed information, certain categories of them, or even do not receive anything within certain period. However this design may cause potential privacy issue or harassment. In the later chapters of the paper you can find the answers about how to prevent the harassment.

From the end users’ view it looks like applying some of RFID (e.g. NFC) features on Wi-Fi devices. But the Wi-Fi devices are varied by categories and the scanning process is much more complicated than RFID, the data exchanging process will be completely different and will be introduced in detail in the following chapters.

1.7 Summary of Chapters

This paper explores the idea of adding rich tags to Wi-Fi devices to allow the Wi-Fi devices to exchange social networking identities and business information before association has been established.

Chapter 2 discusses the changes of the scope (fields and processes) based on the current 802.11 implementations, include the new static and dynamic tags to be added to the beacon frames, the new scanning process and the security protocols to the devices, and the reasons of those changes. In addition to the fields, this chapter introduces the changes to the scanning process which enable the new tags can be accessed by other devices, and how keep the inter-operability between the devices with new tags and the legacy devices.

Chapter 3 discusses the new frames and their structures for this feature to enable the rich tags, and how to set the relative frame headers.

Chapter 4 discusses the side effect of these new features. The changes introduced in this paper will cause more payload and power consumption, need to make changes in software, and require the hardware to have certain capabilities. And this chapter will discuss how to minimize the extra power consumption.

Chapter 5 introduces some business applications of the new features introduced in this paper:

- Device-to-device social networking
- Business advertising with AP
- Vehicle Collision-Avoidance System based on Wi-Fi P2P + GPS

2. Scope change to Wi-Fi scanning and security: Fields and process changes

To solve the problems and reach the approaches addressed in the Chapter 1, we need to make some changes based on current 802.11 scope. The new scope covers the extra tags, new processes, and new security protocols.

2.1 Selection and classification of the tags

There are lots of fields could be added into the tags for the Wi-Fi scanning. However, as we mentioned before, those tags should be exchanged between the Wi-Fi devices before the association has been done, it is necessary to limit the size of these fields to keep the payload of the tags exchange within a rational size. That means only some most important and frequently used fields will be chosen. And for each field there is a limitation in its size to keep the added payload within a controllable range. Some tags can be exchanged automatically in the association, while other tags need to be dynamically requested by the receivers. Such size and category limitations could prevent the devices and the networks from being maliciously attacked by flood traffic. Additionally, not all tags added are mandatory and most of them are optional and the manufacturers can selective implement them.

2.2 Legacy scanning parameters and mode compatibility

To be back compatible to the legacy Wi-Fi devices, all the current scanning parameters (Moataghed) defined in "802.11 standard" should be there untouched:

- Operating mode (BSS Type): Infrastructure or ad-hoc.
- Operating channels (Channel List)
- Network identities (BSSID, SSID)
- Scan Type: Active or passive scanning.
- Probe Delay: Delay in micro seconds before procedure starts
- MinChannelTime and MaxChannelTime: The scanning time for each channel

These parameters have higher priority to be received in the scanning because the new tags can only be received based on these parameters.

2.3 Information publishers and information receivers

As we mentioned in Chapter 1, the new tags are used for identifies and information broadcasting of the AP, P2P and ad-hoc devices. In this paper those devices that have the capability of publishing the tags are called information publishers.

Some other devices, which connect to AP devices so they only receive the identities and parameters rather than publishing them. They are called receivers in this paper.

For the P2P and ad-hoc devices, since they can both publish and receive the tags when acting different roles, each of them can be both a information publisher device and a receiver devices. However, at the same time they can only take one role. Let's consider the case of a P2P device associates with other devices into a group. If it acts as the group owner, then in the implementation it actually acts as a virtual AP (Daniel Camps-Mur) and information publisher and will not be a receiver. Vice versa, when it acts as a group member in the association, it can only act as a receiver rather than an information publisher.

2.4 New tags and related functionalities for information publishers

To implement the rich identities in the Wi-Fi scanning, the information publisher needs to add lots of fields and related functionalities. And such information will be published in extra beacon or can be retrieved per request from information receivers.

(Note: Due to the time limit, some of them have been considered but still not finalized. Those parts need to be considered thoroughly and completed before a formal standard is created. Those fields or details are marked as "TBD[3]". -- Shouchun He)

Extra Beacon frame

As we know, Beacon frame is used in IEEE 802.11 based WLANs for the AP (in an infrastructure BSS) or work station (in an IBSS) to publish the network management information. It consists of the timestamp, beacon interval, network capability, SSID, supported data rate, Frequency-hopping (FH) Parameter Set, Direct-Sequence (DS) Parameter Set, Contention-Free (CF) Parameter Set, IBSS Parameter Set, Traffic indication map (TIM), etc. (WIKIPEDIA)

To keep the backward compatibility, we should not modify the existing beacon frame but try to introduce some extra beacon frames. If the information receivers have the rich Wi-Fi tags support capability, they will receive these extra beacons and handle them. Else, they can simply ignore them.

[3] TBD, stands for "To Be Defined".

Some of the below fields will be included in the extra beacon frame, such as: CATEGORY, flags of tags availability. While other some fields especially the long fields will be retrieved by the information receivers according to the category matching result.

To minimize the extra power consumption and payload caused by extra beacon, the system needs to support the two modes of extra beacon scanning like the regular IEEE 802.11 scanning:

- Active extra scanning: When the information receiver device sends probe request frames for the beacon frames, the information publisher devices will send a response frame followed by an extra beacon frame;
- Passive extra scanning: The information receiver device waits for the extra beacon frames as well as the regular beacon frames from other devices and buffers to analyze.
- Some mobile devices which have very critical requirements about power saving need only support the “passive extra scanning” mode to save power.
- An information publisher device can send extra beacon frames in a lower frequency than the regular beacon frames to save payload and power.

Picture and Avatar

Picture is used to indicate the identity of the owner of an AP or a P2P/ad-hoc device. Avatar is a small size thumbnail view of the picture. The size of avatar is always smaller than 32x32 pixels, and the file size will be smaller than 2KB so that it could be transferred in one or two frames and quickly exchanged among the devices. The pictures are much bigger in size but more clear in quality. It needs longer transfer time and only be exchanged per request from the receivers. And the picture can be cached in the receiver side so it only needs to be retrieved from the information publisher side when necessary. One approach of check the necessity of requesting new picture is firstly compare the local avatar with the avatar from the information publisher to check whether the picture has been updated.

Implementation tip: When the user set these fields, he/she need only set the “picture” field and the avatar should be automatically generated. The device should use some algorithm to make sure the size of the avatar is smaller than 2018 bytes.

Short description

The “Short description” is a text string which describes the owner or this device, in plain text. It can be something like the “status” or “tweet” that users publish in social networking system.

The text in “Short description” will be encoded in UTF-8 character set so that it can support most languages.

Description and Plain Description

The “Description” field indicates the detail description of this device. It can be either in the rich text format (as described in the “Text attributes” field mentioned above) or plain text.

The “Plain Description” is an optional field. It is a plain text representation of the “Description” field. Like “avatar”, it can be automatically generated from the content of the “Description” field. And if it is not there but requested by the receiver, it is strongly recommended that the information publisher device to be capable to generate the plain text and transfer to the receiver on the fly.

The receivers need to handle this field according to its capability. If it is not capable of displaying rich text, it should request the “Plain Description” field to save the transfer payload.

Pre-defined Categories and Customized Categories

The information publisher devices can use the category fields to indicate what kind of information it publishes or what kind of device it is. On the receiver side there are also category fields to indicate the preferred categories of information the receivers would like to receive. So that the receivers devices can match their own category fields with those on the information publishers, to figure out a “preferred” devices list to associate.

The end users can set the proper category fields of their devices to filter out the information published by other devices.

To protect the privacy of the end users, the default setting is an extreme condition that none of the categories is chosen on the receiver device. In this case all the information published from other devices will not be received by default. The scanning process is the same as that on the legacy Wi-Fi devices. However the device should provide some guide to the end user to learn how to set the categories.

Pre-defined category field(s)

The device should have one or more two-byte CATEGORY field(s) to store the category matching criteria:

- Bits 0 to 3 indicate the domains of the categories.
- Bits 4 to 15 indicate the categories of the selected domain. 1 means such category is selected, 0 means such category will not be selected. In each domain there are 12 pre-defined categories.

All the devices should support the following standard for pre-definition of some frequently used categories in various domains. These categories can be classified by the domains:

Table 2-1 the category fields and bits

Bit 0-3	Domain name	Categories (Bit 4-15)
0000	Social networking	12 social networking related categories, such as: Male, Female, Tall, Slim, etc.
0001	Food service	TBD (To be defined)
0010	Wears	TBD
0011	Car related	TBD
0100	Education service	TBD
0101	Electronics	TBD
0110	Life and entertainment	TBD
0111	Outdoor service	TBD
1000	Positioning service	TBD
1001-1111	Reserved for future services	TBD

Generally, the information publisher devices may have only one CATEGORY field to indicate what kind of devices they are. So that it can only indicate that it publishes information within a certain domain.

But for the information receiver devices, they can have up to 16 CATEGORY fields. Each CATEGORY field covers one domain and no two CATEGORY fields have the identical domains. Therefore for those devices which are both information receivers and information publishers (such as Wi-Fi direct devices), only the first CATEGORY field will be used for describing its domain and categories for information publishing.

Category indicator

It is a bit which is used for information receiver only. 0 means that this receiver will filter the information publishing or requests from information publishers by category matching; 1 means that the receiver can match all information publishers.

This bit is always ignored when the device is taking the information publisher role.

Count of CATEGORY fields

As its name, this field indicates how many CATEGORY fields on the information receiver device. Since there are 16 domains then there can be up to 16 CATEGORY fields, and this field takes 4 bits.

Count of customized categories

The devices should allow end users to be possible to set up to 15 customized categories. If there are customized categories, this field takes 4 bits so its value ranges from 0 (no customized categories) to 15 (full).

ZIP flag

This tag indicates whether the long text tags are compressed. Just for saving data payload in the transmission of the text contents.

The compression algorithm is ZIP and the compress rate is maximized.

Text attributes flag

This tag Encoding (7-bit, base64, binary, etc), character set (e.g. UTF-8), representation format (plain text/rich text format/html/xml, etc.). The receiver can decode the tags and present in the correct style.

Data lengths (multiple)

This tag indicates the length of the long fields (such as, description, the picture, etc.). So that these tags can has variable length and the receivers can estimate how many frames are required for transferring these tags and choose whether to request them according to the device policy.

Dynamic fields

As we mentioned in Chapter 1, the information publisher devices should be possible to publish some dynamic information as well as the static information.

On most Wi-Fi enabled devices, there are positioning (GPS, tri-angle positioning via mobile base stations, etc) module, thermometer module, and other modules which can get the mobile information of the current device.

Such information can be used in social networking, and Collision-Avoidance systems. Please refer to the Chapter 5 where some of the applications are introduced.

Flag of the tags availability

Some bits to indicate whether certain identity tags or information broadcasting tags are available. Refer to the graph below, each cell indicates a bit.

Table 2-2 the flag bits of the tags availability

Avatar & description	Picture	Description	Category Indicator	Count of customized categories
1	1	1	1	4
ZIP	Encoding, Charset, MIME type, etc.	Data length of long data	Customized categories (fixed length)	Dynamic fields
1	(TBD)	(TBD)	(TBD)	(TBD)

2.5 New fields and functionalities for information receivers

As the information receiver, the device only needs to receive the beacon, parse out the rich tags, and decide whether it needs to pass such information to the applications to do further processing.

Pre-defined Categories and Customized Categories

Unlike the information publishers, the information receivers can have up to 16 CATEGORY fields. Each CATEGORY field covers one domain and no two CATEGORY fields have the identical domains. Therefore for those devices which are both information receivers and information publishers (such as Wi-Fi direct devices), only the first CATEGORY field will be used for describing its domain and categories for information publishing.

For the category matching algorithm between the information receiver and information publisher, please refer section 2.6, “Category matching algorithm”.

New scanning mode

Just like the normal Wi-Fi devices, the information receiver devices need to periodically receive the beacon frames from the AP or other mobile stations. If a device supports the rich tags, it needs to receive the extra beacon frames from the information publisher devices. After it gets the extra beacon frame, it will take the following actions:

- Parse the frame and make out the flag bits, and the customized categories;
- Check whether it would like to receive the rich tags published by the information publisher by matching the CATEGORY fields and customized category fields between the information publisher and itself;
- If no category match, then it would not receive other rich tags from the information publisher, and the rest behaviors are the same as that of Wi-Fi devices without rich tags support.
- Else, it needs to request the information publisher to transfer the rich tags, such as, pictures, detail description, etc. This process can be done before or after the association, and it has low priority than the association process.
- After receive the rich tags, the information receiver will decode the contents and display them on the client UI.

2.6 Category matching algorithm

If the “category indicator” on the information receiver device is 0, the device needs to compare its CATEGORY fields to the CATEGORY field that it got from the information publisher. If a local CATEGORY field and that of a information publisher have the identical bit 0-3, and both of them have some “1” in the same indexes between 4 and 15, then we can say that the information receiver and the information publisher have matched pre-defined categories.

If the information publisher and the receiver have no matched pre-defined categories, the receiver needs to request the customized category fields from the information publisher and compare it with its own customized category fields. If there are same customized category field from both sides, then we can say that the information receiver and the information publisher have matched pre-defined categories.

2.7 Request & grant permission security protocol for P2P devices

In section 1.5 “The Wi-Fi security protocols for P2P devices” we mentioned the problems of security protocols on Wi-Fi P2P devices. In this section a new security protocol is introduced for P2P devices to associate with each other without knowing the network security key of each other. The two partners in the association only need to finish a “Request& Grant permission” process.

Prerequisites: There are two Wi-Fi P2P devices A and B. They are in the Wi-Fi signal coverage of one another (the distance between them is less than 200 meters). They have received the beacon frames of each other. Both devices should support RSA algorithm to secure the credentials.

- A sends request to B for association. In the request, it publishes its public key and some information typed by the user to let user of device B to accept the association request;
- B receives the request and let its user know that. Then the user can ignore it, or check the information in the request, or check the rich tags of device A, such as avatar, picture, detail description, etc. Then the user can decide whether accept or reject the association request.
- If device B user wants to reject the association request, it can simply ignore the request, or send back a reason of reject to device A. The reason information should be encrypted by the public key of the device A.
- If device B user wants to accept the association request, it creates a credential key exclusively for device A, encrypt it the public key of device A, and send the encrypted credential and its own public key back to device A. The credential contains a time limitation and expires after a given period.
- After device A gets the response from device B, it decrypts the credential or rejection reason.
- If device A gets the permit (receives the credential), it save it, and generate another credential exclusively for device B, encrypt it with the public key of device B, and then send the encrypted credential together with the credential it got from device B back to device B.
- From now on device A and device B can use these two credentials every time when they need to associate with each other until the credential expires. After the association, the data connection between the two devices will be protected by WPA2 (the keys are the credentials they generated).

The figure 2-1 and 2-2 show the two different scenarios (association request rejected or ignored, and association request accepted) of the new Wi-Fi P2P devices association process:

Figure 2-1 the sequence flow of request & grant permission in association

(Request rejected or ignored)

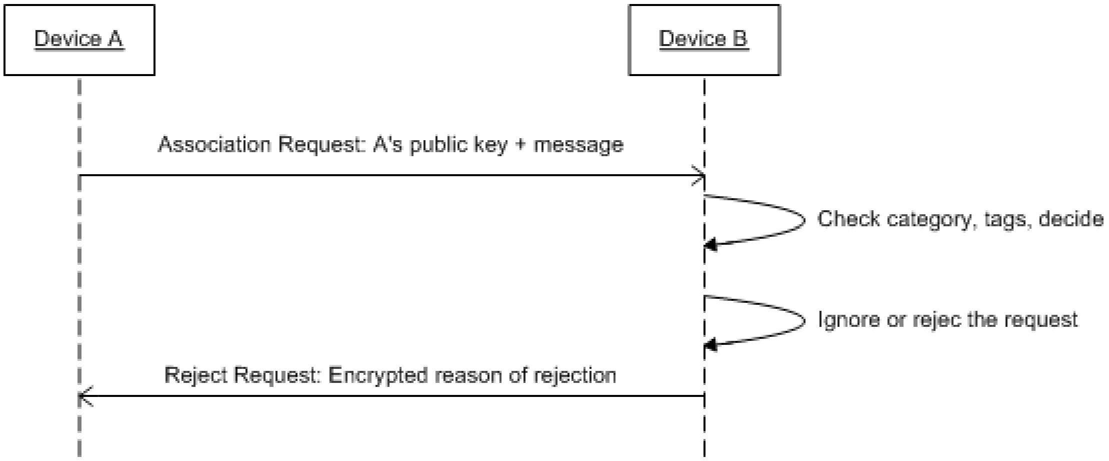
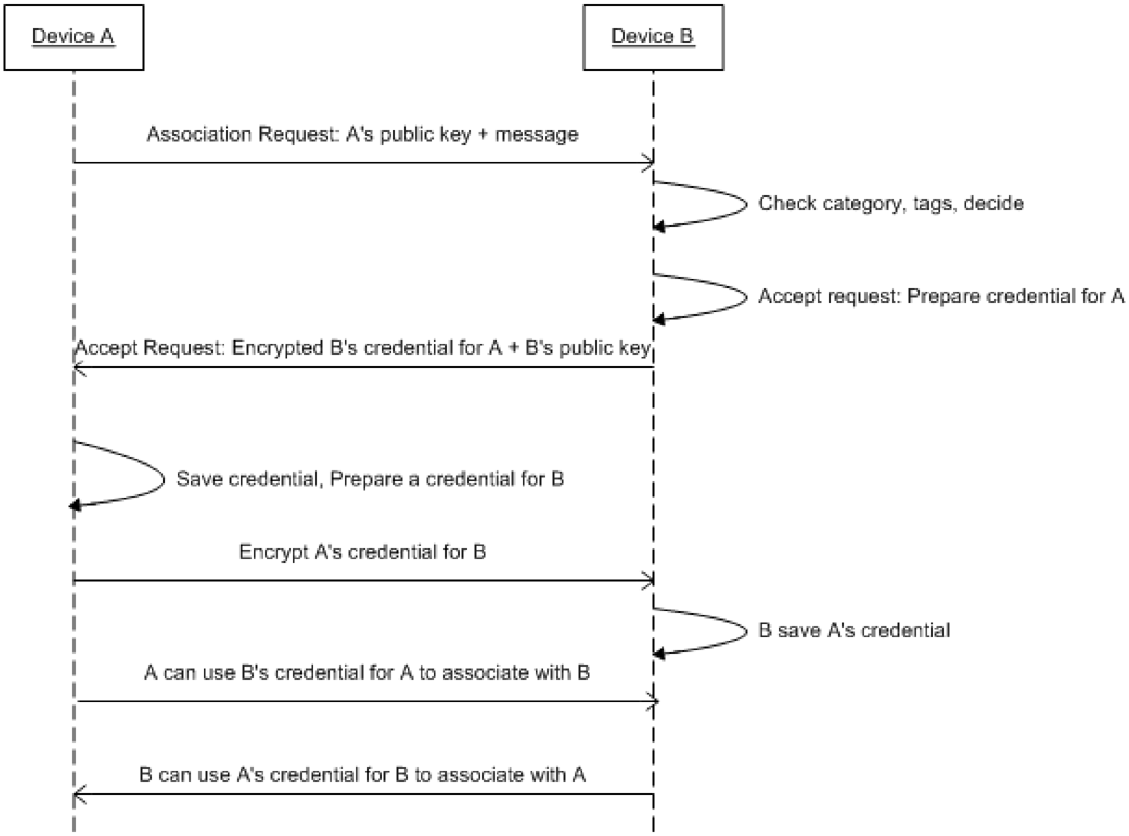

Device A
Device B
Association Request: A's public key + message
Check category, tags, decide
Ignore or rejec the request
Reject Request: Encrypted reason of rejection

Figure 2-2 the sequence flow of request & grant permission in association

(Request accepted)

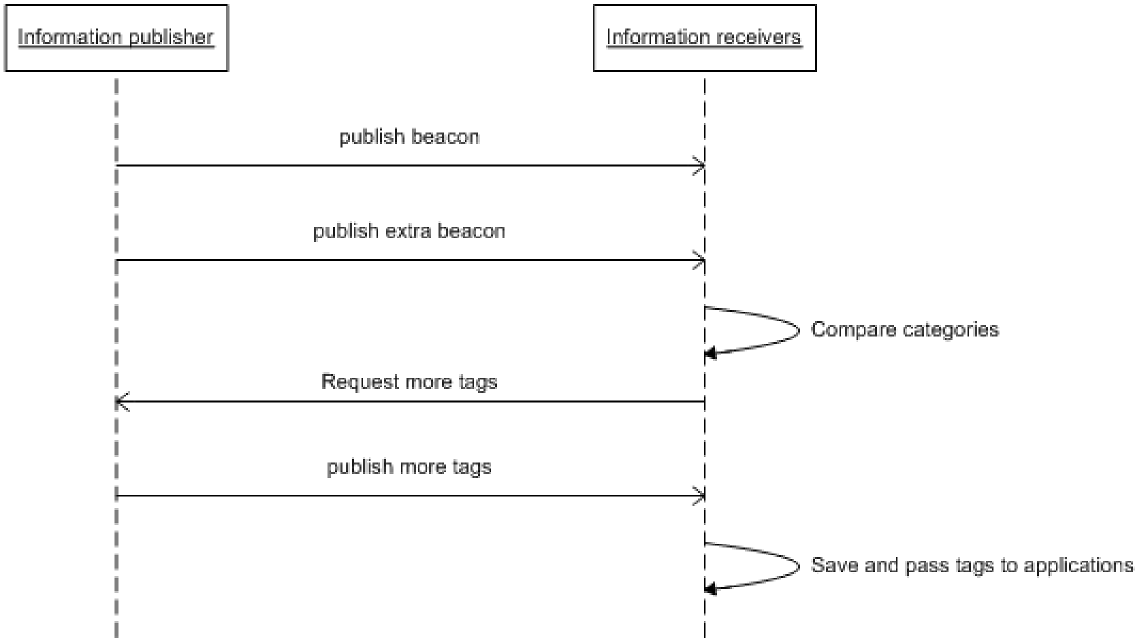

Device A
Device B
Association Request: A's public key + message
Check category, tags, decide
Accept request: Prepare credential for A
Accept Request: Encrypted B's credential for A + B's public key
Save credential, Prepare a credential for B
Encrypt A's credential for B
B save A's credential
A can use B's credential for A to associate with B
B can use A's credential for B to associate with A

Theoretically the association request can be initialized from any Wi-Fi P2P device; no matter they are information publishers or receivers. And this “request/grant permission security protocol” does not applicable for infrastructure BSS network.

2.8 Summary of the new scanning process and association process

In this chapter we introduced the new tags and processes to enable more features on the Wi-Fi enabled devices. In summary, we can get a whole picture of the new scanning process as shown in figure 2-3 below:

Figure 2-3 new Wi-Fi scanning process



When the information receiver wants more tags from the publisher, it will send a request to the information publisher. After the information publisher gets a request for more tags, it broadcasts the response (contents of the tags requested, or TAB_NOT_EXIST) to all the information receivers which listen to it. Every information receiver can receive that response and process it no matter whether it sent out the request. Such implementation can help to reduce the requests and responses for exchanging the rich tags in the network and minimize the payload for the rich tags.

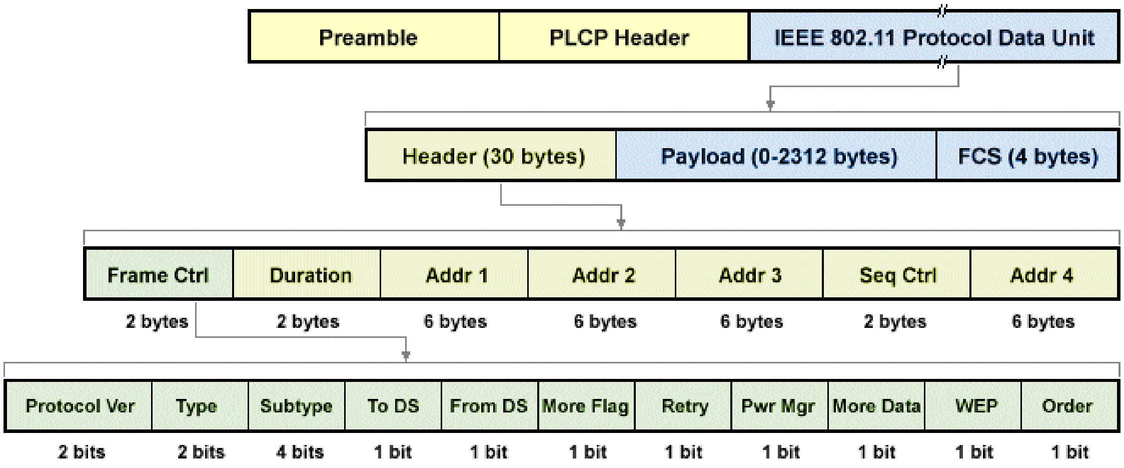
3. New Frames and Structures

This chapter will introduce the new frames and their structures to be created for implementation of the rich tags and the new scanning and association processes that introduced in Chapter 2.

3.1 IEEE802.11 Frame and Structure

All Wi-Fi frames should follow the frame structure defined in the IEEE802.11 specifications. The common frame structure is:

Figure 3-1 IEEE 802.11 Frame Structure



To make backward compatibility, all the syntaxes of the existing IEEE 802.11 frames must keep unchanged. In the new feature implementation, the developers can only implement supplementary functions and processes to achieve the goals of the new tags and new processes.

3.2 Extra beacon frame and structure

As mentioned in section 2.4, the extra beacon frame is very important for the let the information receivers know the existing of information publishers and the availability of rich fields.

In the payload of the extra beacon frame, there are following information:

Frame type indicator (2 bytes to indicate this frame is an extra beacon frame)

Flag of the tags availability (8 bytes)

Pre-defined category field (CATEGORY, 2bytes)

Customized categories (15 entries, 16 bytes each, total 240 bytes. The contents should be stuff with \0x00 if the category name is shorter than 16 bytes.)

Short Description (40 bytes)

Avatar length (2 bytes)

Avatar (0 – 2018 bytes, varied length, for storing a 32 pixel X 32 pixel image file in JPEG format.)

The total payload length of the extra beacon frame is 294 bytes to 2312 bytes (the maximum IEEE802.11 payload length).

Figure 3-2 Extra Beacon Frame Structure (inside the payload)

Bytes	2	8	2	240	40	2	0-2018
	Frame type indicator	Flag of the tags availability	CATEGORY	Customized categories	Short Description	Avatar length	Avatar

In the “Active extra scanning” mode, when an information publisher device receives the probe request frame from an information receiver, it will send back a response frame followed by broadcasting an extra beacon frame. So there is no extra probe request frame for the extra beacon frame.

3.3 Tag information request frame

This frame is use for the information receiver to request the contents of the tags which are not covered in the extra beacon frame from the information publisher. It is a unicast frame and the relative fields in the IEEE802.11 frame header should be set.

Figure 3-3 Tag Information Request Frame Structure (inside the payload)

Bytes	2	2
	Frame type indicator	Request type

Request types:

1: Picture request frame

2: Description request frame

3: Dynamic information request frame, request positions, environment temperature, etc.

> =4: Other information request frames, TBD.

3.4 Tag information response frames

This frame is use for the information publisher to broadcast the contents of the tags which are not covered in the extra beacon frame to all the other devices in the network. It is a broadcast frame, and some responses (such as the picture tag and the detail description tag) are so long that they need several frames to send. So the relative fields in the IEEE802.11 frame header should be set accordingly.

Figure 3-4 Tag Information Response Frame Structure (inside the payload)

Bytes	2	2	XXX
	Frame type indicator	Response type	Tag contents

Information response types are the same as the request types in section 3.3:

The length of the tag contents varied from 1 to 2308. And some responses take more than one frames to transfer all contents of the tag.

3.5 Request & grant permission frames for P2P devices

In section 2.7 we introduced the process of request & grant permission between P2P devices. There are three kinds of frames for this security process:

Request permission frame

It contains its own public key, and some text messages encoded in UTF-8.

Though 128-bit, 256-bit and 512-bit public keys are widely used by the industry, the public key length may be even longer in the future. To make sure the scalability in the future, we reserve 512 bytes (4096 bits) for the public key.

Figure 3-5 Permission Request Frame Structure (inside the payload)

Bytes	2	2	2	512	2	0 – 40
	Frame type indicator	Security operation type	Public key length (bits)	Public key + stuff bits	Message length (bytes)	Message

Grant permission frame

It contains its own public key and the encrypted credential by the public key of the receiver.

Figure 3-6 Grant Permission Frame Structure (inside the payload)

Bytes	2	2	2	512	2	512	8
	Frame type indicator	Security operation type	Public key length (bits)	Public key + stuff bits	Credential length	Encrypted credential	Credential Expire time

Reject permission frame

It contains its some text messages encoded in UTF-8 which specifies the reason of rejection.

Though 128-bit, 256-bit and 512-bit public keys are widely used by the industry, the public key length may be even longer in the future. To make sure the scalability in the future, we reserve 512 bytes (4096 bits) for the public key.

Figure 3-7 Permission Request Frame Structure (inside the payload)

Bytes	2	2	2	0 – 40
	Frame type indicator	Security operation type	Message length (bytes)	Reject Message

3.6 Frame header settings for the new frames

All new frames introduced in this paper are management frames. So the “Type” bits in the “Frame Ctrl” field should be 00. But for the SubType bits, there are two approaches for marking them indicate the type of new added frames for rich tags and new processes.

One approach is using one unused bit set, such as 1110, for all the new frames. The advantage of this approach is that the other unused bit sets in the SubType can be reserved for future use. In the frame structures above, we used this approach and set SubType of all frames to 1110, and differentiate the functionalities of the frames by a 16-bit “Frame Type Indicator” in the payload.

Another approach is using different bit set for different purpose. For example, 0111 for extra beacon, 1101 for tag information request, 1110 for tag information response, and

1111 for the request/grant permission for P2P devices. We did not use this approach in this paper in case of all the management SubType bits are used up.

To save the payload on the network, all the tag information response frames sent from the information publishers should be send in broadcast mode, so that any information receiver could receive and handle them or discard them.

On the contrary, all the tag request frames sent initiated from the information receivers and target to the information publishers should be sent in unicast mode.

4. Side effects

The new features introduced in this paper includes adding extra beacon frames, new scanning processes, and the request & grant permission security protocols. Such new features result in more frequent data communication, new software requirements, new hardware capability requirements, and higher power consumption.

4.1 Software requirement changes

According to chapter 2, the software on the Wi-Fi device needs to be compliant to the following requirements for implementing the new features:

- RSA encryption/decryption
- ZIP data compression/de-compression
- UTF-8 characters encoding/decoding
- Digital image processing (extract avatar from a picture, display avatar/picture)

And at the device driver and application level the device needs to implement the new Wi-Fi scanning process. For P2P devices, the new security protocol (request/grant permission) should be developed for device association.

4.2 Hardware requirement changes

The devices should have powerful CPUs which can perform the RSA encryption and decryption, the data compression and decompression, and the UTF-8 characters encoding and decoding, and the digital image processing, and dynamic data processing.

Secondly, the devices also need more memory spaces to store the rich identities, such as the picture, the detail description.

Additionally, the devices need to work together with other hardware such as GPS, various kinds of sensors, etc. to make full use of the dynamic information publishing.

4.3 Security & Privacy issue

Since all the new features introduced in this paper are about the processes that would have been done before the association has been established. All the frames are not protected by the security protocols, which may cause the information leak. And hackers may create fake frames to break through the devices. So there should be some measures to prevent this.

On the other hand, since the tags set on the information publisher devices are visible to all the information receiver devices around even though they had not been associated, the user needs to share their information carefully. The device manufacturers need to provide warnings to the end user to publish their information carefully.

Even for the information receivers, once their category settings match the category settings from some information publishers, their devices may receive the broadcasted rich tags in the background and some spam information may came to their devices if the categories are not properly set.

4.4 Power management

The new fields and new processes introduced in this paper do not bring any changes to the IEEE 802.11 power management. However, since adding the tags may cause more payloads to the network, we should take some measures to minimize the extra power consumption.

Actually in the previous chapters we have already introduced some measures to reduce the power consumption. For example, to set a lower frequency of extra beacon frames broadcast; to broadcast the response of the tags request, just for reducing the data payload in the network and reduce the power consumption.

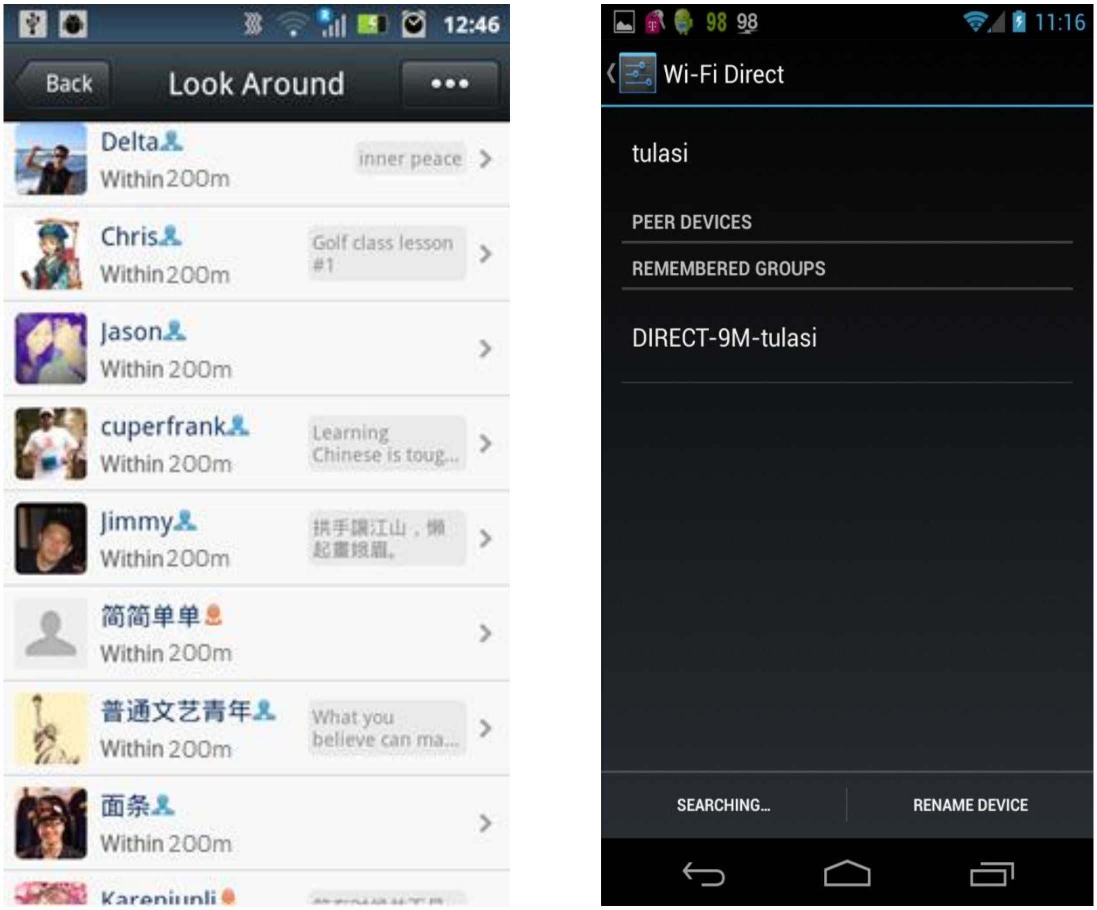
5. Applications

In this chapter four typical applications of the new features will be introduced.

5.1 Wi-Fi P2P based social networking

Wi-Fi P2P (also called Wi-Fi Direct) builds on traditional Wi-Fi strengths like performance, security, ease of use and ubiquity, and adds features that optimize it for consumer uses that don’t require access to an infrastructure network. Rather than connecting first to an infrastructure network and then connecting to another networked device, users can connect directly to those devices offering the services they need. This allows, for example, a mobile device such as a cellular phone to connect directly to a laptop, regardless of whether an infrastructure network is available to the user. Devices certified for Wi-Fi Direct extend the technology’s reach to include the simple, direct connections that many users may accomplish using cables today.

Figure 5-1 Two different UI of friend discovery in Wi-Fi P2P device



Delta
Within 200m
inner peace

Chris
Within 200m
Golf class lesson #1

Jason
Within 200m

cuperfrank
Within 200m
Learning Chinese is toug...

Jimmy
Within 200m
拱手讓江山，懶起畫娥眉。

简简单单
Within 200m

普通文艺青年
Within 200m
What you believe can ma...

面条
Within 200m

Kareniunli

tulasi

DIRECT-9M-tulasi

(a) With features of this paper

(b) Current Wi-Fi Direct UI in ANDROID

The picture in the left is the same as Figure 1-2 in Chapter 1. It shows an example of “Friend Discovery” user interface in a Wi-Fi P2P based social networking application. In that picture, you can see the name, avatar, distance, and status of the users around. It is much easier for users to choose whom to send out the invitation. By clicking the avatar or other areas in the list, people can view a high resolution picture, or view a detail description in rich format of that person. How can you imagine people can social networking with the UI shown in the right side? This picture is a screen-shot captured from the Wi-Fi Direct settings of ANDROID 4.0.4.

With the new features of this paper implemented on the Wi-Fi P2P devices, people can do social networking easily by discovering the friends (by new Wi-Fi scanning process and category matching) with rich identities, sending invitation (association requests) to them, and getting connected. Compared with the traditional social networking system, The Wi-Fi P2P social networking process has many advantages:

Firstly, users can do social networking WITHOUT internet! They can discover the friends in the subway trains, in high speed bus, or in rural communities of the developing countries.

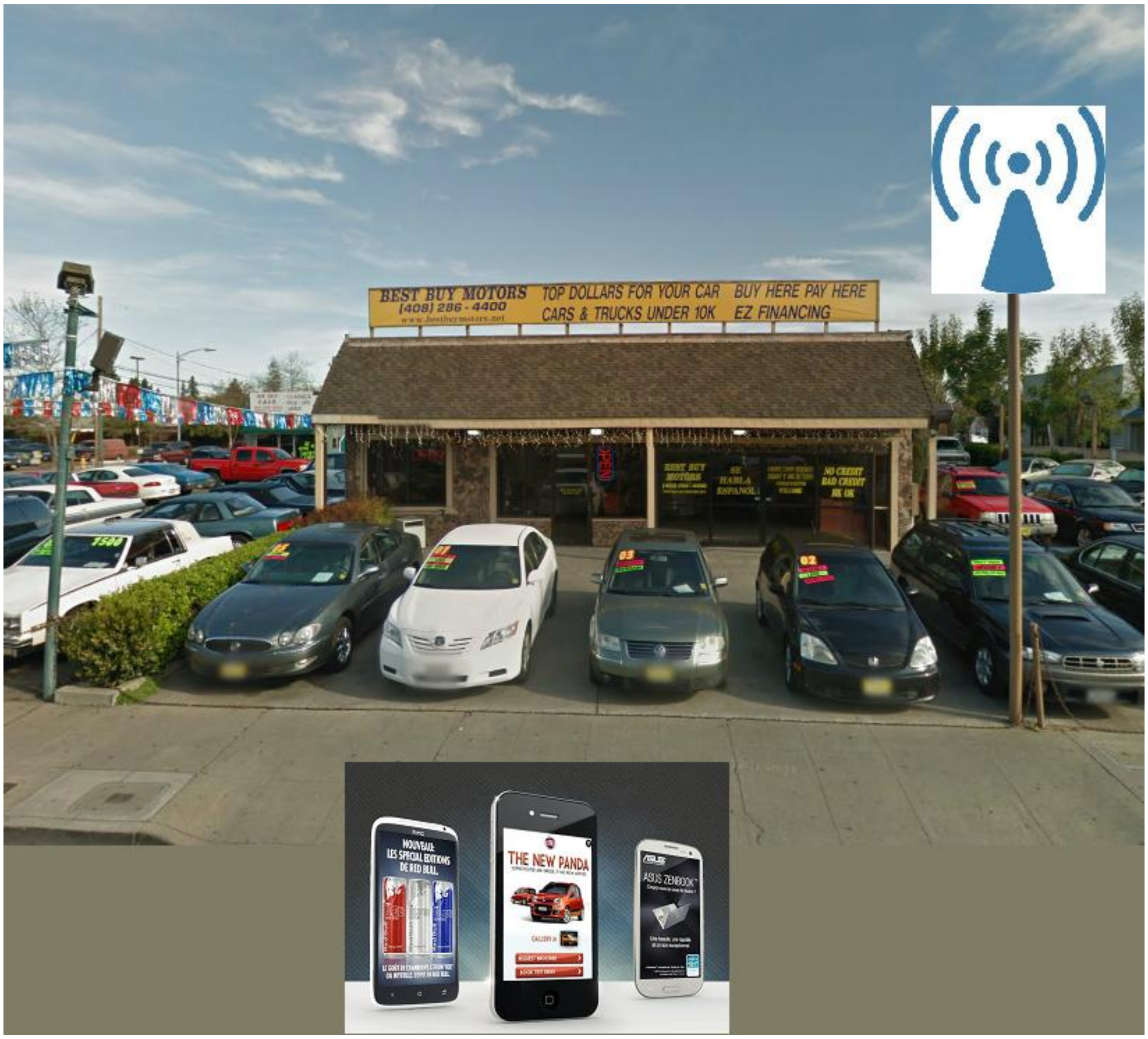
Secondly, it can guarantee that your friends are physically close to you because the range of Wi-Fi coverage is within 200 meters. The friends in cyber world can quickly turn into good friends in the real world.

Thirdly, the rich identities give Wi-Fi P2P devices a new life. The amazing visual effect, real time updates, dynamic information make the Wi-Fi data communications (file exchanges, voice, chatting, etc.) much funnier than ever before.

5.2 Business advertising with AP

In the past, the merchants need to use the TVs or light boxes besides their stores and restaurants. If their APs support the rich identities and the other features specified in this paper, the advertising will be much easier. The merchants upload pictures, detail descriptions in HTML format and embedded hyperlinks to Internet resources to their APs, set the correct domain and categories for their advertisement and turn the AP on. When people pass by driving and walking with their Wi-Fi devices which has certain software installed and the preferred domains and categories are properly set, their Wi-Fi devices can discover the AP and the picture and detail description and have them displayed on the screen of the device.

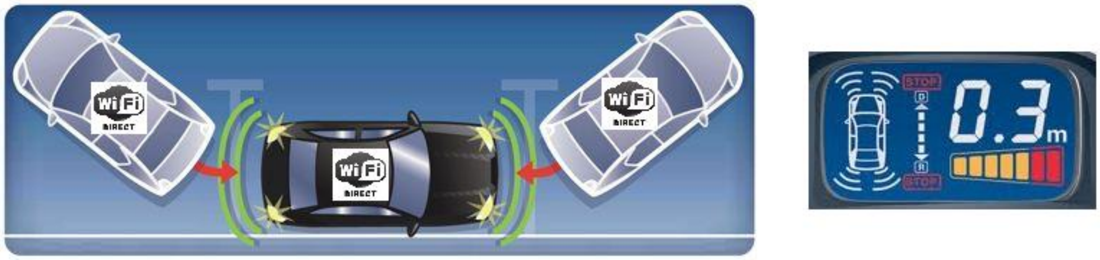
Figure 5-2 Example of Business Advertising with AP



5.3 Vehicle Collision-Avoidance System based on Wi-Fi P2P + GPS

To implement a “Vehicle Collision-Avoidance System”, there should be a device installed on one vehicle, and the device should know the shape and real-time positions of the other vehicles nearby. Then the device calculates whether the vehicle it is installed has kept safe distances to all other vehicles. If not, the devices will alarm the driver or crew to be careful to avoid the collisions.

Figure 5-3 The principle of the Collision-Avoidance System based on Wi-Fi P2P



If the vehicles have Wi-Fi P2P devices installed, and each of Wi-Fi P2P devices supports dynamic tags such as real-time positioning information got from an on-device GPS chipset, then each device installed on one vehicle can receive the real-time position information of other vehicles so that a simple collision-avoidance system can be implemented.

Acronyms

AP	Access Point
GPS	Global Positioning System
MIME	Multipurpose Internet Mail Extensions
NFC	Near Field Communication
P2P	Point-to-point
RFID	Radio Frequency Identification
RSA	Rivest, Shamir, & Adleman (public key encryption technology)
TBD	To Be Defined
UTF-8	UCS Transformation Format—8-bit
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN, Wireless Local Area Network
WPA(2)	Wi-Fi Protected Access (version 2)

Bibliography

Apple. "IOS7 features list." 10 July 2013. Apple official website. <http://www.apple.com/ios/ios7/features/#airdrop>.

Daniel Camps-Mur, Andres Garcia-Saavedra and Pablo Serrano. "Device to device communications with WiFi Direct: overview and experimentation." Wireless Communications, IEEE. Volume: 20, Issue: 3 (2013).

Google. "Wi-Fi Direct." 4 2012. Android Developer's website. 22 July 2013 <http://developer.android.com/guide/topics/connectivity/wifip2p.html>.

He Shouchun, Meenakshy Harikumar, Naga Tulasi Soujanya Vadrevu. Development of a new service using Wi-Fi Direct. Santa Clara, 2013.

IAN, Paul. "Wi-Fi Direct vs. Bluetooth 4.0: A Battle for Supremacy." 26 Octber 2010. PC World. <http://www.pcworld.com/article/208778/Wi_Fi_Direct_vs_Bluetooth_4_0_A_Battle_for_Supremacy.html>.

Lewis, Richard D. When Cultures Collide: Leading across cultures. London: Nicholas Brealey, 2006.

Moataghed, Dr. Keyvan. "COEN331 Wireless and Mobile Networks handouts." July 2013.

Patricia Tamarit, Carlos T. Calafate, Juan-Carlos Cano, Pietro Manzoni. "BlueFriend: Using Bluetooth Technology for Mobile Social Networking." Mobile and Ubiquitous Systems: Networking & Services, MobiQuitous, 2009. MobiQuitous '09. 6th Annual International. Toronto, ON, 2009. July.

Ramezani, E. and S.R. Ameli. "Bluetooth Virtual Community: Bluetooth and Social Networking in Tehran Subway." Computer and Information Technology (CIT), 2012 IEEE 12th International Conference on. Chengdu, Sichuan, China: IEEE, 2012. 602 - 609.

Wi-Fi Association. "Wi-Fi CERTIFIED Wi-Fi Direct™: Personal, portable Wi-Fi® that goes with you anywhere, anytime." 2010. Wi-Fi Alliance homepage. <http://www.wi-fi.org/discover-and-learn/wi-fi-direct>.

Wi-Fi Association. Wi-Fi Security. <http://www.wi-fi.org/discover-and-learn/security>.

WIKIPEDIA. Beacon frame. <http://en.wikipedia.org/wiki/Beacon_frame>.

WikiPedia. "Wi-Fi Direct." <http://en.wikipedia.org/wiki/Wi-Fi_Direct>.