International Journal of Engineering Research and Technology.
ISSN 0974-3154 Volume 6, Number 4 (2013), pp. 585-592

http://www.irphouse.com

Wireless Network Service Using Wi-Fi Push

[1]Anoop Sarathy, [2]Lokesh Bhat and [3]Swati S. Giri

Department of Telecommunication, BNMIT
#235,6th main, 6thCross, Mico layout,
BTM 2nd Stage, Bangalore-560076.

Abstract

Push technology reverses the Internet's content delivery model. Before push, content publishers had to reply upon the end-users own initiative to bring them to a web site or download content. With push technology the publisher can deliver content directly to the users PC, thus substantially improving the likelihood that the user will view it. Push content can be extremely timely, and delivered fresh several times a day. Push can also be used to pump data in the form of news, current affairs and sportsetc, to many computers connected to the internet. Updating software is one of the fastestgrowing uses of push. It is a new and exciting way to manage software update andupgrade hassles. Using the internet today without the aid of a push application can be atedious, time consuming, and less than dependable. Computer programming is an inexactart, and there is a huge need to quickly and easily get bug fixes, software updates, andeven whole new program out to people. Users have to manually hunt down information,search out links, and monitor sites and information sources.

Keywords: Beacon Frames, GAS, ANQP, IEEE802.11u, Server, Access point, client.

1. Introduction

In order to compare wireless communication with wired communication, therefollows an introduction to wireless communication. In the year 1895, Guglielmo Marconiopened the way for modern wireless communication by transmitting Morse code over along distance using electromagnetic waves. From then on, wireless communication has significantly developed into an important element of modern

society. Wireless communication means transmitting signals and data without cables using electromagneticwaves. The principles of wireless communication are that signals are amplified first, thenthey are emitted by the emitting terminal, finally they are received by the receivedterminal and the data can be accessed.

The best means to provide service to the clients (end user) is by communicating wirelessly. There is no physical medium to be laid between the provider and the client.Thus helps to reach every end user without any discrepancies. Our main aim is to reach out every individual and to provide them services without their intervention keeping in mind with their personal interests.

WLAN typically extends an existing wired local area network. WLANs arebuilt by attaching a device called the access point (AP) to the edge of the wired network.Clients communicate with the AP using a wireless network adapter similar in function toa traditional Ethernet adapter. For WLANs that connect to the Internet, WirelessApplication Protocol (WAP) technology allows Web content to be more easilydownloaded to a WLAN and rendered on wireless clients like cell phones, PCsand laptops. Wi-Fi is the name of a popular wireless networking technology that usesradio waves to provide wireless high-speed internet and network connections. Thecornerstone of a wireless network is a device known as an access point (AP). The primaryjob of an access point is to broadcast a wireless signal that computers/mobiles can detect and "tune" into. Since wireless networks are usually connected to wired ones, an accesspoint also often serves as a link to the resources available on the a wired network, such asan Internet connection.

2. Beacon Frames

According to IEEE 802.11 protocol, beacon frames are periodically transmitted bythe Access Point (AP) and carry mostly network specific information. All the wirelessstations (or wireless clients) with in the "vicinity" of transmission range of AP receivecorresponding beacon and use the information embedded in it for various purposes. Thearrangement of information in beacon is standardized by 802.11, thus facilitatingcommunication between different devices manufactured by different vendors.If a wireless client needs to communicate using 802.11 network, it first listens tothe beacon frame. This beacon frame is periodically broadcast by the AP and contains thenecessary and basic information about the network. If the station decides to communicatewith a particular AP (as there can be multiple beacons from multiple APs in the vicinity),it attempts Association. This decision to attempt Association with a particular AP isbased on the parameters standardized by the protocol and are present in variousfields of the beacon. Once Association is successful then only the communication can start.

2.1 Introduction Beacon Fame

IEEE 802.11 [2] attempts to model wireless networks as a replacement for wirednetworks. For example, a wireless client needs to “associate” with an Access

Point (AP)before it can communicate, which is similar to the act of connecting a wired client to anEthernet bridge or a switch. Once a wireless client is associated to an AP, it can no longercommunicate with other APs around it without using sophisticated software [1]. Thiswired model needlessly limits the capabilities of wireless networks. For example, when awireless client can hear APs other than the one with which it is associated, this restrictedcommunication model prevents them from exchanging useful information. One exampleof useful information that APs could communicate to non-associated clients would be theAP load, which clients can use to improve their AP selection strategy. In this paper, wepresent beacon-stuffing, a low bandwidth communication protocol for IEEE 802.11networks that enables APs to communicate with clients without association. This enablesclients to receive information from nearby APs even when they are disconnected, or whenconnected to another AP. Our scheme is complimentary to 802.11 association and worksby overloading 802.11 management frames while not breaking the standard.

The beacon-stuffing protocol is based on two key observations. First, clientsreceive beacons from APs even when they are not associated to them. Second, it ispossible to overload fields in the beacon and other management frames to embed data.APs embed content in Beacon and Probe Response frames, while clients overload ProbeRequests to send data. Beacon-stuffing enables a number of new applications, andexplored three of them. First, APs can embed network selection content into beacons withthe beacon-stuffing protocol, for example to broadcast performance or pricinginformation about their wireless network. The clients can use this information to selecteither the “best” AP or the best wireless network to connect to. For this application, bothclients and APs benefit from being able to exchange information without association.

Another application of beacon-stuffing is for APs to send location-specific advertisementsto nearby clients that are not associated to it. This can be used to advertise networkservices (e.g. network printing), or real-world goods and services (e.g. hospital). Finally,as an extension of location-specific ads, APs may want to provide coupons to nearbyclients without requiring association. Beacon-stuffing also provides an alternativemechanism to implement several other location-based applications that have beenexplored in prior work [3,4].

Mechanism for Broadcasting Information:Our approach is based on the “push model” of information delivery. The key idea is to overload IEEE 802.11 beacons to carry additional information. Beacon frames are used to announce the presence of a Wi-Fi network. As a result, an 802.11 client receives the beacons sent from all nearby APs, even when it is not connected to any network. In fact, even when a client is connected to a specific AP, it periodically scans all the channels to receive beacons from other nearby APs to keep track of networks in its vicinity. The client does not have to transmit anything to receive the beacons; it merely has to listen. This push model is in contrast to the model currently being used where a client establishes an Internet connection, transmits information about its location (obtained in a variety of ways), and “pulls” information relevant to that location.

Under common environmental conditions, the beacons frames have a range of 100-200 meters. Thus, information carried in these beacons is implicitly “localized”. For example, if the AP is located in a restaurant, only clients who are physically in thevicinity of the restaurant will receive the messages (presumably, an advertisement for therestaurant) transmitted by the restaurant AP. Thus, we eliminate the need to explicitly

locate the client. By varying transmit power, and encoding scheme, we can further controlthe range of the beacons. Although beacons are typically sent as the lowest data rate,beacon-stuffing APs may choose to transmit beacons at higher data rates to reduce theairtime utilization or to control the range.

The information to be broadcasted is a string of bytes. In most cases, we expectthe information to be a short text message. However, these techniques could also be usedto deliver non text information in next-gen. The AP splits the message into smallerfragments, and transmits each fragment in a separate beacon. The size of the fragmentdepends on the mechanism being used. The fragment sent in each beacon has thefollowing format:

UniqueID : SequenceNumber : MoreFlag : InfoChunk

UniqueID identifies the message being broadcast, and SequenceNumber is thefragmentnumber, and MoreFlag informs the client if it should expect more fragments: i.e.,

the last fragment has a value of 0, and all others have a value of 1. Finally, the InfoChunkhas the contents of the message. Clients reassemble the message after receiving allfragments.

The main difference between the techniques is the field in the beacon packet thatis used to carry the messages. The format of the 802.11 beacon packet is shown in Fig 2.1. Commercial Aps only allow us to modify the SSID in the beacon packet, and this isone of the techniques that we use. However, if we have access to the source code runningon the AP, other fields can be easily modified. Specifically, either modify the BSSID, oradd an extra Information Element to the beacon. None of the three techniques require anymodifications to the hardware or firmware of the client device to receive the messages.

For the SSID and BSSID based techniques, a simple user-level application is sufficient toreassemble the fragmented messages. The third technique, which uses InformationElement, requires changes to the Wi-Fi driver on the client devices.

SSID Concatenation: The SSID field in the Beacon carries the name of the wireless network. The maximum length is 32 bytes. Assuming the UniqueID is 1 byte and SequenceNumber and MoreFlag can fit in 1 byte, we are left with 29 bytes for the InfoChunk. Fragments are transmitted in successivebeacons. The maximum length of eachunique message is 3712 bytes.This approach is easy to implement. Most commercial APs provide a userinterface to set the SSID. Windows and Linux clients can query the beacon’s SSID from

user-level, so there is no need for kernel modification on client devices. A simple userlevelprogram is sufficient to reassemble the fragments and display the reassembledmessage. For example, a hotspot in Starbucks has an SSID of Starbucks. Our approachenables to send longer messages at a reasonable bandwidth.

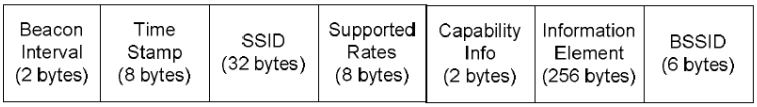

Fig. 3.1: Some fields in the IEEE 802.11 beacon packet.

3. Protocols

A) GAS Protocol: Generic Advertisement Service (GAS) An IEEE 802.11u service that provides over-the-air transportation for frames of higher-layer advertisements between STAs or between a server in an external network and a non-AP STA. GAS may be used while STAs are in the unauthenticated, un-associated or associated states. GAS supports higher-layer protocols that employ a query/response mechanism. The purpose of Generic Advertisement Service (GAS) functionality is to enable a non-AP STA to identify the availability and information related to the desired network services, e.g., information about available SSPs and/or SSPNs or other external networks. While the specification of network services information is out of scope of IEEE 802.11, there is a need for non-AP STAs to query for information on network services provided by SSPNs or other external networks beyond an AP before they associate to the wireless LAN. GAS defines a generic container toadvertise network services information over an IEEE 802.11 network. Public Actionframes are used to transport this information.

B) ANQP Protocol: The Access Network Query Protocol (ANQP) is the query and response protocol for a Wi-Fi station (STA) to automatically discover available Wi-Fi hotspots and to automatically authenticate the stations using hotspot-supported Extensible Authentication Protocol (EAP) mechanisms. Using ANQP a mobile device can discover a range of information, including the hotspot operator's domain name; roaming partners accessible via the hotspot along with their credential type and EAP method supported for authentication; IP address type availability; and other useful metadata for networkselection.

4. Metodology

*A) High Level Design:*The following is a, simplified sequence of events used by an IEEE 802.11u-capable: mobile device to authenticate with a hotspot. 1. The mobile device comes within radio range of one or more hotspots and receivestheir beacons. These beacons indicate support for the IEEE 802.11u protocol viathe Interworking

element. The SSID element in the beacon provides the Wi-Finetwork service. (In the next steps, it's assumed that the mobile device doesn'trecognize any of the received SSIDs.)2. The mobile device uses GAS to post an ANQP query to an access point for eachof the SSIDs discovered in step 1. In response, each access point provides thehotspot operator's name and network access identifier (NAI) realm list.3. The mobile device next retrieves its credential (realm) from local storage and usesit to authenticate. The mobile device then compares that realm to the list ofroaming partner's realms it retrieved in step 2 (in the NAI realm list). If there is amatch, the mobile device knows it should be able to successfully authenticate withthat network. If there is more than one match, the mobile device uses operatorpolicy to determine which Wi-Fi network to join.4. The mobile device next retrieves its operator policy for network selection fromlocal storage and looks up an ordered list of operator name and preference-levelpairs for each of its roaming partners. The mobile device then compares thehotspot operator's name(s) received in step 2 with this list and selects the networkhaving the highest preference level.5. The mobile device authenticates to that network using its credential. In caseswhere the mobile device is in possession of more than one credential (forexample, the mobile has a SIM and username/password credentials), it can use theNAI realm list to learn the acceptable credential type(s) and EAP method(s).As we've just described, using ANQP with GAS, a mobile device can query thenetwork prior to authentication to determine if the hotspot is operated by one of itsroaming partners, as well as the EAP method and credential type to use. A mobiledevice's connection manager can now autonomously (that is, without user intervention)determine which hotspot to select taking into account operator policies, authenticate tothat Wi-Fi network, and establish link-layer security using WPA2-Enterprise. Wi-Fi hasbecome as easy-to-use and as secure as 3G Cellular.

B) Message Flow: The client generic event line, generic event message area, transaction of the data,path taken by the request is explained pictorially. The fig 4.1 shows the message flowdiagram.

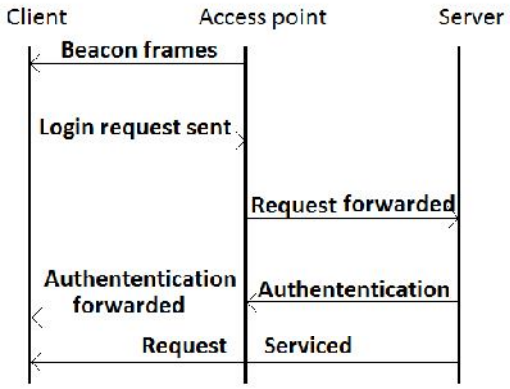

Fig 4.1: Timeline Diagram.

The beacon frames are transmitted by the access point continuously. The beaconframes carries the webpage in the SSID field that has to be pushed on to the client evenbefore the client gets connected to the network. By this we mean that the SSID field in thebeacon frame doesn't merely contain the name of the network that the client can getconnected to. The client gets the webpage that's being pushed by the access point as soon as it switches on the Wi-Fi. The client then, if it wants to, enters the username and password in the given fields and then submits it. The message will be encoded and then transmitted to the access point wirelessly.

The access point decodes the received information using the inverse encodingThe server uses the username and password and it checks with the existingusername and passwords in the database. If it finds any matches then the serverauthenticates. Authentication often involves verifying the validity of the datum. Theserver while authenticating also services the request sent by the client. Depending on thetype of client the request will be serviced.logic. This will also extract the username and password sent by the client which will befurther transmitted to the server.

5. Implementation

We have used wireshark to carry out the encoding and decoding of the message.Wireshark is a free and open-source packet analyser. It is used for networktroubleshooting, analysis, software and communications protocol development, andeducation. Wireshark allows the user to put network interface controllers thatsupport promiscuous mode into that mode, in order to see all traffic visible on thatinterface, not just traffic addressed to one of the interfaces configured addresses andbroadcast/multicast traffic. However, when capturing with a packet analyzer inpromiscuous mode on a port on a network switch, not all of the traffic traveling throughthe switch will necessarily be sent to the port on which the capture is being done.

Wireshark is software that "understands" the structure of different networkingprotocols. Thus, it is able to display the encapsulation and the fields along with theirmeanings of different packets specified by different networking protocols. Wiresharkuses pcap (packet capture) consists of an application programming interface (API)for capturing network traffic) to capture packets, so it can only capture the packets on thetypes of networks that pcap supports.

1. Data can be captured "from the wire" from a live network connection or read from afile that recorded already-captured packets.
2. Live data can be read from a number of types of network, including Ethernet, IEEE802.11, PPP, and loopback.
3. Captured network data can be browsed via a GUI, or via the terminal (command line)version of the utility, TShark.
4. Captured files can be programmatically edited or converted via command-lineswitches to the "editcap" program.

5. Data display can be refined using a display filter.
6. Plug-ins can be created for dissecting new protocols.

6. Conclusion

Push was created to alleviate two problems facing users of net. The first problem is information overload. The volume and dynamic nature of content on the internet is a impediment to users, and has become an ease-of -use of issue. Without push applications can be tedious, time consuming, and less than dependable. Users have to manually hunt down information, search out links, and monitor sites and information sources. Push applications and technology building blocks narrow that focus even further and add considerable ease of use. The second problem is that most end-users are restricted to low bandwidth internet connections, such as 33.3 kbps modems, thus making it difficult to receive multimedia content. Push technology provides means to pre-deliver much larger packages of content.Push technology enables the delivery of multimedia content on the internet through the use of local storage and transparent content downloads. Like a faithful delivery agent, push, often referred to as broadcasting, delivers content directly to user transparently and automatically.

7. Acknowledgement

The completion of any task would remain unfinished without the mention of individuals who guided and nurtured us through their guidance, support and discussions. Acknowledging Prof. P Venkat Rao and Arun V S also the IEEE publications.

References

[1] R. Chandra, V. Bahl, and P. Bahl. MultiNet: Connecting to multiple IEEE 802.11networks using a single wireless card. In Proceedings of the IEEE Conference on computer Communications (Infocom), 2004.

[2] IEEE802.11b/D3.0. Wireless LAN Medium Access Control (MAC) and Physical(PHY) Layer Specification: High Speed Physical Layer Extensions in the 2.4 GHz Band.

[3] J. H. Kang and G. Borriello. Ubiquitous computing using wireless broadcast. InWMCSA, december 2004.

[4] J. H. Kang and G. Borriello.Harvesting of location-specific information through wifinetworks. In LoCA, pages 86–102, 2006

[5] Chandra R., Padhye J., Ravindranath L., Wolman A. Beacon-Stuffing: Wi-Fi withoutAssociations. In Proceedings of the Eighth IEEE workshop Mobile Computing Systemsand Applications (Tucson, Arizona, February 26-27, 2007).