IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 8, October 2014.
www.ijiset.com
ISSN 2348 – 7968

A survey on mobile phone related issues in Wi-Fi calling

Andrew Kipkebut[1], Timothy sawe[2]

Department of Mathematics and computing, Kabarak University, Nakuru, Kenya .

Department of Mathematics and computing, Kabarak University, Nakuru Kenya

Abstract: Wi-Fi is an industry name for wireless local area network (WLAN) communication technology based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 wireless standards. It uses 2.4 GHz UHF and 5 GHz SHF radio waves. It is a system of wirelessly connecting devices allowing connection between devices without the use of cables. Many devices including smart phones can use Wi-Fi in their operations. Wi-Fi Calling uses Wi-Fi to provide better mobile phone coverage. It is based on a Smart Wi-Fi Application that is pre-loaded onto a phone. Wi-Fi Calling enables you make calls and send texts via Wi-Fi when you're out of cell signal range provided Wi-Fi is available. Wireless networks are more often than not physically exposed, so the chances of intrusion in these networks are as well high. This paper investigates mobile phone Wi-Fi calling related issues .A finding from this paper has indicated positive effects on the use of Wi-Fi calling hence consequently a need for more in-depth and longitudinal research into the issues related to this splendid technology.

Keywords: Wi-Fi Calling, WLAN, IEEE, GHz, Smartphones, 802.11

I. INTRODUCTION

Wi-Fi Calling uses Wi-Fi to provide better mobile phone coverage. It is based on a Smart Wi-Fi application an example is Kineto software that is pre-loaded onto a smart phone. Currently one can use Wi-Fi calling in iPhone, Android, and other Smartphone e.g. Samsung Galaxy S2, HTC one, Motorola Defy among others. Wi-Fi calling allows you to make and receive calls, access unlimited high-speed data, send and receive messages over a wireless internet connections[1]. Using Wi-Fi calling is easy and cheaper to use. You simply connect to an available Wi-Fi network of your choice, confirm Wi-Fi calling is enabled on your phone, and continue to use all of your favorite device features. The Apps for Wi-Fi calling provide a great way to save money and make calls from anywhere with a Wi-Fi connection.

II. LITERATURE REVIEW

Wi-Fi is increasingly becoming the preferred mode of internet connection all over the world. To access this type of connection, one must have a wireless adapter on their computer as shown in Figure.1. Wi-Fi provides wireless connectivity by emitting frequencies between 2.4GHz to 5GHz based on the amount of data on the network. Areas which are enabled with Wi-Fi connectivity are known as Hot Spots. One can use advanced software to detect and request connection to Hotspots.

Figure 1: Wi-Fi in action(source ©2008 howstuffworks.com)

To start a Wireless connection for a phone, it is important that the wireless router is plugged into the internet connection and that all the required settings are properly installed as shown Figure 2.

Figure 2: A Wi-Fi phone (Source howstuffworks)

The major advantage of Wi-Fi is that it is compatible with almost every operating system, game devices, Phones, projectors and advanced printer. The 3G radio is disabled when Wi-Fi calling is active in order to maintain long-lasting battery life on the smartphone[2] as shown in Figure. 3.

ISSN 2348 – 7968

Figure. 3- Kineto smartphone using a Wi-Fi calling app.(source Kineto.com)

III. HOW WI-FI CALLING WORKS

The inclination toward communications junction is continually accelerating, with multiple services leveraging common infrastructures. One example is fixed mobile convergence (FMC), which enables users to rely on a single device or handset for all their communications needs[3].
FMC eliminates the requirement for both fixed and mobile phones and enables a single device to use both wireless local and wide area networks. Unlicensed Mobile Access (UMA), also referred to as Generic Access Network (GAN), is a variety of FMC that enables the convergence of fixed, mobile and Internet-based telephony[4]. Essentially UMA known familiarly as Wi-Fi calling enables a mobile phone to connect over a Wi-Fi network and hand off seamlessly to a GSM cellular network if the caller moves beyond the Wi-Fi range as shown in Figure. 4.

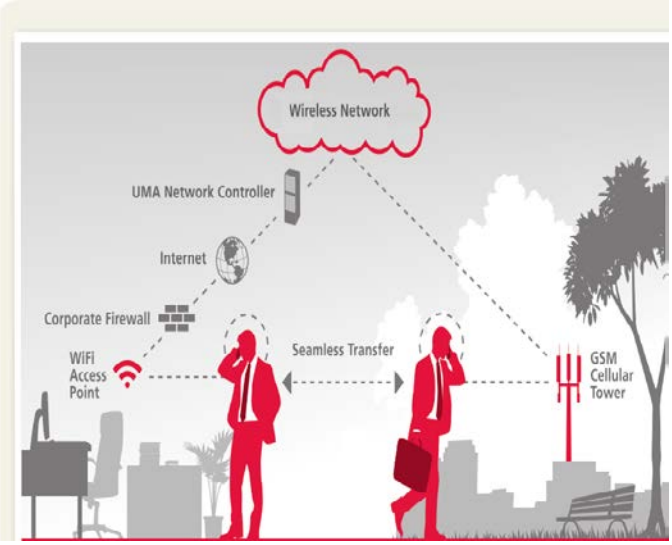

Figure. 4: Unlicensed mobile Access (UMA) devices support a seamless hand offs between a Wi-Fi and a GSM cellular network without user intervention.(Source ©2010 Rogers communication)

This technology provides enhanced coverage and seamless delivery of voice, data and messaging. It can also reduce your telephony costs. Unlike other kinds of FMC, Wi-Fi calling does not interrelate with the organization's private branch exchange (PBX). This makes deployment relatively quick and easy. The input requirements for Wi-Fi calling include the following[4].

A. UMA-enabled dual mode handsets (with GSM and Wi-Fi radios).

Unlicensed Mobile Access or UMA, is the commercial name used by mobile carriers for external IP access into their core networks. The phones should be able to switch seamlessly between the two signals. More recently, the system has been called Wi-Fi Calling by a number of handset manufacturers, including Apple and Samsung, a move that is being mirrored by carriers like T-Mobile USA.

B. A broadband Wi-Fi network

It should be capable of handling voice service of which most of them do. If not, a configuration of the existing network may be required to optimally support Wi-Fi calling.

C. A Wi-Fi Calling plan.

Normally service providers offer different plan options to meet the varying needs of organizations and individual employees, including an access-only plan, a plan for unlimited calling to your local area code, and one for unlimited national calling.
In a nutshell how Wi-Fi calling is as creating an IP extension of the carrier's wireless network. Essentially, the Internet becomes a transport medium for voice calls. When a dual mode handset encounters a Wi-Fi access point that it recognizes, it establishes an IP connection with the access point. The handset then establishes a session with the UMA Network Controller (UNC), which serves as the gateway between the Internet and the wireless network. After authentication and security protocols have been exchanged, the handset is connected to the wireless network. Once the connection is established, the call is transferred seamlessly to the Wi-Fi network. The handover process is completely transparent to the user, just as when a user passes from one wireless network cell to another. Depending on the subscriber's plan, Wi-Fi calling can zero rate calls to the local area code . Data streams, including email, SMS, MMS and WAP browsing, are also passed between the handset and the UNC. As well as decreasing wireless data usage, this can result in superior performance.

IV. WI-FI SECURITY THREATS

Despite the productivity, convenience and cost advantage that Wireless LAN offers, the radio waves used in wireless networks create a risk where the network can be hacked. In this paper we will narrow down to three examples of important threats to WI-FI calling.

ISSN 2348 – 7968

A. Denial of Service attack

In this kind of attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. Due to the nature of the radio transmission, the WLAN are very vulnerable against denial of service attacks. The relatively low bit rates of WLAN can easily be overwhelmed and leave them open to denial of service attacks[5]. By using a powerful enough transceiver, radio interference can easily be generated that would enable WLAN to communicate using radio path.

B. Spoofing and Session Hijacking

This normally happens when an the attacker gains access to privileged data and resources in the network by assuming the identity of a valid user [6] This may occur because 802.11 networks do not authenticate the source address, which is Medium Access Control (MAC) address of the frames. Attackers may therefore spoof MAC addresses and hijack sessions. Moreover, 802.11 does not require an Access Point to prove it is actually an Access Point . This facilitates attackers who may masquerade as Access Point. To eliminate spoofing, proper authentication and access control mechanisms need to be placed in the WLAN.

C. Eavesdropping

Eavesdropping is secretly listening to the private conversation of others without their consent, as defined by Black's Law Dictionary[7]. Eavesdropping involves attack against the confidentiality of the data that is being transmitted across the network. Wi-Fi calling is susceptible to these kind of attacks since by their nature, wireless LANs intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any wireless LAN installation. In the wireless network, eavesdropping by the third parties is the most significant threat because the attacker can intercept the transmission over the air from a distance, away from the premise of an organization.

V. WIRED EQUIVALENT PRIVACY (WEP)

Wired Equivalent Privacy, a deprecated wireless network security standard, is a security protocol for wireless networks. The biggest problem with WEP is when the installer doesn't enable it initially. Even bad security is generally better than no security. Normally when people do use WEP, they forget to change their keys/passwords periodically. Having many clients in a wireless network potentially sharing the identical key for long periods of time is a well-known security vulnerability. If you keep your key long enough, someone can grab all the frames he needs to crack it. Wired Equivalent Privacy (WEP) is a standard encryption for wireless networking. It is a user authentication and data encryption system from IEEE 802.11 used to overcome the security threats. Basically, WEP provides security to WLAN by encrypting the information transmitted over the air, so that only the receivers who have the correct encryption key can decrypt the information. The following section explains the technical functionality of WEP as the main security protocol for WLAN.

A. How WEP Works?

When deploying WLAN, it is important to understand the ability of WEP to improve security. WEP uses a pre-established shared secret key called the base key, the RC4 encryption algorithm and the CRC-32 (Cyclic Redundancy Code) checksum algorithm as its basic building blocks. WEP supports up to four different base keys, identified by KeyIDs 0 1 2 3.[8] Each of these base keys is a group key called a default key, meaning that the base keys are shared among all the members of a particular wireless network. Some implementations also support a set of nameless per-link keys called key-mapping keys. The WEP specification does not permit the use of both key i.e. mapping keys and default keys simultaneously, and most deployments share a single default key across all of the 802.11 devices. WEP tries to achieve its security goal in a very simple way. It operates on MAC Protocol Data Units (MPDUs), the 802.11 packet fragments. To protect the data in an MPDU, WEP first computes an integrity check value (ICV) over to the MPDU data. This is the CRC-32 of the data. WEP appends the ICV to the end of the data, growing this field by four bytes. The ICV allows the receiver to detect if data has been corrupted in flight or the packet is an outright forgery. Next, WEP selects a base key and an initialization vector (IV), which is a 24-bit value. WEP constructs a per-packet RC4 key by concatenating the IV value and the selected shared base key. WEP then uses the per-packet key to RC4, and encrypt both the data and the ICV. The IV and KeyID identifying the selected key are encoded as a four-byte string and pre-pended to the encrypted data. WPA2 (an improvement on Wi-Fi Protected Access) is a much better alternative to WEP. WPA2 uses Advanced Encryption Standard for encryption. Taking into consideration of the vulnerabilities and flaws in WEP, the Wi-Fi Alliance, created the Wi-Fi Protected Access (WPA) standard which is a subset of the 802.11i . WPA was designed to improve upon the security feature deficits of WEP. The technology is designed to work with existing Wi-Fi products that have been enabled with WEP. Figure. 5 depicts a WEP-encoded MPDU[9].

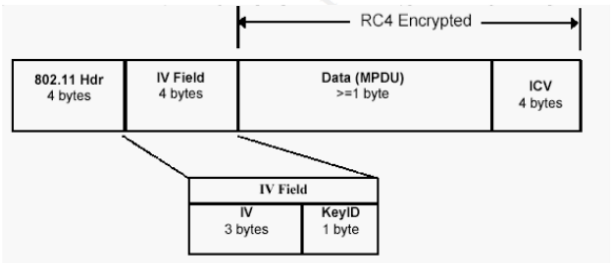

Figure. 5: Encoded MPDU(Source Penton Media, Inc. 2002).

ISSN 2348 – 7968

The IEEE 802.11 standard defines the WEP base key size as consisting of 40 bits, so the per-packet key consists of 64 bits once it is combined with the IV. The difference in key length does not matter in the overall security. An attacker can compromise its privacy goals with comparable effort regardless of the key size used.

B. *Weaknesses of WEP*

WEP has undergone much scrutiny and criticism that it may be compromised. What makes WEP vulnerable? The major WEP flaws can be summarized into three categories:[9]

1) ***No forgery protection:*** There is no forgery protection provided by WEP. Even without knowing the encryption key, an adversary can change 802.11 packets in arbitrary, undetectable ways, deliver data to unauthorized parties, and masquerade as an authorized user. Even worse, an adversary can also learn more about the encryption key with forgery attacks than with strictly passive attacks.

2) ***No protection against replays:*** WEP does not offer any protection again replays. An adversary can create forgeries without changing any data in an existing packet, simply by recording WEP packets and then retransmitting later. Replay, a special type of forgery attack, can be used to derive information about the encryption key and the data it protects.

3) ***Reusing initialization vectors:*** By reusing initialization vectors, WEP enables an attacker to decrypt the encrypted data without the need to learn the encryption key or even resorting to high-tech techniques. While often dismissed as too slow, a patient attacker can compromise the encryption of an entire network after only a few hours of data collection.

A report done by a team at the University of California's computer science department [10] presented the insecurity of WEP which expose WLAN to several types of security breaches. The ISAAC (Internet Security, Applications, Authentication and Cryptography) team which released the report quantifies two types of weaknesses in WEP. The first weakness emphasizes on limitations of the Initialization Vector (IV). The value of the IV often depends on how vendor chose to implement it because the original 802.11 protocol did not specify how this value is derived. The second weakness concerns on RC4's Integrity Check Value (ICV), a CRC-32 checksum that is used to verify whether the contents of a frame have been modified in transit. At the time of encryption, this value is added to the end of the frame. As the recipient decrypts the packet, the checksum is used to validate the data. Because the ICV is not encrypted, however, it is theoretically possible to change the data payload as long as you can derive the appropriate bits to change in the ICV as well. This means data can be tampered and falsified.

VI. PRACTICAL SOLUTIONS FOR SECURING WLAN

Despite the risks and vulnerabilities associated with wireless networking, there are certainly circumstances that demand their usage. Even with the WEP flaws, it is still possible for users to secure their WLAN to an acceptable level. This could be done by implementing the following actions to minimize attacks into the main networks :

A. *Changing Default SSID*

Service Set Identifier (SSID) is a unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to a particular WLAN. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID[11]. In fact, it is the only security mechanism that the access point requires to enable association in the absence of activating optional security features. Not changing the default SSID is one of the most common security mistakes made by WLAN administrators. This is equivalent to leaving a default password in place.

B. *Utilize VPN*

A VPN is a much more comprehensive solution in a way that it authenticates users coming from an untrusted space and encrypts their communication so that someone listening cannot intercept it. Wireless AP is placed behind the corporate firewall within a typical wireless implementation. This type of implementation opens up a big hole within the trusted network space. A secure method of implementing a wireless AP is to place it behind a VPN server. This type of implementation provides high security for the wireless network implementation without adding significant overhead to the users. If there is more than one wireless AP in the organization, it is recommended to run them all into a common switch, then connecting the VPN server to the same switch. Then, the desktop users will not need to have multiple VPN dial-up connections configured on their desktops. They will always be authenticating to the same VPN server no matter which wireless AP they have associated with . **Figure. 6** shows secure method of implementing a wireless AP.

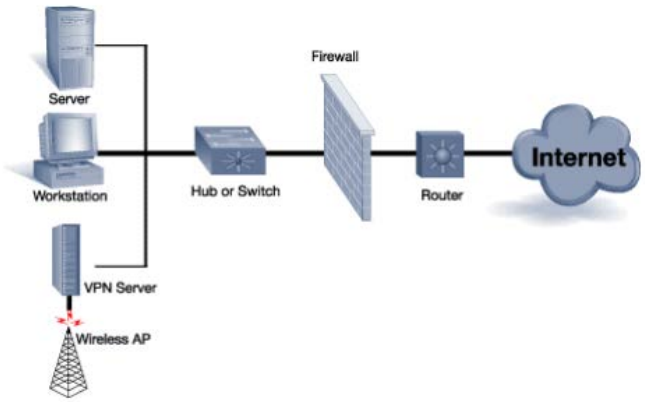

Figure. 6: Securing a wireless AP[12]

ISSN 2348 – 7968

C. Utilize Static IP

By default, most wireless LANs utilize DHCP (Dynamic Host Configuration Protocol) to more efficiently assign IP addresses automatically to user devices. A problem is that DHCP does not differentiate a legitimate user from a hacker. With a proper SSID, anyone implementing DHCP will obtain an IP address automatically and become a genuine node on the network. By disabling DHCP and assigning static IP addresses to all wireless users, you can minimize the possibility of the hacker obtaining a valid IP address. This limits their ability to access network services. On the other hand, someone can use an 802.11 packet analyzer to sniff the exchange of frames over the network and learn what IP addresses are in use. This helps the intruder in guessing what IP address to use that falls within the range of ones in use. Thus, the use of static IP addresses is not fool proof, but at least it is a deterrent. Also keep in mind that the use of static IP addresses in larger networks is very cumbersome, which may prompt network managers to use DHCP to avoid support issues.

D. *Access Point Placement*

WLAN access points should be placed outside the firewall to protect intruders from accessing corporate network resources. Firewall can be configured to enable access only by legitimate users based on MAC and IP addresses. However, this is by no means a final or perfect solution because MAC and IP addresses can be spoofed even though this makes it difficult for a hacker to mimic. Try orienting antennas to avoid covering areas outside the physically controlled boundaries of the facility. By steering clear of public areas, such as parking lots, lobbies, and adjacent offices, the ability for an intruder to participate on the wireless LAN can be significantly reduced. This will also minimize the impact of someone disabling the wireless LAN with jamming techniques.

VII. PHONE RELATED ISSUES IN WIFI CALLING

A. *Compatibility*

Wi-Fi calling is not available to all phones. The Wi-Fi calling functionality is supported on the device. The Wi-Fi calling service providers such as T-mobile(US), Kinetos and Rogers(Canada) provide phones which have the Wi-Fi functionality embedded on the device. Unlike other applications, Wi-Fi calling functionality must be coded within the operating system of the device and not installed onto the phone. This gives the service providers the exclusive ownership of the Wi-Fi calling facility. The service providers should provide mobile phones which have Wi-Fi calling facility.

B. *Interference.*

It has been proved that most of the home appliances such as Bluetooth devices, microwaves, neighbours Wi-Fi or even obstructions from buildings and humans can affect the performance of Wi-Fi enabled devices. A study by Epitiro, a UK based research shows that interference from other radio-based devices can degrade the performance of Wi-Fi connectivity. This is because the 802.11 family of Wi-Fi protocols with the frequency of 2.4GHz is shared with many other types of services such as microwaves, baby monitors, cordless phones and many home communication devices[13]. Since the primary requirement for Wi-Fi calling is Wi-Fi enabled phone, this effect may affect the performance of the call.

C. *Quality of Service(QoS) of Wi-Fi calling*

As much as Wi-Fi calling improve the quality of service in the area of coverage, there are some Wi-Fi calling issues that negatively affect the quality of service. Since Wi-Fi calling enabled phones use multiple signals, calls may be more prone to disconnect when the handset transition from Wi-Fi to standard GSM network. While using Wi-Fi in calling, the range from the access point is important. Moving beyond the range may lead to dropped calls. Furthermore, phone handover from Wi-Fi to GSM is not supported for international calls. The international Wi-Fi calls must be completed on Wi-Fi.

D. *Phone Battery Drain*

Wi-Fi calling will need no other option but to turn on Wi-Fi. Enabling Wi-Fi on cell phones drains the battery fast because it always looks for possible connections, network and information. Though power Saving Mode protocol is supposed to prevent the Wi-Fi from consuming the power too quickly, a study has proved otherwise[14]. The study found out that when a variety of access points use this mode, the setup wasted power and unfairly prioritized some devices over others. There are applications though that can be installed on the smartphones to manage the battery strength on the phone. An application such as JuiceDefender(Android) and myBatteyLife(iPhone) by KVapps helps in battery management by adjusting settings of phones automatically based on several factors.

VIII. TOOLS FOR PROTECTING WLAN

There are some products that can minimize the security threats of WLAN such as:

A. AirDefense

It is a commercial wireless LAN intrusion protection and management system that discovers network vulnerabilities, detects and protects a WLAN from intruders and attacks, and assists in the management of a WLAN. AirDefense also has the capability to discover vulnerabilities and threats in a WLAN such as rogue APs and ad hoc networks. Apart from securing a WLAN from all the threats, it also provides a robust WLAN an example of such tools is Motorola's AirDefense Services Platform (ADSP) simplifies the management, monitoring and protection of WLAN environments.

B. *Isomair Wireless Sentry*

This product from Isomair Ltd. automatically monitors the air space of the enterprise continuously using unique and

ISSN 2348 – 7968

sophisticated analysis technology to identify insecure access points, security threats and wireless network problems. This is a dedicated appliance employing an Intelligent Conveyor Engine (ICE) to passively monitor wireless networks for threats and inform the security managers when these occur. It is a completely automated system, centrally managed, and will integrate seamlessly with existing security infrastructure. No additional man -time is required to operate the system.

C. Wireless Security Auditor(WSA)

This is IBM prototype of 802.11 wireless LAN security running on Linux on IPAQ PDA which helps network administrators to close vulnerability by automatically auditing a wireless network for proper security configuration an example of such tool is Elcomsoft Wireless Security Auditor

IX. CONCLUSION

Since Wi-Fi operates in unlicensed spectrum; it is easy to be deployed by anyone, anywhere; and the required hardware is simple and cheap. Not surprisingly, it has become one of the most widely deployed and popular wireless standards. Travelers and mobile workers frequently turn to free Wi-Fi internet connections in hotels, airports, conference centres and business facilities. These Wi-Fi connections are particularly risky as they are often set up without proper security settings. There is a growing trend of hackers setting up mock Wi-Fi hotspots in public places, in order to capture and record data. The introduction of Wi-Fi calling makes cell phone coverage available almost anywhere . However the WLAN vulnerabilities remain a challenge to the realization of Wi-Fi calling which is primarily caused by WEP as its security protocol. However, these problems can be solved with standards, such as 802.11i.Users can protect their conversations by practicing the suggested actions that are mentioned in this paper, based on the cost and the level of security that they wish.

X. REFERENCES

[1] T-Mobile Inc, “About Wi-Fi calling”, 2014, support.t-mobile.com/docs/DOC-1680.

[2] Andrew Von Nagy, **“**Kineto Smart Wi-Fi Calling on T-Mobile”, 2011, http://www.revolutionwifi.net/2011/10/kineto-smart-wi-fi-calling-on-t-mobile.html.

[3] Ljubljana “Fixed-mobile convergence with survey of numbering related issues”, 2008, Page 2, http://www.erodocdb.dk/docs/doc98/official/pdf/ECCRep126.pdf.

[4] Rogers Inc, “Wi-Fi Calling for business- An executive overview” Rogers White paper, Pg 4, http://redboardbiz.rogers.com/wp-content/uploads/2010/09/Wi-Fi_Calling_whitepaper_Dec2_EN.pdf.

[5] M. Handley, E. Rescorla, "Internet Denial-of-Service Considerations", 2006 RFC 4732

[6] Mirkovic, J., Jevtic, N. & Reiher, P. ”A practical IP (Spoofing Defense through Route-based Filtering”, Technical report, 2006, University of Delaware.

[7] Bryan A. Garner, “Black's Law Dictionary”, 8th Edition 2004.

[8] Chetan Nanjunda Mathur and K.P. Subbalakshmi , “A Light Weight Enhancement to RC4 Based Security for Resource Constrained Wireless Devices” Vol. 5, 2007, I. J. Network Security, Pg. 205-212

[9] Rafidah Abdul Hamid, ”Wireless LAN: Security Issues and Solutions”, GIAC Security Essentials Certification (GSEC) SANS Institute, 2003, version 1.4b

[10] Borisov, Nikita, Goldberg, Ian and Wagner, David. “Security of the WEP Algorithm.” 13 Dec. 2002. URL: http://www.isaac.cs.berkeley.edu/isaac/wep- faq.html (3 Dec. 2002).

[11] Cisco, “An Overview of the Voice Over IP Wireless Network”, http://www.cisco.com/en/US/docs/voice_ip_comm/cuipph/7921g/5_0_1/english/administration/guide/7921wrnt.pdf.

[12] Penton Media, Inc. “Use a VPN for Wireless Security.” 20 Dec. 2002. URL: http://www.mobile-and-wireless.com/Articles/Index.cfm?ArticleID=27095(18 Dec. 2002).

[13] Epitiro Technologies Limited, “A study into the Effect of the ‘Air mile’on consumer broadband performance ” Page 6.

[14] Eric Rozner, Ramachandran Ramjee, Vishnu Navda, Shravan Rayanchu NAPman: *Network-Assisted Power Management for WiFi Devices.* International Conference on Mobile Systems, Applications and Services (MobiSys), San Francisco, CA, June 2010.