QUALITY OF SERVICE (QOS) IN WI-MAX

Ravikant Kaushik[1], Gaurav Khurana[2], Gimmy Dagar[3], Vikas Rohal[4]

[1, 2, 3, 4] *Student, , BMIET, Sonipat (Haryana)*

ravikantkaushik1@gmail.com, khurana.gaurav1989@gmail.com, dagar.gimmy@gmail.com, rohalvikas18@gmail.com

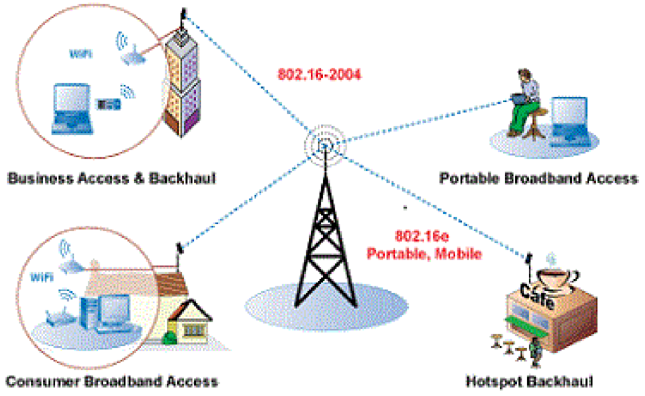
Abstract

This paper is mainly concern with Quality of service in WI-MAX technology. WI-MAX is providing broadband wireless access to the masses and presenting alternatives to digital subscriber lines (DSL) and cable broadband access. WI-MAX is based on IEEE 802.16 standard and is scalable. Super narrow lanes can enables a lot of traffic over them without disturbance. Many technologies and softwares like pathloss4.0,Global Mapper are used for line of sight (LOS) clearance coverage; the technology behind WI-MAX has been optimized to provide excelled non-line of sight (NLOS) coverage.QOS in broadband wireless access is a difficult and complicated business, as it adds an unpredictable radio link and potentially heavy user contention to the usual non-deterministic behavior of IP packet networks. Carriers therefore need to be aware of how QOS works – and what it can do – in the different flavors of 802.16, and how it relates to the more familiar 3G technologies. WiMAX quality of service (QOS) depends crucially on the 802.16 Layers 1 and 2, as these govern the all-important base-station/user-terminal radio access – an inherently difficult environment compared to, say, a wireline broadband network. Because the d/e forms of 802.16 are aimed at different applications – fixed terminals only and mobile terminals, respectively – there are significant differences in technology between them. In particular, 802.16d used Orthogonal Frequency Division Multiplexing.

Keywords: *wireless broadband, wireless fidelity (WIFI), WIMAX.*

1. INTRODUCTION

Wimax stands for Worldwide Interoperability for Microwave Access. Wimax technology is a telecommunications technology that offers transmission of wireless data via a number of transmission methods; such as portable or fully mobile internet access via point to multipoints links. The Wimax technology offers around 72 Mega Bits per second without any need for the cable infrastructure. Wimax technology is based on Standard that is IEEE 802.16, it usually also called as Broadband Wireless Access. WiMAX Forum created the name for Wimax technology that was formed in Mid June 2001 to encourage compliance and interoperability of the Wimax IEEE 802.16 standard. Wimax technology is actually based on the standards that making the possibility to delivery last mile broadband access as a substitute to conventional cable and DSL lines. Wimax (802.16) technology often misinterpreted by the people by the names of mobile WiMAX, 802.16d, fixed WiMAX and 802.16e. Actually 802.16-2004 or 802.16d is developed by the third party as a standard and it is also referred to called as Fixed WiMAX because this standard is lacking behind just because of the non-mobility feature that's why it's often called as Fixed WiMAX. During the maturity period of Wimax (802.16) technology some of the amendments were made to the above mentioned 802.16d and they referred this amending standard as 802.16e. 802.16e introduced mobility and some other features amongst other standards and is also known as Mobile WiMA . These QOS capabilities matter enormously Without sophisticated QOS, many wireless services – from legacy data services to complex interactive IMS-based services – don't work as well as they could.


WiFi
802.16-2004
Business Access & Backhaul
Portable Broadband Access
802.16e
Portable, Mobile
WiFi
Cafe
Consumer Broadband Access
Hotspot Backhaul

But QOS in broadband wireless access is a difficult and complicated business, as it adds an unpredictable radio link and potentially heavy user contention to the usual non-deterministic behavior of IP packet networks. Carriers therefore need to be aware of how QOS works – and what it can do – in the different flavors of 802.16, and how it relates to the more familiar 3G technologies.

And it's crucial to understand the extent to which 802.16 allows vendors wide scope for innovation in implementing improved algorithms for better QOS. This report aims to highlight the importance of over-the-air QOS in the WiMAX operator business case, and to look at the options for implementing QOS capabilities in WiMAX base-station equipment. WiMAX Standardization. WiMAX is based on the 802.16d (or more formally 802.16-2004 or European Telecommunications Standards Institute (ETSI) HiperMAN) and 802.16e standards published in 2004 and 2006, respectively. The scope of these standards is fairly broad, but it is important to remember that they address only Layers 1 and 2 of the network. Higher-layer network architectures and interfaces are not defined by these standards, unlike the situation in the 3GPP and 3GPP2 specifications for 3G mobile networks, for example.To address this gap, the WiMAX Forum is developing a core-network architecture as well as specifications for functions such as Radio Resource Management. This is in addition to the well known work in developing interoperability and conformance test profiles, and the associated WiMAX equipment certification program. So WiMAX is being subject to an essentially full system-level standardization effort, especially in relation to mobility and some of the more advanced applications that WiMAX is likely to support in the future. But WiMAX quality of service (QOS) depends crucially on the 802.16 Layers 1 and 2, as these govern the all-important base-station/user-terminal radio access – an inherently difficult environment compared to, say, a wireline broadband network. Because the d/e forms of 802.16 are aimed at different applications – fixed terminals only and mobile terminals, respectively – there are significant differences in technology between them. In particular, 802.16d used Orthogonal Frequency Division Multiplexing (OFDM or ODM for those in a hurry) and 802.16e uses Orthogonal Frequency Division Multiple Access (OFDMA or ODMA). The capabilities of these technologies have a direct impact on end-user services and QOS.

Table 1: Some Features of Fixed & Mobile WiMAX

WiMAX Fixed (IEEE 802.16-2004/ETSI HiperMAN)	WiMAX Mobile (802.16e)
Frequencies specified as sub-11GHz	Frequencies specified as sub-6GHz
Scalable channel widths specified (1.75MHz to 20MHz)	Scalable OFDMA 128, 512, 1024, 2048 (not 256)
256-carrier OFDM	Sub channelization
FDD and TDD multiplexing	Questions over backward compatibility (256-carrier OFDMA not specified)
Deterministic QOS	
Adaptive modulation (BPSK/QPSK/16QAM/64QAM)	
Uplink subchannelization	

802.16 Key Features

Table 1 summarizes some of the key technical features of the fixed and mobile forms of 802.16. Two basic characteristics are a radio interface that uses adaptive modulation to adapt performance to the prevailing channel conditions of theuser, and OFDM techniques to reduce the impact of multipath interference. This makes WiMAX suitable for near- and non-line-of-sight environments, such as urban areas. Another important feature is the 802.16 media access control (MAC), which, if required, can offer deterministic QOS. This is crucial, because it makes it practical to offer services such as voice and T1/E1-type services. The 802.16e revision was important primarily because it introduced the new physical layer based on OFDMA, but with variable subcarrier permutations from 128 carriers to 2048 carriers. This is sometimes called scalable OFDMA (SOFDMA), since the number of subcarriers would typically scale with the channel bandwidth. Bandwidth scalability is one of the most important advantages of OFDMA. As the WiMAX Forum observes: The fundamental premise of the IEEE 802.16 MAC architecture is QoS. It defines Service Flows which can map to DiffServ code points or MPLS flow labels that enable end-to-end IP-based QoS. Additionally, subchannelization and MAP-based signaling schemes provide a flexible mechanism for optimal scheduling of space, frequency, and time resources over the air interface on a frame-by-frame basis. With high data rate and flexible scheduling, the QoS can be better enforced. As opposed to priority-based QoS schemes, this approach enables support for guaranteed service levels including committed and peak information rates, latency, and jitter for varied types of traffic on a customer-by-customer basis...

2. QOS IN WIRELESS SYSTEMS

QOS means different things to different end users, as much depends on the application and the use to which the end user is putting it. It’s therefore usual to employ a range of measurable performance parameters from which those appropriate to the particular end user can be selected. These parameters are most commonly:

- Bandwidth
- Latency
- Jitter
- Reliability

An obvious question for WiMAX is where the technology fits in with other wireless access technologies (such as 3G and WiFi), but also with fixed-line technologies (such as DSL or fiber), since WiMAX has fixed-access applications. Bandwidth - the unit-time packet throughput - is probably the most basic QOS parameter for many end users, and is obviously limited by the physical-layer pipe between the base station and the client terminal in WiMAX (and other wireless technologies), and also by the number of clients that are active in parallel, since the overall system bandwidth is shared. Generally, if the overall bandwidth of a given system is big enough, some of the other QOS parameters will be less of an issue. For example, with enough bandwidth, access contention among different users is eliminated, which simplifies protocols and reduces latency. Other parameters, such as latency and jitter, only come in once you are servicing multiple users in parallel and groups of subscribers to the system. Latency - the end-to-end packet transmission time - is caused by the granularity of the physical-layer chain, and is typically almost 5ms in 802.16 systems. Latency is also affected by how packet queuing, various QOS protocols, and user characterizations are implemented. Jitter - the variation of latency over different packets - has to be limited by packet buffering. Since the buffer on the mobile terminal is likely to be small, jitter control in wireless networks tends to fall onto the base station, which has to ensure that different packets receive different prioritization if necessary. Reliability - the proportion of successfully delivered packets - leads to more complications in wireless networks than in fixed-line ones, and the problems are specifically acute in mobile networks. The issue is that wireless networks have an inherent unreliability because of the vicissitudes of radiowave propagation - especially to mobile terminals with small antennas and low powers in cluttered environments such as urban areas. So packet loss (and numbers of errored packets) will be higher than for fixed-line networks. This produces a particular problem for wireless IP networks. In a wired IP environment, the physical connection between two stations is more or less errorfree. If there is a packet loss end-to-end, it’s then a pretty safe bet that the loss was deliberate - caused, for example, by a midpoint router dropping a certain packet because of congestion within the network. Such midway deliberate dropping of packets is used in turn by end-to-end protocols, such as Transmission Control Protocol (TCP), as a signal to adapt end-user packet traffic to the available network bandwidth

Table 2: Key Wireless Technologies & Their MAC characteristics

	3G HSPDA	**WiMax 802.16.**	**WiMax 802.16e**	**WiFi**
Bandwidth, MHz	5	<20	20	20
Data rates,Mbit/s	14.4	75	75	11.54
bit/Hz	2.9	3.75	3.75	2.7
Multiple access	TDMA, CDMA	OFDMA	OFDMA	CSMA
Duplexing	FDD	TDD/FDD/ HD-FDD	TDD	
Mobility	FULL	portable	Nomadic/full	Portable
Coverage	LARGE	Mid	Mid	Small

TCP Has Two Main Tasks:

• Provide reliability by controlling end-to-end retransmission of errored or lost packets

• Provide throttle control by limiting connection speed to maximum speed of transport medium. So, if TCP detects a packet loss, it assumes that a router in the middle of the network dropped that packet on purpose. At that point, TCP will assume that the network was congested, it will lower the end-user transmission speed, and it will also retransmit that packet. By lowering the transmission speed, TCP thus tries to even out the bandwidth given to the end user. “The problem with TCP is that, as soon as that packet drop occurs in a wireless system, you cannot be sure that it was deliberate. Even worse, there is a very high probability that it wasn’t deliberate, because a wireless environment is not as secure as a wired environment. So, in such a case, the TCP protocol, by lowering the transmission speed, actually does the opposite of what it should do,” says Freescale's Rouwet. “One of the many jobs that the wireless MAC layer has is to overcome this problem.” Figure 2 shows the unfortunate effect (known as the TCP packet-loss problem) that results. The window size is the size of the buffer on the receiving device; TCP sends this figure to the transmitting device, which in turn will send only enough bytes to fill the window before pausing and waiting for an acknowledgement of successful reception to resume transmission. TCP throttles back the transmission rate under the assumed congestion by reducing the window size, and this causes the radio link to be underutilized.

3. MEDIUM ACCESS CONTROL LAYER

The IEEE 802.16 MAC is a scheduling one where the subscriber station (SS) that wants to attach to the network, has to compete once when it initially enters the network. A time slot allocation is made by the base station (BS) which can be enlarged and constricted. It remains ssigned to the subscriber station meaning that other stations are not supposed to use the same resources. This scheduling algorithm has its advantages since it remains stable under overload and oversubscription, has more bandwidth efficiency and also allows the base station to control QoS, meaning that it is balancing the resources among the needs of the subscriber stations. The main goal of the MAC layer is to manage the resources of the air interface efficiently. Indeed, access and bandwidth allocation algorithms must serve hundreds of terminals per channel. Those terminals can eventually be shared by multiple end users. To support a large variety of services such as voice, data or internet connection, the 802.16 MAC must accommodate both continuous and bursty traffic. The issues concerning the transport efficiency are also addressed at the interface between the MAC and the PHY layers. The modulation and coding schemes are specified in a burst profile adjusted in function of each burst sent to each SS. The MAC can make use of bandwidth-efficient burst profiles under favorable link conditions and shift to more reliable and robust ones if the opposite is the case even though the spectral efficiency will be lower.The MAC includes service-specific convergence sublayers (ATM and Packet) that interface to layers above. At the core, there is the MAC common part sublayer that carries out the key MAC functions. Below the common part sublayer is the privacy sublayer. Extensive bandwidth allocation and QoS mechanisms are provided, but the details of scheduling and reservation management have not been specified in the standard. The functions of the common part sublayer will be discussed more in the following paragraphs. On the downlink, data to Subscriber Stations (SSs) are multiplexed in TDM fashion. The uplink is shared between SSs in TDMA fashion. The 802.16 MAC is connection-oriented, according to which, all services, including connectionless services, are mapped to a connection.This provides a mechanism for requesting bandwidth, associating QoS and traffic parameters, transporting and routing data to the appropriate convergence sublayer, and all other actions associated with the contractual terms of the service. Connections are referenced with 16-bit connection identifiers (CIDs) and may require continuously granted bandwidth or bandwidth on demand. Upon entering the network, the SS is assigned three management connections in each direction. These three connections reflect the three different QoS requirements used by different management levels.

The first of these is the basic connection, which is used for the transfer of short, time-critical MAC and radio link control (RLC) messages. The primary management connection is used to transfer longer, more delay-tolerant messages such as those used for authentication and connection setup. The secondary management connection is used for the transfer of standards-based management messages such as Dynamic Host Configuration Protocol (DHCP), Trivial File Transfer Protocol (TFTP), and Simple Network Management Protocol (SNMP). In addition to these management connections, SSs are allocated transport connections for the contracted services. Transport connections are unidirectional to facilitate different uplink and downlink QoS and traffic parameters. The MAC builds the downlink subframe starting with a frame control section containing the DLMAP and UL-MAP messages. These indicate PHY transitions on the downlink as well as bandwidth allocations and burst profiles on the uplink. The advanced technology of the 802.16 PHY requires equally advanced radio link control (RLC), particularly the capability of the PHY to transition from one burst profile to another. The RLC must control this capability as well as the traditional RLC functions of power control and ranging. Burst profiles for the downlink are each tagged with a Downlink Interval Usage Code (DIUC). Those for the uplink are each tagged with an Uplink Interval Usage Code (UIUC). Burst profile determines the modulation and FEC and is dynamically assigned according to link conditions. It is determined burst by burst and per subscriber station. There is always a trade-off between capacity and robustness in real time. Their utilization has roughly doubled capacity for the same cell area. Burst profile for downlink broadcast channel is well-known and robust, but other burst profiles can be configured “on the fly”. SS capabilities are recognized at registration.

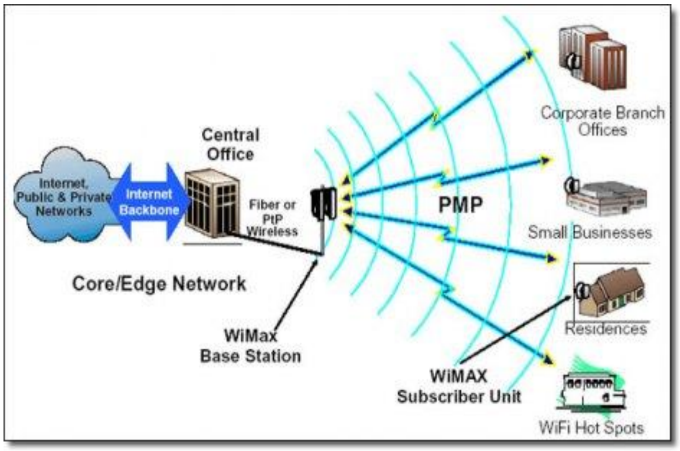
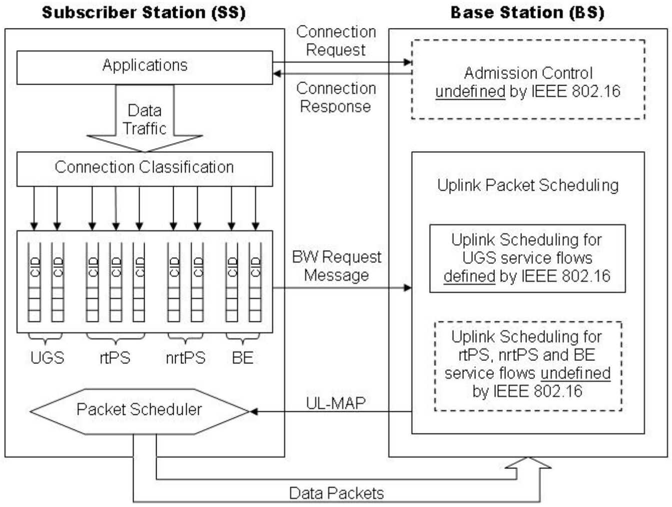


Table 2: Key Wireless Technologies & Their MAC Characteristics

802.16 MAC: Overview

• Point-to-Multipoint
• Metropolitan Area Network
• Connection-oriented
• Supports difficult user environments
- High bandwidth, hundreds of users per channel - Continuous and burst traffic
- Very efficient use of spectrum
• Protocol-Independent core (ATM, IP, Ethernet, …) • Balances between stability of contentionless and efficiency of contention-based operation
• Flexible QoS offerings
- CBR, rt-VBR, nrt-VBR, BE, with granularity within classes • Supports multiple 802.16 PHYs


Subscriber Station (SS)
Base Station (BS)
Connection Request
Connection Response
Applications
Admission Control undefined by IEEE 802.16
Data Traffic
Connection Classification
Uplink Packet Scheduling
CID
BW Request Message
Uplink Scheduling for UGS service flows defined by IEEE 802.16
Uplink Scheduling for rtPS, nrtPS and BE service flows undefined by IEEE 802.16
UGS
rtPS
nrtPS
BE
Packet Scheduler
UL-MAP
Data Packets

4. PHYSICAL LAYER

802.16a PHY Alternatives:

• OFDM (WirelessMAN-OFDM Air Interface)
256-point FFT with TDMA (TDD/FDD)
• OFDMA (WirelessMAN-OFDMA Air Interface)
2048-point FFT with OFDMA (TDD/FDD)
• Single-Carrier (WirelessMAN-SCa Air Interface)
TDMA (TDD/FDD)
BPSK, QPSK, 4-QAM, 16-QAM, 64-QAM, 256-QAM

In this section, we introduce the techniques that are used in the physical layer: Orthogonal Frequency Division Multiplexing (OFDM) and Orthogonal Frequency Division Multiple Access (OFDMA). Those techniques have been developed for the last few years to deliver broad band services that can be compared to those of wired services in terms of data rates. The main issue addressed for the PHY layer is to allocate the resources efficiently by assigning a set of subcarriers and by determining the number of bits to be transmitted for each subcarrier in an OFDMA system. An optimal algorithm has to be chosen to obtain a certain level of performance by considering some constraints such as delays, the total number of connected SS and the total power. Orthogonal frequency-division multiplexing (OFDM) is a transmission technique that is based on the same idea as frequency-division multiplexing (FDM). In FDM, multiple signals are sent out at the same time, but on different frequencies. It actually divides a broadband channel into many narrowband subchannels. In OFDM, a single transmitter transmits on several different orthogonal frequencies. This technique, associated with the use of advanced modulation techniques on each component, give a transmitted signal with high resistance to multi-path terference and a much higher spectral efficiency is obtained. As the chose of the manufacturers, the WiMAN OFDM PHY layer is the most commonly used because of the reasons previously quoted. It was also selected, rather than other techniques such as single-carrier (SC) or CDMA, due to its superior non line-of-sight (NLOS) performance. This multiplexing technique allows important equalizer design simplification to support operations in multipath propagation environments and overcome channel fading quite efficiently (Rayleigh channel model)

5. SUBCHANNELIZATION

The OFDM PHY layer supports UpLink (UL) subchannelization, with the number of subchannels being 16. This feature is particularly useful when a power-limited platform such as a laptop is considered in the subscriber station in an indoor environment. With a sub-channelization factor of 1/16, a 12-dB link budget enhancement can be achieved. Sixteen sets of 12 subcarriers each, are defined, where one, two, four, eight or all of the sets can be assigned to a subscriber station in the uplink. Eight pilot carriers are used when more than one set of sub-channels are allocated. This multiplexing technique supports Time Division Duplexing (TDD), in which the uplink and downlink share a channel but do not transmit simultaneously, and Frequency Division Duplexing.

REFERENCES

[1] Arbaugh, W.A. Wireless security is different. Computer, Volume: 36, 9 – 101, Issue: 8, Aug. 2003.
[2] Arbaugh, W.A. Your 802.11 wireless network has no clothes. Wireless Communications.
[3] Baghaei, N.; Hunt, R IEEE 802.11 wireless LAN security performance using multiple clients. Networks, 2004.
[4] Balachandran, A., Voelker, G., Bahl, P. and Rangan V. Characterizing user behavior and network performance in a public wireless LAN. In Proceedings of ACM.
[5] Bing, B., & Subramanian, R. A Novel Technique for Quantitative Performance Evaluation of Wireless LANs.
[6] Bing B. Measured performance of the IEEE 802.11 wireless LAN. In Proceedings
Conference on Local Computer Networks, pages 34-42, 1999.
[7] Borisov, B., I. Goldberg, & D. Wagner.
[8] Brown, B.; 802.11: the security differences between b and I. Potentials.
[9] M. Beck and E. Tews. Practical Attacks against WEP and WPA. In Second ACM conference on Wireless Network Security, 2008.
[10] N. Borisov, I. Goldberg, and D. Wagner. Intercepting mobile communications: the insecurity of 802.11.
[11] N. Cam-Winget, R. Housley, D.Wagner, and J.Walker. Security flaws in 802.11 data link protocols.
[12] S. Fluhrer, I. Mantin, and A. Shamir. Weaknesses in the Key Scheduling Algorithm of RC4..
[13] C. He and J. C. Mitchell. Analysis of the 802.11i 4-way handshake. In WiSe ’04: Proceedings of the 3rd ACM workshop on Wireless security, pages 43–50, New York, NY, USA, 2004. ACM.
[14] C. He and J. C. Mitchell. Security Analysis and Improvements for IEEE 802.11i. In The 12th Annual Network and Distributed System Security Symposium,
[15] IEEE Standard 802.11-1997, Information Technologytelecommunications And Information exchange Between Systems-Local And Metropolitan Area Networks-specific Requirements-part 11: Wireless Lan Medium Access Control (MAC) And Physical Layer (PHY) Specifications, 1997.
[16] IEEE Standard 802.11-1999, Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 1999.
[17] IEEE Standard 802.11i-2004, IEEE Standard for Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements, Part 11:

Wireless LAN Medium Access Control, (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC), Security Enhancements, 2004.

[18] IEEE Standard 802.11-2007, IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, 2007.

[19] KoreK. Next generation of WEP attacks, 2004. http://www.netstumbler.org/f18/next-generation-wepattacks-12277/index3.html#post93942.

[20] C. Kuo, A. Perrig, and J. Walker. Low-cost Manufacturing, Usability, and Security: An Analysis of Bluetooth Simple Pairing and Wi-Fi Protected Setup. In Usable Security (USEC), February 2007.

[21] Borisov, B., I. Goldberg, & D. Wagner. Intercepting Mobile Communications: The Insecurity of 802.11.