Wireless Communication Methodologies

&

Wireless Application Protocol

(Final Project)

By Sankara Krishnaswamy

31 Chadwick Circle
Apt # E
Nashua
NH – 03062
Ph: 603 – 791 – 8070 (W)
603 – 888 – 0053 (H)
Email: krisj1@hotmail.com

Executive Summary

Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path. In the 21-century, wireless communication and high-speed communication incorporating computation power, mobile network/internet access capability, and consumer electronics, become emerging technologies. Wireless communications are transmitted through the air via radio waves of various frequencies. Radio frequency radiation (RFR) is one of several types of electromagnetic radiation. Data transmission in a Wireless Communication is done by means of an unguided medium. Antennas are used to transmit the signal. There are different kinds of antennas like Whip, Panel and Dish. Antennas need to be placed at specific heights in relation to one another in order to transmit and receive signals. As a result, height is a determining factor in the design and siting of wireless communications facilities.

Analog and Digital technologies are the technologies that are used in the Wireless Communication Traditionally cellular phones have utilized analog transmission signals. But Analog technology has the noise pick up issue, which makes the technology inefficient. In order to diminish this noise and to provide greater calling capacity per channel, the cellular industry is beginning to use digital transmission signals. Digital technology has two forms: time division multiple access (TDMA) and code division multiple access (CDMA).

There are various wireless communications and controls that are available like Global System for Mobile communication (GSM), Enhanced Data GSM Environment (EDGE), General Packet Radio Service (GPRS), I-mode, Bluetooth Technology, Wireless Application Protocol (WAP).

This paper has two sections. The first section explains the wireless communication in general and how data transmission is done in wireless. It explains the analog and digital technologies It then analyses the two digital technologies (TDMA.CDMA). The communication control that are discussed in this papers are Global System for Mobile Communication (GSM), Enhanced Data GSM Environment (EDGE), General Packet Radio Service (GPRS), I-mode, Bluetooth Technology, Wireless Application Protocol (WAP).

Several wireless communication protocols exist today, and new ones are being developed in the quest for satisfying customer demand for efficient information retrieval as the industry's companies are competing for the market share in the new wireless world. The second section of the paper will completely analyze the Wireless Application Protocol. The Wireless Application

Protocol, commonly know as WAP, is an important development in the wireless industry because of its attempt to develop an open standard for wireless protocols, independent of vendor and air link. This section discusses WAP starting from evolution, technical architecture of WAP and how does WAP work. It also describes the advantages and the disadvantages of WAP and finally the future of WAP.

Contents

Wireless Communication Methodologies

1.1 What is Wireless?

Wireless is a term used to describe telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or the entire communication path. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless.

1.2 Data Transmission in Wireless

Wireless communications are transmitted through the air via radio waves of various frequencies. Radio frequency radiation (RFR) is one of several types of electromagnetic radiation. A cellular operates at frequencies between 800 and 900 MHz, and PCS operates at both 900 MHz as well as between 1,850 and 2,200 MHz.

Data transmission generally can happen using Guided Media (propagation is done though twisted pair, coaxial cable or optical fiber) or using unguided media (propagation is done though air, water, vacuum). Data transmission in a Wireless Communication is done by means of an unguided medium. In an unguided medium transmission and reception are achieved by means of an antenna. In the case of wireless for transmission the antenna radiates electromagnetic energy into the medium (usually air), and for reception, the antenna picks up electromagnetic waves from the surrounding medium.

The transmission is classified into directional and omni directional. In the case of directional configuration the transmitting antenna puts out a focused electromagnetic beam. The transmitting and receiving antennas must be aligned carefully. In omni directional configuration the transmitted signal spreads out in all direction and can be received by many antennas. It purely depends on the signal frequency, the higher the frequency of a signal, the more possibility of focusing into a directional beam. If the frequency range of 2Ghz to 40Ghz are referred as microwave frequencies. This frequency makes it possible to have directional configuration. Frequency range of 30Mhz to 1Ghz will be using omni directional configuration.

Microwave signals propagate in straight lines and are affected very little by the troposphere. They are not refracted or reflected by ionized regions in the upper atmosphere. Microwave beams do not readily diffract around barriers such as hills, mountains, and large human-made structures. Some attenuation (Loss of strength of the signal) occurs when microwave energy passes through trees and frame houses.

There are three general types of transmitting and receiving antennas used in the wireless communications technology. These include whip antennas, panel antennas, and dish antennas as shown in Figure-1. While whip and panel antennas are used to transmit and receive radio waves carrying conversation signals, dish antennas provide the link between the central computer switching system and the various whip and panel antennas used throughout the mobile conversation.

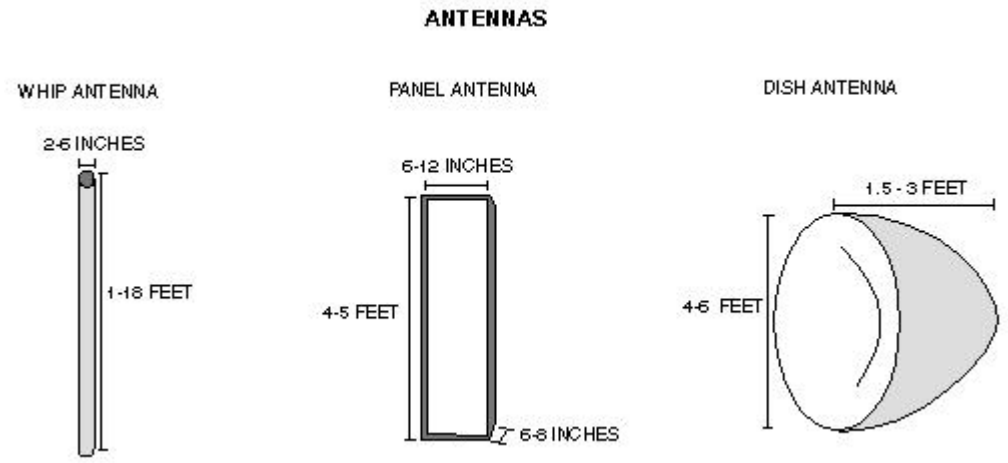


Figure - 1

A common type of microwave antenna is the parabolic “dish”. It has a size of about 3m in diameter. These antennas are mounted in a substantially heights above the ground level. With no intervening obstacles the maximum distance between the antenna is d=7.14 Kh. Here d is the distance between the antennas in kilometers, h is the antenna height in meters and K is an adjustment factor to account for the fact that microwaves are bent or refracted with the curvature of the earth and will hence propagate farther than the optical line of sight.

Antennas need to be placed at specific heights in relation to one another in order to transmit and receive signals. As a result, height is a determining factor in the design and siting of wireless

communications facilities. Typically there are three types of antenna support-structures used to place antennas at desired heights: lattice towers, monopoles, and building-attached facilities.

1.3 Analog and Digital Technologies

Traditionally, cellular phones have utilized analog transmission signals. In the analog technology, voice messages are electronically replicated and amplified as they are carried from the transmitting antenna to the receiving antenna. A problem with this technology is that the amplification procedure tends to pick up "noise," sometimes making the message difficult to hear.

In order to diminish this noise and to provide greater calling capacity per channel, the cellular industry is beginning to use digital transmission signals. In the digital technology, voice messages are converted into digits (zeroes and ones) that represent sound intensities at specific points in time. Because natural pauses in the conversation are eliminated, more calling capacity becomes available from the same amount of spectrum, thus reducing the need for new sites.

An added benefit is that the background noise that is generally heard in the analog system becomes inaudible. As illustrated in figure below the graphic difference between the two technologies is that analog signals are transmitted as continuous waves while digital technology converts the analog signal to binary digits. Figure- 2 shows the two different kinds of transmission signals.

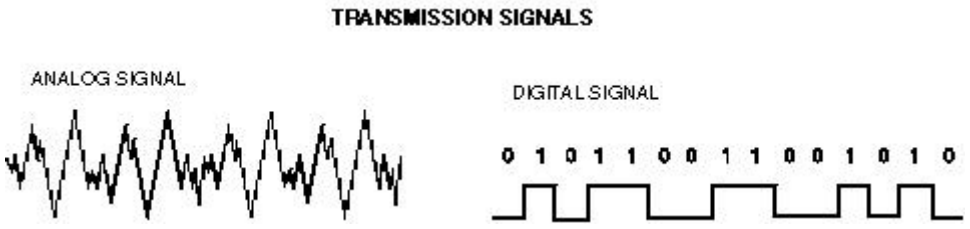


Figure - 2

There are currently two forms of digital technology: time division multiple access (TDMA) and code division multiple access (CDMA). Both of these forms of digital technology attempt to provide multiple access over one frequency, or channel. While TDMA is expected to increase calling capacity three to ten times over analog technology, CDMA is expected to increase calling capacity by ten to twenty times.

1.3.1Time division multiple access (TDMA)

TDMA is a digital transmission technology that allows a number of users to access a single radio-frequency (RF) channel without interference by allocating unique time slots to each user within each channel. The TDMA digital transmission scheme multiplexes three signals over a single channel.

TDMA is based on the IS-136 standard. The current TDMA standard for cellular divides a single channel into six time slots, with each signal using two slots, providing a 3 to 1 gain in capacity over advanced mobile-phone service (AMPS). Each caller is assigned a specific time slot for transmission. It offers efficient coverage and is well suited to emerging applications, such as wireless virtual private networks (VPNs),

1.3.2 Code division multiple access (CDMA)

CDMA is a coding scheme, used as a modulation technique, in which multiple channels are independently coded for transmission over a single wide band channel. In some communication systems, CDMA is used as an access method that permits carriers from different stations to use the same transmission equipment by using a wider bandwidth than the individual carriers. On reception, each carrier can be distinguished from the others by means of a specific modulation code, thereby allowing for the reception of signals that were originally overlapping in frequency and time. Thus, several transmissions can occur simultaneously within the same bandwidth, with the mutual interference reduced by the degree of orthogonality of the unique codes used in each transmission. CDMA permits a more uniform distribution of energy in the emitted bandwidth. The technology is used in ultra-high-frequency (UHF) cellular telephone systems in the 800-MHz and 1.9-GHz bands.

CDMA employs analog-to-digital conversion (ADC) in combination with spread spectrum technology. Audio input is first digitized into binary elements. The frequency of the transmitted signal is then made to vary according to a defined pattern (code), so it can be intercepted only by a receiver whose frequency response is programmed with the same code, so it follows exactly along with the transmitter frequency. There are trillions of possible frequency-sequencing codes; this enhances privacy and makes cloning difficult.

The CDMA channel is nominally 1.23 MHz wide. CDMA networks use a scheme called soft handoff, which minimizes signal breakup as a handset passes from one cell to another. The combination of digital and spread-spectrum modes supports several times as many signals per unit bandwidth as analog modes. CDMA is compatible with other cellular technologies; this allows for nationwide roaming.

1.4 Examples of wireless communications and control

1.4.1 Global System for Mobile Communication (GSM) -- a digital mobile telephone system used in Europe and other parts of the world; the de facto wireless telephone standard in Europe. A GSM network is composed of several functional entities, whose functions and interfaces are specified. The GSM network can be divided into three broad parts. The Mobile Station is carried by the subscriber. The Base Station Subsystem controls the radio link with the Mobile Station. The Network Subsystem, the main part of which is the Mobile services Switching Center (MSC), performs the switching of calls between the mobile users, and between mobile and fixed network users. The MSC also handles the mobility management operations. Not shown is the Operations and Maintenance Center, which oversees the proper operation and setup of the network. The Mobile Station and the Base Station Subsystem communicate across the Um interface, also known as the air interface or radio link. The Base Station Subsystem communicates with the Mobile services Switching Center across an interface.

A variety of data services are offered. GSM users can send and receive data, at rates up to 9600 bps, to users on POTS (Plain Old Telephone Service), ISDN, Packet Switched Public Data Networks, and Circuit Switched Public Data Networks using a variety of access methods and protocols, such as X.25 or X.32. Since GSM is a digital network, a modem is not required between the user and GSM network, although an audio modem is required inside the GSM network to inter work with POTS.

Other data services include Group 3 facsimile, as described in ITU-T recommendation T.30, which is supported by use of an appropriate fax adaptor. A unique feature of GSM, not found in older analog systems, is the Short Message Service (SMS). SMS is a bi-directional service for short alphanumeric (up to 160 bytes) messages. Messages are transported in a store-and-forward fashion. For point-to-point SMS, a message can be sent to another subscriber to the service, and an acknowledgement of receipt is provided to the sender. SMS can also be used in a cell-broadcast mode, for sending messages such as traffic updates or news updates. Messages can also be stored in the SIM card for later retrieval.

1.4.2 Enhanced Data GSM Environment (EDGE) -- a faster version of the Global System for Mobile (GSM) wireless service Universal Mobile Telecommunications System (UMTS) -- a broadband, packet-based system offering a consistent set of services to mobile computer and phone users no matter where they are located in the world. EDGE is intended to enable second-generation GSM (Global System for Mobile Communication) and TDMA (Time division Multiple Access) networks to transmit data at up to 384 kilobits per second (kbps). As it was initially developed for GSM systems only, it has also been called GSM384.

1.4.3 General Packet Radio Service (GPRS) -- A packet-linked technology that enables high-speed (up to 171.2 kilobit per second) wireless Internet and other data communications. GPRS will offer a tenfold increase in data throughput rates, from 9.6kbit/s to 115kbit/s. Using a packet data service, subscribers are always connected and always on line so services will be easy and quick to access.

GPRS involves overlaying a packet based air interface on the existing circuit switched GSM network. This gives the user an option to use a packet-based data service. To supplement a circuit switched network architecture with packet switching is quite a major upgrade. Packet switching means that GPRS radio resources are used only when users are actually sending or receiving data. Rather than dedicating a radio channel to a mobile data user for a fixed period of time, the available radio resource can be concurrently shared between several users. This efficient use of scarce radio resources means that large numbers of GPRS users can potentially share the same bandwidth and be served from a single cell.

GPRS achieves Faster data speeds and "always on" mobility. Connection to an abundance of data sources around the world, through support for multiple protocols, including IP.

1.4.4 I-Mode -- The world's first "smart phone" for Web browsing, first introduced in Japan; provides color and video over telephone sets. NTT DoCoMo's I-Mode is widely used in Japan, and is branching out to Europe and the USA. It is also providing serious competition for WAP. I-Mode recently signed a partnership deal with AT&T Wireless.

I-Mode is a proprietary service that allows users to connect directly to the Internet using Compact HTML (CHTML). It is a packet-switched service and is "always on." Users are charged only for downloading data. Most other wireless networks are circuit-switched and users are charged for

connection time. There are about 20 million wireless Internet users are there in Japan using this I-Mode service.

I-mode phones transmit data at a speed of 9600 bps. Although this sounds slow compared to ordinary 56kps computer modems, it is actually quite satisfactory for I-mode, since each email is limited to only 500 bytes and most I-modes sites are relatively lightweight (i.e., made up mostly of text data with very few graphics, averaging about 1.2K in size). Downloading email and I-mode pages usually takes only a few seconds. I-mode expects to introduce the world's first 3G (third generation) network based on the latest W-CDMA (Wideband Code Division Multiple Access) technology, which will speed data rates 40 times - and allow high-quality streaming video and audio**.** The advantage is that NTT DoCoMo built an Internet-style packet-switched network alongside its existing digital circuit-switched network in the beginning, and equipped its handsets with a micro- browser that understands cHTML a subset of HTML. Europe is only now beginning to build packet-switched (GPRS) networks.

I-Mode also has security issues since they are into Mobile commerce (m-commerce) and it is conducted on I-mode including mobile banking and security trading. So security is a serious issue.

1.4.5 Bluetooth Technology - Bluetooth is a simple, short-range Radio Frequency (RF) technology designed in 1998 by the leaders in the telecommunication and computer industries as the basis of truly wireless, global solution. This industry specification describes how mobile phones, computers, and personal digital assistants (PDA) can easily interconnect with each other and with home and business phones and computers using a short-range wireless connection.

Each device is equipped with a microchip transceiver that transmits and receives in a previously unused frequency band of 2.45 GHz that is available globally (with some variation of bandwidth in different countries). In addition to data, up to three voice channels are available. Each device has a unique 48-bit address from the IEEE (Institute of Electrical and Electronics Engineers) 802 standard. Connections can be point-to-point or multipoint. The maximum range is 10 meters. Data can be exchanged at a rate of 1 megabit per second (up to 2 Mbps in the second generation of the technology). A frequency hop scheme allows devices to communicate even in areas with a great deal of electromagnetic interference. Built-in encryption and verification is provided.

The primary disadvantage of Bluetooth is interference. It does not compete with the HomeRF and 802.11B standards vying for wireless networking dominance, but a pending FCC ruling allowing HomeRF to operate at a faster speed could cause interference with Bluetooth devices. Also, there are concerns with the 802.11b crowd about Bluetooth using the ISM (Instrument, Scientific and Medical) bandwidth. Also the farther away the Bluetooth devices are from the sending unit, there is more chance of interference in the presence of a Wireless Access Point. Another disadvantage is that Bluetooth-enabled devices at a range of 100 feet become seriously compromised when walls are present between devices. Also finally, the standard speed for wireless Ethernet connections is now approaching 10 Mbps and Bluetooth's top speed is very low.

1.4.6 Wireless Application Protocol (WAP) - a set of communication protocols to standardize the way that wireless devices, such as cellular telephones and radio transceivers, can be used for Internet access. The principle and the technical architecture are discussed in detail in the next section.

The Wireless Application Protocol

2.1 General Aspects of WAP

The Wireless Application Protocol is a protocol standard that designs the way for a mobile device to communicate to a server installed in a mobile network. For example it gives the framework used when a mobile phone talks to the server installed in the mobile phone network.

The Wireless Application Protocol, commonly know as WAP, is an important development in the wireless industry because of its attempt to develop an open standard for wireless protocols, independent of vendor and air link.

The WAP Forum was formed after US network operator Omnipoint issued a tender for the supply of mobile information services in early 1997. It received several responses from different suppliers using proprietary techniques for delivering the information such as Smart Messaging from Nokia and HDML from Phone.com (then called Unwired Planet). It was the WAP forum, which developed and deployed the Wireless Application Protocol. Industrial giants like Motorola, Nokia, Ericsson and phone.com are the founder members of the WAP forum. WAP is an attempt to define the standard for how content from the Internet is filtered for mobile communications. Content is now readily available on the Internet and WAP was designed as the overriding (rather than just one among many) way of making it easily available on mobile terminals.

2.1 Principle

The Wireless Application Protocol takes a client server approach. It incorporates a relatively simple microbrowser into the mobile phone, requiring only limited resources on the mobile phone. This makes WAP suitable for thin clients and early smart phones. WAP puts the intelligence in the WAP Gateways whilst adding just a microbrowser to the mobile phones themselves. Microbrowser-based services and applications reside temporarily on servers, not permanently in phones. The Wireless Application Protocol is aimed at turning a mass-market mobile phone into a "network-based smartphone".

The philosophy behind the Wireless Application Protocol's approach as per WAP Forum is to utilize as few resources as possible on the handheld device and compensate for the constraints of the device by enriching the functionality of the network.

The Wireless Application Protocol is envisaged as a comprehensive and scaleable protocol designed for use with any mobile phone, from those with a one line display to a smart phone, any existing or planned wireless service such as the Short Message Service, Circuit Switched Data, Unstructured Supplementary Services Data (USSD) and General Packet Radio Service (GPRS).

Another importance of WAP is the fact that it provides an evolutionary path for application developers and network operators to offer their services on different network types, bearers and terminal capabilities. The design of the WAP standard separates the application elements from the bearer being used. This helps in the migration of some applications from SMS or Circuit Switched Data to GPRS for example mobile networks, such as Code Division Multiple Access (CDMA), Global System for Mobiles (GSM), or Universal Mobile Telephone System (UMTS).

WAP has been designed to work with all cellular standards and is supported by major worldwide wireless leaders such as AT&T Wireless and NTT DoCoMo.

3.0 Technical Analysis of WAP

Phone.com created a version of the standard Hyper Text Markup Language (HTML) internet protocols designed specifically for effective and cost effective information transfer across mobile networks. Wireless terminals incorporated a Handheld Device Markup Language (HDML) microbrowser, and Phone.com's Handheld Device Transport Protocol (HDTP) then linked the terminal to the UP.Link Server Suite which connected to the Internet or intranet where the information being requested resides. The Internet site content was tagged with HDML.

Wireless Application Protocol embraced and extends the previously conceived and developed wireless data protocols.

The Wireless Application Protocol has WMLS, WTP and WSP to take care of the above. WAP uses a built in microbrowser to do various following services.

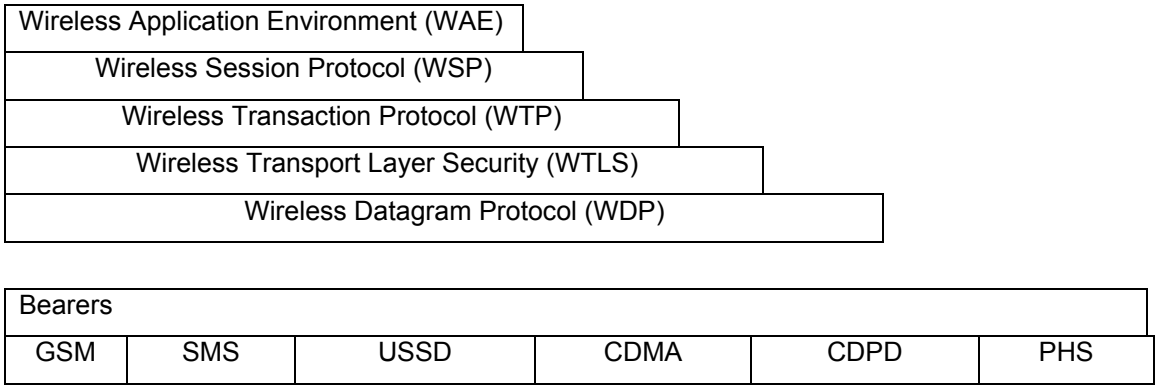
A Request is passed to a WAP Gateway that then retrieves the information from an Internet server either in standard HTML format or directly prepared for wireless terminals using WML. If

the content being retrieved is in HTML format, a filter in the WAP Gateway may try to translate it into WML. To format data such as calendar entries and electronic business cards, the WML scripting language is available. This can be incorporated directly into the client device.

The Wireless Application Protocol (WAP) is not just one protocol, it is the name of a whole suite of protocols. The suite is designed to make it possible to access Internet resources from hand held wireless devices (mobile phones or personal digital assistants PDA) in an efficient manner.

3.1 The WAP Protocol Stack

WAP has a layered architecture as shown in the diagram below:



(Figure -3 WAP Protocol Stack)

3.1.1 Wireless Application Environment (WAE)

WAE offers the software platform environment for the application software. WAE is built into the micro browser program. It works much like normal WWW browsers that interpret HTML and JavaScript. WAE consists of the Wireless Markup Language (WML), WMLScript, and Wireless Telephony Application (WTA).

Wireless Markup Language (WML)

WML is WAP's markup language derived from HTML especially for wireless network characteristics. It is much like HTML in the World Wide Web. Since it is a Document Type Definition (DTD) of XML, it is a tag-based, Standard Generalized Markup Language like HTML.

WMLScript

WMLScript is WML's integrated scripting language, much like JavaScript or ECMA Script, that can control many functions of the browser and the phone itself by scripts downloaded from the server. See Appendix A for a WMLS example.

Wireless Telephony Application (WTA)

WTA is the telephony interface of WAE that can be used to control telephony functions of the device from WML, WMLScript or the network and to invoke functions by requests from the network.

3.1.2 Wireless Session Protocol (WSP)

It is designed to implement a request-response protocol much like the Hypertext Transfer Protocol (HTTP). Using these protocols, the client makes a request and then the server answers with a reply that we know as a response in HTTP terminology.

WSP also includes some features not included in the HTTP protocol. These features are there because of the mobile nature of the WAP clients. For example, a mobile phone, which is a client, should not lose its connection to the server when it changes base stations.

The WSP protocol offers two different services, Connectionless and Connection Oriented service. It is purely to the wish of the client to use either of the services. This is how the two services work.

The connectionless service does not remember the context between two consecutive requests. Every request is handled on its own and there is no guarantee in what order two requests will be served. The client has to mark the requests with a unique transaction identifier (TID) and the server has to add this mark to the reply to allow the client to separate different replies from each other.

The connection-oriented service does remember context between consecutive requests and does not have to use a TID to mark requests or replies.

Both services are designed to provide the same functionality as HTTP and unreliable data transfer. HTTP uses ASCII strings to send protocol information between the client and the server. WSP does this in a better way of sending byte codes. This minimizes the data sent over the air. This way, the same information can be sent using much fewer bytes.

The push facility in the WSP protocol does not have a counterpart in the HTTP protocol. A push is what is performed when a WSP server sends information to a client without a preceding request from the client.

If it is a connection-oriented service, it provides various other services like session suspend and session resume functionality with session migration, reliable data push, protocol feature and negotiation. For example, when a client is connected using connection oriented WSP it may suspend the WSP session and resume it later. It may even be resumed over a different bearer. When this happens WSP resumes later on with a different barrier using SMS messages. This change in the underlying transport layer is called a session migration.

In WSP connection oriented mode, the client and server may negotiate some protocol features to be used in the session. For example, the client and server could agree on the maximum number of outstanding requests.

The Protocol Data Unit (PDU)

The PDU differs a bit depending on whether connection oriented mode or connectionless WSP is used. Connection oriented mode does not require the transaction identifier (TID) and it must be sent in each PDU when using connectionless mode.

TID	TYPE	Specific Contents

The type field in the PDU explains how to understand or interpret the specific contents. For example it identifies types like Connect, Get, Push and Suspend. The WSP specification defines the allowed types and their assigned byte code.

WSP implements the session services of WAP. Sessions can be connection-oriented and connectionless and they may be suspended and resumed at will.

3.1.3 Wireless Transaction Protocol (WTP)

WTP is Wireless Application Protocol's transaction protocol. It works between the session protocol WSP and security protocol WTLS. It is responsible for delivering higher layer messages in a way that satisfies the demands of these upper layers. WTP chops data packets into lower level datagrams and concatenates received datagrams into useful data. Since datagrams are unreliable, WTP uses techniques like retransmission after timeouts and acknowledgement of messages for providing reliable service. WTP uses a transaction identifier (TID) in every message. The TID is used to associate a packet with a particular transaction.

When the receiver receives a TID that is less than or equal to the TID that is in the buffer, then the message the receiver is getting may be a duplicate or a retransmitted message, which was lost earlier. Now the receiver will be able to ask the sender if the TID is valid or not. WTP uses primitive error handling. In the case of error, say a connection break etc the transaction is aborted.

Depending on the demands of the application, WTP defines three classes of transaction, Class 0,1 and 2. In Class 0 the sender sends a transaction to the receiver, but there is no assurance that the transaction will reach its destination. If the transaction reaches the destination then the receiver will not send acknowledgment to the sender. In Class 1 the transaction provides a reliable datagram service. If the sender does not get acknowledgment the sender will retransmit the message after some time. In Class 2 service the sender and receiver transfer acknowledgements promptly. Both sender and receiver are capable of re-transmitting messages if necessary.

The WTP protocol has various protocol features. In some of the protocol features, both the client and the server send and receive packets. During this description of the protocol features, the sender is the one who starts the transaction by sending an Invoke message and the receiver is the recipient of that message. Features include:

Message transfer : Depending on the class of service, various messages like Invoke message (first message to invoke the transaction), Verification (if the message sent is invalid verification process starts) , Hold on acknowledgement (If the receiver needs more time to process before sending acknowledgement this message is sent to avoid retransmission from the sender) , Result

message (This is used when data from invoke message has been processed and then result message is sent), Last acknowledgement. (Sent when the last message of the transaction has been received).

Retransmission : Retransmission of packets happens until acknowledgement arrives. This happens once the retransmission timer expires, then the sender retransmits the packet until sender gets acknowledgement from the receiver.

Linking and Separation of Messages : To provide over the air efficiency there can be multiple WTP data units can be present in one datagram service data unit of the bearer network. By doing this only fewer transmissions will be required over the air. Linking of messages can be done for messages with the same source and destination address and the same source and destination port, essentially the same address information. A last acknowledgement of one transaction can also be concatenated with the new invoke message of the next transaction.

Error Handling: During a transaction if a fatal error occurs then the transaction is aborted and the WTP user is informed with proper abort reason.

Segmentation and Re-assembly (SAR): When the message length is going to exceed the maximum transfer unit (MTU) of the current bearer, the message will be split by the Wireless Transfer Protocol into several packets. This is an optional feature. If Segmentation and Re-assembly is not implemented in WTP, then the higher layer in the stack will take care of this operation.

Abort Transaction: This is done when an abort request is made by the application. There are two kinds of aborts. One is the user requested abort, and the other one is by the invalid protocol feature. If a particular of the feature is tried and not implemented then the protocol aborts that request.

Other features of WTP include getting information last acknowledgement, user acknowledgement, initiating multiple transactions, Transport Identifier verification and information on the Transport information items, etc.

WTP Protocol Data Unit

The header of this may have variable length. It consists of Transport Information Items called TPI. All the transport information items have Transaction Protocol Item Identification, Transaction Protocol Item data. Wireless Transport Protocol has defined only a few TPI. The use of TPIs allows for future extensions of the protocol.

3.1.4 Wireless Transport Layer Security protocol (WTLS)

This is an optional layer providing secure connections to the upper layers. WTLS does all cryptography-oriented features of WAP. WTLS handles crypting, decrypting, user authentications by digital signing, and data integrity checking. WTLS is based on the fixed network Transport Layer Security protocol (TLS), formerly known as Secure Sockets Layer (SSL).

The security layer can be subdivided into Handshake and Record protocol layers. Handshake works somewhat similarly to the Transmission Control Protocol's (TCP) three way handshake, with the exception that here it is just request and response kind of operation only.

HandShake

Client (C1) ----------> Server (S1)
(C1 Hello, Request Authentication of Server)

Client (C1) <---------- Server (S1)
(S1 Hello and initiate certificate of exchange sends S1's certificate)

Client (C1) ---------->Server (S1)
(C1 Sends its Certificate of authentication)

Client (C1) <---------- Server (S1)
(S1 Sends Hello Done, Data transfer starts)

Client (C1) ----------> Server (S1)
(C1 Finished)

Client (C1) <---------- Server (S1)

(S1 Finished)

Client (C1) <----------> Server (S1)

Data Transfer

The handshake allows client and server to agree on the cryptographic algorithm, exchange random values and exchange the necessary cryptographic parameters. It can basically verify the security parameters and the handshake occurs without being tampered with in between.

The client sends a hello message containing the protocol version, set of zeros and other information explaining how the client wants to encrypt the data. The server then responds with a hello message acknowledging the client. The server then initiates the certificate of exchange process since the client asked for the server to authenticate itself through the client hello message. The server may ask the client to send its authentication certificate to the server. Then the server will send the hello done message along with the data if it needs it.

After the client receives the hello done with the data from the server then the client sends a finished message and the server responds with a finished message. This way the handshake is completed and the client and server may send and exchange encrypted data to each other.

Record

This layer takes care of the encryption and decryption operation of the message. When a message is to be transferred the record protocol layer compresses the data, encrypts it and sends it to the other layers which does the transmission. Same way when the message is received it decrypts and decompresses the message before sending to the upper layers.

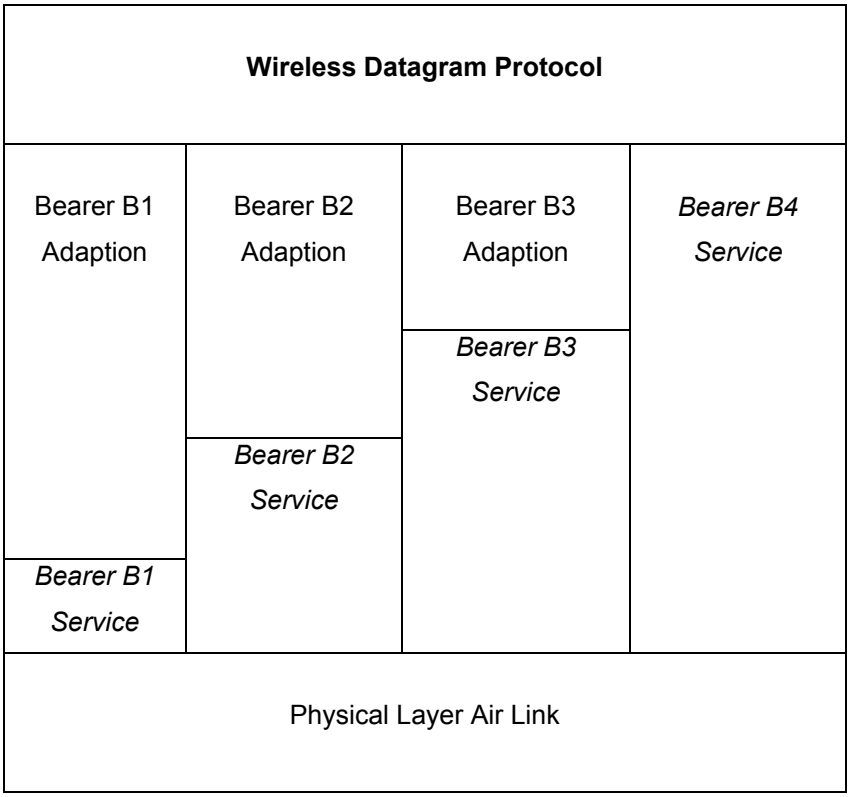
3.1.5 Wireless Datagram Protocol (WDP)

WDP works as the transport layer of WAP. WDP processes datagrams from upper layers to formats required by different physical datapaths, bearers that may be for example GSM SMS or CDMA Packet Data. WDP is adapted to the bearers available in the device so upper layers don't need to care about the physical level.

WDP actually specifies how various existing bearer services should be used to provide a consistent service to the upper layers. This is done by adapting the protocol to the underlying bearer.

Since different bearers have different features therefore some sections in the specification are bigger or smaller than others. For instance, the section on IP bearers is very short. As Wireless Datagram Protocol one must use the UDP protocol from the IP-suite. Consider the following diagram, bearer B4 is the example of showing how as WDP one must use the UDP protocol from the IP-suite.

Adaption of WDP



(Figure -4 Adaption of WDP)

Say if one uses GSM SMS (Short Message Service) as the bearer, then WDP has to adapt to support port numbers. The adaptation process is described in the specification.

3.1.6 Bearer Service

Bearer Service is a telecommunication service that allows transmission of user information signals between user network interfaces.

The WAP protocols are designed to operate over a variety of different bearer services. The bearers offer differing levels of quality of service with respect to throughput, error rate, and delays. The WAP protocols are designed to compensate for, or at least tolerate, these varying levels of service.
Short Message Service (SMS): It has the ability to send and receive text messages to and from mobile telephones. The text can be comprised of words or numbers or an alphanumeric combination. SMS was created as part of the GSM Phase 1 standard. Each short message is up to 160 characters in length. WAP services can be developed based on SMS.

Circuit Switch Data (CSD): Most of the trial WAP based services use CSD as the underlying bearer. However, CSD lacks immediacy- a dial up connection taking about 10 seconds is required to connect the WAP client to the WAP Gateway.

Unstructured Supplementary Services Data (USSD): Unstructured Supplementary Services Data (USSD) is a means of transmitting information or instructions over a GSM network. USSD has some similarities with SMS since both use the (Global System for Mobiles) GSM network's signaling path. Unlike SMS, USSD is not a store and forward service and is session-oriented such that when a user accesses a USSD service, a session is established and the radio connection stays open until the user, application, or time out releases it.

3.2 How does WAP work?

Internet servers have resources stored from all around the world. A web client can download the information from the web servers. The interaction happens using HTTP protocol (Hypertext Transfer Protocol). Wireless Application Protocol does not include HTTP. Instead a Wireless Application Protocol client uses the Wireless Session Protocol (WSP) to retrieve information from the server.

Since an Internet web server and WAP use different protocol approaches, this creates a contradiction between the way Internet servers work and the WAP approach to retrieving information.

So directly a WAP client cannot download information from a web server. Now to solve this the WAP client should use a translator between HTTP and WSP. This is called a proxy server. The proxy server in WAP is called the WAP Gateway. The existence of a WAP gateway is totally transparent to the WAP client or the web server. WAP process of downloading information from World Wide Web server is shown in the following figure. (Figure -5)

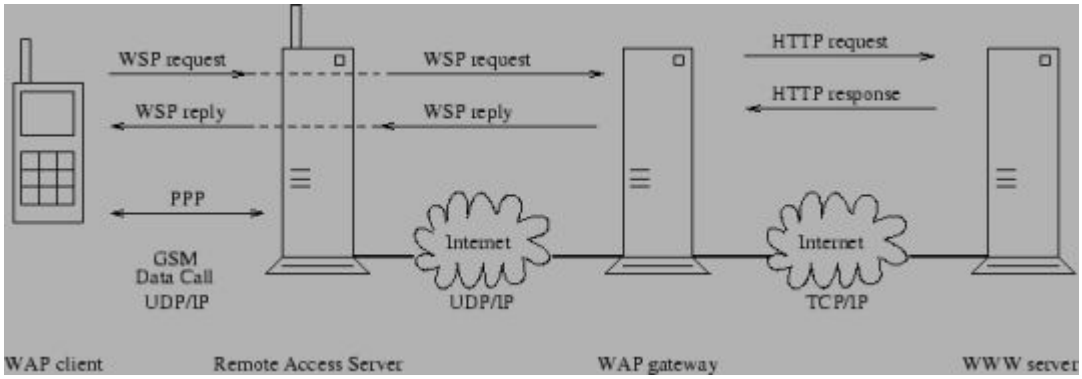


Figure - 5 WAP Process for downloading information from World Wide Web server

Client

The client makes (A mobile phone) establishes the connection to the remote access server. Once the connection is established then the remote access server will be the forwarding agent to and from the client. The client runs a WAP application (typical client show in Figure - 6) like a browser, and makes the WSP request to the gateway.

Figure - 6 A typical WAP enabled Client

Server

A server will run a web browser and will not understand WML and will understand only HTTP. Since the gateway takes care of transferring the request to HTTP from WSP, the server will not even know that there is such a translation happening in between. It basically responds to the HTTP request and processes it.

Gateway

The Gateway is generally located in the same local network of the remote access server. It also takes care of making the message suitable for the client. Basically a WAP client only understands the binary encoding of WML even though a page is written in WML. The Gateway takes care of this transfer and makes it suitable for the client.

Say a client needs a document (Uniform Resource Identifier URI) from the Web. It sends a WSP request to the Gateway. The Gateway parses the client's request then the Gateway receives the request and takes the responsibility of translation of the request between the WSP and HTTP protocols. Then it makes a HTTP request for the document specified in the URI. Then the server will respond to the request of the Gateway. The Gateway parses the response from the HTTP server. If the content is WML then it takes care of compiling it and creating a binary encoding of WML. The Gateway then sends a WSP response to the client. The Client is presented with the document it requested.

3.3 Comparison of World Wide Web and Wireless Application Protocol

WAP uses the Wireless Markup Language (WML) for application contents in the same way what Hyper Text Mark-up Language (HTML) is used in WWW.

In the Internet model there is a client and a server. The Internet is used for transmission. The WWW client sends a request to the WWW server and the server sends a response for that request. The Internet is used as the transmission medium. In the WAP model, the same client server model is used but there is a Proxy/Gateway between the server and the client to allow protocol conversion and encoding plus encoding of WML.

WMLScript makes it possible to add procedural logic and computational functions to WAP based services like Javascript in HTML.

Wireless devices have slow connection speeds and small screen sizes. In small terminals, power consumption is very important and these terminals can't provide microprocessor resources like in a PC. Wireless networks have high latency compared to wired networks. WAP is optimized to fulfill these requirements.
WAP uses the same addressing model as the one used in the Internet (URL). WAP also can use URIs(Uniform Resource identifiers) for addressing resources that are not necessarily accessed using well-known protocols.

WAP allows Wireless Telephony Applications that are not available in the WWW.

WWW and WAP Architecture

<table>
<tr><th>WWW</th><th>WAP</th></tr>
<tr><td>HTML, Javascript, VBScript</td><td>Wireless Application Environment(WAE) WML and WMLScript</td></tr>
<tr><td>Gif and Jpeg graphics</td><td>Wbmp</td></tr>
<tr><td rowspan="2">HTTP</td><td>Wireless Session Protocol(WSP)</td></tr>
<tr><td>Wireless Transaction Protocol(WTP)</td></tr>
<tr><td>TLS-SSL</td><td>Wireless Transport Layer Security(WTLS)</td></tr>
<tr><td rowspan="2">TCP/IP
UDP/IP</td><td>Wireless Datagram Protocol(WDP)</td></tr>
<tr><td>Bearers(Not inside of the WAP Stack)</td></tr>
</table>

(Table - 1 Comparison between WWW and WAP)

3.4 Advantages of WAP

Wireless Application Protocol is open standard. It is totally vendor independent and Network Standard Independent. Wireless Application Protocol's transport mechanism is optimized for wireless data bearers.

WAP applications downloaded from the server enable faster service creation and introduction than embedded software.

Some of the other WAP features are similar to HTML. Using WML you can have your own WAP page (home page) which can be viewed on your future mobile phone.

We can have Route-finder on the WAP page, which can be useful for finding routes. This may come in very handy for heavy business travelers.

You can also have newsletter page to announce your news there everyday.

3.5 Disadvantages of the WAP architecture

WAP's disadvantages stem mainly from client limitations. It has a thin client architecture. That is one of the reasons why normal web technology cannot be used in the WAP client. Now WAP clients are handheld wireless devices like mobile phones or personal digital assistants (PDAs). These devices are in no way powerful compared to a stationary computer. So technically speaking all the disadvantages of these clients become constraints for WAP to deal with. Following are the constraints of handheld devices.

Handheld devices

- have less powerful CPU's.
- have less memory.
- have lower transfer rates.
- connection is less stable.
- availability is less predictable.
- connection media generates higher latency.
- Power supply and consumption is an important issue.
- Input devices are far from as powerful as those in stationary computers.

As the study that was done to measure the usability of WAP in FALL of 2000 clearly shows WAP is not matured yet, with a ways to go. During the study 70% of the users rejected the idea of WAP

enabled phones. Some of the disadvantages of WAP clearly made the users to decide not to like this.

WAP application interfaces (like menu labels and navigation items) need to be more user friendly.

Because of the misguided use of design principles from traditional Web design, the usability of the current WAP services is reduced considerably. WAP is facing the same problem as WEB desgins faced in 1994 during the evolution of the Internet. For example, some of the WAP designs that use more screens to display information could have been displayed in a lesser number of screens. This kind of design may work on the Web if users have a big-screen PC, but on a small-screen device, designers must cut short each service down to its essence and show much less information.

The time taken to perform a query on the Internet through the WAP is also not acceptable by the users. Here is the analysis on some of the time taken to perform certain operations using WAP phones during the study.

Action	Time in Minutes
Read world headlines	1.1
Check local weather forecast	1.9
Read TV program listing	1.6

(Table - 2 Performance of WAP)

WAP Gap

There are more than 400 million existing digital wireless phones in use today. Most of these are not Wireless Application Protocol (WAP)-enabled, with only a few being WAP enabled devices. This situation is called the WAP Gap. The gap is created by all the development going on of WAP applications. The WAP applications cannot be deployed because of the lack of compatible devices.

There are some companies that are coming out with solutions to bridge the WAP gap. Communication companies like BulletIN.net (a mobile messaging company), and DataPlex (an Australian based data communications company) are marketing applications that serve both Short Message Service (SMS) and WAP users. They market a WAP emulator, which translates

between the WAP-based (WML) and text messaging. The companies say this provides wireless carriers with a migration path to encourage users to sign up now for SMS solutions, then transition to WAP when handsets become more widely available

The WAP forum says that the latest version of WAP (from version 1.3 onwards, current version is 2.0) will eliminate the WAP gap via a client-side WAP proxy server that communicates authentication and authorization details to the wireless network server.

3.6 Security Issues

WTLS Issue

The implementation of WTLS is similar to the Internet implementation of TLS (Transport Layer Security). TLS is used to encrypt the transmission between a web browser and the web server. WTLS is used to encrypt the transmission between the wireless device and the WAP gateway. WTLS was designed to cope with long round-trip times, low bandwidth connections and processing power, small memory capacities and cryptography exportation regulations. Currently these differences in behavior pose serious security problems. WTLS and TLS are not compatible. Take for example, when a wireless user is purchasing an item through a web site using TLS. The user fills out the form with their credit card information and submits it. The wireless device creates a WTLS connection to the WAP gateway. The Gateway recognizes that a security channel is required and attempts to use TLS to connect to the web site. Here is where the problem arises. The WAP Gateway cannot simply pass the WTLS connection along to the web server because the server only understands TLS. The WAP gateway has only one possibility of making this work. It must decrypt WTLS and then re-encrypt it under TLS. This means the WAP gateway has the un-encrypted data that the wireless user is trying to keep secret.

The above scenario will definitely cause alarm for any user's secret information like their credit card information. Even though we can say the conversion occurs in the memory of a trusted gateway computer. The users can become aware of the situation and take advantage of the trust and exploit systems. In this case, the WAP gateway is giving opportunity for the hacker to access all of this confidential information by dumping the contents of memory into a log and then searching for known patterns that contain credit card numbers.

There is no specific solution to this problem currently in WAP. The suggested solution is to use trusted WAP gateways or combine the WAP gateway into the web server, which is called the WAP server. In this way the decryption of data occurs on the computer that the user wants it to. The problem with this solution is that a typical cell phone can only be configured with one or two gateways. If the user wants to use another provider's services, they have to manually change this data and that will be very cumbersome on a cell phone.

Unauthenticated Alert Messages Issue

In the WAP Specifications, there are alert messages that are used to notify the client of a problem in sending the data grams. Some of these alert messages are sent in plain text and are not properly authenticated. This allows a hacker to replace an encrypted datagram with an unencrypted response. This will cause a truncation attack that allows arbitrary packets to be removed from the data stream.

35-bit DES Encryption

In early versions, rather than using 40-bit DES (Data Encryption Standard) encryption, the WAP standard effectively uses 35-bit encryption. In every byte that WAP sends encrypted, there is a parity bit added. This means that there are only 35 effective key bits in five encrypted bytes. This causes a key space reduction by a factor of 32 and allows a hacker easier access to break the encryption using brute force.

4.0 Future of WAP

By 2004, there could be more than 700m mobile commerce users. M-commerce is emerging more rapidly in Europe and in Asia, where mobile services are relatively advanced, than in the US where mobile telephony has only just begun to take off. With the advent of next generation services, however, it is likely that the US will have closed the gap within the next few years.

WAP is one of a family of technologies that have the potential of bringing about the convergence of mobile communications and the Internet. Technologies like bluetooth will connect the mobile device to the personal computers. GPRS has the potential to deliver Internet information to mobile phones many times faster than conventional GSM technology. By allowing the mobile device to be in an always-connected state, GPRS (or other services like CDPD) will bring Internet closer to mobility. All this should make adoption of WAP much more attractive and desirable. This

is important because all these developments are helping to create new user requirements and demand patterns, which are all beneficial for WAP. The appetite for mobile data services like WAP is a fact.

According to the WAP forum the current interest areas include end-to-end security, smartcard interfaces, connection-oriented transport protocols, persistent storage, billing interfaces, and push technology.

WAP is an open protocol that allows the transport of many forms of multimedia content. However, some multimedia services, especially those based on streaming media, will require further enhancements to WAP.

WAP has been designed to be as independent as possible from the underlying network technology which basically complies with third generation wireless standards. There is a question that is being asked whether WAP is necessary with higher bandwidth 3G networks. WAP was designed for -- intermittent coverage, small screens, low power consumption, wide scalability over bearers and devices, and one-handed operation -- which are still valid in 3G networks. As we know the bandwidth required by application users will steadily increase. So there is still a need to optimize the device and network resources for wireless environments. If WAP is very successful in mass-markets on 2.5G networks, 3G networks may be needed purely for capacity relief.

Backed by 75 percent of the companies behind the world's mobile telephone market and the huge development potential of the WAP, the future for WAP looks bright

However according to a recent poll of wireless developers by Evans Data Corp of Santa Cruz, CA is not in favor of WAP. The results shows that 30 percent of developers plan to implement their wireless applications in Sun's Java2Micro Edition. 25 percent will use the Palm operating system, 22 percent will use Windows CE and only small number would consider WAP for wireless application development.

5.0 Conclusions

WAP provides a markup language and transport protocol standards that create the opportunity for the wireless environment and give businesses from all levels of the industry access to a new market still in its infancy. WAP is one of the standards for wireless devices to connect to the

Internet in North America. These days, most cell phones that can be purchased on the market going forward have WAP support built in. Major companies are beginning to develop WAP applications that allow people to control their finances on their WAP devices. There is a lot of money being invested in this technology.

This means that it is a standard that will be around for quite a while because users and companies will be reluctant to abandon their applications that they have already invested a great amount of time and money into should the holes in WAP not be fixed.

WAP has the potential to lead or restrict the wireless revolution. This is why it is important to discuss the security issues that are present. Nobody will want to use a system where his or her personal information can be compromised. The WAP Forum must address these issues raised in up coming WAP versions to make sure that information remains safe when someone uses their wireless device for confidential data transmission and thinks they are getting a secure connection from one end to the other. If their vision is what they are planning to implement WAP will definitely bridge the gap between the mobile world and the Internet.

6.0 References

http://www.mwif.org/
Web site owned by The Mobile Wireless Internet Forum (MWIF). Last visited on 12/03/2001

Computer World -- Magazine Reference
http://www.wirelessethernet.org: Wireless Eithernet Compatibility Alliance. Won the PC Magazine's Technical Excellence Award 1999. Last visited on 12/03/2001

WAP Usability Report: Field Study Fall 2000
(A Nielsen Norman Group report, December 2000)

http://www.unisysworld.com : Unisys World Magazine. Last visited 12/03/2001. Site visited http://www.unisysworld.com /monthly/2001/03/wap.shtml

http://www.nngroup.com
Owned by Nielsen Norman Group. Article on WAP usability. Last visited on 12/03/2001
Site visited http://www.nngroup.com/reports/wap/

http://www.palowireless.com - Owned by Palowireless, Wireless Resource Center. Last visited 12/03/2001. Site visited http://www.palowireless.com /wireless/articles.asp

http://www.cwc.uwaterloo.ca : Owned by Center for Wireless Communications. Last visited on 12/03/2001.

http://www.columbia.edu : Owned by Columbia University. Last visited on 12/03/2001. Site visited - http://www.columbia.edu/~ir94/wireless.html (Analysis of Existing Wireless Communication Protocols)

http://ccnga.uwaterloo.ca : Owned by Shoshin Research Group. Paper on GSM services. Last visited on 12/03/2001. Site visited : http://ccnga.uwaterloo.ca/~jscouria/GSM/gsmreport.html#2

http://www.cc.nctu.edu.tw/~ctr/lee_mti/research_topic/wireless_communication.htm. Article on Wireless Communication. Site last visited 12/03/2001.

http://www.cewindows.net/ - Owned by Chris De Herrera's on Windows CE . Site last visited on 12/03/2001.

http://www.mobileinfo.com: Owned by Mobile info. Article on Future of WAP. Last visited on 12/03/2001. Site visited http://www.mobileinfo.com/WAP/future_outlook.htm

http://winwww.rutgers.edu : Owned by WINLAB (Wireless Information Network Laboratory), a National Science Foundation Industry/University Cooperative, was founded at New Jersey's Rutgers University in 1989. Its research mission is to advance the development of wireless networking technology by combining the powerful resources of government, industry and academia.
Last visited on 12/03/2001. Site visited http://winwww.rutgers.edu/pub/Links.html#Wireless

http://www.raleigh.ibm.com/cgi-bin/bookmgr/BOOKS/EZ315000/CCONTENTS: An article on introduction to Wireless Networking. Site last visited 04/12/2001.

http://www.sandag.cog.ca.us/ftp/html/publications/wireless.html. Article on Wireless Resources. Site last visited on 12/03/2001.

http://www.gsmdata.com: Owned by Mobile Data initiation Next generation. Paper on General Packet Radio Service (GPRS). Last visited on 12/03/2001. Site visited http://www.gsmdata.com/es53060/paprysavy.htm

http://murray.newcastle.edu.au: Owned by The University of Newcastle Department of Electrical and Computer Engineering. Articles on Digital Data Communications. Last visited on 12/03/2001. http://murray.newcastle.edu.au/users/staff/eemf/ELEC351/SProjects/ChanChng/wireless.html#What

Other Sites For References

http://www.diffuse.org/mobile.html#WAP
http://www.cs.berkeley.edu/~gribble/summaries/wireless/
http://www.cis.ohio-state.edu/~jain/netsem/netsem6.htm
http://murray.newcastle.edu.au/users/staff/eemf/ELEC351/SProjects/ChanChng/wireless.html#What
http://murray.newcastle.edu.au/users/staff/eemf/ELEC351/SProjects/ChanChng/wireless.html
http://www.boulder.nist.gov/div853/Annual%20Report%202000%20HTML/Program%202.html
http://citeseer.nj.nec.com/96066.html
http://www.cis.ohio-state.edu/~jain/papers.html
http://www.epanorama.net/tele_datacom.html
http://www.wapforum.org/faqs/#faq11
http://www.tml.hut.fi/Opinnot/Tik-111.550/1999/Esitelmat/Wap/wap/WAP.html
http://triton.cc.gatech.edu/ubicomp/502
http://www.allnetdevices.com/marketdata/000217two_way.htm
http://www.wapforum.org/new/M-CommerceWorld.ppt
http://www.useit.com/alertbox/20001210.html
http://www.sans.org/infosecFAQ/wireless/WAP4.htm
http://www.cas.mcmaster.ca/~wmfarmer/SE-4C03-01/papers/Zrobok-WAP.html
http://www.sans.org/infosecFAQ/wireless/WAP.htm
http://www.waptechnology.narod.ru/competition.htm
www.networking.com
http://www.calsoft.co.in/techcenter/Whitepaper.html
http://www.xircom.com/cda/page/1,1298,1-840-1_1-1022-1033,00.html
http://www.gsmdata.com/es53060/paprysavy.htm