Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, No. 1, April : 2023

BUILDING NEXT-GENERATION MOBILE APPLICATIONS WITH WIRELESS APPLICATION PROTOCOL

B. Durga Prasad, PG Scholar, Department of ECE, JNTUA College of Engineering Pulivendula, A.P, India. E-mail: durgaprasad2451999@gmail.com
Shaik Taj Mahaboob, Assistant Professor, Department of ECE, JNTUA College of Engineering Pulivendula, A.P, India. E-mail: shaiktajmahaboob@gmail.com
K. Ravindra Reddy, Assistant Professor (Adhoc), Department of ECE, JNTUA College of Engineering Pulivendula, A.P, India. E-mail: ravindra.kalvapalli@gmail.com

Abstract: Wireless Application Protocol (WAP) is a standard protocol that allows mobile devices to connect to and browse the internet. such as smartphones and tablets. It was developed to provide a seamless browsing experience on devices with limited processing power and memory, such as those with small screens and slow internet connections. Wireless Markup Language (WML) is a markup language that is used by WAP to show web pages on mobile devices. Which is optimized for low bandwidth connections. It also uses Wireless Transport Layer Security (WTLS) for encryption and security purposes.
WAP has been widely adopted by mobile network operators and device manufacturers, allowing users to access a range of internet services such as email, social media, and online banking on their mobile devices. Networking Protocols shows the easiest ways to get data from one place to another, and it also explains how routers pass information between each other so that the goal can be reached. And with secure authentication was add in WAP with static protocol. The static protocol uses an updated version of Distance Vector, which was made by the company Cisco.
In this paper, specific and detailed information about WAP protocols and secure authentication is discussed. We get to learn about how different protocols' WAP features work. By using Packet Tracer to send PDUs (Protocol data unit), we'll get simulation results for the required WAP that uses static protocols.

Keywords: Wireless Application Protocol (WAP), Wireless Transport Layer Security (WTLS), Wireless Network, Wireless communication**.**

1. INTRODUCTION

Wireless Application Protocol (WAP) is a set of rules that lets mobile devices like smartphones and tablets connect to the internet. to access and browse the internet. [1] It was developed in the late 1990s as a solution to the challenge of accessing internet content on devices with limited processing power, memory, and screen size. Before WAP, accessing the internet on mobile devices was difficult because the internet was designed for desktop computers with large screens, high-speed connections, and powerful processors. [2] The content was also presented in HTML, which was not suitable for mobile devices with limited resources. WAP solved this problem by introducing a new markup language It was made for mobile devices and was called Wireless Markup Language (WML).[3] WML made it possible to display web pages on mobile devices with limited processing power and memory.

In addition to WML, WAP also introduced a security There is a protocol called Wireless Transport Layer Security (WTLS) that lets wireless communications be encrypted and verified.[4] This ensures that users' data is protected from interception and unauthorized access. WAP has been widely adopted by mobile network operators and device manufacturers, enabling mobile users to access a range of internet services such as email, social media, and online banking on their devices.[5] However, with the rise of mobile apps and advancements in mobile technology. WAP is still an important part of the history of mobile internet, and it paved the way for modern mobile browsing technologies. [6].

1.1 Why WAP?

Wireless Application Protocol (WAP) was developed to address the challenges of accessing internet content on mobile devices with limited processing power, memory, and screen size. The main reasons for the development of WAP are:

- Limited processing power: Mobile devices have limited processing power, making it difficult to process and display web pages designed for desktop computers.
- Limited memory: Mobile devices have limited memory, making it difficult to store large amounts of data, such as web pages.
- Limited screen size: The screens on mobile devices are smaller than those on desktop computers, which makes it difficult to display web pages designed for desktop screens.
- Limited internet connectivity: Most mobile devices connect to the internet more slowly than desktop computers.it difficult to download and display web pages quickly.

WAP addressed these challenges by introducing a new markup language Most mobile devices take longer to connect to the internet than desktop computers do. WML makes it possible to display web pages on mobile devices with limited processing power and memory. In addition, WAP introduced Wireless Transport Layer Security (WTLS), which offers encryption and authentication for wireless communications, ensuring the security of users' data. Overall, WAP was created to help mobile users access and surf the internet more easily despite the restrictions placed on them by their devices.

1.2 What is WAP?

Wireless communication plays a critical role in the functioning of Wireless Transport Layer Security (WTLS), which encrypts data and verifies users for such as mobile phones, to access and interact with internet services. In order to achieve this, WAP relies on wireless communication technologies, such as GSM, CDMA, and 3G. Wireless communication enables mobile devices to send and receive data over the internet through the use of radio waves. This data can include text, images, and other types of multimedia content. The quality and reliability of wireless communication are critical factors in the success of WAP-enabled services, as users need to be able to access and interact with internet services quickly and reliably from their mobile devices. WAP uses a lightweight protocol to ensure that data is transmitted efficiently over wireless networks. It also uses encryption and authentication technologies to ensure that data is transmitted securely, protecting users from unauthorized access and malicious attacks.

In recent years, advancements in wireless communication technologies, such as 4G and 5G, have enabled faster and more reliable connections, which in turn have enabled more advanced mobile applications and services. devices to access internet services and communicate with one another. The Wireless Application Protocol, or WAP, made its debut in 1999. It offers mobile web application development, Internet connections across wireless platforms including mobile phones and networking It was made for small devices, like micro-browsers. WAP, TDMA, CDMA, and GSM are all used by most wireless networks. There may also be a wireless application protocol on all OS systems. It makes use of markup languages like WML, or Wireless Markup Language, often known as XML 1.0 application, and permits internet access on mobile devices. WAP enables the compatibility of wireless standards and makes it easier for To connect to the internet, you can use interactive wireless devices like cell phones.

1.3 WAP Model

The user opens the web browser on the network device, logs in, and then goes to the necessary URLs. The WAP protocol is used to send the URL request from the mobile device to a WAP gateway on the other side of the network. The WAP gateway changes this request into a standard

HTTP URL request before sending it across the internet. The requested Web server gets the request and takes care of it. The answer is then sent back to the mobile device in the form of a WML file through the WAP gateway. where the web browser on the device will display it.

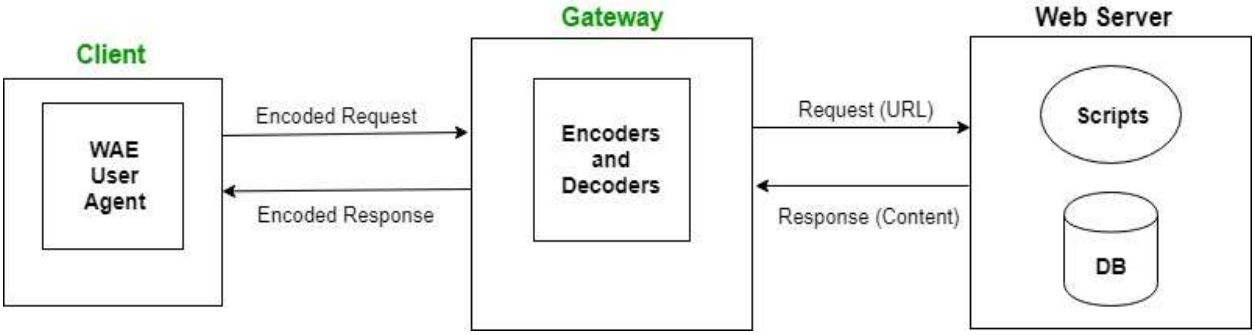

Figure 1: WAP Model

1.4 Wireless Application Protocol (WAP) client:

In Wireless Application Protocol (WAP), a client is a software application or device that requests and receives data from a server. The client is typically a mobile device, such as a smartphone, that uses the WAP protocol to connect to internet services.as shown in Figure 1. WAP clients use a web browser or a dedicated application to send requests to WAP-enabled servers, and to receive responses that contain the requested data. These requests can include browsing web pages, accessing email, and performing other internet-based activities.

WAP clients are designed to work efficiently on devices with limited processing power and memory, such as mobile phones. As such, they are typically lightweight and optimized for display on small screens. In order to ensure secure communications between clients and servers, WAP includes built-in support for encryption and authentication technologies. This helps to protect user data from unauthorized access and malicious attacks.

1.5 WAP Gateway

A software programme called the Wireless Application Protocol (WAP) gateway decodes and encodes the questions and answers sent between smartphone micro browsers and the internet. A WAP gateway is used to send access requests to websites because it offers security. It facilitates communication between WAP-enabled wireless devices and online programmes and websites. The Gateway handles this transfer and makes sure it works well for the client. The Gateway then sends the client a response that has been encoded. The Client is given the document it asked for. in particular format called WML (Wireless Markup Language).as shown in Figure 1.

1.6 Wireless Application Protocol (WAP) web server

In Wireless Application Protocol (WAP), a web server is a software application that responds to requests from WAP-enabled clients, such as mobile phones. The web server is responsible for processing these requests and sending responses that contain the requested data back to the client.as shown in Figure 1.

WAP web servers are similar to traditional web servers, but they are optimized to work with the WAP protocol, which is designed to work efficiently on devices with limited processing power and memory. This often involves using lightweight markup languages such as Wireless Markup Language (WML) to create pages that are optimized for display on small screens.

Web servers that support WAP typically offer a range of services, including web browsing, email, and other internet-based activities. They also incorporate security features, such as encryption and authentication technologies, to make sure that data sent between the client and the server is sent safely.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, No. 1, April : 2023

1.7 WAP Protocol stack

The user launches a mobile device's mini-browser. He chooses the website he wants to visit. The mobile device communicates with a WAP gateway across the network by sending the URL-encoded request using the WAP protocol.

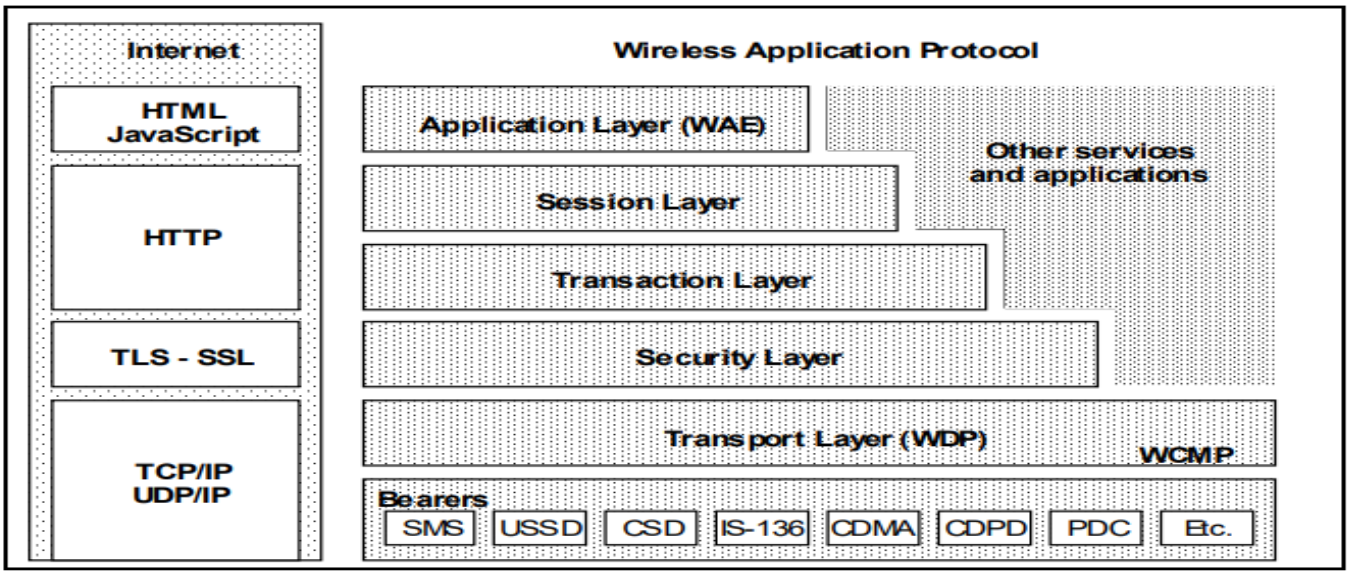

Figure 2: WAP Protocol stack

1.7.1 Application Layer (WAE)

The Wireless Application Environment has both standards for mobile devices and programming languages for making content, such as WML. It has the tools that content on the wireless Internet creators utilise, and it works quite similarly to JavaScript. It contains scripting languages that are used with WML, such WML and WML Script. as shown in Figure 2.

1.7.2. Session Layer (WSP)

It specifies whether or not the device's session with the network will be based on connections or not, and it will offer fast disconnection and reconnection. Data is exchanged back and forth between the network and the device during a session that is connection-oriented. From layer WTP to layer WSP, the packet is then sent (Wireless Transaction Protocol). When data is broadcast or streamed from the network to the device, a connectionless session is typically employed. After then, the Wireless Datagram Protocol (WDP) layer receives the packet from the Wireless Service Protocol (WSP).as shown in Figure 2.

1.7.3. Transaction Layer (WTP)

The Wireless Transaction Protocol makes it possible to do transactions. It is part of the TCP/IP system and uses the User Datagram Protocol (UDP), as its foundation.as shown in Figure 2.

1.7.4. Security layer (WTLS)

The Wireless Transport Layer Security helps to keep your data safe by making sure that your data is secure, private, and authenticated. It can operate in a manner akin to Transport Layer Security. Transport Layer Security is used in its security components as well.as shown in Figure 2.

1.7.5. Transfer Layer (WDP)

The carrier layer of the network is used in conjunction with the Wireless Datagram Protocol. gives higher layers of the WAP protocol stack a continuous data format. as shown in Figure 2.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, No. 1, April : 2023

2. LITERATURE REVIEW OF WIRELESS APPLICATION PROTOCOL AND WIRELESS COMMUNICATION

Table 1. Comparison study of wireless application protocols

S.NO	AUTHOR NAME	YEAR OF PUBLICATION	TITLE	TECHNIQUE	METHOD
1.	**WeilianSu et al [1]**	2005	"Time-diffusion ideas and protocols for sensor networks"	The Time Diffusion Synchronization Protocol (TDP) Was It Enables Synchronization Procedure.	TDP (TIME DIFFUSION SYNCHRONIZATION PROTOCOL) it enables a sensor network to get minimal time deviation and reaches equilibrium time.
2.	**Marcin Metter et al [2]**	2000	"WAP Enabling existing HTML applications"	Wml Apps for Use in Wap Devises by Using HtmlApps.	WML (WIRELESS MARKUP LANGUAGE) usage in transform already-existing HTML apps through WAP capable devices.
3.	**Rene Struik et al [7]**	2006	"Security for the 802.15.3 Personal Area Network that is wireless"	Wpan Servies Has Been Implimented in Wap Protocol.	IEEE 802.15.3 it describes the security and architecture of WPANN it's easier to talk about the security services.
4.	**Dave Singe lee et al [8]**	2003	"WAP" stands for the Wireless Application Protocol.	Wtls Is Used to Secure the Communication Between Mobiles and Other Components By Wap Architectur.	SSL/TLS protocol's equivalent IS USED BY wap IN IMPLEMENTED IN WTLS

5.	**K.Muruganandam et al [9]**	2009	"Implementation of WAP Gateway Technologies by Means of Wireless Communication"	The protocol stack is made up of small pieces called There are versions of UDP, TCP, SLP, and HTTP that have shorter and simpler headers so they can work in wireless sensor networks.	The combination of WAP, WWW, and all the protocols that go with them make it possible for services to go from one terminal to the next.businesses. Transactional service development apps
6.	**Gökhan Kahraman et al [10]**	2003	Wireless Application Protocol Transport Layer Performance	To manage mobility, a The MIL-STD-188-220B protocol, which works on packet radio networks, is modelled as a simulation. utilized as a companion network for WTP.	There is no support for Wireless Transport Layer Security (WTLS).The User Datagram Protocol (UDP) is used to mimic the bearer adaption protocol of the WAP transport layer. FTP, HTTP, and email are all options. WTP's entire capability is represented by Are.

The Wireless Application Protocol (WAP) is a set of rules for sending data wirelessly over mobile networks. The WAP Forum, a prominent industry organization of mobile network operators and device makers, created it to provide a global standard for accessing content on the Internet from any type of wireless device. WAP allows users to use their mobile phones or other portable devices to access information such as e-mail, newsgroups, chat rooms, and web pages.

3. DIFFERENT TECHNIQUES USED FOR WIRELESS AREA NETWORK OF WIRELESS DEVICES:

3.1 Open shortest path first (OSPF)

OSPF, or "Open Shortest Path First," is an acronym. It is a well-known routing technique used in computer networks to determine the most effective path for data to travel across networks. The Internet Protocol (IP) family's OSPF link-state protocol is designed to function well in big industrial networks. OSPF works by creating a database of network topology, which includes information about the status and availability of network links. The protocol uses this database to calculate the

shortest way for data to move from one network to another. OSPF also uses a complex algorithm that looks at metrics like link bandwidth, delay, and cost to figure out the best way for data to travel.
One of the best things about OSPF is that it can quickly adapt to changes in how the network is set up. When a network link goes down or when a new link is added, OSPF quickly updates its database and recalculates the shortest path for data to travel. This makes OSPF a robust and reliable routing protocol, particularly in large enterprise networks where changes to the network can happen often. OSPF also allows for a network to be set up in a hierarchical way, enables network administrators to organize networks into smaller sub-networks, or areas. This helps to reduce the amount of traffic that needs to be processed by each router, which in turn improves network performance.
In big industrial networks, OSPF is a strong and adaptable routing protocol that enables effective and dependable network routing.

3.2 Routing information protocol (RIP)

"Routing Information Protocol" is what it's called. In computer networks, it is a distance-vector routing system used to determine the most effective path for data to travel across networks. RIP is one of the oldest and most basic routing protocols used on IP networks.
Routers in the network share routing information with each other so that RIP can work. Each router keeps track of the topology of the network in a database. This database has information about the status and availability of network links. Routers share this information so that they all have the same picture of how the network is set up.
RIP uses the number of hops to figure out the best way for data to move. Each router along the path adds one to the hop count as the data passes through it. The path with the fewest number of stops is thought to be the best path. and data is routed along that path. One of the limitations of RIP is its slow convergence time. When a network link goes down or a new link is added, RIP may take several minutes to update its routing table and find a new path for data to travel. This can result in network downtime or slow performance. Another limitation of RIP is its inability to support large networks with complex topologies. As the network size grows, RIP may become overwhelmed with the amount of routing information it needs to process, leading to network congestion and poor performance.
Overall, RIP is a simple and easy-to-configure routing protocol suitable for small networks with simple topologies. However, for larger networks with complex topologies, more advanced Most of the time, routing protocols like OSPF and BGP are used.

3.3 Enhanced interior gateway routing protocol (EIGRP)

Improved Interior Gateway Routing Protocol is the name of this system. It is a Cisco routing protocol used in computer networks to determine the most effective path for data to travel across networks. EIGRP is a hybrid routing protocol that combines elements of the link-state and distance-vector protocols.
EIGRP works by creating a database of network topology, which includes information about the status and availability of network links. The protocol uses this database to calculate the shortest path for data to travel from one network to another. EIGRP also employs a sophisticated algorithm that takes into account Using metrics like link bandwidth, delay, and reliability, we can find the most efficient path for data to travel.

One of the most important things about EIGRP is that it can converge quickly in response to changes in network topology. When a network link goes down or a new link is added, EIGRP quickly updates its routing table and finds a new path for data to travel. This makes EIGRP a robust and reliable routing protocol, particularly in large enterprise networks where network changes can occur frequently. EIGRP also supports load balancing, which enables multiple paths to be used simultaneously to increase network throughput. EIGRP uses a sophisticated algorithm to determine the best paths for load balancing, which includes metrics like link bandwidth, delay, and reliability.

In big industrial networks, EIGRP is a sophisticated and adaptable routing protocol that is used to quickly and reliably route traffic. However, because it is a proprietary protocol, only Cisco hardware may use it. This makes it hard for it to work with equipment from other companies.

3.4 Static protocol (STATIC)

Network routing known as "static routing" entails manually configuring the routing tables on each router in the network by the network administrator. With static routing, the best way for data to move from one network to another is chosen by hand by the network administrator, based on how the networks are set up.

Static routing is a simple way to route that is easy to set up and works well for small networks. with simple topologies. It is also useful in situations where network traffic is predictable and does not change frequently.

One advantage of static routing is that it is easier to understand and uses less resources than dynamic routing protocols. such as OSPF and EIGRP. Since routing tables are manually configured, Routers don't need to talk to each other or run complicated routing algorithms. This can result in faster routing and lower network overhead. However, static routing also has several limitations. Its inability to react to changes in the way the network is set up is one of its key drawbacks. The network administrator must manually update the routing tables on all impacted routers whenever a network link is lost or a new one is established. This can take a long time and lead to mistakes, especially in large networks with a lot of routers.

4. AUTHENTICATION SERVICE

To authenticate a service in the WAP protocol, we would typically use a combination of authentication mechanisms provided by the underlying transport protocol and the WAP protocol itself. Here are some steps that you would take to authenticate a WAP service:

- To secure the connection between the client and server in Figure 2, use Transport Layer Security (TLS) or Secure Sockets Layer (SSL).This will provide encryption and authentication of the communication channel.
- Use HTTP authentication mechanisms such as Basic authentication or Digest authentication to authenticate the client to the server. This requires the client to provide a username and password, which are verified by the server.
- Use the WAP User Agent Profile (UAProfile) to authenticate the client device to the server. This involves exchanging profile information from the client to the server to identify the capabilities of the client device Figure 3.
- Use digital certificates to authenticate the client and server to each other. This involves exchanging certificates between the client and server to verify the identity of each party.

By using a combination of these authentication mechanisms, you can ensure that the WAP service is secure and only accessible to authorized clients.

Industrial Engineering Journal
ISSN: 0970-2555
Volume : 52, Issue 4, No. 1, April : 2023

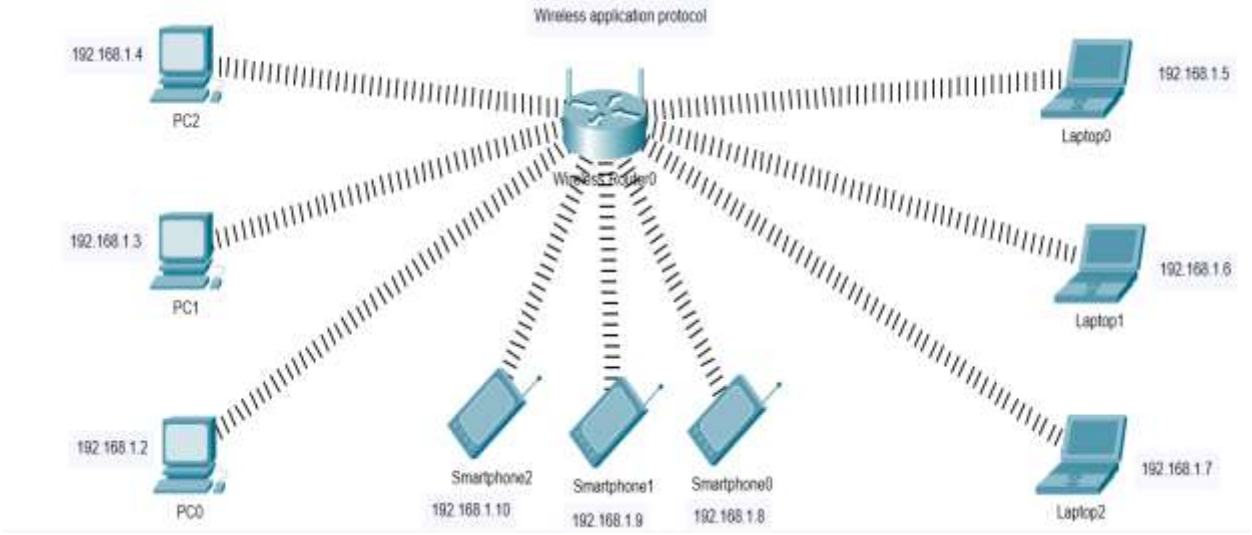

Figure 3: Implementation of WAP with Secure Authentication

5. RESULTS AND DISCUSSIONS

Table 2. Result and discussion

List of Protocols with Time taken to deliver the packets	OSPF Time taken values	STATIC Time taken values	RIP Time taken values	EIGRP Time taken values	With WAP Protocols Time taken values
Source	PC	PC	Router	PC	Router
Destination	Router	Router	PC	Router	Pc
Min time taken to delivery	11ms	11ms	13ms	10 ms	2ms
Max time taken to delivery	19ms	17ms	15ms	15 ms	6ms
Average Time taken to delivery	29ms	27ms	30ms	17 ms	3ms
Packet loss	0	0	0	0	0

The wireless application protocol was user accessibility and flexible networking, and the technology that moves very quickly, multiple platforms can be used to implement it. Implementation near to internet model. WAP works on the newest mobile phones.

Advantages

• WAP lets you send and receive data in real time, and most modern cell phones can use it.
• Close to the Internet model for implementation
• Saves time.
• Helps manufacturers of devices, infrastructure, and gateways sell more.
• Personalized

Disadvantages

- Small screens for displays

- A little bandwidth
- Accessibility quickly and limited availability

Applications

The following are a some of the most popular WAP or wireless application protocol applications:

- WAP makes it easier for you to use your mobile devices to be able to use the Internet.
- You can play games on mobile devices that are wireless.
- It makes it easier for you to access emails on mobile networks.
- Mobile devices may be used to fill out expense claims and access timesheets.
- Nowadays, online mobile banking is increasingly common.
- It may also be utilised in a variety of Internet-based services, including traffic updates, weather forecasts, flight information, movie and theatre information, and geographic location. All of them are made feasible by WAP technology.

6. CONCLUSION

• The independence of WAP is a welcome change in a sector where proprietary standards have hindered the development of the next generation of mobile Internet communications. WAP is a rapidly developing technology. It is a free, open-source technology that doesn't cost anything. It can be used on more than one platform. It works with any network standard. It gives you more ways to control it. It is set up similarly to how the Internet works. With WAP, you can send and receive data in real time.

WAP is now supported by most modern cell phones and other devices. The wireless environment is made feasible by WAP's markup language and transport protocol standards, which provide companies of all sizes access to an emerging market. In North America, WAP is one of the rules for how wireless devices can connect to the Internet. Most cell phones you can buy today and, in the future, already have WAP support built in. Big companies are starting to make WAP apps that let people use their WAP devices to manage their finances. A lot of money is going into making this technology better. This means that it will be a standard for a long time because users and companies will not want to give up their applications that they have already spent a lot of time and money on if WAP's flaws are not fixed. WAP could either lead the wireless revolution or slow it down. This is why it's important to talk about the security problems. Nobody will use a system where they can have their personal data taken.

The WAP Forum talks about these problems and is working to solve them in new versions of WAP so that information stays safe when someone uses their wireless device to send private data and we get a secure connection from one end to the other. If we see WAP as a way to connect the mobile world to the Internet and we do a good job of putting it into place, it will happen. Because of the cost of delivery, modest additional expenses, or unneeded costs, the amount of static is measured against the highest standard when evaluating WAP protocols. In comparison to the other protocols, the WAP protocols are also the most effective. To achieve the optimal performance, WAP and static measurements are always precise.

REFERENCES

[1]: “Weilian Su.”Time diffusion concepts and protocol for sensor networks”, Emerging location aware broadband wireless ad hoc networks,2005.

[2]: “WAP enabling existing HTML applications” Marcin Metter, Dr Robert Colomb Department of Computer Science and Electrical Engineering The University of Queensland, QLD 4072, Australia 2000

[3]: “Wireless Communication Methodologies & Wireless Application Protocol” By Sankara Krishnaswamy NH – 03062

[4]: “Study of WAP Mobile E-Commerce Security on WPKI” Feng TIAN, Xiao-bing HAN Xi’an, China

[5]: “Hua Jiang. Study on Mobile E-commerce Security Payment System” 2008 International Symposium on Electronic Commerce and Security. August 2008. pp.754-757
[6]: “David Wright. The Role of Wireless Access Interconnection in Mobile e-Commerce Industry Evolution. Eighth World Congress on the Management of eBusiness” (WCMeB 2007).July 2007 pp. 1
[7]: “Security for the 802.15.3 Wireless Personal Area Network” Rene Struik 2006
[8]: “The Wireless Application Protocol (WAP)” Dave Singel´ee, Bart Preneel COSIC Internal Report September 2003
[9]: “Implementation of WAP Gateway Technologies through Wireless Communication” ”K. Muruganandam”, ©2009 IEEE.
[10] “Wireless Application Protocol Transport Layer Performance” “Gökhan Kahraman”, © 2003 IEEE.
[11] Jin Yan, Li Tong "Compare and Analysis of Security Strategy in WAP and I-Mode Network"
[12] Salvatore P. Savino "WAP: Wireless Application Protocol - Wireless Wave of the Future" Cap Gemni Ernst and Young, Telecom Media and Networks, 100 Walnut Avenue Clark, New Jersey 07066 USA
[13] Feng TIAN, Xiao-bing HAN "Study of WAP Mobile E-Commerce Security on WPKI" 978-0-7695-3643-9/09 $25.00 © 2009 IEEE DOI 10.1109/ISECS.2009.81
[14] Marc Bechler, Jochen Schiller "THE NEED FOR THE WIRELESS APPLICATION PROTOCOL (WAP) IN CARS"
[15] Weilian Su, Member, IEEE, and Ian F. Akyildiz "Time-Diffusion Synchronization Protocol" IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 13, NO. 2, APRIL 2005
[16]: “Study of WAP Mobile E-Commerce Security on WPKI” Feng TIAN, Xiao-bing HAN Xi’an, China
[17]: “Hua Jiang. Study on Mobile E-commerce Security Payment System” 2008 International Symposium on Electronic Commerce and Security. August 2008. pp.754-757
[18]: “David Wright. The Role of Wireless Access Interconnection in Mobile e-Commerce Industry Evolution. Eighth World Congress on the Management of eBusiness” (WCMeB 2007).July 2007 pp. 1
[19] “Design and Implementation of a PKI-Based End-to-End Secure Infrastructure for Mobile E-commerce” T. Cheung , S. Chanson. Second International Conference on Web Information Systems Engineering (WISE'01) Volume 1. December 2001. pp. 0003
[20]: “A Reliable and Configurable E-commerce Mechanism Based on Mobile Agents in Mobile Wireless” Hu Haiyang , Hu Hua. Environments. The 2007 International Conference on Intelligent Pervasive Computing (IPC 2007),October 2007 pp. 7-10
[21]: “New secure mobile Electronic commerce solution based on WAP” CUI Jian-qi, YAO Dan-li. Application Research of Computers. Vol.24 No.9 2007(9)
[22]: “Security for the 802.15.3 Wireless Personal Area Network” Rene Struik
[23]: “The Wireless Application Protocol (WAP)” Dave Singel´ee, Bart Preneel COSIC Internal Report September 2003