CS8601 -MOBILE COMPUTING

UNIT 4

MOBILE TRANSPORT AND APPLICATION LAYER

4.1. Mobile TCP

There are several mechanisms of the Transmission Control Protocol (TCP) that influence the efficiency of TCP in a mobile environment.

Traditional TCP improvements

Improvement in TCP: TCP was initially designed for wired (traditional) networks

4.1.1 Slow start

4.1.2 Congestion Avoidance

4.1.3 Fast retransmit/fast recovery

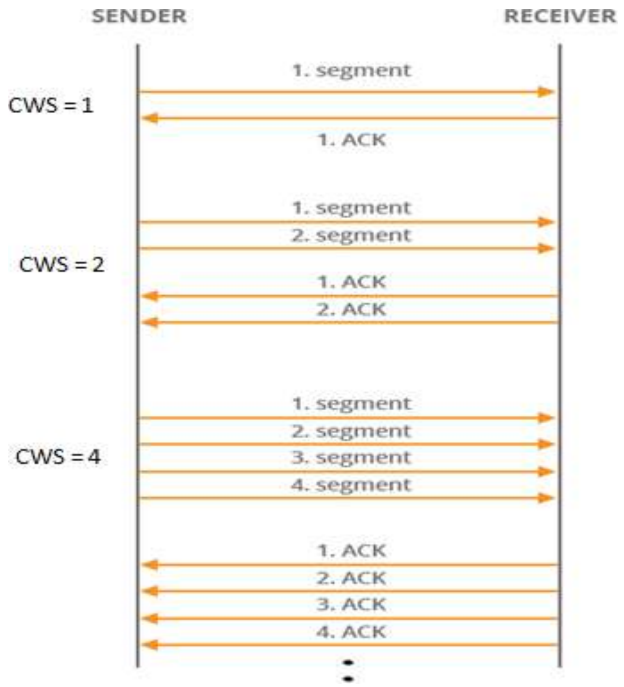
4.1.1 Slow start

The behaviour TCP shows after the detection of congestion is called slow start .Instead of starting transmission at a fixed transmission window size, the transmission is started at the lowest window size and then doubled after each successful transmission.

If congestion is detected, the transmission window size is reduced to half of its current size.

The sender always calculates a congestion window for a receiver.

1. The start size of the congestion window is one segment.
2. The sender sends one packet and waits for acknowledgement.
3. If this acknowledgement arrives, the sender increases the congestion window by one, now sending two packets.
4. After arrival of the two corresponding acknowledgements, the sender again adds 2 to the congestion window, one for each of the acknowledgements.
5. Now the congestion window equals 4.
6. This scheme doubles the congestion window every time the acknowledgements come back, which takes one round trip time (RTT). This is called the exponential growth of the congestion window in the slow start mechanism.

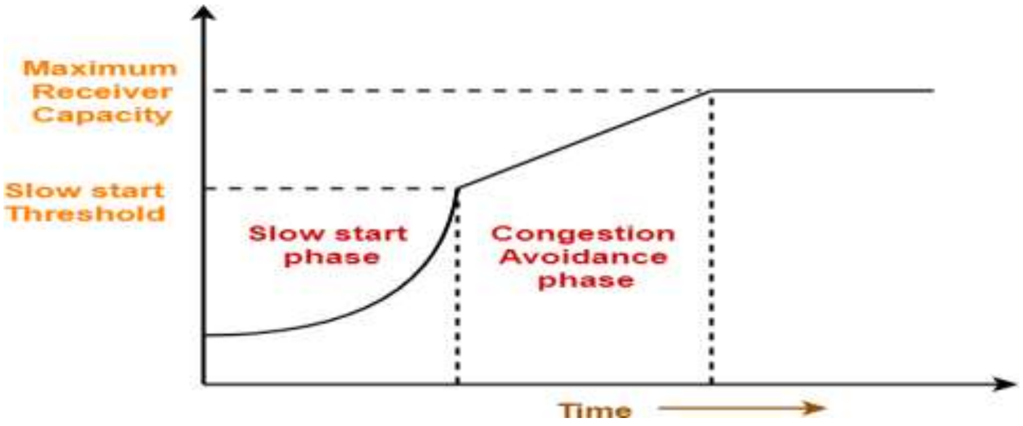


4.1.2 Congestion Avoidance

Congestion avoidance start when slow start stops. Drawback in slow start: It is too dangerous to double the congestion window each time because the steps might become too large.

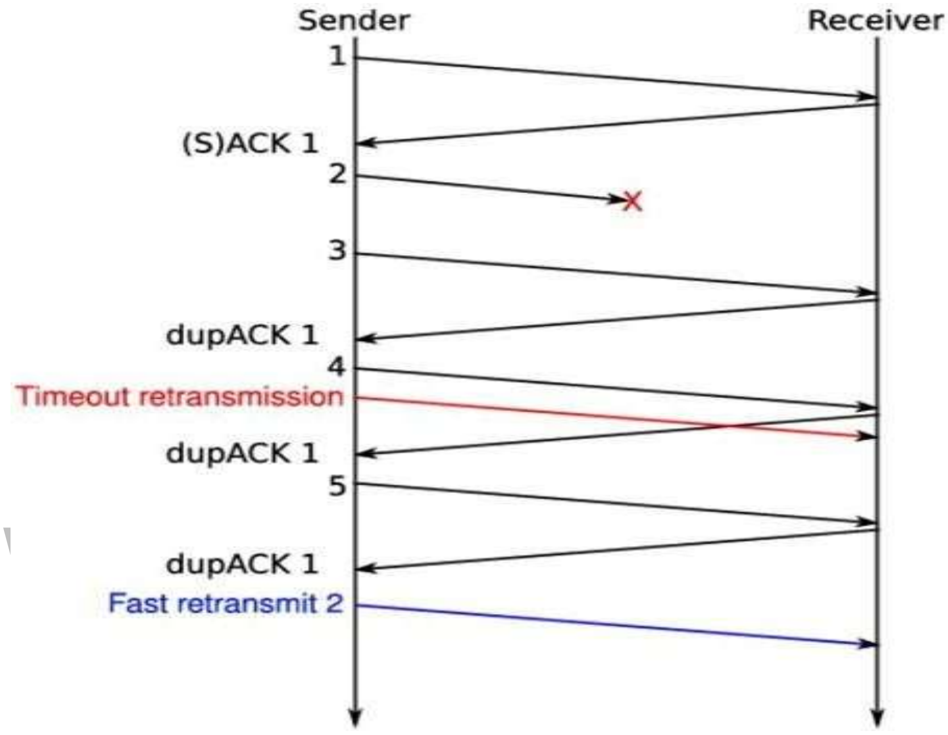
Solution:

- Window size is doubled until it reaches a threshold level.
- When it reaches a threshold level, then window size is increased linearly.
- If congestion is occurred, then the window size is reduced to half of its size.
- If it reaches zero then again slow start begins



4.1.3 Fast retransmit/fast recovery

- The sender can retransmit the missing packet(s) before the timer expires.
- It does not wait until the timer expires it retransmit a packet whenever sender is getting 3 duplicate acknowledgements.
- After retransmitting a packet it sets the window size is reduced to its half



Classical TCP Improvements For Wireless NETWORK

Mechanisms to increase TCP's performance in wireless and mobile environments:

- Indirect TCP (I-TCP)
- Snooping TCP (S-TCP)
- Mobile TCP (M-TCP)
- Fast retransmit/fast recovery
- Transmission/time-out freezing
- Selective retransmission
- Transaction-oriented TCP (T-TCP)

i)Indirect TCP (I-TCP)

Two competing insights led to the development of indirect TCP:

1)TCP performs poorly together with wireless links

2)TCP within the fixed network cannot be changed

Working:

- I-TCP segments a TCP connection into a fixed part and a wireless part.
- Mobile host connected via a wireless link and an access point to the 'wired' internet where the correspondent host resides. The correspondent node could also use wireless access.
- Standard TCP is used between the fixed computer and the access point.
- The foreign agent (access point) acts as a proxy and relays all data in both directions.

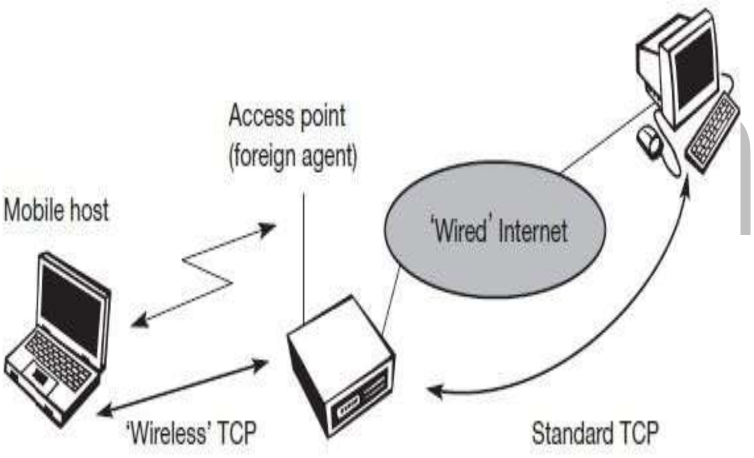
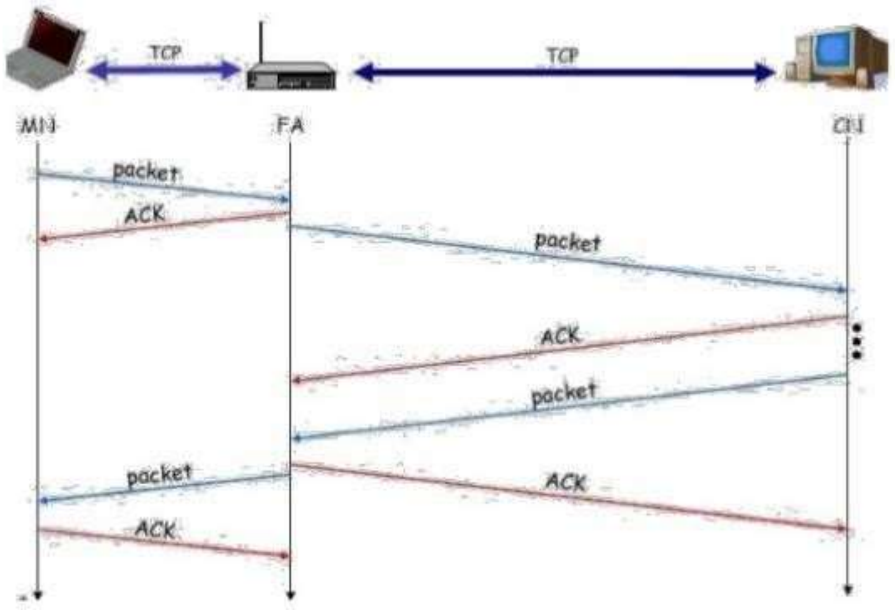


Fig. I-TCP segments a TCP connection into two parts

Packet delivery:

- If CN sends packet, FA acknowledges packet and forwards packet to MN
- If MN receives packet, it acknowledges
- This acknowledgement only used by CN
- Similarly if MN sends packet, FA acknowledges packet and forwards it to CN



Packet Loss:

Case1 : If a packet is lost on the wireless link due to a transmission error:

•Then the CN would not notice this.

•The FA tries to retransmit this packet locally to maintain reliable data transport.

Case2:If the packet is lost on the wireless link:

•The MN notice this much faster due to the lower round trip time and can directly retransmit the packet.

•Packet loss in the wired network is now handled by the FA.

Advantages with I-TCP:

1.TCP does not require any changes in the TCP protocol as used by the hosts in the fixed network.

2.Due to the strict partitioning into two connections, transmission error cannot propagate into the fixed network.

3.Partitioning into two connections allows the use of a different transport layer protocol between the FA and the MN.

4.Different solutions can be tested or used at the same time without disturbing the stability of the Internet.

Disadvantages of I-TCP:

1. The loss of the end-to-end semantics of TCP might cause problems if the FA partitioning the TCP connection crashes:

2. Increased handover latency may be much more problematic

3. The FA must be integrated into all security mechanisms.

ii)Snooping TCP (S-TCP)

The segmentation drawback of I-TCP is eliminated by Snooping TCP."The FA buffers all packets with destination MN and additionally 'snoops' the packet flow in both directions to recognize acknowledgements".Reason for buffering: To enable the FA to perform a local retransmission in case of packet loss on the wireless link.

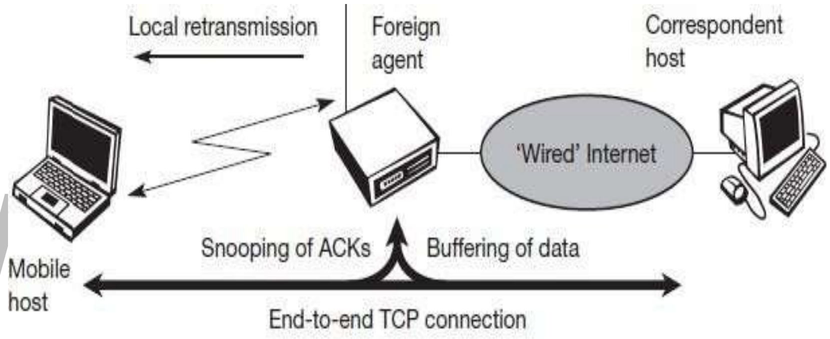


Fig. Snooping TCP

Data transfer to the MH (Mobile Host)

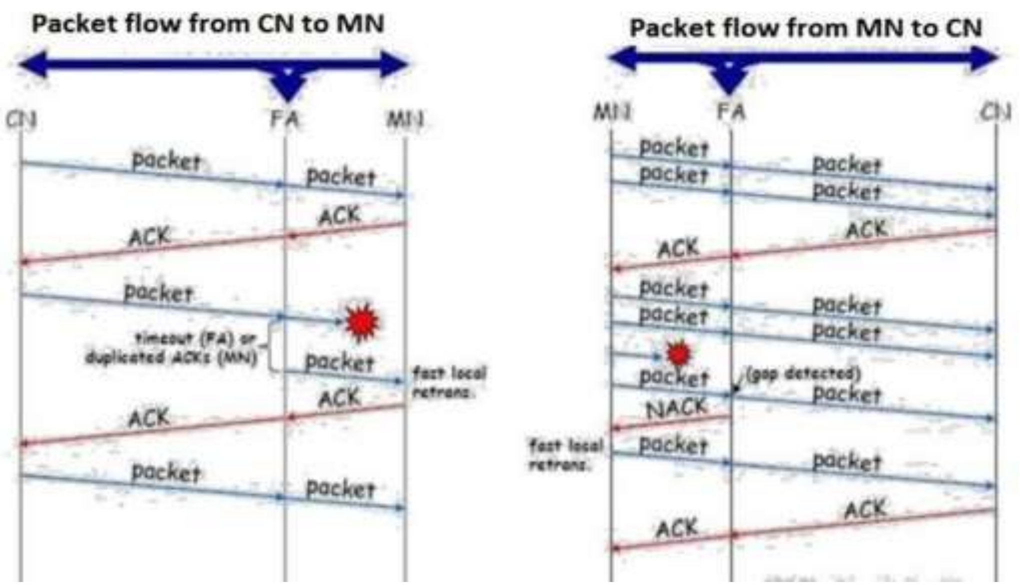
•FA buffers data until it receives ACK of the MH

•FA detects packet loss via duplicated ACKs or time-out

Data transfer from the MH (Mobile Host)

•FA detects packet loss on the wireless link via sequence numbers, FA answers directly with a negative acknowledgement (NACK) to the MH

•MH can now retransmit data with only a very short delay



Advantages:

1.The approach automatically falls back to standard TCP if the enhancements stop working.

2.The CN does not need to be changed since most of the enhancements are in the FA.

3.It does not need a handover of state as soon as the MH moves to another FA.

4.It does not matter if the next FA uses the enhancement or not. If not, the approach automatically falls back to the standard solution.

Disadvantages:

1.Snooping TCP does not isolate the behaviour of the wireless link as good as I-TCP.

2.Additional mechanism for negative acknowledgements (NACK) between FA and MH.

3.Snooping and buffering data may be useless if certain encryption schemes are applied end-to-end between the correspondent host and mobile host.

iii) Mobile TCP (M-TCP)

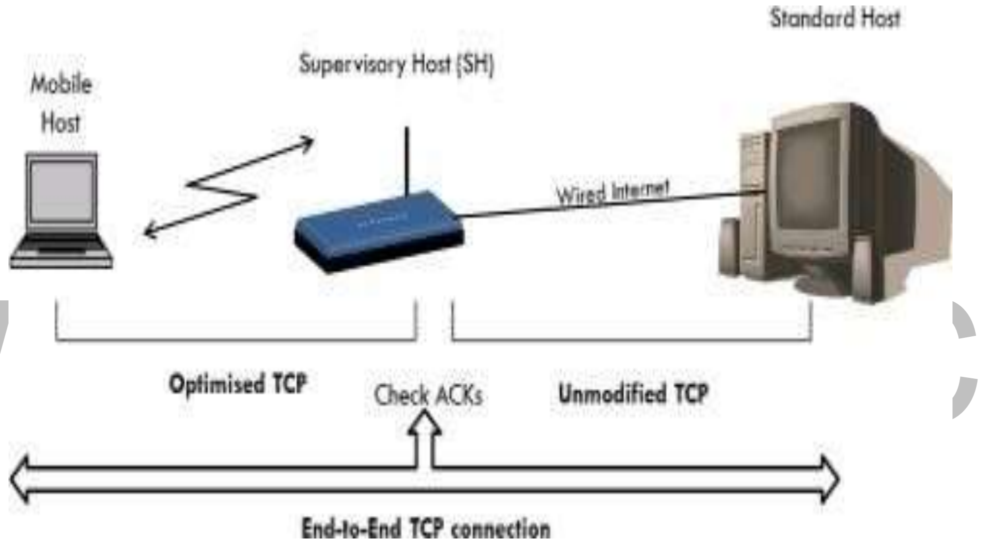
I-TCP and S-TCP does not work well, if a MH is disconnected. The M-TCP has the same goals as I-TCP and snooping TCP

Goals of M-TCP:

- ✓ Prevent the sender window from shrinking if bit errors or disconnection.
- ✓ Improve overall throughput
- ✓ Lower the delay
- ✓ Maintain end-to-end semantics of TCP
- ✓ Provide a more efficient handover
- ✓ Adapted to the problems arising from lengthy or frequent disconnections

The M-TCP splits up the connection into two parts:

- ❖ An unmodified TCP is used on the Standard host-Supervisory Host section
- ❖ An optimised TCP is used on the Supervisory Host- Mobile Host section.



The SH is responsible for exchanging data to both the Standard host and the Mobile host. In this approach, we assume that the error bit rate is less as compared to other wireless links. So if any packet is lost, the retransmission has to occur from the original sender and not by the SH.

1. The SH monitors the ACKs being sent by the MH.

2. If for a long period ACKs have not been received, then the SH assumes that the MH has been disconnected.

3. If so the SH blocks the sender by setting its window size to 0.

4. Then the sender goes into persistent mode i.e. the sender will not try to retransmit the data.

5. Now when the SH detects a connectivity established again with the MH, the window of the sender is restored to original value.

Advantages of Mobile TCP:

1.M-TCP maintains the TCP end-to-end semantics.

2.If the MH is disconnected, it avoids useless retransmissions, slow starts or breaking connections by simply shrinking the sender's window to 0.

3.M-TCP does not buffer data so, no forwarding.

Disadvantages of Mobile TCP:

1.The SH does not act as proxy

2.M-TCP assumes low bit error rates, which is not always a valid assumption.

3.Requires new network elements like the bandwidth manager.

iv) Fast retransmit/fast recovery

Change of FA often results in a packet loss. TCP reacts with slow start although there is no congestion.

Solution: Fast retransmit method.

Fast retransmit method: When a MH moves to a new FA, it transmits the ACK of the last packet was received. It is indication for the CN to continue transmission at the same rate it did before MH moves to another FA. This approach puts the CN to fast retransmission mode.

Advantages:

1.It is simple.

2.Only minor changes in the MN software results in performance increase.

3.No FA or CN host has to be changed.

Disadvantages: Increased time delay in the retransmitted packets to move from CN to MH.

v) Transmission/time-out freezing

In normal TCP, a disconnection takes place when the connection is lost for a longer time.

Example: When a MN moving through a tunnel or passing black out areas, the connection is lost and it needs to make connection once again, when it comes back.

TCP freezing:

- MAC layer is often able to detect interruption in advance
- MAC can inform TCP layer of upcoming loss of connection
- TCP stops sending, but does not assume a congested link.
- MAC layer signals again if reconnected.

Advantages:

1.Offers a way to resume TCP connection even after longer interruptions of the connection.

2.Independent of any other TCP mechanism, such as ACKs, sequence numbers etc.

Disadvantages:

(i)The software on the MN and CN needs to be changed.

(ii)Depends on MAC layer

vi) Selective retransmission

TCP acknowledgements are cumulative. ACK n acknowledges correct & in-sequence receipt of packet up to n. If a single packet is lost quite often a whole packet sequence beginning at the gap has to be retransmitted. Bandwidth wastage.

Solution: Selective Retransmission

•Allows the receiver acknowledge a single packets

•Now the sender can retransmit only the missing packet.

Advantage:

•The sender retransmits only the lost packets.

•Much higher efficiency. Lowers bandwidth requirement

Disadvantage: More complex software on the MH.

vii)Transaction-oriented TCP (T-TCP)

TCP requires several trans reception of packets for:

- ❖ Connection setup
- ❖ Data transmission
- ❖ Connection release.

(-) Even a short message needs minimum of 7 packets leads to connection overhead.

Solution: T-TCP

Connection setup,Data transmission,Connection release can be combined,thus only 2 or 3 packets are needed.Reduces the total overhead.

Advantage: Reduction in overhead.

Disadvantage: Requires changed TCP, Mobility not longer transparent.

COMPARISON OF VARIOUS TCP

Approach	Mechanism	Advantages	Disadvantages
Indirect TCP	Splits TCP connection into two connections	Isolation of wireless link, simple.	Loss of TCP semantics. Higher latency athandover, security problems.
Snooping TCP	Snoops data and acknowledgements, local retransmission	Transparent for end to end connection, MAC integration possible	Insufficient isolation of Wireless link, security problems
M-TCP	Splits TCP connection, chokes sender via window size	Maintains end to end semantics, handles long term and frequent disconnections	Bad isolation of wireless link, processing overhead due to bandwidth management, security problems
Fast Retransmission /Fast Recovery	Avoids slow start ate roaming	Simple and efficient	Mixed layers, nottransparent.
Transmission / Time out freezing	Freezes TCP state at disconnection, resumes after reconnection	Independent of content, works for longer interruptions	Changes in TCPrequired, MAC dependent
Selective retransmission	Retransmits only lost data.	Very efficient	Slightly more complex receiver software, more bufferspace needed
Transaction oriented TCP	Combines connection setup-/ release and data retransmission	Efficient for certain applications	Changes in TCPrequirednot transparent, security problems.

CS8601 -MOBILE COMPUTING

UNIT 4

MOBILE TRANSPORT AND APPLICATION LAYER

4.7. Wireless application environment (WAE)

WAE is used to create a general-purpose application environment based WWW. Allow service providers, software manufacturers, or hardware vendors to integrate their applications. WAE has already integrated the following technologies and adapted them for use in handheld devices.

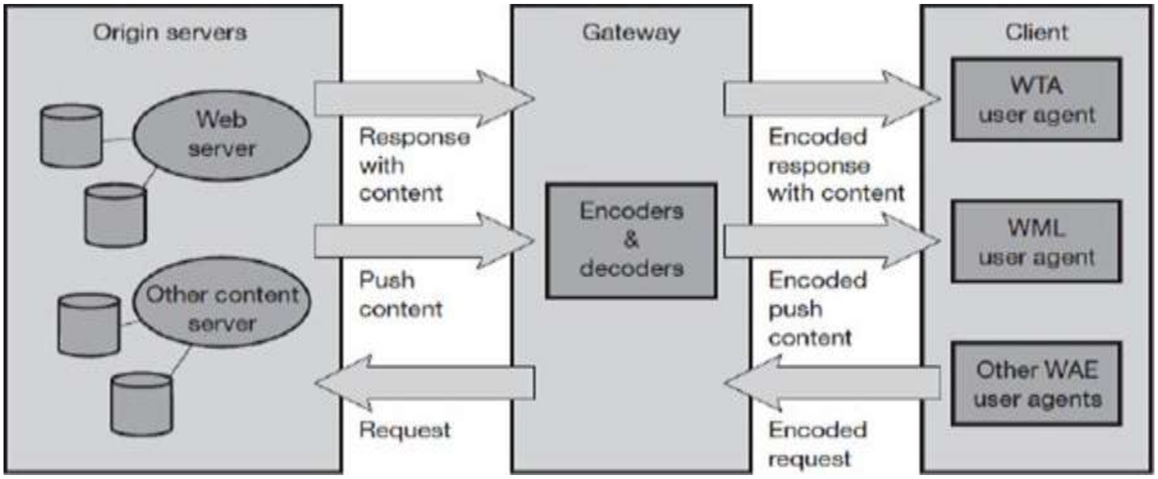
Integrated technologies: HTML, JavaScript, and the handheld device mark- up language HDML form the basis of the wireless mark-up language (WML) and the scripting language WMLscript. The exchange formats for business cards and phone books vCard and for calendar vCalendar have been included.

URLs from the web can be used. A wide range of mobile telecommunication technologies have been adopted and integrated into the wireless telephony application (WTA).

Goal: To minimize over-the-air traffic and resource consumption on the handheld device.

WAE: Logical model:

- Model is close to WWW model but assumes an additional gateway.
- ***Client:*** Issues an encoded request for an operation on a remote server. This is usually a WAP browser
- ***Encoding:*** Used to minimize data sent over the air and to save resources on the handheld device
- **Decoders:** Translate the encoded request into a standard request as understood by the origin servers. This could be a request to get a web page.
- ***Gateway:*** Transfers the request to the appropriate origin server.



•***Origin server:*** Standard web servers running HTTP and generating content using scripts, providing pages using a database, or applying any other technology. Origin servers will respond to the request. Then the gateway encodes the response and its content & then transfers the encoded response with the content to the client.

•***Push services:*** The WAE logical model also includes push services.

- ✓ Then an origin server pushes content to the gateway.
- ✓ The gateway encodes the pushed content and transmits the encoded push content to the client.

•***User Agent:*** Several user agents can reside within a client.

- ✓ User agents include such items as: browsers, phonebooks, message editors etc.
- ✓ WAE does not specify the number of user agents or their functionality.
- ✓ User agent handles access to, and interaction with, mobile telephone features.

CS8601 -MOBILE COMPUTING

UNIT 4

MOBILE TRANSPORT AND APPLICATION LAYER

4.2. Wireless Application Protocol (WAP)

WAP is used to enable the access of internet in the mobile phones or PDAs.The wireless application protocol forum (WAP Forum) was founded in June 1997 by Ericsson, Motorola, Nokia, and Unwired Planet.WAP is independent of OS that means WAP can be implemented on any OS.

Features:

Interoperable: Allowing terminals and software from different vendors to communicate with networks from different providers

Scalable: Protocols and services should scale with customer needs and number of customers

Efficient: Provision of QoS suited to the characteristics of the wireless and mobile networks

Reliable: Provision of a consistent and predictable platform for deploying services

Secure: Preservation of the integrity of user data, protection of devices and services from security problems.

WAP Architecture:

WAP is designed in a layered fashion, so that it can be extensible, flexible, and scalable. The WAP protocol stack is divided into five layers −

Layers of WAP Protocol:

- Application Layer (Wireless Application Environment (WAE))
- Session Layer(Wireless Session Protocol (WSP))
- Transaction Layer(Wireless Transaction Protocol (WTP))
- Security Layer(Wireless Transport Layer Security (WTLS))
- Transport Layer(Wireless Datagram Protocol (WDP))

a)Bearer services

The basis for transmission of data is formed by different bearer services. WAP uses existing data services and will integrate further services.

Example:

Message services such as short message service (SMS) of GSM, Circuit- switched data such as high-speed circuit switched data (HSCSD) in GSM. Packet switched data such as general packet radio service (GPRS) in GSM. Many other bearers are supported, such as CDPD, IS-136,PHS. No special interface has been specified between the bearer service

b) Transport Layer (Wireless Datagram Protocol (WDP))

- The transport layer with its wireless datagram protocol (WDP) and the additional wireless control message protocol (WCMP) offers a bearer independent, reliable datagram-oriented service to the higher layers of the WAP architecture.Communication is done transparently over one of the available bearer services. Transport layer service access point (T-SAP) - The common interface to be used by higher layers independent of the underlying network.

c)Security Layer (Wireless Transport Layer Security (WTLS))

The security layer with its wireless transport layer security protocol offers its service at the security SAP (SEC-SAP).WTLS is based on the transport layer security / secure sockets layer (TLS/SSL).WTLS has been optimized for use in wireless networks with narrow-band channels.It can offer data integrity, privacy, authentication and denial-of-service protection.

d) Transaction Layer (Wireless Transaction Protocol (WTP))

Transaction layer with its wireless transaction protocol (WTP) offers a lightweight transaction service at the transaction SAP (TR-SAP).This service efficiently provides reliable or unreliable requests and asynchronoustransactions.

e) Session Layer (Wireless Session Protocol (WSP))

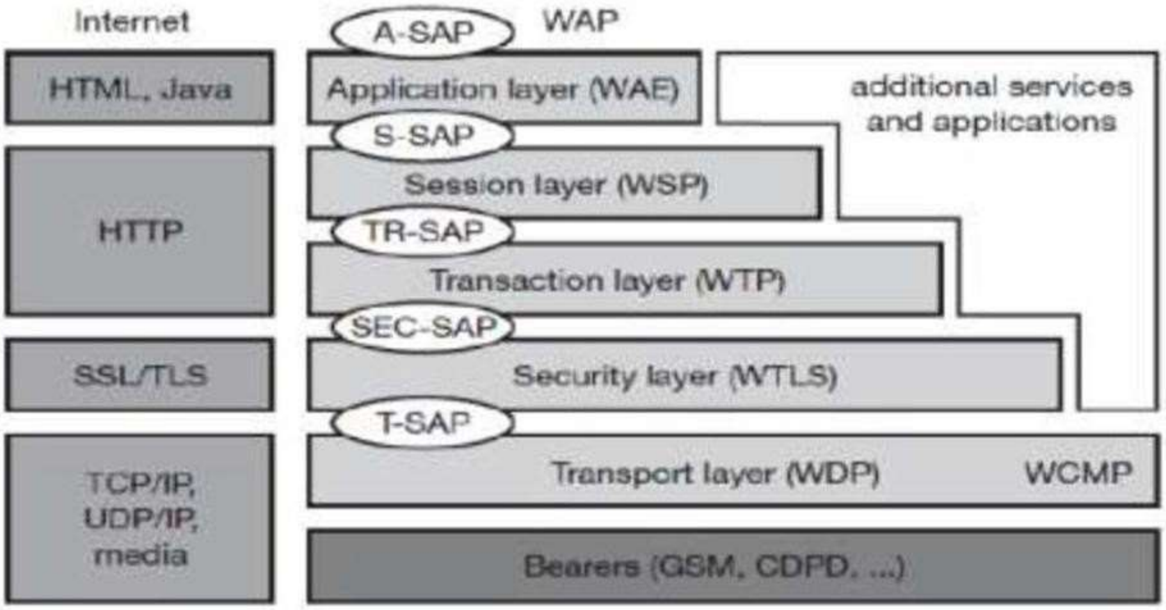
Session layer with the wireless session protocol (WSP) currently offers two services at the session-SAP (S-SAP):

- ✓ Connection-oriented
- ✓ Connectionless

A special service for browsing the web (WSP/B) has been defined that offers HTTP/1.1 functionality, long-lived session state, session suspend and resume, session migration and other features needed for wireless mobile access to the web.

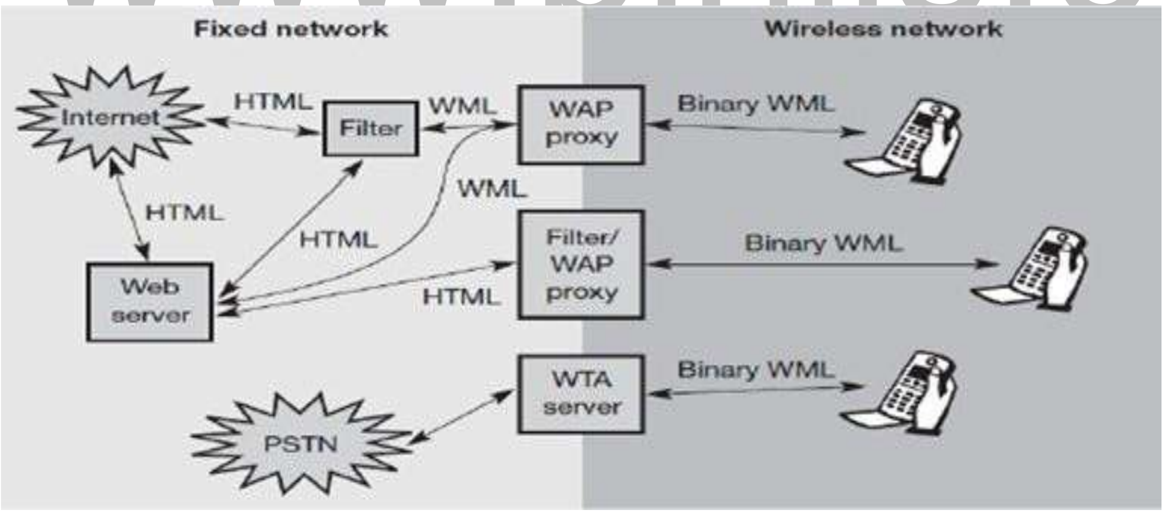
f) Application Layer (Wireless Application Environment (WAE))

The application layer with the wireless application environment (WAE) offers a framework for the integration of different www and mobile telephony applications.It offers many protocols and services with special service access



Components and Interface of WAP Architecture

Integration of WAP components:



- On the left side, different fixed networks, such as the traditional internet and the public switched telephone network (PSTN), are shown.
- Several new elements will be implemented between these networks
- WAP-enabled wireless, mobile devices in a wireless network on the right- hand side.

•To browse web pages with handheld devices, a wireless mark-up language (WML) has been defined in WAP.

•Special filters within the fixed network can translate HTML into WML, web servers can already provide pages in WML, or the gateways between the fixed and wireless network can translate HTML into WML. These gateways not only filter pages but also act as proxies for web access.

•WML is additionally converted into binary WML for more efficient transmission.

•Wireless telephony application (WTA) server translates all incoming signals into WML events displayed at the handheld device.

CS8601 -MOBILE COMPUTING

UNIT 4

MOBILE TRANSPORT AND APPLICATION LAYER

4.6. Wireless session protocol (WSP)

WSP has been designed to operate on top of the datagram service WDP or the transaction service WTP. Provides a shared state between a client and a server.

WSP offers the following needed for content exchange between cooperating clients and servers:

1.Session management:

- ✓ WSP introduces sessions that can be established from a client to a server.
- ✓ The capabilities of suspending and resuming a session are important to mobile applications.
- ✓ Assume a mobile device is being switched off – it would be useful for a user to be able to continue operation at exactly the point where the device was switched off.

2. Capability negotiation:

- ✓ Clients and servers can agree upon a common level of protocol functionality during session establishment.
- ✓ Example parameters to negotiate are:
  - ❖ Maximum client SDU size
  - ❖ Maximum outstanding requests
  - ❖ Protocol options
  - ❖ Server SDU size.
  - ❖ Content encoding

WSP defines the efficient binary encoding for the content it transfers.WSP offers content typing and composite objects.Wireless Session Protocol/Browsing (WSP/B) - comprises protocols and services most suited for browsing-type applications.

WSP/B offers the following features:

- ❖ HTTP/1.1 functionality:
  - ✓ WSP/B supports the HTTP/1.1 functions, such as
  - ✓ Extensible request/reply methods
  - ✓ Composite objects
  - ✓ Content type negotiation.

- ❖ Exchange of session headers:
  - ✓ Client and server can exchange request/reply headers that remain constant over the lifetime of the session.
  - ✓ These headers may include:Content types, character sets, languages, device capabilities, and other static parameters.
  - ✓ WSP/B will not interpret header information but passes all headers directly to service users.
- ❖ Push and pull data transfer:
  - ✓ Pulling data from a server is supported by WSP/B using the request/response mechanism.

WSP/B supports three push mechanisms for data transfer:

i. A confirmed data push within an existing session context

ii. A non-confirmed data push within an existing session context

iii. A non-confirmed data push without an existing session context.

- ❖ Asynchronous requests:
  - ✓ Optionally, WSP/B supports a client that can send multiple requests to a server simultaneously.
  - ✓ This improves efficiency & latency

CS8601 -MOBILE COMPUTING

UNIT 4

MOBILE TRANSPORT AND APPLICATION LAYER

4.8. Wireless Telephony Application (WTA) architecture

WTA is a collection of telephony specific extensions for call and feature control mechanisms, merging data networks and voice networks. It is an extension of basic WAE application model

Features:

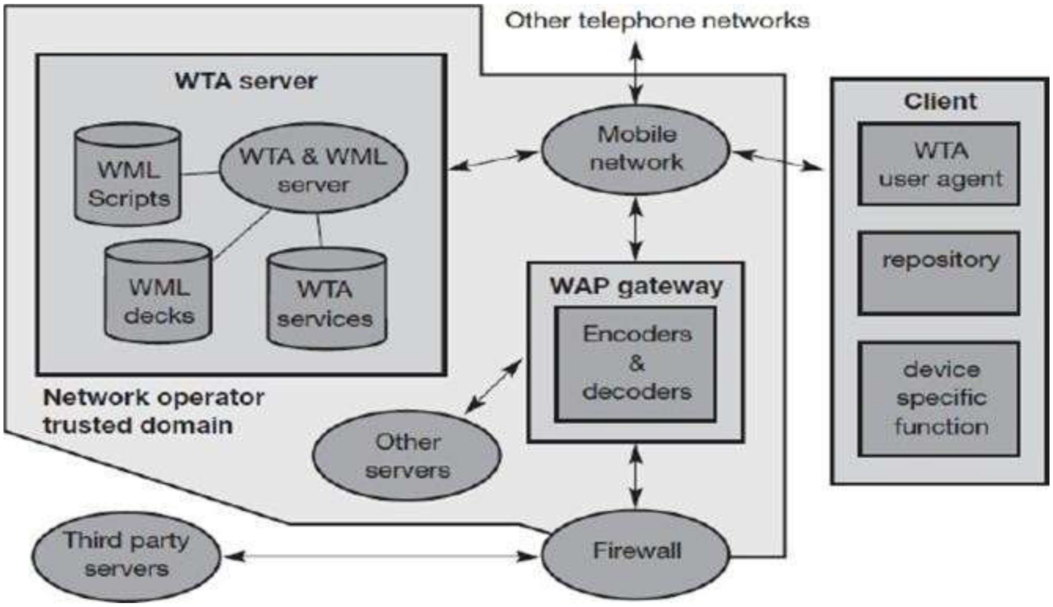
•***Content push:*** A WTA origin server can push content to the client. A push can take place without prior client request. The content can enable the client to handle new network events.

•***Access to telephony functions:*** The wireless telephony application interface (WTAI) provides many functions to handle telephony events such as call accept, call setup, change of phone book entries etc....

•***Repository for event handlers:*** The repository represents a constant storage on the client for content required to offer WTA services. Content are either channels or resources.

- ✓ Examples for resources: WML decks, WMLScript objects, or WBMP pictures.
- ✓ A channel comprises references to resources and is associated with a lifetime.
- ✓ Within this lifetime, it is guaranteed that all resources the channel points to are locally available in the repository.
- ✓ The motivation behind the repository is the necessity to react very quickly for time-critical events.

•***Security model:*** Mandatory for WTA is a security model. WTA allows the client to only connect to trustworthy gateways and check if the servers providing content are authorized to send this content to the client.



a) Client

•The client is connected via a mobile network with a WTA server, other telephone networks and a WAP gateway.

•A WML user agent running on the client.

•The client may have voice and data connections over the network.

b) Firewall: Firewall is useful to connect third-party origin servers outside the trusted domain.

c)WTA server: One difference between WTA servers and other servers besides security is the tighter control of QoS.

d) Other servers: Other origin servers can be connected via the WAP gateway. Other servers located in the internet, may not be able to give as good QoS guarantees as the network operator.

e) Network operator: A network operator knows the latency, reliability, and capacity of its mobile network and can have more control over the behaviour of the services.

f) WTA user agent: The WTA user agent has a very rigid and real-time context management for browsing the web compared to the standard WML user agent.

<u>Interaction between a WTA client, a WTA gateway, a WTA server, the mobile network and a voice box server:</u>

•WTA server to generate new content for pushing to the client.

•The server sends a push message containing a single URL to the client.

•The WTA gateway translates the push URL into a service indication and codes it into a more compact binary form

•The WTA user agent then indicates that new messages are stored.

•If the user wants to listen to the stored messages, he or she can request a list of the messages. This is done with the help of the URL. A WSP get requests the content the URL points to.

•The gateway translates this WSP get into an HTTP get and the server responds with the prepared list of callers.

•After displaying the content, the user can select a voice Powered by TSS message from the list.

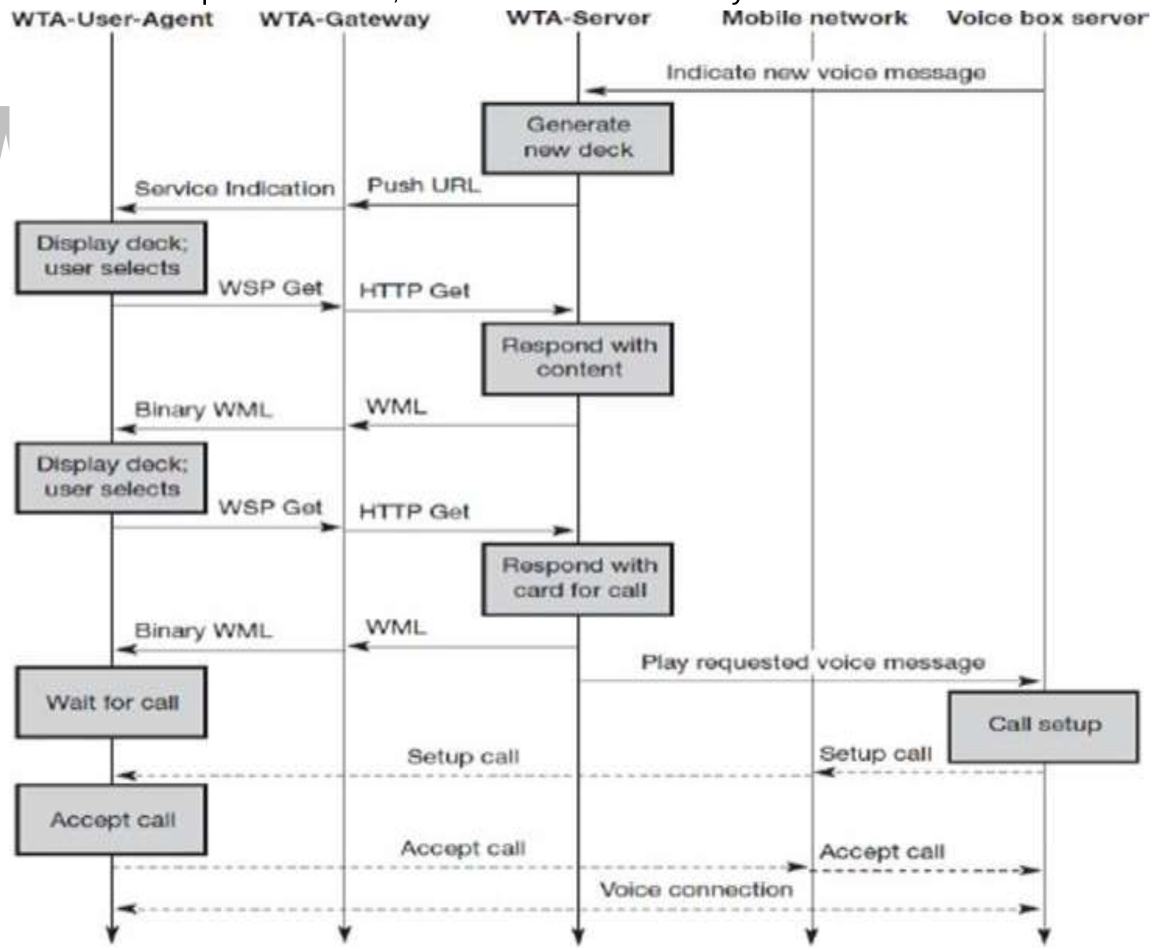
•Each voice message in this example has an associated URL, which can request a certain WML card from the server. The purpose of this card is to prepare the client for an incoming call.

•As soon as the client receives the card, it waits for the incoming call.

•The call is then automatically accepted.

•The WTA server also signals the voice box system to set up a voice connection to play the selected voice message.

•Setting up the call and accepting the call is shown using dashed lines, as these are standard interactions from the mobile phone network, which are not controlled by WAP.



Wireless mark-up language (WML)

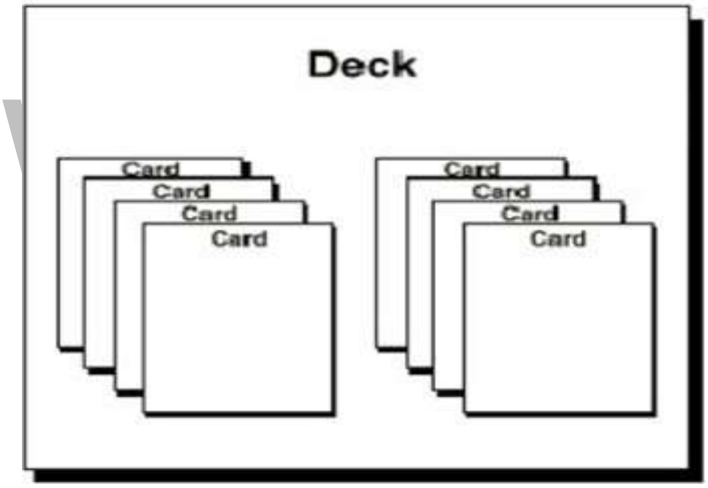
The wireless mark-up language (WML) is based on the standard HTML and on HDML.WML is specified as an XML document type.

•Constraints of wireless handheld devices when designing WML :

- ✓ Wireless link will always have a very limited capacity compared to a wire.
- ✓ Current handheld devices have small displays
- ✓ Limited user input facilities
- ✓ Limited memory
- ✓ Low performance computational resources.

•WML follows a deck and card metaphor. A WML document is made up of multiple cards. Cards can be grouped together into a deck. A WML deck is similar to an HTML page.

•A user navigates with the WML browser through a series of WML cards, reviews the contents, enters requested data, makes choices etc. The WML browser fetches decks as required from origin servers.



•Either these decks can be static files on the server or they can be dynamically generated.

•WML describes the intent of interaction in an abstract manner. The user agent on a handheld device has to decide how to best present all elements of a card.

Features of WML:

Text and images: WML gives hints how text and images can be presented to a user. However, the exact presentation of data to a user is up to the user agent running on the handheld device.

User interaction: WML supports different elements for user input. Examples: text entry controls for text or password entry, option selections or controls for task invocation.

Navigation: WML offers a history mechanism with navigation through the browsing history, hyperlinks and other inter card navigation elements.

Context management: WML allows for saving the state between different decks without server interaction so state can be shared across different decks.

WML	HTML
Mark-up language for wireless communication	Mark-up language for wired communication
Makes use of variables	Does not use of variables
WML script stored in a separate file	JavaScript is embedded in the same HTML file
Images are stores as WBMP(Wireless Bitmap)	Images are stores as GIF, JPEG orPNG
WBMP is a 2 bit image	Size of the images are much larger in HTML
Case sensitive	Not Case sensitive
WML has fewer tags than HTML	HTML has more tags than WML
A set of 'WML cards' make a 'DECK'	A set of 'HTML pages' make a 'SITE'

WMLScript:

•Provides a general scripting capability in the WAP architecture

•Offers several capabilities not supported by WML

Validity check of user input: Before user input is sent to a server, WMLScript can check the validity and save bandwidth and latency in case of an error. Otherwise, the server has to perform all the checks

Access to device facilities: WMLScript offers functions to access hardware components and software functions of the device.

Local user interaction: WMLScript can directly and locally interact with a user, show messages or prompt for input.

Extensions to the device software: With the help of WMLScript a device can be configured and new functionality can be added even after deployment.

CS8601 -MOBILE COMPUTING

UNIT 4

MOBILE TRANSPORT AND APPLICATION LAYER

4.5. Wireless transaction Protocol (WTP)

WTP is on top of either WDP or, if security is required, WTLS.WTP has been designed to run on very thin clients, such as mobile phones.

Advantages of WTP:

- Improved reliability over datagram services
- Improved efficiency over connection-oriented services
- Support for transaction-oriented services such as web browsing.

Three classes of WTP transaction service:

- Class 0 provides unreliable message transfer without any result message.
- Classes 1 provides reliable message transfer without any result message.
- Class 2 provides reliable message transfer with one reliable result message.

WTP achieves reliability using:

- Duplicate removal
- Retransmission
- Acknowledgements
- Unique transaction identifiers.

No class requires any connection set-up or tear-down phase. This avoids unnecessary overhead on the communication link.Allows for

- Asynchronous transactions
- Abort of transactions
- Concatenation of messages
- Report success or failure of reliable messages.

The three service primitives offered by WTP are:

- TR-Invoke - to initiate a newtransaction
- TR-Result - to send back the result of a previously initiated transaction
- TR-Abort - to abort an existing transaction.

Types of WTP PDU:

- ✓ Invoke PDU – used to convey a request from an initiator to a responder
- ✓ ACK PDU – used to acknowledge an Invoke or Result PDU
- ✓ Result PDU – used to convey response of the server to the client
- ✓ Abort PDU – used to abort a transaction
- ✓ Segmented invoke PDU and segmented result PDU used for segmentation and reassembly
- ✓ Negative acknowledgment PDU – used to indicate that some packets did not arrive

WTP Class 0 : Unreliable Message Transfer without result message

- In this class the responder does not ACK & initiator does not perform any retransmission.
- The transaction is stateless and cannot be aborted.
- Requested with TR-Invoke.reqprimitive.
- Parameters are: (SA, SP, DA, DP, A, UD, C=0, H) SA - source address

SP - source port

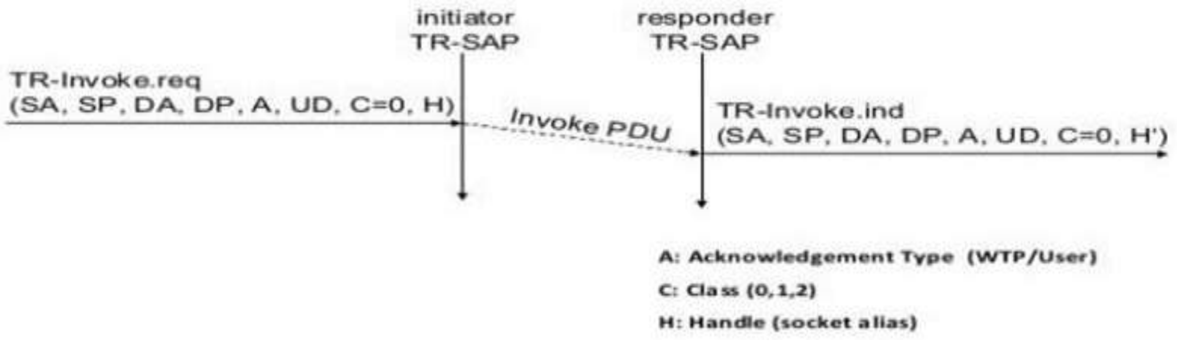
DA - destination address DP - destination port

A - acknowledgement flag, if the responder WTP should generate an ACK or if a user acknowledgement is used.

UD - User data

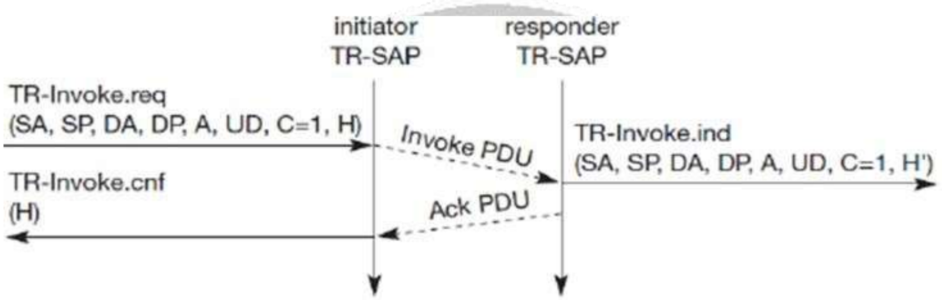
C - class type which is 0 for this class.

H - handle simple index to uniquely identify the transaction

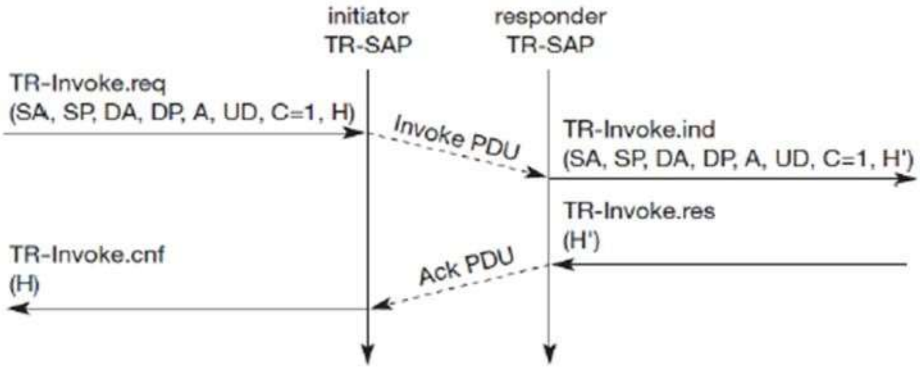


WTP Class 1 : Reliable Message Transfer without result message

- Sender send a TR-Invoke.req
- Parameters are: (SA, SP, DA, A, UD, C=1, H)
- C is class type which is 1 for this class.
- Responder signals the incoming TR-Invoke.ind & ACK automatically
- Sender on receipt of ACK will close the connection.
- Responder maintains the connection for sometime in case it receives the duplicate TR-Invoke.req indicating the loss of ACK.



Basic Transaction, WTP class 1, no user acknowledgement



Basic transaction, WTP class 1, with user acknowledgement

WTP Class 2 : Reliable Message Transfer with one result message

- Reliable request/respond transaction.
- Depending on user requirements, many different scenarios are possible for initiator/responder interaction

WTP class 2 transaction, No user Ack & No hold on:

1. Initiator requests the service using TR-Invoke.req and the WTP entity sends the invoke PDU to the responder.

2. Responder request with the TR-Invoke.ind.

3. The responder sent back the result PDU to the initiator using TR- Result.req.

4. The initiator indicate the successful transmission of the invoke message and the result with the two service primitives:
   - ✓ TR-Invoke.cnf
   - ✓ TR-Result.ind.

5. A user respond with TR-Result.res.

6. An acknowledgement PDU is then generated which finally triggers the TR-Result.cnf primitive on the responder.

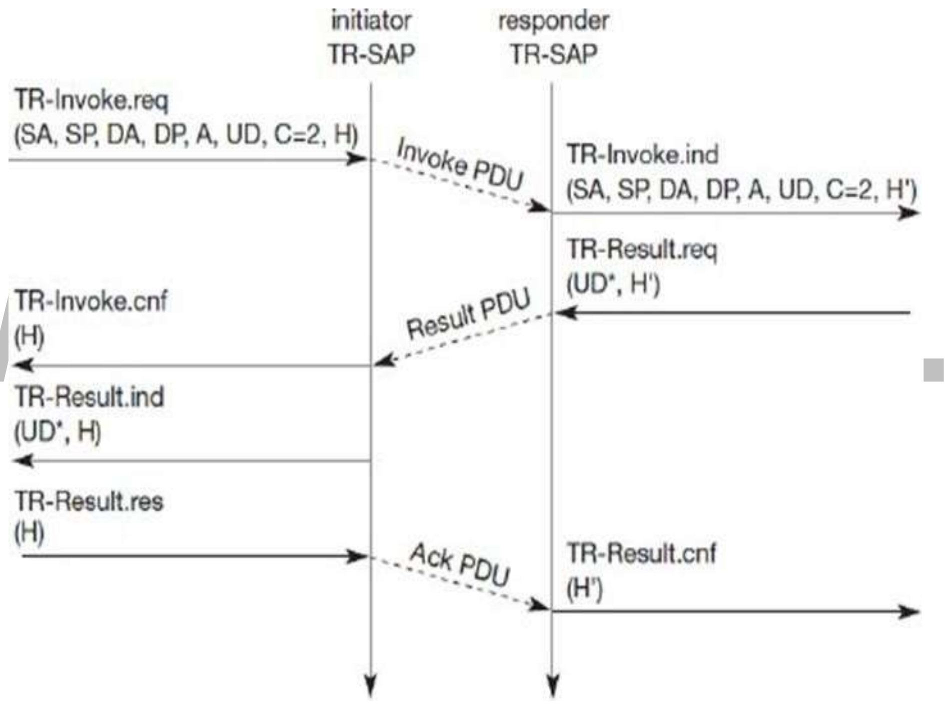
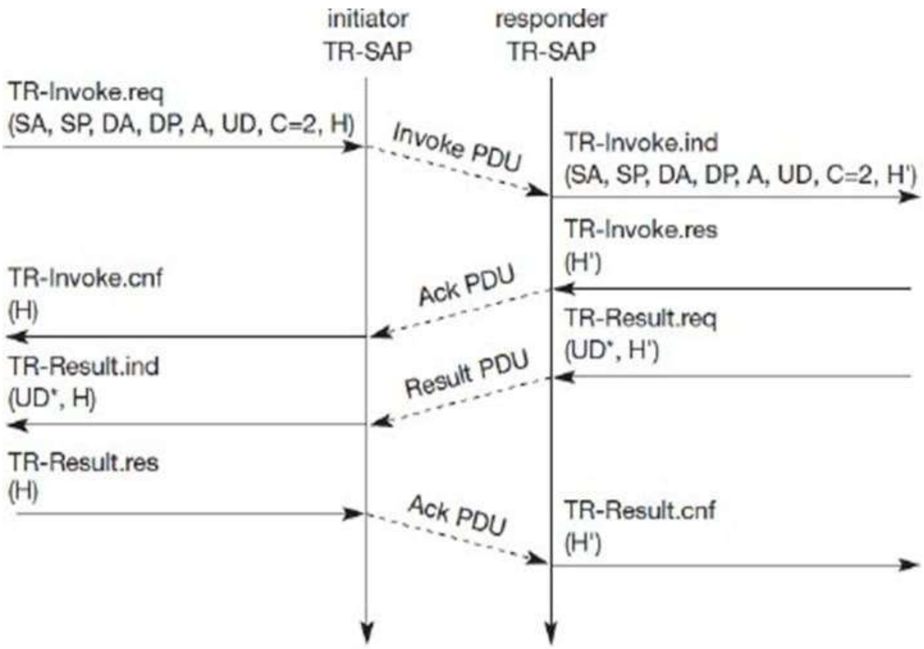


Fig. Basic transaction of class 2 without-user acknowledgement

WTP class 2 transaction, user Ack:

1. The responder explicitly responds to the Invoke PDU using the TR- Invoke.res.

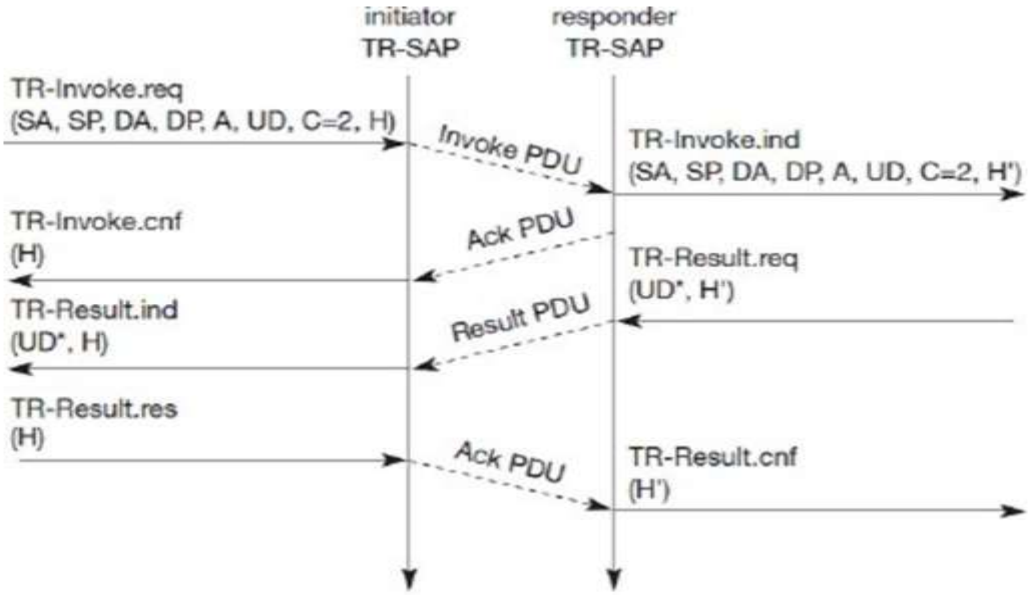
2. Then the initiator triggers the TR-Invoke.cnf via an Ack PDU.



Basic transcation, WTP class2, with user Ack

WTP class 2 transaction, hold on & no user Ack:

If the calculation of the result takes some time, the responder can put the initiator on "hold on" to prevent a retransmission.



WTP class 2 transaction with "hold on", no user Ack

CS8601 -MOBILE COMPUTING

UNIT 4

MOBILE TRANSPORT AND APPLICATION LAYER

4.4. Wireless transport layer security (WTLS)

The wireless transport layer security (WTLS) can be integrated into the WAP architecture on top of WDP. Supports datagram and connection-oriented transport layer protocols. Based on TLS/SSL protocol.

Provide different levels of security for:

- Privacy
- Data integrity
- Authentication

Optimized for low bandwidth, high-delay bearer networks.

Takes into account:

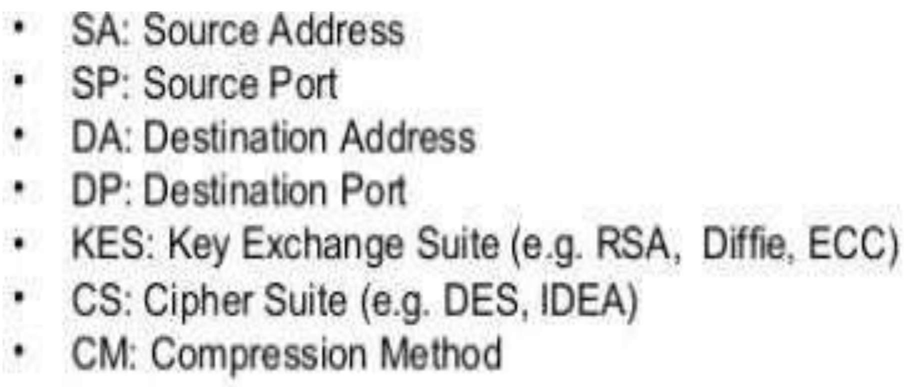
- Low processing power
- Limited memory capacity

Before data can be exchanged via WTLS, a secure session has to be established. Both originator & peer can interrupt the session at any time.

Steps in the Session establishment:

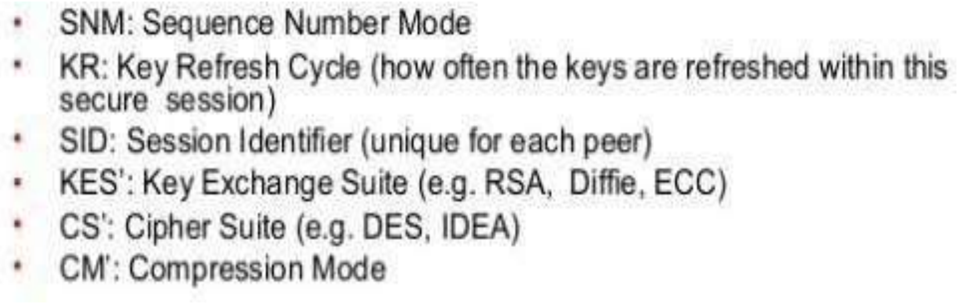
Step 1: Negotiation of the security parameters and suites:

1.1.Initiate the session with the SEC-Create :



- SA: Source Address
- SP: Source Port
- DA: Destination Address
- DP: Destination Port
- KES: Key Exchange Suite (e.g. RSA, Diffie, ECC)
- CS: Cipher Suite (e.g. DES, IDEA)
- CM: Compression Method

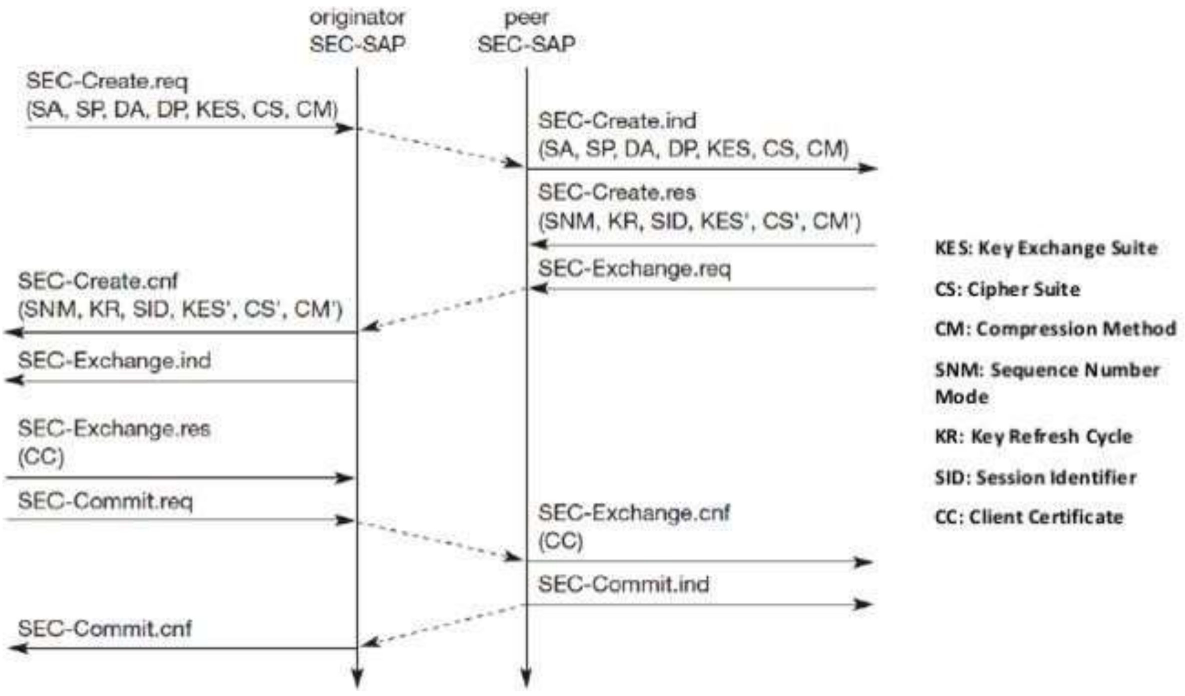
1.2The peer answers with parameters:



- SNM: Sequence Number Mode
- KR: Key Refresh Cycle (how often the keys are refreshed within this secure session)
- SID: Session Identifier (unique for each peer)
- KES': Key Exchange Suite (e.g. RSA, Diffie, ECC)
- CS': Cipher Suite (e.g. DES, IDEA)
- CM': Compression Mode

Step 2: Peer also issues SEC-Exchange:

Indicate that peer wishes to perform public-key authentication i.e., peerrequests a certificate from the originator.



Step 4: SEC-Commit.ind :

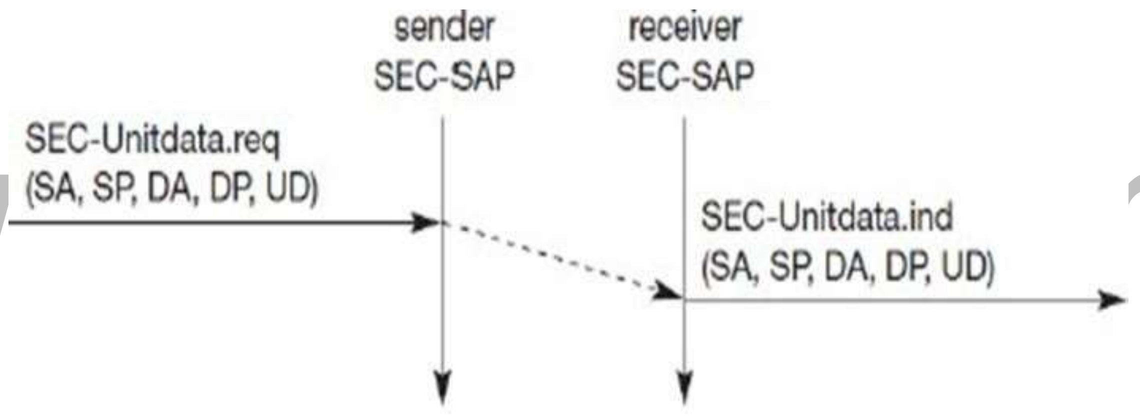
- Indicates that the certificate is delivered
- Concludes the full handshake.

Step 5: User datagram can be exchanged using SEC-Unitdata:

- Same function as T-DUnitdata on the WDP layer

The parameters are the same here:

source address (SA), source port (SP), destination address (DA), destination port (DP), and user data (UD)



WTLS datagram transfer