01/01/2022

Mobile computing

① Mobile Communication – Jochen Schiller Pearson Educat^n
② Wireless communication & Nlw's – William Stallings, 2nd Ed^n
③ Mobile Computing – Raj Kamal, Oxford University Press.

Ref:

PDA - Personal Digital Assistant
ubiquity - being very common
nomadic - wandering.
pervasive - spreading widely throughout an area or a group of people
AMPS - Advanced Mobile Phone System
GSM - Global system for Mobile
CDMA - Code Division Multiple Access
RTT - Round - Trip Time.
GPRS - General Packet Radio Service
EDGE - Enhanced Data Rate for GSM Evolution
PSK - Phase Shift Keying
IMT - International Mobile Telecommunications
ITU - International Telecomm^n Unit
TDMA - Time Division Multiple Access.
PSTN - Public Switch Telephone nlw.

classmate

08/02/22

(Circuit switch (call) & pkt switch (data) nlw)

UMTS - Universal Mobile Telecomm^n System (3G)

UTRAN - UMTS Terrestrial Radio Access nlw
Brain of UMTS

UMTS = UTRAN + (core Nlw (CMAP) + Authenticat^n of user via SIM.

CN - core nlw.

tx 42Mbps data

- 3GPP (3rd Generation Partnership Project)
- WCDMA (wideband CDMA) when voice call is connected it enhances (spreads) the frequency of it because of which call gets easily setup & connected
- In this, the air interfaces are known as UTRAN.

Diag:

- UE: User interface also user (USIM) SIM. called user equipment. ME - mobile equipment
- NodeB - BTS or base station
- RNC - Radio nlw controller (BSC or MSC)
- when mobile stat^n initiates the call, the NodeB which is antenna catches the signal & tx to RNC
- RNC is kind of device that maintains all the ~~sce~~ sceneris or f^{n}s of user equipment or antenna.
- one Radio nlw controller (RNC) connects to to other RNC via Iur interface

classmate

I_u = A interface.

- RNC will analyse that the signal is of what type whether a voice call or data transfer. & based on it it distributes it.
  - i. If it is a call signal then it connects to MSC/ VLR (ckt switch)
  - ii. If it is a data signal then it connects to SGSN (pkt switch) & then to PDN (pkt data nlw) via SGSN & GGSN support node
- Next it sends signals to the external PSTN nlws.

UTRAN:

- This consists of several radio nlw subsys (RNS)
- Each RNS is controlled by a radio nlw controller (RNC) & comprises several components that are called Node B. is similar to a BTS
- Each node B can control several antennas which make a radio cell.
- This comm^n nlw, commonly reffered to as 3G can carry many traffic types from real-time ckt switched to IP based Pckt switched

* Mobile IP:

Care of Address: Mobile Node's current loctn in foreign nlw.

* Mobile IP Working:

1. Agent Discovery: Home Agents or Foreign agents usko discover karna ki where it is.

- HA with home nlw; FA with foreign nlw.
- when MN is connected to HNlw or a new device which is introducely newly in the nlw. It should know which router is resp for that nlw - Home Agent is therouter which is associated with home nlw.
- Through advertisement from HA to all the nodes in that nlw.
- MN learns from this advertisment because HA is connected to Internet.
- If any data packets are coming for MN or if I have to send any data to other nlw so HA will do it for me.
- If MN moves to some other nlw it should know its COA.
- For that even FA does the same thing of advertisement.
- with this the mobile nodes gets to know that the router is there to help the MN.

- So MNs try to discover the ~~router~~ agents. which is assigned with that nlw. & whatever advertisements are done by agents, the mobile nodes are learning from it

2. Registration: If your MN moves from one nlw to foreign nlw so its current COA has to be known to home nlw & to foreign nlw's router.
- HA has to know that MN, which was belonging to my nlw, now its current location is what.
- And FA who is totally unaware of this new node has to also know about its current loct^n.
- HA & FA has to know current loct^n of MN,
- so MN, has to register itself.
- Firstly, MN, has reached F nlw ; FA agent discover kartay ; when FA advertises itself that time MN, will get to know that this is F nlw to him because the advertisement is of FA, not my HA adver.
- MN, has IP address which is unique, security keys which was unique which

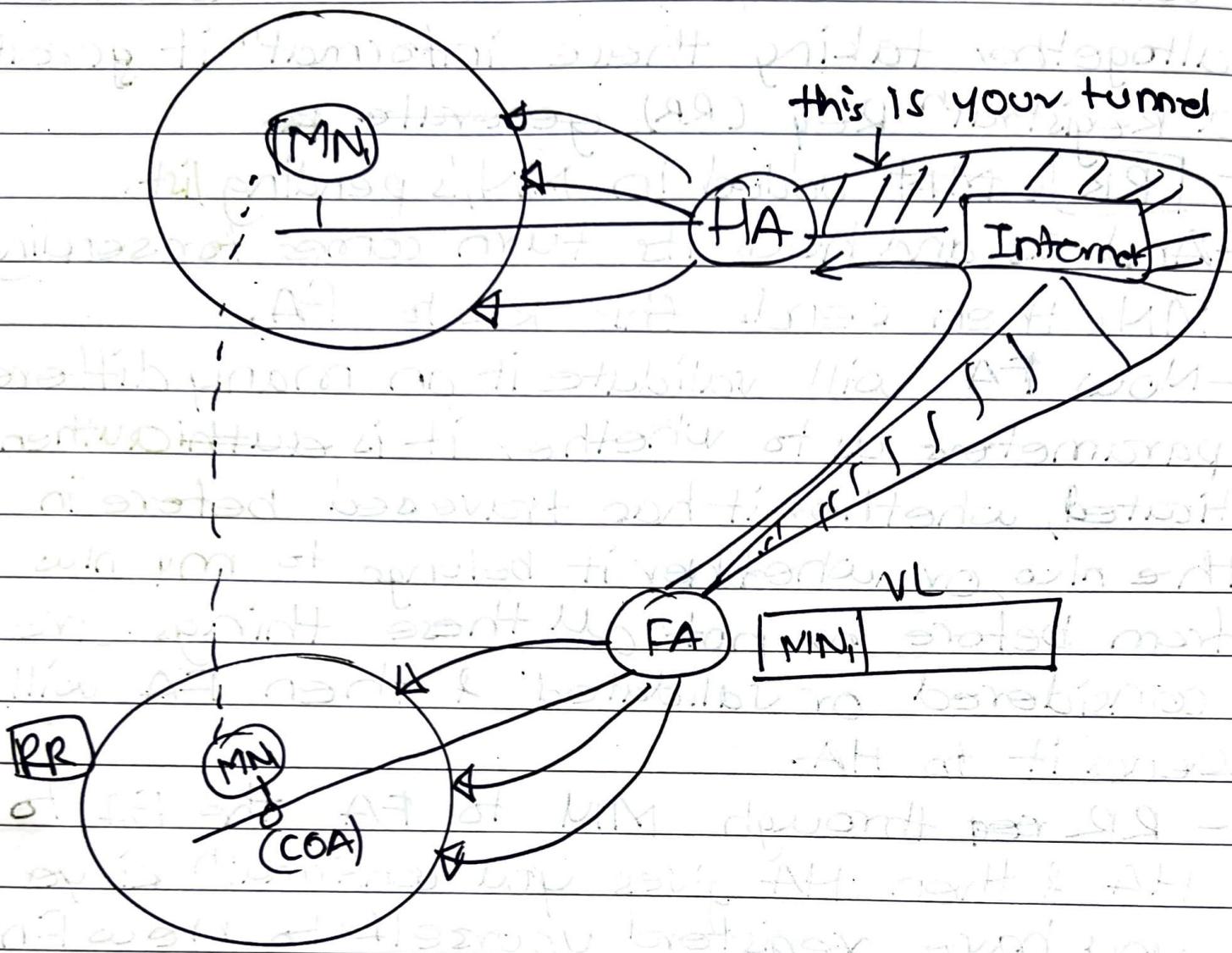
was being used to authenticate itself so these unique keys & IP address together with what he learnt from FA's advertisement altogether taking these informath it creates a Registrath Req (RR). ~~generate~~

- RR is ~~MN~~ added in MN,'s pending list.
- And as and how its turn comes for sending MN, then sends this RR to FA.
- Now FA will validate it on many different parameters as to whether it is ~~authi~~ authenticated, whether it has traversed before in the nlw, or whether it belongs to my nlw from before or not. all these things are considered or validated & then FA will send it to HA.
- RR ~~req~~ through MN to FA the FA to HA & then HA gives you confirmath ki yes you have registerd yourself to new Fnlw ~~HA & FA~~ have received your COA ~~to HA & FA.~~
- As soon as FA gives RR to HA now HA plays an imp ~~to~~ task - HA will ~~to~~ validate MN, saying it from ~~my~~ my nlw & decides to register it, COA ko register kartey.
- And after registering it, after validating it

classmate

- HA does 2 things (very imp)

i. It creats a tunnel to COA



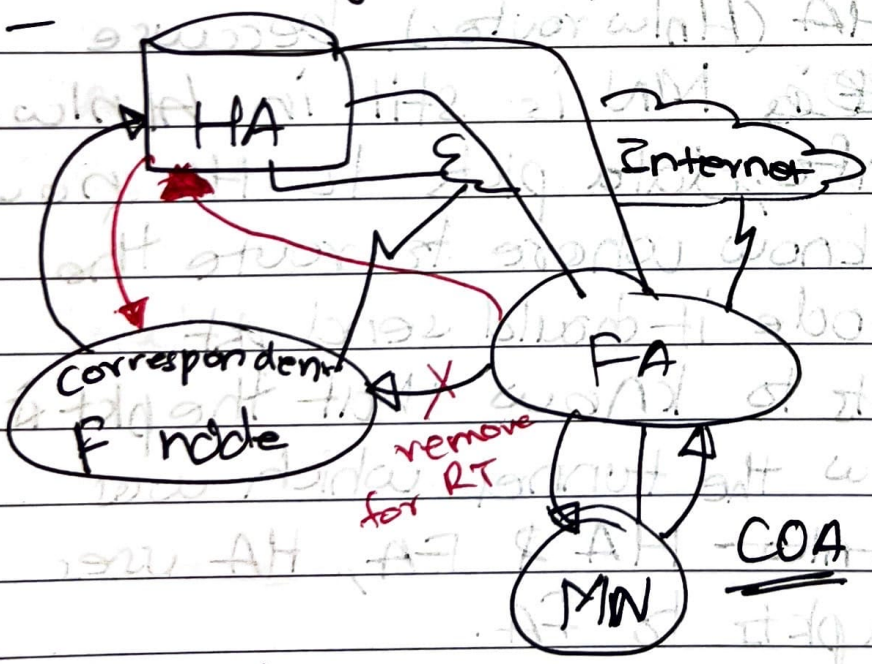
ii. Mobility binding (associatn of mobile node with its COA).

- MN, ko iski khud ki jo COA hai usko bond karnay. associate karnay.
- HA now sends reply to FA saying yes MN, is of my nlw it went in your nlw by mistake now you add it in your visitors list

classmate

- Now FA will validate that reply by seeing that the req sent to that particular HA is the same one replying to the req. If so its valid
- Now MN_i is added to FA's VL $[MN_i]$
- Now finally FA will reply to MN_i (a response that, reply that who) MN_i will now understand that ther regist^n ki req which I had initiated is successful.
- MN_i has to be re-registed before its registrath life-time finishes.
- reregister.

3. Tunneling: 2 things to remember : pckt lvod disadvantages of pckt lvod gives reverse tunnel



- Now we had already registered nodes to the nlw.

classmate

- Now for eg: corresponden nodes (the node which belongs to 3rd nlw)
- HA Hnlw kaa router HA. F nlw kaa router FA & MN has traversed to Fnlw
- Now MN has done agent discovery, registratn. now both HA & FA is known that it is in Fnlw. & current locth is COA.
- Now correspondent node is the one not belonging to Hnlw nor Fnlw its belonging to some 3rd nlw.
- now CN wants to send some data to MN.
- CN doesn't know that MN has traversed to Fnlw so CN will send data pkts to HA (Hnlw router) because CN feels that MN is still in Hnlw.
- CN sends all info, data pkts to HA now HA will get to know where to route the pck, to which node it should send pkt
- so now HA gets to know that the pkt is for MN so now the tunnel which was created btwn Hnlw HA & FA, HA uses it to send data pkts to FA.
- Now HA firstly encapsulates all the data pkts.

classmate

- The functionality of tunnel is to :
i. encapsulate - start mein encapsulate karnay
ii. decapsulate - other end mein deappsulate karnay.
- & now FA will send it to MN. will have original data it
- Now MN has to give response to ~~FA~~ CN so it will respond it through FA & then FA sends the reply directly to ~~to~~ CN.
- This is part fwding.
- But problem is that if CN has sent data to one particular node & if it is waiting for response, it will wait for response from the one who has sent it.
- so CN is expecting the response from HA & not FA
- so CN discards FA's responses at times.
- So to overcome this reverse tunneling is used.
- In red in diagram chaning arrows.
- Now FA sends response to HA & then HA sends response to correspondent node.

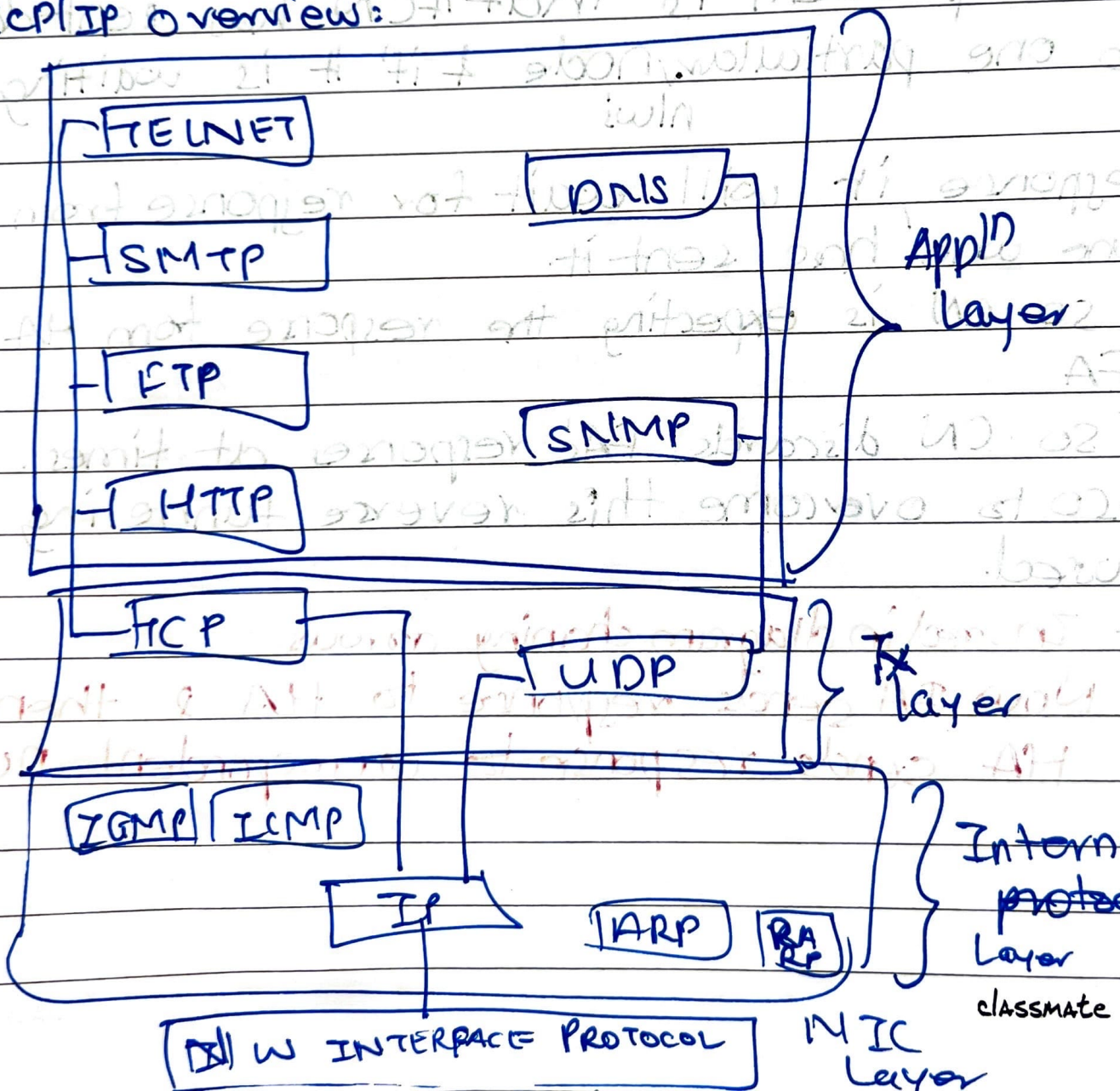
classmate

07/03/22

* Mobile TCP:
  - Traditional TCP
  - Classical TCP improvements like Indirect TCP
  - Snooping TCP & Mobile TCP
  - Fast Retransmit / Fast Recovery
  - Transmission / Timeout Freezing,
  - Selective Retransmission.

* Mobile Transport Layer:

TCP/IP overview:



classmate

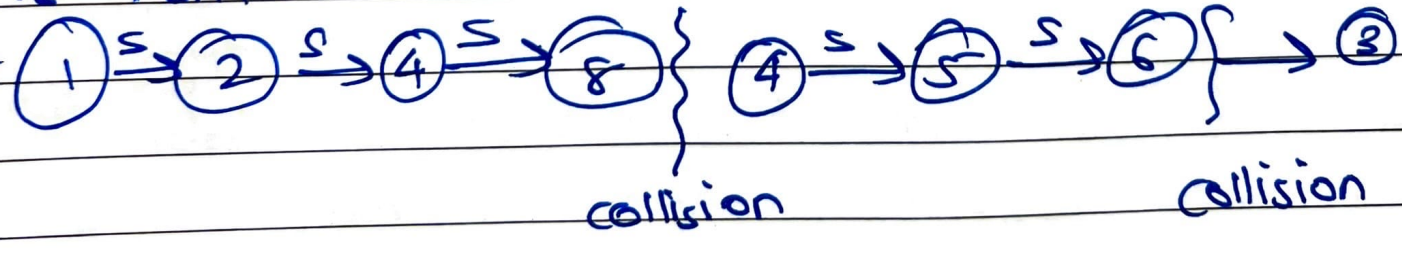
- 4 different layers in this archi.
- It is a collectⁿ of large no. of protocols which helps in data commⁿ, pckt tx
  - TCP → Transmission control protocol.
  - IP → Internet protocol.

i. slow start.

Traditional TCP: It is used when TCP session is started.

- Tx is started at lowest window size & then doubled after each successful tx.
- If congestion is there, (duplicate ack), tx window size is reduced to half

ii. Congestion Avoidance: After slow start, if collision is detected window size is halfed. Then after receiving of "ACK" window size is increased linearly instead of doubling.
- Again if collision is detected, window size is halfed.

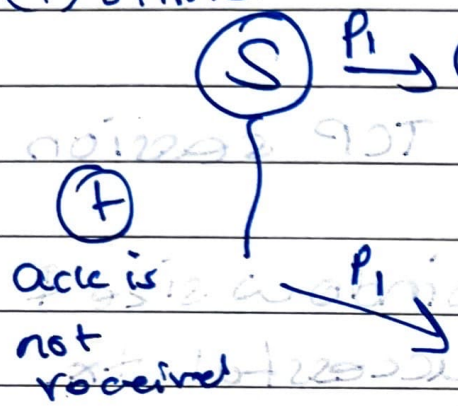


iii. Fast Retransmit / Fast Recovery:

-Retransmission is not triggered by time

-If three (03) duplicate copies of the Ack for a pkt received from sender

(t) → timer



it is taken as missed pkt & retransmission starts.

↓

window size is reduced by half if pkt loss.

63rd slide

- TCP - connectn oriented & not transactn oriented
- nlw friendly - timeout
  If any congestion has occured in nlw, it is going to slow down the transmission.
- eg: HTTP 3-way handshake.
- commn will establish & ~~commn will~~ data tx is taking place below 15s no data avlb to connectn released.
- wireless & mobile nlw the server performance will be degraded.

65nd slide (Motivation).

- Transport protocols typically designed for
- fixed end systems.
- fixed wired nlws.
- For mobile systems it should be wireless & the research activities are performance, congestion control & efficient retrans.

~~66th~~ 66th slide (classical TCP improvements)

- How TCP can be improved in wireless environment.
- Improve TCP performance in .. & mobile environment

classmate

1- Indirect TCP:

- There is no change to the TCP protocol for connected hosts. (wired nlw).
- to optimize TCP protocol for mobile host, split the TCP connection eg the foreign agent into 2 TCP connectn (for wired & one for wireless).
- Fixed host (HA) doesn't know what type of wireless is to participate in the nlw. so it does not notice the characteristic of wireless part because it is connected via wired internet to FA (access pt).
- FA is access pt to mobile host & fixed host (HA)
- TCP is divided into 2 std is connected to fixed host & mobile host & access pt will be connected by wireless TCP.

7th slide:

- eg: Socket & state migratn after handover of a mobile host
- If access pt is not accessing to mobile host, reaching to the mobile host there is a chance to handover of a mobile host means the state migration of a mobile host after handover of a MH. so MH is handover to another access pt

classmate

- Diagram:

Access pt 2 → FA old

The access pt 2 is not reaching to MH then there is chance that you can migrate to another access pt (access pt 1 new).

- socket & state migiat^n after handover of MH
- access pt is socket it is changed & the state is going to get transfered to the mobile host.

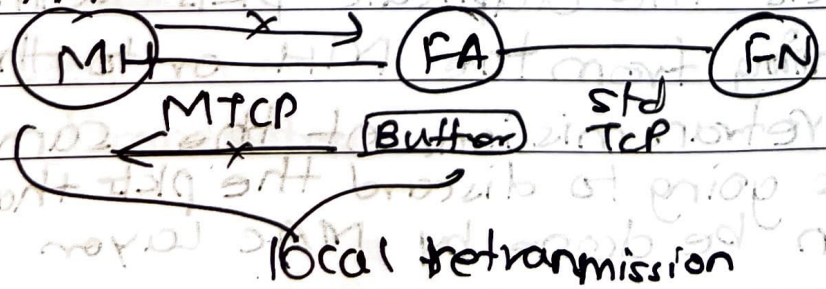
- 8th slide:

Adv: Disadv.

~~9th~~ 72nd slide

2. Snooping TCP:

- FA is holding the buffering of pkts send to the mobile host one by one
- suppose if last packet on the wireless link ie in both directions will be retransmitted immediately by the MH or FA resp. so called local retransmission is there in MH & FA

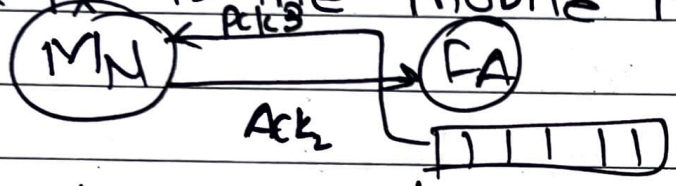


classmate

- The FA ∴ "snoops" the pkt flow & recog acks in both direction, it also filters ACK.
- changes of TCP is only within the FA.
- 74th slide.
eg: Snooping TCP as a transparent TCP ext?
ii → from the MH.
i. ← to the MH

→ Data Tx in case of snooping.

i. Data Tx to the mobile host



Ack 2 is received even if pkt 3 is sent. this is pckt loss

ii. Data Tx from the MH.
- FA sends negative pck NACK saying that FA is getting duplicate Ack
- within a short delay the MN sends the data

75th slide

- MAC layer.

It detects the duplicate pkts which are coming from the MH or to the MH due to retransmissions of the same seq no & it is going to discard the pkts that classmate work can be done by MAC layer

Problems in snooping

11th slide 76th slide.

Mobile TCP:

- Main use of mobile TCP is handling of lengthy and/or frequent disconnections.
- M-TCP is split as same as I-TCP does:
  i. unmodified TCP fixed nlw to supervisory host (SH) — FN
  ii. optimized TCP SH to MH.
  MH — SH
- SH has no caching, no retransmission only supervise
- SH monitors all pckts if disconnect^n detected. & after that it sets sender window size to 0. & sender automatically goes in persistent mode
- Supervisory Host same as FA in snooping.
- Assumes low bit error rate on the wireless link.
- It will see whether proper comm^n is going on btwn std host & mobile host or not.
- Ack is sent from MH to 2nd Host but through supervisory Host (SH)
- SH checks it & fwds it
- If SH doesn't receive Ack from MH so he thinks MH is disconnected

classmate

- It wont receive pkts so the SH tells or forcefully makes std hosts window size to 0.
- So then std host stops pkt fwding
- so then sender goes in persistent mode forcefully
- Std Host keeps itself on the state it closes itself.
- MH is not sending Ack. so the retrans is done by std host ie the sender
- std host size is 0; SH will wait.
- when SH sees that the connectn is established from MH. ~~SH~~ std host window size is now restarted from the window size if went to 0.

Fast retransmit / Fast recovery:

- There is change in FA due to its failure or not receiving signals or any other issues within the same nlw we can migrate it to any other FA & the connects can be established btwn the MH & the FA by new FA.
- Change of FA often results in pkt loss.
-

802.11 architecture. (207)

WEP (Wired Equivalent Privacy Protocol) Protocol
- Security for wired systems
- It is nlw protocol that adds security to wifi systems & other 802.11 wireless nlws. ie. for WLAN systems.
- It provides privacy to systems which is equivalent to wired. like cable or ethernet
- Provides data encryption & integrity protection for 802.11 std.
- Confidientiality Integrity & Authentication
- Aims to protect link-level data during wireless tx means all the data which is transported at secondary layer ie data link layer whether its frame structure or frame bits it complies to that kind of security.
- WEP clients share a secret key called WEP keys which are used by them for authentication & encryption & decrypt of msg
- WEP key needs to be updated & stored in clients & can be cracked easily by WEP 802.11x called as dynamic WEP which exploits weakness of static WEP.

classmate

- 2 types of WEP < static (can be easily cracked with dynamic)
dynamic

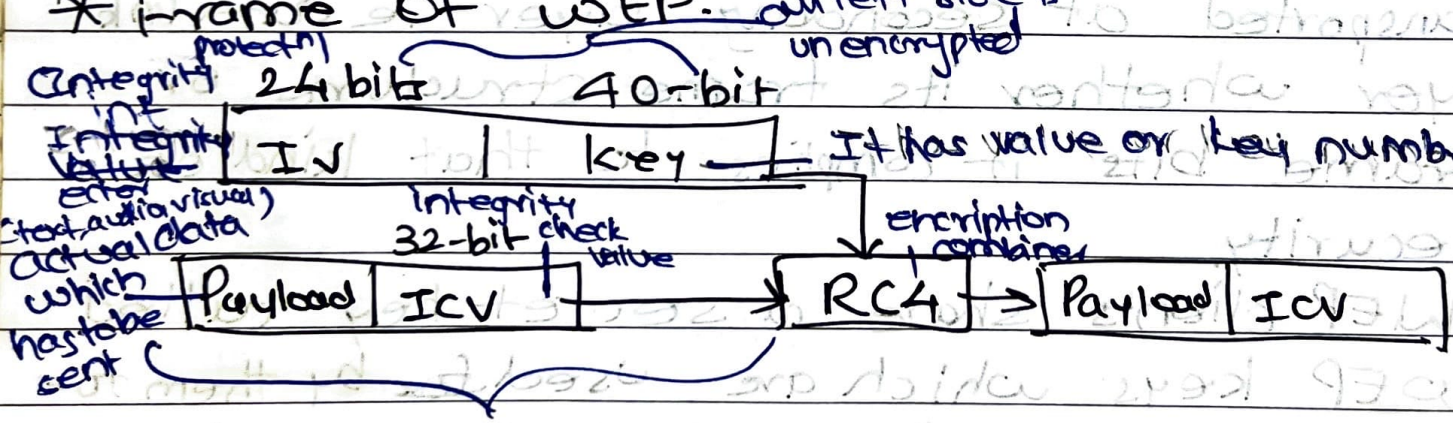
* Working

① Data encryption scheme where user values + system generated values are combined & applied to the algo RC4 (Rivest cipher) is there & through that its being generated

② Original implementation of WEP supported encryption of (40+24) bits (user + system) of system data of total 64 bits.

- To increase protection longer keys were developed of 128, 152 & 256 bits.

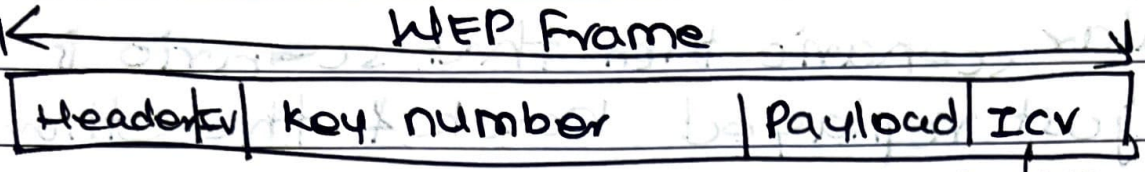
* Frame of WEP.



- left side of RC4 is unencrypted so IV + key just forms a layer on top of the actual data
- so at the o/p you have just the payload + ICV value which is encrypted

classmate

- Now this encrypted value is attached to set of 3 headers:



i. Header - version number of WEP frame. other basic details regarding that WEP frame

ii. IV - Integrity value - Integrity check being done & no. of times it is being versioned.

iii. Keynumber - The key which is being used in series so it is chronological order where you get the key no & then you have payload & ICV which was encrypted above

Flaws: It fails to check on certain param.
- Does not ~~allow~~ prevent forgery of pkts. forgery of pkts happen. does not do any kind of validtn over the pkts; it just accepts the pkts & sends to the end syst so at other ent there is attacker being present & if its ~~being~~ with evil intention then its not possible to identify with the help of WEP & the sender will get compromis

2 Does not prevent replay attack
- Replay attack is first you record a particular scenario then that scenario is being just replayed back & the other system will be under the impression that its being coming from a valid legitimate system so those kind of checks are not done in this
3. RC4 used is vulnerable & so its done under improper implementations.
4. Lacks key mgmt - since all the keys are shared among different WEP clients & there is no proper or poor updtn.

- As of now WEP is replaced in 2004 by Wifi - Protected Access (WPA) & supplanted by WPA2

WPA2 PSK - Phase shift keying

~~Wireless Appl^n Protocol~~

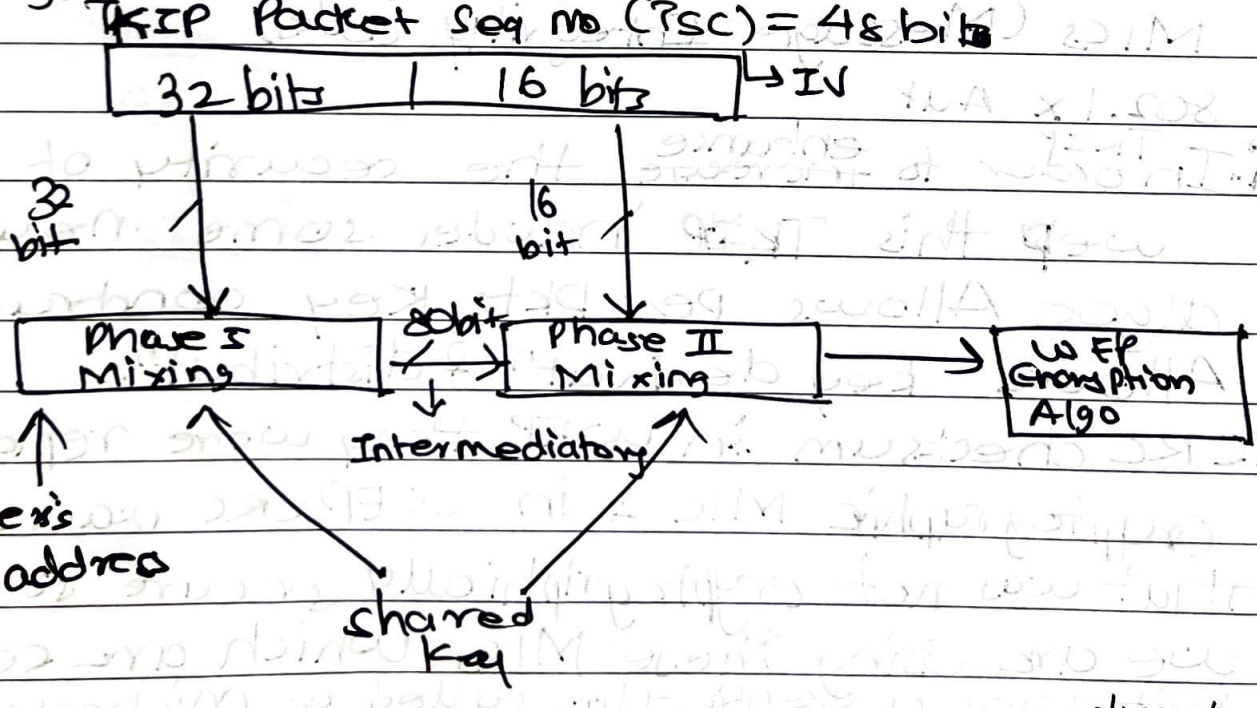
WPA (WiFi Protected Access)

- To overcome the vulnerabilities of WEP, sw patches were developed as an interim std.
- Fast pkt keying.
- Hashing technique is used to generate per pkt keying.
- Each new pkt is encrypted using a unique key.
- It was given by WiFi Alliance ing 2002-03
- Not required a hw upgradtn in existing 802.11 equipment
- TKIP (Temporal key Integrity Protocol)
  MICs (Message Integrity codes)
  802.1x Aut
- In order to enhance the security of wep this TKIP includes some new algos. Allows per pkt key construct^n. Allows key derivat^n & distribut^n.
- CRC checksum in WEP they were replaced by cryptographic MIC & in WEP CRC was used that was not cryptographically secure so here we are using these MICs which are secure & it uses a specific algo called as Michael Algorithm to compute the MICs & it used to detect msg forgery

attack

iii. It provides port ways authentictn & that why it has port based access ctrl that allows a frame to allow user of robust upper layer authentication protocol & also it facilititates use of session keys.

* Temporal key Integrity Protocol (TKIP)
- slw enhancement on WEP protocol & works on same hlw or backward compatibility with the WEP devices.
- It is based on RC4 algo stream cipher but it uses 48-bit Initilizat° vector & 64 bit authenticat° key & 128 bit encryption key.



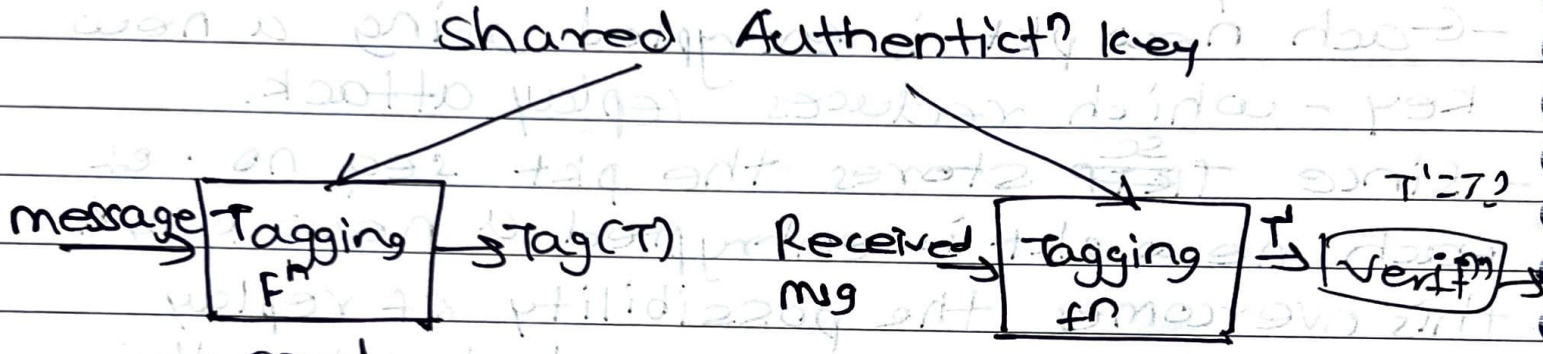
classmate

- The encryption keys are generated from the combinat^{n} of shared keys, sender's MAC addr & pkt sequence number.
- 2 Mixing phases I & II
- Mixing involve XOR & AND Op^{n} to generate the keys.
- Each new pkt is encrypted using a new key - which reduces replay attack.
- Since TSC stores the pkt seq no. of each new pkt is encrypted a new key & this overcomes the possibility of replay attack however we need to sinc the sender & receiver the received pkt should have seq no. greater than the previously received pkt.
- Using MAC address in generat^{n} of keys guarantees every station & AP pair will generate a different set of encryption keys.
- Because of breaking of MIXING Op^{n} & TSC into 2 parts, there is no direct relat^{n}ship btwn IV & encryption keys. If somehow attacker gets the IV during the comm^{n} it is not going to provide any extra info to attacker.

classmate

- Thus sending TSC in clear does not give any extra info to attacker.

* Message Integrity Code (MIC)
- We are sending cryptographically secure checksum.
-



- If same accept the msg or reject
- The msg ~~msg~~ is partitioned into 32 bit chunks & 0's are padded.
- ↓go by no. of iterations & in each iterat^n or in each step one chunk is mixed with key using XORs, Bit-wise swaps & additions.
- The o/p of each step or iterat^n is 64 bit o/p & treated as MIC
- This defeats forgery attacks.

* IEEE 802.1x
- Port based nlw access ctrl protocol
- used to achieve mutual authentn.
- Efficient key exchange is provided by port based access ctrl protocol.
- Based on 3 nlw elements:
1. Suppli'cant - In a wireless nlw supplicant is the wireless stn. / wireless device that we are using to access the wireless nlw.
2. Authenticator - A value which is hash mic or checksum. It is used to authenticate ~~the~~ our entity / msg.
3. Authentn server = nlw access node it can be AP & this allows to access the nlw ~~by~~ exchanging certain parameters
- Any server with authentication mechanism.

classmate

* Threats:
1. wardriving 2. Eavesdropping
3. Rogue APs 4. Denial of service

1. wardriving: Term used to describe someone who uses a laptop & a wireless NIC to look for wireless nlws.
- It uses GPS device to record the loc^{n}, & a discovery tool such as Netstumbler

2. ~~Re~~

3. Fakes AP. & user gets connected to it.

4. DoS - when collision occurs in the nlw new pkts are denied the access of the nlw.
The amt of traffic reqd to affect a target device can be much higher than the capabilities of a single m/c.

28/03/21

MC.

~~Optimization:~~

* Functions of Mobility Management:

1. Locatⁿ Mgmt: Identifying the physical loctⁿ of the user so that calls directed to that user can be routed to that locatⁿ.
2. Call routing: Setting up a route through the nlw over which data is directed to particular user.

Mobility Mgmt categorized as:

Handover Mgmt < Intra cell / Inter cell

Location Mgmt - current loctⁿ of mobile user for call delivery.

* Optimizations:

- Triangular routing: CN - HA, HA - COA/MN, MN -
- optimizations of the route can be obtained by conveying the current locatⁿ of MN to CN.
- CN can learn the locatⁿ by caching it in a binding cache.
- The " " is a part of local routing table for the CN.
- It needs 4 additional protocols.

1. Binding req: Any node that wants to know the current loctⁿ of a MN can send the binding req to HA. The HA can check if MN has allowed dissemination of its current loctⁿ

classmate

- If the HA is allowed to reveal the loc? it sends back a binding update.

2. Binding Update: The current loc? of the MN is revealed by the message sent by HA to CN.
- The msg contains the fixed IP address of the MN & the CoA. The binding update can req an ack.

3. Binding Ack: A node returns this ack after receiving a binding update msg if requested.

4. Binding warning: when the node decapsulates a pkt for an MN, but it is not the current FA for this MN, this node sends a binding warning.
- The recipient of the warning can be HA. Hence HA can send a binding update to the node that has a wrong CoA for the MN.

* CN $\xrightarrow{\text{loc?n req}}$ HA
HA $\xrightarrow{\text{CoA via msg}}$ update
CN $\xrightarrow{\text{Ack}}$ stores the mobility binding
CN can send data directly to FAold & then to MN.

Hence CN encapsulates the data pkts for tunnelling purpose & not the HA

classmate

- MN changes loctn & registers with FA_{new}
- forwarded to HA to update its loctn.
- FA_{new} conveys to FA_{old} regarding the new registratn of MN. Registratn msg contains the addr of FA_{old}
- CN is not aware of this. & ~~sends~~ keeps tunnelling the pkt to FA_{old}
- FA_{old} fwds pkts to new coa, FA_{new}
- smooth handovers, provides optimizations.