EVOLVING INTERNET

2020/2021

17/09

MOBILE IP PROTOCOL (DIRECT/INDIRECT ROUTING)

ISSUE WITH MOBILITY ?

! IP vs ID

WHAT'S MOBILITY? → When you change GATEWAY or IP

(1) FIND SOMEONE

- IP is a LOCATOR → used to send packet to you
- ID is a IDENTIFICATOR → used to find you

- ~~DNS~~ → way of giving an <IP,ID> tuple to you, the issue is that does not scale, is fixed

(2) MANTAIN CONNECTION

- IP == ID
- You cannot maintain a connection while moving, TCP/UDP protocols open an END to END connection

---

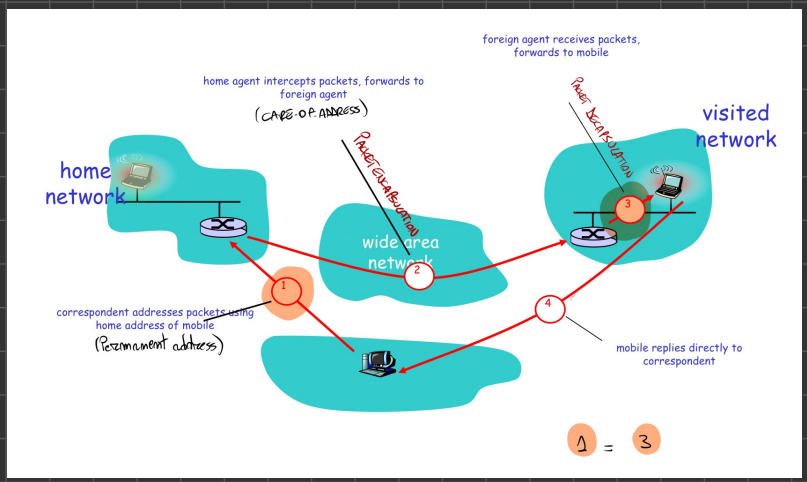
MOBILITY APPROACHES

(1) change routing => Not scalable (PERMANENT IP for every device)

↳ used in JAPAN to handle INFRASTRUCTURE FAILURE for EARTHQUAKE

(2) let end point handle it : DIRECT AND INDIRECT ROUTING

- INDIRECT ROUTING



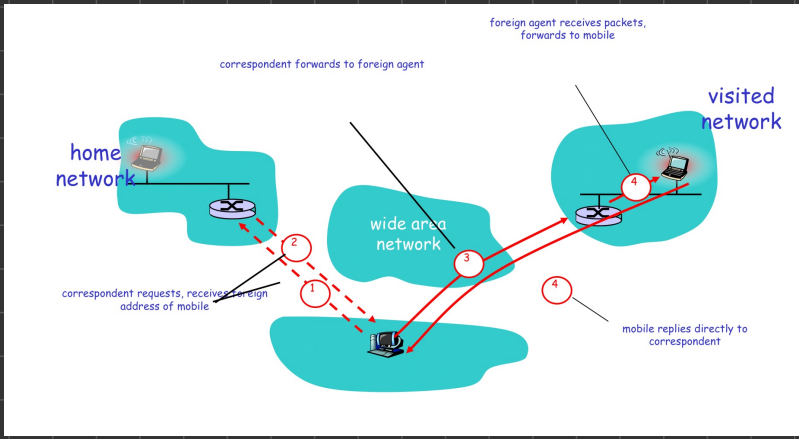
PRIVACY ADVANTAGE

- The sender, in this way, knows only your HOME ADDRESS

BUT

- WORST CASE: given d the diameter of the network
  - In INDIRECT ROUTING is 4d (if you are in the same position of the sender)
  - In DIRECT ROUTING the longest distance is 2d

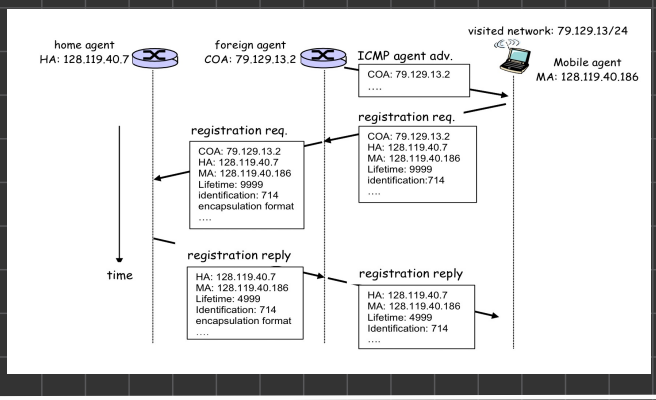
- DIRECT ROUTING



- in ③ there is a legal IP SPOOFING
- not the PRIVACY of indirect routing

NOTE

ICMP SIGNALING IN MOBILE (registering to a foreign network)



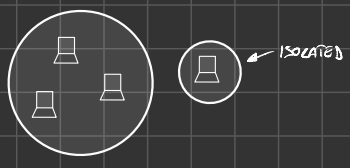
WIRLESS NETWORKING

NOTE

- The END TO END PRINCIPLE says that routers don't store packets

Scenarios

- INFRASTRUCTURE BASED
  - ALL traffic pass through the network infrastructure, providing services as ROUTING, DNS, ...
- AD HOC
  - No ROUTING, packets travels directly from node to node



SINGLE VS MULTI HOP

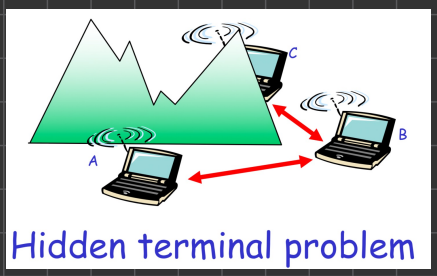
	Infrastructure-based	Infrastructure-less
Single hop	Base station connected to larger wired network (e.g., WiFi wireless LAN, and cellular telephony networks)	No wired network; one node coordinates the transmissions of the others (e.g., Bluetooth, and ad hoc 802.11)
Multi-hop	Base station exists, but some nodes must relay through other nodes (e.g., wireless sensor networks, and wireless mesh networks)	No base station exists, and some nodes must relay through others (e.g., mobile ad hoc networks, like vehicular ad hoc networks)

ISSUES WITH WIRELESS LINKS

- Signal can decrease NATURALLY or by INTERFERENCES
- Multipath propagation: signal reflects on objects, ground etc...

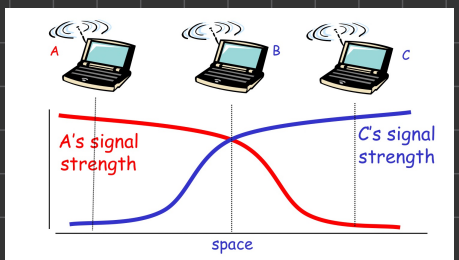
Does CSMA works for wifi?

CSMA is "sense before transmit" (COLLISION AVOIDANCE)



Hidden terminal problem

- CSMA not work because A is aware if C is already communicating with B



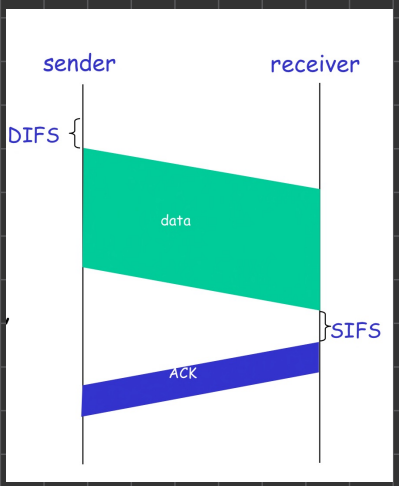
Signal fading:

- A cannot sense if C is transmitting because of the signal fading

IEEE 802.11 MAC PROTOCOL

CSMA/CA

- We can use CSMA/CA, PROTOCOL for COLLISION AVOIDANCE (but not detection)
  - → DIFS: wait time to check if there are connection
  - → SIFS: same as DIFS but shorter
  - → sender wait for Ack, if it don't receive there is a COLLISION

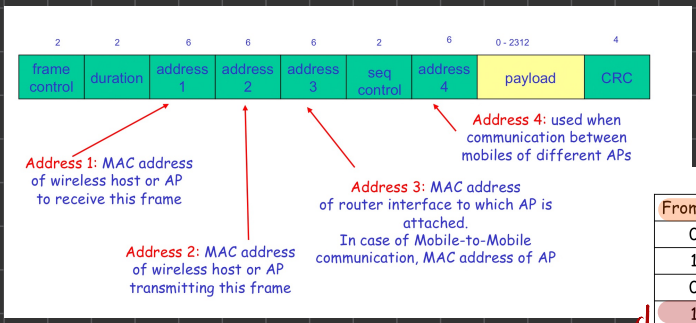


NOTE

- To avoid loss of big packet we can use 2 small one: REQUEST-TO-SEND (RTS) and a CLEAR-TO-SEND (CTS). CTS is broadcasted from the receiver of the RTS
- If RTS collide the sender should wait some RANDOM TIME before sending a second RTS

FRAME

ADDRESSING

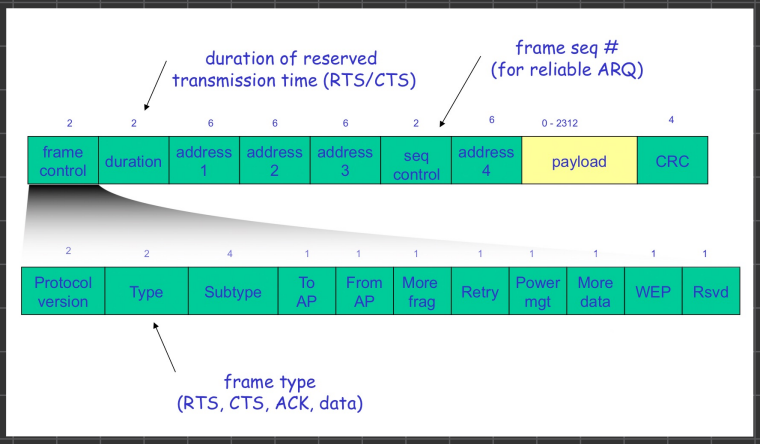


How to put addresses

From AP	To AP	Add 1	Add 2	Add 3	Add 4
0	0	Dst M	Src M	AP	0
1	0	Dst M	AP	Src R	0
0	1	AP	Src M	Dst R	0
1	1	Dst AP	Src AP	Dst M	Src M

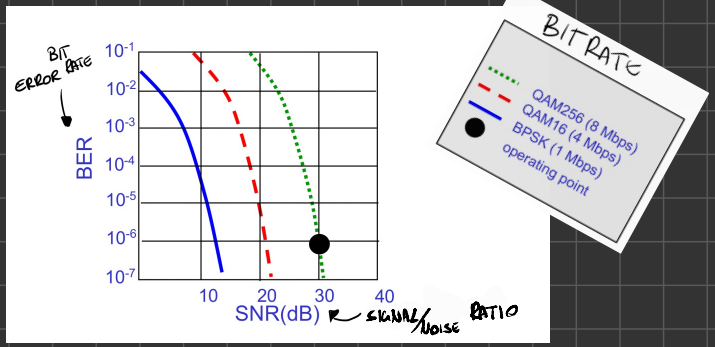
↳ NO ROUTER, just communication beg two Acc. Point.

OTHER FIELDS



BIT RATE MODULATION

- If we decrese bit RATE, the BER decrese, because it's like speaking slowly in noisy room



FAIRNESS PROBLEM

- You have 2 station transmit at 11 Mbps and 1 Mbps
- one occupy the channels $11 \cdot \frac{1}{12}$ and the other $1 \cdot \frac{11}{12}$, so the channel occupation is divided in a way that they transmit at the same thoughput, the second SENDS MORE PACKET PER s

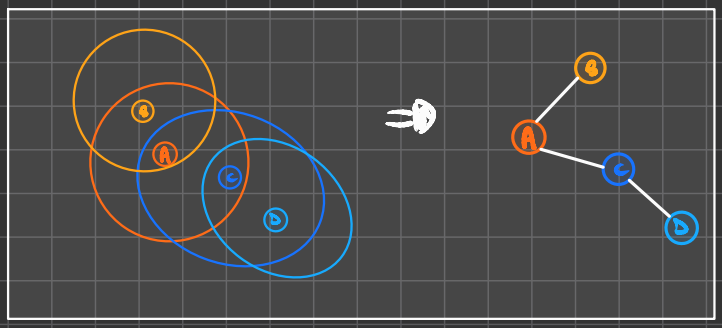
byte per second

24/01/21

MANET (MOBILE AD HOC NETWORK)

DYNAMIC TOPOLOGY

- Every node can be a ROUTER!
- We can draw a graph by checking neighbours in the communication range of every node, it has more links than a traditional network
- a MANET should check neighbors continuously (the topology changes fast)



Assumption

- We will assume the END-TO-END principle in the order of milliseconds, so a Path should be stable for some millisecond

TCP / IP

- Only END HOST will need TCP, every node in beetween is used just for IP routing.
- A Node has only an INTERFACE (only one IP address), a normal router can have multiple interface

ROUTING

- We can choose:
  - SOURCE ROUTING: Path is computed at the sender; so routing tables are not needed
  - HOP-BY-HOP ROUTING: routing decision are made in intermediate nodes ↑ BEST OPT.

MANET PROTOCOLS

REACTIVE PROTOCOLS

- Network compute the path only if I ask it. There is OVERHEAD when you ask for a route

PROACTIVE PROTOCOLS

- Node are continuously computing routes, when you ask for it, it will be ready. It uses routing tables

OLSR protocol (OPTIMIZED LINK STATE ROUTING)

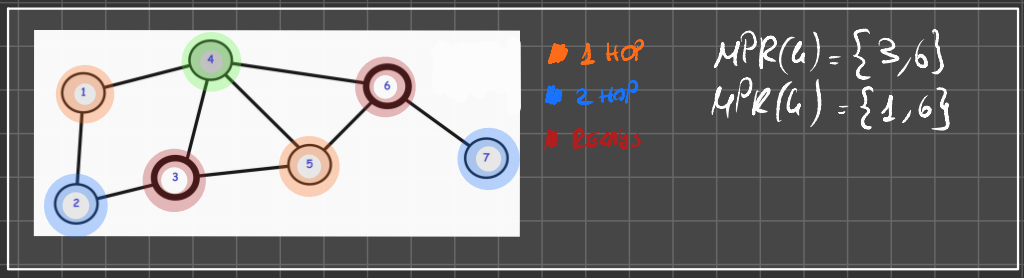
- PROACTIVE and HOP-BY-HOP Protocol
- Nodes get infos only from Neighbourhood

HPR(i)

- Uses MULTIPOINT RELAYS nodes to send infos (reducing FLOODING)

How do we choose relays?

→ Every node i select a set $MPR(i) \subseteq N(i)$ in such a way that every 2HOP neighbor of i is covered by it's 1HOP relays

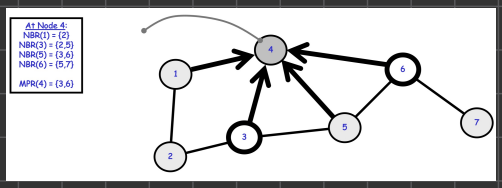


MR(i)

- A MULTI-POINT SELECTOR SET $MS(i)$ for a node i is the set of nodes that has chosen i in their MPR set

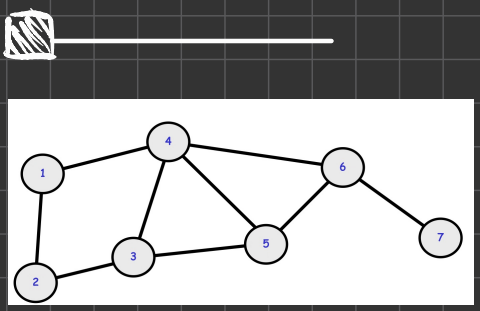
HELLO MSG

- Hello messages are sent periodically to 1-HOP neighbors, in order to determine MPRs, by checking 2-HOP NEIGHBORS thank to the neighbor list in the HELLO MSGS



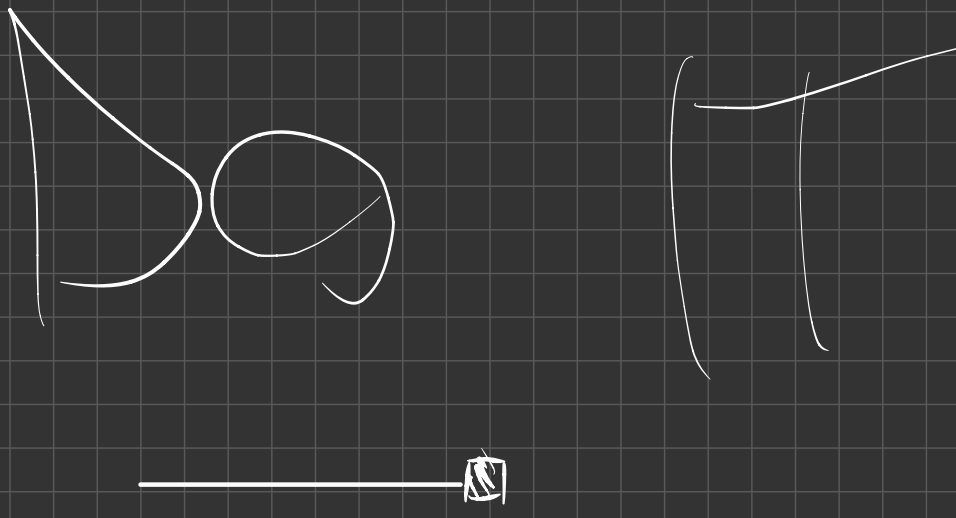
TC MSG

- used to send topology infos from MPRs to their MS; only MPR nodes propagate TC msgs



MPR(1) = { 4 }
MPR(2) = { 3 }
MPR(3) = { 4 }
MPR(4) = { 3, 6 }
MPR(5) = { 3, 4, 6 }
MPR(6) = { 4 }
MPR(7) = { 6 }

MS(1) = { }
MS(2) = { }
MS(3) = { 2, 4, 5 }
MS(4) = { 1, 3, 5, 6 }
MS(5) = { }
MS(6) = { 4, 5, 7 }
MS(7) = { }



AODV protocol
(Ad Hoc on demand distance vector)

- ACTIVE (on demand) and HOP-BY-HOP so DYNAMIC TABLES are stored on intermediate nodes of active path
- Every node store {NODE SEQ. NUMB. , BROADCAST ID}

RREQ MSG

- Source request a route by BC to N(SOURCE) an RREQ packet
  - → SOURCE AND DEST seq. numbers are used to checke the version of the path (How much fresh it is?)
  - → (SRC_ADD, BC_ID) is the key of the RREQ msg:
    - BC_ID is incremented for each RREQ packet sent.

type	flags	resvd	hopcnt
broadcast_id			
dest_addr			
dest_sequence_#			
source_addr			
source_sequence_#			

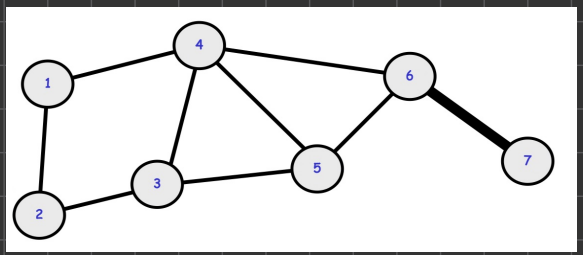
RREP MSG

- sent if RREQ reach a node who knows the destination
  - → Hop_count is needed to choose beetween multiple RREP packets

type	flags	rsvd	prsz	hopcnt
dest_addr				
dest_sequence_#				
source_addr				
lifetime				

RERR MSG

- If a node on (s,t)-path detect an error (ex. node touched), a RERR is sent to s with HOP_CUT = ∞



- ❑ Node 1 needs to send a data packet to Node 7
- ❑ Assume Node 6 knows a current route to Node 7
- ❑ Assume that no other route information exists in the network (related to Node 7)