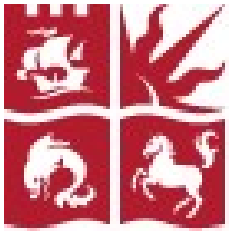
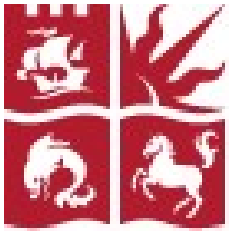


EENGM4221:
Broadband Wireless Communications

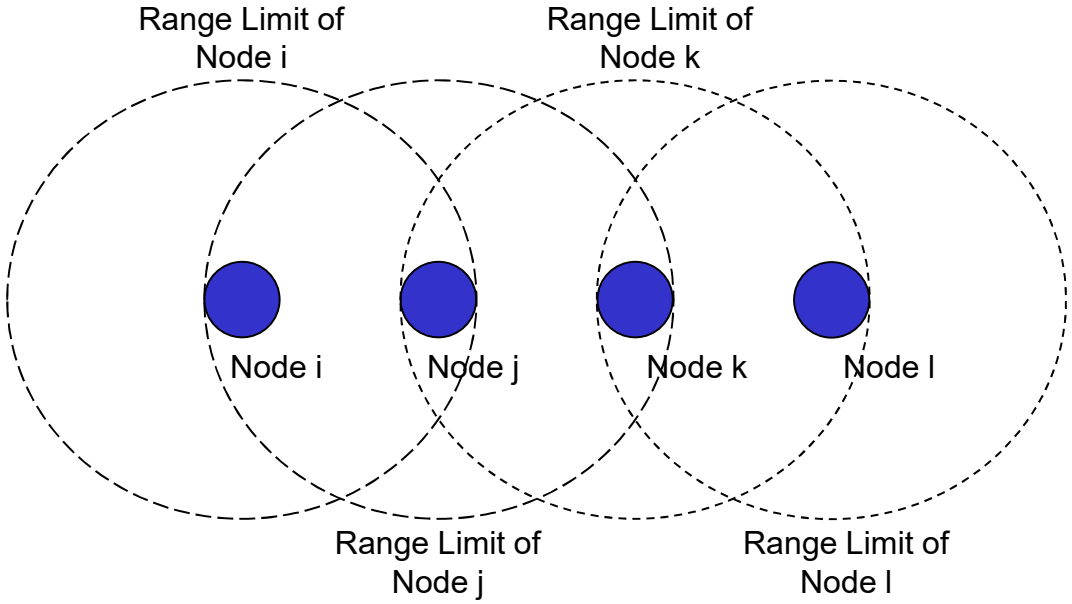
Lecture 14: 802.11 Hidden Nodes, RTS/CTS and 4 way handshaking

Dr Simon Armour

The Hidden Node Problem (1)

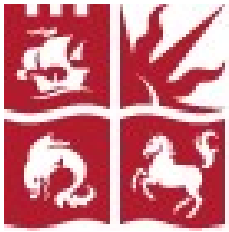


- CSMA is vulnerable to the Hidden Node Problem
  - This problem is not solved by other features of the 2-way handshake protocol either
- Consider the simple scenario below
  - Not entirely realistic given what we know about multipath
  - But a simple representation of what could occur even in a realistic radio environment



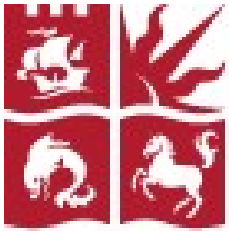
Ref:

The Hidden Node Problem (2)



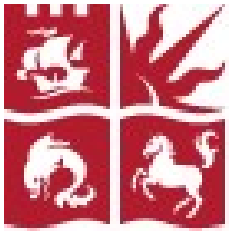
- Assume j transmits to k
  - CSMA will not prevent l transmitting during j's MPDU since it cannot 'hear' j
  - CSMA will not prevent i transmitting during k's ACK since it cannot 'hear' k
    - Use of the NAV should prevent this latter problem
  - Nodes j and l are 'hidden' from each other
  - If l transmits, k may receive l's transmission simultaneously with the MPDU from j
    - A collision has occurred and the transmission of data from j to k fails

Solutions to the Hidden Node Problem



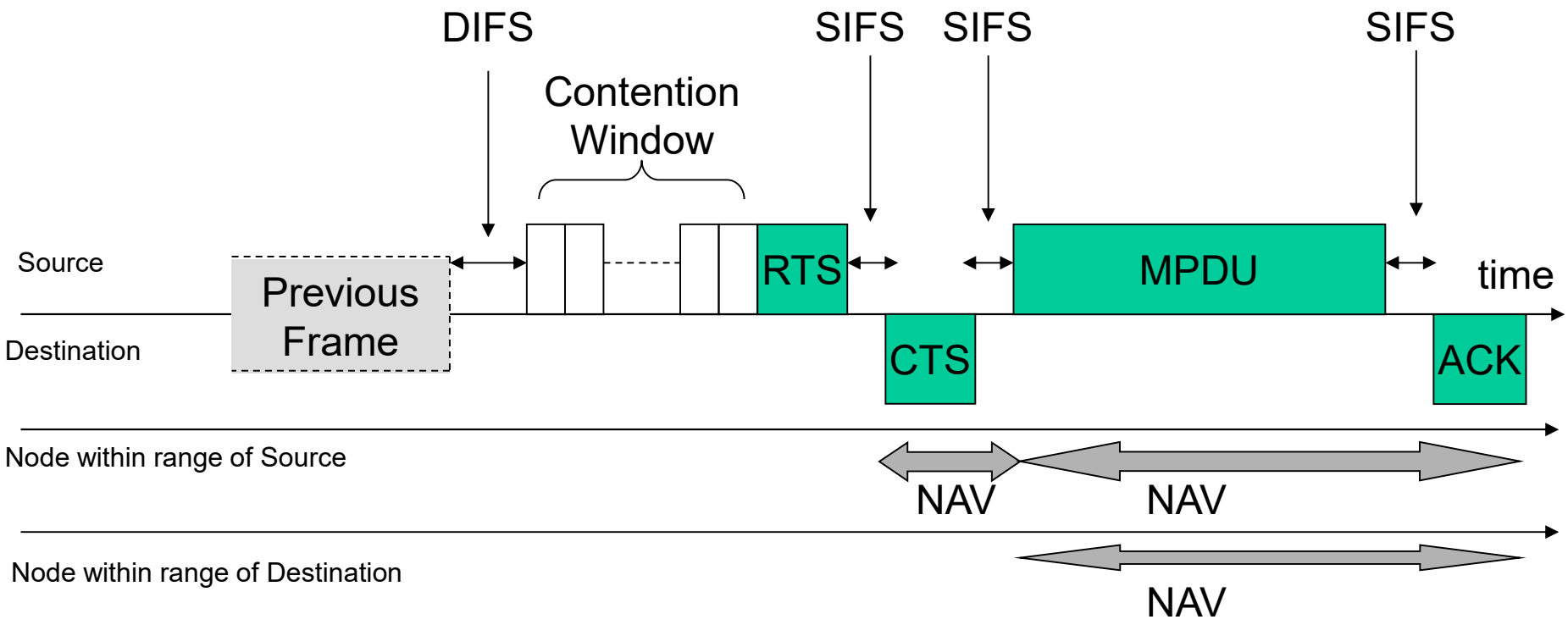
- There are two possible means to tackle the hidden node problem
- The first is to set a low fragmentation threshold which
  - Reduces the likelihood of collisions
  - Requires that only those fragments suffering collision need to be retransmitted
  - This method is essentially one of trusting to luck and minimising the damage when luck doesn't work
    - Not surprisingly, it is limited in its effectiveness
    - It may be adequate in networks with low load where collisions are unlikely
    - In networks with low loads, collisions will still occur
    - In networks with high loads, hidden nodes could have a disastrous effect
- The alternative is called RTS/CTS

RTS/CTS (1)

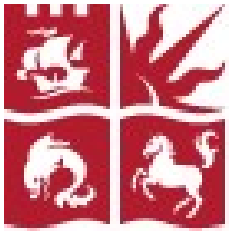


- RTS/CTS converts the 2-way handshake DCF frame exchange to a 4-way handshake frame exchange by adding two additional frames between the CW and MPDU
  - Request to Send (RTS)
  - Clear to Send (CTS)
- Both of these consist of only control information (including the length of the MPDU to follow, for NAV purposes) and no actual data
- Extra SIFS between frames are required
- The result is to add further redundancy

RTS/CTS (2)

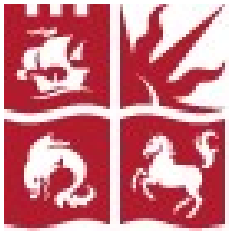

DIFS
Contention Window
SIFS
SIFS
SIFS
Source
Destination
Previous Frame
RTS
CTS
MPDU
ACK
time
Node within range of Source
NAV
NAV
Node within range of Destination
NAV

RTS/CTS (3)

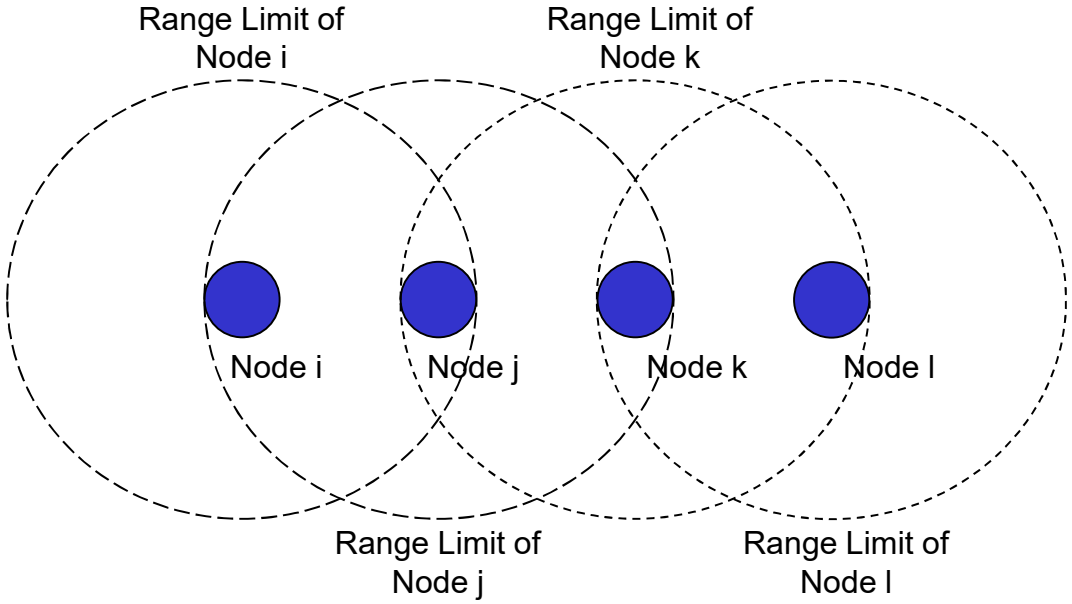


- Any node hearing the RTS OR CTS can set an accurate NAV to the end of the ACK and thereby avoid causing a collision
- For the previous hidden node example:
  - Node j transmits RTS after its CW expires
  - Node k responds with a CTS
  - Upon hearing the RTS, node i sets its NAV to after the expected CTS and SIFS and defers
  - Upon hearing the CTS, node l sets its NAV to after the expected ACK and defers
  - Upon hearing the MPDU, node i again sets its NAV to after the expected ACK and defers
- The source node will only transmit its MPDU IF it receives a valid CTS
- RTS/CTS cannot prevent all collisions but it:
  - Reduces the likelihood of collisions
  - Reduces the 'cost' of collisions
    - Short RTS and CTS frames may be lost but not long data frames
- Similarly to Fragmentation, a threshold is usually set; any MSDU beyond a certain length must use RTS/CTS
  - This is again controlled by the network manager – usually via a GUI

The Exposed Node Problem

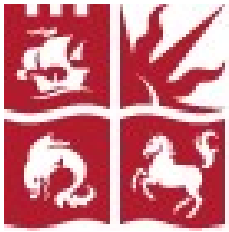


- The exposed node problem is the opposite of the hidden node problem
- If node j transmits to node i, node k can transmit to node l with no collision taking place (assuming suitable frame lengths)
- Use of RTS/CTS can be seen to prevent this



Ref:

Review of Lecture 14



- We discussed the concept of the ‘Hidden Node Problem’; ‘you can’t hear a receiver’
  - Not specific to 802.11 but IS a challenge for 802.11 DCF
- We discussed two possible solutions to this:
  - Fragmentation
  - RTS/CTS
- We introduced the 4-way handshaking version of DCF
- We briefly addressed the term, ‘Exposed Node Problem’

Ref: