Mobile IP Network Layer

Lesson 08

Reverse Tunnelling, Multicasting and Firewall Security

Reverse Tunnel

- If a reverse tunnel is formed then another tunnel is present through the paths from 10 to 3 in Figure 6.3
- Reverse tunnelling from FA to HA

Advantage of reverse tunnelling

- Multicasting needs bi-directional tunnelling
- Reverse tunnelling is required when a firewall is employed

Time-to-live for forward and reverse tunnelling

- Time-to-live defines the number of attempts to hop before expiry of packets at the network

Time-to-live for forward and reverse tunnelling

- GRE header encapsulation during tunnelling sets time-to-live = 1, so the packets are forwarded only once
- The tunnel does not need extra hops, has fixed endpoints

Time-to-live = 1 for forward tunnelling

- Results in once-only forwarding through the tunnel from the HA to the FA when the MN visits a foreign network
- The tunnel does not need extra hops
- It has fixed endpoints

Time-to-live for MN_L on visit sending to CN_K

- At the FA, the time-to-live setting might be too low
- Therefore, when the MN_l sends the response to the correspondent network (CN_k), then the time-to-live set at the FA may not be sufficient

Time-to-live for forward and reverse tunnelling

- When the COA is used to send the response to the CN without reverse tunnelling, then a very low setting of time-to-live blocks the packets after a very small number of hops (attempts) to the CN

Time-to-live for reverse tunnelling

- Sets the time-to-live equal to 1 because IP packets need to be sent only once
- The tunnel does not need extra hop
- It has fixed source and destination endpoints

Reverse tunnelling

- Facilitates guaranteed transmission of the IP packet responses through the tunnel to the HA
- Now, the HA transmits the response to the CN
- A low value of time-to-live at the FA does not lead to packet expiries

Multicasting by reverse tunnelling

- Information is multicast to a mobile node (MN) when it sets the option for multicast listening
- Uses Bi-directional tunnelling method over a mobile IP network

Multicasting by reverse tunnelling

- Assume that a MN_i visits a foreign network with FA_j
- A multicast-tree multicasts a packet to HA_j
- HA_j forwards the multicasted IP packets to MN_j after registration

Multicasting by reverse tunnelling

- HA_j establishes a bi-directional tunnel between HA_i and FA_j
- FA_j transmits the received multicast message or packet to MN_j

Multicasting by reverse tunnelling

- Suppose MN_i visits another foreign network with FA_k
- MN_i requests FA_k, and FA_k forwards the transmit request for the multicast to HA_j

Disadvantages of reverse tunnel approach

- Duplication of multicast IP packets when multiple MNs of HA_j and other HAs visit the same FA
- Because several HAs create several bi-directional tunnels, through which they transmit multicast packets multiple times

Disadvantages of reverse tunnel approach

- When the built bi-directional tunnels do not converge into one, the packets maybe duplicated

Disadvantages of reverse tunnel approach

- IP packets reach by short and long paths, when there is no DMSP (designated multicast provider)

Mobile multicast (MoM) protocol

- Convergence of the tunnels by defining an HA as the DMSP
- Only the DMSP can build bi-direction tunnels
- When DMSP providing the multicast service— the IP packets reach by the longer path; The DMSP-route length may not be the shortest

The advantage of multicasting by reverse tunnelling

- No reconfiguration (updating of the routing tables) of routers at the multicast tree

Remote subscription approach of multicast

- Without the reverse tunnelling
- Assume that MN_i visits a foreign network with FA_i
- FA_i transmits a ‘join’ request in case it is not presently registered for multicast at the multicast tree

Remote subscription approach advantages

- No duplication of multicast IP packets
- IP packets reach through an optimal (shortest) path
- When MN_i moves to the next FA_k , it again transmits a ‘join’ request and the previous subscription cancels

Firewall Security

- Filters the packets assigned to an IP address received from another IP address
- IP address of the MN is at HA
- When MN moves to FA, the MN sends the IP packets using COA assigned at FA

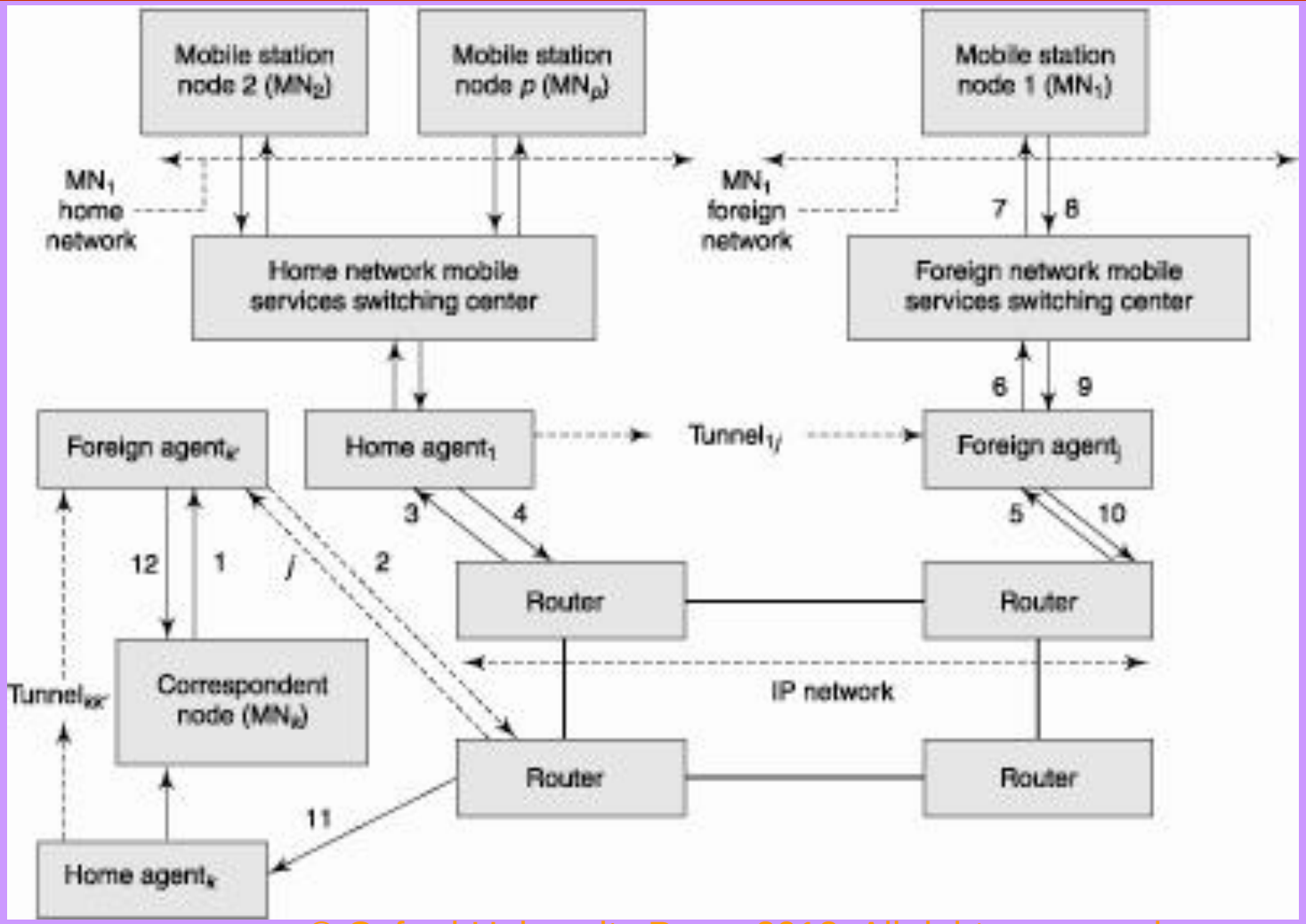
Firewall Security

- In case the firewall that permits another IP address (at the FA) assigned to an IP address (at the HA), there is a security risk

Advantage of reverse tunnelling of the packet from the COA

- FA to the HA and HA transmits to the correspondent node (CN)
- The firewall gets the packets from the same IP address as the IP address registered at the firewall
- It does not filter these packets

Tunnels



Firewall at the CN sending the IP packets to MN_L

- The path followed– 1, 2, 3, 4, 5, 6 and 7
- Sub-paths 4 and 5– across the forward tunnel

Firewall at the CN sending the IP packets to MN_L

- When the firewall at the CN receives the IP packets sent to MN_l, then the path followed will be 8, 9, 10, 3, 4, and *i*

Firewall at the CN sending the IP packets to MN_L

- Sub-paths 10 and 3– across the reverse tunnel
- The CN firewall continues to use the same IP address for the MN when transmitting and receiving packets

Summary

- Multicasting
- Reverse tunnelling approach for short paths
- Remote subscription approach

Summary

- No duplication of multicast IP packets
- IP packets reach through an optimal (shortest) path
- Firewall security by reverse tunnelling

End of Lesson 08

Reverse Tunnelling, Multicasting and Firewall Security