Lecture 8 Notes – First Half

Security in Wireless Protocol (802.11)

Proposed protocol – Wireless Equivalent Privacy

3 goals for a secure protocol

1) Privacy
2) Integrity
3) Access Control

Mechanism used for security

RC4 (V, K) xor P -> C

V - Initial vector
K – Key
P – Message
C – Encrypted Message

Problems with the above mechanism

1) Having the same initialization vector.

   C1 = RC (V, K) xor P1
   C2 = RC (V, K) xor P2

   C1 xor C2 = P1 xor P2

2) Knowing C1 and P1, you can get to RC and can send message without knowing key

Multicast

Why?

1. Efficiency

What Layer?

1. IP router
   a. Advantages - Efficiency
2. Multicast Overlay (e.g. CDN)
   a. Advantages – 1) Flexibility 2)Simplicity 3) Deployment

Why in every router?

1. Customer Driven

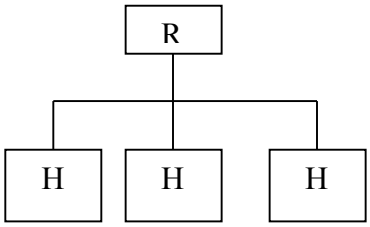
Why not used?

1. Multicast doesn't matter
2. Control inefficiency of broadcast and prune
3. No applications
4. No business model (could be efficient when used in an intranet)

Service Model

1. Best Effort
2. Uses Group addresses
3. Multiple Senders (Single Source could be simpler and have better access control)
4. Receivers (can join explicitly or implicitly)

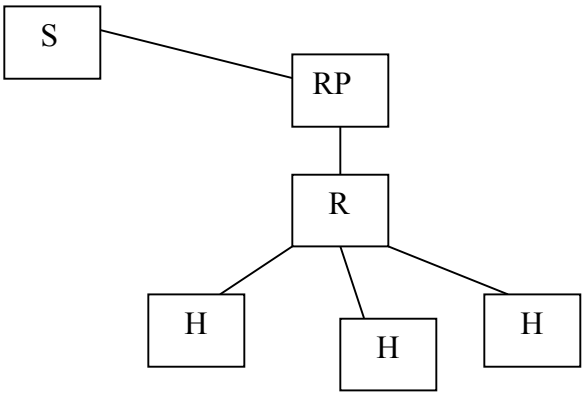
Implicit Join - Uses broadcast and prune.



1. R broadcasts asking if anyone wants to join multicast group G
2. One of H broadcasts it's desire to join the group
3. R stores this information and broadcasts this to all other hosts

Hosts join multicast group using a protocol IGMP.

Explicit Join - Protocol Independent Multicast (PIM)



PIM assigns a RP for each group.
The Routers send a Join message to the RP using Unicast transmission
RP keeps track of the Routers that have joined the group.
Sender sends the message to RP and RP then sends it to the routers part of the multicast group.