802.11b/Wi-Fi:
Internet inalámbrica para todos

Grupo de Sistemas y Comunicaciones
Universidad Rey Juan Carlos

gsyc-profes@gsyc.escet.urjc.es

ATI – Capítulo Territorial de Madrid
26 de febrero de 2002

Contenidos

- Redes de Área Local Inalámbricas
- IP Móvil

Redes de Área Local Inalámbricas

Introducción

Sistemas de transmisión inalámbrica:

- Satélites (a distintas órbitas)
- Telefonía móvil: GSM, GPRS, UMTS
- IRDA
- Bluetooth
- WLAN

Terminología

- IEEE 802.11: Especificaciones para 1-2 Mbps en la banda de los 2.4 GHz. usando salto de frecuencias (FHSS) o secuencia directa (DSSS).
- IEEE 802.11b: Extensión de 802.11 para proporcionar 11 Mbps usando DSSS.
- Wi-Fi (Wireless Fidelity): Término registrado promulgado por la WECA para certificar productos IEEE 802.11b capaces de interoperar con los de otros fabricantes.
- IEEE 802.11a: Extensión de 802.11 para proporcionar 54 Mbps usando OFDM.
- IEEE 802.11g: Extensión de 802.11 para proporcionar 20-54 Mbps usando DSSS y OFDM. Es compatible hacia atrás con 802.11b. Tiene mayor alcance y menor consumo de potencia que 802.11a.

Espectro expandido (Spread Spectrum)

- Idea: transmitir ocupando una banda de frecuencias mayor de la requerida
- Desarrollado originalmente con fines militares, para evitar ataques/escuchas. Patente de Lamarr/Antheils, en 1942. Usada por primera vez en un sistema de guiado de torpedos de la armanda americana en 1962.
- Dos tipos:
  - FHSS: Salto de Frecuencias (Frecuency Hopping)
  - DSSS: Secuencia Directa (Direct Sequence)

Salto de Frecuencias (FHSS)

- Se transmite en diferentes bandas de frecuencias, saltando de una a otra en forma aleatoria pero predecible.
- Emisor y receptor deben compartir generador de números aleatorios y semilla.
- 802.11 establece 75 bandas de 1 MHz.

Secuencia Directa (DSSS)

- Aquí el ≪espectro se expande≫ al transmitir varios bits por cada bit de información real.
- Para cada bit, enviamos el XOR de él y de n bits aleatorios (*chipping code*):
  - Para enviar un 0: 00100100010
  - Para enviar un 1: 10010100110
- 802.11: Código chipping de 11 bits, permitiendo 2 Mbps (cayendo a 1 Mbps en entornos ruidosos).
- 802.11b: Utiliza una nueva forma de modulación, CCK (complementary coding keying), para proporcionar 11 Mbps (con caídas a 5.5 Mbps, 2 Mbps y 1 Mbps).

Acceso al medio: CSMA/CA

- En redes inalámbricas, no se puede escuchar a la vez que se trasmite: no pueden detectarse colisiones.
- Técnica: intentar evitarlas: CSMA with Collision Avoidance:
  - Si el canal está ocupado se espera a que esté libre
  - Si está libre, se espera un tiempo, y si sigue libre se transmite.

Problemas de CSMA/CA

- Nodos ocultos: Una estación cree que el canal está libre, pero en realidad está ocupado por otro nodo al que no oye.
- Nodos expuestos: Una estación cree que el canal está ocupado, pero en realidad está libre pues el nodo al que oye no le interferiría.

MACA: Multi Access Collision Avoidance

- Antes de transmitir el emisor envía una trama RTS (RequestToSend), indicando la longitud de datos que quiere enviar.
- El receptor le contesta con una trama CTS (ClearToSend), repitiendo la longitud.
- Al recibir el CTS, el emisor envía sus datos

Reglas para evitar los nodos ocultos y expuestos:

- Al ver un RTS, hay que esperar un tiempo por el CTS
- Al ver un CTS, hay que esperar según la longitud

802.11: MACA con CSMA/CA para enviar los RTS.

Modos de operación

- Modo ad-hoc: Un nodo se comunica directamente con otro
- Modo infraestructura: Los nodos móviles se comunican con un punto de acceso (access point).
  - la misión principal del punto de acceso suele ser dar acceso a la red fija
  - la comunicación entre nodos móviles se hace a través del punto de acceso
  - cada nodo móvil ha de asociarse a un punto de acceso antes de transmitir: los puntos de acceso envían periódicamente una señal de baliza.
  - un punto de acceso es simplemente un concentrador/puente (hub/bridge): puede construirse con un ordenador, una tarjeta inalámbrica y una tarjeta fija.

Seguridad

- El aire es un medio compartido: cualquiera puede escuchar.
- No es muy distinto del cable: hay que alcanzar la misma seguridad. Sin embargo se usan mecanismos adicionales.
- En 802.11b: WEP (Wireless Encryption Protocol):
  - razonablemente fuerte
  - computacionalemente eficiente
  - exportable internacionalmente
  - opcional
  - recientemente roto (U.Berkeley).

Características de WEP

- Cifrado: clave simétrica de 64 bits (40 secretos), algoritmo RC4
- Integridad: CRC-32
- Autenticación de las estaciones: reto con la misma clave de cifrado (también SSID y direcciones MAC, pero se transmiten en claro)

Debilidades:

- Clave secreta pequeña (propuestas de 128 bits)
- Integridad pensada para el cable
- Misma clave de cifrado y autenticación

En desarrollo: Estándar IEEE 802.11i

Consecuencias para la salud

¿?

IP Móvil

Movilidad

Ahora que tenemos:

- terminales ligeros y portables
- redes inalámbricas

¡queremos poder movernos con nuestro terminal por toda la red!

- Micromovilidad: Entre puntos de acceso
- Macromovilidad: Entre subredes de una organización
- Movilidad Global: Entre zonas geográficas u operadores

IP Móvil (Mobile IP): Soporte a la movilidad en IP. Pensado fundamentalmente para macromovilidad

Encaminamiento en IP

- Un terminal en la red tiene una dirección IP con una parte fijada por la subred en que se encuentra (prefijo de red).
- Las tablas de encaminamiento en los encaminadores (routers) de Internet hacen que lleguen los datagramas IP a su destino mirando el prefijo de la dirección IP de destino
- Si un terminal cambia de red, tiene que cambiar su dirección IP: las conexiones (TCP) que tuviera abiertas se terminan.
- Aunque se empeñara en mantener su dirección IP, los datagramas no le llegarían a la nueva subred.

Fundamentos de IP Móvil

- El terminal móvil tiene dos direcciones IP:
  - Dirección Local (Home Address): Fija. Es con la que el terminal mantiene las conexiones. Corresponde con su red local.
  - Dirección de Auxilio (Care-of Address): Cambiante. Es la que corresponde a la red en que se encuentre el móvil en un momento dado.
- En la red local, un Agente Local (Home Agent) sabe qué Dirección de Auxilio tiene en cada momento el terminal móvil:
  - recoge los datagramas destinados a ls Dirección Local del terminal móvil
  - los reenvía dentro de un nuevo datagrama dirigido a la Dirección de Auxilio (túnel).

Fases

- Descubrimiento de la Dirección de Auxilio por parte del terminal móvil
- Registro de la Dirección de Auxilio en el Agente Local.
- Túnel desde el Agente Local a la Dirección de Auxilio.

Problemas de IP Móvil

- El encaminamiento en triángulo es ineficiente.
- La creación de túneles es un sobrecoste.
- Cuello de botella en el Agente Local.
- Implicaciones de seguridad en cortafuegos.

Referencias

- Larry L. Peterson, Bruce S. Davie, *Computer Networks: A Systems Approach*. 2nd ed. Morgan Kaufmann 2000.
- IEEE 802.11 Wireless
  `http://standards.ieee.org/getieee802/802.11.html`
- Sultan Weatherspoon, *Overview of IEEE 802.11b Security*.
  `http://developer.intel.com/technology/itj/q22000/articles/art_5.htm`
- RFC 2002: IP Mobility Support.
  `http://www.faqs.org/rfcs/rfc2002.html`
- Charles E. Perkins, *Mobile Networking Through Mobile IP*
  `http://www.computer.org/internet/v2n1/perkins.htm`