
DIFERENCIAS ENTRE *WI-FI DIRECT* Y EL MODO *AD-HOC*

DEL ESTÁNDAR IEEE 802.11

Diferencias entre *Wi-Fi Direct* y el Modo *Ad-Hoc*

del Estándar IEEE 802.11

M. en C. Cyntia E. Enríquez Ortiz

M. en C. Raúl Fernández Zavala

M. en C. Carlos De La Cruz Sosa

Unidad Profesional Interdisciplinaria de Ingeniería y Tecnologías

Avanzadas del Instituto Politécnico Nacional (UPIITA-IPN)

Academia de Telemática

Resumen

En este trabajo se describen los conceptos básicos del protocolo WiFi Direct ("WiFi P2P") y del modo Ad-Hoc ("IBSS") del estándar IEEE 802.11, se exponen las diferencias que existen entre ambos y se explican las razones por las que WiFi Direct no puede sustituir por completo al modo Ad-Hoc.

Introducción

Recientemente el protocolo *WiFi Direct* es promovido como un reemplazo del modo de operación *Ad-Hoc* del estándar IEEE 802.11, con el argumento de que es un protocolo "*seguro y fácil de configurar que permite una comunicación directa entre dispositivos WiFi*". Sin embargo, en

términos generales ambos protocolos tienen la misma funcionalidad, es decir ambos protocolos permiten que los dispositivos *WiFi* se conecten directamente entre sí de una manera de igual a igual ("*Peer to Peer*"), sin el uso de un Punto de Acceso (*Access Point, AP*) tradicional [1].

WiFi Direct ha alcanzado una gran relevancia actualmente debido a que está implementado en la mayoría de los dispositivos móviles actuales y logra su objetivo principal, que es permitir la conexión de dispositivos *WiFi* sin el uso de infraestructura, sin embargo, este protocolo funciona bien bajo las condiciones para las cuales fue diseñado, esto implica que *WiFi Direct* no cubre todas las posibilidades que ofrece el modo *Ad-Hoc*.

Wi-Fi Direct

Wi-Fi Direct no es un estándar IEEE, sino una especificación técnica definida por la *WiFi Alliance* llamada "*Wi-Fi Peer-to-Peer (P2P) Technical Specification*", la cual permite que los dispositivos que la soportan puedan formar grupos y conectarse entre ellos de forma rápida y segura para realizar tareas básicas sin la necesidad de un punto de acceso inalámbrico. Para poder implementar la comunicación de dispositivo a dispositivo, *WiFi Direct* se basa en la infraestructura del estándar IEEE 802.11 y deja que los dispositivos *P2P* negocien la pertenencia a un grupo y el rol que tendrán en la conexión cada uno de ellos, es decir, un dispositivo del grupo debe asumir el rol tradicional de un punto de acceso, el cual será llamado Propietario del Grupo (*Group Owner, GO*) y los demás dispositivos se conectarán como clientes con él. Para el establecimiento de una conexión en *WiFi Direct*, los dispositivos *P2P* tiene que realizar al menos cuatro operaciones [2].

1) Descubrimiento de dispositivos

Para poder establecer una conexión, los dispositivos *P2P* deben primero encontrarse, para lo cual alternadamente envían y escuchan tramas *probe request* (solicitud de prueba) a través de los canales 1, 6 y 11 de la banda de 2.4 GHz, denominados canales sociales. Los dispositivos *P2P* desconectados y los propietarios de grupo responden con tramas *probe response* (respuesta de prueba) a dichas solicitudes.

Ambas tramas (*probe request* y *probe response*) incluyen elementos de información *P2P*, los cuales describen características del dispositivo y del grupo. Entre las características del

dispositivo que se envían se incluye, el nombre del dispositivo, el tipo de dispositivo, los canales de operación soportados y el descubrimiento de servicios. Por su parte, las características del grupo incluyen, el número de dispositivos permitidos en el grupo (límite del grupo), el permiso o no de intercambio de datos entre los clientes, la información sobre si el GO proporciona una conexión a otra *WLAN* o a Internet y si el grupo es persistente o no.

2) *Servicio de descubrimiento*

Después de la fase de descubrimiento los dispositivos *P2P* pueden describir los servicios que brinda cada uno de ellos. Este intercambio de tramas es opcional y admite diferentes protocolos de descripción de servicios tales como *DNS-SD*, *UPnP* o *WS-Discovery*. Con la información obtenida a partir del servicio de descubrimiento, la aplicación o el usuario puede optar por conectarse a un dispositivo *P2P* en función de su nombre o los servicios proporcionados.

3) *Formación de grupos*

Cuando un dispositivo *P2P* desea conectarse con otro, puede enviarle a un dispositivo que ya esté conectado una *P2P Invitation request* (solicitud de invitación *P2P*) para pedirle que se una a un nuevo grupo, o puede iniciar directamente la formación de un grupo con un dispositivo desconectado enviando una trama *GO Negotiation request* (solicitud de negociación *GO*). Debido a que los roles en el grupo se negocian, cualquiera de los dos dispositivos *P2P* puede asumir el rol de propietario del grupo *P2P* (*GO*) o cliente *P2P*. El objetivo principal de esta negociación es determinar cuál de los dispositivos participantes se convertirá en el *GO* y el intercambio de algunas características del grupo, como el canal de operación, el método de configuración de *WPS* y la persistencia o no de un grupo. Cualquier dispositivo *P2P* puede comunicar su interés de convertirse en propietario del grupo con el atributo *GO Intent* (0-15) de las tramas *GO Negotiation request / response GO*, y puede negarse a formar un grupo si los parámetros del grupo no son aceptables.

Después de que se haya tomado una decisión sobre qué dispositivo se convertirá en el propietario del grupo, se envía una trama *Confirmación de Negociación de GO* y ambos dispositivos se moverán al canal de operación negociado. El *GO* comienza a operar en modo de punto de acceso, enviando balizas con el Identificador de Red (*SSID*, por sus siglas en inglés) negociado y el bit de formación de grupo establecido en 1, porque la formación del grupo aún no se ha completado.

4) *Aprovisionamiento y Encriptación*

Posteriormente comienza la fase de aprovisionamiento, donde el cliente se conecta al *GO* para intercambiar credenciales con el protocolo *WPS*, que es un intercambio de ocho mensajes *EAP* (*Extensible Authentication Protocol*). Para permitir la conexión, el usuario normalmente debe ingresar un código PIN o presionar un botón en el dispositivo. Después de eso, *WPA2* (*Wi-Fi Protected Access 2*) comienza a intercambiar las claves de cifrado, el *GO* asume el rol de autenticador y el cliente es el solicitante. Luego, el cliente solicitará una dirección IPv4 al *GO*, y

finalmente puede ocurrir la transferencia de datos. Para evitar que los usuarios tengan que ingresar un código PIN cada vez que se forma un grupo entre algunos dispositivos, el grupo puede hacerse persistente, en cuyo caso los dispositivos almacenan las credenciales y pueden volver a conectarse automáticamente cuando sea necesario.

Modo *Ad-hoc* (IBSS)

El modo *Ad-hoc* se denomina oficialmente *IBSS* (conjunto de servicios básicos independientes) en el estándar IEEE 802.11 y, es una parte activa del estándar actual IEEE802.11-2012 que establece que "*un IBSS es el tipo más básico de LAN IEEE 802.11*". Todos los dispositivos que cumplen con el estándar deben implementarlo. El modo *IBSS* es muy simple y pasa por cuatro etapas [3].

1) Formación de redes *Ad-hoc*

Cualquier dispositivo puede iniciar un *IBSS*, y no existe una jerarquía entre los dispositivos, por lo que se suele llamar a cualquier dispositivo *IBSS* simplemente "*nodo*". Un dispositivo que desee unirse a un *IBSS* con un nombre determinado (*Identificador de Red* o *SSID*) explorará para ver si la red ya existe, escuchando pasivamente en el canal y recibiendo balizas de otros nodos o enviando *solicitudes de sondeo*. Si se detecta un *IBSS* existente, se toma su *BSSID* (*Basic Service Set Identifier*) y se pueden intercambiar tramas de datos directamente entre todos los nodos *IBSS* dentro del alcance del radio de cobertura.

2) Balizas

Al igual que los *AP*, los nodos *IBSS* envían balizas regularmente, que contienen el nombre de red (*SSID*), un *BSSID* y un valor de temporizador (*TSF*) para anunciar la existencia de la red *IBSS*. Para ahorrar ancho de banda, los dispositivos en el mismo *IBSS* comparten la tarea de enviar balizas: si un nodo ya recibió una baliza desde otro dispositivo dentro de un período de baliza, se abstendrá de enviar una baliza en este período. Para ser compatible con el estándar 802.11b, las balizas y las tramas de administración se envían a velocidades de datos bajas (1 o 2 Mbps) de manera predeterminada, pero cualquier implementación del controlador permite elegir las tasas básicas, por lo que se pueden usar tasas OFDM como en *Wi-Fi Direct*.

3) Fusión de *IBSS*

Cuando dos o más nodos con el mismo nombre de red (*SSID*) han elegido previamente diferentes *BSSID*, posiblemente porque no estaban dentro del radio alcance el uno del otro, pero ahora se quieren unir, deben fusionarse. En este caso, la regla es que el *IBSS* "más joven" debe hacerse cargo del *BSSID* del *IBSS* "anterior". La edad de un *IBSS* se conoce por los valores del temporizador *TSF* enviados en las balizas.

4) Seguridad

No existe un requisito estándar para la seguridad en el modo *IBSS*, por lo que las redes *IBSS* son libres de elegir entre el uso de cifrado, *WEP*, *WPA* o *RSN* (*WPA2*). Entonces, al igual que los *AP* y *Wi-Fi Direct*, el modo *Ad-hoc* también se puede usar con las claves precompartidas de *RSN*

(WPA2). Para intercambiar las claves de cifrado, los dispositivos *IBSS* tienen que realizar el *handshake* de 4 vías entre ellos.

Comparación entre Wi-Fi Direct (P2P) y el Modo Ad-Hoc (IBSS)

Considerando la definición de *Peer-to-Peer (P2P)*, la cual es "*los pares son participante igualmente privilegiados y equipotentes en una aplicación*" [2], se puede concluir que *Wi-Fi Direct* realmente no es un protocolo *P2P*. En esencia es un protocolo para formar grupos jerárquicos, y se usa principalmente para conectar solo dos dispositivos. Los dispositivos solo son pares iguales hasta que se conectan entre sí, y uno de ellos se convierte en propietario del grupo. Después de eso, siguen los roles jerárquicos de *AP* y cliente (maestro y esclavo). El protocolo en combinación con el descubrimiento de servicios puede proporcionar una forma conveniente y segura de conectar temporalmente dos dispositivos, pero no funciona adecuadamente más que para unos pocos dispositivos en estrecha proximidad.

Por otro lado, el modo *Ad-hoc* es una verdadera solución *P2P* sin jerarquías, donde todos los participantes son iguales. Esto abre muchas de posibilidades y modos de comunicación, entre ellos: redes oportunistas, con tolerancia al retardo y redes de malla de gran escala, que son especialmente útiles en escenarios donde la infraestructura local no es de confianza o no está disponible, sin embargo, el modo *IBSS* tiene muchas opciones de configuración y puede ser difícil de usar.

En la tabla 1 se muestra se manera resumida las ventajas y desventajas que presentan *Wi-Fi Direct* y el modo *Ad-hoc*.

Ventajas de <i>Wi-Fi Direct</i>	Ventajas del modo <i>Ad-hoc</i>
✓ Fácil uso para la conexión temporal de dispositivos. ✓ Seguridad y cifrado integrados en el protocolo. ✓ El descubrimiento del servicio es parte del protocolo.	✓ Solución real <i>P2P</i>. ✓ Puede manejar cambios de topología dinámicos. ✓ Permite redes en malla de gran escala. ✓ No es necesario intercambiar tramas adicionales antes del tráfico de datos.
Desventajas de <i>Wi-Fi Direct</i>	Desventajas del modo <i>Ad-hoc</i>
✓ No funciona bien con algunas topologías. ✓ No responde bien a los cambios dinámicos de topología. ✓ Se deben intercambiar muchas tramas antes del tráfico de datos.	✓ Difícil de usar para usuarios inexpertos. ✓ Sin cifrado o seguridad incorporada. ✓ Sin descubrimiento de servicio incorporado.

Tabla 1. Ventajas y desventajas de *Wi-Fi Direct* y modo *Ad-hoc*.

Conclusiones

Wi-Fi Direct y el modo *Ad-hoc* resuelven casos de uso muy diferentes, por lo que uno no puede reemplazar al otro. *Wi-Fi Direct* está diseñado para conectar temporalmente algunos dispositivos de una manera fácil y segura, pero no funciona bien para topologías de red más grandes. El modo *IBSS* es más versátil y difícil de configurar, pero se puede usar junto con protocolos de nivel superior para formar redes de malla de gran escala. Utilizar el término *P2P* para ambos protocolos es engañoso ya que se puede pensar que la forma limitada de "*P2P*" de *Wi-Fi Direct* podría sustituir la capacidad *P2P* real del modo *Ad-hoc*, lo cual es incorrecto.

Referencias

- [1] W.-F. Alliance, «Wi-Fi Direct | Wi-Fi Alliance,» 2018. [En línea]. Available: <https://wi-fi.org/discover-wi-fi/wi-fi-direct>. [Último acceso: 18 01 2018].
- [2] Wi-Fi Alliance, «Wi-Fi Peer-to-Peer (P2P) Technical Specification v1.5,» 2014. [En línea]. Available: <https://groups.wi-fi.org/kwspub/home/>. [Último acceso: 18 01 2018].
- [3] IEEE (Institute of Electrical and Electronic Engineers), «IEEE-SA - News, Press Release & Updates,» 2018. [En línea]. Available: <http://standards.ieee.org>. [Último acceso: 18 01 2018].