Modelado y Análisis Inicial del Establecimiento de una Conexión Bluetooth Usando las Redes de Petri Coloreadas

María E. Villapol
Universidad Central de Venezuela, Facultad de Ciencias, Escuela de Computación, Laboratorio de Redes Móviles, Inalámbricas y Distribuidas (ICARO)
Av. Los Ilustres, Los Chaguaramos, Caracas, Venezuela
Tel: +212 58 605 1132, Fax: +212 58 605 1131
mvillap@ciens.ucv.ve

Abstract

Bluetooth provides communication between devices via radio frequency in an area of around 10 meters. The Bluetooth specification includes a set of, adopted and fundamental, protocols hierarchically structured. Baseband is a fundamental protocol. Connection establishment is one of the functions of the baseband protocol. The protocol specification is not clear and ambiguous and hardly uses protocol specification tools such as state tables. In this paper, *Coloured Petri Nets (CPNs)*, which are formal techniques, are used to model the baseband connection establishment procedure carried out in a master and a slave Bluetooth device. Then the model is validated and debugged using the state space. The initial analysis shows that the model is behaved as expected and according to the model and analysis assumptions. The main contribution of this work is a clear and precise specification of the baseband connection establishment procedure using CPNs.

Keywords: Bluetooth, Baseband Connection Establishment, CPNs.

Resumen

Bluetooth es una tecnología de comunicación que proporciona comunicación entre dispositivos vía radio frecuencias en un área de alrededor de los 10 metros. La especificación de Bluetooth incluye un conjunto de protocolos, adoptados y propios, organizados de forma jerárquica. Uno de los protocolos propios de esta tecnología es el de bandabase. El establecimiento de una conexión es parte de la funciones de dicho protocolo. La especificación de este procedimiento es poco clara y ambigua y hace poco uso de herramientas para la descripción de protocolos tales como las tablas de estado. En este trabajo, las *Redes de Petri Coloreadas* (*Coloured Petri Nets*, *CPNs*), las cuales son una técnica formal, se utilizan para modelar el establecimiento de una conexión en un dispositivo Bluetooth maestro y en uno esclavo. Dicho modelo es entonces validado y depurado usando la técnica del espacio de estado. El análisis inicial muestra que el modelo se comporta acorde a lo esperado dadas las asunciones del modelo y las hechas para fines del análisis. La mayor contribución de este trabajo es el haber logrado una especificación clara y precisa del procedimiento a través del uso de la CPNs.

Palabras claves: Bluetooth, Establecimiento de la Conexión Bandabase, CPNs.

1 Introducción

Bluetooth Wíreless Technology es una tecnología de comunicación orientada a las *Redes de Área Personal Inalámbricas* (*Wíreless Personal Area Networks*, *WPANs*) [13], caracterizadas por proporcionar comunicación entre dispositivos vía radio frecuencias en un área muy limitada de alrededor de 10 metros. La especificación de Bluetooth [3] incluye una serie de protocolos estructurados en forma jerárquica, divididos en protocolos específicos de Bluetooth y otros adoptados de otras especificaciones. Uno de los protocolos fundamentales de esta tecnología es el conocido como *bandabase* (*baseband*). Entre las funciones de este protocolo se encuentra el establecimiento de una conexión Bluetooth entre un dispositivo maestro y uno o más esclavos.

Los métodos formales proporcionan técnicas para soportar el diseño y mantenimiento de los protocolos de comunicación [1]. Las *Redes de Petri Coloreadas* [7] son técnicas formales con bases matemáticas sólidas las cuales ya han sido utilizadas para el modelado de diversos sistemas tales como los protocolos de comunicación [7][14].

La especificación de Bluetooth hace poco uso de técnicas para la descripción de protocolos, tales como las tablas de estados, siendo la misma ampliamente narrativa. Como consecuencia, alguna de sus partes, tales como la descripción del establecimiento de una conexión bandabase, son ambiguas y difíciles de entender. Por otra parte, el autor ha encontrado pocos trabajos que incluyen la aplicación de técnicas formales a las actividades de ingeniería de protocolos [1] asociadas a la tecnología Bluetooth. Uno de estos trabajos es el de Feldmann et al. [4], quien modela una *scatternet* Bluetooth completa usando las CPNs, para estudiar el rendimiento de la red. A diferencia de dicho trabajo, en este artículo, las CPNs, con la ayuda del software CPN Tools [11], son usadas para el modelado del procedimiento de establecimiento de una conexión bandabase en un dispositivo Bluetooth, con la finalidad de presentar de una forma clara y precisa dicho procedimiento. Adicionalmente, se realiza un análisis inicial de dicho modelo usando la técnica de espacio de estado, basado en las propiedades generales de las CPNs.

Hay varias razones para usar CPNs para modelar y analizar Bluetooth. Las principales se resumen a continuación. Las Redes de Petri son una técnica madura. Eso se puede observar en los miles de artículos de revistas e informes de investigación generados en más de 30 años de trabajo teórico y práctico. Las Redes de Petri son soportadas por un estándar internacional [5] y varios libros de texto [10][12]. Las Redes de Petri son una herramienta gráfica bien definida, que permiten el análisis formal.

Con la finalidad de alcanzar los objetivos planteados, este artículo está organizado de la siguiente manera. En la Sección II se da una breve introducción a Bluetooth haciendo énfasis en la descripción del procedimiento de establecimiento de una conexión bandabase. En la Sección III se describe el modelo del procedimiento de establecimiento de una conexión bandabase, mientras que en la sección IV se realiza un análisis de dicho modelo basado en las propiedades básicas de las CPNs [7]. Finalmente, la Sección V presenta las conclusiones, recomendaciones y trabajos futuros generados por este trabajo.

2 Bluetooth Wireless Technology

Bluetooth Wireless Technology [2] es una tecnología de radio frecuencia (*Radio Fraquency*, *RF*) que ofrece conectividad a corta distancia para equipos personales, portables, PDAs, entre otros. Bluetooth está orientado al reemplazo de interfaces tradicionales, tales como RS-232 y conectores propietarios, proporciona una interfaz uniforme para acceder servicios de voz y datos, proporciona acceso a una red de área amplia usando un gateway personal, tal como un teléfono celular, y proporciona una comunicación sin infraestructura, que se puede usar para el soporte a grupos colaborativos (reuniones, conferencias).

2.1 Pila de Protocolos

La especificación de Bluetooth [3] incluye una especificación del núcleo que describe los detalles de los diversos protocolos que conforman la pila de protocolos; y una especificación de perfiles que incluye los detalles del uso de la tecnología para soportar varias aplicaciones e indica cuales de los aspectos de la especificación del núcleo son obligatorios, opcionales y no aplicables. La Figura 1 muestra la pila de protocolos que conforman el estándar. La misma divide los protocolos en los siguientes niveles:

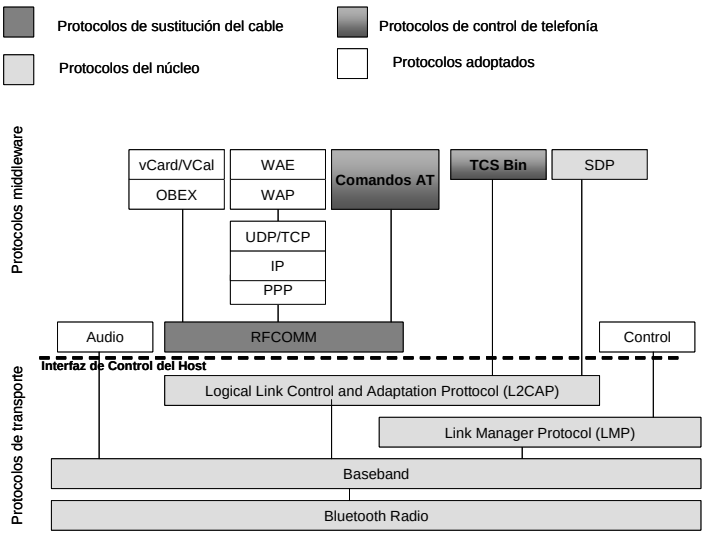

Figura 1: Pila de Protocolos de Bluetooth.

a) **Protocolos fundamentales de Bluetooth (protocolos del núcleo):** son específicos de Bluetooth y han sido desarrollados por el *Grupo de Interés Especial* (*Special Interest Group, SIG)* de Bluetooth.
b) **Protocolos de sustitución de cable:** suministran señalización de control que emulan el tipo de señalización que se asocia usualmente con los enlaces de cable
c) **Protocolos de control de telefonía:** definen la señalización de control de llamada para establecer llamadas de voz y datos con dispositivos Bluetooth. También define un protocolo (Comandos AT) que especifica como puede controlarse un MODEM y un teléfono móvil.
d) **Protocolos adoptados:** son protocolos existentes que se utilizan para diversos fines en las capas superiores.

2.2 Protocolos Fundamentales

La especificación de Bluetooth establece el uso de la frecuencia de 2.4 GHz (más específicamente la banda de frecuencia en la mayoría de países es de 2.4 – 2.4835 GHz). Definiéndose 79 canales físicos de 1 MHz sobre esta banda, siendo la tasa de transmisión es de 1 Mbps.

En Bluetooth, una *piconet* es una colección de dispositivos que pueden comunicarse. La *piconet* se forma de una forma ad hoc y contiene un dispositivo maestro y a lo sumo 7 dispositivos esclavos. Adicionalmente, un dispositivo en una *piconet* puede ser parte de otra *piconet* (como maestro o esclavo). Esta especie de solapamiento se conoce como *scatternet*.

La transmisión de la señal ocurre usando una técnica de saltos de frecuencia elegidos de forma aleatoria, entre los 79 canales físicos de 1 MHz. Ya que la tasa de salto es de 1600 saltos / seg cada canal es ocupado por 0,625 ms. Este período es llamado *slot*. Los *slots* están numerados secuencialmente. Adicionalmente, los dispositivos (radios) se comunican usando *Time Division Duplex (TDD)* [13], donde la data es transmitida en una dirección a la vez y la transmisión se alterna entre las dos direcciones. La frecuencia de salto es determinada por el maestro.

Existen dos tipos de enlaces que se pueden establecer entre el maestro y un esclavo: uno *Sincrono Orientado a Conexión (SCO)* para el tráfico con restricciones de tiempo (audio), donde se reserva un ancho de banda fijo en una conexión punto-a-punto (M/E) a intervalos regulares de tiempo. El maestro reserva *slots* (en pares, uno por cada dirección). El otro es el *Asíncrono no Orientado a Conexión (ACL)* y está destinado a tráfico de mejor esfuerzo sin ninguna restricción de tiempo. La comunicación se realiza en *slots* no reservados para el tráfico SCO.

La operación de Bluetooth se basa en el establecimiento de una conexión, gestión de la conexión y desconexión. El establecimiento de una conexión es explicado en la Sección 2.3. Una vez conectado un dispositivo puede estar en varios estados: un estado activo donde participa en una *piconet*. En este estado escucha, transmite y recibe paquetes; un estado de husmeo (s*niff*) donde escucha en *slots* específicos; un estado de sostenido (*hold*) que es un estado de potencia reducida, donde aun puede participar en el intercambio de paquetes SCO; y un estado de estacionado (*park*) donde no participa en la *piconet*, pero es retenido como parte de ella. Finalmente, el dispositivo puede desconectarse en cualquier momento.

Bluetooth establece ciertos mecanismos de seguridad [3][9]. Uno es la *autenticación* que tiene como finalidad verificar identidades de las unidades involucradas en el procedimiento. Y el otro es el *cifrado* donde la información del usuario puede ser protegida cifrando el paquete; sin embargo, el código de acceso y el encabezado del paquete nunca se cifran.

Adicionalmente a las capas anteriores, existen dos protocolos más que conforman los protocolos fundamentales de Bluetooth. El primero es el *Manejador del Enlace (Link Manager Protocol, LMP)*, que es el encargado de gestionar diversos aspectos del enlace de radio entre el maestro y el esclavo. Se entiende por enlace la conexión física establecida entre los dispositivos. El otro es el L2CAP, el cual es un protocolo de la capa de enlace entre entidades con un número de servicios. Esta capa confía en los protocolos de las capas más bajas para el control de error y flujo y hace uso de los enlaces ACL pero no soporta enlaces SCO.

2.3 Establecimiento de una Conexión Bandabase

La Figura 2 muestra el diagrama de transición de estados involucrados en el establecimiento de una conexión bandabase, el cual ha sido tomado de la especificación de Bluetooth [3]. Dichos estados se agrupan en estado de Prevenido (*Standby*), estado de Indagación (*Inquiry*), estado de *Page* y estado de Conexión (*Connection*). El estado de *standby* es el estado inicial en que se encuentra un dispositivo el cual no ha establecido una conexión. En el estado de *inquiry*, un dispositivo colecta información acerca de otros dispositivos cercanos para obtener información básica, tal como la dirección Bluetooth del dispositivo y valores del reloj. Esta compuesto por varios sub estados; el de *inquiry*, ejecutado por el potencial maestro y los estados de *inquiry scan* y *inquiry response* ejecutados por los potenciales esclavos.

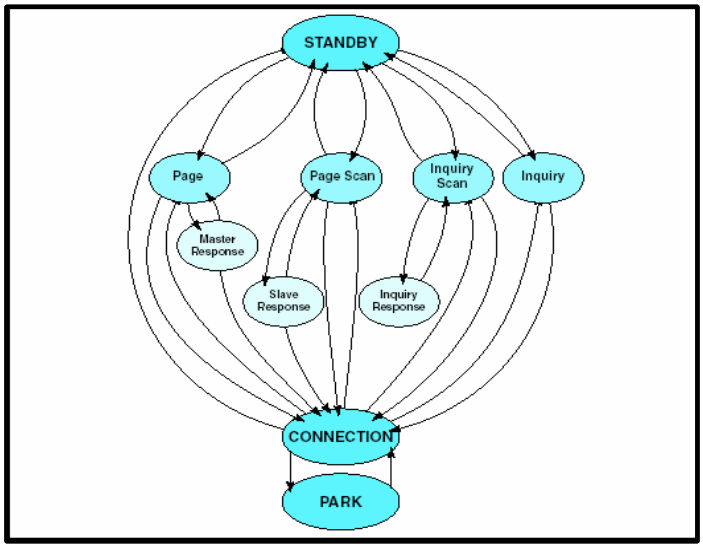

Figura 2: Diagrama de transición de estados del establecimiento de una conexión bandabase.

En el sub estado de *inquiry*, un potencial maestro transmite paquetes de indagación los cuales son recibidos por los esclavos en el sub estado de *inquiry scan*. Ya que durante el procedimiento de establecimiento de una conexión bandabase, los roles del maestro y del esclavo no están definidos, se denomina un *potencial maestro* aquel dispositivo que inicia un proceso de indagación destinado a establecer una conexión. En el sub estado de *inquiry scan*, un dispositivo busca mensajes de *inquiry* enviados por un potencial maestro. Una vez recibido un mensaje de *inquiry* un potencial esclavo debe entrar al estado de *inquiry response*.

En el estado de *page*, un dispositivo invita a otro a juntarse a su *piconet*. Similarmente al estado de indagación, el estado de *page* está compuesto por varios sub estados. Los sub estados de *page* y *master response* los cuales son ejecutado por el potencial maestro y los de *page scan* y *slave response* ejecutados por los esclavos. En el sub estado de *page*, un maestro activa y puede conectarse a un esclavo que esta en el sub estado de *page scan*. Un esclavo entra en el sub estado de *slave response* cuando recibe un mensaje de *page*. En este estado el esclavo espera recibir un mensaje de *master response*. Después de recibir dicho mensaje, responde con otro mensaje y entra al estado de *connection* (es decir, está conectado con el dispositivo maestro). En el sub estado de *page scan*, el esclavo escucha por mensajes de *page* del esclavo. Un maestro entra en el estado de *master response* una vez recibido un mensaje de *page response* del esclavo. El maestro transmite un paquete conteniendo la información necesaria para que el esclavo pueda entrar en el estado de *connection*. Una vez que recibe una respuesta del esclavo, el maestro puede entrar al estado de *connection*. El estado de *park* fue descrito anteriormente.

2.4 Perfiles de Bluetooth

Los perfiles de Bluetooth definen los protocolos y las características que soporta un *modelo de uso*. Un modelo de uso es un conjunto de protocolos que implementan una aplicación particular basada en Bluetooth. Los perfiles se pueden dividir en [9]: generales y específicos. Entre los perfiles generales se encuentra el perfil de acceso genérico que define los procedimientos genéricos para descubrir dispositivos Bluetooth y aspectos relacionados a la gestión de enlace para dispositivos que están estableciendo una conexión. El perfil de puerto serial establece como deben configurarse los dispositivos Bluetooth para emular una conexión serial usando RFCOMM. RFCOMM permite que las aplicaciones que han sido diseñadas e implementadas para operar sobre cables seriales corran sobre Bluetooth sin ser modificadas. El perfil de aplicación de descubrimiento de servicios describe como un dispositivo puede descubrir servicios registrados en otros dispositivos Bluetooth, al igual que otra información acerca de estos servicios. El perfil genérico de intercambio de objetos define como los objetos pueden ser intercambiados usando el protocolo OBEX [13].

Se han definido varios perfiles específicos [7], entre ellos se encuentran el perfil de transferencia de archivos que ofrece la capacidad de transferir objetos de datos de un dispositivo a otro, tales como una hoja de cálculo, presentaciones, imágenes. El perfil de acceso a una red de área local le permite a un dispositivo Bluetooth acceder a una LAN, tal como si estuviera conectado a la red. El perfil de sincronización define los requerimientos de la aplicación para los dispositivos Bluetooth para el soporte del modelo de uso de sincronización. Otros perfiles se encuentran descritos en [3][9].

3 Modelo CPN del Establecimiento de una Conexión Bandabase

En la especificación de Bluetooth no se describen claramente las transiciones entre los estados mostradas en la Figura 2. A continuación se presenta un modelo del establecimiento de una conexión bandabase basado en la interpretación del autor de dicha especificación [3] y en la descripción dada en [8]. El modelo es creado usando las *Redes de Petri Coloreadas* (*Coloured Petri Nets, CPNs*) con la ayuda de *CPN Tools* versión 1.2.0 [11].

3.1 Alcance

La especificación bandabase de Bluetooth es compleja [3]. Por lo cual se ha tomado una aproximación incremental para la realización del modelo del establecimiento de una conexión bandabase. En este artículo, se presenta una versión inicial del mismo que incluye el procedimiento realizado localmente, es decir, en un dispositivo que tiene instalado Bluetooth. Adicionalmente, el modelo se limita al establecimiento de una conexión entre un maestro y un solo esclavo. Aunque las CPNs soportan el modelado de las restricciones temporales, en esta versión del modelo ellas han sido omitidas. Esto es porque inicialmente solo se está interesado en la especificación funcional de todas las transiciones mostradas en la Figura 2.

3.2 Modelo Jerárquico

Similarmente a otros modelos de protocolos de comunicación complejos (tales como el presentado en [14]), en este trabajo se utilizan los constructores jerárquicos de las CPNs [7]. Las jerarquías se construyen usando la noción de una *transición de sustitución*, la cual puede ser considerada como una macro expansión. El modelo se inicia con un diagrama CPN en el nivel superior, el cual proporciona una visión general del sistema que esta siendo modelado y su ambiente. En las CPNs jerárquicas, este diagrama en el nivel superior contendrá un número de transiciones de sustitución. Cada una de estas transiciones de sustitución es refinada en otro diagrama CPN, el cual puede a su vez contener transiciones de sustitución. El diagrama en el nivel superior y cada una de la transiciones de sustitución es definida por un modulo, denominado *página*.

3.3 Declaración Global

En el modelo presentado en este trabajo, también se incluye una Declaración Global. Esta define las declaraciones requeridas por las inscripciones CPN. La Figura 3 muestra los conjuntos de colores (tipos) y variables de la declaración global. Los colores BOOL e INT representan los tipos boolean y entero, respectivamente, presentes en otros lenguajes de programación. El color STATE es del tipo enumerado y representa los estados en que un dispositivo intentando establecer una conexión bandabase puede estar. Estos estados fueron explicados en la Sección 2.3. El color TYPE es un enumerado y representa los tipos de paquetes involucrados en el intercambio de mensajes entre maestro y esclavos que están intentando establecer una conexión. El color AC es también un tipo enumerado y contiene el parámetro de control de acceso usado para identificar dispositivos durante el establecimiento de una conexión [3]. El color PACKET es el producto del tipo TYPE y AC y representa un paquete bandabase. El color IND es un enumerado con un solo valor usado para controlar ciertas acciones en el modelo. Las demás declaraciones corresponden a variables (var) usadas en el modelo.

```
color INT = int;
color BOOL = bool;
color STATE = with STANDBY| INQUIRY|INQUIRYSCAN|INQUIRYRESPONSE|
                  PAGE|PAGESCAN|MASTERRESPONSE| SLAVERESPONSE| CONNECTION;
color TYPE = with ID|FHS|POLL;
color AC = with IAC|DAC|NLL;
color PACKET = product TYPE * AC;
color IND =with  NONE1;
var state: STATE;
var prevstate: STATE;
var anypacket: TYPE;
var state2: STATE;
var packettype: TYPE;
var par: AC;
```

Figura 3: Declaraciones globales.

3.4 Página de Establecimiento de una Conexión Bandabase

La jerarquía CPN del modelo del establecimiento de una conexión bandabase consiste de tres (3) páginas. La página en el nivel superior se muestra en la Figura 4, e incluye una transición de sustitución para el procedimiento de establecimiento de la conexión que se realiza en el maestro (MASTERCONNSETUP) y otra para el que se realiza en el esclavo (SLAVECONNSETUP), las cuales son definidas en sus propias páginas. Una transición de sustitución es identificada por una etiqueta en la esquina inferior izquierda con el nombre de la página asociada a dicha transición. Las páginas en el nivel inferior describen las acciones para pasar de un estado del establecimiento de la conexión a otro. La elipse, DEVSTATE, es una *plaza* CPN y tiene asociado el tipo STATE definido en la Figura 3. Ella representa los estados del establecimiento de una conexión bandabase en los cuales un dispositivo puede estar. Las plazas TONETWORK y FROMNETWORK son del tipo PACKET y representan los paquetes bandabase que viajan hacia la red o vienen de la red, respectivamente. Las plazas y transiciones de sustitución están conectadas por *arcos*, los cuales indican el tipo de data requerida o producida por las transiciones de sustitución.

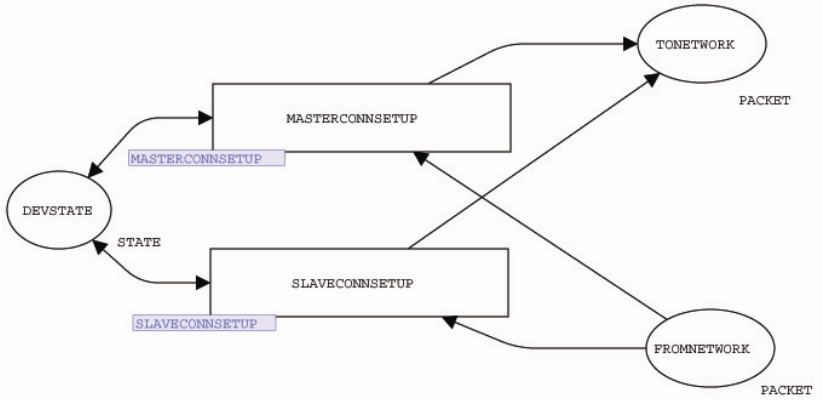

Figura 4: Página del nivel superior del modelo CPN del establecimiento de una conexión bandabase.

3.5 Página de Establecimiento de una Conexión en el Maestro

La Figura 5 muestra la página de establecimiento de una conexión en el maestro. La misma incluye once (11) transiciones, las cuales representa las acciones para pasar de un estado a otro. La transición INQUIRING modela las acciones a través de las cuales el maestro colecta información de otros dispositivos Bluetooth cercanos, a través de la transmisión de paquetes ID enviados periódicamente. Un dispositivo sale del estado de INQUIRY, INQUIRYABORT, cuando el Manejador de Recursos de Bandabase decide que hay suficientes número de respuestas de los esclavos, cuando se ha alcanzado un *timeout* (*inquiryTO*) o cuando el procedimiento es cancelado por el host [3]. En dicho caso el dispositivo debe retornar al estado desde el cual entró al estado de INQUIRY y el cual es almacenado en la plaza PREVSTATE.

La transición PAGING modela las acciones ejecutadas por el (potencial) maestro, destinadas a activar y conectarse a un esclavo. Un dispositivo sale del estado de PAGE, PAGINGTO, cuando un *timeout* (*pageTO*) es excedido [3]. En cuyo caso debe retornar al estado en el cual se encontraba cuando inicio el procedimiento de PAGING y el cual está almacenado en la plaza PREVSTATE. Si estando en el estado de PAGE, el maestro recibe una respuesta del esclavo, se debe cambiar al estado de MASTERRESPONSE y enviar un paquete FHS con ciertos parámetros necesarios para el establecimiento de la conexión posteriormente; esto es modelado por la transición MARRESPONSE. En este modelo, estos parámetros han sido ignorados porque no son necesarios para modelar las transiciones entre estados. El maestro debe mantenerse enviado paquetes FHS, lo cual es modelado por la transición MASTERRESPONDING. El maestro ejecuta esta acción, hasta que un *tinmeout* (*pagerespTO*) es excedido, modelado por MARRESPONDINGTO, o una segunda respuesta del esclavo, es decir, un paquete ID, con un código de acceso DAC, es recibido. En este último caso, el maestro ejecuta las acciones para finalmente establecer una conexión y las cuales son representadas por la transición CONNECTING. El maestro entonces se cambia al estado de CONNECTION. El maestro envía su primer paquete de tráfico denominado POLL al esclavo. Luego el maestro debe esperar una respuesta del esclavo, representada por un paquete de cualquier tipo. Con la finalidad de evitar una explosión de estados innecesaria durante el análisis del modelo, se utiliza un paquete del tipo POLL. La transición ANSWERRECIEVED modela la recepción de este paquete por parte del maestro. Si el maestro no recibe este paquete en cierto tiempo (*newconnectionTO*) [3], debe retornar al estado de PAGE. Esto es modelado por la transición NOSLVANSWER. Finalmente, el maestro puede desconectarse, DISCONNETING, e ir al estado de STANDBY en cualquier momento.

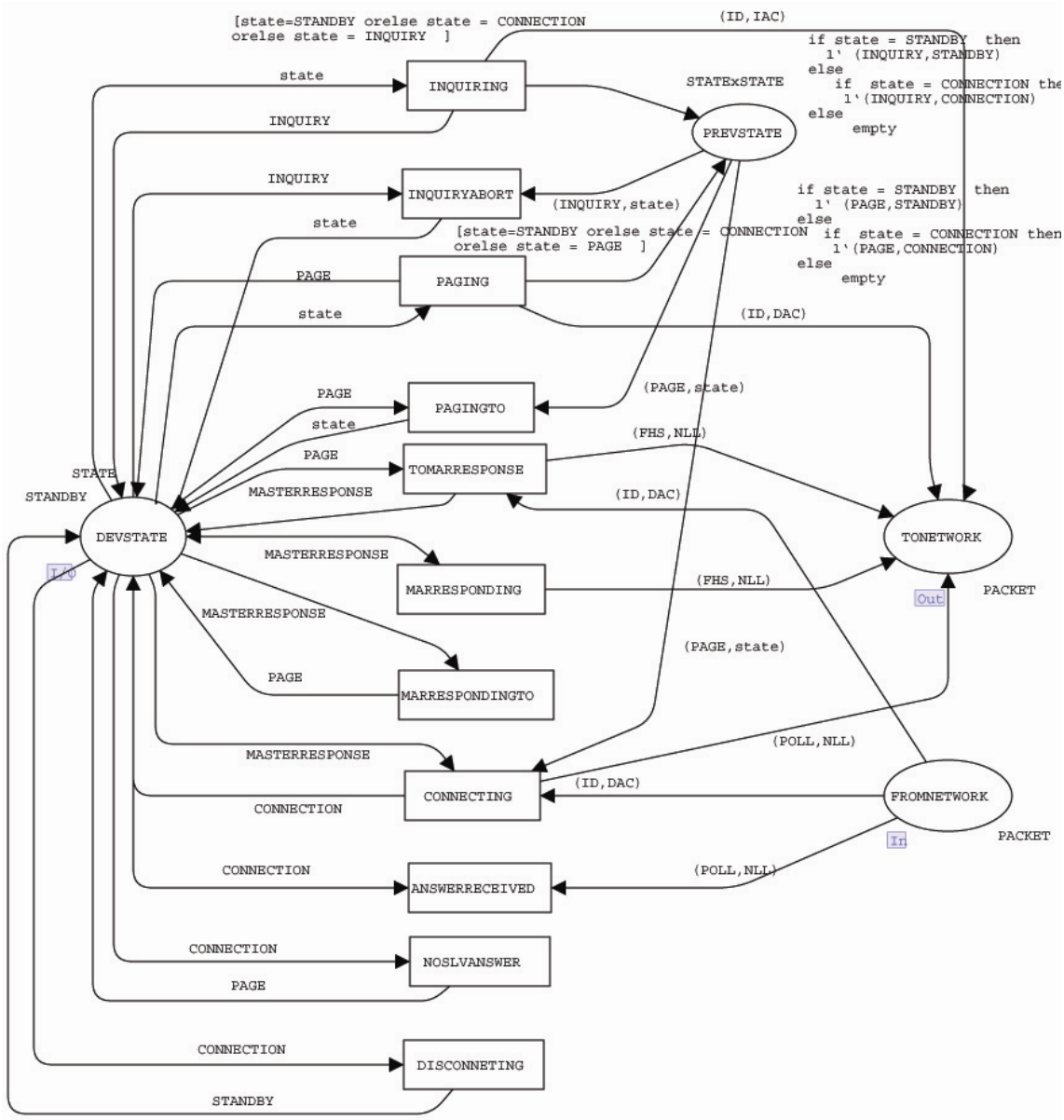

Figura 5: Página de establecimiento de una conexión en el maestro.

3.6 Página de Establecimiento de una Conexión en el Esclavo

La Figura 6 muestra la página de establecimiento de una conexión en el esclavo. La misma incluye doce (12) transiciones. La transición INSCANNING modela las acciones ejecutadas por un esclavo destinadas a buscar paquetes de *inquiry* (paquetes ID) enviados por el maestro. Un esclavo puede salir del estado de INQUIRYSCAN una vez finalizado el período de *scan*; esto es modelado por la transición INSCANEXIT. La transición INRESPONDING modela las acciones ejecutadas por un esclavo una vez que recibe un paquete de *inquiry*, paquete ID, del maestro. En este caso el maestro envía un paquete FHS al maestro y se cambia al estado de INQUIRYRESPONSE. Desde que un problema de contención puede ocurrir cuando varios dispositivos esclavos tratan de responder los paquetes de *inquiry* enviados por el potencial maestro, la especificación establece un procedimiento para aliviar este problema [3]. Este procedimiento dispone que el esclavo debe retornar al estado de STANDBY o CONNECTON dependiendo del caso, pasando a través del estado de *inquiry scan*, por cierto tiempo calculado de forma aleatoria (ver [3]). Cabe destacar que la especificación dice que el dispositivo debe pasar a través del estado de *page scan* (ver Sección 8.4.3 de [3]). Esto contradice el diagrama de la Figura 2, por lo cual el autor deduce que existe un error de trascripción en la especificación. Lo correcto debería ser que el dispositivo debe pasar a través del estado de *inquiry scan*, tal como se ha asumido en este trabajo. Esto es modelado por la transición GOTOINQSCAN.

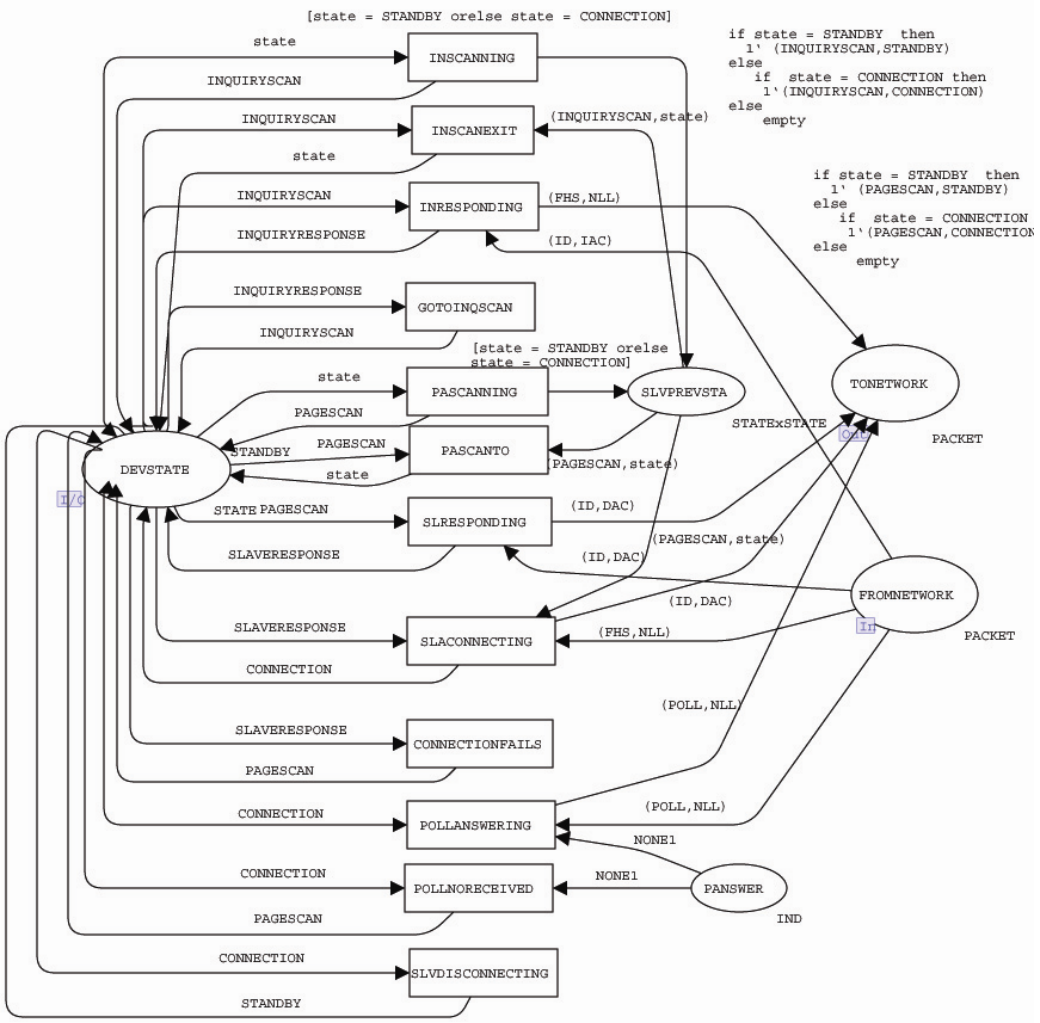

Figura 6: Página de establecimiento de una conexión en el esclavo.

Un dispositivo esclavo en el estado de STANDBY o CONNECTION puede cambiar al estado de PAGESCAN con la finalidad de escuchar por paquetes de *page scan* (es decir, paquetes ID) enviados por el maestro en el estado de PAGE y tratar así de establecer una conexión de forma exitosa. Esto es modelado por la transición PASCANNING. Una vez recibido el paquete de *page* enviado por el maestro (ver Sección 3.5), es decir, el paquete del tipo ID, el esclavo entra el estado SLAVERESPONSE y le responde al maestro con un paquete ID. Esto es modelado por la transición SLRESPONDING. Después de cierto tiempo, sin recibir ningún paquete de *page* del maestro, el esclavo retorna al estado de STANDBY o CONNECTION desde el cual entró al estado de PAGE y el cual esta almacenado en la plaza SLVPREVSTATE. Esto es modelado por la transición PASCANTO.

Si el esclavo recibe un paquete te FHS enviado por el potencial maestro en el estado MASTERRESPONSE (ver Sección 3.5), el esclavo entra en el estado de CONNECTION y realiza varias acciones modelas por la transición SLACONNECTING. El esclavo también envía una respuesta al maestro (un paquete del tipo ID). Si, por el contrario, no se recibe ningún paquete del tipo FHS durante cierto tiempo la conexión ha fallado, CONNECTIONFAILS, y el esclavo debe retornar al estado de PAGESCAN.

Si la conexión es exitosa, es decir el esclavo está en el estado de CONNECTION, el mismo debe responder al mensaje de POLL enviado por el maestro (ver Sección 3.5). Como se dijo anteriormente, el esclavo puede contestar con cualquier paquete, pero en este trabajo, a fin de simplificar el análisis del modelo, se asume que el maestro responde con un paquete del tipo POLL. Esto se modela con la transición POLLANSWERING. En caso contrario, el mensaje de POLL no es recibido o no es contestado, entonces el esclavo debe retornar al estado de PAGESCAN, tal como es modelado por la transición POLLNORECEIVED. Similarmente al maestro, un esclavo puede desconectarse en cualquier momento, retornando al estado de STANDBY; lo cual es modelado por la transición SLVDISCONNECTING.

4 Simulación y Análisis

Se usó CPN Tools versión 1.2.0 [11] para simular y analizar el modelo CPN. El modelo es analizado generando el *espacio de estado* o *Grafo* de *Ocurrencias* (*Occurrence Graph*, *OG*) y su correspondiente grafo de *Componentes Fuertemente Conectados* (*Strongly Connected Component*, *SCC*) [7]. CPN Tools corrió en una máquina con procesador Celeron de 1,8 GHZ y 512 de memoria RAM. El grafo de estado es usado para investigar algunas propiedades dinámicas de las CPNs [7], tales como acotamiento (*boundedness*), vivacidad (*liveness*) y propiedades locales (*home properties*), así como también para chequear al protocolo.

En esta fase inicial, el modelo del establecimiento de la conexión bandabase en el maestro es analizado independientemente del esclavo. Es decir, para fines del análisis se asume que una vez que un dispositivo inicia el procedimiento de establecimiento de la conexión como potencial maestro o esclavo no cambia su rol. Esto facilita el análisis del modelo y permite chequear si el modelo se adapta a la especificación.

El modelo CPN descrito en la Sección 3.5, genera un OG infinito debido a los paquetes periódicos (de *inquiry* y *page*) que envía el maestro, y al hecho de que las plazas de comunicación (FROMNETWORK y TONETWORK) no están acotadas. Así, se ha modificado el modelo usando una aproximación estándar [6][14], de forma tal que las plazas de comunicación tengan una capacidad finita. La Figura 7 muestra el modelo modificado del establecimiento de una conexión bandabase en el maestro. El paquete tipo SLOT ha sido incluido en el *color set* del tipo TYPE (ver Sección 3.3). Cada vez que se desea enviar un paquete debe existir suficiente capacidad en la plaza de comunicación TONETWORK; dicha capacidad viene determinada por el número de *tokens* (SLOT,NLL). Adicionalmente, se ha incluido la transición SENDPKT la cual modela el envío de un paquete a la red.

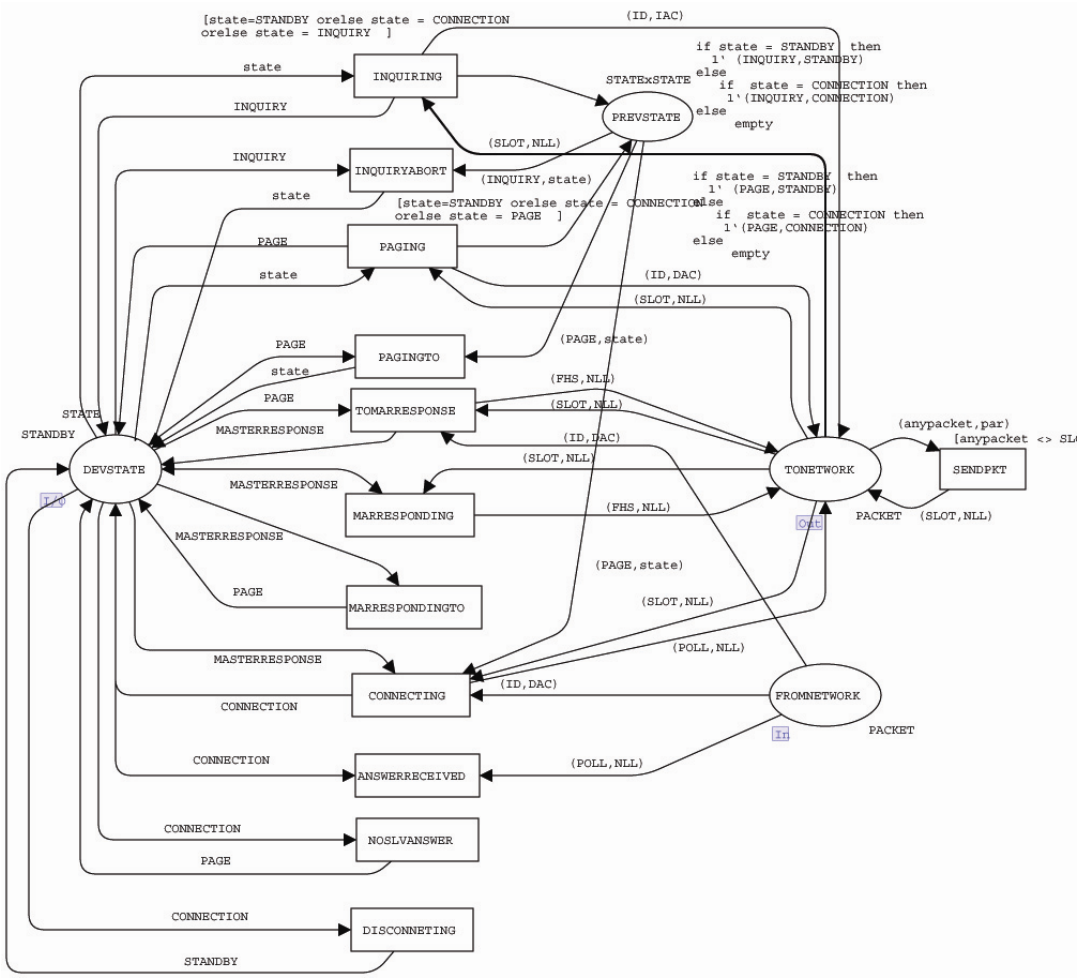

Figura 7: Página del establecimiento de una conexión en el maestro modificada.

4.1 Marcado Inicial

Un *marcado* de una plaza comprende un (*multi*) conjunto de valores (conocidos como *tokens* o marcas) tomadas del tipo de la plaza. El *marcado inicial* incluye la distribución de *tokens* en cada una de las plazas del modelo. A continuación se especifican los marcados iniciales usados para el análisis del modelo. Estos marcados permiten

analizar los eventos destinados al establecimiento (exitoso o no) de una sola conexión bandabase y estudiar así las transiciones de estados mostradas en la Figura 2. A fin de analizar el modelo de establecimiento de la conexión bandabase en el maestro, la plaza DEVSTATE es inicializada con el estado de STANDBY. La plaza TONETWORK acepta un máximo de dos paquetes, es decir es inicializada con dos *tokens* del tipo (SLOT,NLL) (es decir, 2`(SLOT,NLL)). La plaza FROMNETWORK es inicializada con 2`(ID,DAC)++1`(POLL,NLL), es decir dos paquetes del tipo ID y uno del tipo POLL enviados por el esclavo han llegado.

A fin de analizar el modelo de establecimiento de la conexión bandabase en el esclavo, la plaza DEVSTATE es inicializada con el estado de STANDBY. La plaza FROMNETWORK es inicializada con los siguientes valores de los *tokens*, 1`(ID,DAC)++1`(ID,IAC)++1`(FHS,NLL)++1`(POLL,NLL), es decir, dos paquetes del tipo ID, un paquete del tipo FHS y uno del tipo POLL, los cuales han sido enviados por el maestro con el cual este esclavo desea establecer una conexión. Note que en este caso el número de *tokens* de las plazas de comunicación no se incrementa infinitamente y por lo tanto no es necesario modificar el modelo para limitar la capacidad de las mismas.

4.2 Estadística del Grafo de Ocurrencia

Se generaron los reportes de estado completos para el análisis del modelo de establecimiento de la conexión bandabase en el maestro y en el esclavo. La información estadística que incluye el tamaño del OG y el grafo SCC se muestran en la Tabla 1. En ambos casos, se observa que hay menos nodos SCC que nodos OG, por lo cual se concluye que existen algunos ciclos en el modelo. Esto es esperado ya que tanto los procedimiento de indagación (*inquiry*) y de *page* ejecutados por un maestro y los procedimientos de *inquiry scan* y *page scan* ejecutados por el esclavo son periódicos. Esto con la finalidad del maestro de encontrar a los dispositivos cercanos y de los esclavos de escuchar por un potencial maestro para establecer una conexión.

El OG del establecimiento de una conexión bandabase en el maestro es más grande que el OG del esclavo. Esto es porque las acciones del esclavo están limitadas por los paquetes enviados por el maestro y en este caso se ha inicializado la CPN con el número mínimo de paquetes.

	Establecimiento de la Conexión Bandabase en el Maestro		**Establecimiento de la Conexión Bandabase en el Esclavo**	
Información estadística	**OG**	**Grafo SCC**	**OG**	**Grafo SCC**
Número de Nodos	209	47	46	22
Número de Arcos	579	207	74	26
Tiempo de cálculo (hh:mm:ss)	(00:00:01)	(00:00:01)	(00:00:01)	(00:00:01)

Tabla 1: Información estadística del espacio de estado.

4.3 Propiedades Generales

Las propiedades de acotamiento y vivacidad [7] son investigadas para validar y depurar el modelo y para estudiar el comportamiento del protocolo bandabase en lo que respeta al establecimiento de una conexión. Esta información es tomada del reporte de OG generada por CPN Tools [11].

4.3.1 Acotamiento

Las cotas enteras y las cotas de los multi-conjuntos son analizadas para las plazas del modelo. Esta información es resumida en la Tabla 2 . Las *cotas enteras superiores* describen el máximo número de *tokens* que pueden ocurrir en una plaza, mientras que las *cotas de los multi-conjuntos* indican que *tokens* pueden estar en una plaza [7]. La plaza DEVSTATE puede tener una máximo de un *token* ya que un dispositivo solo puede encontrarse en un estado en un momento dado. El valor de las cotas de los multi-conjuntos superiores indican todos los estados en que puede estar un maestro y un esclavo. Estos valores están acordes a lo explicado en la Sección 2.3 y a la especificación de Bluetooth [3]. El número máximo de paquetes que puede venir de la red (FROMNETWORK) es de tres (3) para el caso del maestro y cuatro (4) para el caso del esclavo. Estos valores se corresponden con el estado inicial de estas plazas (ver Sección 4.1). El número máximo de paquetes que pueden ser enviados a la red (TONETWORK) es de dos (2) en el caso del maestro, ya que esta plaza ha sido acotada para hacer el OG finito. Aunque el maestro puede enviar múltiples paquetes ID, el número de paquetes FHS y POLL que puede enviar está limitado por la cantidad de paquetes de respuesta enviados por el esclavo y establecidos en el marcado inicial (ver Sección 4.1). El número máximo de paquetes que un esclavo puede enviar a la red (TONETWORK) es de cuatro (4). Esta cantidad de paquetes está determinada por el marcado inicial de la plaza FROMNETWORK, el cual solo permite que se establezca una conexión. La plaza PREVSTATE puede contener un número máximo de un *token*, que indica el estado previo, de STANDBY o CONNECTION, en el que un dispositivo maestro se encontraba antes de ejecutar los procedimientos de *inquiry* y *page*. Todos estos estados pueden ser alcanzados como es esperado. La plaza

PANSWER es de control y por lo tanto no es relevante para el análisis. Finalmente, la plaza SLVPREVSTATE puede contener un número máximo de un *token*, que indica el estado previo, de STANDBY o CONNECTION, en el que un dispositivo esclavo se encontraba antes de ejecutar los procedimientos de *inquiryscan* y *pagescan*.

	Establecimiento de la Conexión Bandabase en el Maestro		**Establecimiento de la Conexión Bandabase en el Esclavo**	
Plaza	**Cota Entera**	**Cota de los Multi-Conjuntos**	**Cota Entera**	**Cota de los Multi-Conjuntos**
DEVSTATE	1	1`STANDBY++ 1`INQUIRY++ 1`PAGE++ 1`MASTERRESPONSE++ 1`CONNECTION	1	1`STANDBY++ 1`INQUIRYSCAN++ 1`INQUIRYRESPONSE++ 1`PAGESCAN++ 1`SLAVERESPONSE++ 1`CONNECTION
FROMNETWORK	3	2`(ID,DAC)++ 1`(POLL,NLL)	4	1`(ID,IAC)++1`(ID,DAC)++ 1`(FHS,NLL)++1`(POLL,NLL)
TONETWORK	2	2`(ID,IAC)++2`(ID,DAC)++ 2`(FHS,NLL)++ 1`(POLL,NLL)++ 2`(SLOT,NLL)	4	2`(ID,DAC)++ 1`(FHS,NLL)++ 1`(POLL,NLL)
PREVSTATE	1	1`(INQUIRY,STANDBY)++ 1`(INQUIRY,CONNECTION)++ 1`(PAGE,STANDBY)++ 1`(PAGE,CONNECTION)	.	.
PANSWER	-	-	1	1`NONE1
SLVPREVSTA	-	-	1	1`(INQUIRYSCAN,STANDBY)++ 1`(INQUIRYSCAN,CONNECTION)++ 1`(PAGESCAN,STANDBY)++ 1`(PAGESCAN,CONNECTION)

Tabla 2: Cotas superiores de las plazas del modelo.

4.3.2 Propiedades Locales y de Vivacidad

La Tabla 3 muestra las propiedades locales y de vivacidad. Un marcado muerto (*dead marking*) es un marcado sin elementos de asociación habilitados, es decir, ninguna transición puede ocurrir a partir de dicho marcado. En el modelo del establecimiento de una conexión en el maestro, no hay marcados muertos, ya que la transición PAGING esta viva. Un transición esta *viva* si puede ocurrir al menos una vez en una secuencia de ocurrencias para cada marcado de la red que es alcanzable desde el marcado inicial. Un *marcado local* (*home marking*) es un marcado que puede ser siempre alcanzado por el resto de los marcados alcanzables. No hay marcados locales. Todas las transiciones del modelo deberían estar vivas y un marcado inicial que indique que el dispositivo se inicia en el estado de STANDBY y que no hay paquetes en las plazas de comunicación debería ser el marcado local. Sin embargo, como el modelo presentado en este trabajo no incluye el intercambio de paquetes entre el maestro y los esclavos, la ocurrencia de las transiciones está sujeta al marcado inicial de las plazas de comunicación. Una *transición muerta* es aquella que no está habilitada en ningún marcado alcanzable [7]. El reporte del espacio de estado generado por CPN Tools muestra que no hay transiciones muertas. Esto es esperado ya que no debería haber "código muerto" en la especificación.

En el modelo del establecimiento de una conexión en el esclavo hay dos (2) marcados muertos. Ellos fueron analizados usando las facilidades provistas por CPN Tools [11]. Ellos se corresponden con los marcados donde el dispositivo está en el estado de PAGESCAN y no hay mas paquetes enviados por el maestro en la plaza FROMNETWORK para que alguna de las transiciones este habilitada. Esto ocurre porque el modelo presentado en este trabajo no incluye el intercambio de paquetes entre maestros y esclavos a través de la red y la ocurrencia de varias transiciones está sujeta al marcado inicial de las plazas de comunicación. Debido a esta razón tampoco existen transiciones vivas y marcados locales. El reporte del espacio de estado generado por CPN Tools muestra que no hay transiciones muertas. Esto es esperado ya que, al igual que el caso del maestro, no debería haber "código muerto" en la especificación.

	Establecimiento de la Conexión Bandabase en el Maestro	Establecimiento de la Conexión Bandabase en el Esclavo
Marcados Muertos	Ninguno	[11] [40]
Marcados Locales	Ninguno	Ninguno
Transiciones Muertas	Ninguna	Ninguna
Transiciones Vivas	SNDPKT, PAGING	Ninguna

Tabla 3: Propiedades locales y de vivacidad.

5 Conclusiones

En este artículo, las CPNs han sido utilizadas para desarrollar un modelo inicial del establecimiento de una conexión Bluetooth a nivel del protocolo bandabase. Se ha modelado dicho procedimiento en un dispositivo, sin incluir el intercambio de paquetes a través de la red entre maestro y esclavos. Adicionalmente, los procedimientos en el maestro y en el esclavo fueron analizados de forma independiente. Ya que la especificación del procedimiento de establecimiento de una conexión bandabase es compleja, se ha seguido una aproximación incremental, a través de la cual se irán incluyendo más características y casos de estudios al modelo a fin de aumentar la confiabilidad de que el mismo está correcto.

La especificación del establecimiento de una conexión bandabase [3], similarmente a otras partes de la especificación Bluetooth, se caracteriza por ser poco clara y en algunos casos ambigua. Adicionalmente, y como se explicó anteriormente existen algunos errores de trascripción en la especificación. El modelo presentado en este trabajo define claramente, con la ayuda de un método formal, tal como los son las CPNs, el establecimiento de una conexión bandabase cuando el dispositivo actúa como maestro y cuando actúa como esclavo. El análisis inicial del modelo basado en el espacio de estado y las propiedades generales de una CPN muestra que los resultados son los esperados y el procedimiento de establecimiento de una conexión funciona acorde a lo especificado.

Los trabajos futuros comprenden el incluir el intercambio de paquetes entre un maestro y uno o más esclavos en una *piconet*. Adicionalmente, se desea analizar el modelo en función de ciertas propiedades específicas del protocolo bandabase usando técnicas tales como el chequeo de modelos (*Model Checking*). También, se desea incorporar tiempo al modelo de forma tal de realizar algunos análisis en términos de sincronización del maestro y los esclavos. Finalmente, se desea comparar los resultados obtenidos de la simulación del modelo con los obtenidos de pruebas reales usando equipos Bluetooth (con la ayuda de una herramienta de captura de paquetes Bluetooth) para conocer si la implementación está acorde a la especificación.

Referencias

[1] Billington J. *Formal Specification of Protocols: Protocol Engineering*. Encyclopedia of Microcomputers, Marcel Dekker, New York, 1991, Vol. 7, pp 299-314.

[2] Bisdikian C. *An Overview of the Bluetooth Wireless Technology*. IEEE Communications Magazine. December 2002. pp 86-95.

[3] Bluetooth SIG, Inc. *Specification of the Bluetooth System version 2.0*. November 2003.

[4] Feldmann S, Hartmann T, Kyamakya K. *Modeling and Evaluation of Scatternets Performance by using Petri Nets*. In Proceedings of the International Conference on Wireless Networks, ICWN '03, June 23 - 26, 2003, Las Vegas, Nevada, USA. CSREA Press 2003, ISBN 1-932415-03-3.

[5] ISO/IEC. *High-Level Petri Nets- Concepts, Definitions and Graphical Notation.* Final Draft International Standard ISO/IEC 15909, Version 4.6, ISO, October, 2000.

[6] Kristensen L.M., Christensen S., and Jensen K. *The practitioner's guide to coloured Petri nets*. International Journal on Software Tools for Technology Transfer, Springer, 1998, Vol. 2, Number 2, pp 98-132.

[7] Jensen K. *Coloured Petri Nets: Basic Concepts, Analysis Methods and Practical* Use. Vol. 1, 2 and 3. Springer-Verlag, 2nd edition, April, 1997.

[8] Millar B.A, Bisdikian C. *Bluetooth Revealed: The Insider's Guide to an Open Specification for Global Wireless Communications.* Prentice Hall (September 25, 2000).

[9] Muller N. *Tecnología Bluetooth*. McGraw-Hill Professional. España, 2002.

[10] Peterson J. *Petri Net Theory and Modeling of Systems*. Prentice-Hall, 1998.

[11] Ratzer A.V, Wells L, at el. *CPN Tools for Editing, Simulating, and Analysing Coloured Petri Net.* Lecture Notes in Computer Science, Volume 2679 / 2003, pp. 450 – 462.

[12] Reisig W. *Petri Nets: An Introduction*. Springer-Verlag. 1985.

[13] Stallings W. *Wireless Communications and Networks*. Prentice Hall. 2002.

[14] Villapol M.E. and Billington. *Analysing Properties of the Resource Reservation Protocol*. LNCS 2679, Springer, 2003, pp 377-396.