REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
TELEM@TICA
Revista Telem@tica. Vol. 13. No. 2, mayo-agosto, 2014, p. 22-31 ISSN 1729-3804

Método para la definición y verificación formal de protocolos para aplicaciones de control domótico

Arian Trujillo Díaz[1], José Raúl Vento Álvarez[2]

*[1]Universidad de Pinar del Río "Hermanos Saiz Montes de Oca". Ingeniero en Informática*arian@upr.edu.cu

[2]Dpto. de Telecomunicaciones. Facultad de Informática y Telecomunicaciones. Universidad de Pinar del Río. Doctor en Ciencias vento@tele.upr.edu.cu

RESUMEN / ***ABSTRACT***

Este artículo ofrece unmétodo para la elaboración de protocolos de aplicación de control domóticos, aplicados a un caso de estudio, utilizando herramientas de software libre, PROMELA como su lenguaje de definición formal, y SPIN como su editor, verificador y validador, mediante la simulación.

Palabras claves: Domótica, Ingeniería de Protocolos, Método, PROMELA, SPIN, Software Libre, Verificación, Validación

This article provides a method for developing application protocols automation control, applied to a case study, using free software tools, language PROMELA as its formal definition, and SPIN as its editor, verifier and validator, by simulating

.***Key words:*** *Home Automation, Engineering Protocols, Method, PROMELA, SPIN, Free Software, Verification, Validation*

INTRODUCCIÓN

El desarrollo acelerado de la producción de software ha hecho que la ingeniería de protocolos se desarrolle considerablemente. Sin embargo, un gran tropiezo en dicho desarrollo es el desconocimiento de la existencia de métodos de descripción formal y verificación de protocolos de red, que ayudan a la corrección, robustez y rendimiento al protocolo de comunicación que se desea aplicar. Por otra parte, en ocasiones, teniendo este conocimiento, se hace difícil asegurar estos aspectos, debido a que no se cuenta con las herramientas automatizadas correspondientes a estos métodos ya que están bajo licencias privativas y se carece de un método adecuado que guie el flujo de trabajo para lograr los objetivos deseados.

El objetivo de este artículo es presentar un método desarrollado por los autores, para la definición y verificación formal de protocolos para aplicaciones de control domótico. El método se apoya en mecanismos de descripción formal disponibles y herramientas de verificación, validación y simulación bajo licencia libre.

La definición formal depende de la herramienta que se usará para la verificación, además de la validación que se apoya con la simulación. Cinderella SDL[1] es una herramienta de modelado visual para el desarrollo de sistemas integrados de software, servicios de comunicaciones, protocolos, o cualquier tipo de sistema basado en mensajes. Telelogic TAU [2] también es un paquete de herramientas para el diseño y la implementación en tiempo real de software. Por otra parte SPIN [3] que permite la verificación de software multi-hilo, es compatible con un lenguaje de alto nivel para especificar las descripciones de los sistemas, llamado PROMELA. La herramienta SPIN comprueba la consistencia lógica de una especificación e informa sobre los bloqueos, las condiciones de carrera (competencia), diferentes tipos de lazos cerrados y suposiciones injustificadas sobre las velocidades relativas de los procesos.

Otros lenguajes de especificación formal fueron analizados, entre ellos los más destacados, ESTELLE y SDL. Ambos fueron descartados para el desarrollo del método propuesto porque sus herramientas de trabajo no son libres.

La verificación formal de protocolos es el proceso de examinar las especificaciones formales en la búsqueda de posibles errores que puedan afectar la operación del mismo. Estos métodos son usados para garantizar la seguridad y la confiabilidad en el diseño de protocolos.

En la investigación bibliográfica para este artículo se revisaron los resultados de aplicar mecanismos para la descripción formal, verificación o simulación de protocolos, donde mayoritariamente se realizaron con herramientas bajo licencias privativas y no cuentan con un método que agrupe todos estos mecanismos.

CASO DE ESTUDIO. PROTOCOLO LDPROT

LDPROT es un protocolo que trabaja en la capa de aplicación del modelo de referencia TCP/IP, protocolo propietario que funciona en la red de la Universidad de Pinar del Río. Está destinado a las aplicaciones de control y monitorización centralizada, en configuración punto-multipunto (donde en este caso el Controlador es el extremo centralizado “punto” y los Agentes en el extremo “multipunto”).

Se confeccionó para ser un protocolo punto a punto aunque su paradigma cliente-servidor posibilita que el servidor realice multidifusión o punto-multipunto. Es un protocolo orientado a conexión. Este protocolo es simple; de parada y espera que tiene un tamaño fijo de carga útil y está diseñado para la recuperación ante fallas.

Este protocolo se diseñó con el método propuesto en este artículo y será usado como caso de estudio durante el desarrollo de la explicación del método para una mayor comprensión del mismo.

METODO PROPUESTO

El diseño y estudio de protocolos de comunicación comprende varias etapas, entre las que se encuentran requisitos de usuario, su análisis cuantitativo y cualitativo, su realización práctica y documentación. El primer aspecto, la definición del protocolo, es de suma importancia, ya que es el punto de partida de un largo proceso el cual se describe en la Figura 1.

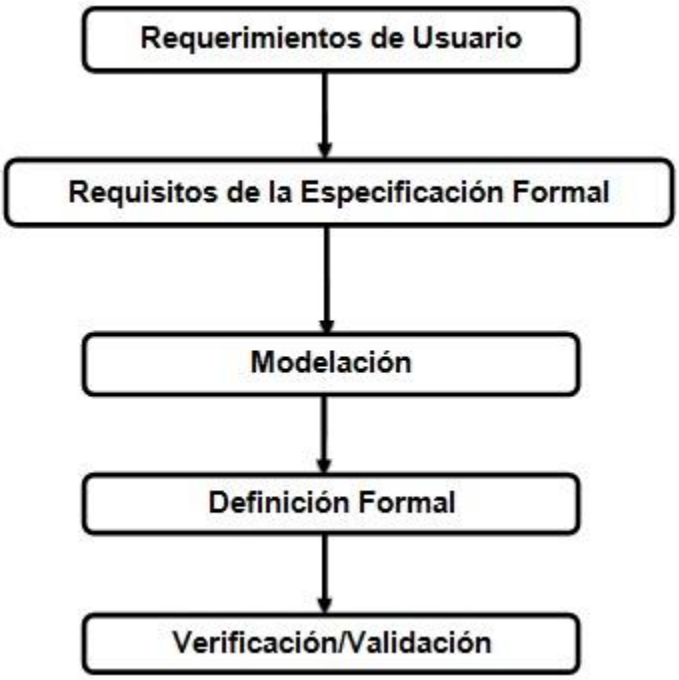

Figura 1. Método de desarrollo.

REQUERIMIENTOS DE USUARIO

Los requerimientos del protocolo deseado se conforman con el conjunto de necesidades que establece la comunicación, se describen con un lenguaje natural. Desde 1979, Hoffmann le confiere gran importancia a esta parte, aunque no deja de introducir ambigüedades propias del leguaje humano, con el consiguiente riesgo de interpretaciones distintas por parte de las personas encargadas de implementar el protocolo. Diversos autores han definido métodos formales para la definición de protocolos, para el estudio de sus características y basados en los siguientes aspectos:

- Nivel del modelo de referencia en el cual trabajará.
- Forma de delimitación de unidad de datos (trama, paquete, celda, etc.)
- Si debe tener capacidad de multidifusión, broadcast o solamente punto a punto.
- Si va a tener direccionado para encaminamiento final o multiplexación correspondientes al nivel del modelo de referencia en el cual trabaja.
- Si va a tener orientación a conexión o no, o ambas posibilidades.
- Para participar en conmutación, repetición o punto a punto.
- Si tiene direccionado, su alcance y procesamiento para accesar la entidad final.
- Longitud de la carga útil. Si será fija o variable.
- Si tendrá detección y corrección de errores, y si se aplicarán mecanismos de repetición automática sobre la base de confirmaciones y almacenamiento en ventanas deslizantes.
- Si se aplicarán mecanismos de control de errores hacia delante FEC.
- Si va a tener control de flujo o de congestión.
- Capacidad de recuperación frente a fallas.

Este paso ayuda a identificar las necesidades del protocolo a diseñar, como se explica en el protocolo LDPROT, donde se refiere, que haciendo uso de la red universitaria instaurada, funciona en la capa de aplicación del modelo de referencia TCP/IP.

El protocolo LDPROT destinado para aplicaciones de control y monitorización centralizada, aspecto que conlleva a definir otro requisito de usuario, funcionará bajo el paradigma cliente-servidor, posibilitando que el servidor realice multidifusión o punto-multipunto.

La necesidad de tener un mecanismo de control de errores en el protocolo, ayuda definir que la estructura de los datos en el protocolo, además de ser fija, tendrá dos campos de control, secuencia y el chequeo, como se muestra en la figura 2.

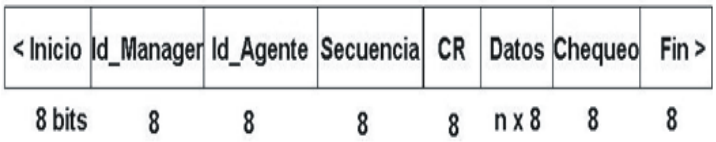

Figura 2. Unidad de datos del protocolo LDPROT

En este protocolo es necesario saber el estado de los agentes domóticos, para que la aplicación controladora pueda actualizar los estados y así poder enviar órdenes, este requisito hace definir que el protocolo sea simple y de parada y espera.

REQUISITOS DE LA ESPECIFICACIÓN FORMAL

Se realiza un análisis de los requerimientos de usuarios para hacer una transformación a los requisitos necesarios de la herramienta de modelación, paso importante para lograr una correcta interpretación y por consiguiente una modelación lo más exacta posible a lo deseado.

Tomando como análisis la carta de mensajes del protocolo LDPROT como se muestra en la figura 3 y teniendo como referencia la información obtenida de los requerimientos de usuario (paso anterior), en este paso sin llegar a especificar los detalles de modelación (paso posterior), se define con sé que modeló teniendo en cuenta las características del protocolo.

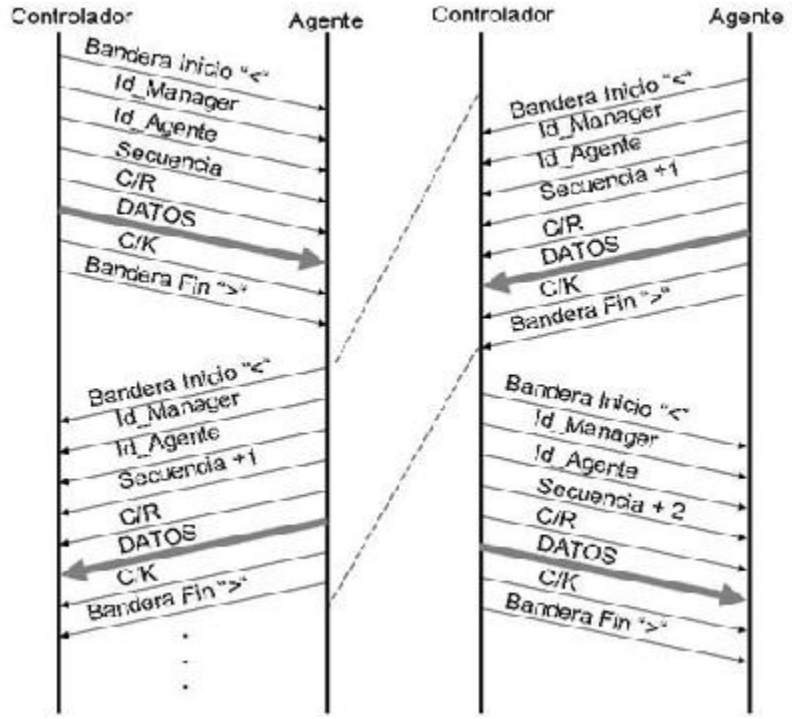

Figura 3. Carta de mensajes en el funcionamiento del protocolo LDPROT.

Los requerimientos de usuario reflejan que el protocolo LDPROT necesita ser un protocolo de parada y espera, donde cada espera estará determinada por las respuestas que son enviadas de ambos extremos de la comunicación.

Este paso ayuda a definir que el protocolo LDPROT es necesario modelarse con máquina de estado finitos, por lo expuesto en el párrafo anterior.

MODELACIÓN

En esta etapa se lleva todo el análisis realizado en las etapas anteriores a un modelo usando la tecnología adecuada según las características del protocolo. La modelación constituye un paso importante en el desarrollo del protocolo, siendo el primer paso de abstracción de los requerimientos de usuario deseados para ser llevados al análisis con herramientas de cómputo. Se puede realizar con máquina de estado finito o con redes de Petri.

Continuando el desarrollo del método sobre el protocolo LDPROT, en la figura 4 se muestra su modelación en una máquina de estado finito. Los estados S0 hasta S8 son los estados necesarios para analizar la información recibida, con la estructura como se muestra en la figura 1, que se definió en el primer paso del método aplicado a este protocolo.

La modelación obtenida en esta etapa es consecuente con los requerimientos de usuarios capturados al principio del método, por lo que resta pasar a la siguiente etapa del método donde se realiza la definición formal.

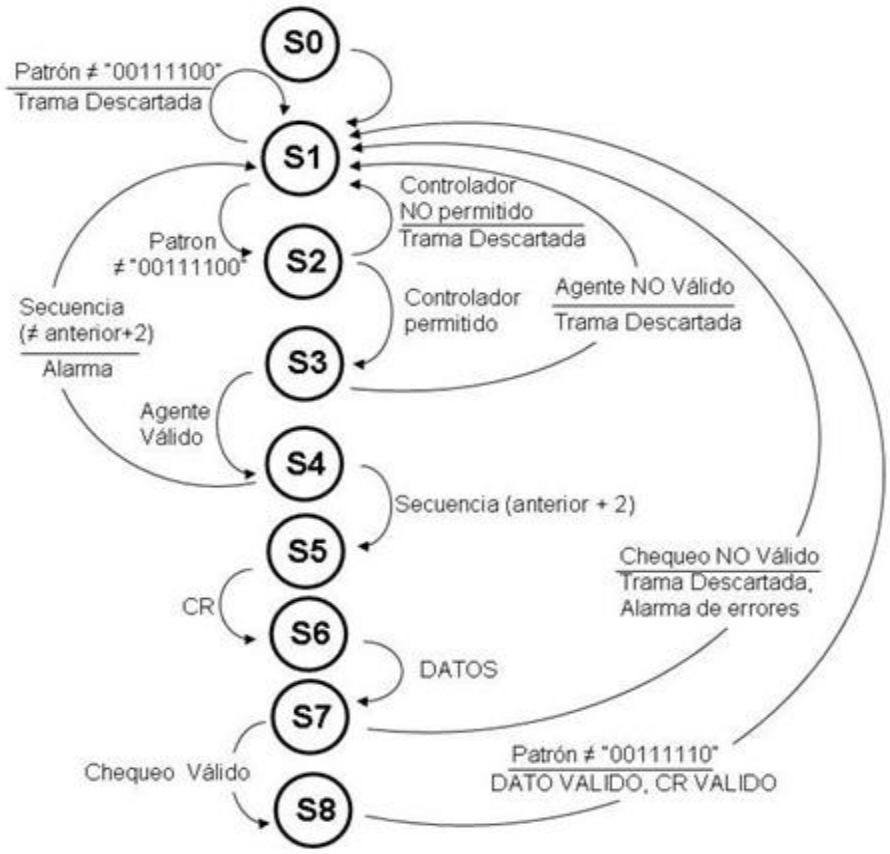

Figura 4. Máquina de estados finitos del protocolo LDPROT

DEFINICIÓN FORMAL

Esta etapa es cuando comienza a cambiar el lenguaje utilizado, pasando del lenguaje natural a un lenguaje de máquina. PROMELA es un lenguaje que permite escribir en código el resultado de la etapa de modelación utilizando también SPIN como editor.

PROMELA es una extensión de un lenguaje llamado ARGOS, que fue desarrollado en 1983 para la validación de protocolos. La validación de programas está definida directamente en términos de tres tipos de objetos en específico y estos son:

- Procesos.
- Canales de mensajes.
- Variables de estados.

Todos los procesos se definen como objetos globales, los cuales pueden contener variables y/o canales de comunicación, que representan datos que pueden ser locales o globales a un proceso. Las variables en PROMELA son usadas para almacenar, ya sea información global acerca del sistema como un todo, o como información que es local para un proceso en específico, dependiendo de dónde se haya localizada la declaración de la variable.

La figura 4 muestra el código escrito en PROMELA visualizado con SPIN, herramienta que en este paso del método se usa como editor.

Usando PROMELA, los datos que se necesitan enviar en la comunicación, como se refiere en la figura 2 se convierten en variables, la máquina de estado finito generada en el paso anterior, se convierte en un proctype, nombre que recibe el segmento de código donde se ejecutan todas las acciones deseadas, y se conforman los chan, término utilizado, para simular el canal de comunicación, entre los extremos de la comunicación.

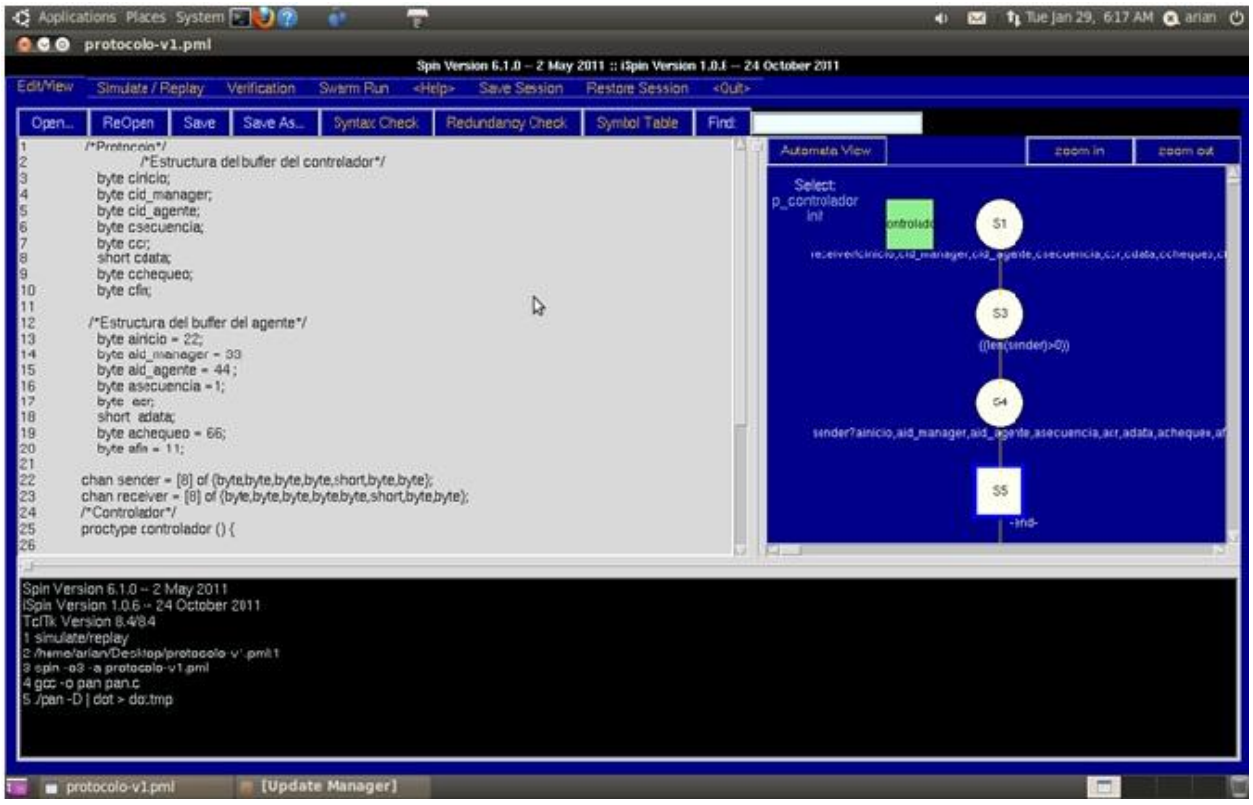

Figura 5. Editor SPIN para código PROMELA

SPIN como editor código PROMELA, tiene la capacidad de graficar la máquina de estado finito como se muestra en la parte derecha de la figura 5, generado con el código que se escribe en la parte izquierda

de dicha figura, permitiendo realizar una comprobación con la máquina de estado finito definida en el paso anterior.

Verificación/Validación

Al finalizar la especificación formal queda listo para la Verificación y Validación.

El método descrito debe permitir:

- Escribir especificaciones sin ambigüedad, claras, precisas y concisas.
- Analizar y corregir en su plenitud una especificación.
- Determinar si un diseño cumple con determinada especificación.
- Utilizar herramientas para crear, mantener, analizar y simular especificaciones.

Para validar y verificar el diseño realizado del protocolo es preciso llevar los requisitos de la especificación formal a un lenguaje que sea capaz de entender la computadora, siendo capaz así de lograr el proceso de verificación y simulación automática del protocolo.

Con la validación se persiguen varios objetivos:

- Corrección: la garantía de mostrar los comportamientos previstos en cualquier situación específica.
- Robustez: la propiedad de ser capaz de trabajar correctamente en condiciones anormales.
- Rendimiento: La capacidad de lograr el ancho de banda disponible en el medio físico.

Con la realización de la verificación y validación se persigue:

- Reducir la complejidad.
- Eliminar la ambigüedad.
- Preparar protocolo estructurado.

Haciendo uso de SPIN en este paso del método, se pone a prueba el código modelado en el paso anterior, que refleja de manera más abstracta la máquina de estado finito que se obtuvo en el paso de modelación.

SPIN permite visualizar todo el proceso de simulación, observando el cambio de variables, el flujo de intercambio de datos entre los extremos, durante la simulación, además calcula la carga de cálculo que recibe el procesador con la máquina de estado finito definida, como se muestra en la figura 6.En la parte superior de la ventana se muestran las distintas opciones que tiene esta herramienta, entre ellas está, la cantidad de iteraciones en que se desea realizar la simulación, la velocidad de dicha simulación, si se desea hacerla guiada o automática, en la parte central, se muestra el código donde se ve resaltado la sección que corresponde en cada paso, cuando se marca en la sección inferior central, así, como en la

parte central derecha, se muestra el intercambio de mensajes por los extremos de la comunicación simulada, y por último, al extremo izquierdo inferior, se va mostrando el cambio de valores de las variables que intervienen en la simulación.

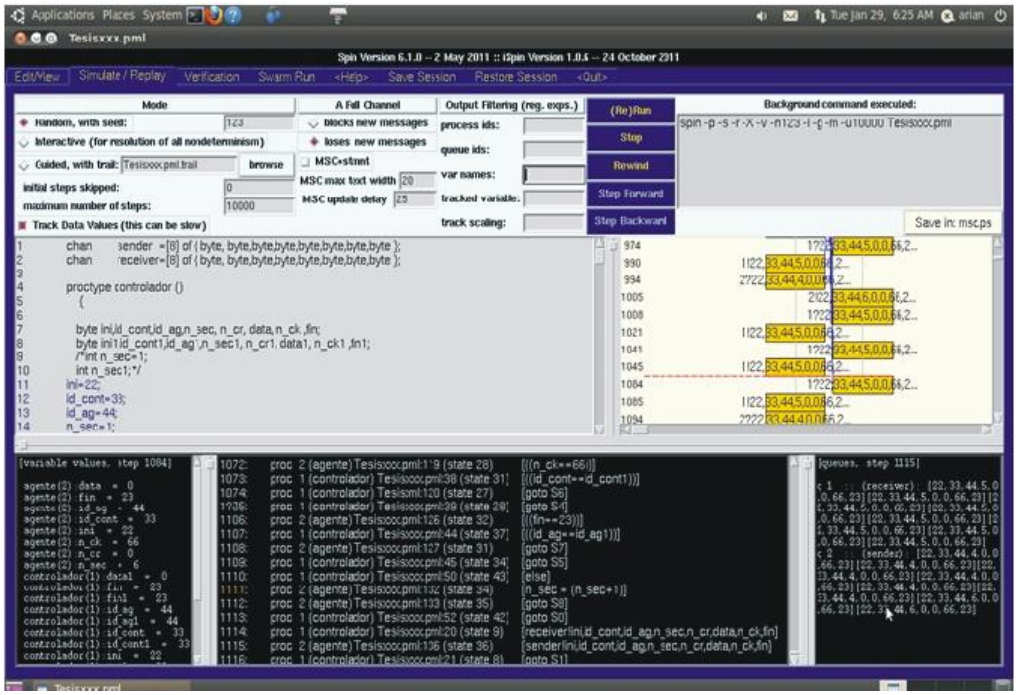

Figura 6. Simulación del Protocolo LDPROT mediante SPIN.

CONCLUSIONES

Está demostrado que la modelación y verificación formal de protocolos es eficiente para poner a punto los protocolos de comunicación. El método que se ha demostrado en este artículo, constituye una herramienta idónea de trabajo en la ingeniería de protocolos, debido a que brinda una línea organizada, incorporando los eficientes métodos de definición, modelación y simulación como pasos finales del método.

A partir de los requerimientos demandados al protocolo, se estudian las vías de su modelación, teniendo en cuenta los requisitos de especificación formal, se determina la tecnología de modelación adecuada, posteriormente, se realiza la definición formal a partir del lenguaje PROMELA, así como su verificación con la herramienta SPIN.

PROMELA y SPIN son las herramientas sugeridas y utilizadas en este método, siendo una solución factible para el desarrollo de la ingeniería de protocolos, puesto que están libres de licencias y consorcios privatizados, donde sus herramientas no dejan de ser eficientes y poderosas, pero incapacitan la posibilidad de que el sector académico y en desarrollo con bajo presupuesto, pueda desarrollar sus ídeas.