REVISTA DIGITAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES
TELEM@TICA
Revista Telem@tica. Vol. 13. No. 3, septiembre-diciembre, 2014, p. 21-34 ISSN 1729-3804

Autoconfiguración en *MANETs*.

Ing. Talia Odete Ledesma Quiñones[1], Dr. Walter Baluja García[2], Ing. Lucy Coya Rey[3]

[1]Complejo de Investigaciones Tecnológicas Integradas (CITI),talia.lq@udio.cujae.edu.cu

[2]Instituto Superior Politécnico "José A. Echeverría", walter@tesla.cujae.edu.cu

[3]Complejo de Investigaciones Tecnológicas Integradas (CITI), lucy.cr@udio.cujae.edu.cu

RESUMEN

Las redes ad hoc móviles (*MANETs*) permiten la comunicación entre nodos en movimiento a través de rutas multi-saltos inalámbricas. A diferencia de las redes tradicionales, no dependen de una infraestructura previa, y por tanto tienen que ser capaces de auto-configurarse. Antes de comenzar una comunicación, los nodos requieren de identificadores exclusivos para cada uno de ellos. En particular, cada nodo en la red necesita una dirección única para que los paquetes de datos puedan ser entregados a su destino.

Este artículo presenta un breve análisis del estado del arte de los protocolos de autoconfiguración que han sido propuestos para este tipo de redes y selecciona el/los más adecuados para implementar redes ad hoc con equipamiento típico de cliente (teléfonos móviles) e importantes niveles de movilidad.

Palabras claves: ad hoc, métricas de rendimiento, protocolos de autoconfiguración, *MANETs*

ABSTRACT

Mobile Ad hoc NETworks (MANETs) enable communication between mobile nodes through wireless multi-hop paths. In contrast with conventional networks, MANETs don't need any previous infrastructure and therefore they need to be able to self-configuring. Before beginning a communication each node requires a unique identifier. In particular, each node in the network requires a unique address so that data packets can be delivered to its destination.

This paper presents a brief analysis of the state of the art about autoconfiguration protocols that have been proposed for such networks and selects the best suited in order to implement ad hoc networks with typical client equipment (mobile phones) and substantial levels of mobility.

Keywords: ad hoc, autoconfiguration protocols, MANETs, performance metrics

INTRODUCCIÓN

Una red ad hoc móvil (*MANET*, por las siglas en inglés de *Mobile Ad hoc NETwork*) se conforma por un conjunto de nodos que se comunican entre ellos a través de enlaces inalámbricos. Al contrario de las redes convencionales, una *MANET* no necesita infraestructura previa, ya que los nodos dependen de ellos mismos para operar de forma colaborativa, formando lo que se llama una comunicación multi-saltos[1].Los nodos que se encuentren en el rango de alcance de otros se pueden comunicar directamente y son responsables de descubrirse dinámicamente entre sí. Con el fin de permitir la comunicación entre los nodos que no están directamente en el rango de señal de otros, los nodos intermedios actúan como enrutadores que reenvían los paquetes generados entre los extremos[2].

Para poder comunicarse, los nodos en una red ad hoc necesitan configurar sus interfaces con direcciones que son válidas dentro de la red. Los nodos ad hoc pueden necesitar también configurar direcciones de enrutamiento globales para comunicarse con otros dispositivos en Internet. Desde la perspectiva de la capa de red, una red ad hoc se presenta como una red multi-salto de nivel 3 constituida por una serie de enlaces[1].

AUTOCONFIGURACIÓN EN REDES *MANETS*

En las redes cableadas o inalámbricas con una infraestructura, existe un servidor o nodo que asigna centralmente las direcciones IP[1].El protocolo más utilizado en este caso es *DHCP* (*Dynamic Host Configuration Protocol*) [3], que asume que todos los nodos se pueden conectar a un servidor *DHCP*, ya sea directamente o a través de varios saltos. Debido a la topología *MANET*, la conexión directa al servidor *DHCP* no es muy frecuente con la consecuencia que la conexión a través de varios saltos, con movilidad, puede hacer al servidor inalcanzable [1]. Por tanto, debido a la naturaleza multi-saltos de las redes móviles inalámbricas, este protocolo no puede ser aplicado directamente en ellas [4]. Las *MANETs*, necesitan entonces algún protocolo que gestione la configuración de la red de forma dinámica y automática, el cual utilizarán todos los nodos de la red (o una parte de ellos) como si fueran servidores que gestionan las configuraciones[1].

Debido a la topología dinámica de las *MANETs* (constante movimiento de los nodos que pueden unirse y dejar la red frecuentemente e incluso simultáneamente), los protocolos de autoconfiguración existentes aún presentan deficiencias para garantizar que las direcciones IP sean únicas para cada nodo, y permitir la integración y separación de los nodos de la red[1].

CLASIFICACIÓN DE LOS PROTOCOLOS DE AUTOCONFIGURACIÓN

Los protocolos de autoconfiguración se pueden clasificar en tres categorías de acuerdo a sus características de asignación de direcciones [5]:

- ✓ **Estado completo** (*Stateful*): el estado de cada dirección es conocido de tal forma que la red tiene una visión de las IP asignadas y no asignadas, por tanto se evita el duplicado de direcciones. Algunos ejemplos son: *DHCP*, *DAAP* (*Dynamic Address Allocation Protocol*) [6], *Manetconf* [7], *Prophet*[8], *Prime DHCP* [9],*EPNA*(*Extended Prime Number Address Allocation*) [10], *OSA* (*One-Step Addressing*) [11], *D2HCP* (*Distributed Dynamic Host Configuration Protocol*) [12] y la solución de autoconfiguración utilizando el campo SSID de la trama *beacon* 802.11[13].

- ✓ **Sin Estado** (*Stateless*): Cada nodo elige aleatoriamente su dirección propia y lleva a cabo un proceso de detección de dirección duplicada (*DAD*[1], por las siglas en inglés de *Duplicate Address Detection*) para asegurar que la dirección seleccionada no ha sido utilizada aún. Algunos ejemplos son: *AAA* (*Ad-Hoc Address Autoconfiguration*)[17], *AIPAC (Automatic IP Address Configuration in Mobile Ad Hoc Networks)*[18], *AROD* (*Address autoconfiguration with address Reservation and Optimistic duplicated address Detection*) [19] y*APAC* (*Agent based Passive Autoconfiguration*) [20].
- ✓ **Híbridos**: Combinan los mecanismos de las anteriores para mejorar la escalabilidad y fiabilidad de la autoconfiguración. Sus algoritmos tienen un alto nivel de complejidad. Algunos ejemplos son: *HCQA* (*Hybrid Centralized Query-based Autoconfiguration*)[21], también conocido como *DACP* (*Dynamic Address Configuration Protocol*),*ODACP* (*Optimized DACP*) [17] y *PACMAN* (*Passive Autoconfiguration for Mobile ad hoc Networks*) [22].

PROTOCOLOS DE ESTADO COMPLETO

En este epígrafe se describen los protocolos de estado completo que presentan mejores características de acuerdo al análisis presentado en la Tabla 1.

DAAP (*Dynamic Address Allocation Protocol*)

DAAP[6]se basa en el concepto de asignación de direcciones por un líder. La funcionalidad del líder se comparte entre todos los nodos de la red. Cuando un nuevo nodo se une a la red, este se convierte en el líder hasta que se una el próximo. El líder tiene la mayor dirección IP dentro de la red ad hoc (desde el punto de vista jerárquico, similar al *subnetting*) y un identificador único se asocia con la red. Cada nodo almacena la mayor dirección IP (la del líder), y periódicamente envía mensajes *HELLO* a sus vecinos. Estos mensaje *HELLO* incluyen el identificador de red, de manera que se puedan identificar las integraciones y las separaciones. Cuando un nodo recibe un mensaje *HELLO* con un *ID* de red diferente, se detecta una integración. Si un nodo no recibe el mensaje que contiene el *ID* de red actual, entonces después de un tiempo, se detecta una separación [1, 17].

Prime DHCP[9]

El protocolo convierte a cada host en un proxy *DHCP*, lo cual hace que todos los nodos de la *MANET* sean elegibles para asignar direcciones y por tanto un nuevo nodo puede elegir una dirección simplemente de sus vecinos. Además, cada proxy *DHCP* ejecuta individualmente un algoritmo de asignación de dirección de numeración prima (*PNAA*, por las siglas en inglés de*prime numbering address allocation*) para calcular direcciones únicas para la asignación de direcciones, por tanto no requiere realizar *DAD*.

PNAA se origina de un teorema de factorización canónica de enteros positivos, que plantea que cada entero positivo puede ser escrito como un producto de números primos de una única forma. El nodo que crea la *MANET* (proxy raíz), tiene una dirección con valor 1 en la porción de *host* del rango a asignar, y puede entonces asignar direcciones con números primos en la porción de *host*, en orden ascendente, a los nuevos nodos que se quieran integrar. Los nodos proxy *DHCP* que no son la raíz pueden asignar la dirección igual a su propia dirección, con la porción de *host* multiplicada por los números primos que siguen al mayor factor primo de su propia porción de host, empezando por este mayor factor primo. Por ejemplo, el nodo no raíz G con valor 6 en el último octeto de la dirección (en la Figura 1 solo se representa el nodo con el valor del último octeto), tiene los factores primos 2 y 3, de ellos, el 3 es el

mayor factor primo. Por tanto, el nodo 6 podrá asignar la secuencia de valores 6*3, 6*5, 6*7 y así sucesivamente hasta llegar a la mayor dirección definida por el espacio de direcciones.

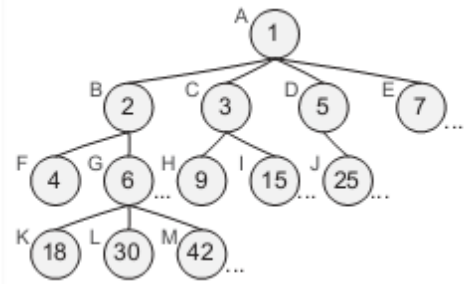

Figura 1. Ejemplo del árbol de asignación de direcciones en Prime DHCP[9].

Los proxies *DHCP* y el *PNAA*, en combinación, eliminan las necesidades de difusión en la *MANET*. De esta forma se puede reducir significativamente la sobrecarga y la latencia durante la adquisición de direcciones que realizan los hosts.

OSA (One-Step Addressing)

En el protocolo *OSA*, la *MANET* comienza con un solo nodo iniciando el proceso de configuración, donde otros nodos posteriormente pueden unirse y dejar la *MANET*. Cada nodo puede generar hasta $\boldsymbol{m}$ IPs que se concederán a los nodos que soliciten unirse a la *MANET*. Cuando un nuevo nodo desea unirse, censa el medio en busca de mensajes *beacon* de otros nodos. Cuando el tiempo se agota sin recibir ningún mensaje *beacon*, el nodo solicitante repite el proceso hasta T intentos. Si todos los intentos fallan (expira el *timer*), el nuevo nodo concluye que es el único nodo en la red y se configura él mismo con la primera dirección IP del espacio de direcciones. En caso de recibir un mensaje *beacon*, este envía un mensaje *Address Request* (*Add Req*) a sus vecinos. Los vecinos responden a este mensaje con un mensaje *unicast Address Replay* (*Add Rep*) que incluye un parámetro $\boldsymbol{Cav}$ con las direcciones IP disponibles ($\boldsymbol{Cav} = \boldsymbol{m}$). De todos los vecinos que respondieron el nodo selecciona el del valor de $\boldsymbol{Cav}$ más grande e ignora los demás. Luego de esto comienza un intercambio de mensajes entre ambos nodos para que este obtenga su dirección IP [11, 23]. En este protocolo cada nodo almacena dos registros y una tabla que se utilizan durante el proceso de asignación de dirección [23].

D2HCP (Distributed Dynamic Host Configuration Protocol)

D2HCP[12] hace que los nodos de la *MANET* colaboren entre sí para gestionar la asignación de direcciones IP únicas y correctas de manera distribuida. Todos los nodos de la red tienen la misma función; no hay ningún tipo especial de nodo que centralice la gestión de la misma.

Los nodos tienen un sistema de sincronización que se apoya en el protocolo de enrutamiento *OLSR* (*Optimized Link State Routing*). Gracias a este mecanismo, la sincronización se realiza de forma pasiva, monitorizando el protocolo de enrutamiento mencionado, por lo que se genera una sobrecarga nula en el tráfico de la red con respecto al generado por el protocolo *OLSR*. Debido a que todos los nodos son responsables de la gestión de la integración de cualquier nuevo nodo a la red, esta operación puede realizarse rápidamente. Un nodo que desea unirse a una red trata de comunicarse con cualquier nodo perteneciente a la misma, enviando un mensaje *SERVER_DISCOVERY*, a nivel MAC. Los nodos de la red que reciben este mensaje, responden con un mensaje *SERVER_OFFER*, también a nivel MAC, en el que ofrecen un número de direcciones IP (la mitad del rango disponible) y otras informaciones que el nodo cliente utilizará como criterios para elegirlo como su servidor de direcciones. El nodo cliente ordenará los mensajes recibidos de acuerdo a una serie de criterios y enviará al primer servidor un mensaje

SERVER_POLL (de nuevo, por la capa MAC) para indicarle que le ha elegido para que le asigne un bloque de direcciones IP libres. Si las direcciones ofrecidas por el nodo servidor no eran propias, sino de un tercer nodo de la red, con el mensaje*IP_RANGE_REQUEST* se le solicitan formalmente a ese nodo. Al ser una comunicación entre dos nodos ya configurados correctamente, se realiza en la capa IP. Ese tercer nodo envía un mensaje *IP_RANGE_RETURN* al nodo que envió el mensaje *IP_RANGE_REQUEST* autorizándolo a asignar al nodo cliente el bloque de direcciones indicado en este mensaje (también es un mensaje enviado por IP).

Tras recibir el *SERVER_POLL*, si las direcciones ofrecidas eran del propio nodo servidor, o tras el mensaje *IP_RANGE_RETURN* en caso de que se haya tenido que pedir las direcciones a un tercer nodo, el nodo servidor envía el mensaje *IP_ASSIGNED* al cliente (transmitido por la capa MAC), indicando el bloque de direcciones libres que se le asignan al cliente, y la tabla Free_IP_Blocks que anuncia los bloques que aún están libres. La tabla que se transmite en este mensaje no refleja la entrada del nodo cliente. Tras este intercambio de mensajes, el nodo cliente elige como su dirección IP la primera del bloque que se le ha asignado. En caso de tener más de una interfaz de red, usará las primeras del bloque en orden, y será la primera de todas la que use como dirección principal que identifica al nodo. La alta disponibilidad y redundancia que supone la gestión distribuida, hace que las posibilidades de éxito de unirse a la red sean elevadas [4, 24].

Solución de autoconfiguración utilizando el campo *SSID* de la trama *beacon*802.11

Esta solución de configuración descentralizada toma en consideración que 802.11 es la tecnología preferida por la mayoría de las *MANETs* y permite a los usuarios unirse a una *red* sin tener que recurrir a cualquier tecnología adicional, e incluso en presencia de comunicaciones cifradas. La solución permite que todos los pasos de configuración necesarios tengan una duración del orden de los milisegundos y sin provocar sobrecarga de tráfico adicional en el canal. Se implementa en el sistema operativo *Android* ya que es ampliamente utilizado en los dispositivos móviles [13].

La idea es aprovechar que una limitación del campo *SSID* de las tramas *beacon* a un tamaño menor no representaría un problema significativo para la mayoría de los usuarios. Entonces, el SSID se utilizaría no sólo para incluir el nombre de la red, sino también para informar sobre los detalles de configuración de las estaciones (modo de seguridad, protocolo de enrutamiento, dirección IP, entre otros) que le permitirán ser configurados de forma transparente. Las estaciones 802.11 generan tramas *beacon* periódicamente para proporcionar la información básica de la red. Las nuevas estaciones que escuchen e interpreten estas tramas serán capaces de determinar todos los parámetros de conexión para unirse a la *MANET*. En el caso de utilizar IPv6 se garantiza que la dirección IP sea única, para el caso de IPv4 no.

PROTOCOLOS SIN ESTADO

En este epígrafe se describe el protocolo sin estado que presenta mejores características de acuerdo al análisis presentado en la Tabla 1.

AIPAC (Automatic IP Address Configuration in Mobile Ad Hoc Networks)

AIPAC[18]es un protocolo de autoconfiguración de dirección IP que maneja la duplicación de direcciones de forma reactiva(solo trabaja cuando un nodo desea comunicarse con otro que tiene una dirección duplicada).

AIPAC funciona con los nodos solicitante e iniciador. El primero es un nodo que entra a la red y el último es un nodo ya configurado. El nodo iniciador negocia una dirección dentro de la red en nombre del solicitante. Para comunicarse con su iniciador, el solicitante utiliza una dirección temporal, que se

desecha cuando recibe la negociada. Para el procedimiento de negociación, el nodo iniciador selecciona al azar una dirección de un espacio predefinido y la comprueba con la red con el procedimiento *DAD* (de manera similar a *Strong DAD*) [25].Cada nodo en *AIPAC* está consciente de sus vecinos de radio, por lo que la cantidad de información almacenada por el nodo se limita a los nodos dentro de su rango de cobertura[1, 26].

PROTOCOLOS HÍBRIDOS

En este epígrafe se describen dos de los protocolos híbridos mencionados anteriormente con el objetivo de que se pueda reconocer su funcionamiento básico, aun cuando sus características no son buenas para *MANETs* con equipamiento de clientes.

HCQA (*Hybrid Centralized Query-based Autoconfiguration*)

HCQA[21] fue el primer protocolo de autoconfiguración híbrido. Un nodo que desea unirse a la red experimenta un proceso *SDAD*. Si el proceso es exitoso, el nodo tendrá que registrar su dirección IP tentativa con una Autoridad de Direccionamiento. Para hacer eso, esperará un mensaje de la Autoridad de Direccionamiento y cuando este mensaje haya sido recibido, este enviará una petición de registro y la Autoridad de Direccionamiento la confirmará. El nodo inicia un contador en cuanto comienza el proceso, si el tiempo del temporizador expira, comenzará el proceso otra vez hasta que pueda registrar la dirección IP. Cuando se crea la red, el primer nodo se convierte en una Autoridad de Direccionamiento, elige un identificador único (por ejemplo la dirección MAC) y lo anuncia periódicamente a través de mensajes de difusión para identificar la red. Si un nodo no lo recibe, este asume que la red ha sido dividida y creará su propia red, convirtiéndose en la Autoridad de Direccionamiento. Este protocolo asegura la no duplicidad de direcciones IP pero produce sobrecarga por el proceso *SDAD* y los mensajes periódicos de la Autoridad de Direccionamiento y además, la red depende de una entidad central con la cual todos los nodos tienen que comunicarse directamente con el fin de registrar su dirección IP, por tanto se añade mucha latencia en la integración de los nodos a la red[1, 17, 26, 27].

PACMAN (*Passive Autoconfiguration for Mobile ad hoc Networks*)

PACMAN[22]es un nuevo y eficiente enfoque para la asignación distribuida de direcciones IP en redes *MANETs*. El estado de la información sobre las direcciones asignadas se recolecta de manera pasiva para conservar el ancho de banda. Como ocurre en los protocolos sin estado, el nodo se auto asigna una dirección.

Para lograr la mínima sobrecarga, la información se comparte entre diferentes capas de red. Específicamente, se revisa la información intercambiada por el protocolo de enrutamiento. El método utilizado para elegir la dirección IP propia se basa en un algoritmo probabilístico. La probabilidad de intentar elegir una dirección IP que esté siendo utilizada en ese momento por otro nodo es cercana a cero. Este algoritmo toma en cuenta, entre otros factores, una tabla de asignación que es creada con información del protocolo de enrutamiento de las direcciones IP que ya están en uso. *PACMAN* utiliza el proceso *PDAD* para monitorizar las comunicaciones en busca de direcciones duplicadas. Esto es necesario ya que el mecanismo utilizado para la asignación de direcciones no garantiza que estas sean únicas y esto puede causar integraciones de redes que contienen nodos con dirección IP coincidente[1].

MÉTRICAS DE RENDIMIENTO PARA LOS SISTEMAS DE AUTOCONFIGURACIÓN EN *MANETs*

A continuación se muestran algunas métricas de rendimiento para los sistemas de autoconfiguración en *MANETs*[28],a partir de las cuales se realizará una comparación entre los principales protocolos del estado del arte.

- ✓ **Dirección IP única**: Cada nodo *MANET* debe obtener una dirección única para cada interfaz de red, debido a que las direcciones duplicadas pueden causar graves problemas en el enrutamiento y la comunicación en general. La garantía de una dirección asignada única es la métrica de rendimiento más importante, porque los conflictos de direcciones afectan todo el rendimiento y el tráfico de la red.
- ✓ **Escalabilidad**: Se pueden considerar dos factores fundamentales al aumentar la cantidad de nodos en la red: las sobrecargas de comunicación y la latencia de configuración. Un buen esquema de autoconfiguración no debe depender del número total de nodos o del tamaño de la red.
- ✓ **Independencia de los protocolos de enrutamiento**: Los protocolos de autoconfiguración pueden trabajar de dos formas: independiente o dependiente de un protocolo de enrutamiento[1]. Un enfoque dependiente de un protocolo de enrutamiento específico está mejor diseñado y debe tener mejor rendimiento, pero la ventaja de un enfoque independiente es su alta flexibilidad [27]. Los esquemas de autoconfiguración de direcciones deben ser compatibles con la mayoría de los protocolos de enrutamiento.
- ✓ **Uniformidad**[1]: Todos los nodos desempeñan las mismas funciones en el proceso de autoconfiguración.
- ✓

COMPARACIÓN DE LOS PROTOCOLOS DE AUTOCONFIGURACIÓN ANALIZADOS

La Tabla 1 muestra una comparación de los protocolos de autoconfiguración en redes *MANETs* mencionados en las primeras secciones de este artículo. Las publicaciones más recientes de estos protocolos presentan comparaciones en cuanto a: la eficiencia y la seguridad [1, 26]. No existe acceso a los códigos que se han utilizado, para las simulaciones que aparecen en la bibliografía. De igual manera, se desconoce el código de alguna implementación de los protocolos analizados hasta aquí, así como de su inclusión en sistemas operativos conocidos, excepto para el protocolo *PACMAN*, que dispone de una implementación en C diseñada para Linux, la cual se puede descargar en *Sourceforge* [29].

Tabla 1. Comparación de los protocolos de autoconfiguración en redes *MANETs*.

Métricas / Protocolos		Primera publicación	Garantía IP única	Sobrecarga	Latencia	Dependencia del protocolo de enrutamiento	Uniformidad	Simulación	Implementación
Estado completo	*DHCP* [26]	1997	Sí	Alta	Alta	No	No	-	-
	DAAP[1, 17]	2001	Sí	Media	Media	No	No	-	-
	ManetConf[1, 7, 17]	2002	No	Alta	Alta	No	Sí	*NS*-2	-
	Prophet[8, 9, 26, 27]	2003	No	Baja	Baja	No	Sí	*NS*-2	-
	Prime DHCP[9]	2005	Sí	Baja	Baja	No	Sí	-	-
	OSA[11, 23]	2008	Sí	Baja	Baja	No	Sí	-	JAVA
	D2HCP[4, 12]	2009	Sí	Baja	Baja	Sí	Sí	*NS*-3	-
	Solución 802.11 [13, 30, 31]	2010	No	Baja	Baja	No	Sí	-	Linux Android
Sin estado	*AAA*[17, 26]	2001	No	Alta	Alta	Sí	Sí	*NS*-2	-
	AIPAC[18, 25, 26]	2004	Sí	Baja	Baja	Sí	Sí	*NS*-2	C++
	AROD[1, 25]	2007	Sí	Alta	Alta	No	No	*NS*-2	C++
	APAC[1]	2007	No	Alta	Alta	Sí	No	-	-
Híbrido	*HCQA*[1, 17, 26, 27]	2003	Sí	Alta	Alta	No	No	*NS*-2	-
	PACMAN[1, 22, 29]	2005	No	Alta	Alta	Sí	Sí	*GloMoSim*	C (Linux)

La mayoría de los protocolos han sido simulados con la aplicación *Network Simulator* (NS2 y NS3). Según la bibliografía consultada, estos protocolos no han sido implementados en ambientes reales, sino que se encuentran en fase experimental, con la excepción del protocolo PACMAN que fue presentado en *ACM Mobicom* 2004, ejecutándose en dispositivos *Pocket PCs* basados en Linux y equipados con tarjetas inalámbricas IEEE 802.11b [29].

Los protocolos analizados no se simulan en esta investigación. Por tanto, para realizar la comparación en base a la sobrecarga y a la latencia, se tuvieron en cuenta los criterios que se utilizaron en la bibliografía consultada.

Hsu[9] plantea la sobrecarga que produce el protocolo *DHCP* como$\boldsymbol{O}(\boldsymbol{4l})$y la latencia en la asignación de direcciones como$\boldsymbol{O}(\boldsymbol{4td})$, donde$\boldsymbol{l}$ es el número de enlaces,$\boldsymbol{t}$ es la latencia promedio de un salto y$\boldsymbol{d}$es el diámetro de la red. Sin embargo, Rohit[26] define la sobrecarga, para este mismo protocolo, como$\boldsymbol{O}(\boldsymbol{n^2})$, donde$\boldsymbol{n}$ es el número de nodos móviles en la red, y la latencia como$\boldsymbol{O}(\boldsymbol{4td})$, y coincide con Hsu [9]. Se toma como referencia a Rohit [26] por ser una contribución más reciente. Entonces, se considera que la sobrecarga y la latencia para *DHCP* en redes *MANETs* son elevadas, ya que dependen del número de nodos y del diámetro de la red, respectivamente.

En otro orden, Sun [17] compara al protocolo *DAAP* con otros y define la sobrecarga como$\boldsymbol{O}(\boldsymbol{rhN})$y la latencia como $\boldsymbol{O}(\boldsymbol{rht})$, donde$\boldsymbol{r}$es el número de intentos de obtener una dirección,$\boldsymbol{h}$es el número promedio de saltos,Nes el número de nodos en la red y $\boldsymbol{t}$es la latencia promedio de un salto. Por su parte, García [1] plantea la sobrecarga y la latencia de este protocolo como medias. Este último enfoque es el que se toma en el contexto de esta investigación, ya que la sobrecarga depende en menor medida del número de nodos y la latencia no depende del diámetro de la red, pero si del número promedio de saltos.

El protocolo *Manetconf* se analiza por Sun [17], quien define la sobrecarga como$\boldsymbol{O(rN^2)}$y la latencia como$\boldsymbol{O(rDt)}$. Sin embargo, Wehbi [27] plantea que la sobrecarga que provoca este protocolo por asignación de dirección es$\boldsymbol{2l + 2N + N\,{}^{d}/_{2}}$ y la latencia es$\boldsymbol{(2 + d)t}$, donde les la cantidad promedio de nodos vecinos, $\boldsymbol{N}$es el número total de nodos, $\boldsymbol{d}$es el diámetro promedio de la red y$\boldsymbol{t}$ es el tiempo de ida y vuelta (*RTT,* por las siglas en inglés de *round trip time*) para un salto de comunicación. Hsu [9] plantea la sobrecarga como$\boldsymbol{O(2l)}$ y la latencia como$\boldsymbol{O(2td)}$. Finalmente, García [1] define a la sobrecarga y a la latencia de este protocolo como altas. Se coincide con este último autor, porque se observa una fuerte dependencia de la cantidad de nodos y del diámetro de la red.

El protocolo *Prophet* se analiza -junto a otros protocolos- por Sun [17]. Este autor establece la sobrecarga como$\boldsymbol{O(dN)}$y la latencia como$\boldsymbol{O(t)}$, donde$\boldsymbol{d}$ es el grado promedio del nodo. Para Wehbi [27], la sobrecarga para este protocolo es$\boldsymbol{2l}$y la latencia es $\boldsymbol{2t}$; mientras que Hsu [9] plantea que la sobrecarga, para el mismo, es$\boldsymbol{O({}^{n}/_{2})}$ y la latencia es$\boldsymbol{O(2t)}$, donde$\boldsymbol{n}$ es la cantidad de nodos. Por último, Rohit [26] define la sobrecarga para *Prophet* como $\boldsymbol{O({}^{n}/_{2})}$ y la latencia como $\mathrm{O(2t)}$. Debido a que existe coincidencia entre los dos últimos autores, estos setoman como referencia.

El protocolo *Prime DHCP* se describe por Hsu [9]. Este autor plantea que la sobrecarga y la latencia son iguales que para *Prophet*, o sea, $\boldsymbol{O({}^{n}/_{2})}$ y$\boldsymbol{O(2t)}$, respectivamente. Por tanto, la sobrecarga y la latencia se consideran bajas, como en el caso anterior.

Nassar y Al-Mahdi [11, 23] analizan el protocolo *OSA*, lo simulan y como resultado plantean que la latencia y la sobrecarga son bajas. En este artículo ambas métricas también se consideran bajas.

El protocolo *D2HCP* solo se comparó con otros por García [1]. En su trabajo, se plantea que la sobrecarga y la latencia para el mismo son bajas. Por tanto, en esta investigación ambas métricas se consideran de igual manera.

Ozaine [13] plantea que la solución basada en la modificación del campo SSID de la trama *beacon* 802.11 no introduce sobrecarga de tráfico adicional en el canal y el proceso de autoconfiguración es bastante rápido, en el orden de los milisegundos. Es por esto que se considera que la sobrecarga y la latencia son bajas.

Otro protocolo, el *AAA,* se estudia por Sun [17], quien plantea la sobrecarga como$\boldsymbol{O(rN^2)}$y la latencia como $\boldsymbol{O(rDt)}$, igual que para *Manetconf*. Rohit [26] define la sobrecarga como $\mathrm{O(n^2)}$ y la latencia como $\mathrm{O(2td)}$. En ambos casos se puede observar que la sobrecarga depende del número de nodos en la red al cuadrado y la latencia depende del diámetro de la red. Tal comportamiento hace que estas métricas se consideren elevadas.

García [1] compara *AIPAC* con otros protocolos y obtiene que la sobrecarga y la latencia son elevadas. Sin embargo, Rohit [26] determina la sobrecarga para este protocolo como$\boldsymbol{O({}^{n}/_{2})}$ yla latencia como $\boldsymbol{O(2t)}$, al igual que para *Prophet* y para *Prime DHCP*. Al ser esta última contribución más reciente que la primera, se toma como referencia a los efectos de esta investigación.

Paralelamente, la sobrecarga y la latencia para los protocolos *AROD*, *APAC* y *PACMAN* son elevadas en los tres casos [1] y se asumen como tales en este trabajo.

En el caso del protocolo *HCQA*, las fórmulas son iguales a: sobrecarga,$\boldsymbol{O(rN^2)}$; y latencia,$\boldsymbol{O(rDt)}$[17], igual que para *Manetconf* y *AAA*. Mientras que para Wehbi [27], la sobrecarga por asignación de dirección -que provoca este protocolo- es $\boldsymbol{kN + d}$, y la latencia es $\boldsymbol{kT + {}^{T}/_{2} + d\,{}^{t}/_{2}}$, donde $\boldsymbol{T}$es el periodo de sincronización, inundación o cualquier procedimiento repetitivo; y $\boldsymbol{k}$ es el número de

iteraciones, si existen. En otro contexto, García[1] encuentra a la sobrecarga y a la latencia elevadas, para este protocolo. En general, se observa una fuerte dependencia de la cantidad de nodos y del diámetro de la red. Por tanto, se supone que la sobrecarga y la latencia son elevadas para este protocolo.

A partir de la comparación anterior, y considerando también su baja complejidad de implementación, se concluye que el protocolo Prime DHCP es el más acertado para desplegarse en una MANET regular, en particular en las que se despliegan sobre teléfonos móviles. Adicionalmente, se considera que el protocolo DAAP no deja de ser una buena opción ya que su gestión es semi-distribuida, y presenta sobrecarga y latencia medias. La solución basada en la modificación del campo SSID de la trama *beacon* 802.11, también puede utilizarse, cuando la MANET está formada por pocos nodos (menos de 100), ya que en este caso la probabilidad de que haya una IP repetida es relativamente baja.

CONCLUSIONES

Los nodos que forman parte de una red, ya sea alambrada o totalmente inalámbrica, como las *MANETs*, necesitan direcciones IP únicas con el objetivo de que los paquetes de datos puedan ser enrutados y entregados a un destino unívoco. Con esta finalidad se introducen en estas redes los denominados protocolos de autoconfiguración. Debido a la topología dinámica de las *MANETs*, los protocolos de autoconfiguración aún presentan algunas dificultades para garantizar que las direcciones IP sean únicas para cada nodo, y permitir la integración y separación de los nodos de la red de un modo eficiente.

En este artículo se ha presentado un breve análisis de algunos protocolos de autoconfiguración que han sido propuestos para las redes *MANETs*. Además, se realizó una comparación en cuanto a métricas de desempeño y otras características de los protocolos con el fin de proponer los más adecuados para implementar una red *MANET* regular, en particular en las que se despliegan sobre teléfonos móviles, arribando a la conclusión de que el protocolo que parece el más acertado es *Prime DHCP*, aunque el protocolo *DAAP* también podría ser efectivo en este tipo de redes. En caso de contar con pocos nodos en la *MANET*, la solución basada en la modificación del campo *SSID* de la trama *beacon* 802.11, es una buena opción.

REFERENCIAS

1. **García Villalba, L.J., et al.**, (2011) "*Auto-Configuration Protocols in Mobile Ad Hoc Networks*". sensors, ISSN: 1424-8220, Disponible en: https://www.scienceopen.com/document_file/6e13ff13-3c7d-460b-8062-c24cbd48c657/PubMedCentral/6e13ff13-3c7d-460b-8062-c24cbd48c657.pdf, p. 3652-3666. (Journal Article) (Review)
2. **Hoebeke, J., et al.**, (2004) "*An Overview of Mobile Ad Hoc Networks: Applications and Challenges*". Department of Information Technology (INTEC). p. 60-66. Ghent University – IMEC vzw. Disponible en: http://cwi.unik.no/images/Manet_Overview.pdf. (Electronic Article)
3. **Droms, R.**,(1997) "*Dynamic Host Configuration Protocol* ". Disponible en: http://www.freesoft.org/CIE/RFC/2131/. (RFC 2131)
4. **García Villalba, L.J., et al.**, (2011) "*Distributed Dynamic Host Configuration Protocol (D2HCP)*". sensors, ISSN: 1424-8220, Disponible en: http://www.mdpi.com/1424-8220/11/4/4438/pdf, p. (Journal Article)
5. **Caputo, L., et al.**, (2013) "*AutoBeeConf: A swarm intelligence algorithm for MANET administration*". International Journal of Advanced Research in Artificial Intelligence (IJARAI), Vol. 2, ISSN, Disponible en: http://thesai.org/Downloads/IJARAI/Volume2No2/Paper_9-AutoBeeConf.pdf, p. 8. (Journal Article)
6. **Patchipulusu, P.**, (2001), "*Dynamic Address Allocation Protocols for Mobile Ad Hoc Networks*" (en Inglés), Tesis de maestría, Texas A&M University. (Thesis)
7. **Nesargi, S. and R. Prakash**, (2002) "*MANETconf: Configuration of Hosts in a Mobile Ad Hoc Network*". INFOCOM, p. 10. Department of Computer Science, University of Texas at Dallas. Disponible en: http://www.utdallas.edu/~ravip/papers/infocom2002.pdf. (Electronic Article)
8. **Zhou, H., L.M. Ni, and M.W. Mutka**, (2003), "*Prophet Address Allocation for Large Scale MANETs*". San Francisco: Proceedings of the IEEE Conference on Computer Communications (INFOCOM). (Conference Proceedings)
9. **Hsu, Y.-Y. and C.-C. Tseng**, (2005) "*Prime DHCP: A Prime Numbering Address Allocation Mechanism for MANETs*". IEEE COMMUNICATIONS LETTERS, Vol. 9. No. 8. ISSN, Disponible en: http://front.cc.nctu.edu.tw/Richfiles/14353-35.pdf, p. 712-714. (Journal Article)
10. **Kumar, H. and R.K. Singla**, (2009) "*Architecture for address auto-configuration in MANET based on Extended Prime Number Address Allocation (EPNA)*". WSEAS TRANSACTIONS on COMPUTERS, Vol. 8. No. 3. ISSN: 1109-2750, Disponible en: http://www.wseas.us/e-library/transactions/computers/2009/31-838.pdf, p. 549-558. (Journal Article)
11. **Nassar, H., et al.**, (2008), "*Design and Analysis of a One-Step Addressing Protocol for Ad Hoc Networks*", presentado en 7th WSEAS Int. Conf. on Electronics, Hardware, Wireless and Optical Communications, Cambridge, UK, , ISBN/ISSN: 978-960-6766-40-4/1790-5117, pp. 140-145. (Conference Paper)
12. **Sandoval Orozco, A.L.**, (2009), "*PROTOCOLO DISTRIBUIDO PARA LA CONFIGURACIÓN DINÁMICA DE DIRECCIONES EN REDES MÓVILES AD HOC*" (en Español), PROYECTO FIN DE MÁSTER EN SISTEMAS INTELIGENTES, UNIVERSIDAD COMPLUTENSE DE MADRID, Disponible en: http://eprints.ucm.es/9909/1/Master_2008-2009.pdf, p. (Thesis)
13. **Ozaine, O., A. Díaz-Ramírez, and C.T. Calafate**, (2013), "*MANET auto-configuration using the 802.11 SSID field in Android* ", presentado en 1er CONGRESO INTERNACIONAL DE ROBÓTICA Y COMPUTACIÓN, CIRC 2013, Instituto Tecnológico de La Paz, México, ISBN/ISSN: 978-607-95534-5-6, pp. 256-261. (Conference Paper)
14. **Perkins, C.E., et al.**,(2001) "*IP Address Autoconfiguration for Ad Hoc Networks*". Disponible en: http://tools.ietf.org/html/draft-perkins-manet-autoconf-01.txt. (Internet Draft)

15. **Vaidya, N.H.**, (2002) "*Weak Duplicate Address Detection in Mobile Ad Hoc Networks*". Department of Electrical and Computer Engineerin and Coordinated Science Laboratory. University of Illinois at Urbana-Champaign. MOBIHOC'02, p. 11. EPFL Lausanne, Switzerland. Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.11.3403&rep=rep1&type=pdf. (Electronic Article)
16. **Weniger, K.**, (2003) "*Passive Duplicate Address Detection in Mobile Ad Hoc Networks*". University of Karlsruhe,Germany. p. 7. Institute of Telematics. Disponible en: http://doc.tm.uka.de/2003/weniger-passive-dad-lsr-wcnc2003.pdf. (Electronic Article)
17. **Sun, Y. and E.M. Belding-Royer**, (2004) "*A Study of Dynamic Addressing Techniques in Mobile Ad hoc Networks*". Wireless Communications and Mobile Computing. Disponible en: http://www.cs.ucsb.edu/~ebelding/txt/wcmc04.pdf, p. 14. (Journal Article)
18. **Fazio, M., M. Villari, and A. Puliafito**, (2004) "*AIPAC: Automatic IP Address Configuration in Mobile Ad Hoc Networks*". p. 27. Universita di Messina, Dipartimento di Matematica, Italy. Disponible en: http://cia.unime.it/documents/comcom.pdf. (Electronic Article) (DRAFT)
19. **Kim, N., S. Ahn, and Y. Lee**, (2007) "*AROD: An address autoconfiguration with address reservation and optimistic duplicated address detection for mobile ad hoc networks*". Computer Communications, 30, p. 1913-1925. Disponible en. (Electronic Article)
20. **Li, L., et al.**, (2007) "*Agent-Based Passive Autoconfiguration for Large Scale MANETs*". Wireless Personal Communications, Vol. 43. No. 4. ISSN, Disponible en, p. 1741-1749. (Journal Article)
21. **Sun, Y. and E.M. Belding-Royer**,(2003) "*Dynamic Address Configuration in Mobile Ad hoc Networks*": University of California, Santa Barbara.. Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.331.6772&rep=rep1&type=pdf. (Technical Report)
22. **Weniger, K.**, (2005) "*PACMAN: Passive Autoconfiguration for Mobile Ad hoc Networks*". p. 14. Universit¨at Karlsruhe (TH), Germany. Disponible en: http://www.tm.uka.de/doc/2004/autoconf_jsac_epub.pdf. (Electronic Article)
23. **Al-Mahdi, H., H. NASSAR, and S. El-Aziz**, (2013) "*Performance Analysis of an Autoconfiguration Addressing Protocol for Ad Hoc Networks*". Journal of Computer and Communications. Disponible en: http://www.scirp.org/journal/PaperDownload.aspx?paperID=38653, p. 33-40 (Journal Article)
24. **García Matesanz, J., et al.**, (2011) "*An Improved Buddy System Auto-Configuration Protocol for Mobile Ad Hoc Networks*". The 5th International Conference on Information Technology, Vol. No., ISSN, Disponible en: http://www.zuj.edu.jo/conferences/icit11/paperlist/Papers/Computer%20Networks%20&%20Communications/635_javier3.pdf, p. 6. (Journal Article)
25. **Schmidt, R.d.O., A. Pras, and R. Gomes**, (2011) "*Evaluating Self-Addressing Proto cols for Ad-Hoc Networks*". p. 6. Disponible en: http://doc.utwente.nl/79749/1/schmidt.pdf. (Electronic Article)
26. **Rohit, R. and D.A.P. Singh**, (2014) "*A Study of various Address Allocation Schemes for Mobile Ad Hoc Networks*". International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Vol. 3. No. 1. ISSN: 2278-6856, Disponible en: http://www.ijettcs.org/Volume3Issue1/IJETTCS-2014-02-09-056.pdf, p. 100-115. (Journal Article)
27. **Wehbi, B.**, (2005) "*Address Autoconfiguration in Ad Hoc Networks*". Departement Logiciels Reseaux (LOR). p. 20. Institut National des Telecommunications (INT). Disponible en: http://www.bachwehbi.net/autoconf_report.pdf. (Electronic Article) (Internal Report)

28. **Ahn, S., et al.**, (2003) "*A Comparison Study of Address Autoconfiguration Schemes for Mobile Ad hoc Network*". p. 7. Information and Communications University, Computer Networks Lab., School of Engineering. Disponible en: http://pdf.aminer.org/000/369/889/a_comparison_study_of_address_autoconfiguration_schemes_for_mobile_ad.pdf. (Electronic Article)
29. (2004) "*Passive Autoconfiguration for Mobile Ad hoc Networks (PACMAN)*". Última modificación: 9 de noviembre; Disponible en: http://pacman-autoconf.sourceforge.net/. (Web Page)
30. **Villanueva, M.J., C.T. Calafate, and J.-C. Cano**, (2010) "*Solving the MANET autoconfiguration problem using the 802.11 SSID field*". MoMM2010. Disponible en: http://dbonline.igroupnet.com/ACM.TOOLS/Rawdata/Acm1105/fulltext/1980000/1971537/p87-villanueva.pdf, p. (Journal Article)
31. **Villanueva Del Pozo, M.J., et al.**, (2013) "*Seamless MANET autoconfiguration through enhanced 802.11 beaconing*". Mobile Information Systems, Vol. 9. No. 1. ISSN, Disponible en: http://riunet.upv.es/bitstream/handle/10251/35991/ssid_autoconf_MOBIS%20%282%29.pdf?sequence=2&isAllowed=y, p. 19-35. (Journal Article)