

ANÁLISIS ACERCA DE LA IMPLEMENTACIÓN DE SISTEMAS DE VIDEO VIGILANCIA SOBRE REDES MESH

AN ANALYSIS OF VIDEO SURVEILLANCE SYSTEMS IMPLEMENTATION OVER MESH NETWORKS

Abstract

In recent years, Ad-hoc Mesh networks have attracted great attention due to their potential use in various fields such as military activities, rescue operations and time critical applications. This article presents the implementation analysis of a video surveillance system that covers marginalized areas of Bogotá and uses Ad-hoc Mesh Networks. Internationally recognized protocols such as AODV, OLSR, BATMAN are described and compared in order to select the most suitable. Similarly, the router with the best cost-benefit relation to fit the Night-wing Firmware is selected from an extensive list of hardware components. Finally, the cost of implementing a wired phase and the cost of a wireless phase, both offering video surveillance services, are compared.

Keywords: Architecture, protocol, mesh network.

Resumen

En los últimos años las redes Ad-hoc Mesh, han estado atrayendo la atención por su uso potencial en varios campos tales como las actividades militares, operaciones de rescate y aplicaciones en tiempo crítico. En este artículo se presenta el análisis de la implementación de un sistema de video vigilancia para sectores marginados de Bogotá usando redes Ad-hoc Mesh. Se describen los protocolos más usados internacionalmente AODV, OLSR, BATMAN y se comparan para seleccionar el más óptimo. De igual forma se selecciona de una extensa lista de hardware el router con el mejor costo beneficio que se adecua al firmware nightwing. Al final se relacionan los costos de implementación de un escenario cableado contra un escenario inalámbrico que ofrecen sistemas de video vigilancia.

Palabras clave: Arquitectura, protocolo, redes Mesh.

Christian C. Fuquene

Ingeniero Electrónico, estudiante de Especialización en Teleinformática de la Universidad Distrital Francisco José de Caldas, de Bogotá, Colombia.
ccfuquenec@correo.udistrital.edu.co

Octavio J. Salcedo

Ingeniero de Sistemas, MSc. en Teleinformática de la Universidad Distrital, MSc. en Economía, se desempeña como docente de planta de la Universidad Distrital "Francisco José de Caldas"
ojsalcedop@udistrital.edu.co

John J. Triana

Ingeniero de Sistemas, estudiante de Especialización en Teleinformática de la Universidad Distrital Francisco José de Caldas, de Bogotá, Colombia.
jt trianae@udistrital.edu.co

Tipo: Artículo de revisión

Fecha de Recepción: Marzo 29 de 2010

Fecha de Aceptación: Mayo 14 de 2010

1. INTRODUCCIÓN

Las redes Mesh tienen su origen en las primeras redes ad-hoc. (Una red ad-hoc inalámbrica es aquella en la que no hacen falta nodos especiales que enrutan y gestionan el tráfico, sino que cada nodo tiene la capacidad de reenviar paquetes dirigidos a otros nodos de la red). Las primeras redes inalámbricas ad-hoc fueron desarrolladas por DARPA (Agencia de Investigación de Proyectos Avanzados de Defensa) en los años 70 y operaban en radiofrecuencias UHF y se denominaban Packet Radio Networks. Las primeras redes fueron ALOHNET y PRNET. De allí surgen las comunidades de radioaficionados que implementaron sus primeras redes, la más importante y aún en funcionamiento AMPRNET, implementa el protocolo TCP/IP y tiene su propio rango de direcciones IP reservado. A continuación las redes ad-hoc adquieren la capacidad de moverse y se crean las redes MANET (Mobile Ad-hoc Network), promovidas nuevamente por la investigación militar y DARPA. En 1983 esta agencia inicia el proyecto SURAN (Survivable Radio Network) cuya finalidad era desarrollar una red ad-hoc móvil de bajo coste y que pudiese implementar protocolos Packet radio más complejos que PRNET. En los años 90 se iniciaron distintos proyectos en el ámbito militar y de defensa, como GloMo (Global Mobile) y NTDR (Near Term Digital Radio). En 1997 el ejército de EE.UU. empezó el desarrollo del Tactical Internet (TI), una red inalámbrica multsalto (multi-hop) packet radio que conformase un campo de batalla militar totalmente digitalizado, en el que cada unidad tiene comunicación bidireccional de datos con todas las demás unidades [1].

Con la impresionante difusión de internet en los años 90 y la aparición de los dispositivos móviles las redes inalámbricas empiezan a ser una alternativa a las redes cableadas, el IEEE en 1997 define la especificación IEEE 802.11, un estándar internacional que define las características de una red de área local inalámbrica WLAN

(Wireless Local Area Network). En 1999 el IEEE aprueba la revisión 802.11b de la norma original 802.11, la cual aumentaba la tasa de transferencia hasta los 11 Mbit/s. Ese mismo año nace la asociación WECA (Wireless Ethernet Compatibility Alliance), creada por Nokia y Symbol Technologies., cuya finalidad era crear una marca que permitiese fomentar más fácilmente la tecnología inalámbrica y asegurar la compatibilidad de equipos. Esta asociación pasó a denominarse Wi-Fi Alliance en 2003. De esta forma, en abril de 2000 WECA certifica la interoperabilidad de equipos según la norma IEEE 802.11b, bajo la marca Wi-Fi [2]. Gracias a esta interoperabilidad las implementaciones de la tecnología Wifi se expanden a los hogares mediante enrutadores y AP (Acces Points) inalámbricos que permiten conectar diferentes dispositivos a Internet sin necesidad de cables. Este auge permite que el costo de los dispositivos inalámbricos sea cada vez menor y aparezcan las primeras comunidades de redes comunitarias con desarrolladores y entusiastas de software libre, que impulsarían nuevos protocolos y tecnologías inalámbricas libres. Es en este contexto cuando surgen comunidades, centros de investigación y docencia y empresas interesadas en desarrollar tecnologías inalámbricas en malla o redes Mesh, que poseen la particularidad de utilizar la infraestructura de las redes existentes y las redes ad-hoc, y que son capaces de extender y compartir conectividad inalámbrica en lugares donde por razones económicas las posibilidades son mínimas. En la Fig. 1 se presenta un esquema básico de las redes Mesh.

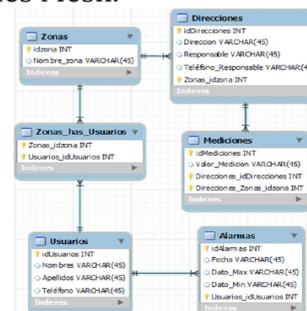


Fig. 1. Redes Mesh [3].

La expectativa generada por las redes de malla inalámbricas han disparado los avances en distintos niveles. En primer lugar, los fabricantes están impulsando sus soluciones de redes inalámbricas con protocolos de malla propietarios, como Sky-Pilot, BelAiry SaxNet. En segundo lugar, las redes comunitarias en malla han crecido y ofrecen conectividad y capacidad. El MIT Roofnet o el Freifunk en Berlín son claros ejemplos que han crecido a un tamaño de hasta 200 puntos de acceso y siguen aumentando. En tercer lugar, bancos de pruebas de investigación tales como Magnets y RescueMesh han desarrollado pruebas experimentales de redes en malla y han entendido sus limitaciones y capacidades. En cuarto lugar, las actividades de normalización se han centrado en las redes en malla multisalto, incluida la 802.11s para redes WLAN y la IEEE 802.15 para redes inalámbricas de área personal (WPAN) y redes de sensores. Esfuerzos similares están encaminados hacia el futuro de la tecnología, tales como el estándar IEEE 802.16, el cual incluye un esquema de conexión (multipunto a multipunto) junto al tradicional punto a multipunto (PMP). Al mismo tiempo se ha establecido un nuevo grupo (IEEE 802.16j) el cual se centra en la especificación multisalto[4]. A nivel internacional, este concepto de WMN (Wireless Mesh network) o red inalámbrica en malla está muy difundido tanto en Europa como en Norte América. Son diversos los servicios que se están brindando a través de la implementación de este tipo de red [5]. En los siguientes párrafos se relacionan algunos de los proyectos desarrollados a nivel mundial empleando las bondades ofrecidas por las redes Mesh.

En la ciudad de Zaragoza en España, donde se brindan servicios de ToIP y VoIP, y en Oklahoma, Estados Unidos, se generó una red para el servicio público y servicios de vigilancia en los patrulleros [5]. En Massachusetts, el Departamento de Policía de Haverhill selecciono esta tecnología para su sistema de videovigilancia [6]. En Aruba se

implanto un sistema inalámbrico de video vigilancia con diseño en malla, el cual proporciona una cobertura de vídeo de calidad HD para las tiendas, restaurantes y zonas de aparcamiento de un importante centro comercial. El diseño utilizo 13 cámaras de vídeo conectadas por 10 enrutadores inalámbricos en malla [7].

En Alemania se encuentra el proyecto Freifunk, esta red experimental de comunidad urbana está conformada por unos 200 nodos basado en OLSR Firmware Freifunk. A este software se le han dado muchos usos en proyectos comunitarios y de desarrollo [8]. La red inalámbrica CUWiN en Illinois, es una iniciativa de desarrollo e investigación con una implementación de código abierto del protocolo de enrutamiento HSLS, apostando a una red Ad-Hoc inalámbrica escalable y altamente robusta [9]. En la India existe una red comunitaria en Dharamsala, la cual está encargada de realizar la conexión de varios campus. Actualmente en Bogotá se encuentra en marcha un proyecto denominado Bogotá-Mesh, el cual busca la creación de una red abierta, descentralizada, comunitaria, independiente y autónoma que sirva como herramienta para difundir proyectos de carácter comunitario, social, cultural y científico [10].

2. ARQUITECTURA DEL SISTEMA

2.1 Protocolos

Dado que se trata de una red de topología dinámica y auto configurable, las rutas que se establecen entre dispositivos cambian dinámicamente, con lo cual son necesarios una serie de protocolos para transmitir los datos con un bajo coste de transmisión, como por ejemplo, encontrar la ruta con menos saltos.

Una clasificación tradicional de los protocolos de enrutamiento los divide en:

- Reactivos, en los que un nodo sólo intercambia información de control cuando

quiere iniciar una comunicación con otro nodo. AODV y DSR son los más extendidos en esta categoría.

- Proactivos, en los que los nodos intercambian información de forma periódica para aprender la topología de la red. OLSR y TBRPF son los más populares.

Además, hay un problema concreto que solo recientemente ha sido abordado por algunos grupos de investigación y por muy escasos proyectos de desarrollo: la QoS, como demostró un grupo del MIT en [12], los protocolos anteriormente citados establecen rutas que no siempre son óptimas debido a que usan como métrica el número de saltos. Con frecuencia en redes Mesh, cuando hay más de una ruta alternativa para unir dos nodos no contiguos, el camino con menor número de saltos usa algún enlace más lento e inestable; los protocolos anteriores escogen con frecuencia este tipo de rutas. Algunos, como AODV, son en este sentido mejores que el resto por definir un umbral de nivel de señal para considerar que un enlace existe [13].

2.1.1 AODV (*Ad hoc on-demand distance vector*)

Cuando un nodo S necesita una ruta a un destino D (Fig. 2), este difunde un ROUTE REQUEST (Solicitud de ruta) en un mensaje a sus vecinos, incluyendo el último número de secuencia conocido para ese destino. La solicitud de ruta es inundada de forma controlada a través de la red hasta que llega a un nodo que conoce la ruta hacia el destino. Cada nodo que reenvía la solicitud de ruta crea un camino inverso hacia el nodo S. Cuando la solicitud de ruta llega a un nodo que conoce la ruta a D, este dispositivo genera un ROUTE REPLY (respuesta de ruta) que contiene el número de saltos necesarios para llegar a D y el último número de secuencia conocido para D por el nodo que genera la respuesta. Cada nodo que participa en el envío de esta RESPUESTA hacia el autor de la solicitud de ruta (nodo S), crea una hacia D. El estado creado en cada nodo a lo largo de la ruta de S a D es un estado

salto por salto, es decir, cada elemento sólo recuerda el siguiente salto y no toda la ruta, como se haría en el enrutamiento de origen [14].

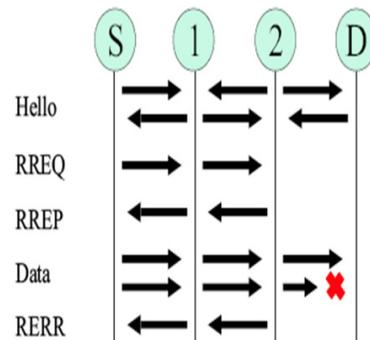


Fig. 2. Mensajes en AODV.

A fin de mantener las rutas, AODV normalmente requiere que cada componente periódicamente transmita un mensaje de HELLO, con una tasa de una vez por segundo. Si no se reciben tres mensajes consecutivos de HOLA de un vecino se toma como una indicación de que el vínculo con el vecino en cuestión está abajo. Por otra parte, la breve especificación AODV sugiere que un DCE puede usar métodos de la capa física o de la capa de enlace para detectar rupturas en los enlaces con otros pares que consideran vecinos [15]. Cuando un enlace se cae, cualquier elemento activo que recientemente ha enviado paquetes a un destino utilizando ese enlace es notificado a través de un UNSOLICITED ROUTE REPLY que contenga una métrica infinita hacia el destino. Tras la recepción de tal respuesta de ruta, este debe adquirir una nueva ruta hacia el destino utilizando el descubrimiento de ruta descrito anteriormente [14].

2.1.2 OLSR (*Optimized link state routing protocol*)

Es una tecnología de enrutamiento por IP para redes móviles o inalámbricas ad-hoc. Actualmente es uno de los protocolos más prometedores siendo la base de la mayoría de las redes mesh instaladas en Europa [11]. Posee la característica de ser proactivo, que envía de forma distribuida men-

sajes "Hello" para conocer su entorno; una vez establecidos los nodos contiguos envía mensajes de TC (Topology Control) a un subconjunto de estos para establecer las conexiones. OLSR funciona bien en redes con alto número de usuarios y con una topología cambiante. Para llevar un control, se intercambian periódicamente mensajes de tal forma que se va aprendiendo la topología de la red y el estado de los nodos vecinos. El intercambio de tantos paquetes, congestiona la red y supone un grave problema en las comunicaciones. Para solucionar esto, OLSR utiliza la técnica de MPR (Multi Point Relay). Gracias a ella se reduce el número de retransmisiones [15].

Cuando un nodo recibe un paquete básico OLSR, analiza sus campos. Lo primero que hace es determinar de qué tipo se trata. Mira el campo Message Type, para determinar qué se encontrará en el mensaje. A continuación mira el Message Size, para ver si el paquete es correcto o si por el contrario debe descartarlo. Mira el Message Sequence Number para saber si ha tratado ese mensaje con anterioridad o por el contrario se trata de uno nuevo. En el caso de no ser un mensaje repetido evalúa el valor del campo TTL. Al analizar el TTL, decrementa en uno su valor; si el valor resultante igual a cero debe ser eliminado de la red. Luego mira la información del estado de enlace para poder encaminar hacia otros nodos con el fin de llegar a su destino.

2.1.3 **BATMAN**

Es un protocolo de enrutamiento proactivo para Redes Mesh Ad-Hoc, incluyendo las Redes Móviles Ad-hoc (Mobile Ad-hoc Networks MANETs). Mantiene proactivamente la información sobre la existencia de todos los nodos en la red Mesh que son accesibles con unas comunicaciones de un solo salto o de múltiples saltos. La estrategia es determinar para cada destino de la red topología un único salto vecino que pueda ser usado como la mejor puerta de enlace para comu-

nicarse con el host destino. Con BATMAN no es necesario encontrar o calcular la ruta completa, ello hace que sea una implementación muy rápida y eficiente.

Debido a las altas probabilidades de fallos en las conexiones, las pérdidas de paquetes, y demás problemáticas que trae implícito el uso del medio inalámbrico, B.A.T.M.A.N. tiene en cuenta estos desafíos al hacer en análisis estadístico de la pérdida de paquetes del protocolo y la velocidad de propagación y no depende del estado o topología de la información de otros dispositivos. En lugar de confiar en los metadatos contenidos en el protocolo del tráfico recibido (que pueden ser retardados, desactualizados o perdidos) las decisiones de enrutamiento son basadas en el conocimiento de la existencia o la falta de información. Los paquetes usados por BATMAN, contienen solo una cantidad limitada de información y son por ende muy pequeños. Los paquetes perdidos debido a enlaces poco fiables, no son contrarrestados con redundancia, pero son detectados y utilizados para mejores decisiones de enrutamiento BATMAN. Elige la ruta más confiable para las decisiones del próximo salto de los nodos individuales [16]. No fue diseñado para operar en medios estables y confiables, como las redes cableadas, sino más bien en función de medios poco fiables que si experimentan altos niveles de inestabilidad y de pérdida de datos. Específicamente fue concebido para contrarrestar los efectos de las fluctuaciones de una red y compensar su inestabilidad, permitiendo así un alto nivel de robustez. También incorpora la idea de Inteligencia Colectiva opuesta a la idea de routing de estado de enlace. No hay entidad central que conozca todas las posibles vías a través de la red. Todo elemento capa 3 solo determina el dato para elegir el próximo salto, haciendo al protocolo muy liviano y rápidamente adaptable a fluctuaciones de la topología. En la Fig. 3 se muestra la estructura del estándar BATMAN.

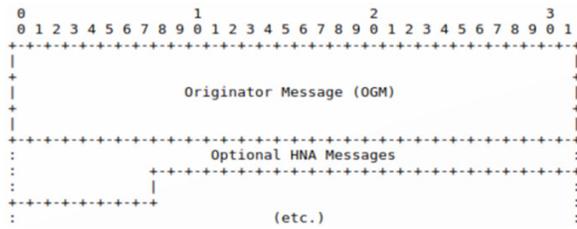


Fig. 3. Formatos del paquete general BATMAN [17].

2.1.4 Comparación entre protocolos

La evaluación del rendimiento entre los diferentes estándares trabajados se basará en la revisión de algunos artículos investigativos que se han enfocado en esta área de estudio. A continuación se presentan los principales resultados obtenidos.

2.1.5 AODV Vs OLSR

La comparación entre AODV y OLSR está basada en las pruebas y resultados obtenidos en [15], los cuales fueron encontrados utilizando diferentes topologías. Los primeros escenarios se usaron para calcular el tiempo que se tarda en el envío de pings, recalcular nuevas rutas y ver el número de paquetes perdidos. AODV se ha comportado mejor al necesitar menos tiempo para reencaminar los mensajes y como consecuencia de ello ha perdido un número menor. En la Fig. 4 se observa los resultados obtenidos y en la Fig. 5 se muestra el comportamiento del ancho de banda en función del tiempo al emplear el emulador MobiEmu.

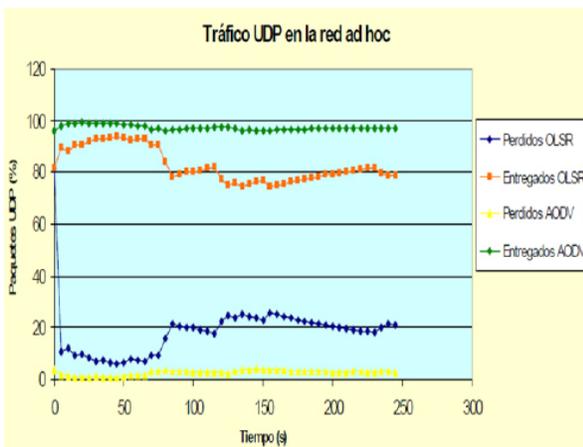


Fig. 4. Paquetes entregados y perdidos para cada protocolo [15].

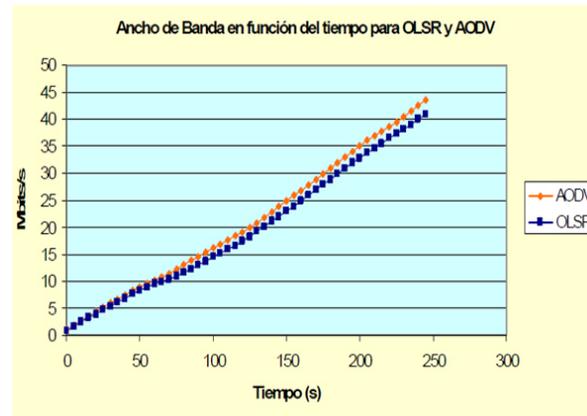


Fig. 5. Ancho de banda [15].

Se puede concluir que AODV inyecta un número menor de paquetes pero sin embargo termina por entregar un porcentaje mayor a su destino. Esto no pasa con OLSR ya que tarda más tiempo en detectar la rotura de enlaces y continúa enviando los datos por el mismo sitio congestionando los buffers. Los resultados encontrados indican que no se recomienda la utilización de OLSR para transmisiones en tiempo real que no admitan un porcentaje de pérdidas.

2.1.6 AODV Vs BATMAN

El análisis se basa en las pruebas y resultados obtenidos en [18], y apunta específicamente al caso en el que los nodos fuente y destino están en movimiento. Particularmente es el que presente mayores dificultades para mantener una conexión estable entre los diferentes nodos. En la Fig. 6, 7 y 8 se presentan los resultados arrojados.

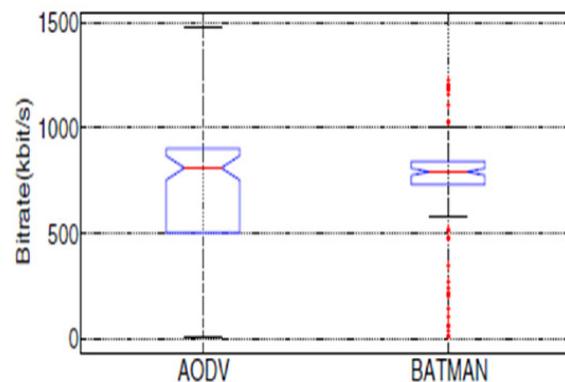


Fig. 6. Taza de Bits [18].

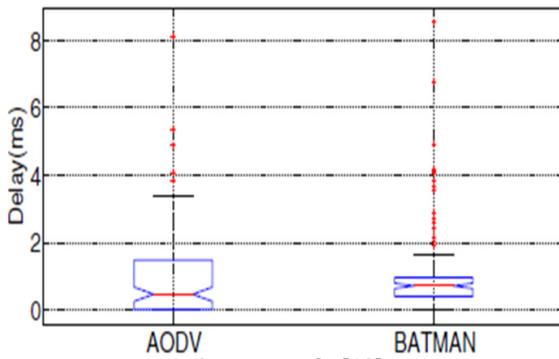


Fig. 7. Retardo [18].

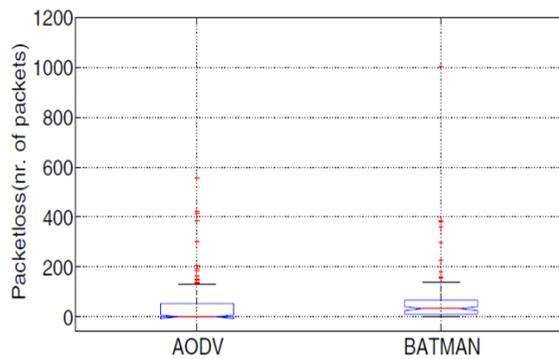


Fig. 8. Paquetes perdidos [18].

Se establece que BATMAN tiene un mejor desempeño que AODV en cuanto a la tasa de transmisión. Por otro lado se obtuvo que BATMAN muestra aunque ligero, un mejor desempeño en el retardo en comparación con AODV. Analizando la pérdida de paquetes generada por cada uno, se concluye que son muy similares.

2.2 Software y hardware

Evaluando la necesidad de evitar Software propietario que obligue a utilizar determinadas marcas o estándares privativos que aumenten los costos de implementación, se propone como firmware base de los enrutadores el sistema operativo GNU/Linux para dispositivos embebidos y enrutadores inalámbricos Openwrt [19], con las modificaciones realizadas por la fundación argentina de redes-mesh Lugro-mesh [20] en su distribución Nighthwing que incluye activo el protocolo B.AT.M.AN y scripts con opciones para disminuir al máximo el trabajo de

configuración.

El hardware se ha seleccionado tomando como base la lista de routers inalámbricos compatibles publicada en OpenWRT [21]. A continuación se evaluaron las características técnicas de los equipos (procesador, memoria flash y RAM, potencia TX, antenas y conectores, POE) y el valor económico en pesos así como la posibilidad de hallar distribuidores en el país depurando la lista a 5 dispositivos que se observan en la tabla 1.

Tabla 1. Enrutadores y sus características.

Marca/modelo	Procesador	RAM (MB)	Memoria Flash (MB)
Ubiquiti Nanostation 2	Atheros R2315	16	4
Ubiquiti Loco Station	Atheros R2315	16	4
Meraki outdoor	Atheros R2315	32	8
Airlink 102 AR430W	Atheros R2315	16	4
La Fonera 2.0	Atheros R2315	32	8

Al verificar la compatibilidad del dispositivo con el firmware de la distribución de Lugro-Mesh Nighthwing y comparar las características técnicas se selecciono el enrutador NanoStation2 de la marca Ubiquiti que es un dispositivo adecuado para uso en interiores y exteriores. Todas las características técnicas de este dispositivo se encuentran en [22], dentro de las cuales cabe resaltar:

- Procesador: Atheros AR2315 SOC, MIPS 4KC, 180 MHZ.
- Memoria: 16MB SDRAM, 4MB Flash
- Interfaz de red: 1 X 10/100 BASE-TX (Cat. 5, RJ-45) Et-hernet
- Antena: Antena Integrada + RP-SMA
- Potencia TX: 22 dBm (160 mW) ~ 26 dBm (400 mW)

3. ESTRUCTURA GENERAL

3.1 Sistema cableado

En la Fig. 9 se presenta el esquema general del sistema de video vigilancia implementado con cámaras IP cableadas. Está compuesto por cámaras IP, que se conectan a un

concentrador de una red local. El concentrador a su vez es conectado a un enrutador y posteriormente este a un modem (ADSL/Cable) que permita el acceso a internet. Configurando el sistema de esta manera es posible visualizar en directo las imágenes bien dentro de una red local, o a través de cualquier equipo conectado a Internet pudiendo estar situado en cualquier parte del mundo.

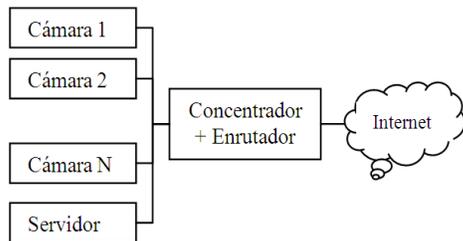


Fig. 9. Esquema general del sistema IP cableado.

3.2 Sistema con redes Mesh

Un sistema de cámaras de video vigilancia implementado con redes Mesh tiene como estructura general la encontrada en la Fig. 10.

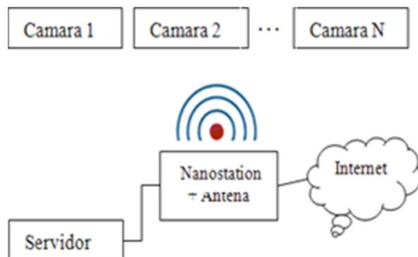


Fig. 10. Esquema general con redes Mesh.

Según el esquema el sistema, está compuesto por cámaras IP inalámbricas, que se conectan al enrutador inalámbrico gracias a la antena que éste tiene conectada con el fin de prolongar su cobertura. De igual manera al enrutador se conecta un servidor local para la visualización local y remota de las cámaras. Este sistema de igual manera al sistema cableado puede transmitir la señal de las cámaras a través de internet conectando el enrutador inalámbrico a un punto de acceso (modem) proporcionado por un proveedor de servicios de internet,

la diferencia radica en que no es necesario realizar esta conexión en cada uno de los nodos de la red gracias a la topología en malla de este tipo de redes.

4. ANALISIS COMPARATIVO

Con el fin de determinar la conveniencia y beneficios de la implementación de sistemas de video vigilancia mediante redes Mesh se realizara la comparación de esta tecnología contra sistemas tradicionales cableados teniendo en cuenta diferentes aspectos como los son costos, escalabilidad y la facilidad de acceso a cada una de las tecnologías.

4.1 Costos

En la tabla 2 se relaciona el listado de equipos necesarios y su correspondiente valor para la instalación de un sistema cableado de cámaras IP que cubran un área de 3 X 2 manzanas con una longitud promedio de 100 metros.

Tabla 2. Equipos y costos sistema cableado.

CANT	ARTICULO	Vr Unitario	Vr Total
34	camara IP con PoE	200000	6800000
6	Switch	150000	900000
6	Router	250000	1500000
6	PC - servidor	500000	3000000
12	Carreta cable utp cat 5e	250000	3000000
6	monitor 19"	218000	1308000
92	conectores RJ45	500	46000
6	UPS de 1000 vA	260000	1560000
TOTAL EQUIPOS			18114000

De igual manera en la tabla 3 se relacionan los equipos necesarios para cubrir un área de igual envergadura con un sistema de cámaras de video vigilancia por medio de redes mesh.

Tabla 3. Equipos y costos sistema inalámbrico.

CANT	ARTICULO	Vr unitario	Vr Total
34	camara Wifi con PoE	200000	6800000
4	Antena 15 dBi	150000	600000
4	Nanoestation 2 con PoE	200000	800000
6	PC - servidor	500000	3000000
1	Carreta cable Ftp Ext.	400000	400000
6	monitor 19"	218000	1308000
4	Pigtail LMR 400	40000	160000
6	UPS de 1000 vA	260000	1560000
TOTAL EQUIPOS			14628000

A primera vista se concluye que en términos de costos, es mejor opción el sistema

implementado con redes Mesh. No obstante, en este análisis no se tiene en cuenta otros aspectos muy importantes, como lo son los gastos asociados a instalación y administración.

Teniendo en cuanto lo anteriormente expuesto y realizando un análisis superficial se puede afirmar que los sobrecostos de instalación tienden a ser superiores en el sistema cableado, esto debido a la necesidad de tender tantos metros de cableado para la conexión de las cámaras. A nivel de administración los gastos en las redes cableadas son más elevados, gracias a la misma arquitectura del sistema ya que para permitir la interconexión de los distintos nodos y su acceso a internet es necesario tener un punto de acceso ofrecido por un ISP en cada uno de los dispositivos del sistema lo que se traduce en mayores cambios, en cambio en el sistema con redes Mesh simplemente sería necesario un punto de acceso.

4.2 Escalabilidad

Analizando las características propias de las redes Mesh, entre las que cabe mencionar su dinamismo, este tipo de estructuras facilita la salida e ingreso de usuarios al sistema, lo que permite a la vez la entrada sin inconvenientes de nuevos nodos con el fin de brindar acceso a más usuarios. Por otro lado y al contrario de lo que ocurre en las redes cableadas, en las redes Mesh el número de usuarios que se puedan conectar a la red, no depende del número de cables físicos que se tengan, por lo tanto un usuario puede conectarse a ella simplemente con estar en el rango de cobertura de alguno de sus nodos y sin la necesidad de ninguna infraestructura previa.

4.3 Facilidad de acceso

En cuanto a la facilidad de acceso por parte de la población en general se puede afirmar que las redes en malla son una excelente opción, esto gracias a su naturaleza

propia, las cuales buscan la creación de redes abiertas, libres, comunitarias, descentralizadas, independientes y autónomas que provean las herramientas y la estructura tecnológica para la implementación de diferentes proyectos de carácter comunitario y social.

5. CONCLUSIONES

Disponer de sistemas de comunicación y vigilancia a través de redes inalámbricas en malla con alta confiabilidad y fácil despliegue fue el inicio de las redes en malla, no extraña que su inicio sea en la Agencia de Investigación de Proyectos Avanzados de Defensa (DARPA), lo cual es un antecedente muy importante para la elección de esta infraestructura en proyectos de video vigilancia en comunidades marginadas de la ciudad de Bogotá.

Después de comparar y evaluar los protocolos seleccionados en este artículo, se puede evidenciar que BATMAN requiere menos consumo de procesamiento de CPU, sin disminuir sus niveles de estabilidad permitiendo usar dispositivos de comunicación inalámbrica de menores prestaciones técnicas disminuyendo sus costos.

Las redes inalámbricas en malla ofrecen un acceso simple y fácil a la network, dado que cualquier usuario con un dispositivo móvil dentro de la cobertura de la red es capaz de conectarse a ella, sin la necesidad de disponer de una infraestructura previa. Desde este punto se puede afirmar que las redes en malla ofrecen mayor disponibilidad de acceso.

6. AGRADECIMIENTOS

Se destaca el agradecimiento a los proyectos de redes inalámbricas libres Bogotá-mesh y al proyecto argentino Lugro-mesh quienes nos proporcionaron mucha información técnica sobre el hardware y el firmware necesarios para la implementación de redes Mesh.

Referencias Bibliográficas

- [1] Sevilla Mesh, “Orígenes de las redes Mesh: redes MANET y expansión de Wi-Fi”, [en línea]. Consultado en Marzo 7 de 2010, disponible en <https://sevillamesh.wordpress.com>.
- [2] L. Pedraza, J. González, Diseño e implementación de un prototipo de sistema de monitoreo para los equipos de laboratorio mediante RFID, Universidad Nacional de Colombia, Facultad de ingeniería, Bogotá, 2010
- [3] Wi-Fi 802.11s per le reti ibride, [en línea]. Consultado en Marzo 20 de 2010, disponible en <http://blog.skydiamond.org/linux/wifi-80211s-per-le-reti-ibride/>
- [4] N. Bayer, A. Ross, R. Karrer, B. Xu, C. Esteve, Towards carrier grade wireless Mesh networks for broadband access, proc, First IEEE international workshop on operator-assisted (wireless Mesh) community networks 2006 (OPCOMM '06), Berlin, Germany, September 2006.
- [5] E. Copas, P. Lizondo, M. Savoy, Wireless Mesh networks: estudio, diseño y aplicaciones, [en línea]. Consultado en Enero 21 de 2010, disponible en www.frfsf.utn.edu.ar/cneisi2010/archivos/33-WMN_estudio_dise%C3%B1o_y_aplicaciones.pdf
- [6] F. Licandro, G. Schembra, Wireless Mesh Networks to Support Video Surveillance: Architecture, Protocol, and Implementation Issues”, Hindawi Publishing Corporation EURASIP Journal on Wireless Communications and Networking, Volume 2007.
- [7] Aruba wireless mesh network supports video surveillance system at Lakewood Center mall, [en línea]. Consultado en Febrero 10 de 2010, disponible en <http://www.arubanetworks.com>.
- [8] Página oficial, [en línea]. Consultado en Enero 7 de 2010, disponible en: <http://www.freifunk.net>
- [9] Página oficial, Página oficial, [en línea]. Consultado en Enero 7 de 2010, disponible en: <http://cuwireless.net/>
- [10] Página oficial, Página oficial, [en línea]. Consultado en Enero 7 de 2010, disponible en: <http://www.bogota-mesh.org>
- [11] B. Gómez, Javier Maimo, Juan Merideño, “Wireless Mesh Networks”, Universidad de las Islas Baleares, Ingeniería Informática, 2010.
- [12] D. de Couto, Performance of multihop wireless networks: shortest path is not enough”, ACM SIGCOMM computer communication review, Vol. 33, N. 1, Enero de 2003.
- [13] J. Simón, P. Osuna, J. Seoane, A. Martínez, Enrutador solar auto configurable para redes Mesh, IEEE 802.11 de telemedicina rural en América Latina, Universidad politécnica de Madrid, 2010.
- [14] J. Broch, D. Maltz, D. Johnson, Y. Hu, J. Jetcheva, A performance comparison of multi-hop wireless ad hoc network routing protocols”, MobiCom98 4th Annual ACM international conference on mobile computing and networking, Octubre de 1998.
- [15] A. Santos, Comparativa de los protocolos AODV y OLSR con un emulador de redes Ad-Hoc”, Universidad Politécnica de Cataluña, Facultad de Ingeniería, 2006.
- [16] Batman-adv, Página oficial, [en línea]. Consultado en Diciembre de 2010, disponible en: <http://www.open-mesh.org/wiki/open-mesh/2010-04-18-batman-adv-2010-1-0-release>
- [17] A. Neuman, C. Aichele, M. Lindner, Better Approach To Mobile Ad-hoc Networking (B.A.T.M.A.N.) draft-wunderlich-openmesh-manet-routing Página oficial, [en línea]. Consultado en Enero 7 de 2010, disponible en: <http://tools.ietf.org/html/draft-underlichopenmesh-manet-routing-00>
- [18] L. Barolli, E. Kula, M. Ikeda, R. Miho,

- Impact of source and destination movement on MANET performance considering BATMAN and AODV protocols, International conference on broadband, wireless computing, communication and applications, 2010.
- [19] Pagina oficial open WRT, [en línea]. Consultado en Enero 7 de 2010, disponible en: <https://www.openwrt.org>
- [20] Pagina oficial Lugro-Mesh, [en línea]. Consultado en Enero 10 de 2010, disponible en: <http://www.lugro-mesh.org>
- [21] Complete table of hardware, Página oficial, [en línea]. Consultado en Febrero 10 de 2010, disponible en: <http://wiki.openwrt.org/oldwiki/completetableofhardware>
- [22] Ubiquiti Networks, Nanostation2 datasheet, [en línea]. Consultado en Febrero 14 de 2010, disponible en: http://www.ubnt.com/downloads/ns2_datasheet.pdf